
Elastic Load Balancing

Network Load Balancers



Elastic Load Balancing: Network Load Balancers

Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Network Load Balancer란 무엇입니까?	1
Network Load Balancer 구성 요소	1
Network Load Balancer 개요	1
Classic Load Balancer에서 마이그레이션하는 것의 이점	2
시작하는 방법	2
요금	2
시작하기	3
시작하기 전	3
1단계: 로드 밸런서 유형 선택	3
2단계 로드 밸런서 및 리스너 구성	3
3단계: 대상 그룹 구성	4
4단계: 대상 그룹에 대상 등록	4
5단계: 로드 밸런서 생성 및 테스트	4
6단계: 로드 밸런서 삭제(선택 사항)	5
자습서: AWS CLI를 사용하여 Network Load Balancer 생성	6
시작하기 전	6
로드 밸런서 생성	6
로드 밸런서의 탄력적 IP 주소 지정	7
포트 재정의를 사용하여 대상 추가	7
로드 밸런서 삭제	8
로드 밸런서	9
로드 밸런서 상태	9
로드 밸런서 속성	9
가용 영역	10
교차 영역 로드 밸런싱	10
삭제 방지	10
유휴 연결 제한 시간	11
로드 밸런서 생성	11
1단계: 로드 밸런서 및 리스너 구성	3
2단계: 대상 그룹 구성	4
3단계: 대상 그룹에 대상 등록	12
4단계: 로드 밸런서 생성	13
태그 업데이트	13
로드 밸런서 삭제	14
리스너	15
리스너 구성	15
리스너 규칙	15
리스너 생성	15
사전 조건	15
리스너 추가	15
리스너 업데이트	16
리스너 삭제	16
대상 그룹	17
라우팅 구성	17
대상 유형	17
라우팅 및 IP 주소 요청	18
원본 IP 보존	18
등록된 대상	18
대상 그룹 속성	19
등록 취소 지연	19
프록시 프로토콜	20
상태 확인 연결	20
VPC 엔드포인트 서비스	20
프록시 프로토콜 활성화	20

대상 그룹 생성	21
상태 확인 구성	21
상태 확인 설정	22
대상 상태	23
상태 확인 사유 코드	23
대상의 상태 확인	24
대상 그룹의 상태 설정 변경	24
대상 등록	25
대상 보안 그룹	25
대상 및 인터넷 경계 로드 밸런서	26
네트워크 ACL	26
대상 등록 또는 등록 취소	26
태그 업데이트	27
대상 그룹 삭제	28
로드 밸런서 모니터링	29
CloudWatch 지표	29
네트워크 로드 밸런서 측정치	30
네트워크 로드 밸런서의 측정치 차원	30
Network Load Balancer 지표에 대한 통계	31
로드 밸런서를 위한 CloudWatch 지표 보기	31
CloudTrail 로그	32
CloudTrail의 Elastic Load Balancing 정보	33
Elastic Load Balancing 로그 파일 항목 이해	33
문제 해결	36
등록된 대상은 서비스되지 않고 있습니다.	36
요청이 대상으로 라우팅되지 않음	36
대상이 예상보다 많은 상태 확인 요청을 수신함	37
대상이 예상보다 적은 상태 확인 요청을 수신함	37
비정상 대상이 로드 밸런서로부터 요청을 수신	37
대상에서 로드 밸런서로의 요청에서 연결이 시간 초과됨	37
대상을 Network Load Balancer로 이동할 때 성능이 저하됨	37
제한	38
문서 기록	39

Network Load Balancer란 무엇입니까?

Elastic Load Balancing는 다음 유형의 로드 밸런서를 지원합니다. Application Load Balancers, Network Load Balancers, Classic Load Balancers. 이 안내서는 Network Load Balancers에 대해 설명합니다. 다른 로드 밸런서에 대한 자세한 내용은 [User Guide for Application Load Balancers](#) 및 [User Guide for Classic Load Balancers](#)를 참조하십시오.

Network Load Balancer 구성 요소

로드 밸런서는 클라이언트에 대한 단일 점점 역할을 수행합니다. 로드 밸런서는 수신 트래픽을 Amazon EC2 인스턴스와 같은 다수 대상으로 분산합니다. 이렇게 하면 애플리케이션의 가용성이 향상됩니다. 로드 밸런서에 하나 이상의 리스너를 추가할 수 있습니다.

리스너는 사용자가 구성한 프로토콜과 포트를 사용하여 클라이언트의 연결 요청을 확인하고, 요청을 대상 그룹으로 전달합니다.

각 대상 그룹은 지정된 TCP 프로토콜과 포트 번호를 사용하여 EC2 인스턴스 같은 하나 이상의 등록된 대상으로 요청을 라우팅합니다. 여러 대상 그룹에 대상을 등록할 수 있습니다. 대상 그룹 기준으로 상태 확인을 구성할 수 있습니다. 로드 밸런서의 리스너 규칙에서 지정된 대상 그룹에 등록된 모든 대상에서 상태 검사가 수행됩니다.

자세한 내용은 다음 문서(들)를 참조하십시오.

- [로드 밸런서 \(p. 9\)](#)
- [리스너 \(p. 15\)](#)
- [대상 그룹 \(p. 17\)](#)

Network Load Balancer 개요

Network Load Balancer는 개방형 시스템 간 상호 연결(OSI) 모델의 네 번째 계층에서 작동합니다. 초당 수백만 개의 요청을 처리할 수 있습니다. 로드 밸런서가 연결 요청을 받으면 기본 규칙의 대상 그룹에서 대상을 선택합니다. 리스너 구성에 지정된 포트에서 선택한 대상에 대한 TCP 연결을 열려고 시도합니다.

로드 밸런서에서 가용 영역을 활성화하면 Elastic Load Balancing이 해당 가용 영역에서 로드 밸런서 노드를 생성합니다. 기본적으로 각 로드 밸런서 노드는 해당 가용 영역의 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 활성화하면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 대상 간에 트래픽을 분산합니다. 자세한 내용은 Elastic Load Balancing User Guide의 [교차 영역 로드 밸런싱](#)을 참조하십시오.

로드 밸런서에 대해 여러 가용 영역을 활성화하고 각 대상 그룹에 각 활성화된 가용 영역에 하나 이상의 대상이 있는지 확인하면 응용 프로그램의 내결함성이 향상됩니다. 예를 들어, 하나 이상의 대상 그룹이 가용성 영역에서 정상 대상이 없는 경우 DNS에서 해당 서브넷의 IP 주소를 제거하지만 다른 가용 영역의 로드 밸런서 노드는 여전히 트래픽을 라우팅할 수 있습니다. 클라이언트가 TTL(time-to-live)을 인식하지 못하고 DNS에서 제거된 IP 주소로 요청을 보내면 요청이 실패합니다.

로드 밸런서 노드는 프로토콜, 원본 IP 주소, 원본 포트, 대상 IP 주소, 대상 포트, TCP 시퀀스 번호에 따라 흐름 해시 알고리즘을 사용하여 대상을 선택합니다. 클라이언트로부터의 TCP 연결은 소스 포트와 시퀀스 번호가 서로 다르므로 다른 대상에 라우팅될 수 있습니다. 각 TCP 연결은 연결 수명 동안 하나의 대상에 라우팅됩니다.

Elastic Load Balancing은 사용자가 활성화하는 각 가용 영역에 대해 네트워크 인터페이스를 만듭니다. 가용 영역의 각 로드 밸런서 노드는 이 네트워크 인터페이스를 사용하여 고정 IP 주소를 가져옵니다. 인터넷 경계 로드 밸런서를 생성하는 경우 필요에 따라 서브넷당 하나의 탄력적 IP 주소를 연결할 수 있습니다.

인스턴스 ID 또는 IP 주소로 대상을 등록하도록 대상 그룹을 구성할 수 있습니다. 인스턴스 ID를 사용하여 대상을 지정하는 경우 클라이언트의 원본 IP 주소가 보존되고 애플리케이션에 제공됩니다. IP 주소로 대상을 지정하는 경우 원본 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다.

애플리케이션에 대한 요청의 전체적인 흐름을 방해하지 않고 필요에 따라 로드 밸런서에서 대상을 추가 및 제거할 수 있습니다. 애플리케이션에 대한 트래픽이 시간에 따라 변화하므로 Elastic Load Balancing이 로드 밸런서를 자동으로 확장합니다. Elastic Load Balancing은 대다수의 워크로드에 자동으로 확장될 수 있습니다.

로드 밸런서가 정상적인 대상에만 요청을 보낼 수 있도록 등록된 대상의 상태를 모니터링하는 데 사용되는 상태 확인을 구성할 수 있습니다.

자세한 내용은 Elastic Load Balancing User Guide의 [How Elastic Load Balancing Works](#)를 참조하십시오.

Classic Load Balancer에서 마이그레이션하는 것의 이점

Classic Load Balancer 대신 Network Load Balancer를 사용하면 다음과 같은 이점이 있습니다.

- 일시적 워크로드를 처리하고 초당 수백만 개의 요청으로 확장할 수 있습니다.
- 로드 밸런서에 고정 IP 주소를 지원합니다. 또한 로드 밸런서에 대해 활성화된 서브넷당 하나의 탄력적 IP 주소를 할당할 수 있습니다.
- 로드 밸런서의 VPC 외부 대상을 포함하여 IP 주소로 대상을 등록하는 것을 지원합니다.
- 단일 EC2 인스턴스의 여러 애플리케이션으로 요청을 라우팅하는 것을 지원합니다. 여러 포트를 사용하여 각 인스턴스 또는 IP 주소를 동일한 대상 그룹에 등록할 수 있습니다.
- 컨테이너화된 애플리케이션을 지원합니다. Amazon Elastic Container Service(Amazon ECS)는 작업을 예약할 때 사용하지 않는 포트를 선택하고, 이 포트를 사용하여 대상 그룹에 작업을 등록할 수 있습니다. 이를 통해 클러스터를 효율적으로 사용할 수 있습니다.
- 대상 그룹 수준에서 상태 확인이 정의되고 많은 Amazon CloudWatch 지표가 보고되므로 각 서비스의 상태를 독립적으로 모니터링할 수 있게 지원합니다. Auto Scaling 그룹에 대상 그룹을 연결하면 필요에 따라 동적으로 각 서비스를 확장할 수 있습니다.

각 로드 밸런서 유형에서 지원하는 기능에 대한 자세한 내용은 [Elastic Load Balancing 제품 비교](#)를 참조하십시오.

시작하는 방법

Network Load Balancer를 생성하려면 다음 자습서 중 하나를 시도해 보십시오.

- [Network Load Balancers 시작하기 \(p. 3\)](#)
- [자습서: AWS CLI를 사용하여 Network Load Balancer 생성 \(p. 6\)](#)

요금

자세한 내용은 [Network Load Balancer 요금](#)을 참조하십시오.

Network Load Balancers 시작하기

이 자습서에서는 웹 기반 인터페이스인 AWS Management Console을 통해 Network Load Balancers에 대한 실습 소개를 제공합니다. 첫 번째 Network Load Balancer를 생성하려면 다음 단계를 완료하십시오.

작업

- 시작하기 전 (p. 3)
- 1단계: 로드 밸런서 유형 선택 (p. 3)
- 2단계 로드 밸런서 및 리스너 구성 (p. 3)
- 3단계: 대상 그룹 구성 (p. 4)
- 4단계: 대상 그룹에 대상 등록 (p. 4)
- 5단계: 로드 밸런서 생성 및 테스트 (p. 4)
- 6단계: 로드 밸런서 삭제(선택 사항) (p. 5)

또는 Application Load Balancer를 생성하려면 User Guide for Application Load Balancers의 [Application Load Balancers 시작하기](#)를 참조하십시오. Classic Load Balancer를 생성하려면 User Guide for Classic Load Balancers의 [Classic Load Balancer 생성](#)을 참조하십시오.

시작하기 전

- EC2 인스턴스에 대해 사용할 가용 영역을 결정합니다. 각 가용 영역에 있는 하나 이상의 퍼블릭 서브넷으로 VPC(Virtual Private Cloud)를 구성합니다. 이 퍼블릭 서브넷은 로드 밸런서를 구성하는데 사용됩니다. 대신 이러한 가용 영역의 다른 서브넷에서 EC2 인스턴스를 시작할 수 있습니다.
- 각 가용 영역에서 하나 이상의 EC2 인스턴스를 시작합니다. 이러한 인스턴스에 대한 보안 그룹이 리스너 포트에서 클라이언트로부터의 TCP 액세스와 VPC의 상태 확인 요청을 허용하는지 확인합니다. 자세한 내용은 [대상 보안 그룹 \(p. 25\)](#) 단원을 참조하십시오.

1단계: 로드 밸런서 유형 선택

Elastic Load Balancing은 세 가지 로드 밸런서 유형을 지원합니다. 이 자습서에서는 Network Load Balancer를 생성합니다.

Network Load Balancer를 생성하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 모음에서 로드 밸런서의 리전을 선택합니다. EC2 인스턴스에 사용한 리전과 동일한 리전을 선택해야 합니다.
3. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
4. Create Load Balancer를 선택합니다.
5. [Network Load Balancer]에서 [Create]를 선택합니다.

2단계 로드 밸런서 및 리스너 구성

[Configure Load Balancer] 페이지에서 다음 절차를 완료합니다.

로드 밸런서 및 리스너를 구성하려면

1. Name에 로드 밸런서 이름을 입력합니다.
Network Load Balancer의 이름은 해당 리전의 Application Load Balancers 및 Network Load Balancers 내에서 고유한 이름이어야 하고, 최대 32자여야 하며, 알파벳 문자 및 하이픈만 포함해야 하고, 하이픈으로 시작하거나 끝나지 않아야 하며 "internal-"로 시작하지 않아야 합니다.
2. [Scheme]의 [internet-facing]은 기본 값으로 유지합니다.
3. 포트 80에서 TCP 트래픽을 수락하는 리스너를 뜻하는 [Listeners]는 기본 값으로 유지합니다.
4. [Availability Zones]에서 EC2 인스턴스에 사용한 VPC를 선택합니다. EC2 인스턴스를 시작할 때 사용한 각 가용 영역에서 가용 영역을 선택한 후 해당 가용 영역에 대한 퍼블릭 서브넷을 선택합니다.
인터넷 경계 로드 밸런서를 생성하는 경우 필요에 따라 [Elastic IP]에서 탄력적 IP 주소를 선택할 수 있습니다. 그러면 로드 밸런서 노드에 정적 IPv4 주소가 제공됩니다.
5. [Next: Configure Routing]을 선택합니다.

3단계: 대상 그룹 구성

라우팅 요청에서 사용되는 대상 그룹을 만듭니다. 리스너의 규칙은 이 대상 그룹에 등록된 대상으로 요청을 라우팅합니다. 로드 밸런서는 해당 대상 그룹에 대해 정의된 상태 확인 설정을 사용하여 이 대상 그룹의 대상 상태를 확인합니다. [Configure Routing] 페이지에서 다음 절차를 완료합니다.

대상 그룹을 구성하려면

1. Target group에서는 기본 값인 [New target group]을 유지합니다.
2. Name에 새 대상 그룹의 이름을 입력합니다.
3. [Protocol]을 TCP로, [Port]를 80으로 [Target type]을 인스턴스로 유지합니다.
4. [Health checks]에서 기본 프로토콜을 유지합니다.
5. Next: Register Targets를 선택합니다.

4단계: 대상 그룹에 대상 등록

[Register Targets] 페이지에서 다음 절차를 완료합니다.

대상 그룹에 대상을 등록하려면

1. [Instances]에서 인스턴스를 하나 이상 선택합니다.
2. 기본 포트를 80으로 유지하고 [Add to registered]를 선택합니다.
3. 인스턴스 선택을 마치면 [Next: Review]를 선택합니다.

5단계: 로드 밸런서 생성 및 테스트

로드 밸런서를 생성하기 전에 설정을 검토합니다. 로드 밸런서를 생성한 후에는 EC2 인스턴스에 트래픽을 전송하고 있는지 확인할 수 있습니다.

로드 밸런서를 생성 및 확인하려면

1. [Review] 페이지에서 [Create]을 선택합니다.
2. 로드 밸런서가 생성되었다는 통보를 받은 후 [Close]를 선택합니다.

3. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
4. 새로 생성한 대상 그룹을 선택합니다.
5. [Targets]를 선택하고 인스턴스가 준비되었는지 확인합니다. 인스턴스 상태가 `initial`인 경우 아직 인스턴스 등록이 진행 중이거나 정상으로 간주될 만한 최소 상태 확인 횟수를 통과하지 못했기 때문일 가능성이 높습니다. 하나 이상의 인스턴스 상태가 `healthy`여야 로드 밸런서를 테스트할 수 있습니다.
6. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
7. 새로 생성한 로드 밸런서를 선택합니다.
8. [Description]을 선택하고, 로드 밸런서의 DNS 이름(예: `my-load-balancer-1234567890.us-west-2.elb.amazonaws.com`)을 복사합니다. DNS 이름을 인터넷에 연결된 웹 브라우저의 주소 필드에 붙여넣습니다. 모든 것이 잘 작동하는 경우 브라우저에 서버 기본 페이지가 표시됩니다.

6단계: 로드 밸런서 삭제(선택 사항)

로드 밸런서를 사용할 수 있는 순간부터 실행이 지속되는 매 시간 단위 또는 60분 미만의 시간 단위로 비용이 청구됩니다. 더 이상 로드 밸런서가 필요 없을 때는 이를 삭제할 수 있습니다. 로드 밸런서가 삭제되면 그 즉시 요금 발생이 중지됩니다. 로드 밸런서를 삭제해도 로드 밸런서에 등록된 대상에는 영향을 미치지 않습니다. 예를 들어 EC2 인스턴스는 계속 실행됩니다.

로드 밸런서를 삭제하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Actions], [Delete]를 차례로 선택합니다.
4. 확인 메시지가 나타나면 [Yes, Delete]를 선택합니다.

자습서: AWS CLI를 사용하여 Network Load Balancer 생성

이 자습서에서는 AWS CLI를 통해 Network Load Balancers에 대한 실습 소개를 제공합니다.

시작하기 전

- Network Load Balancers를 지원하지 않는 버전을 사용하는 경우 AWS CLI를 설치하거나 최신 버전의 AWS CLI로 업데이트합니다. 자세한 내용은 AWS Command Line Interface User Guide의 [AWS 명령줄 인터페이스 설치](#)를 참조하십시오.
- EC2 인스턴스에 대해 사용할 가용 영역을 결정합니다. 각 가용 영역에 있는 하나 이상의 퍼블릭 서브넷으로 VPC(Virtual Private Cloud)를 구성합니다.
- 각 가용 영역에서 하나 이상의 EC2 인스턴스를 시작합니다. 이러한 인스턴스에 대한 보안 그룹이 리스너 포트에서 클라이언트로부터의 TCP 액세스와 VPC의 상태 확인 요청을 허용하는지 확인합니다. 자세한 내용은 [대상 보안 그룹 \(p. 25\)](#) 단원을 참조하십시오.

로드 밸런서 생성

첫 번째 로드 밸런서를 생성하려면 다음 단계를 완료합니다.

로드 밸런서를 생성하려면

1. `create-load-balancer` 명령을 사용하여 로드 밸런서를 만들고, 인스턴스를 실행한 가용 영역 각각에 대해 퍼블릭 서브넷을 지정합니다. 가용 영역당 1개의 서브넷만 지정할 수 있습니다.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets subnet-12345678
```

출력에는 다음 형식과 함께 로드 밸런서의 Amazon 리소스 이름(ARN)이 포함됩니다.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/net/my-load-balancer/1234567890123456
```

2. `create-target-group` 명령을 사용하여 대상 그룹을 만들고 EC2 인스턴스에 사용한 VPC와 동일한 VPC를 지정합니다.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id vpc-12345678
```

출력에는 다음 형식과 함께 대상 그룹의 ARN이 포함됩니다.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/1234567890123456
```

3. 다음과 같이 `register-targets` 명령을 사용하여 인스턴스를 대상 그룹에 등록합니다.

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets Id=i-12345678  
Id=i-23456789
```

- 다음과 같이 `create-listener` 명령을 사용하여 요청을 대상 그룹에 전달하는 기본 규칙이 있는 로드 밸런서에 대한 하나 이상의 리스너를 생성합니다.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --port 80  
\  
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

출력에는 다음 형식과 함께 리스너의 ARN이 포함됩니다.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/net/my-load-  
balancer/1234567890123456/1234567890123456
```

- (선택 사항) 다음과 같이 이 `describe-target-health` 명령을 사용하여 대상 그룹에 등록된 대상의 상태를 확인할 수 있습니다.

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

로드 밸런서의 탄력적 IP 주소 지정

Network Load Balancer를 생성할 때 서브넷 매핑을 사용하여 서브넷당 하나의 탄력적 IP 주소를 지정할 수 있습니다.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \  
--subnet-mappings SubnetId=subnet-12345678,AllocationId=eipalloc-12345678
```

포트 재정의를 사용하여 대상 추가

단일 인스턴스에 여러 서비스가 있는 마이크로서비스 아키텍처가 있는 경우, 각 서비스는 서로 다른 포트에서 연결을 허용합니다. 매번 다른 포트를 사용하여 대상 그룹에 인스턴스를 여러 번 등록할 수 있습니다.

포트 재정의를 사용하여 대상을 추가하려면

- 다음과 같이 `create-target-group` 명령을 사용하여 대상 그룹을 만듭니다.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 \  
--vpc-id vpc-12345678
```

- 다음과 같이 `register-targets` 명령을 사용하여 인스턴스를 대상 그룹에 등록합니다. 각 컨테이너마다 인스턴스 ID가 동일하지만 포트는 서로 다릅니다.

```
aws elbv2 register-targets --target-group-arn targetgroup-arn \  
--targets Id=i-12345678,Port=80 Id=i-12345678,Port=766
```

- 다음과 같이 `create-listener` 명령을 사용하여 요청을 대상 그룹에 전달하는 기본 규칙이 있는 로드 밸런서에 대한 하나 이상의 리스너를 생성합니다.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \  
--protocol TCP --port 80 \  
\
```

```
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

로드 밸런서 삭제

더 이상 로드 밸런서 및 대상 그룹이 필요하지 않으면 다음과 같이 삭제할 수 있습니다.

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn  
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Network Load Balancers

로드 밸런서는 클라이언트에 대한 단일 접점 역할을 수행합니다. 클라이언트는 로드 밸런서에 요청을 전송하고 로드 밸런서는 하나 이상의 가용 영역에 있는 EC2 인스턴스 같은 대상으로 이를 전송합니다.

로드 밸런서를 구성하려는 경우, [대상 그룹 \(p. 17\)](#)을 생성한 다음 대상을 해당 대상 그룹에 등록합니다. 활성화된 각 가용 영역에 등록된 대상이 하나 이상 있는지 확인하는 경우에 로드 밸런서가 가장 효과적입니다. [리스너 \(p. 15\)](#)를 생성하여 클라이언트의 연결 요청을 확인하고, 클라이언트에서 대상 그룹에 있는 대상으로 요청을 라우팅합니다.

해당 클라이언트가 C5, i3.metal, R5, R5D, M5 또는 Z1D 인스턴스가 아닌 한, Network Load Balancers는 리전 내 VPC 피어링을 통한 클라이언트에서 로드 밸런서로의 연결을 지원합니다. Network Load Balancers는 리전 내 VPC 피어링 또는 AWS 관리형 VPN을 통한 클라이언트에서 로드 밸런서로의 연결을 지원하지 않습니다.

목차

- [로드 밸런서 상태 \(p. 9\)](#)
- [로드 밸런서 속성 \(p. 9\)](#)
- [가용 영역 \(p. 10\)](#)
- [삭제 방지 \(p. 10\)](#)
- [유휴 연결 제한 시간 \(p. 11\)](#)
- [Network Load Balancer 생성 \(p. 11\)](#)
- [Network Load Balancer 태그 \(p. 13\)](#)
- [Network Load Balancer 삭제 \(p. 14\)](#)

로드 밸런서 상태

로드 밸런서는 다음 중 하나의 상태일 수 있습니다.

provisioning

로드 밸런서를 설정하는 중입니다.

active

로드 밸런서가 완전히 설정되어 트래픽을 라우팅할 준비가 되었습니다.

failed

로드 밸런서를 설정할 수 없습니다.

로드 밸런서 속성

다음은 로드 밸런서의 속성입니다.

deletion_protection.enabled

삭제 방지 기능의 활성화 여부를 나타냅니다. 기본값은 `false`입니다.

```
load_balancing.cross_zone.enabled
```

교차 영역 로드 밸런싱의 활성화 여부를 나타냅니다. 기본값은 `false`입니다.

가용 영역

로드 밸런서를 생성할 때 하나 이상의 가용 영역을 활성화합니다. 생성한 후에는 Network Load Balancer의 가용 영역을 활성화하거나 비활성화할 수 없습니다. 로드 밸런서에서 가용 영역을 여러 개 활성화하면 애플리케이션의 내결함성이 높아집니다.

가용 영역을 활성화할 때 해당 가용 영역에서 서브넷을 하나 지정합니다. 서브넷에는 최소 8개의 사용 가능한 IP 주소가 있어야 합니다. Elastic Load Balancing은 가용 영역에 로드 밸런서 노드를 생성하고 서브넷의 네트워크 인터페이스를 만듭니다(설명은 "ELB net"으로 시작하며 로드 밸런서의 이름이 포함됨). 가용 영역의 각 로드 밸런서 노드는 이 네트워크 인터페이스를 사용하여 고정 IP 주소를 가져옵니다. 이 네트워크 인터페이스를 볼 수 있으나 수정할 수는 없습니다.

인터넷 경계 로드 밸런서를 생성하는 경우 필요에 따라 서브넷당 하나의 탄력적 IP 주소를 연결할 수 있습니다. 로드 밸런서를 생성한 후에는 서브넷의 탄력적 IP 주소를 추가하거나 변경할 수 없습니다.

교차 영역 로드 밸런싱

기본적으로 각 로드 밸런서 노드는 해당 가용 영역의 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 활성화하면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 대상 간에 트래픽을 분산합니다. 자세한 내용은 Elastic Load Balancing User Guide의 [교차 영역 로드 밸런싱](#)을 참조하십시오.

콘솔을 사용하여 교차 영역 로드 밸런싱을 활성화하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. 로드 밸런서 속성 편집 페이지에서 교차 영역 로드 밸런싱에 대해 활성화를 선택하고 저장을 선택합니다.

AWS CLI를 사용하여 교차 영역 로드 밸런싱을 활성화하려면

`load_balancing.cross_zone.enabled` 속성과 함께 `modify-load-balancer-attributes` 명령을 사용합니다.

삭제 방지

로드 밸런서가 실수로 삭제되지 않도록 방지하려면, 삭제 방지 기능을 활성화할 수 있습니다. 기본 설정상 로드 밸런서에 대한 삭제 방지 기능은 비활성화되어 있습니다.

로드 밸런서용 삭제 방지 기능을 활성화하는 경우 로드 밸런서를 삭제하기 전에 이 기능을 먼저 비활성화해야 합니다.

콘솔을 사용하여 삭제 방지 기능을 활성화하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.

3. 로드 밸런서를 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. 로드 밸런서 속성 편집 페이지에서 삭제 보호에 대해 활성화를 선택하고 저장을 선택합니다.

콘솔을 사용하여 삭제 방지 기능을 비활성화하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. [Edit load balancer attributes] 페이지에서 [Enable delete protection]을 취소하고 [Save]를 선택합니다.

AWS CLI를 사용하여 삭제 방지 기능을 활성화 또는 비활성화하려면

`deletion_protection.enabled` 속성과 함께 `modify-load-balancer-attributes` 명령을 사용합니다.

유휴 연결 제한 시간

클라이언트가 네트워크 로드 밸런서를 통해 생성하는 각 요청에 대해 연결 상태는 추적됩니다. 대상별로 연결이 종료됩니다. 유휴 제한 시간보다 오래 클라이언트 또는 대상에 의한 연결을 통해 데이터가 전송되지 않으면 연결이 닫힙니다. 유휴 제한 시간이 지난 후 클라이언트에서 데이터를 보내면 연결이 더 이상 유효하지 않음을 나타내는 TCP RST 패킷이 수신됩니다.

Elastic Load Balancing은 유휴 제한 시간을 350초로 설정합니다. 이 값은 수정할 수 없습니다. 대상은 TCP keepalive 패킷을 사용하여 유휴 제한 시간을 리셋할 수 있습니다.

Network Load Balancer 생성

로드 밸런서는 클라이언트로부터 요청을 가져와서 EC2 인스턴스 같은 대상 그룹의 대상에 이를 분산합니다.

시작하기 전에 하나 이상의 가용 영역에서 EC2 인스턴스를 시작합니다. Virtual Private Cloud(VPC)의 각 가용 영역에 퍼블릭 서브넷이 하나 이상 있는지 확인합니다.

AWS CLI를 사용하여 로드 밸런서 생성하려면 [자습서: AWS CLI를 사용하여 Network Load Balancer 생성 \(p. 6\)](#) 단원을 참조하십시오.

AWS Management Console을 사용하여 로드 밸런서를 생성하려면 다음 작업을 완료합니다.

작업

- 1단계: 로드 밸런서 및 리스너 구성 (p. 3)
- 2단계: 대상 그룹 구성 (p. 4)
- 3단계: 대상 그룹에 대상 등록 (p. 12)
- 4단계: 로드 밸런서 생성 (p. 13)

1단계: 로드 밸런서 및 리스너 구성

먼저 이름, 네트워크, 1개 이상의 리스너 등 로드 밸런서의 몇 가지 기본 구성 정보를 제공합니다. 리스너는 연결 요청을 확인하는 프로세스입니다. 클라이언트와 로드 밸런서 간의 연결을 위한 프로토콜 및 포트로 구성됩니다. 지원되는 프로토콜 및 포트에 대한 자세한 내용은 [리스너 구성 \(p. 15\)](#) 단원을 참조하십시오.

로드 밸런서 및 리스너를 구성하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. [Create Load Balancer]를 선택합니다.
4. [Network Load Balancer]에서 [Create]를 선택합니다.
5. [Name]에 로드 밸런서 이름을 입력합니다. 예를 들어 **my-nlb**를 입력합니다.
6. [Scheme]에서 인터넷 경계 로드 밸런서는 인터넷을 통해 클라이언트의 요청을 대상으로 라우팅합니다. 내부 로드 밸런서는 프라이빗 IP 주소를 사용하여 요청을 대상으로 라우팅합니다.
7. Listeners에서 기본값은 포트 80에서 TCP 트래픽을 수락하는 리스너입니다. 기본 리스너 설정을 그대로 두거나 프로토콜 또는 포트를 변경합니다. [Add]를 선택하여 다른 리스너를 추가합니다.
8. [Availability Zones]에서 EC2 인스턴스에 사용한 VPC를 선택합니다. EC2 인스턴스를 시작할 때 사용한 각 가용 영역에서 가용 영역을 선택한 후 해당 가용 영역에 대한 퍼블릭 서브넷을 선택합니다. 탄력적 IP 주소를 서브넷에 연결하려면 [Elastic IP]에서 이를 선택합니다.
9. [Next: Configure Routing]을 선택합니다.

2단계: 대상 그룹 구성

EC2 인스턴스 같은 대상을 대상 그룹에 등록합니다. 이 단계에서 구성하는 대상 그룹은 리스너 규칙의 대상 그룹으로 사용되며, 이 규칙은 요청을 대상 그룹에 전달합니다. 자세한 내용은 [Network Load Balancers 대상 그룹 \(p. 17\)](#) 섹션을 참조하십시오.

대상 그룹을 구성하려면

1. Target group에서는 기본 값인 [New target group]을 유지합니다.
2. [Name]에 대상 그룹의 이름을 입력합니다.
3. 필요에 따라 Protocol과 Port를 설정합니다.
4. [Target type]에서 인스턴스 ID 또는 ip로 대상을 지정할 instance를 선택하여 IP 주소로 대상을 지정합니다.
5. Health checks은 기본 상태 확인 설정을 그대로 둡니다.
6. Next: Register Targets를 선택합니다.

3단계: 대상 그룹에 대상 등록

EC2 인스턴스를 대상 그룹에 대상으로 등록할 수 있습니다.

인스턴스 ID로 대상을 등록하려면

1. [Instances]에서 인스턴스를 하나 이상 선택합니다.
2. 기본 인스턴스 리스너 포트를 유지하거나 새 포트를 입력하고 [Add to registered]를 선택합니다.
3. 인스턴스 등록을 마치면 [Next: Review]를 선택합니다.

IP 주소로 대상을 등록하려면

1. 등록할 각 IP 주소에 대해 다음을 수행합니다.
 - a. IP 주소가 대상 그룹 VPC의 서브넷에서 온 경우 [Network]에서 VPC를 선택합니다. 그렇지 않은 경우 [Other private IP address]를 선택합니다.
 - b. [Availability Zone]에서 가용 영역 또는 [all]을 선택합니다. 이는 대상이 지정된 가용 영역의 로드 밸런서 노드에서 오는 트래픽만 수신할지, 활성화된 모든 가용 영역에서 오는 트래픽을 수신할지 결

정합니다. VPC에서 온 IP 주소를 등록하는 경우 이 필드는 표시되지 않습니다. 이 경우 가용 영역이 자동으로 검색됩니다.

- c. [IP]에 주소를 입력합니다.
 - d. [Port]에 포트를 입력합니다.
 - e. [Add to list]를 선택합니다.
2. 목록에 IP 주소를 추가했으면 [Next: Review]를 선택합니다.

4단계: 로드 밸런서 생성

로드 밸런서를 생성한 후, EC2 인스턴스가 초기 상태 확인을 통과했는지 확인한 다음 로드 밸런서가 EC2 인스턴스로 트래픽을 전송하고 있는지 검사할 수 있습니다. 로드 밸런서를 완료하면 이를 삭제할 수 있습니다. 자세한 내용은 [Network Load Balancer 삭제 \(p. 14\)](#) 섹션을 참조하십시오.

로드 밸런서를 생성하려면

1. [Review] 페이지에서 [Create]를 선택합니다.
2. 로드 밸런서가 생성된 후 [Close]를 선택합니다.
3. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
4. 새로 생성한 대상 그룹을 선택합니다.
5. [Targets]를 선택하고 인스턴스가 준비되었는지 확인합니다. 인스턴스 상태가 `initial`인 경우 아직 인스턴스 등록이 진행 중이거나 정상으로 간주될 만한 최소 상태 확인 횟수를 통과하지 못했기 때문일 가능성이 높습니다. 하나 이상의 인스턴스 상태가 정상이어야 로드 밸런서를 테스트할 수 있습니다.

Network Load Balancer 태그

태그는 용도, 소유자, 환경 등 다양한 방식으로 로드 밸런서를 분류할 수 있도록 해줍니다.

각 로드 밸런서에 여러 태그를 추가할 수 있습니다. 태그 키는 각 로드 밸런서에 대해 고유해야 합니다. 로드 밸런서에 이미 연결된 키를 통해 태그를 추가하면 해당 태그의 값이 업데이트됩니다.

태그 사용을 마치면 로드 밸런서에서 이를 제거할 수 있습니다.

제한 사항

- 리소스당 최대 태그 수 - 50개
- 최대 키 길이 - 유니코드 문자 127자
- 최대 값 길이 - 유니코드 문자 255자
- 태그 키와 값은 대/소문자를 구분합니다. 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 공백 및 숫자와 특수 문자 `+ = . _ : / @`. 선행 또는 후행 공백을 사용하면 안 됩니다.
- 태그 이름이나 값에서 `aws:` 접두사는 사용하지 마십시오. 이 단어는 AWS용으로 예약되어 있습니다. 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다. 이 접두사가 지정된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.

콘솔을 사용하여 로드 밸런서 태그를 업데이트하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Tags], [Add/Edit Tags]를 선택한 후 다음 중 하나 이상의 작업을 수행합니다.

- a. 태그를 업데이트하려면 [Key] 및 [Value] 값을 수정합니다.
 - b. 새 태그를 추가하려면 [Create Tag]를 선택합니다. [Key] 및 [Value]에 값을 입력합니다.
 - c. 태그를 삭제하려면 해당 태그 옆의 삭제 아이콘(X)을 선택합니다.
5. 태그 업데이트를 마쳤으면 [Save]를 선택합니다.

AWS CLI를 사용하여 로드 밸런서 태그를 업데이트하려면

`add-tags` 및 `remove-tags` 명령을 사용합니다.

Network Load Balancer 삭제

로드 밸런서를 사용할 수 있는 순간부터 실행이 지속되는 매 시간 단위 또는 60분 미만의 시간 단위로 비용이 청구됩니다. 더 이상 로드 밸런서가 필요 없을 때는 이를 삭제할 수 있습니다. 로드 밸런서가 삭제되면 그 즉시 요금 발생이 중지됩니다.

삭제 방지 기능이 활성화되어 있으면 로드 밸런서를 삭제할 수 없습니다. 자세한 내용은 [삭제 방지 \(p. 10\)](#) 섹션을 참조하십시오.

로드 밸런서를 삭제해도 등록된 대상에는 영향을 미치지 않습니다. 예를 들어 EC2 인스턴스는 계속 실행되고 대상 그룹에 계속 등록됩니다. 대상 그룹을 삭제하려면 [대상 그룹 삭제 \(p. 28\)](#) 단원을 참조하십시오.

콘솔을 사용하여 로드 밸런서를 삭제하려면

1. 로드 밸런서를 가리키는 도메인을 위한 CNAME 레코드가 있는 경우에는 새로운 위치를 가리키도록 하고 로드 밸런서를 삭제하기 전에 DNS 변경이 적용될 때까지 기다립니다.
2. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
3. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
4. 로드 밸런서를 선택합니다.
5. [Actions], [Delete]를 선택합니다.
6. 확인 메시지가 나타나면 Yes, Delete를 선택합니다.

AWS CLI를 사용하여 로드 밸런서를 삭제하려면

`delete-load-balancer` 명령을 사용합니다.

Network Load Balancers의 리스너

Network Load Balancer를 사용하기 전에 먼저 하나 이상의 리스너를 추가해야 합니다. 리스너는 구성된 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. 리스너에 대해 정의한 규칙에 따라 로드 밸런서가 하나 이상의 대상 그룹에서 대상으로 요청을 라우팅하는 방법이 결정됩니다.

목차

- 리스너 구성 (p. 15)
- 리스너 규칙 (p. 15)
- Network Load Balancer의 리스너 생성 (p. 15)
- Network Load Balancer의 리스너 업데이트 (p. 16)
- Network Load Balancer의 리스너 삭제 (p. 16)

리스너 구성

리스너는 다음과 같은 프로토콜 및 포트를 지원합니다.

- 프로토콜: TCP
- 포트: 1-65535

TCP 리스너에 WebSockets를 사용할 수 있습니다.

리스너 규칙

리스너를 생성할 때 라우팅 요청의 규칙을 지정합니다. 이 규칙은 요청을 지정된 대상 그룹으로 전달합니다. 이 규칙을 업데이트하려면 [Network Load Balancer의 리스너 업데이트 \(p. 16\)](#) 단원을 참조하십시오.

Network Load Balancer의 리스너 생성

리스너는 연결 요청을 확인하는 프로세스입니다. 로드 밸런서를 생성할 때 리스너를 정의하면 언제든지 로드 밸런서에 리스너를 추가할 수 있습니다.

사전 조건

- 리스너 규칙에 대한 대상 그룹을 지정해야 합니다. 자세한 내용은 [Network Load Balancer 대상 그룹 생성 \(p. 21\)](#) 섹션을 참조하십시오.

리스너 추가

리스너에서 클라이언트에서 로드 밸런서로의 연결을 위한 프로토콜 및 포트 번호와 기본 리스너 규칙에 대한 대상 그룹을 구성합니다. 자세한 내용은 [리스너 구성 \(p. 15\)](#) 섹션을 참조하십시오.

콘솔을 사용하여 리스너를 추가하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Listener], [Add listener]를 선택합니다.
5. [Protocol]에서 [TCP]를 유지합니다.
6. [Port]에 리스너 포트를 입력합니다.
7. [Default target group]에서 TCP 프로토콜에 사용 가능한 대상 그룹을 선택합니다.
8. Create를 선택합니다.

AWS CLI를 사용하여 리스너를 추가하려면

`create-listener` 명령을 사용하여 리스너를 생성합니다.

Network Load Balancer의 리스너 업데이트

리스너 포트와 리스너 규칙을 업데이트할 수 있습니다. 규칙은 TCP 리스너가 요청을 대상 그룹으로 라우팅하는 방법을 결정합니다. 리스너를 생성할 때 리스너의 규칙을 처음으로 정의합니다. 자세한 내용은 [리스너 규칙 \(p. 15\)](#) 단원을 참조하십시오.

콘솔을 사용하여 리스너를 업데이트하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 LOAD BALANCING에서 Load Balancers를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Listener]를 선택하고, 해당 리스너의 확인란을 선택한 후 [Actions], [Edit]를 선택합니다.
5. (선택 사항) [Port]의 지정된 값을 변경합니다.
6. (선택 사항) [Default target group]에서 다른 대상 그룹을 선택합니다.
7. Save를 선택합니다.

AWS CLI를 사용하여 리스너를 업데이트하려면

`modify-listener` 명령을 사용하십시오.

Network Load Balancer의 리스너 삭제

언제든 리스너를 삭제할 수 있습니다. 로드 밸런서를 삭제하면 해당 리스너도 삭제됩니다.

콘솔을 이용하여 리스너를 삭제하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택하고 로드 밸런서를 선택합니다.
3. [Listener]를 선택하고, 해당 리스너의 확인란을 선택한 후 [Actions], [Delete]를 선택합니다.
4. 확인 메시지가 나타나면 Yes, Delete를 선택합니다.

AWS CLI를 사용하여 리스너를 삭제하려면

`delete-listener` 명령을 사용하십시오.

Network Load Balancers 대상 그룹

각 대상 그룹은 하나 이상의 등록된 대상에 요청을 라우팅하는 데 사용됩니다. 각 리스너 규칙을 생성할 때 대상 그룹 및 조건을 지정합니다. 규칙 조건이 충족되면 해당하는 대상 그룹으로 트래픽이 전달됩니다. 서로 다른 유형의 요청에 대해 서로 다른 대상 그룹을 생성할 수 있습니다. 예를 들어, 일반 요청인 경우 하나의 대상 그룹을 생성하고 애플리케이션에 대한 마이크로 서비스의 요청인 경우 다른 대상 그룹을 생성합니다. 자세한 내용은 [Network Load Balancer 구성 요소 \(p. 1\)](#) 단원을 참조하십시오.

대상 그룹 기준으로 로드 밸런서에 대한 상태 확인 설정을 정의합니다. 대상 그룹을 만들거나 나중에 변경할 때 재정의하지 않는 이상 각 대상 그룹은 기본 상태 확인 설정을 사용합니다. 리스너에 대한 규칙에 대상 그룹을 지정한 후, 로드 밸런서는 해당 로드 밸런서에 대해 활성화된 가용 영역의 대상 그룹에 등록된 모든 대상의 상태를 지속적으로 모니터링합니다. 로드 밸런서는 정상 상태로 등록된 대상으로 요청을 라우팅합니다.

목차

- [라우팅 구성 \(p. 17\)](#)
- [대상 유형 \(p. 17\)](#)
- [등록된 대상 \(p. 18\)](#)
- [대상 그룹 속성 \(p. 19\)](#)
- [등록 취소 지연 \(p. 19\)](#)
- [프록시 프로토콜 \(p. 20\)](#)
- [Network Load Balancer 대상 그룹 생성 \(p. 21\)](#)
- [대상 그룹에 대한 상태 확인 \(p. 21\)](#)
- [대상 그룹에 대상 등록 \(p. 25\)](#)
- [대상 그룹에 대한 태그 \(p. 27\)](#)
- [대상 그룹 삭제 \(p. 28\)](#)

라우팅 구성

기본적으로 로드 밸런서는 대상 그룹을 생성할 때 지정한 프로토콜과 포트 번호를 사용하여 대상으로 요청을 라우팅합니다. 또는 대상 그룹에 등록할 때 대상으로 트래픽을 라우팅하는 데 사용되는 포트를 재정의할 수 있습니다.

Network Load Balancers 대상 그룹은 다음과 같은 프로토콜 및 포트를 지원합니다.

- 프로토콜: TCP
- 포트: 1-65535

대상 유형

대상 그룹을 생성할 때는 대상 유형을 지정하며, 이 대상 유형은 해당 대상을 지정하는 방법을 결정합니다. 대상 그룹을 생성한 후에는 대상 유형을 변경할 수 없습니다.

가능한 대상 유형은 다음과 같습니다.

instance

대상이 인스턴스 ID에 의해 지정됩니다.

ip

대상이 IP 주소에 의해 지정됩니다.

대상 유형이 ip인 경우, 다음 CIDR 블록 중 하나에서 IP 주소를 지정할 수 있습니다.

- 대상 그룹에 대한 VPC의 서브넷
- 10.0.0.0/8(RFC 1918)
- 100.64.0.0/10(RFC 6598)
- 172.16.0.0/12(RFC 1918)
- 192.168.0.0/16(RFC 1918)

지원되는 이러한 CIDR 블록을 사용하여 ClassicLink 인스턴스, IP 주소 및 포트 주소 지정할 수 있는 AWS 리소스(예: 데이터베이스), AWS Direct Connect 또는 소프트웨어 VPN 연결을 통해 AWS에 연결되는 온프레미스 리소스를 대상 그룹에 등록할 수 있습니다.

Important

공개적으로 라우팅 가능한 IP 주소는 지정할 수 없습니다.

라우팅 및 IP 주소 요청

인스턴스 ID를 사용하여 대상을 지정하면 해당 인스턴스의 기본 네트워크 인터페이스에 지정된 기본 프라이빗 IP 주소를 사용하여 트래픽이 인스턴스로 라우팅됩니다. IP 주소를 사용하여 대상을 지정하면 하나 이상의 네트워크 인터페이스에서 프라이빗 IP 주소를 사용하여 트래픽을 인스턴스로 라우팅할 수 있습니다. 그러면 한 인스턴스의 여러 애플리케이션이 동일한 포트를 사용할 수 있습니다. 각 네트워크 인터페이스에는 자체 보안 그룹이 있을 수 있습니다.

원본 IP 보존

인스턴스 ID를 사용하여 대상을 지정하는 경우 클라이언트의 원본 IP 주소가 보존되고 애플리케이션에 제공됩니다.

IP 주소로 대상을 지정하는 경우 원본 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 클라이언트의 IP 주소가 필요한 경우, 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다.

Network Load Balancer에 등록된 인스턴스에 마이크로 서비스가 있는 경우, 로드 밸런서가 인터넷 경계이거나 인스턴스가 IP 주소로 등록되지 않은 한 로드 밸런서를 사용하여 이들 간의 통신을 제공할 수 없습니다. 자세한 내용은 [대상에서 로드 밸런서로의 요청에서 연결이 시간 초과됨 \(p. 37\)](#) 단원을 참조하십시오.

등록된 대상

로드 밸런서는 클라이언트에 대해 단일 접점의 역할을 하며 정상적으로 등록된 대상 간에 수신 트래픽을 자동으로 분산합니다. 각 대상 그룹에는 로드 밸런서에 사용되는 각 가용 영역에 하나 이상의 등록된 대상이 있어야 합니다. 하나 이상의 대상 그룹에 각 대상을 등록할 수 있습니다. 서로 다른 포트를 사용하여 각 EC2 인스턴스 또는 IP 주소를 동일한 대상 그룹에 여러 번 등록할 수 있으며, 이를 통해 로드 밸런서는 요청을 마이크로서비스로 라우팅할 수 있습니다.

애플리케이션에 대한 요구가 증가하면 이를 처리하기 위해 하나 이상의 대상 그룹에 추가 대상을 등록할 수 있습니다. 등록 과정이 완료되는 즉시, 로드 밸런서는 새로 등록된 대상으로 트래픽을 라우팅하기 시작합니다.

애플리케이션에 대한 요구가 감소하거나 대상을 서비스해야 하는 경우에는 대상 그룹에서 대상 등록을 취소할 수 있습니다. 대상을 등록 취소하면 대상 그룹에서 제거되지만 대상에 영향을 미치지 않습니다. 등록이 취소되는 즉시 로드 밸런서는 대상으로 트래픽을 라우팅하는 것을 중지합니다. 진행 중인 요청이 완료될 때까지 해당 대상은 `draining` 상태를 유지합니다. 트래픽 수신을 다시 시작할 준비가 되면 대상 그룹에 대상을 다시 등록할 수 있습니다.

인스턴스 ID로 대상을 등록하는 경우 Auto Scaling 그룹에 로드 밸런서를 사용할 수 있습니다. Auto Scaling 그룹에 대상 그룹을 연결하면 Auto Scaling은 대상을 시작할 때 대상 그룹에 해당 대상을 등록합니다. 자세한 내용은 Amazon EC2 Auto Scaling User Guide의 [Auto Scaling 그룹에 로드 밸런서 연결](#)을 참조하십시오.

제한

- C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, T1 인스턴스 유형인 경우 인스턴스 ID로 인스턴스를 등록할 수 없습니다. 이러한 인스턴스 유형은 IP 주소로 등록할 수 있습니다.
- 피어링된 VPC에 등록할 수 있는 유일한 대상은 C5, `i3.meta1` 및 M5 인스턴스입니다. 인스턴스는 로드 밸런서와 같은 리전에 있어야 합니다.
- **AWS 관리형 VPN**을 통해 연결된 대상은 등록할 수 없습니다.

대상 그룹 속성

다음은 대상 그룹의 속성입니다.

`deregistration_delay.timeout_seconds`

등록 취소된 대상의 상태를 `draining`에서 `unused`로 변경하기 전에 Elastic Load Balancing이 대기하는 시간입니다. 범위는 0~3600초입니다. 기본 값은 300초입니다.

`proxy_protocol_v2.enabled`

프록시 프로토콜 버전 2의 활성화 여부를 나타냅니다. 기본값으로 프록시 프로토콜은 비활성화됩니다.

등록 취소 지연

Elastic Load Balancing은 등록 취소 중인 인스턴스로 요청을 전송하는 것을 중지합니다. 연결 드레이닝은 기존 연결이 닫히기 전에 진행 중인 요청이 완료되도록 합니다. 등록을 취소하는 대상의 초기 상태는 `draining`입니다. 기본적으로 등록 취소된 대상의 상태는 300초 후 `unused`로 변경됩니다. `unused`로 상태를 변경하기 전에 Elastic Load Balancing이 대기하는 시간을 변경하려면 등록 취소 지연 값을 업데이트합니다.

콘솔을 사용하여 등록 취소 지연 값을 업데이트하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. 필요에 따라 [Deregistration delay] 값을 변경한 후 [Save]를 선택합니다.

AWS CLI를 사용하여 등록 취소 지연 값을 업데이트하려면

`modify-target-group-attributes` 명령을 사용합니다.

프록시 프로토콜

Network Load Balancers는 프록시 프로토콜 버전 2를 사용하여 원본 및 대상과 같은 추가 연결 정보를 보냅니다. 프록시 프로토콜 버전 2는 프록시 프로토콜 헤더의 이진 인코딩을 제공합니다.

IP 주소로 대상을 지정하는 경우 애플리케이션에 제공된 원본 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 애플리케이션이 클라이언트의 IP 주소가 필요한 경우 로드 밸런서의 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다.

인스턴스 ID로 대상을 지정하는 경우 애플리케이션에 제공되는 원본 IP 주소는 클라이언트 IP 주소입니다. 하지만 원하는 경우 로드 밸런서의 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다.

상태 확인 연결

프록시 프로토콜을 활성화한 이후 프록시 프로토콜 헤더는 또한 로드 밸런서의 상태 확인 연결에 포함됩니다. 하지만 상태 확인 연결을 통해 클라이언트 연결 정보는 프록시 프로토콜 헤더에 전송되지 않습니다.

VPC 엔드포인트 서비스

서비스 소비자에서 VPC 엔드포인트 서비스를 통해 오는 트래픽의 경우 애플리케이션에 제공된 원본 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 애플리케이션이 서비스 소비자의 IP 주소가 필요한 경우 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 이를 가져옵니다.

프록시 프로토콜 헤더에는 또한 엔드포인트의 ID가 포함됩니다. 이 정보는 다음과 같은 사용자 지정 TLV(유형-길이-값) 벡터를 사용하여 인코딩됩니다.

필드	길이(자리)	설명
Type	1	PP2_TYPE_AWS(0xEA)
길이	2	값의 길이
값	1	PP2_SUBTYPE_AWS_VPCE_ID(0x01)
	변수(값 길이 -1)	엔드포인트의 ID

TLV 유형 0xEA를 구문 분석하는 예는 <https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot>를 참조하십시오.

프록시 프로토콜 활성화

대상 그룹에 프록시 프로토콜을 활성화하기 전에 애플리케이션이 프록시 프로토콜 v2 헤더를 분석할 수 있도록 해야 합니다. 그렇지 않은 경우 실패할 수 있습니다. 자세한 내용은 [프록시 프로토콜 버전 1 및 2](#)를 참조하십시오.

콘솔을 사용하여 프록시 프로토콜을 활성화하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. [Enable proxy protocol v2]를 선택한 다음 [Save]를 선택합니다.

AWS CLI를 프록시 프로토콜을 활성화하려면

`modify-target-group-attributes` 명령을 사용합니다.

Network Load Balancer 대상 그룹 생성

Network Load Balancer 대상을 대상 그룹에 등록합니다. 기본적으로 로드 밸런서는 대상 그룹에 대해 지정한 프로토콜과 포트 번호를 사용하여 등록된 대상으로 요청을 전송합니다. 또는 대상 그룹에 각 대상을 등록할 때 이 포트를 재정의할 수 있습니다.

대상 그룹을 만든 후에는 태그를 추가할 수 있습니다.

대상 그룹의 대상으로 트래픽을 라우팅하려면 TCP 리스너를 생성하고 해당 리스너의 기본 작업에 대상 그룹을 지정합니다. 자세한 내용은 [리스너 규칙 \(p. 15\)](#) 섹션을 참조하십시오.

언제든지 대상 그룹에서 대상을 추가하거나 삭제할 수 있습니다. 자세한 내용은 [대상 그룹에 대상 등록 \(p. 25\)](#) 섹션을 참조하십시오. 대상 그룹에 대한 상태 확인 설정을 변경할 수도 있습니다. 자세한 내용은 [대상 그룹의 상태 설정 변경 \(p. 24\)](#) 섹션을 참조하십시오.

콘솔을 사용하여 대상 그룹을 생성하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. [Create target group]을 선택합니다.
4. [Target group name]에 대상 그룹의 이름을 입력합니다.
5. [Protocol]에 TCP를 선택합니다.
6. (선택 사항) [Port]에서 필요에 따라 기본값을 변경합니다.
7. [Target type]에서 인스턴스 ID 또는 ip로 대상을 지정할 instance를 선택하여 IP 주소로 대상을 지정합니다.
8. [VPC]에서 Virtual Private Cloud(VPC)를 선택합니다.
9. (선택 사항) [Health check settings] 및 [Advanced health check settings]에서 필요에 따라 기본 설정을 변경합니다. Create를 선택합니다.
10. (선택 사항) 다음과 같이 하나 이상의 태그를 추가합니다.
 - a. 새로 생성한 대상 그룹을 선택합니다.
 - b. [Tags], [Add/Edit Tags]를 선택합니다.
 - c. [Add/Edit Tags] 페이지에서 추가한 각 태그에 대해 [Create Tag]를 선택한 후 태그 키와 태그 값을 지정합니다. 태그 추가를 마쳤으면 [Save]를 선택합니다.
11. (선택 사항) 대상을 대상 그룹에 추가하려면 [대상 그룹에 대상 등록 \(p. 25\)](#) 단원을 참조하십시오.

AWS CLI를 사용하여 대상 그룹을 생성하려면

`create-target-group` 명령을 사용하여 대상 그룹을 생성하고, `add-tags` 명령으로 대상 그룹에 태그를 지정하고, `register-targets` 명령으로 대상을 추가합니다.

대상 그룹에 대한 상태 확인

Network Load Balancers는 능동 및 수동 상태 확인을 사용하여 대상이 요청을 처리하는 데 사용 가능한지 결정합니다. 기본적으로 각 로드 밸런서 노드는 해당 가용 영역에서 정상 대상으로만 요청을 라우팅합니다. 교

차 영역 로드 밸런싱을 활성화하면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 정상 대상으로 요청을 라우팅합니다. 자세한 내용은 [교차 영역 로드 밸런싱 \(p. 10\)](#) 단원을 참조하십시오.

능동 상태 확인의 경우 로드 밸런서가 주기적으로 각 등록된 대상에 요청을 전송하여 상태를 확인합니다. 각각의 로드 밸런서 노드는 대상이 등록된 대상 그룹에 대한 상태 확인 설정을 사용하여 각 대상의 상태를 확인합니다. 각각의 상태 확인이 완료되고 나면 로드 밸런서 노드는 상태 확인을 위해 설정된 연결을 종료합니다.

수동 상태 확인의 경우 로드 밸런서가 대상이 어떻게 연결에 응답하는지 관찰합니다. 수동 상태 확인에서는 로드 밸런서가 능동 상태 확인에 의해 비정상적으로 보고되기 전에 비정상 대상을 감지할 수 있습니다. 사용자가 수동 상태 확인을 비활성화, 구성 또는 모니터링할 수는 없습니다.

하나 이상의 대상 그룹이 활성화 가용 영역에서 정상적인 대상이 없는 경우 DNS에서 해당 서브넷의 IP 주소를 제거하여 해당 가용 영역의 대상으로 요청을 라우팅할 수 없습니다. 각 대상 그룹에 정상적인 대상이 있는 활성화된 가용 영역이 없는 경우 요청은 모든 활성화된 가용 영역의 대상으로 라우팅됩니다.

상태 확인 설정

다음 설정을 사용하여 대상 그룹에서 대상에 대한 능동 상태 확인을 구성합니다. 로드 밸런서는 지정된 포트, 프로토콜 및 ping 경로를 사용하여 HealthCheckIntervalSeconds 초마다 모든 등록 대상에 상태 확인 요청을 전송합니다. 응답 제한 시간 내에 대상이 응답할 때까지 기다립니다. 상태 확인이 연속적인 응답 실패의 임계값을 초과하면 로드 밸런서는 대상을 서비스에서 제외시킵니다. 상태 확인이 연속적인 응답 성공의 임계값을 초과하면 로드 밸런서는 대상을 다시 서비스합니다.

설정	설명
HealthCheckProtocol	대상에 대한 상태 확인을 수행할 때 로드 밸런서가 사용하는 프로토콜입니다. HTTP, HTTPS, TCP 프로토콜이 여기에 해당됩니다. TCP 프로토콜이 기본 설정값입니다.
HealthCheckPort	대상에 대한 상태 확인을 수행할 때 로드 밸런서가 사용하는 포트입니다. 각 대상이 로드 밸런서에서 트래픽을 수신하는 포트를 사용하도록 기본 설정되어 있습니다.
HealthCheckPath	[HTTP/HTTPS 상태 확인] 상태 확인을 위한 대상에서 목적지가 되는 ping 경로입니다. 기본값은 /입니다.
HealthCheckTimeoutSeconds	상태 확인 실패를 의미하는 대상으로부터 응답이 없는 기간(초 단위)입니다. 이는 TCP 및 HTTPS 상태 확인의 경우 10초이고, HTTP 상태 확인의 경우 6초입니다.
HealthCheckIntervalSeconds	개별 인스턴스의 상태 확인 간의 대략적인 간격(초 단위)입니다. 이 값은 10초 또는 30초일 수 있습니다. 기본값은 30초입니다.

Important

Network Load Balancer에 대한 상태 확인은 분산되며 대상 상태를 결정하는 데 합의 메커니즘을 사용합니다. 그러므로 대상은 구성된 수보다 많은 상태 확인을 수신할 수 있습니다. 대상에 대한 상태 확인 수를 줄려면 정적 HTML 파일을 HTTP 대상으로 사용하거나 TCP 상태 확인을 사용합니다.

설정	설명
HealthyThresholdCount	비정상 상태의 대상을 정상으로 간주하기까지 필요한 연속적인 상태 확인 성공 횟수입니다. 범위는 2 ~ 10회입니다. 기본값은 3입니다.
UnhealthyThresholdCount	대상을 비정상 상태로 간주하기까지 필요한 연속적인 상태 확인 실패 횟수입니다. 이 값은 정상 임계값 개수와 동일해야 합니다.
Matcher	[HTTP/HTTPS 상태 확인] 대상으로부터 응답 성공을 확인할 때 사용하는 HTTP 코드입니다. 이 값은 200~399여야 합니다.

대상 상태

로드 밸런서가 대상으로 상태 확인 요청을 전송할 수 있으려면 먼저 대상 그룹에 이를 등록하고 리스너 규칙에서 대상 그룹을 지정한 다음, 로드 밸런서에서 대상의 가용 영역을 활성화해야 합니다.

다음 표에는 등록 대상의 상태로 가능한 값이 나와 있습니다.

값	설명
initial	로드 밸런서에서는 대상 등록이나 대상에 대해 초기 상태 확인이 진행 중에 있습니다.
healthy	대상이 정상 상태입니다.
unhealthy	대상이 상태 확인에 응답하지 않았거나 상태 확인에 실패했습니다.
unused	대상이 대상 그룹에 등록되어 있지 않거나, 대상 그룹이 로드 밸런서를 위한 리스너 규칙에서 사용되지 않거나, 대상이 로드 밸런서에서 활성화되지 않은 가용 영역에 있습니다.
draining	대상이 등록 취소되고 있으며 연결 드레이닝이 진행 중입니다.

상태 확인 사유 코드

대상의 상태가 Healthy 이외의 값인 경우에는 API가 문제에 대한 사유 코드와 설명을 반환하고 콘솔이 도구 설명에 동일한 설명을 표시합니다. Elb로 시작되는 사유 코드는 로드 밸런서 측에서 호출되고, Target로 시작되는 사유 코드는 대상 측에서 호출됩니다.

사유 코드	설명
Elb.InitialHealthChecking	초기 상태 확인이 진행 중
Elb.InternalError	내부 오류로 인한 상태 확인 실패
Elb.RegistrationInProgress	대상 등록이 진행 중
Target.DeregistrationInProgress	대상 등록 취소가 진행 중
Target.FailedHealthChecks	상태 확인 실패

사유 코드	설명
<code>Target.InvalidState</code>	대상이 중지 상태에 있음 대상이 종료 상태에 있음 대상이 종료 또는 중지 상태에 있음 대상이 잘못된 상태에 있음
<code>Target.NotInUse</code>	대상 그룹이 로드 밸런서에서 트래픽을 수신하도록 구성되지 않음 대상이 로드 밸런서에서 활성화되지 않은 가용 영역에 있음
<code>Target.NotRegistered</code>	대상이 대상 그룹에 등록되지 않음
<code>Target.ResponseCodeMismatch</code>	[code] 등의 코드에서 상태 확인 실패
<code>Target.Timeout</code>	요청 시간 초과

대상의 상태 확인

대상 그룹에 등록된 대상의 상태를 확인할 수 있습니다.

콘솔을 사용하여 대상의 상태를 확인하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Targets]를 선택한 후, [Status] 열에서 각 대상의 상태를 봅니다. 상태가 `Healthy` 이외의 값인 경우에는 도구 설명에서 자세한 내용을 확인합니다.

AWS CLI를 사용하여 대상의 상태를 확인하려면

`describe-target-health` 명령을 사용하십시오. 이 명령의 출력에는 대상 상태가 포함되어 있고, 상태가 `Healthy` 이외의 값인 경우에는 사유 코드가 포함되어 있습니다.

대상 그룹의 상태 설정 변경

대상 그룹에 대한 일부 상태 확인 설정을 변경할 수 있습니다.

콘솔을 사용하여 대상 그룹의 상태 확인 설정을 변경하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Health checks], [Edit]를 선택합니다.
5. [Edit target group] 페이지에서 필요에 따라 설정을 변경한 다음 [Save]를 선택합니다.

AWS CLI를 사용하여 대상 그룹의 상태 확인 설정을 변경하려면

`modify-target-group` 명령을 사용하십시오.

대상 그룹에 대상 등록

하나 이상의 대상 그룹에 대상을 등록합니다. 각 대상 그룹에는 로드 밸런서에 사용되는 각 가용 영역에 하나 이상의 등록된 대상이 있어야 합니다. 인스턴스 ID 또는 IP 주소로 대상을 등록할 수 있습니다. 자세한 내용은 [Network Load Balancers 대상 그룹 \(p. 17\)](#) 섹션을 참조하십시오.

최근 등록된 대상에 대한 요구가 증가하면 이를 처리하기 위해 하나 이상의 대상 그룹에 추가 대상을 등록할 수 있습니다. 대상이 요청을 처리할 준비가 되면 대상 그룹에 등록합니다. 로드 밸런서는 등록 프로세스가 완료되고 대상이 초기 상태 확인을 통과하자마자 해당 대상에 대한 라우팅 요청을 시작합니다.

등록된 대상에 대한 요구가 감소하거나 대상을 서비스해야 하는 경우에는 대상 그룹에서 등록을 취소할 수 있습니다. 등록이 취소되는 즉시 로드 밸런서는 대상으로의 요청 라우팅을 중지합니다. 대상이 요청 수신을 시작할 준비가 되면 대상 그룹에 다시 등록할 수 있습니다.

대상이 등록 취소되면 Elastic Load Balancing은 진행 중인 요청이 완료될 때까지 대기합니다. 이를 연결 드레이닝이라고 합니다. 연결 드레이닝이 진행 중인 동안 대상의 상태는 `draining`입니다.

인스턴스 ID로 대상을 등록하는 경우 Auto Scaling 그룹에 로드 밸런서를 사용할 수 있습니다. Auto Scaling 그룹에 대상 그룹을 연결하고 해당 그룹이 확장되면, Auto Scaling 그룹에서 시작한 인스턴스가 대상 그룹에 자동으로 등록됩니다. Auto Scaling 그룹에서 로드 밸런서를 분리하면 인스턴스가 대상 그룹에서 자동으로 등록 취소됩니다. 자세한 내용은 Amazon EC2 Auto Scaling User Guide의 [Auto Scaling 그룹에 로드 밸런서 연결](#)을 참조하십시오.

대상 보안 그룹

EC2 인스턴스를 대상으로 등록할 때 이러한 인스턴스에 대한 보안 그룹은 리스너 포트와 상태 확인 포트 모두에서 트래픽을 허용해야 합니다.

제한

- Network Load Balancers는 연결된 보안 그룹을 갖지 않습니다. 따라서 대상의 보안 그룹은 IP 주소를 사용하여 로드 밸런서로부터의 트래픽을 허용해야 합니다.
- 대상의 보안 그룹에 있는 클라이언트의 보안 그룹을 사용하여 로드 밸런서를 통해 클라이언트에서 대상으로의 트래픽을 허용할 수 없습니다. 대신 대상 보안 그룹에 있는 클라이언트 CIDR 블록을 사용하십시오.

권장 규칙

인바운드		
소스	포트 범위	Comment
<code>##### IP ##</code>	<code>#### ###</code>	인스턴스 리스너 포트의 클라이언트에서 트래픽을 허용합니다
<code>VPC CIDR</code>	<code>## ##</code>	상태 확인 포트의 로드 밸런서에서 트래픽을 허용합니다

전체 VPC CIDR에 대한 액세스 권한을 부여하지 않으려는 경우, 로드 밸런서 노드에서 사용하는 프라이빗 IP 주소에 대한 액세스 권한을 부여할 수 있습니다. 로드 밸런서 서브넷당 한 개의 IP 주소가 있습니다. 이러한 주소를 찾으려면 다음 절차를 사용합니다.

화이트리스트에 등록할 프라이빗 IP 주소를 찾으려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창에서 Network Interfaces를 선택합니다.

3. 검색 필드에 Network Load Balancer 이름을 입력합니다. 로드 밸런서 서브넷당 한 개의 네트워크 인터페이스가 있습니다.
4. 각 네트워크 인터페이스의 [Details] 탭에서 [Primary private IPv4 IP]의 주소를 복사합니다.

대상 및 인터넷 경계 로드 밸런서

인터넷 경계 로드 밸런서를 사용하면, 인스턴스 ID에 의해 등록된 대상에는 연결을 제공하는 인터넷에 대한 경로가 있어야 합니다. 퍼블릭 서브넷에 있는 대상에는 인터넷 게이트웨이를 통해 직접 인터넷에 연결되는 경로가 있습니다. 프라이빗 서브넷에 있는 대상이 인스턴스 ID에 의해 등록된 경우, 해당 서브넷의 라우팅 테이블에는 인터넷에 연결되는 경로가 있어야 합니다(예: NAT 게이트웨이 또는 EC2 인스턴스를 통해).

네트워크 ACL

VPC의 기본 네트워크 ACL(액세스 제어 목록)은 인바운드 트래픽과 아웃바운드 트래픽을 모두 허용합니다. 사용자 지정 네트워크 ACL을 생성하는 경우 ACL이 로드 밸런서 및 인스턴스가 리스너 포트, 상태 확인 포트 및 휘발성 포트(1024-65535)에서 양방향으로 통신하도록 허용해야 합니다.

대상 등록 또는 등록 취소

대상 그룹을 생성할 때 인스턴스 ID 또는 IP 주소로 대상을 등록해야 하는지 여부를 지정합니다.

제한

- C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, T1 인스턴스 유형인 경우 인스턴스 ID로 인스턴스를 등록할 수 없습니다. 이러한 인스턴스 유형은 IP 주소로 등록할 수 있습니다.
- 피어링된 VPC에 등록할 수 있는 유일한 대상은 C5, i3.metal 및 M5 인스턴스입니다. 인스턴스는 로드 밸런서와 같은 리전에 있어야 합니다.
- [AWS 관리형 VPN](#)을 통해 연결된 대상은 등록할 수 없습니다.

인스턴스 ID로 대상 등록 또는 등록 취소

인스턴스를 등록할 때 인스턴스가 running 상태여야 합니다.

인스턴스 ID로 대상을 등록하거나 등록 취소하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Targets], [Edit]를 선택합니다.
5. (선택 사항) [Registered instances]에서 등록을 취소할 인스턴스를 선택하고 [Remove]를 선택합니다.
6. (선택 사항) [Instances]에서 등록을 취소할 실행 중인 인스턴스를 선택하고 필요에 따라 기본 인스턴스를 변경한 다음 [Add to registered]를 선택합니다.
7. Save를 선택합니다.

IP 주소로 대상 등록 또는 등록 취소

등록하는 IP 주소는 대상 그룹에 대한 VPC의 서브넷에서 오고, RFC 1918 범위(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) 및 RFC 6598 범위(100.64.0.0/10)여야 합니다. 공개적으로 라우팅 가능한 IP 주소는 등록할 수 없습니다.

IP 주소로 대상을 등록하거나 등록 취소하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택하고 [Targets], [Edit]를 선택합니다.
4. IP 주소를 등록하려면 메뉴 모음의 [Register targets] 아이콘(더하기 기호)을 선택합니다. 각 IP 주소에 대해 네트워크, 가용 영역, IP 주소, 포트를 지정한 후 [Add to list]를 선택합니다. 주소 지정을 마치면 [Register]를 선택합니다.
5. IP 주소를 등록 취소하려면 메뉴 모음의 [Deregister targets] 아이콘(마이너스 기호)을 선택합니다. 등록 취소된 IP 주소가 많은 경우 필터를 추가하거나 정렬 순서를 변경하는 것이 유용할 수 있습니다. IP 주소를 선택하고 [Deregister]를 선택합니다.
6. 이 화면에서 나가려면 메뉴 모음에서 [Back to target group] 아이콘(뒤로 버튼)을 선택합니다.

AWS CLI를 사용하여 대상을 등록 또는 등록 취소하려면

`register-targets` 명령을 사용하여 대상을 추가하고 `deregister-targets` 명령을 사용하여 대상을 제거합니다.

대상 그룹에 대한 태그

태그를 사용하면 용도, 소유자 또는 환경 등에 따라 대상 그룹을 다양한 방식으로 분류할 수 있습니다.

각 대상 그룹에 여러 태그를 추가할 수 있습니다. 태그 키는 대상 그룹별로 고유해야 합니다. 대상 그룹에 이미 연결된 키를 통해 태그를 추가하면 해당 태그의 값이 업데이트됩니다.

사용이 끝난 태그는 삭제할 수 있습니다.

제한 사항

- 리소스당 최대 태그 수 - 50개
- 최대 키 길이 - 유니코드 문자 127자
- 최대 값 길이 - 유니코드 문자 255자
- 태그 키와 값은 대/소문자를 구분합니다. 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 공백 및 숫자와 특수 문자 + - = . _ : / @. 선행 또는 후행 공백을 사용하면 안 됩니다.
- 태그 이름이나 값에서 `aws:` 접두사는 사용하지 마십시오. 이 단어는 AWS용으로 예약되어 있습니다. 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다. 이 접두사가 지정된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.

콘솔을 사용하여 대상 그룹 태그를 업데이트하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Tags] 탭에서 [Add/Edit Tags]를 선택하고 다음 중 하나 이상의 작업을 수행합니다.
 - a. 태그를 업데이트하려면 [Key] 및 [Value] 값을 수정합니다.
 - b. 새로운 태그를 추가하려면 [Create Tag]를 선택한 다음 [Key] 및 [Value] 값을 입력합니다.
 - c. 태그를 삭제하려면 해당 태그 옆의 삭제 아이콘(X)을 선택합니다.
5. 태그 업데이트를 마쳤으면 [Save]를 선택합니다.

AWS CLI를 사용하여 대상 그룹 태그를 업데이트하려면

`add-tags` 및 `remove-tags` 명령을 사용합니다.

대상 그룹 삭제

작업이 참조하지 않는 경우 대상 그룹을 삭제할 수 있습니다. 대상 그룹을 삭제해도 대상 그룹에 등록된 대상에는 영향을 미치지 않습니다. EC2 인스턴스가 더 이상 필요하지 않은 경우 종료할 수 있습니다.

콘솔을 사용하여 대상 그룹을 삭제하려면

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택하고 [Actions], [Delete]를 차례로 선택합니다.
4. 확인 메시지가 표시되면 [Yes]를 선택합니다.

AWS CLI를 사용하여 대상 그룹을 삭제하려면

`delete-target-group` 명령을 사용합니다.

Network Load Balancers 모니터링

다음 기능을 사용하여 로드 밸런서를 모니터링하고 트래픽 패턴을 분석하며 로드 밸런서 및 대상의 문제를 해결할 수 있습니다.

CloudWatch 지표

Amazon CloudWatch를 사용하면 로드 밸런서 및 대상을 위한 데이터 요소에 대한 통계를 지표라고 하는 정렬된 시계열 집합으로 검색할 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 [Network Load Balancer의 CloudWatch 측정치 \(p. 29\)](#) 단원을 참조하십시오.

VPC 흐름 로그

VPC 플로우 로그를 사용하여 Network Load Balancer로 들어오고 나가는 트래픽에 대한 세부 정보를 캡처할 수 있습니다. 자세한 정보는 Amazon VPC User Guide에서 [VPC 흐름 로그](#)를 참조하십시오.

로드 밸런서의 각 네트워크 인터페이스에 대한 흐름 로그를 생성합니다. 로드 밸런서 서브넷당 한 개의 네트워크 인터페이스가 있습니다. Network Load Balancer의 네트워크 인터페이스를 식별하려면 네트워크 인터페이스의 설명 필드에서 로드 밸런서의 이름을 찾습니다.

Network Load Balancer을 통한 각 연결은 두 가지 항목을 가집니다. 프론트엔드 연결은 클라이언트와 로드 밸런서 사이의 연결이고 백엔드 연결은 로드 밸런서와 대상 사이의 연결입니다. 대상이 인스턴스 ID로 등록되어 있으면 그 연결은 인스턴스에 클라이언트로부터의 연결로 나타납니다. 인스턴스의 보안 그룹이 클라이언트로부터의 연결을 허용하지 않고 로드 밸런서 서브넷 네트워크 ACL이 연결을 허용하면 로드 밸런서의 네트워크 인터페이스 로그는 프론트엔드 연결과 백엔드 연결에 대해 'ACCEPT OK(승인 확인)'를 표시하고 인스턴스의 네트워크 인터페이스 로그는 그 연결에 대해 'REJECT OK(거절 확인)'를 표시합니다.

CloudTrail 로그

AWS CloudTrail을 사용하여 Elastic Load Balancing API에 보낸 요청에 대한 자세한 정보를 캡처하고 Amazon S3에 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하여 어떤 요청이 이루어졌는지, 어떤 소스 IP 주소에서 요청을 했는지, 누가 언제 요청했는지 등을 확인할 수 있습니다. 자세한 내용은 [AWS CloudTrail을 사용하여 Network Load Balancer에 대한 API 호출 로깅 \(p. 32\)](#) 섹션을 참조하십시오.

Network Load Balancer의 CloudWatch 측정치

Elastic Load Balancing은 Amazon CloudWatch에 로드 밸런서 및 대상에 대한 데이터 요소를 게시합니다. CloudWatch를 사용하면 지표라고 알려진, 그러한 데이터 요소에 대한 통계를 정렬된 시계열 집합으로 검색할 수 있습니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 예를 들어 지정된 기간 동안 로드 밸런서에 대한 정상 상태 대상의 총 수를 모니터링할 수 있습니다. 각 데이터 요소에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어 CloudWatch 경보를 생성하여 지정된 지표를 모니터링할 수 있으며, 지표가 허용 범위를 벗어난다고 간주되는 경우 작업(예: 이메일 주소로 알림 전송)을 시작할 수 있습니다.

요청이 로드 밸런서를 통과하고 있는 경우에만 Elastic Load Balancing이 CloudWatch로 지표를 보고합니다. 로드 밸런서를 통과하고 있는 요청이 있는 경우, Elastic Load Balancing은 60초마다 지표를 측정해서 전송합니다. 로드 밸런서를 통과하고 있는 요청이 없는 경우나 지표에 대한 데이터가 없는 경우에는 지표가 보고되지 않습니다.

자세한 내용은 [Amazon CloudWatch User Guide](#) 단원을 참조하십시오.

목차

- [네트워크 로드 밸런서 측정치 \(p. 30\)](#)
- [네트워크 로드 밸런서의 측정치 차원 \(p. 30\)](#)
- [Network Load Balancer 지표에 대한 통계 \(p. 31\)](#)
- [로드 밸런서를 위한 CloudWatch 지표 보기 \(p. 31\)](#)

네트워크 로드 밸런서 측정치

AWS/NetworkELB 네임스페이스에는 다음 지표가 포함되어 있습니다.

지표	설명
ActiveFlowCount	클라이언트에서 대상까지의 동시 TCP 흐름(또는 연결)의 총 수입니다. 이 지표에는 SYN_SENT 및 ESTABLISHED 상태의 연결만 포함됩니다. TCP 연결은 로드 밸런서에서 종료되지 않으므로 대상에 대한 TCP 연결을 여는 클라이언트는 단일 흐름으로 계산됩니다. 통계: 가장 유용한 통계는 Average, Maximum 및 Minimum입니다.
ConsumedLCUs	로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수. 시간 단위로 사용한 LCU 수만큼 요금을 지불하면 됩니다. 자세한 내용은 Elastic Load Balancing 요금 을 참조하십시오.
HealthyHostCount	정상 상태로 간주되는 대상 수 Statistics(통계): 가장 유용한 통계는 Maximum 및 Minimum입니다.
NewFlowCount	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 TCP 흐름(또는 연결)의 총 수입니다. 통계: 가장 유용한 통계는 sum입니다.
ProcessedBytes	TCP/IP 헤더를 포함하여 로드 밸런서가 처리하는 총 바이트 수. 통계: 가장 유용한 통계는 sum입니다.
TCP_Client_Reset_Count	클라이언트에서 대상까지 전송된 재설정(RST) 패킷의 총 수입니다. 이러한 재설정은 클라이언트에 의해 생성되고 로드 밸런서에 의해 전달됩니다. 통계: 가장 유용한 통계는 sum입니다.
TCP_ELB_Reset_Count	로드 밸런서에 의해 생성되는 재설정(RST) 패킷의 총 수입니다. 통계: 가장 유용한 통계는 sum입니다.
TCP_Target_Reset_Count	대상에서 클라이언트로 전송된 재설정(RST) 패킷의 총 수입니다. 이러한 재설정은 대상에 의해 생성되고 로드 밸런서에 의해 전달됩니다. 통계: 가장 유용한 통계는 sum입니다.
UnHealthyHostCount	비정상 상태로 간주되는 대상 수 Statistics(통계): 가장 유용한 통계는 Maximum 및 Minimum입니다.

네트워크 로드 밸런서의 측정치 차원

로드 밸런서 측정치를 필터링하려면 다음 차원을 사용하십시오.

차원	설명
AvailabilityZone	가용 영역을 기준으로 지표 데이터를 필터링합니다.
LoadBalancer	로드 밸런서를 기준으로 지표 데이터를 필터링합니다. 로드 밸런서는 다음과 같이 지정합니다. net/load-balancer-name/1234567890123456(로드 밸런서 ARN의 마지막 구간).
TargetGroup	대상 그룹을 기준으로 지표 데이터를 필터링합니다. 대상 그룹은 다음과 같이 지정합니다. targetgroup/target-group-name/1234567890123456(대상 그룹 ARN의 마지막 구간).

Network Load Balancer 지표에 대한 통계

CloudWatch는 Elastic Load Balancing이 게시한 지표 데이터 요소에 따라 통계를 제공합니다. 통계는 지정한 기간에 걸친 지표 데이터 집계입니다. 통계를 요청하면 지표 이름 및 차원으로 반환된 데이터 스트림이 식별됩니다. 차원이란 지표를 고유하게 식별하는 데 도움이 되는 이름/값 쌍을 말합니다. 예를 들어 특정 가용 영역에서 시작된 로드 밸런서를 지원하는 정상 상태의 모든 EC2 인스턴스에 대한 통계를 요청할 수 있습니다.

Minimum 및 Maximum 통계는 개별 로드 밸런서 노드가 보고한 최소 및 최대 값을 반영합니다. 예를 들어 로드 밸런서 노드가 2개라고 가정해 보겠습니다. 하나의 노드에는 Minimum이 2, Maximum이 10, Average가 6인 HealthyHostCount가 있으며 다른 노드에는 Minimum이 1, Maximum이 5, Average가 3인 HealthyHostCount가 있습니다. 따라서 로드 밸런서의 Minimum은 1, Maximum은 10, Average는 4입니다.

Sum 통계는 모든 로드 밸런서 노드의 집계 값입니다. 지표에는 기간별 보고서가 여러 개 있기 때문에 Sum은 모든 로드 밸런서 노드에서 집계된 지표에만 적용할 수 있습니다.

SampleCount 통계는 측정된 샘플의 수입니다. 지표는 샘플링 간격 및 이벤트를 토대로 수집이 되기 때문에 일반적으로 이 통계는 유용하지 않습니다. 예를 들어 HealthyHostCount에 대해 SampleCount는 각 로드 밸런서 노드가 보고하는 샘플 수를 기반으로 하며 정상 호스트 수는 아닙니다.

로드 밸런서를 위한 CloudWatch 지표 보기

Amazon EC2 콘솔을 사용해 로드 밸런서를 위한 CloudWatch 지표를 볼 수 있습니다. 이 측정치들은 모니터링 그래프로 표시됩니다. 로드 밸런서가 활성 상태로 요청을 수신 중에 있으면 모니터링 그래프에 데이터 요소가 표시됩니다.

또는 CloudWatch 콘솔을 사용해 로드 밸런서를 위한 지표를 볼 수 있습니다.

Amazon EC2 콘솔을 사용한 메트릭 확인

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. 대상 그룹을 기준으로 필터링한 지표를 보려면 다음 작업을 수행합니다.
 - a. 탐색 창에서 [Target Groups]를 선택합니다.
 - b. 대상 그룹을 선택하고 [Monitoring]을 선택합니다.
 - c. (선택 사항) 시간을 기준으로 결과를 필터링하려면 [Showing data for]에서 시간 범위를 선택합니다.
 - d. 단일 지표를 크게 보려면 그래프를 선택합니다.
3. 로드 밸런서를 기준으로 필터링한 지표를 보려면 다음 작업을 수행합니다.
 - a. 탐색 창에서 [Load Balancers]를 클릭합니다.
 - b. 로드 밸런서를 선택하고 [Monitoring]을 선택합니다.
 - c. (선택 사항) 시간을 기준으로 결과를 필터링하려면 [Showing data for]에서 시간 범위를 선택합니다.

- d. 단일 지표를 크게 보려면 그래프를 선택합니다.

CloudWatch 콘솔을 사용한 메트릭 확인

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. 탐색 창에서 [Metrics]를 선택합니다.
3. [NetworkELB] 네임스페이스를 선택합니다.
4. (선택 사항) 모든 차원의 지표를 보려면 검색 필드에 이름을 입력합니다.

AWS CLI를 사용하여 지표를 보려면

사용 가능한 지표의 목록을 표시하려면 아래 [list-metrics](#) 명령을 사용하십시오.

```
aws cloudwatch list-metrics --namespace AWS/NetworkELB
```

AWS CLI를 사용하여 지표에 대한 통계를 구하려면

지정된 지표 및 차원에 대한 통계를 구하려면 아래 [get-metric-statistics](#) 명령을 사용하십시오. CloudWatch는 각각의 고유한 차원의 조합을 별도의 지표로 처리합니다. 특별 계시가 되지 않은 차원의 조합을 사용해 통계를 검색할 수는 없습니다. 지표 생성 시 사용한 것과 동일하게 차원을 지정해야 합니다.

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \
--metric-name UnHealthyHostCount --statistics Average --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

다음은 예제 출력입니다.

```
{
  "Datapoints": [
    {
      "Timestamp": "2017-04-18T22:00:00Z",
      "Average": 0.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2017-04-18T04:00:00Z",
      "Average": 0.0,
      "Unit": "Count"
    },
    ...
  ],
  "Label": "UnHealthyHostCount"
}
```

AWS CloudTrail을 사용하여 Network Load Balancer에 대한 API 호출 로깅

Elastic Load Balancing은 Elastic Load Balancing에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Elastic Load Balancing에 대한 API 호출을 모두 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Management Console의 호출과 Elastic Load Balancing API 작업에 대한 호출이 포함됩니다. 추적을 생성하면 Elastic Load Balancing 이벤트를 비

못하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다. CloudTrail에서 수집하는 정보를 사용하여 Elastic Load Balancing에 어떤 요청이 이루어졌는지, 어떤 IP 주소에서 요청했는지, 누가 언제 요청했는지 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail User Guide](#) 단원을 참조하십시오.

CloudTrail의 Elastic Load Balancing 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. 활동이 Elastic Load Balancing에서 이루어지면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트 로그에 기록됩니다. 이를 통해 AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기를](#) 참조하십시오.

Elastic Load Balancing 이벤트를 비롯하여 AWS 계정의 이벤트 기록을 보유하려면 추적을 생성하십시오. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있게 해 줍니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 기타 AWS 서비스를 사용하여 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)
- [여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기](#)

모든 Network Load Balancers의 Elastic Load Balancing 작업이 CloudTrail에서 로깅되고 [Elastic Load Balancing API Reference version 2015-12-01](#)에 문서화됩니다. 예를 들어, `CreateLoadBalancer` 및 `DeleteLoadBalancer` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 루트 또는 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 사용하여 요청했는지 여부.
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청을 다른 AWS 서비스로 했는지.

자세한 정보는 [CloudTrail userIdentity 요소](#)를 참조하십시오.

Elastic Load Balancing 로그 파일 항목 이해

추적은 지정된 Amazon S3 버킷에 이벤트를 로그 파일로 제공할 수 있도록 해주는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 어떤 소스로부터의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

로그 파일에는 Elastic Load Balancing API 호출 외에 AWS 계정의 모든 AWS API 호출 이벤트가 포함되어 있습니다. `elasticloadbalancing.amazonaws.com` 값이 있는 `eventSource` 요소를 확인하여 Elastic Load Balancing API에 대한 호출의 위치를 찾을 수 있습니다. `CreateLoadBalancer` 같은 특정 작업에 대한 레코드를 보려면 작업 이름이 있는 `eventName` 요소를 확인합니다.

다음은 AWS CLI를 사용하여 Network Load Balancer를 생성한 후 삭제한 사용자의 Elastic Load Balancing에 대한 CloudTrail 로그 레코드의 예제입니다. `userAgent` 요소를 사용해 CLI를 식별할 수 있습니다. `eventName` 요소를 사용해 요청된 API 호출을 식별할 수 있습니다. 그리고 사용자(Alice)에 대한 정보는 `userIdentity` 요소를 보면 알 수 있습니다.

Example 예: CreateLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-8360a9e7", "subnet-b7d581c0"],
    "securityGroups": ["sg-5943793c"],
    "name": "my-load-balancer",
    "scheme": "internet-facing"
  },
  "responseElements": {
    "loadBalancers": [{
      "type": "application",
      "loadBalancerName": "my-load-balancer",
      "vpcId": "vpc-3ac0fb5f",
      "securityGroups": ["sg-5943793c"],
      "state": {"code": "provisioning"},
      "availabilityZones": [
        {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
        {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
      ],
      "dnsName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
      "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
      "createdTime": "Apr 11, 2016 5:23:50 PM",
      "loadBalancerArn": "arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-balancer/ffcdace1759e1d0",
      "scheme": "internet-facing"
    }]
  },
  "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
  "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-12-01",
  "recipientAccountId": "123456789012"
}
```

Example 예: DeleteLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
```

```
"eventName": "DeleteLoadBalancer",
"awsRegion": "us-west-2",
"sourceIPAddress": "198.51.100.1",
"userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
"requestParameters": {
  "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0"
},
"responseElements": null,
"requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
"eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
"eventType": "AwsApiCall",
"apiVersion": "2015-12-01",
"recipientAccountId": "123456789012"
}
```

Network Load Balancer 문제 해결

다음 정보는 Network Load Balancer와 관련된 문제를 해결하는 데 도움이 될 수 있습니다.

등록된 대상은 서비스되지 않고 있습니다.

대상이 InService 상태로 들어가는 데 예상보다 시간이 오래 걸릴 경우 상태 확인에 실패할 수 있습니다. 한번이라도 상태 확인을 통과할 때까지 대상이 서비스되지 않습니다. 자세한 내용은 [대상 그룹에 대한 상태 확인 \(p. 21\)](#) 섹션을 참조하십시오.

인스턴스가 상태 확인에 실패하고 있는지 확인한 다음, 다음을 점검합니다.

보안 그룹이 트래픽을 허용하지 않음

인스턴스에 연결된 보안 그룹은 반드시 상태 확인 포트와 상태 확인 프로토콜을 사용하여 로드 밸런서에서의 트래픽을 허용해야 합니다.

ACL(액세스 제어 목록)이 트래픽을 허용하지 않음

인스턴스를 위해 서브넷에 연결된 네트워크 ACL은 상태 확인 포트에서 인바운드 트래픽을, 휘발성 포트(1024-65535)에서 아웃바운드 트래픽을 허용해야 합니다. 로드 밸런서 노드를 위해 서브넷에 연결된 네트워크 ACL은 휘발성 포트에서 인바운드 트래픽을, 상태 확인 및 휘발성 포트에서 아웃바운드 트래픽을 허용해야 합니다.

인스턴스가 피어링된 VPC에서 지원되지 않음

피어링된 VPC에 등록할 수 있는 유일한 대상은 C5, i3.meta1 및 M5 인스턴스입니다.

요청이 대상으로 라우팅되지 않음

다음 사항을 확인합니다.

보안 그룹이 트래픽을 허용하지 않음

인스턴스와 연결된 보안 그룹이 리스너 포트에서 클라이언트 IP 주소(대상이 인스턴스 ID로 지정된 경우) 또는 로드 밸런서 노드(대상이 IP 주소로 지정된 경우)로부터의 트래픽을 허용해야 합니다.

ACL(액세스 제어 목록)이 트래픽을 허용하지 않음

VPC의 서브넷과 연결된 네트워크 ACL이 로드 밸런서 및 대상이 리스너 포트에서 양방향으로 통신하도록 허용해야 합니다.

대상이 활성화되지 않은 가용 영역에 있음

가용 영역에 대상을 등록하지만 가용 영역은 활성화하지 않는 경우 이러한 등록된 대상은 로드 밸런서로부터 트래픽을 수신하지 않습니다.

트래픽의 리턴 경로가 없음

인터넷 경계 로드 밸런서에 등록된 대상은 인터넷에 대한 경로가 있어야 합니다. 퍼블릭 서브넷에 있는 대상은 인터넷 게이트웨이로 0.0.0.0/0을 라우팅할 수 있습니다. 프라이빗 서브넷에 있는 대상은 NAT 게이트웨이로 또는 퍼블릭 서브넷의 EC2 인스턴스로 0.0.0.0/0을 라우팅할 수 있습니다.

클라이언트가 피어링된 VPC 또는 AWS 관리형 VPN에 있음

클라이언트가 C5, i3.meta1 또는 M5 인스턴스가 아닌 한, Network Load Balancers는 VPC 피어링 또는 AWS 관리형 VPN을 통한 클라이언트에서 로드 밸런서로의 연결을 지원하지 않습니다. VPC 피어링의 경우 두 VPC가 동일한 리전에 있어야 합니다.

대상이 예상보다 많은 상태 확인 요청을 수신함

Network Load Balancer에 대한 상태 확인은 분산되며 대상 상태를 결정하는 데 합의 메커니즘을 사용합니다. 그러므로 대상은 HealthCheckIntervalSeconds 설정을 통해 구성된 수보다 많은 상태 확인을 수신할 수 있습니다.

대상에 대한 상태 확인 수를 줄이려면 정적 HTML 파일을 HTTP 대상으로 사용하거나 TCP 상태 확인을 사용합니다.

대상이 예상보다 적은 상태 확인 요청을 수신함

net.ipv4.tcp_tw_recycle이 활성화되었는지 여부를 확인합니다. 이 설정은 로드 밸런서에 문제를 야기하는 것으로 알려져 있습니다. net.ipv4.tcp_tw_reuse 설정이 더 안전한 대안입니다.

비정상 대상이 로드 밸런서로부터 요청을 수신

로드 밸런서에 정상 상태의 대상이 한 개 이상 등록되어 있으면 로드 밸런서는 정상 상태의 등록 대상으로만 요청을 라우팅합니다. 비정상 상태의 대상만 등록되어 있으면 로드 밸런서는 모든 등록 대상에 요청을 라우팅합니다.

대상에서 로드 밸런서로의 요청에서 연결이 시간 초과됨

인스턴스 ID로 대상이 등록되는 내부 로드 밸런서가 있는지 확인합니다. 내부 로드 밸런서는 헤어핀 또는 루프백을 지원하지 않습니다. 대상을 인스턴스 ID로 등록하는 경우 클라이언트의 원본 IP 주소가 보존됩니다. 인스턴스가 인스턴스 ID로 등록된 내부 로드 밸런서의 클라이언트일 경우, 요청이 다른 인스턴스로 라우팅되는 경우에만 연결이 성공합니다. 그렇지 않으면 원본 및 대상 IP 주소가 동일하여 연결이 시간 초과됩니다.

인스턴스가 자신이 등록된 로드 밸런서로 요청을 전송해야 하는 경우 다음 중 하나를 수행합니다.

- 인스턴스를 인스턴스 ID 대신 IP 주소로 등록합니다. Amazon Elastic Container Service를 사용하는 경우, 작업에 awsvpc 네트워크 모드를 사용하여 대상 그룹을 IP 주소로 등록하도록 해야 합니다.
- 통신해야 하는 컨테이너가 다른 컨테이너 인스턴스에 있는지 확인합니다.
- 인터넷 경계 로드 밸런서를 사용합니다.

대상을 Network Load Balancer로 이동할 때 성능이 저하됨

Classic Load Balancers와 Application Load Balancers는 모두 연결 멀티플렉싱을 사용하지만 Network Load Balancers는 그렇지 않습니다. 그러므로 대상이 Network Load Balancer 뒤에서 더 많은 TCP 연결을 수신할 수 있습니다. 대상이 수신할 수 있는 연결 요청 볼륨을 처리할 준비가 되었는지 확인하십시오.

Network Load Balancers 제한

Network Load Balancers에 대한 현재 제한을 보려면 Amazon EC2 콘솔에서 제한 페이지를 확인하거나 [describe-account-limits](#)(AWS CLI) 명령을 사용합니다. 제한 증가를 요청하려면 [Elastic Load Balancing 제한 양식](#)을 사용하십시오.

AWS 계정에는 Network Load Balancers와 관련된 다음과 같은 제한이 있습니다.

리전 제한

- 리전당 Network Load Balancers: 20
- 리전당 대상 그룹: 3000 *

로드 밸런서 제한

- 로드 밸런서당 리스너: 50
- 로드 밸런서당 가용 영역당 서브넷: 1
- [교차 영역 로드 밸런싱이 비활성화된 경우] 로드 밸런서당 가용 영역당 대상: 500
- [교차 영역 로드 밸런싱이 활성화된 경우] 로드 밸런서당 대상: 500
- 대상 그룹당 로드 밸런서: 1

* 이 제한은 Application Load Balancers 및 Network Load Balancers의 대상 그룹에서 공유합니다.

Network Load Balancers 문서 기록

다음 표에서는 Network Load Balancers 릴리스를 설명합니다.

update-history-change	update-history-description	update-history-date
교차 영역 로드 밸런싱 (p. 39)	이 릴리스에서는 교차 영역 로드 밸런싱을 활성화하기 위한 지원이 추가되었습니다.	February 22, 2018
프록시 프로토콜	이번 릴리스에서는 프록시 프로토콜 활성화에 대한 지원을 추가합니다.	November 17, 2017
IP 주소를 대상으로 사용	이 릴리스에서는 IP 주소를 대상으로 등록에 대한 지원이 추가되었습니다.	September 21, 2017
새로운 로드 밸런서 유형 (p. 39)	이 Elastic Load Balancing 릴리스에는 Network Load Balancers가 도입되었습니다.	September 7, 2017