Elastic Load Balancing

Network Load Balancer

Elastic Load Balancing: Network Load Balancer

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 3

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

AWS CLI를 사용하여 시작하기 7
- 시작하기 전에 7
- 로드 밸런서 생성 7
- 로드 밸런서의 탄력적 IP 주소 지정 8
- 로드 밸런서 삭제 8

로드 밸런서 9
- 로드 밸런서 상태 9
- 로드 밸런서 속성 9
- 가용 영역 10
  - 교차 영역 로드 밸런싱 11
- 삭제 방지 11
- 연결 유휴 제한 시간 12
- DNS 이름 12
- 로드 밸런서 생성 13
  - 1단계: 로드 밸런서 및 리스너 구성 4
  - 2단계: 대상 그룹 구성 5
  - 3단계: 대상 그룹에 대상 등록 14
  - 4단계: 로드 밸런서 생성 15
- 태그 업데이트 15
- 로드 밸런서 삭제 16

리스너 17
- 리스너 구성 17
- 리스너 규칙 17
- 리스너 생성 17
  - 사전 조건 18
  - 리스너 추가 18
- TLS 리스너 구성 18
  - 서버 인증서 19
  - 보안 정책 20
  - ALPN 정책 22
- 리스너 업데이트 23
- TLS 리스너 업데이트 24
  - 기본 인증서 교체 24
  - 인증서 목록에 인증서 추가 24
  - 인증서 목록에서 인증서 제거 25
  - 보안 정책 업데이트 25
  - ALPN 정책 업데이트 26
- 리스너 삭제 26

대상 그룹 27
- 라우팅 구성 27

Target type(대상 유형) 28
라우팅 및 IP 주소 요청 28
소스 IP 보존 29
등록된 대상 29
대상 그룹 속성 30
등록 취소 지연 30
프록시 프로토콜 31
상태 확인 연결 31
VPC 엔드포인트 서비스 31
프록시 프로토콜 활성화 32
고정 세션 32
대상 그룹 생성 33
상태 확인 구성 35
상태 확인 설정 36
대상 상태 37
상태 확인 사유 코드 37
대상의 상태 확인 38
대상 그룹의 상태 확인 설정 수정 39
대상 등록 39
대상 보안 그룹 40
네트워크 ACL 40
대상 등록 또는 등록 취소 41
태그 업데이트 43
대상 그룹 삭제 44
로드 밸런서 모니터링 46
CloudWatch 지표 46
네트워크 로드 밸런서 지표 47
Network Load Balancer에 대한 지표 차원 52
Network Load Balancer 지표에 대한 통계 53
로드 밸런서에 대한 CloudWatch 지표 보기 53
액세스 로그 54
액세스 로그 파일 55
액세스 로그 항목 55
버킷 요구 사항 57
액세스 로그 활성화 58
액세스 로그 비활성화 58
액세스 로그 파일 처리 59
CloudTrail 로그 59
CloudTrail의 Elastic Load Balancing 정보 59
Elastic Load Balancing 로그 파일 항목 이해 60
문제 해결 62
등록된 대상은 서비스되지 않고 있습니다. 62
요청이 대상으로 라우팅되지 않음 62
대상이 예상보다 많은 상태 확인 요청을 수신함 62
대상이 예상보다 적은 상태 확인 요청을 수신함 63
비정상 대상이 로드 밸런서로부터 요청을 수신 63
호스트 헤더 불일치로 인해 대상이 HTTP 또는 HTTPS 상태 확인에 실패 63
대상에서 로드 밸런서로의 요청에서 연결 시간이 초과됨 63
대상을 Network Load Balancer로 이동할 때 성능이 저하됨 63
AWS PrivateLink를 통해 연결하는 포트 할당 오류 63
할당량 65
문서 기록 66

Network Load Balancer란 무엇입니까?

Elastic Load Balancing는 다음 유형의 로드 밸런서를 지원합니다. Application Load Balancer, Network Load Balancer, Classic Load Balancer. 이 안내서에서는 Network Load Balancer에 대해 설명합니다. 다른 로드 밸런서에 대한 자세한 내용은 Application Load Balancer 사용 설명서 및 Classic Load Balancer 사용 설명서 섹션을 참조하십시오.

Network Load Balancer 구성 요소

로드 밸런서는 클라이언트에 대한 단일 접점 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 지정한 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 지정한 대상 그룹에 등록된 모든 대상에서 상태 검사가 수행됩니다.

자세한 내용은 다음 설명서를 참조하세요.

- 로드밸런서 (p. 9)
- 리스너 (p. 17)
- 대상 그룹 (p. 27)

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 Balancing가 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 가용 영역 (p. 10) 단원을 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.

TCP 트래픽의 경우, 로드 밸런서는 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 포트

와 시퀀스 번호가 서로 다르므로 다른 대상에 라우팅될 수 있습니다. 각 TCP 연결은 연결 수명 동안 하나의 대상에 라우팅됩니다.

UDP 트래픽의 경우, 로드 밸런서는 프로토콜, 원본 IP 주소, 원본 포트, 대상 IP 주소, 대상 포트에 따라 흐름 해시 알고리즘을 사용하여 대상을 선택합니다. UDP 흐름은 소스와 목적지가 동일하기 때문에 수명이 다할 때까지 일관되게 단일 대상으로 라우트됩니다. 서로 다른 UDP 흐름에는 서로 다른 소스 IP 주소와 포트가 있으므로 다른 대상으로 라우팅될 수 있습니다.

Elastic Load Balancing는 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.

대상 그룹을 생성할 때 인스턴스 ID 또는 IP 주소로 대상을 등록해야 하는지 여부를 결정하는 대상 유형을 지정합니다. 인스턴스 ID로 대상을 등록하는 경우 클라이언트의 원본 IP 주소가 보존되고 애플리케이션에 제공됩니다. IP 주소로 대상을 등록하는 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 Balancing가 로드 밸런서를 확장합니다. Elastic Load Balancing는 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 사용 설명서의 Elastic Load Balancing 작동 방식을 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)은 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. 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 비교를 참조하십시오.

시작하는 방법

Network Load Balancer를 생성하려면 다음 자습서 중 하나를 시도해 보십시오.

- Network Load Balancer 시작하기 (p. 4)

- 자습서: AWS CLI를 사용하여 Network Load Balancer 생성 (p. 7)

일반적인 로드 밸런서 구성에 대한 데모는 Elastic Load Balancing 데모를 참조하십시오.

요금

자세한 내용은 Network Load Balancer 요금을 참조하십시오.

Network Load Balancer 시작하기

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

작업

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

또는 Application Load Balancer를 생성하려면 Application Load Balancer 사용 설명서의 Application Load Balancer 시작하기를 참조하십시오. Classic Load Balancer를 생성하려면 Classic Load Balancer 사용 설명서에서 Classic Load Balancer 생성을 참조하십시오.

일반적인 로드 밸런서 구성에 대한 데모는 Elastic Load Balancing 데모를 참조하십시오.

시작하기 전에

- 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. 40) 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 모음에서 로드 밸런서의 리전을 선택합니다. EC2 인스턴스에 사용한 리전과 동일한 리전을 선택해야 합니다.
3. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
4. 로드 밸런서 생성을 선택합니다.
5. Network Load Balancer에서 생성을 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 Balancer 및 Network Load Balancer 세트 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 하나의 퍼블릭 서브넷을 선택합니다.

   기본적으로 AWS는 가용 영역에 대한 서브넷의 각 로드 밸런서 노드에 IPv4 주소를 할당합니다. 또는 인터넷 경계 로드 밸런서를 생성하는 경우 각 가용 영역에 대해 탄력적인 IP 주소를 선택할 수 있습니다. 그러면 로드 밸런서에 고정 IP 주소가 제공됩니다.
5. 다음: 라우팅 구성을 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 group(대상 그룹)에는 기본 값인 New target group(새 대상 그룹)을 그대로 둡니다.
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 Targets(다음: 대상 등록)를 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 로드 밸런싱에서 로드 밸런서를 선택합니다.
7. 새로 생성한 로드 밸런서를 선택합니다.
8. [Description]을 선택하고, 로드 밸런서의 DNS 이름(예: my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com)을 복사합니다. DNS 이름을 인터넷에 연결된 웹 브라우저의 주소 필드에 붙여 넣습니다. 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Actions], [Delete]를 차례로 선택합니다.
4. 확인 메시지가 나타나면 예, 삭제합니다를 선택합니다.

자습서: AWS CLI를 사용하여 Network Load Balancer 생성

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

시작하기 전에

- AWS CLI를 설치하거나 Network Load Balancer를 지원하지 않는 버전을 사용하는 경우 AWS CLI로 업데이트합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS Command Line Interface 설치를 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. 40) 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-0e3f5cac72EXAMPLE
```

   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-0598c7d356EXAMPLE
```

   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-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. 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
```

5. (선택 사항) 다음과 같이 이 https://docs.aws.amazon.com/cli/latest/reference/elbv2/describe-target-health.html 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-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

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 Balancer

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. 27)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. 17)를 생성하여 클라이언트의 연결 요청을 확인하고, 클라이언트에서 대상 그룹에 있는 대상으로 요청을 라우팅합니다.

Network Load Balancer는 VPC 피어링, AWS 관리형 VPN, AWS Direct Connect 및 타사 VPN 솔루션을 통해 클라이언트에서의 연결을 지원합니다.

목차

- 로드 밸런서 상태 (p. 9)
- 로드 밸런서 속성 (p. 9)
- 가용 영역 (p. 10)
- 삭제 방지 (p. 11)
- 연결 유휴 제한 시간 (p. 12)
- DNS 이름 (p. 12)
- Network Load Balancer 만들기 (p. 13)
- Network Load Balancer 태그 (p. 15)
- Network Load Balancer 삭제 (p. 16)

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 (p. 11) 기능의 활성화 여부를 나타냅니다. 기본값은 `false`입니다.

`load_balancing.cross_zone.enabled`

교차 영역 로드 밸런싱 (p. 11)의 활성화 여부를 나타냅니다. 기본값은 `false`입니다.

가용 영역

로드 밸런서를 생성할 때 하나 이상의 가용 영역을 활성화합니다. 로드 밸런서에서 가용 영역을 여러 개 활성화하면 애플리케이션의 내결함성이 높아집니다. 생성한 후에는 Network Load Balancer에 대한 가용 영역을 비활성화할 수 없지만 추가 가용 영역을 활성화할 수 있습니다.

가용 영역을 활성화할 때 해당 가용 영역에서 서브넷을 하나 지정합니다. Elastic Load Balancing은 가용 영역에 로드 밸런서 노드를 생성하고 서브넷의 네트워크 인터페이스를 만듭니다(설명은 'ELB net'으로 시작하며 로드 밸런서의 이름을 포함함). 가용 영역의 각 로드 밸런서 노드는 이 네트워크 인터페이스를 사용하여 IPv4 주소를 가져옵니다. 이 네트워크 인터페이스를 볼 수 있으나 수정할 수는 없습니다.

인터넷 경계 로드 밸런서를 생성하는 경우 필요에 따라 서브넷당 하나의 탄력적인 IP 주소를 지정할 수 있습니다. 고유한 탄력적인 IP 주소 중 하나를 선택하지 않는 경우 Elastic Load Balancing는 서브넷당 하나의 탄력적인 IP 주소를 제공합니다. 이러한 탄력적인 IP 주소는 로드 밸런서 수명 동안 변경되지 않는 고정 IP 주소를 로드 밸런서에 제공합니다. 로드 밸런서를 생성한 후에는 이러한 탄력적인 IP 주소를 변경할 수 없습니다.

내부 로드 밸런서를 생성하는 경우 필요에 따라 서브넷당 하나의 프라이빗 IP 주소를 지정할 수 있습니다. 서브넷에서 IP 주소를 지정하지 않으면 Elastic Load Balancing에서 하나를 자동으로 선택합니다. 이러한 프라이빗 IP 주소는 로드 밸런서 수명 동안 변경되지 않는 고정 IP 주소를 로드 밸런서에 제공합니다. 로드 밸런서를 생성한 후에는 이러한 프라이빗 IP 주소를 변경할 수 없습니다.

요구 사항

- 인터넷 경계 로드 밸런서의 경우, 사용자가 지정하는 서브넷에 사용 가능한 IP 주소가 8개 이상 있어야 합니다. 내부 로드 밸런서의 경우, AWS가 서브넷에서 프라이빗 IPv4 주소를 선택할 수 있는 경우에만 필요합니다.
- 제약된 가용 영역의 서브넷은 지정할 수 없습니다. 해당 오류 메시지는 "유형이 'network'인 로드 밸런서는 az_name에서 지원되지 않음"과 같습니다. 제약되지 않은 다른 가용 영역의 서브넷을 지정하고 교차 영역 로드 밸런싱을 사용하여 제약된 가용 영역의 대상에 트래픽을 분산할 수 있습니다.
- 로컬 영역에서는 서브넷을 지정할 수 없습니다.

가용 영역을 활성화하고 나면 로드 밸런서가 해당 가용 영역의 등록 대상으로 요청을 라우팅하기 시작합니다. 활성화된 각 가용 영역에 등록된 대상이 하나 이상 있는지 확인하는 경우에 로드 밸런서가 가장 효과적입니다.

콘솔을 사용하여 가용 영역을 추가하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. [Description] 탭에서 [Basic Configuration] 아래 [Edit subnets]을 선택합니다.
5. 가용 영역을 활성화하려면 해당 가용 영역 확인란을 선택합니다. 가용 영역에 대해 서브넷 한 개가 있는 경우 해당 서브넷이 선택됩니다. 가용 영역에 대해 서브넷이 두 개 이상 있는 경우 서브넷 중 하나를 선택합니다. 가용 영역당 서브넷을 한 개만 선택할 수 있습니다.

   인터넷 경계 로드 밸런서의 경우, 각 가용 영역에 대해 탄력적인 IP 주소를 선택할 수 있습니다. 내부 로드 밸런서의 경우, Elastic Load Balancing에서 할당하는 대신 각 서브넷의 IPv4 범위에서 프라이빗 IP 주소를 할당할 수 있습니다.

6. 저장을 선택합니다.

AWS CLI를 사용하여 가용 영역을 추가하려면

set-subnets 명령을 사용합니다.

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 사용 설명서의 교차 영역 로드 밸런싱을 참조하십시오.

콘솔을 사용하여 교차 영역 로드 밸런싱을 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 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.

연결 유휴 제한 시간

클라이언트가 Network Load Balancer를 통해 생성하는 각 TCP 요청에 대해 연결 상태는 추적됩니다. 유휴 제한 시간보다 오래 클라이언트 또는 대상에 의한 연결을 통해 데이터가 전송되지 않으면 연결이 닫힙니다. 유휴 제한 시간이 지난 후 클라이언트 또는 대상에서 데이터를 보내면 연결이 더 이상 유효하지 않음을 나타내는 TCP RST 패킷이 수신됩니다.

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

UDP가 연결이 없는 동안 로드 밸런서는 소스 및 대상 IP 주소와 포트를 기반으로 UDP 흐름 상태를 유지하므로 동일한 흐름에 속한 패킷이 일관되게 동일한 대상으로 전송됩니다. 유휴 시간 초과 기간이 지나면 로드 밸런서는 들어오는 UDP 패킷을 새 흐름으로 간주하여 새 대상으로 라우트합니다. Elastic Load Balancing는 UDP 흐름의 유휴 제한 시간 값을 120초로 설정합니다.

EC2 인스턴스는 반환 경로를 설정하기 위해 30초 이내에 새 요청에 응답해야 합니다.

DNS 이름

각 Network Load Balancer는 *name*-*id*.elb.*region*.amazonaws.com을 포함하는 기본 설정된 DNS(Domain Name System) 이름을 수신합니다. 예: my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com.

기억하기 쉬운 DNS 이름을 사용하는 것을 선호하는 경우, 사용자 지정 도메인 이름을 생성하고 이를 로드 밸런서의 DNS 이름과 연결할 수 있습니다. 클라이언트가 이러한 사용자 지정 도메인 이름을 사용해 요청을 하면 DNS 서버는 이를 로드 밸런서의 DNS 이름으로 해석합니다.

먼저 인증된 도메인 등록 대행자를 이용해 도메인 이름을 등록합니다. 다음으로 CNAME 레코드를 생성하여 쿼리를 로드 밸런서로 라우팅 요청을 하려면 도메인 등록 대행자와 같은 DNS 서비스를 사용하면 됩니다. 자세한 내용은 DNS 서비스에 대한 설명서를 참조하십시오. 예를 들면, Amazon Route 53을 DNS 서비스로 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 ELB 로드 밸런서로 트래픽 라우팅을 참조하십시오.

로드 밸런서는 활성화된 각 가용 영역에 대하여 하나의 IP 주소를 가집니다. 이는 로드 밸런서 노드의 주소입니다. 로드 밸런서의 DNS 이름은 이러한 주소로 확인됩니다. 예를 들어, 로드 밸런서의 사용자 지정 도메인 이름이 `example.networkloadbalancer.com`이라고 가정해 보겠습니다. 다음 dig 또는 nslookup 명령을 사용하여 로드 밸런서 노드의 IP 주소를 확인합니다.

Linux 또는 Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

로드 밸런서는 로드 밸런서 노드를 위한 DNS 레코드를 가집니다. *az*.*name*-*id*.elb.*region*.amazonaws.com을 포함하는 이름의 DNS 이름을 사용하여 로드 밸런서 노드의 IP 주소를 확인할 수 있습니다.

Linux 또는 Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Network Load Balancer 만들기

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

시작하기 전에 로드 밸런서의 Virtual Private Cloud(VPC)에 대상이 있는 각 가용성 영역에 하나 이상의 공용 서브넷이 있는지 확인하십시오.

AWS CLI를 사용하여 로드 밸런서 생성하려면 자습서: AWS CLI를 사용하여 Network Load Balancer 생성 (p. 7) 단원을 참조하십시오.

AWS Management 콘솔을 사용하여 로드 밸런서를 생성하려면 다음 작업을 완료합니다.

작업

- 1단계: 로드 밸런서 및 리스너 구성 (p. 4)
- 2단계: 대상 그룹 구성 (p. 5)
- 3단계: 대상 그룹에 대상 등록 (p. 14)
- 4단계: 로드 밸런서 생성 (p. 15)

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. 17) 섹션을 참조하십시오.

로드 밸런서 및 리스너를 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. 로드 밸런서 생성을 선택합니다.
4. Network Load Balancer에서 생성을 선택합니다.
5. Name에 로드 밸런서 이름을 입력합니다. 예: **my-nlb**.
6. 체계에서 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.

   기본적으로 AWS는 가용 영역에 대한 서브넷의 각 로드 밸런서 노드에 IPv4 주소를 할당합니다. 또는 인터넷 연결 로드 밸런서를 만드는 경우 각 가용 영역에 대해탄력적인 IP 주소를 선택할 수 있습니다. 그러

면 로드 밸런서에 고정 IP 주소가 제공됩니다. 내부 로드 밸런서의 경우, AWS에서 할당하는 대신 각 서브넷의 IPv4 범위에서 프라이빗 IP 주소를 할당할 수 있습니다.

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 Balancer 대상 그룹 (p. 27) 섹션을 참조하십시오.

대상 그룹을 구성하려면

1. 대상 그룹에서는 기본값인 New target group(새 대상 그룹)을 유지합니다.
2. 이름에 대상 그룹의 이름을 입력합니다.
3. 프로토콜에 대해 다음과 같이 프로토콜을 선택합니다.
   - 리스너 프로토콜이 TCP인 경우, TCP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TLS인 경우, TCP 또는 TLS를 선택합니다.
   - 리스너 프로토콜이 UDO인 경우, UDP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TCP_UDP인 경우, TCP_UDP를 선택합니다.
4. (선택 사항) 필요한 대로 포트를 설정합니다.
5. 대상 유형에서 인스턴스 ID 또는 `ip`로 대상을 지정할 `instance`를 선택하여 IP 주소로 대상을 지정합니다. 대상 그룹 프로토콜이 UDP 또는 TCP_UDP인 경우, `instance`를 선택해야 합니다.
6. 상태 검사는 기본 상태 확인 설정을 그대로 둡니다.
7. Next: Register Targets(다음: 대상 등록)를 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 결정합니다. 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. 16) 섹션을 참조하십시오.

로드 밸런서를 생성하려면

1. [Review] 페이지에서 [Create]을 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 LOAD BALANCING에서 로드 밸런서를 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. 11) 단원을 참조하십시오.

로드 밸런서가 다른 서비스에서 사용 중인 경우 삭제할 수 없습니다. 예를 들어 로드 밸런서가 VPC 엔드포인트 서비스와 연결되어 있는 경우 연결된 로드 밸런서를 삭제하기 전에 엔드포인트 서비스 구성을 삭제해야 합니다.

로드 밸런서를 삭제하면 리스너도 삭제됩니다. 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. 44) 섹션을 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
3. 탐색 창의 LOAD BALANCING에서 로드 밸런서를 선택합니다.
4. 로드 밸런서를 선택합니다.
5. [Actions], [Delete]를 선택합니다.
6. 확인 메시지가 나타나면 예, 삭제를 선택합니다.

AWS CLI를 사용하여 로드 밸런서를 삭제하려면

delete-load-balancer 명령을 사용합니다.

Network Load Balancer용 리스너

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

자세한 내용은 Elastic Load Balancing 사용 설명서의 라우팅 요청을 참조하십시오.

목차

- 리스너 구성 (p. 17)
- 리스너 규칙 (p. 17)
- Network Load Balancer용 리스너 생성 (p. 17)
- Network Load Balancer를 위한 TLS 리스너 (p. 18)
- Network Load Balancer용 리스너 업데이트 (p. 23)
- Network Load Balancer용 TLS 리스너 업데이트 (p. 24)
- Network Load Balancer용 리스너 삭제 (p. 26)

리스너 구성

리스너는 다음과 같은 프로토콜 및 포트를 지원합니다.

- 프로토콜: TCP, TLS, UDP, TCP_UDP
- 포트: 1-65535

애플리케이션이 비즈니스 로직에 집중할 수 있도록 TLS 리스너를 사용하여 암호화 및 암호 해독 작업을 로드 밸런서로 오프로드할 수 있습니다. 리스너 프로토콜이 TLS인 경우에는 리스너에 정확히 한 개의 SSL 서버 인증서를 반드시 배포해야 합니다. 자세한 내용은 Network Load Balancer를 위한 TLS 리스너 (p. 18) 단원을 참조하십시오.

동일한 포트에서 TCP와 UDP를 모두 지원하려면 TCP_UDP 리스너를 만드십시오. TCP_UDP 리스너의 대상 그룹은 TCP_UDP 프로토콜을 사용해야 합니다.

리스너에 WebSockets를 사용할 수 있습니다.

구성된 리스너로 전송된 모든 네트워크 트래픽은 의도된 트래픽으로 분류됩니다. 구성된 리스너와 일치하지 않는 네트워크 트래픽은 의도하지 않은 트래픽으로 분류됩니다. 유형 3 이외의 ICMP 요청도 의도하지 않은 트래픽으로 간주됩니다. Network Load Balancer는 의도하지 않은 트래픽을 임의의 대상으로 전달하지 않고 삭제합니다. 새 연결이 아니거나 활성 TCP 연결의 일부가 아닌 구성된 리스너에 대해 리스너 포트로 전송된 TCP 데이터 패킷은 RST(TCP 재설정)를 통해 거부됩니다.

리스너 규칙

리스너를 생성할 때 라우팅 요청의 규칙을 지정합니다. 이 규칙은 요청을 지정된 대상 그룹으로 전달합니다. 이 규칙을 업데이트하려면 Network Load Balancer용 리스너 업데이트 (p. 23) 섹션을 참조하십시오.

Network Load Balancer용 리스너 생성

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

사전 조건

- 리스너 규칙에 대한 대상 그룹을 지정해야 합니다. 자세한 내용은 Network Load Balancer 대상 그룹 생성 (p. 33) 섹션을 참조하십시오.
- TLS 리스너에 대해 SSL 인증서를 지정해야 합니다. 로드 밸런서는 이 인증서를 사용해 연결을 종료하고 대상으로 전송하기 전에 클라이언트의 요청을 해독합니다. 자세한 내용은 서버 인증서 (p. 19) 단원을 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. 17) 섹션을 참조하십시오.

콘솔을 사용하여 리스너를 추가하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. 리스너 추가를 선택합니다.
5. Protocol: port(프로토콜: 포트)에서 TCP, UDP, TCP_UDP, 또는 TLS를 선택합니다. 기본 포트를 그대로 두거나 다른 포트를 입력합니다.
6. [TLS 리스너] ALPN 정책의 경우 ALPN을 활성화할 정책을 선택하거나 [None]을 선택하여 ALPN을 비활성화합니다. 자세한 내용은 ALPN 정책 (p. 22) 단원을 참조하십시오.
7. Default actions(기본 작업)에서 Add action(작업 추가), Forward to(다음으로 전달)를 선택하고 사용 가능한 대상 그룹을 선택합니다.
8. [TLS 리스너] Select policy(정책 선택)에서 기본 보안 정책을 유지하는 것이 좋습니다.
9. [TLS 리스너] Default SSL certificate(기본 SSL 인증서)에서 다음 중 한 가지를 수행합니다.
   - AWS Certificate Manager을 사용하여 인증서를 생성하거나 가져온 경우 ACM에서 시작을 선택하고 인증서를 선택하십시오.
   - IAM을 사용하여 인증서를 업로드한 경우 IAM에서 시작을 선택하고 인증서를 선택하십시오.
10. Save를 선택합니다.
11. [TLS 리스너] SNI 프로토콜에 사용할 인증서 목록을 추가(선택 사항)하려면 인증서 목록에 인증서 추가 (p. 24) 단원을 참조하십시오.

AWS CLI를 사용하여 리스너를 추가하려면

create-listener 명령을 사용하여 리스너를 생성합니다.

Network Load Balancer를 위한 TLS 리스너

TLS 리스너를 사용하려면 로드 밸런서에 한 개 이상의 서버 인증서를 반드시 배포해야 합니다. 로드 밸런서는 서버 인증서를 사용해 프런트 엔드 연결을 종료한 다음, 대상으로 전송하기 전에 클라이언트의 요청을 해독합니다.

Elastic Load Balancing는 보안 정책(security policy)이라고 하는 TLS 협상 구성을 사용해 클라이언트와 로드 밸런서 간에 TLS 연결을 협상합니다. 보안 정책은 프로토콜과 암호의 조합입니다. 프로토콜은 클라이언트와 서버 간에 보안 연결을 설정하여 클라이언트와 로드 밸런서 간에 전달되는 모든 데이터를 안전하게 보호합니다. 암호는 코딩된 메시지를 생성하기 위해 암호화 키를 사용하는 암호화 알고리즘입니다. 프로토콜은 여러

개의 암호를 사용해 인터넷 상의 데이터를 암호화합니다. 연결 협상이 이루어지는 동안 클라이언트와 로드 밸런서는 각각이 지원하는 암호 및 프로토콜 목록을 선호도 순으로 표시합니다. 서버의 목록에서 클라이언트의 암호 중 하나와 일치하는 첫 번째 암호가 보안 연결을 위해 선택됩니다.

Network Load Balancer는 TLS 재협상을 지원하지 않습니다.

TLS 리스너를 생성하려면 리스너 추가 (p. 18) 단원을 참조하십시오. 관련 데모는 Network Load Balancer에서의 TLS 지원 및 Network Load Balancer에서의 SNI 지원을 참조하십시오.

서버 인증서

로드 밸런서에는 X.509 인증서(서버 인증서)가 필요합니다. 인증서는 인증 기관(CA)에서 발행한 디지털 형태의 ID 증명서입니다. 인증서에는 식별 정보, 유효 기간, 퍼블릭 키, 일련번호, 발행자의 디지털 서명이 들어 있습니다.

로드 밸런서와 함께 사용할 인증서를 생성할 때 도메인 이름을 지정해야 합니다.

AWS Certificate Manager(ACM)을 사용하여 로드 밸런서에 대한 인증서를 생성하는 것이 좋습니다. ACM은 Elastic Load Balancing와 통합하므로 로드 밸런서에 인증서를 배포할 수 있습니다. 자세한 내용은 AWS Certificate Manager 사용 설명서 섹션을 참조하십시오.

또는 TLS 도구를 사용해 인증서 서명 요청(CSR)을 생성하고 CA가 서명한 CSR을 가져와서 인증서를 만든 다음, ACM으로 인증서를 가져오거나 AWS Identity and Access Management(IAM)으로 인증서를 업로드할 수 있습니다. 자세한 내용은 AWS Certificate Manager 사용 설명서의 인증서 가져오기 또는 IAM 사용 설명서의 서버 인증서 작업을 참조하십시오.

> **Important**
>
> Network Load Balancer에 2,048비트가 넘는 RSA 키 또는 EC 키가 포함된 인증서를 설치할 수 없습니다.

기본 인증서

TLS 리스너를 생성할 때 인증서 하나를 꼭 지정해야 합니다. 이 인증서를 기본 인증서라고 합니다. TLS 리스너를 생성한 후 기본 인증서를 교체할 수 있습니다. 자세한 내용은 기본 인증서 교체 (p. 24) 단원을 참조하십시오.

인증서 목록 (p. 19)에서 추가 인증서를 지정하면 클라이언트가 SNI(서버 이름 표시) 프로토콜을 사용하지 않고 호스트 이름을 지정하여 연결하거나 인증서 목록에 일치하는 인증서가 없는 경우에만 기본 인증서가 사용됩니다.

추가 인증서를 지정하지 않지만 단일 로드 밸런서를 통해 보안 애플리케이션을 여러 개 호스팅해야 하는 경우, 와일드카드 인증서를 사용하거나 인증서에 각 추가 도메인의 주체 대체 이름(SAN)을 추가할 수 있습니다.

인증서 목록

TLS 리스너를 생성한 후 리스너에는 기본 인증서와 빈 인증서 목록이 있습니다. 필요에 따라 리스너의 인증서 목록에 인증서를 추가할 수 있습니다. 인증서 목록을 사용하면 로드 밸런서가 동일한 포트의 여러 도메인을 지원하고 각 도메인에 대해 다른 인증서를 제공할 수 있습니다. 자세한 내용은 인증서 목록에 인증서 추가 (p. 24) 단원을 참조하십시오.

로드 밸런서는 SNI를 지원하는 스마트 인증서 선택 알고리즘을 사용합니다. 클라이언트가 제공한 호스트 이름이 인증서 목록의 단일 인증서와 일치하면 로드 밸런서는 이 인증서를 선택합니다. 클라이언트가 제공한 호스트 이름이 인증서 목록의 여러 인증서와 일치하면 로드 밸런서는 클라이언트가 지원할 수 있는 최선의 인증서를 선택합니다. 인증서 선택은 다음 조건에 따라 다음 순서대로 이루어집니다.

- 퍼블릭 키 알고리즘(RSA보다 ECDSA 선호)

- 해싱 알고리즘(MD5보다 SHA 선호)
- 키 길이(가장 큰 길이 선호)
- 유효 기간

로드 밸런서 액세스 로그 항목은 클라이언트가 지정한 호스트 이름과 클라이언트에 제공된 인증서를 나타냅니다. 자세한 내용은 액세스 로그 항목 (p. 55) 단원을 참조하십시오.

인증서 갱신

각 인증서에는 유효 기간이 있습니다. 유효 기간이 끝나기 전에 로드 밸런서의 각 인증서를 갱신 또는 교체해야 합니다. 여기에는 기본 인증서와 인증서 목록의 인증서가 포함됩니다. 인증서를 갱신 또는 교체해도 로드 밸런서 노드에 수신되어 상태가 양호한 대상으로 라우팅이 보류 중인 진행 중 요청에는 영향을 주지 않습니다. 인증서를 갱신하면 새 요청에서 갱신된 인증서를 사용합니다. 인증서를 교체하면 새 요청에서 새 인증서를 사용합니다.

인증서 갱신 및 교체를 다음과 같이 관리할 수 있습니다.

- AWS Certificate Manager가 제공하고 로드 밸런서에 배포된 인증서는 자동으로 갱신이 가능합니다. ACM는 인증서가 만료되기 전에 인증서 갱신을 시도합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서의 관리형 갱신을 참조하십시오.
- ACM에 인증서를 가져온 경우에는 인증서의 만료일을 반드시 모니터링해서 만료되기 전에 인증서를 갱신해야 합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서의 인증서 가져오기를 참조하십시오.
- IAM으로 인증서를 가져온 경우, 새 인증서를 만들어 ACM 또는 IAM으로 가져온 후 로드 밸런서에 새 인증서를 추가하고, 만료된 인증서를 로드 밸런서에서 제거해야 합니다.

보안 정책

TLS 리스너를 생성할 때 보안 정책을 선택해야 합니다. 필요에 따라 보안 정책을 업데이트할 수 있습니다. 자세한 내용은 보안 정책 업데이트 (p. 25) 단원을 참조하십시오.

프런트 엔드 연결에서 사용되는 보안 정책을 선택할 수 있습니다. 백엔드 연결에는 `ELBSecurityPolicy-2016-08` 보안 정책이 항상 사용됩니다. Network Load Balancer는 사용자 지정 보안 정책을 지원하지 않습니다.

Elastic Load Balancing는 Network Load Balancer에 대해 다음과 같은 보안 정책을 제공합니다.

- `ELBSecurityPolicy-2016-08` (default)
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-FS-2018-06`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-2015-05`(`ELBSecurityPolicy-2016-08`과 동일)

호환성을 위해 `ELBSecurityPolicy-2016-08` 정책을 사용하는 것이 좋습니다. FS(Forward Secrecy)가 필요한 경우 `ELBSecurityPolicy-FS` 정책 중 하나를 사용할 수 있습니다. `ELBSecurityPolicy-TLS` 정책 중 하나를 사용하여 특정한 TLS 프로토콜 버전을 비활성화해야 하는 규정 준수 및 보안 표준을 충족하거나 암호 사용 중지가 필요한 기존 클라이언트를 지원할 수 있습니다. 인터넷 클라이언트만 TLS 버전 1.0

이 필요한 인터넷 클라이언트 비율은 적습니다. 로드 밸런서에 대한 요청에서 TLS 프로토콜 버전을 확인하려면 로드 밸런서에서 액세스 로깅을 활성화하고 액세스 로그를 검사하십시오. 자세한 내용은 액세스 로그 (p. 54)를 참조하십시오.

다음 표에서는 기본 정책과 `ELBSecurityPolicy-TLS` 정책에 대해 설명합니다.

보안 정책	기본값	TLS 1.0 †	TLS 1.1	TLS 1.2	TLS 1.2 ext
TLS 프로토콜					
Protocol-TLSv1	◆	◆			
Protocol-TLSv1.1	◆	◆	◆		
Protocol-TLSv1.2	◆	◆	◆	◆	◆
TLS 암호					
ECDHE-ECDSA-AES128-GCM-SHA256	◆	◆	◆	◆	◆
ECDHE-RSA-AES128-GCM-SHA256	◆	◆	◆	◆	◆
ECDHE-ECDSA-AES128-SHA256	◆	◆	◆	◆	◆
ECDHE-RSA-AES128-SHA256	◆	◆	◆	◆	◆
ECDHE-ECDSA-AES128-SHA	◆	◆	◆		◆
ECDHE-RSA-AES128-SHA	◆	◆	◆		◆
ECDHE-ECDSA-AES256-GCM-SHA384	◆	◆	◆	◆	◆
ECDHE-RSA-AES256-GCM-SHA384	◆	◆	◆	◆	◆
ECDHE-ECDSA-AES256-SHA384	◆	◆	◆	◆	◆
ECDHE-RSA-AES256-SHA384	◆	◆	◆	◆	◆
ECDHE-RSA-AES256-SHA	◆	◆	◆		◆
ECDHE-ECDSA-AES256-SHA	◆	◆	◆		◆
AES128-GCM-SHA256	◆	◆	◆	◆	◆
AES128-SHA256	◆	◆	◆	◆	◆
AES128-SHA	◆	◆	◆		◆
AES256-GCM-SHA384	◆	◆	◆	◆	◆
AES256-SHA256	◆	◆	◆	◆	◆
AES256-SHA	◆	◆	◆		◆
DES-CBC3-SHA		◆			

† 보안이 약한 DES-CBC3-SHA 암호를 필요로 하는 기존 클라이언트를 지원하지 않는 한 이 정책을 사용해서는 안 됩니다.

다음 표에서는 기본 정책과 `ELBSecurityPolicy-FS` 정책에 대해 설명합니다.

보안 정책	기본값	FS	FS 1.1	FS 1.2	FS 1.2 res
TLS 프로토콜					
Protocol-TLSv1	♦	♦			
Protocol-TLSv1.1	♦	♦	♦		
Protocol-TLSv1.2	♦	♦	♦	♦	♦
TLS 암호					
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA	♦	♦	♦	♦	
ECDHE-RSA-AES128-SHA	♦	♦	♦	♦	
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦	
ECDHE-ECDSA-AES256-SHA	♦	♦	♦	♦	
AES128-GCM-SHA256	♦				
AES128-SHA256	♦				
AES128-SHA	♦				
AES256-GCM-SHA384	♦				
AES256-SHA256	♦				
AES256-SHA	♦				

AWS CLI를 사용하여 로드 밸런서에 대한 보안 정책 구성을 보려면 describe-ssl-policies 명령을 사용하십시오.

ALPN 정책

ALPN(Application-Layer Protocol Negotiation)은 최초 TLS 핸드셰이크 hello 메시지를 통해 전송되는 TLS 확장입니다. ALPN을 사용하면 애플리케이션 계층이 HTTP/1 및 HTTP/2 같은 보안 연결을 통해 사용해야 하는 프로토콜을 협상할 수 있습니다.

클라이언트가 ALPN 연결을 시작하면 로드 밸런서는 클라이언트 ALPN 기본 설정 목록을 해당 ALPN 정책과 비교합니다. 클라이언트가 ALPN 정책의 프로토콜을 지원하는 경우 로드 밸런서는 ALPN 정책의 기본 설정 목록을 기반으로 연결을 설정합니다. 그렇지 않을 경우 로드 밸런서는 ALPN을 사용하지 않습니다.

요구 사항

- TLS 리스너
- TLS 대상 그룹

지원되는 ALPN 정책

지원되는 ALPN 정책은 다음과 같습니다.

`HTTP1Only`

HTTP/1.*만 협상합니다. ALPN 기본 설정 목록은 http/1.1, http/1.0입니다.

`HTTP2Only`

HTTP/2만 협상합니다. ALPN 기본 설정 목록은 h2입니다.

`HTTP2Optional`

HTTP/2보다 HTTP/1.*를 선호합니다(HTTP/2 테스트에 유용할 수 있음). ALPN 기본 설정 목록은 http/1.1, http/1.0, h2입니다.

`HTTP2Preferred`

HTTP/1.*보다 HTTP/2를 선호합니다. ALPN 기본 설정 목록은 h2, http/1.1, http/1.0입니다.

`None`

ALPN을 협상하지 않습니다. 이 값이 기본값입니다.

ALPN 연결 활성화

TLS 리스너를 생성하거나 수정할 때 ALPN 연결을 활성화할 수 있습니다. 자세한 내용은 리스너 추가 (p. 18) 및 ALPN 정책 업데이트 (p. 26) 단원을 참조하십시오.

Network Load Balancer용 리스너 업데이트

리스너 포트, 리스너 프로토콜 또는 기본 리스너 규칙을 업데이트할 수 있습니다.

기본 리스너 규칙은 요청을 지정된 대상 그룹으로 전달합니다.

프로토콜을 TCP 또는 UDP에서 TLS로 변경하는 경우, 보안 정책 및 서버 인증서를 지정해야 합니다. 프로토콜을 TLS 또는 UDP에서 TCP로 변경하는 경우, 보안 정책 및 서버 인증서는 제거됩니다.

콘솔을 사용하여 리스너를 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. 리스너의 확인란을 선택하고 Edit(편집)를 선택합니다.
5. (선택 사항) Protocol: port(프로토콜: 포트)에 대해 지정된 값을 변경하십시오.
6. (선택 사항) 연필 아이콘을 클릭하여 기본 작업에 대해 다른 대상 그룹을 선택합니다.
7. [Update]를 선택합니다.

AWS CLI를 사용하여 리스너를 업데이트하려면

modify-listener 명령을 사용하십시오.

Network Load Balancer용 TLS 리스너 업데이트

TLS 리스너를 생성한 후 기본 인증서를 교체하거나, 인증서 목록의 인증서를 추가 또는 제거하거나, 보안 정책을 업데이트하거나, ALPN 정책을 업데이트할 수 있습니다.

제한

Network Load Balancer에 2,048비트가 넘는 RSA 키 또는 EC 키가 포함된 인증서를 설치할 수 없습니다.

작업

- 기본 인증서 교체 (p. 24)
- 인증서 목록에 인증서 추가 (p. 24)
- 인증서 목록에서 인증서 제거 (p. 25)
- 보안 정책 업데이트 (p. 25)
- ALPN 정책 업데이트 (p. 26)

기본 인증서 교체

다음 절차에 따라 TLS 리스너의 기본 인증서를 교체할 수 있습니다. 자세한 내용은 기본 인증서 (p. 19) 단원을 참조하십시오.

콘솔을 사용하여 기본 인증서를 교체하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. 리스너의 확인란을 선택하고 Edit(편집)를 선택합니다.
5. Default SSL certificate(기본 SSL 인증서)에 대해 다음 중 하나를 수행합니다.
   - AWS Certificate Manager을 사용하여 인증서를 생성하거나 가져온 경우 ACM에서 시작을 선택하고 인증서를 선택하십시오.
   - IAM을 사용하여 인증서를 업로드한 경우 IAM에서 시작을 선택하고 인증서를 선택하십시오.
6. [Update]를 선택합니다.

AWS CLI를 사용하여 기본 인증서를 교체하려면

--certificates 옵션과 함께 modify-listener 명령을 사용합니다.

인증서 목록에 인증서 추가

다음 절차에 따라 리스너 인증서 목록에 인증서를 추가할 수 있습니다. TLS 리스너를 처음 생성할 때 인증서 목록은 비어 있습니다. 인증서를 하나 이상 추가할 수 있습니다. 필요에 따라 기본 인증서를 추가하여 이 인증서가 기본 인증서로 교체되더라도 SNI 프로토콜에 이 인증서가 사용되도록 할 수 있습니다. 자세한 내용은 인증서 목록 (p. 19) 단원을 참조하십시오.

콘솔을 사용하여 인증서 목록에 인증서를 추가하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.

4. 업데이트할 HTTPS 리스너에 대해 View/edit certificates(인증서 보기/편집)를 선택합니다. 그러면 기본 인증서가 표시되고 리스너에 추가한 다른 인증서가 그 다음에 표시됩니다.
5. 메뉴 모음에서Add certificates(인증서 추가) 아이콘(플러스 기호)을 선택하십시오. 그러면 기본 인증서가 나타나고 ACM 및 IAM에서 관리하는 기타 인증서가 그 뒤에 표시됩니다. 리스너에 인증서를 이미 추가한 경우 해당 확인란이 선택되고 비활성화됩니다.
6. ACM 또는 IAM에서 이미 관리하는 인증서를 추가하려면 인증서의 확인란을 선택하고 추가를 선택하십시오.
7. ACM 또는 IAM에서 관리하지 않는 인증서가 있으면 다음과 같이 ACM로 가져온 후 리스너에 추가하십시오.

   a. [Import certificate]를 선택합니다.
   b. [Certificate private key]에 인증서의 암호화되지 않은 PEM 인코딩 형식 프라이빗 키를 붙여 넣습니다.
   c. [Certificate body]에 PEM 인코딩 형식의 인증서를 붙여 넣습니다.
   d. (선택 사항) [Certificate chain]에 PEM 인코딩된 인증서 체인을 붙여넣습니다.
   e. [Import]를 선택합니다. 새로 가져온 인증서가 사용 가능 인증서 목록에 나타나고 선택됩니다.
   f. [추가]를 선택합니다.
8. 이 화면에서 나가려면 메뉴 모음에서 [Back to the load balancer] 아이콘(뒤로 버튼)을 선택합니다.

AWS CLI를 사용하여 인증서 목록에 인증서를 추가하려면

add-listener-certificates 명령을 사용합니다.

인증서 목록에서 인증서 제거

다음 절차에 따라 TLS 리스너의 인증서 목록에서 인증서를 제거할 수 있습니다. TLS 리스너의 기본 인증서를 제거하려면 기본 인증서 교체 (p. 24) 단원을 참조하십시오.

콘솔을 사용하여 인증서 목록에서 인증서를 제거하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. 업데이트할 리스너에 대해 View/edit certificates(인증서 보기/편집)를 선택합니다. 그러면 기본 인증서가 표시되고 리스너에 추가한 다른 인증서가 그 다음에 표시됩니다.
5. 메뉴 모음에서 [Remove certificates] 아이콘(마이너스 기호)을 선택합니다.
6. 인증서의 확인란을 선택하고 Remove(제거)를 선택합니다.
7. 이 화면에서 나가려면 메뉴 모음에서 [Back to the load balancer] 아이콘(뒤로 버튼)을 선택합니다.

AWS CLI를 사용하여 인증서 목록에서 인증서를 제거하려면

remove-listener-certificates 명령을 사용합니다.

보안 정책 업데이트

TLS 리스너를 생성할 때 요구를 충족하는 보안 정책을 선택할 수 있습니다. 새로운 보안 정책이 추가되면 새로운 보안 정책을 사용하도록 TLS 리스너를 업데이트할 수 있습니다. Network Load Balancer는 사용자 지정 보안 정책을 지원하지 않습니다. 자세한 내용은 보안 정책 (p. 20) 섹션을 참조하십시오.

콘솔을 사용하여 보안 정책을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.

2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. TLS 리스너의 확인란을 선택하고 Edit(편집)를 선택합니다.
5. Security policy(보안 정책)에서 보안 정책을 선택합니다.
6. [Update]를 선택합니다.

AWS CLI를 사용하여 보안 정책을 업데이트하려면

--ssl-policy 옵션과 함께 modify-listener 명령을 사용합니다.

ALPN 정책 업데이트

다음 절차에 따라 TLS 리스너의 ALPN 정책을 업데이트할 수 있습니다. 자세한 내용은 ALPN 정책 (p. 22) 단원을 참조하십시오.

콘솔을 사용하여 ALPN 정책을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Load Balancers]를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다.
4. TLS 리스너의 확인란을 선택하고 Edit(편집)를 선택합니다.
5. ALPN 정책의 경우 ALPN을 활성화할 정책을 선택하거나 [None]을 선택하여 ALPN을 비활성화합니다.
6. [Update]를 선택합니다.

AWS CLI를 사용하여 ALPN 정책을 업데이트하려면

--alpn-policy 옵션과 함께 modify-listener 명령을 사용합니다.

Network Load Balancer용 리스너 삭제

언제든 리스너를 삭제할 수 있습니다.

콘솔을 이용하여 리스너를 삭제하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택한 다음 [Listeners]를 선택합니다. 리스너의 확인란을 선택하고 Delete(삭제)를 선택합니다.
4. 확인 메시지가 나타나면 Yes, Delete(예, 삭제)를 선택합니다.

AWS CLI를 사용하여 리스너를 삭제하려면

delete-listener 명령을 사용하십시오.

Network Load Balancer 대상 그룹

각 대상 그룹은 하나 이상의 등록된 대상에 요청을 라우팅하는 데 사용됩니다. 리스너를 생성할 때 기본 작업에 대한 대상 그룹을 지정합니다. 트래픽은 리스너 규칙에 지정된 대상 그룹으로 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) 섹션을 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. 자세한 내용은 대상 그룹에 대한 상태 확인 (p. 35) 단원을 참조하십시오.

내용

- 라우팅 구성 (p. 27)
- Target type(대상 유형) (p. 28)
- 등록된 대상 (p. 29)
- 대상 그룹 속성 (p. 30)
- 등록 취소 지연 (p. 30)
- 프록시 프로토콜 (p. 31)
- 고정 세션 (p. 32)
- Network Load Balancer 대상 그룹 생성 (p. 33)
- 대상 그룹에 대한 상태 확인 (p. 35)
- 대상 그룹에 대상 등록 (p. 39)
- 대상 그룹에 대한 태그 (p. 43)
- 대상 그룹 삭제 (p. 44)

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 Balancer 대상 그룹은 다음과 같은 프로토콜 및 포트를 지원합니다.

- 프로토콜: TCP, TLS, UDP, TCP_UDP
- 포트: 1-65535

대상 그룹이 TLS 프로토콜로 구성된 경우 로드 밸런서는 대상에 설치하는 인증서를 사용하여 대상과의 TLS 연결을 설정합니다. 로드 밸런서는 이러한 인증서를 검증하지 않습니다. 따라서 자체 서명된 인증서 또는 만료된 인증서를 사용할 수 있습니다. 로드 밸런서가 VPC(Virtual Private Cloud)에 있으므로 로드 밸런서와 대상 간의 트래픽은 패킷 수준에서 인증됩니다. 따라서 대상의 인증서가 유효하지 않더라도 중간자 공격이나 스푸핑이 발생할 위험이 없습니다.

다음 테이블은 리스너 프로토콜과 대상 그룹 설정의 지원되는 조합을 요약합니다.

리스너 프로토콜	대상 그룹 프로토콜	대상 그룹 유형	상태 확인 프로토콜
TCP	TCP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP

리스너 프로토콜	대상 그룹 프로토콜	대상 그룹 유형	상태 확인 프로토콜
TLS	TCP | TLS	instance | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP
TCP/UDP	TCP/UDP	instance | ip	HTTP | HTTPS | TCP

Target type(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 `ip`인 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)

Important

공개적으로 라우팅 가능한 IP 주소는 지정할 수 없습니다.

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

대상 유형이 `ip`인 경우, 로드 밸런서는 각각의 고유 대상(IP 주소 및 포트)에 대해 55,000건의 동시 연결 또는 분당 약 55,000건의 연결을 지원할 수 있습니다. 연결 건수가 이보다 더 많을 경우, 포트 할당 오류가 발생할 가능성이 증가합니다. 포트 할당 오류가 발생할 경우, 대상 그룹에 더 많은 대상들을 추가하십시오.

Network Load Balancer는 `lambda` 대상 유형을 지원하지 않으며 Application Load Balancer만 `lambda` 대상 유형을 지원합니다. 자세한 내용은 Application Load Balancer 사용 설명서의 대상으로서 Lambda 함수를 참조하십시오.

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 연결 시간이 초과됨 (p. 63) 섹션을 참조하십시오.

라우팅 및 IP 주소 요청

인스턴스 ID를 사용하여 대상을 지정하면 해당 인스턴스의 기본 네트워크 인터페이스에 지정된 기본 프라이빗 IP 주소를 사용하여 트래픽이 인스턴스로 라우팅됩니다. 로드 밸런서는 데이터 패킷의 목적지 IP 주소를 대상 인스턴스로 전송하기 전에 다시 작성합니다.

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. 로드 밸런서는 목적지 IP 주소를 대상 인스턴스로 전송하기 전에 다시 작성합니다.

트래픽을 인스턴스에 허용하는 방법에 대한 자세한 내용은 대상 보안 그룹 (p. 40) 단원을 참조하십시오.

소스 IP 보존

인스턴스 ID로 대상을 지정하는 경우 클라이언트의 소스 IP 주소가 보존되고 애플리케이션에 제공됩니다.

IP 주소로 대상을 지정하는 경우 제공된 소스 IP 주소는 다음과 같이 대상 그룹의 프로토콜에 따라 달라집니다.

- TCP 및 TLS: 소스 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 클라이언트의 IP 주소가 필요한 경우, 로드 밸런서에서 프록시 프로토콜 (p. 31)을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다.
- UDP 및 TCP_UDP: 소스 IP 주소는 클라이언트의 IP 주소입니다.

Network Load Balancer를 VPC 엔드포인트 서비스 또는 AWS Global Accelerator와 함께 사용하는 경우 애플리케이션에 제공되는 소스 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 서비스 소비자의 IP 주소가 필요한 경우 로드 밸런서에서 프록시 프로토콜 (p. 31)을 활성화합니다.

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.

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 미치지는 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 Scaling는 대상을 시작할 때 대상 그룹에 해당 대상을 등록합니다. 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling 그룹에 로드 밸런서 연결을 참조하십시오.

요구 사항

- C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 또는 T1 인스턴스 유형 중 하나를 사용하는 경우 인스턴스 ID로 인스턴스를 등록할 수 없습니다.
- 로드 밸런서 VPC(동일한 리전 또는 다른 리전)로 피어링된 VPC의 인스턴스는 인스턴스 ID로 등록할 수 없습니다. 이러한 인스턴스는 IP 주소로 등록할 수 있습니다.
- IP 주소로 대상을 등록하고 IP 주소가 로드 밸런서와 동일한 VPC에 있는 경우 로드 밸런서는 해당 주소가 연결할 수 있는 서브넷에서 온 것인지 확인합니다.
- UDP 및 TCP_UDP 대상 그룹의 경우 인스턴스가 로드 밸런서 VPC 외부에 있거나 C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, 또는 T1 인스턴스 유형 중 하나를 사용하는 경우에는 IP 주소

로 인스턴스를 등록하지 마십시오. 로드 밸런서 VPC 외부에 있거나 지원되지 않는 인스턴스 유형을 사용하는 대상은 로드 밸런서로부터 트래픽을 수신할 수 있지만 응답할 수는 없습니다.

대상 그룹 속성

다음은 대상 그룹의 속성입니다.

`deregistration_delay.timeout_seconds`

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

`proxy_protocol_v2.enabled`

프록시 프로토콜 버전 2의 활성화 여부를 나타냅니다. 기본적으로 프록시 프로토콜은 비활성화되어 있습니다.

`stickiness.enabled`

고정 세션을 활성화할지 여부를 나타냅니다.

`stickiness.type`

고정의 유형. 가능한 값은 `source_ip`입니다.

등록 취소 지연

인스턴스 등록을 취소하면 로드 밸런서가 인스턴스에 대한 새 연결 생성을 중지합니다. 로드 밸런서는 연결 드레이닝을 사용하여 기존 연결에서 인플라이트 트래픽이 완료되도록합니다. 등록 취소된 인스턴스가 정상 상태를 유지하고 기존 연결이 유휴 상태가 아닌 경우 로드 밸런서는 트래픽을 인스턴스로 계속 전송할 수 있습니다. 기존 연결을 닫으려면 등록 취소하기 전에 인스턴스가 비정상 상태인지 확인하거나 클라이언트 연결을 주기적으로 닫으면 됩니다.

등록 취소하는 대상의 초기 상태는 `draining`입니다. 기본적으로 로드 밸런서는 300초 후에 등록 취소된 대상의 상태를 `unused`로 변경합니다. 등록 취소 대상의 상태를 `unused`로 변경하기 전에 로드 밸런서가 대기하는 시간을 변경하려면 등록 취소 지연 값을 업데이트하십시오. 요청이 완료될 수 있도록 120초 이상의 값을 지정하는 것이 좋습니다.

New console

새 콘솔을 사용하여 등록 취소 지연 값을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 그룹 세부 정보(Group details) 페이지의 속성(Attributes) 섹션에서 편집(Edit)을 선택합니다.
5. 속성 편집(Edit attributes) 페이지에서 필요에 따라 등록 취소 지연(Deregistration delay) 값을 변경합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Old console

기존 콘솔을 사용하여 등록 취소 지연 값을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.

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 Balancer는 프록시 프로토콜 버전 2를 사용하여 소스 및 대상과 같은 추가 연결 정보를 보냅니다. 프록시 프로토콜 버전 2는 프록시 프로토콜 헤더의 이진 인코딩을 제공합니다. 로드 밸런서는 TCP 데이터에 프록시 프로토콜 헤더를 추가합니다. 로드 밸런서는 클라이언트에서 전송한 모든 프록시 프로토콜 헤더 또는 네트워크 경로에 있는 그 밖의 모든 프록시, 로드 밸런서 또는 서버를 포함해 기존 데이터를 폐기하거나 덮어쓰지 않습니다. 따라서 하나 이상의 프록시 프로토콜 헤더를 수신할 수 있습니다. 또한 Network Load Balancer 외부의 대상에 대한 다른 네트워크 경로가 있을 경우, 첫 번째 프록시 프로토콜 헤더는 Network Load Balancer의 헤더가 아닐 수도 있습니다.

IP 주소로 대상을 지정하는 경우 애플리케이션에 제공되는 소스 IP 주소는 다음과 같이 대상 그룹의 프로토콜에 따라 달라집니다.

- TCP 및 TLS: 소스 IP 주소는 로드 밸런서 노드의 프라이빗 IP 주소입니다. 클라이언트의 IP 주소가 필요한 경우, 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다.
- UDP 및 TCP_UDP: 소스 IP 주소는 클라이언트의 IP 주소입니다.

인스턴스 ID로 대상을 지정하는 경우 애플리케이션에 제공되는 원본 IP 주소는 클라이언트 IP 주소입니다. 하지만 원하는 경우 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져올 수 있습니다.

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. 애플리케이션에 서비스 소비자의 IP 주소가 필요한 경우, 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 서비스 소비자 IP 주소를 가져옵니다.

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

필드	길이(자리)	설명
형식	1	PP2_TYPE_AWS(0xEA)
길이	2	값의 길이
값	1	PP2_SUBTYPE_AWS_VPCE_ID(0x01)

필드	길이(자리)	설명
	변수(값 길이 -1)	엔드포인트의 ID

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

프록시 프로토콜 활성화

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

New console

새 콘솔을 사용하여 프록시 프로토콜 v2를 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 그룹 세부 정보(Group details) 페이지의 속성(Attributes) 섹션에서 편집(Edit)을 선택합니다.
5. 속성 편집(Edit attributes) 페이지에서 프록시 프로토콜 v2(Proxy protocol v2)를 선택합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Old console

기존 콘솔을 사용하여 프록시 프로토콜 v2를 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. 프록시 프로토콜 v2의 경우 활성화를 선택합니다.
6. 저장을 선택합니다.

AWS CLI를 사용하여 프록시 프로토콜 v2를 활성화하려면

modify-target-group-attributes 명령을 사용합니다.

고정 세션

고정 세션은 대상 그룹의 동일한 대상으로 클라이언트 트래픽을 라우팅하는 메커니즘입니다. 이는 클라이언트에게 지속적인 경험을 제공하기 위해 상태 정보를 유지하는 서버에 유용합니다.

고려 사항

- 고정 세션을 사용하면 연결 및 흐름이 고르지 않게 분포되어 대상의 가용성에 영향을 줄 수 있습니다. 예를 들어 동일한 NAT 디바이스 뒤에 있는 모든 클라이언트는 동일한 소스 IP 주소를 가집니다. 따라서 이러한 클라이언트의 모든 트래픽은 동일한 대상으로 라우팅됩니다.

- 로드 밸런서는 대상의 상태가 변경되거나 대상 그룹에 대상을 등록 또는 등록 취소하는 경우 대상 그룹에 대한 고정 세션을 재설정할 수 있습니다.
- 고정 세션은 TLS 리스너 및 TLS 대상 그룹에서는 지원되지 않습니다.

New console

새 콘솔을 사용하여 고정 세션을 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 그룹 세부 정보(Group details) 페이지의 속성(Attributes) 섹션에서 편집(Edit)을 선택합니다.
5. 속성 편집(Edit attributes) 페이지에서 고정성(Stickiness)을 선택합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Old console

기존 콘솔을 사용하여 고정 세션을 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택합니다.
4. [Description], [Edit attributes]를 선택합니다.
5. 고정성(Stickiness)에서 사용(Enable)을 선택합니다.
6. 저장을 선택합니다.

AWS CLI를 사용하여 고정 세션을 활성화하려면

`stickiness.enabled` 속성과 함께 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 리스너를 생성하고 해당 리스너의 기본 작업에 대상 그룹을 지정합니다. 자세한 내용은 리스너 규칙 (p. 17) 단원을 참조하십시오.

언제든지 대상 그룹에서 대상을 추가하거나 삭제할 수 있습니다. 자세한 내용은 대상 그룹에 대상 등록 (p. 39) 섹션을 참조하십시오. 대상 그룹에 대한 상태 확인 설정을 변경할 수도 있습니다. 자세한 내용은 대상 그룹의 상태 확인 설정 수정 (p. 39) 섹션을 참조하십시오.

New console

새 콘솔을 사용하여 대상 그룹을 생성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.

3. [Create target group]을 선택합니다.
4. 대상 유형 선택(Choose a target type)에서 인스턴스(Instances)를 선택하여 인스턴스 ID로 대상을 등록하거나 IP 주소(IP addresses)를 선택하여 IP 주소로 대상을 등록합니다.
5. [Target group name]에 대상 그룹의 이름을 입력합니다. 이 이름은 계정당 리전당 고유해야 하고, 최대 32자여야 하며, 알파벳 문자 또는 하이픈만 포함해야 하고, 하이픈으로 시작하거나 끝나지 않아야 합니다.
6. 프로토콜에 대해 다음과 같이 프로토콜을 선택합니다.
   - 리스너 프로토콜이 TCP인 경우, TCP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TLS인 경우, TCP 또는 TLS를 선택합니다.
   - 리스너 프로토콜이 UDO인 경우, UDP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TCP_UDP인 경우, TCP_UDP를 선택합니다.
7. (선택 사항) 포트에서 필요에 따라 기본값을 변경합니다.
8. [VPC]에서 Virtual Private Cloud(VPC)를 선택합니다.
9. (선택 사항) 상태 확인(Health checks) 섹션에서 필요에 따라 기본 설정을 수정합니다.
10. (선택 사항) 다음과 같이 하나 이상의 태그를 추가합니다.
    a. 태그 섹션을 확장합니다.
    b. [Add tag]를 선택합니다.
    c. 태그 키와 태그 값을 입력합니다.
11. [Next]를 선택합니다.
12. (선택 사항) 다음과 같이 하나 이상의 대상을 추가합니다.
    - 대상 유형이 인스턴스(Instances)인 경우 하나 이상의 인스턴스를 선택하고 하나 이상의 포트를 입력한 다음 아래에 보류 중인 것으로 포함(Include as pending below)을 선택합니다.
    - 대상 유형이 IP 주소(IP addresses)인 경우 네트워크를 선택하고 IP 주소와 포트를 입력한 다음 아래에 보류 중인 것으로 포함(Include as pending below)을 선택합니다.
13. [Create target group]을 선택합니다.
14. (선택 사항) 기본 리스너 규칙에서 대상 그룹을 지정할 수 있습니다. 자세한 내용은 리스너 생성 (p. 17) 및 리스너 업데이트 (p. 23)를 참조하십시오.

Old console

기존 콘솔을 사용하여 대상 그룹을 생성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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. 이 이름은 계정당 리전당 고유해야 하고, 최대 32자여야 하며, 알파벳 문자 또는 하이픈만 포함해야 하고, 하이픈으로 시작하거나 끝나지 않아야 합니다.
5. 프로토콜에 대해 다음과 같이 프로토콜을 선택합니다.
   - 리스너 프로토콜이 TCP인 경우, TCP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TLS인 경우, TCP 또는 TLS를 선택합니다.
   - 리스너 프로토콜이 UDO인 경우, UDP 또는 TCP_UDP를 선택합니다.
   - 리스너 프로토콜이 TCP_UDP인 경우, TCP_UDP를 선택합니다.
6. (선택 사항) 포트에서 필요에 따라 기본값을 변경합니다.
7. [Target type]에서 인스턴스 ID 또는 `ip`로 대상을 지정할 `instance`를 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. 39) 섹션을 참조하십시오.
12. (선택 사항) 기본 리스너 규칙에서 대상 그룹을 지정할 수 있습니다. 자세한 내용은 리스너 생성 (p. 17) 및 리스너 업데이트 (p. 23)를 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

하나 이상의 대상 그룹에 대상을 등록합니다. 등록 과정이 완료되는 즉시, 로드 밸런서는 새로 등록된 대상으로 요청을 라우팅하기 시작합니다. 등록 프로세스가 완료되고 상태 확인이 시작되는 데 몇 분 정도 걸릴 수 있습니다.

Network Load Balancer는 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. 교차 영역 로드 밸런싱을 활성화하면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 정상 대상으로 요청을 라우팅합니다. 자세한 내용은 교차 영역 로드 밸런싱 (p. 11) 섹션을 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 비정상으로 보고되기 전에 비정상 대상을 감지할 수 있습니다. 사용자가 수동 상태 확인을 비활성화, 구성 또는 모니터링할 수는 없습니다. 수동적인 상태 검사는 UDP 트래픽에 대해 지원되지 않습니다.

대상이 비정상 상태이면 로드 밸런서가 대상과 관련된 클라이언트 연결에서 수신된 패킷에 대해 TCP RST를 보냅니다.

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.

HTTP 또는 HTTPS 상태 확인 요청의 경우 호스트 헤더에는 대상의 IP 주소 및 상태 확인 포트 대신 로드 밸런서 노드의 IP 주소 및 리스너 포트가 포함됩니다.

Network Load Balancer에 TLS 리스너를 추가하면 리스너 연결 테스트가 진행됩니다. TLS 종료 시 TCP 연결도 종료되므로 로드 밸런서와 대상 간에 새로운 TCP 연결이 설정됩니다. 따라서 이 테스트의 TCP ping이 로드 밸런서에서 TLS 리스너에 등록된 대상으로 전송된 것을 볼 수 있습니다. 이들 TCP ping은 Network Load Balancer의 소스 IP 주소가 있으며 연결에는 데이터 패킷이 포함되어 있지 않기 때문에 식별할 수 있습니다.

UDP 서비스의 경우 가용성은 TCP 활성 상태 검사를 사용하여 대상의 TCP 포트로 이동하여 테스트됩니다. 대상에서 TCP 포트를 사용하여 UDP 서비스의 가용성을 확인할 수 있습니다. 상태 확인 포트를 수신하는 서

비스가 실패하면 대상을 사용할 수 없는 것으로 간주됩니다. UDP 서비스의 상태 확인 정확도를 높이려면 상태 확인 포트를 수신하는 서비스가 UDP 서비스의 상태를 추적하도록 구성하고 서비스를 사용할 수 없는 경우 상태 확인 포트를 닫습니다.

상태 확인 설정

다음 설정을 사용하여 대상 그룹에서 대상에 대한 능동 상태 확인을 구성합니다. 상태 확인이 UnhealthyThresholdCount 연속 실패를 초과하면 로드 밸런서는 대상을 서비스에서 제외합니다. 상태 확인이 HealthyThresholdCount 연속 성공을 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. 이 값은 HTTP 상태 확인의 경우 6초이고 TCP 및 HTTPS 상태 확인의 경우 10초입니다.
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 수신합니다. HTTP 상태 확인을 사용하는 경우, 대상에 미치는 영향을 줄이려면 정적 HTML 파일과 같은 대상에서 보다 간단한 대상을 사용하거나 TCP 상태 확인으로 전환하십시오.
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. 관련 사유 코드: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	대상이 정상 상태입니다. 관련 사유 코드: 없음
`unhealthy`	대상이 상태 확인에 응답하지 않았거나 상태 확인에 실패했습니다. 관련 사유 코드: `Target.FailedHealthChecks`
`unused`	대상이 대상 그룹에 등록되어 있지 않거나, 대상 그룹이 리스너 규칙에서 사용되지 않거나, 대상이 활성화되지 않은 가용 영역에 있거나, 대상이 중지 상태 또는 종료 상태입니다. 관련 사유 코드: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`
`draining`	대상이 등록 취소되고 있으며 연결 드레이닝이 진행 중입니다. 관련 사유 코드: `Target.DeregistrationInProgress`
`unavailable`	대상 상태를 확인할 수 없습니다. 관련 사유 코드: `Elb.InternalError`

상태 확인 사유 코드

대상의 상태가 `Healthy` 이외의 값인 경우에는 API가 문제에 대한 사유 코드와 설명을 반환하고 콘솔이 도구 설명에 동일한 설명을 표시합니다. `Elb`로 시작되는 사유 코드는 로드 밸런서 측에서 호출되고, `Target`로 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
`Target.InvalidState`	대상이 중지 상태에 있음 대상이 종료 상태에 있음 대상이 종료 또는 중지 상태에 있음 대상이 잘못된 상태에 있음
`Target.IpUnusable`	로드 밸런서에서 사용 중인 IP 주소이므로 대상으로 사용할 수 없음
`Target.NotInUse`	대상 그룹이 로드 밸런서에서 트래픽을 수신하도록 구성되지 않음 대상이 로드 밸런서에서 활성화되지 않은 가용 영역에 있음
`Target.NotRegistered`	대상이 대상 그룹에 등록되지 않음

대상의 상태 확인

대상 그룹에 등록된 대상의 상태를 확인할 수 있습니다.

New console

새 콘솔을 사용하여 대상의 상태를 확인하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 대상 탭에서 상태 열은 각 대상의 상태를 나타냅니다.
5. 대상 상태가 `Healthy` 이외의 값인 경우 상태 세부 정보(Status details) 열에 자세한 정보가 포함됩니다.

Old console

기존 콘솔을 사용하여 대상의 상태를 확인하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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 출력 화면에는 대상 상태 설명이 포함됩니다. 상태가 `Healthy` 이외의 값인 경우에는 화면에 사유 코드도 포함됩니다.

비정상 대상에 대한 이메일 알림을 받으려면

CloudWatch 경보를 사용하여 비정상 대상에 대한 세부 정보를 전송하는 Lambda 함수를 트리거합니다. 단계별 지침은 블로그 게시물 로드 밸런서의 비정상 대상 식별을 참조하십시오.

대상 그룹의 상태 확인 설정 수정

대상 그룹에 대한 일부 상태 확인 설정을 변경할 수 있습니다. 대상 그룹의 프로토콜이 TCP, TLS, UDP 또는 TCP_UDP일 경우 상태 확인 프로토콜, 간격, 제한 시간 또는 성공 코드를 수정할 수 없습니다.

New console

새 콘솔을 사용하여 대상 그룹의 상태 확인 설정을 변경하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 그룹 세부 정보(Group details) 탭의 상태 확인 설정(Health check settings) 섹션에서 편집(Edit)을 선택합니다.
5. 상태 확인 설정 편집(Edit health check settings) 페이지에서 필요에 따라 설정을 수정한 다음 변경 사항 저장(Save changes)을 선택합니다.

Old console

기존 콘솔을 사용하여 대상 그룹의 상태 확인 설정을 변경하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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

대상이 요청을 처리할 준비가 되면 하나 이상의 대상 그룹에 대상을 등록합니다. 인스턴스 ID 또는 IP 주소로 대상을 등록할 수 있습니다. 로드 밸런서는 등록 프로세스가 완료되고 대상이 초기 상태 확인을 통과하자마자 해당 대상에 대한 라우팅 요청을 시작합니다. 등록 프로세스가 완료되고 상태 확인이 시작되는 데 몇 분 정도 걸릴 수 있습니다. 자세한 내용은 대상 그룹에 대한 상태 확인 (p. 35) 단원을 참조하십시오.

최근 등록된 대상에 대한 요구가 증가하면 이를 처리하기 위해 하나 이상의 대상 그룹에 추가 대상을 등록할 수 있습니다. 등록된 대상에 대한 요구가 감소하는 경우에는 대상 그룹에서 대상의 등록을 취소할 수 있습니다. 등록 취소 프로세스가 완료되고 로드 밸런서가 대상에 대한 요청 라우팅을 중지하는 데 몇 분 정도 걸릴 수 있습니다. 이후에 요구가 증가하면 등록을 취소한 대상을 대상 그룹에 다시 등록할 수 있습니다. 대상을 서비스해야 하는 경우 등록을 취소한 다음 서비스가 완료되면 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. 등록 취소가 완료된 후 대상의 상태는 `unused`로 변경됩니다. 자세한 내용은 등록 취소 지연 (p. 30) 단원을 참조하십시오.

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 사용 설명서의 Auto Scaling 그룹에 로드 밸런서 연결을 참조하십시오.

대상 보안 그룹

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

제한 사항

- Network Load Balancer는 연결된 보안 그룹을 갖지 않습니다. 따라서 대상의 보안 그룹은 IP 주소를 사용하여 로드 밸런서로부터의 트래픽을 허용해야 합니다.
- 클라이언트의 보안 그룹을 대상에 대한 보안 그룹의 소스로 사용할 수 없습니다. 대신 클라이언트 CIDR 블록을 대상 보안 그룹의 소스로 사용하십시오.

인스턴스 보안 그룹에 권장되는 규칙

Inbound			
소스	프로토콜	포트 범위	Comment(설명)
##### IP ##	***##***	***##***	클라이언트 트래픽 허용(`instance` 대상 유형)
VPC CIDR	***##***	***##***	클라이언트 트래픽 허용(`ip` 대상 유형)
VPC CIDR	***## ##***	***## ##***	로드 밸런서의 상태 확인 트래픽 허용

IP 주소로 대상을 등록하고 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.

허용할 프라이빗 IP 주소를 찾으려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Network Interfaces]를 선택합니다.
3. 검색 필드에 Network Load Balancer 이름을 입력합니다. 로드 밸런서 서브넷당 한 개의 네트워크 인터페이스가 있습니다.
4. 각 네트워크 인터페이스의 세부 정보 탭에서 기본 프라이빗 IPv4 IP의 주소를 복사합니다.

네트워크 ACL

EC2 인스턴스를 대상으로 등록할 때 인스턴스에 대한 서브넷의 네트워크 ACL은 리스너 포트와 상태 확인 포트 모두에서 트래픽을 허용해야 합니다. VPC의 기본 네트워크 ACL(액세스 제어 목록)은 인바운드 트래픽과 아웃바운드 트래픽을 모두 허용합니다. 사용자 지정 네트워크 ACL을 생성하는 경우 해당 ACL이 적절한 트래픽을 허용하는지 확인합니다.

인스턴스의 서브넷과 연결된 네트워크 ACL은 인터넷 경계 로드 밸런서에 대해 다음 트래픽을 허용해야 합니다.

인스턴스 서브넷에 권장되는 규칙

Inbound			
소스	프로토콜	포트 범위	Comment(설명)

##### IP ##	###	###	클라이언트 트래픽 허용(instance 대상 유형)
VPC CIDR	###	###	클라이언트 트래픽 허용(ip 대상 유형)
VPC CIDR	## ##	## ##	로드 밸런서의 상태 확인 트래픽 허용
Outbound			
대상 주소	프로토콜	포트 범위	Comment(설명)
##### IP ##	###	###	클라이언트에 대한 응답 허용(instance 대상 유형)
VPC CIDR	###	###	클라이언트에 대한 응답 허용(ip 대상 유형)
VPC CIDR	## ##	1024~65535	상태 확인 트래픽 허용

로드 밸런서의 서브넷과 연결된 네트워크 ACL은 인터넷 경계 로드 밸런서에 대해 다음 트래픽을 허용해야 합니다.

로드 밸런서 서브넷에 권장되는 규칙

Inbound			
소스	프로토콜	포트 범위	Comment(설명)
##### IP ##	###	###	클라이언트 트래픽 허용(instance 대상 유형)
VPC CIDR	###	###	클라이언트 트래픽 허용(ip 대상 유형)
VPC CIDR	## ##	1024~65535	상태 확인 트래픽 허용
Outbound			
대상 주소	프로토콜	포트 범위	Comment(설명)
##### IP ##	###	###	클라이언트에 대한 응답 허용(instance 대상 유형)
VPC CIDR	###	###	클라이언트에 대한 응답 허용(ip 대상 유형)
VPC CIDR	## ##	## ##	상태 확인 트래픽 허용
VPC CIDR	## ##	1024~65535	상태 확인 트래픽 허용

내부 로드 밸런서의 경우 인스턴스 및 로드 밸런서 노드의 서브넷에 대한 네트워크 ACL은 리스너 포트 및 휘발성 포트에서 VPC CIDR을 주고받는 인바운드 및 아웃바운드 트래픽을 모두 허용해야 합니다.

대상 등록 또는 등록 취소

각 대상 그룹에는 로드 밸런서에 사용되는 각 가용 영역에 하나 이상의 등록된 대상이 있어야 합니다.

대상 그룹의 대상 유형에 따라 해당 대상 그룹에 대상을 등록하는 방법이 결정됩니다. 자세한 내용은 Target type(대상 유형) (p. 28) 단원을 참조하십시오.

요구 사항

- C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 또는 T1 인스턴스 유형 중 하나를 사용하는 경우 인스턴스 ID로 인스턴스를 등록할 수 없습니다.
- 로드 밸런서 VPC(동일한 리전 또는 다른 리전)로 피어링된 VPC의 인스턴스는 인스턴스 ID로 등록할 수 없습니다. 이러한 인스턴스는 IP 주소로 등록할 수 있습니다.
- IP 주소로 대상을 등록하고 IP 주소가 로드 밸런서와 동일한 VPC에 있는 경우 로드 밸런서는 해당 주소가 연결할 수 있는 서브넷에서 온 것인지 확인합니다.
- UDP 및 TCP_UDP 대상 그룹의 경우 인스턴스가 로드 밸런서 VPC 외부에 있거나 C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, 또는 T1 인스턴스 유형 중 하나를 사용하는 경우에는 IP 주소로 인스턴스를 등록하지 마십시오. 로드 밸런서 VPC 외부에 있거나 지원되지 않는 인스턴스 유형을 사용하는 대상은 로드 밸런서로부터 트래픽을 수신할 수 있지만 응답할 수는 없습니다.

목차

- 인스턴스 ID로 대상 등록 또는 등록 취소 (p. 42)
- IP 주소로 대상 등록 또는 등록 취소 (p. 43)
- AWS CLI를 사용하여 대상 등록 또는 등록 취소 (p. 43)

인스턴스 ID로 대상 등록 또는 등록 취소

인스턴스를 등록할 때 인스턴스가 `running` 상태여야 합니다.

New console

새 콘솔을 사용하여 인스턴스 ID별로 대상을 등록 또는 등록 취소하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 대상 탭을 선택합니다.
5. 인스턴스를 등록하려면 대상 등록(Register targets)을 선택합니다. 하나 이상의 인스턴스를 선택하고 필요에 따라 기본 인스턴스 포트를 입력한 다음 아래에 보류 중인 것으로 포함(Include as pending below)을 선택합니다. 인스턴스 추가를 마쳤으면 보류 중인 대상 등록(Register pending targets)을 선택합니다.
6. 인스턴스의 등록을 취소하려면 인스턴스를 선택한 다음 등록 취소(Deregister)를 선택합니다.

Old console

기존 콘솔을 사용하여 인스턴스 ID로 대상을 등록 또는 등록 취소하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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. 저장을 선택합니다.

IP 주소로 대상 등록 또는 등록 취소

사용자가 등록하는 IP 주소는 다음 CIDR 블록 중 하나를 출처로 한 주소여야 합니다.

- 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)

New console

새 콘솔을 사용하여 IP 주소로 대상을 등록 또는 등록 취소하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 대상 탭을 선택합니다.
5. IP 주소를 등록하려면 대상 등록(Register targets)을 선택합니다. 각 IP 주소에 대해 네트워크, 가용 영역, IP 주소, 포트를 선택한 다음 아래에 보류 중인 것으로 포함(Include as pending below)을 선택합니다. 주소 지정을 마치면 보류 중인 대상 등록(Register pending targets)을 선택합니다.
6. IP 주소의 등록을 취소하려면 IP 주소를 선택한 다음 등록 취소(Deregister)를 선택합니다. 등록 취소된 IP 주소가 많은 경우 필터를 추가하거나 정렬 순서를 변경하는 것이 유용할 수 있습니다.

Old console

기존 콘솔을 사용하여 IP 주소로 대상을 등록 또는 등록 취소하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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 대상 등록 또는 등록 취소

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.

New console

새 콘솔을 사용하여 대상 그룹 태그를 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 태그(Tags) 탭에서 태그 관리(Manage tags)를 선택하고 다음 중 하나 이상의 작업을 수행합니다.
   a. 태그를 업데이트하려면 키(Key) 및 값(Value)에 새 값을 입력합니다.
   b. 태그를 추가하려면 태그 추가(Add tag)를 선택하고 키(Key) 및 값(Value)에 값을 입력합니다.
   c. 태그를 삭제하려면 태그 옆의 제거(Remove)를 선택합니다.
5. 태그 업데이트를 마쳤으면 변경 사항 저장(Save changes)을 선택합니다.

Old console

콘솔을 사용하여 대상 그룹 태그를 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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

리스너 규칙의 전달 작업에서 참조하지 않는 대상 그룹을 삭제할 수 있습니다. 대상 그룹을 삭제해도 대상 그룹에 등록된 대상에는 영향을 미치지 않습니다. 등록된 EC2 인스턴스가 더 이상 필요하지 않은 경우 중지 또는 종료할 수 있습니다.

New console

새 콘솔을 사용하여 대상 그룹을 삭제하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [LOAD BALANCING] 아래에서 [Target Groups]를 선택합니다.
3. 대상 그룹을 선택하고 [Actions], [Delete]를 차례로 선택합니다.
4. 확인 메시지가 나타나면 예, 삭제합니다(Yes, delete)를 선택합니다.

Old console

기존 콘솔을 사용하여 대상 그룹을 삭제하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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 Balancer 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 지표 (p. 46) 섹션을 참조하십시오.

VPC 흐름 로그

VPC 플로우 로그를 사용하여 Network Load Balancer로 들어오고 나가는 트래픽에 대한 세부 정보를 캡처할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 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. 프런트엔드 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 프런트엔드 연결과 백엔드 연결에 대해 'ACCEPT OK(승인 확인)'를 표시하고 인스턴스의 네트워크 인터페이스 로그는 그 연결에 대해 'REJECT OK(거절 확인)'를 표시합니다.

액세스 로그

액세스 로그를 사용하면 로드 밸런서에 대한 TLS 요청에 관하여 자세한 정보를 캡처할 수 있습니다. 로그 파일은 Amazon S3에 저장된 상태입니다. 또한 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 대상의 문제를 해결할 수 있습니다. 자세한 내용은 Network Load Balancer에 대한 액세스 로그 (p. 54) 섹션을 참조하십시오.

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 CloudTrail를 사용하여 Network Load Balancer에 대한 API 호출 로깅 (p. 59) 섹션을 참조하십시오.

Network Load Balancer의 CloudWatch 지표

Elastic Load Balancing는 해당 로드 밸런서 및 대상에 대한 데이터 포인트를 Amazon CloudWatch에 게시합니다. CloudWatch를 사용하면 그러한 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 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)를 시작할 수 있습니다.

Elastic Load Balancing는 요청이 로드 밸런서를 통과하는 경우에만 CloudWatch에 지표를 보고합니다. 로드 밸런서를 통과하는 요청이 있는 경우, Elastic Load Balancing는 60초마다 지표를 측정하여 전송합니다. 로드

밸런서를 통과하고 있는 요청이 없는 경우나 지표에 대한 데이터가 없는 경우에는 지표가 보고되지 않습니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

목차

- 네트워크 로드 밸런서 지표 (p. 47)
- Network Load Balancer에 대한 지표 차원 (p. 52)
- Network Load Balancer 지표에 대한 통계 (p. 53)
- 로드 밸런서에 대한 CloudWatch 지표 보기 (p. 53)

네트워크 로드 밸런서 지표

`AWS/NetworkELB` 네임스페이스에는 다음 지표가 포함되어 있습니다.

지표	설명
`ActiveFlowCount`	클라이언트에서 대상까지의 동시 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. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Average`, `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ActiveFlowCount_TCP`	클라이언트에서 대상까지의 동시 TCP 흐름(또는 연결)의 총 수입니다. 이 지표에는 ESTABLISHED 상태의 연결만 포함됩니다. TCP 연결은 로드 밸런서에서 종료되지 않으므로 대상에 대한 TCP 연결을 여는 클라이언트는 단일 흐름으로 계산됩니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Average`, `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ActiveFlowCount_TLS`	클라이언트에서 대상까지의 동시 TLS 흐름(또는 연결)의 총 수입니다. 이 지표에는 ESTABLISHED 상태의 연결만 포함됩니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Average`, `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`

지표	설명
`ActiveFlowCount_UDP`	클라이언트에서 대상까지의 동시 UDP 흐름(또는 연결)의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Average`, `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ClientTLSNegotiationErrorCount`	클라이언트와 TLS 리스너 간의 협상 중에 실패한 전체 TLS 핸드셰이크의 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Sum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ConsumedLCUs`	로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수. 시간 단위로 사용한 LCU 수만큼 요금을 지불하면 됩니다. 자세한 내용은 Elastic Load Balancing 요금을 참조하십시오. 보고 기준: 항상 보고 통계: 모두 Dimensions • `LoadBalancer`
`ConsumedLCUs_TCP`	TCP의 로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수. 시간 단위로 사용한 LCU 수만큼 요금을 지불하면 됩니다. 자세한 내용은 Elastic Load Balancing 요금을 참조하십시오. 보고 기준: 항상 보고 통계: 모두 Dimensions • `LoadBalancer`

지표	설명
`ConsumedLCUs_TLS`	TLS의 로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수. 시간 단위로 사용한 LCU 수만큼 요금을 지불하면 됩니다. 자세한 내용은 Elastic Load Balancing 요금을 참조하십시오. 보고 기준: 항상 보고 통계: 모두 Dimensions • `LoadBalancer`
`ConsumedLCUs_UDP`	UDP의 로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수. 시간 단위로 사용한 LCU 수만큼 요금을 지불하면 됩니다. 자세한 내용은 Elastic Load Balancing 요금을 참조하십시오. 보고 기준: 항상 보고 통계: 모두 Dimensions • `LoadBalancer`
`HealthyHostCount`	정상 상태로 간주되는 대상 수 Reporting criteria(보고 기준): 상태 확인을 활성화한 경우 보고됨 통계: 가장 유용한 통계는 `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer`, `TargetGroup` • `AvailabilityZone`, `LoadBalancer`, `TargetGroup`
`NewFlowCount`	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 흐름(또는 연결)의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Sum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`

지표	설명
NewFlowCount_TCP	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 TCP 흐름(또는 연결)의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
NewFlowCount_TLS	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 TLS 흐름(또는 연결)의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
NewFlowCount_UDP	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 UDP 흐름(또는 연결)의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes	TCP/IP 헤더를 포함하여 로드 밸런서가 처리하는 총 바이트 수. 이 수는 대상부터의 트래픽, 대상까지의 트래픽, 마이너스 상태 확인 트래픽을 포함합니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer

지표	설명
ProcessedBytes_TCP	TCP 리스너에서 처리한 총 바이트 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes_TLS	TLS 리스너에서 처리한 총 바이트 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
ProcessedBytes_UDP	UDP 리스너에서 처리한 총 바이트 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
TargetTLSNegotiationErrorCount	TLS 리스너와 대상 간의 협상 중에 실패한 전체 TLS 핸드셰이크의 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer
TCP_Client_Reset_Count	클라이언트에서 대상까지 전송된 재설정(RST) 패킷의 총 수입니다. 이러한 재설정은 클라이언트에 의해 생성되고 로드 밸런서에 의해 전달됩니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. Dimensions • LoadBalancer • AvailabilityZone, LoadBalancer

지표	설명
`TCP_ELB_Reset_Count`	로드 밸런서에 의해 생성되는 재설정(RST) 패킷의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Sum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`TCP_Target_Reset_Count`	대상에서 클라이언트로 전송된 재설정(RST) 패킷의 총 수입니다. 이러한 재설정은 대상에 의해 생성되고 로드 밸런서에 의해 전달됩니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 `Sum`입니다. Dimensions • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`UnHealthyHostCount`	비정상 상태로 간주되는 대상 수 Reporting criteria(보고 기준): 상태 확인을 활성화한 경우 보고됨 통계: 가장 유용한 통계는 `Maximum` 및 `Minimum`입니다. Dimensions • `LoadBalancer`, `TargetGroup` • `AvailabilityZone`, `LoadBalancer`, `TargetGroup`

Network Load Balancer에 대한 지표 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 Balancing가 게시한 지표 데이터 포인트에 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 각 샘플링 창에서 개별 로드 밸런서 노드가 보고한 최소 및 최대 데이터 포인트 값을 반영합니다. `HealthyHostCount` 최댓값을 늘리면 `UnHealthyHostCount` 최솟값이 감소합니다. 따라서 `HealthyHostCount` 최댓값 또는 `UnHealthyHostCount` 최솟값을 사용하여 Network Load Balancer를 모니터링하는 것이 좋습니다.

`Sum` 통계는 모든 로드 밸런서 노드의 집계 값입니다. 지표에는 기간별 보고서가 여러 개 있기 때문에 `Sum`은 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 `HealthyHostCount`에 대해 `SampleCount`는 각 로드 밸런서 노드가 보고하는 샘플 수를 기반으로 하며 정상 호스트 수는 아닙니다.

로드 밸런서에 대한 CloudWatch 지표 보기

Amazon EC2 콘솔을 사용해 로드 밸런서에 대한 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. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 [Metrics]를 선택합니다.
3. [NetworkELB] 네임스페이스를 선택합니다.
4. (선택 사항) 모든 차원의 지표를 보려면 검색 필드에 이름을 입력합니다.

AWS CLI을(를) 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 게시가 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"
}
```

Network Load Balancer에 대한 액세스 로그

Elastic Load Balancing는 Network Load Balancer에 전송된 TLS 요청에 관한 자세한 정보를 캡처하는 액세스 로그를 제공합니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

> Important
>
> 로드 밸런서에 TLS 리스너가 있고 액세스 로그가 TLS 요청에 관한 정보만 포함하는 경우에만 액세스 로그가 생성됩니다.

액세스 로그는 Elastic Load Balancing의 옵션 기능으로, 기본적으로 비활성화됩니다. 로드 밸런서에 대해 액세스 로그를 활성화하면 Elastic Load Balancing가 로그를 압축 파일로 캡처하여 이를 지정된 Amazon S3 버킷에 저장합니다. 액세스 로그는 언제든지 비활성화할 수 있습니다.

S3 버킷에 대한 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 서버 측 암호화를 활성화하는 경우, 각 액세스 로그 파일은 S3 버킷에 저장되기 전에 자동으로 암호화되고 액세스 시 암호화가 해제됩니다. 암호화된 로그 파일이나 암호화되지 않은 로그 파일을 액세스하는 방식과 다르지 않으므로 별도의 조치가 필요 없습니다. 각 로그 파일은 고유 키로 암호화되며, 주기적으로 바뀌는 마스터 키를 사용하여 키 자체가 암호화됩니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화를 사용하여 데이터 보호를 참조하십시오.

액세스 로그에 대한 추가 요금은 없습니다;. Amazon S3에 대한 스토리지 비용은 청구되지만 Elastic Load Balancing가 Amazon S3에 로그 파일을 전송하기 위해 사용하는 대역폭에 대해서는 비용이 청구되지 않습니다. 스토리지 비용에 대한 자세한 내용은 Amazon S3 요금을 참조하십시오.

액세스 로그 파일

Elastic Load Balancing는 5분마다 각 로드 밸런서 노드에 대한 로그 파일을 게시합니다. 로그 전달은 결과의 일관성이 있습니다. 로드 밸런서는 같은 기간 동안 여러 개의 로그를 전달할 수 있습니다. 이러한 상황은 보통 사이트에 트래픽이 많은 경우에 발생합니다.

액세스 로그의 파일 이름은 다음 형식을 사용합니다.

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-balancer-id_end-time_random-string.log.gz
```

버킷

S3 버킷의 이름

prefix

버킷의 접두사(논리적 계층 구조)입니다. 접두사를 지정하지 않는 경우 로그는 버킷의 루트 수준에 저장됩니다.

aws-account-id

소유자의 AWS 계정 ID입니다.

region

로드 밸런서 및 S3 버킷을 위한 리전입니다.

yyyy/mm/dd

로그가 전달된 날짜입니다.

load-balancer-id

로드 밸런서의 리소스 ID입니다. 리소스 ID에 포함되어 있는 슬래시(/)가 마침표(.)로 대체됩니다.

end-time

로깅 간격이 끝나는 날짜와 시간입니다. 예를 들어, 종료 시간이 20181220T2340Z이면 23시 35분과 23시 40분 사이에 발생한 요청에 대한 항목들이 포함됩니다.

random-string

시스템에서 생성된 임의 문자열입니다.

원하는 기간만큼 버킷에 로그 파일을 저장할 수 있습니다. 그러나 Amazon S3 수명 주기 규칙을 정의하여 자동으로 로그 파일을 보관하거나 삭제할 수도 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 수명 주기 관리를 참조하십시오.

액세스 로그 항목

다음 표에서는 액세스 로그 항목의 필드를 순서대로 설명합니다. 모든 필드는 공백으로 구분됩니다. 새 필드가 도입되면 로그 항목 끝에 추가됩니다. 로그 파일을 처리할 때 예상하지 못했던 방식으로 로그 항목이 끝나면 모든 필드를 무시해야 합니다.

필드	설명
type	리스너 유형. 지원되는 값은 `tls`입니다.
version	로그 항목의 버전입니다. 현재 버전은 2.0입니다.
시간	TLS 연결이 끝나면 ISO 8601 형식으로 기록되는 시간입니다.

필드	설명
elb	로드 밸런서의 리소스 ID입니다.
리스너	연결을 위한 TLS 리스너의 리소스 ID입니다.
client:port	클라이언트의 IP 주소 및 포트입니다.
destination:port	대상의 IP 주소 및 포트입니다. 클라이언트가 로드 밸런서에 직접 연결하는 경우 대상은 리스너입니다. 클라이언트가 VPC 엔드포인트 서비스를 사용하여 연결하는 경우 대상은 VPC 엔드포인트입니다.
connection_time	연결이 시작될 때부터 종료될 때까지 걸린 총 시간(단위: 밀리 초)입니다.
tls_handshake_time	클라이언트 측 지연을 포함해 TCP 연결이 설정된 후 TLS 핸드셰이크가 완료되는 데 걸리는 총 시간(단위: 밀리 초)입니다. 이 시간은 connection_time 필드에 포함됩니다.
received_bytes	해독 후 클라이언트에서 로드 밸런서가 수신한 바이트의 수입니다.
sent_bytes	암호화 전에 로드 밸런서가 클라이언트로 전송한 바이트의 수입니다.
incoming_tls_alert	클라이언트로부터 로드 밸런서가 수신한 TLS 알림의 정수 값(있는 경우). 그렇지 않으면 이 값은 -로 설정됩니다.
chosen_cert_arn	클라이언트에 제공된 인증서의 ARN입니다. 유효한 클라이언트 hello 메시지가 전송되지 않을 경우, 이 값은 -로 설정됩니다.
chosen_cert_serial	추후 사용 예약 이 값은 항상 -로 설정됩니다.
tls_cipher	클라이언트와 협상한 암호 그룹(OpenSSL 형식). TLS 협상이 완료되지 않을 경우, 이 값은 -로 설정됩니다.
tls_protocol_version	클라이언트와 협상한 TLS 프로토콜(문자열 형식)입니다. 가능한 값은 `tlsv10`, `tlsv11` 및 `tlsv12` 입니다. TLS 협상이 완료되지 않을 경우, 이 값은 -로 설정됩니다.
tls_named_group	추후 사용 예약 이 값은 항상 -로 설정됩니다.
domain_name	클라이언트 hello 메시지에서 server_name 확장명의 값입니다. 이 값은 URL로 인코딩된 것입니다. 유효한 클라이언트 hello 메시지가 전송되지 않거나 확장명이 없을 경우, 이 값은 -로 설정됩니다.
alpn_fe_protocol	클라이언트와 협상한 애플리케이션 프로토콜(문자열 형식)입니다. 가능한 값은 `h2`, `http/1.1` 및 `http/1.0` 입니다. TLS 리스너에 ALPN 정책이 구성되어 있지 않거나, 일치하는 프로토콜이 없거나, 유효한 프로토콜 목록이 전송되지 않은 경우 이 값은 -로 설정됩니다.
alpn_be_protocol	대상과 협상한 애플리케이션 프로토콜(문자열 형식)입니다. 가능한 값은 `h2`, `http/1.1` 및 `http/1.0` 입니다. TLS 리스너에 ALPN 정책이 구성되어 있지 않거나, 일치하는 프로토콜이 없거나, 유효한 프로토콜 목록이 전송되지 않은 경우 이 값은 -로 설정됩니다.
alpn_client_preference_list	클라이언트 hello 메시지에서 application_layer_protocol_negotiation 확장의 값입니다. 이 값은 URL로 인코딩된 것입니다. 각 프로토콜은 큰따옴표로 묶여 있으며 프로토콜은 쉼표로 구분됩니다. TLS 리스너에 ALPN 정책이 구성되어 있지 않거나, 유효한 클라이언트 hello 메시지가 전송되지 않거나, 확장이 없을 경우, 이 값은 -로 설정됩니다. 문자열이 256바이트보다 길면 잘리게 됩니다.

로그 항목 예제

다음은 로그 항목의 예제입니다. 보다 읽기 쉽도록 텍스트가 여러 줄에 나타납니다.

다음은 ALPN 정책이 없는 TLS 리스너의 예입니다.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - -
```

다음은 ALPN 정책이 있는 TLS 리스너의 예입니다.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1"
```

버킷 요구 사항

액세스 로그를 활성화할 때는 반드시 액세스 로그에 대한 S3 버킷을 지정해야 합니다. 로드 밸런서를 소유한 계정과 다른 계정으로 버킷을 소유할 수 있습니다. 버킷은 다음 요구 사항을 충족해야 합니다.

요구 사항

- 버킷은 로드 밸런서와 같은 리전에 있어야 합니다.
- 지정하는 접두사에는 AWSLogs가 포함되지 않아야 합니다. AWSLogs로 시작하는 파일 이름의 일부가 지정한 버킷 이름 및 접두사 뒤에 추가됩니다.
- Amazon S3- 관리형 암호화 키(SSE-S3)가 필요합니다. 다른 암호화 옵션은 지원되지 않습니다.
- 버킷에 대한 액세스 로그 쓰기 권한을 부여하는 버킷 정책이 이 버킷에 있어야 합니다. 버킷 정책은 버킷에 대한 액세스 권한을 정의하기 위해 액세스 정책 언어로 작성된 JSON 문의 집합입니다. 다음은 정책 예제입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket_name/prefix/AWSLogs/123456789012/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::bucket_name"
    }
  ]
}
```

액세스 로그 활성화

로드 밸런서에 대한 액세스 로그를 활성화할 때는 로드 밸런서가 로그를 저장할 S3 버킷의 이름을 지정해야 합니다. 자세한 내용은 버킷 요구 사항 (p. 57) 단원을 참조하십시오.

콘솔을 이용하여 액세스 로그를 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서를 선택합니다.
4. [Description] 탭에서 [Edit attributes]를 선택합니다.
5. [Edit load balancer attributes] 페이지에서 다음 작업을 수행합니다.
   a. [Access logs]에 대해 [Enable]을 선택합니다.
   b. S3 location]에 접두사를 포함하는 S3 버킷의 이름을 입력합니다(예: `my-loadbalancer-logs/my-app`). 기존 버킷의 이름이나 새 버킷의 이름을 지정할 수 있습니다. 기존 버킷을 지정하는 경우, 해당 버킷을 소유해야 하고 필요한 버킷 정책을 구성해야 합니다.
   c. (선택 사항) 버킷이 존재하지 않는 경우에는 [Create this location for me]를 선택합니다. Amazon S3의 모든 기존 버킷 이름에 대해 고유한 이름을 지정해야 하고 DNS 이름 지정 규칙을 따릅니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 버킷 이름 지정 규칙을 참조하십시오.
   d. 저장을 선택합니다.

AWS CLI를 이용하여 액세스 로그를 활성화하려면

modify-load-balancer-attributes 명령을 사용합니다.

액세스 로그 비활성화

언제든지 로드 밸런서에 대한 액세스 로그를 비활성화할 수 있습니다. 액세스 로그를 비활성화하면 액세스 로그는 사용자가 삭제할 때까지 S3 버킷에 남아 있습니다. 자세한 내용은 Amazon Simple Storage Service 콘솔 사용 설명서의 버킷을 사용한 작업을 참조하십시오.

콘솔을 이용하여 액세스 로그를 비활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서를 선택합니다.
4. [Description] 탭에서 [Edit attributes]를 선택합니다.
5. [Access logs]에 대해 [Enable]을 선택 해제합니다.
6. Save를 선택합니다.

AWS CLI를 이용하여 액세스 로그를 비활성화하려면

modify-load-balancer-attributes 명령을 사용합니다.

액세스 로그 파일 처리

액세스 로그 파일은 압축이 됩니다. Amazon S3; 콘솔을 사용해 파일을 열면 압축이 해제되고 정보가 표시됩니다. 파일을 다운로드하는 경우에는 압축을 해제해야 정보를 볼 수 있습니다.

웹 사이트에서 요청이 많은 경우에는 로드 밸런서가 수 기가바이트의 데이터로 로그 파일을 생성할 수 있습니다. 라인별 처리로는 이렇게 대량의 데이터를 처리할 수 없습니다. 따라서 병렬 처리 솔루션을 제공하는 분석 도구를 사용해야 할 수 있습니다. 예를 들어, 다음과 같은 분석 도구를 사용하여 액세스 로그를 분석 및 처리할 수 있습니다.

- Amazon Athena은 Amazon S3에서 표준 SQL을 사용하여 데이터를 쉽게 분석할 수 있는 대화형 쿼리 서비스입니다. 자세한 내용은 Amazon Athena 사용 설명서의 Network Load Balancer 로그 쿼리를 참조하십시오.
- Loggly
- Splunk
- Sumo Logic

AWS CloudTrail를 사용하여 Network Load Balancer에 대한 API 호출 로깅

Elastic Load Balancing은 AWS CloudTrail에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 Elastic Load Balancing과 통합됩니다. CloudTrail은 Elastic Load Balancing에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Management 콘솔의 호출과 Elastic Load Balancing API 작업에 대한 호출이 포함됩니다. 추적을 생성하면 Elastic Load Balancing에 대한 이벤트를 비롯하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 배포할 수 있습니다. 추적을 구성하지 않은 경우 Event history(이벤트 기록)에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다. CloudTrail에서 수집하는 정보를 사용하여 Elastic Load Balancing에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail User Guide 섹션을 참조하십시오.

CloudTrail의 Elastic Load Balancing 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Elastic Load Balancing에서 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하십시오.

Elastic Load Balancing 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려는 경우 추적을 생성합니다. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있도록 합니다. 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 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 정보는 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

Network Load Balancer에 대한 모든 Elastic Load Balancing 작업을 CloudTrail에서 로깅하여 Elastic Load Balancing API 참조 버전 2015-12-01에 기록됩니다. 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.

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Elastic Load Balancing 로그 파일 항목 이해

추적은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 제공할 수 있도록 해 주는 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 포함되어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 추적이 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 예입니다. `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",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
```

```
            "ipAddressType": "ipv4",
            "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/net/my-load-balancer/ffcddace1759e1d0",
            "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/net/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. 35) 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. 자세한 내용은 대상 보안 그룹 (p. 40) 단원을 참조하십시오.

ACL(액세스 제어 목록)이 트래픽을 허용하지 않음

인스턴스의 서브넷 및 로드 밸런서의 서브넷과 연결된 네트워크 ACL은 로드 밸런서의 트래픽 및 상태 확인을 허용해야 합니다. 자세한 내용은 네트워크 ACL (p. 40) 단원을 참조하십시오.

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. 자세한 내용은 대상 보안 그룹 (p. 40) 단원을 참조하십시오.

ACL(액세스 제어 목록)이 트래픽을 허용하지 않음

VPC의 서브넷과 연결된 네트워크 ACL이 로드 밸런서 및 대상이 리스너 포트에서 양방향으로 통신하도록 허용해야 합니다. 자세한 내용은 네트워크 ACL (p. 40) 단원을 참조하십시오.

대상이 활성화되지 않은 가용 영역에 있음

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

인스턴스가 피어링된 VPC에 속해 있음

로드 밸런서와 피어링된 VPC에 인스턴스가 있는 경우, 인스턴스를 인스턴스 ID가 아닌 IP 주소로 로드 밸런서에 등록해야 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 수신합니다.

대상이 예상보다 적은 상태 확인 요청을 수신함

`net.ipv4.tcp_tw_recycle`이 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.

호스트 헤더 불일치로 인해 대상이 HTTP 또는 HTTPS 상태 확인에 실패

상태 확인 요청의 HTTP 호스트 헤더에는 대상의 IP 주소 및 상태 확인 포트 대신 로드 밸런서 노드의 IP 주소 및 리스너 포트가 포함됩니다. 호스트 헤더별로 수신 요청을 매핑하는 경우 상태 확인이 HTTP 호스트 헤더와 일치하는지 확인해야 합니다. 또 다른 옵션은 다른 포트에 별도의 HTTP 서비스를 추가하고 대상 그룹이 상태 확인에 해당 포트를 대신 사용하도록 구성하는 것입니다. 또는 TCP 상태 확인을 사용할 수도 있습니다.

대상에서 로드 밸런서로의 요청에서 연결 시간이 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 Service을 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 Balancer와 Application Load Balancer는 모두 연결 멀티플렉싱을 사용하지만 Network Load Balancer는 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.

AWS PrivateLink를 통해 연결하는 포트 할당 오류

VPC 엔드포인트 서비스에 연결된 경우 Network Load Balancer는 각각의 고유 대상(IP 주소 및 포트)에 대해 55,000건의 동시 연결 또는 분당 약 55,000건의 연결을 지원합니다. 연결 건수가 이보다 더 많을 경우, 포트

할당 오류가 발생할 가능성이 증가합니다. 포트 할당 오류를 해결하려면 대상 그룹에 더 많은 대상들을 추가하십시오.

Network Load Balancer에 대한 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

Network Load Balancer에 대한 할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS services(AWS 서비스)를 선택하고 Elastic Load Balancing을 선택합니다. Elastic Load Balancing에 describe-account-limits(AWS CLI) 명령을 사용할 수도 있습니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 Elastic Load Balancing 제한 증가 양식을 사용합니다.

AWS 계정에는 Network Load Balancer와 관련하여 다음과 같은 할당량이 있습니다.

리전

- 리전당 Network Load Balancer: 50
- 리전당 대상 그룹: 3,000 *

로드 밸런서

- 로드 밸런서당 리스너: 50
- 로드 밸런서당 대상: 3,000
- 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
- 로드 밸런서당 인증서(기본 인증서는 포함되지 않음): 25

대상 그룹

- 대상 그룹당 로드 밸런서: 1
- 대상 그룹당 대상: 1,000

* 이 할당량은 Application Load Balancer 및 Network Load Balancer의 대상 그룹에서 공유합니다.

Network Load Balancer 문서 기록

다음 표에서는 Network Load Balancer의 릴리스를 설명합니다.

update-history-change	update-history-description	update-history-date
ALPN 정책	이 릴리스에는 ALPN(Application-Layer Protocol Negotiation) 기본 설정 목록에 대한 지원이 추가되었습니다.	May 27, 2020
고정 세션	이 릴리스에서는 소스 IP 주소 및 프로토콜을 기반으로 고정 세션에 대한 지원이 추가되었습니다.	February 28, 2020
공유 서브넷 (p. 66)	이 릴리스에는 다른 AWS 계정에 의해 사용자와 공유된 서브넷을 지정할 수 있는 지원이 추가되었습니다.	November 26, 2019
프라이빗 IP 주소 (p. 66)	이 릴리스에서는 내부 로드 밸런서에 대해 가용 영역을 활성화할 때 지정하는 서브넷의 IPv4 주소 범위에서 프라이빗 IP 주소를 제공할 수 있습니다.	November 25, 2019
서브넷 추가 (p. 66)	이 릴리스에는 로드 밸런서를 생성한 후 추가 가용 영역 활성화에 대한 지원이 추가되었습니다.	November 25, 2019
SNI 지원	이번 릴리스에는 SNI(Server Name Indication)에 대한 지원이 추가되었습니다.	September 12, 2019
UDP 프로토콜 (p. 66)	이 릴리스에서는 UDP 프로토콜을 추가로 지원합니다.	June 24, 2019
TLS 프로토콜	이 릴리스에서는 TLS 프로토콜을 추가로 지원합니다.	January 24, 2019
교차 영역 로드 밸런싱 (p. 66)	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. 66)	이 Elastic Load Balancing 릴리스에는 Network Load Balancer가 도입되었습니다.	September 7, 2017