aws

Network Load Balancers

Elastic Load Balancing

Elastic Load Balancing: Network Load Balancers

Table of Contents

Network Load Balancer란 무엇인가요?

Elastic Load Balancing은 둘 이상의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 등록된 대상의 상태를 모니터링하면서 상태가 양호한 대상으로만 트래픽을 라우팅합니다. Elastic Load Balancing은 수신 트래픽이 시간이 지남에 따라 변경됨에 따라 로드 밸런서를 확장합니다. 대다수의 워크로드에 맞게 자동으로 조정할 수 있습니다.

Elastic Load Balancing은 다음 로드 밸런서를 지원합니다. Application Load Balancers, Network Load Balancers, Gateway Load Balancers 및 Classic Load Balancer 각자 필요에 따라 가장 적합한 로드 밸런서 유형을 선택할 수 있습니다. 이 안내서에서는 Network Load Balancer에 대해 설명합니다. 다른 로드 밸런서에 대한 자세한 내용은 Application Load Balancer 사용 설명서, Gateway Load Balancer 사용 설명서, Classic Load Balancer 사용 설명서를 참조하세요.

Network Load Balancer 구성 요소

로드 밸런서는 클라이언트에 대한 단일 접점 역할을 수행합니다. 로드 밸런서는 수신 트래픽을 Amazon EC2 인스턴스와 같은 여러 대상에 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.

대상 그룹은 지정한 프로토콜과 포트 번호를 사용하여 EC2 인스턴스 같은 하나 이상의 등록된 대상으로 요청을 라우팅합니다. Network Load Balancer 대상 그룹은 TCP, UDP, TCP_UDP 및 TLS 프로토콜을 지원합니다. 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.

- 로드 밸런서
- 리스너
- 대상 그룹

Network Load Balancer 개요

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

로드 밸런서에서 가용 영역을 활성화하면 Elastic Load Balancing이 해당 가용 영역에서 로드 밸런서 노드를 생성합니다. 기본적으로 각 로드 밸런서 노드는 해당 가용 영역의 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 활성화하면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 대상 간에 트래픽을 분산합니다. 자세한 설명은 가용 영역 섹션을 참조하세요.

애플리케이션의 내결함성을 향상하려면 로드 밸런서에 대해 여러 가용 영역을 활성화하고 각 활성화된 가용 영역에 대해 각 대상 그룹에 하나 이상의 대상이 있는지 확인할 수 있습니다. 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 time-to-live (TTL) 을 준수하지 않고 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 포트와 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 Balancing은 활성화된 각 가용 영역에 대해 네트워크 인터페이스를 생성합니다. 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 대상 유형을 지정하며, 이 유형에 따라 대상을 등록하는 방법이 결정됩니다. 예를 들어 인스턴스 ID, IP 주소 또는 Application Load Balancer를 등록할 수 있습니다. 대상 유형은 클라이언트 IP 주소의 보존 여부에도 영향을 줍니다. 자세한 설명은 the section called “클라이언트 IP 보존” 섹션을 참조하세요.

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

Balancing은 로드 밸런서를 확장합니다. Elastic Load Balancing은 대다수의 워크로드에 맞게 자동으로 조정할 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 참조하세요.

Classic Load Balancer에서 마이그레이션할 때의 이점

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

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

각 유형의 로드 밸런서가 지원하는 기능에 대한 자세한 내용은 Elastic Load Balancing 제품 비교를 참조하세요.

시작하는 방법

Network Load Balancer를 만들려면 다음 자습서 중 하나를 사용하세요.

- Network Load Balancer 시작하기
- 자습서: AWS CLI를 사용하여 Network Load Balancer 생성

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

요금

자세한 내용은 Network Load Balancer 가격 책정을 참조하세요.

Network Load Balancer 시작하기

이 가이드에서는 웹 기반 인터페이스인 를 통해 네트워크 로드 밸런서를 직접 소개합니다. AWS Management Console첫 번째 Network Load Balancer를 생성하려면 다음 단계를 완료하세요.

Tasks

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

시작하기 전 준비 사항

- 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 정보는 대상 보안 그룹을 참조하세요.

1단계: 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.

콘솔을 사용하여 대상 그룹을 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.

3. 대상 그룹 생성을 선택합니다.
4. 대상 유형을 인스턴스로 유지합니다.
5. [대상 그룹 이름(Target group name)]에 새 대상 그룹의 이름을 입력합니다.
6. Protocol(프로토콜)에서 TCP를 선택하고 Port(포트)에서 80을 선택합니다.
7. VPC에서 인스턴스가 포함된 VPC를 선택합니다.
8. Health checks(상태 확인)에는 기본 설정을 그대로 둡니다.
9. 다음을 선택합니다.
10. 대상 등록(Register Targets) 페이지에서 다음 단계를 완료합니다. 이 단계는 대상 그룹을 만드는 선택적 단계입니다. 그러나 로드 밸런서를 테스트하고 대상으로 트래픽을 라우팅하고 있는지 확인하려면 대상을 등록해야 합니다.

    a. 사용 가능한 인스턴스(Available instance)에서 인스턴스를 하나 이상 선택합니다.

    b. 기본 포트 80을 유지하고 아래에서 보류 중인 것으로 포함(Include as pending below)을 선택합니다.
11. 대상 그룹 생성을 선택합니다.

2단계: 로드 밸런서 유형 선택

A: Elastic Load Balancing은 여러 타입의 로드 밸런서를 지원합니다. 이 자습서에서는 Network Load Balancer를 생성합니다.

콘솔을 사용하여 Network Load Balancer를 만들려면

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 Load Balancing에서 로드 밸런서를 선택합니다.
4. 로드 밸런서 생성을 선택하세요.
5. Network Load Balancer에 대해 [생성(Create)]을 선택합니다.

3단계: 로드 밸런서 및 리스너 구성

Network Load Balancer를 생성하려면 먼저 이름, 구성표 및 IP 주소 유형과 같은 로드 밸런서에 대한 기본 구성 정보를 제공해야 합니다. 그런 다음 네트워크와 하나 이상의 리스너에 대한 정보를 제공합니

다. 리스너는 연결 요청을 확인하는 프로세스입니다. 클라이언트와 로드 밸런서 간의 연결을 위한 프로토콜 및 포트로 구성됩니다. 지원되는 프로토콜 및 포트에 대한 자세한 내용은 리스너 구성 단원을 참조하십시오.

로드 밸런서 및 리스너를 구성하려면

1. 로드 밸런서 이름(Load Balancer name)에 로드 밸런서의 이름을 입력합니다. 예: `my-nlb`.
2. [Scheme] 및 [IP address type]은 기본값으로 유지합니다.
3. 네트워크 매핑에서 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 가용 영역의 서브넷에서 각 로드 밸런서 노드에 IPv4 주소를 AWS 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.
4. 보안 그룹에서 VPC의 기본 보안 그룹을 미리 선택합니다. 필요에 따라 다른 보안 그룹을 선택할 수 있습니다. 적합한 보안 그룹이 없는 경우 새 보안 그룹 생성을 선택하고 보안 요구 사항을 충족하는 보안 그룹을 생성합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 보안 그룹 생성을 참조하세요.

   > **Warning**
   >
   > 지금 보안 그룹을 로드 밸런서와 연결하지 않으면 나중에 연결할 수 없습니다.
5. 리스너 및 라우팅에 대해 기본 프로토콜과 포트를 유지하고 목록에서 대상 그룹을 선택합니다. 포트 80에서 TCP 트래픽을 수락하고 기본으로 선택한 대상 그룹에 트래픽을 전달하는 리스너를 구성합니다.
6. (선택 사항) 태그를 추가하여 로드 밸런서를 분류합니다. 태그 키는 각 로드 밸런서에 대해 고유해야 합니다. 허용되는 문자는 문자, 공백, 숫자(UTF-8 형식) 및 특수 문자 + - = . _ : / @입니다. 선행 또는 후행 공백을 사용하면 안 됩니다. 태그 값은 대소문자를 구분합니다.
7. 구성을 검토하고 로드 밸런서 생성(Create load balancer)을 선택합니다. 생성 중에 로드 밸런서에 몇 가지 기본 특성이 적용됩니다. 로드 밸런서를 생성한 후 이를 보고 편집할 수 있습니다. 자세한 내용은 로드 밸런서 속성 섹션을 참조하세요.

4단계: 로드 밸런서 테스트

로드 밸런서를 생성한 후에는 EC2 인스턴스에 트래픽을 전송하고 있는지 확인할 수 있습니다.

로드 밸런서를 테스트하려면

1. 로드 밸런서가 생성되었다는 통보를 받은 후 [Close]를 선택합니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 새로 생성한 대상 그룹을 선택합니다.
4. [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.
5. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
6. 새로 만든 로드 밸런서의 이름을 선택하여 세부 정보 페이지를 엽니다.
7. 로드 밸런서의 DNS 이름을 복사합니다 (예: -1234567890abcdef. elb.us-east-2.amazonaws.com). my-load-balancer DNS 이름을 인터넷에 연결된 웹 브라우저의 주소 필드에 붙여넣습니다. 모든 것이 잘 작동하는 경우 브라우저에 서버 기본 페이지가 표시됩니다.

5단계: (선택 사항) 로드 밸런서 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. 로드 밸런서를 삭제해도 로드 밸런서에 등록된 대상에는 영향을 미치지 않습니다. 예를 들어 EC2 인스턴스는 계속 실행됩니다.

콘솔을 사용하여 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 밸런서에 대한 확인란을 선택한 후 Actions(작업), Delete(삭제)를 선택합니다.
4. 확인 메시지가 나타나면 **`confirm`**을 입력하고 Delete(삭제)를 선택합니다.

자습서: AWS CLI를 사용하여 Network Load Balancer 생성

이 자습서에서는 AWS CLI를 통해 Network Load Balancer를 직접 소개합니다.

시작하기 전에

- Network Load Balancer를 지원하지 않는 버전을 사용하는 경우 AWS CLI를 설치하거나 AWS CLI의 현재 버전으로 업데이트합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서에서 AWS Command Line Interface 설치를 참조하세요.
- EC2 인스턴스에 대해 사용할 가용 영역을 결정합니다. 각 가용 영역에 있는 하나 이상의 퍼블릭 서브넷으로 VPC(Virtual Private Cloud)를 구성합니다.
- IPv4 또는 듀얼스택 로드 밸런서 중 무엇을 생성할지 결정합니다. 클라이언트가 IPv4 주소만을 사용하여 로드 밸런서와 통신하도록 하려는 경우 IPv4를 사용합니다. 클라이언트가 IPv4 및 IPv6 주소를 사용하여 로드 밸런서와 통신하도록 하려는 경우 듀얼스택을 사용합니다. 또한 듀얼스택을 사용하면 IPv6 애플리케이션 또는 듀얼스택 서브넷 등의 IPv6를 사용하는 백엔드 대상과 통신할 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 설명은 대상 보안 그룹 섹션을 참조하세요.

IPv4 로드 밸런서 생성

첫 번째 로드 밸런서를 생성하려면 다음 단계를 완료합니다.

IPv4 로드 밸런서를 생성하려면

1. create-load-balancer명령을 사용하여 IPv4 로드 밸런서를 생성하고, 인스턴스를 시작한 각 가용 영역의 퍼블릭 서브넷을 지정합니다. 가용 영역당 1개의 서브넷만 지정할 수 있습니다.

   기본적으로 Network Load Balancer는 AWS CLI를 사용하여 생성될 때 VPC의 기본 보안 그룹을 자동으로 사용하지 않습니다. 생성 중 보안 그룹을 로드 밸런서와 연결하지 않으면 나중에 추가할 수 없습니다. `--security-groups` 옵션을 사용하여 생성 중 로드 밸런서의 보안 그룹을 지정하는 것이 좋습니다.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
    subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
   ```

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-group명령을 사용하여 IPv4 대상 그룹을 생성하고 EC2 인스턴스에 사용한 것과 동일한 VPC를 지정합니다. IPv4 대상 그룹은 IP 및 인스턴스 유형 대상을 지원합니다.

```
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) 다음 명령을 사용하여 대상 그룹에 등록된 대상의 상태를 확인할 수 있습니다. describe-target-health

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

듀얼스택 로드 밸런서 생성

첫 번째 로드 밸런서를 생성하려면 다음 단계를 완료합니다.

듀얼스택 로드 밸런서를 생성하려면

1. create-load-balancer명령을 사용하여 이중 스택 로드 밸런서를 생성하고, 인스턴스를 시작한 각 가용 영역의 퍼블릭 서브넷을 지정합니다. 가용 영역당 1개의 서브넷만 지정할 수 있습니다.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
    subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
   ```

   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-group명령을 사용하여 대상 그룹을 만들고 EC2 인스턴스에 사용한 것과 동일한 VPC를 지정합니다.

   듀얼스택 로드 밸런서와 함께 TCP 또는 TLS 대상 그룹을 사용해야 합니다.

   듀얼스택 로드 밸런서와 연결할 IPv4 및 IPv6 대상 그룹을 생성할 수 있습니다. 대상 그룹의 IP 주소 유형에 따라 로드 밸런서가 백엔드 대상과 통신하고 상태를 확인하는 데 사용할 IP 버전이 결정됩니다.

   IPv4 대상 그룹은 IP 및 인스턴스 유형 대상을 지원합니다. IPv6 대상은 IP 대상만 지원합니다.

   ```
   aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
    vpc-0598c7d356EXAMPLE  --ip-address-type [ipv4 or ipv6]
   ```

   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 규칙을 적용해서 로드 밸런서에 대한 리스너를 생성합니다. 듀얼스택 로드 밸런서에는 TCP 또는 TLS 리스너가 있어야 합니다.

```
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) 다음 명령을 사용하여 대상 그룹에 등록된 대상의 상태를 확인할 수 있습니다. describe-target-health

```
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 그룹을 생성한 다음 대상을 해당 대상 그룹에 등록합니다. 활성화된 각 가용 영역에 등록된 대상이 하나 이상 있는지 확인하는 경우에 로드 밸런서가 가장 효과적입니다. 리스너를 생성하여 클라이언트의 연결 요청을 확인하고, 클라이언트에서 대상 그룹에 있는 대상으로 요청을 라우팅합니다.

네트워크 로드 밸런서는 VPC 피어링 AWS , 관리형 VPN AWS Direct Connect, 타사 VPN 솔루션을 통한 클라이언트 연결을 지원합니다.

내용

로드 밸런서 상태

로드 밸런서는 다음 중 하나의 상태를 가집니다.

`provisioning`

로드 밸런서를 설정하는 중입니다.

`active`

로드 밸런서가 완전히 설정되어 트래픽을 라우팅할 준비가 되었습니다.

`failed`

로드 밸런서를 설정할 수 없습니다.

로드 밸런서 속성

로드 밸런서는 다음과 같은 속성을 가지고 있습니다.

`access_logs.s3.enabled`

Amazon S3의 액세스 로그를 저장할지 여부를 나타냅니다. 기본값은 `false`입니다.

`access_logs.s3.bucket`

액세스 로그에 대한 Amazon S3 버킷 이름입니다. 이 속성은 액세스 로그가 활성화된 경우에 필요합니다. 자세한 내용은 버킷 요구 사항 단원을 참조하세요.

`access_logs.s3.prefix`

Amazon S3 버킷의 위치에 대한 접두사입니다.

`deletion_protection.enabled`

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

`ipv6.deny_all_igw_traffic`

인터넷 게이트웨이를 통해 내부 로드 밸런서에 대한 의도하지 않은 액세스가 발생하지 못하도록 로드 밸런서에 대한 인터넷 게이트웨이(IGW) 액세스를 차단합니다. 인터넷 연결 로드 밸런서에 대해서는 `false`로, 내부 로드 밸런서에 대해서는 `true`로 설정됩니다. 이 속성은 IGW가 아닌 인터넷 액세스 (예: 피어링, Transit Gateway 또는) 를 차단하지 않습니다. AWS Direct Connect AWS VPN

`load_balancing.cross_zone.enabled`

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

`dns_record.client_routing_policy`

로드 밸런서 가용 영역 간에 트래픽이 분산되는 방식을 나타냅니다. 가능한 값은 영역 친화도가 100%인 `availability_zone_affinity`, 영역 친화도가 85%인 `partial_availability_zone_affinity`, 영역 친화도가 0% 인 `any_availability_zone`입니다.

IP 주소 유형

클라이언트에게 로드 밸런서에 사용할 수 있도록 허용할 IP 주소 유형을 설정할 수 있습니다.

네트워크 로드 밸런서는 다음 IP 주소 유형을 지원합니다.

`ipv4`

클라이언트는 IPv4 주소(예: 192.0.2.1)를 사용하여 로드 밸런서에 연결해야 합니다. IPv4 지원 로드 밸런서(인터넷 연결 및 내부 모두)는 TCP, UDP, TCP_UDP 및 TLS 리스너를 지원합니다.

`dualstack`

클라이언트는 IPv4 주소(예: 192.0.2.1) 및 IPv6 주소(예: 2001:0db8:85a3:0:0:8a2e:0370:7334)를 사용하여 로드 밸런서에 연결할 수 있습니다. 듀얼스택 지원 로드 밸런서(인터넷 연결 및 내부 모두)는 TCP 및 TLS 리스너를 지원합니다.

고려 사항

- 로드 밸런서는 대상 그룹의 IP 주소 유형에 따라 대상과 통신합니다.
- 로드 밸런서에 대해 듀얼스택 모드를 활성화하면 Elastic Load Balancing에서 해당 로드 밸런서의 AAA DNS 레코드를 제공합니다. IPv4 주소를 사용하여 로드 밸런서와 통신하는 클라이언트는 A DNS 레코드를 확인합니다. IPv6 주소를 사용하여 로드 밸런서와 통신하는 클라이언트는 AAA DNS 레코드를 확인합니다.
- 의도하지 않은 인터넷 액세스를 방지하기 위해 인터넷 게이트웨이를 통한 내부 듀얼스택 로드 밸런서로의 액세스가 차단됩니다. 그러나 이렇게 해도 다른 인터넷 액세스 (예: 피어링, Transit Gateway 등 AWS VPN) 는 차단되지 않습니다. AWS Direct Connect

IP 주소 유형에 대한 자세한 내용은 을 참조하십시오Network Load Balancer의 IP 주소 유형.

Network Load Balancer 리소스 맵

Network Load Balancer 리소스 맵은 관련 리스너, 대상 그룹, 대상을 포함하여 로드 밸런서의 아키텍처를 대화식으로 표시합니다. 또한 리소스 맵은 모든 리소스 간의 관계와 라우팅 경로를 강조하여 로드 밸런서의 구성을 시각적으로 보여줍니다.

콘솔을 사용하여 네트워크 로드 밸런서의 리소스 맵을 보려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. 리소스 맵 탭을 선택하여 로드 밸런서의 리소스 맵을 표시합니다.

리소스 맵 구성 요소

맵 뷰

Network Load Balancer 리소스 맵에는 개요 및 비정상 대상 맵이라는 두 가지 보기가 있습니다. 개요는 기본적으로 선택되며 로드 밸런서의 모든 리소스를 표시합니다. 비정상 대상 맵 보기를 선택하면 비정상 대상 및 이와 관련된 리소스만 표시됩니다.

비정상 타겟 맵 뷰는 상태 확인에 실패한 대상의 문제를 해결하는 데 사용할 수 있습니다. 자세한 정보는 리소스 맵을 사용하여 비정상 대상 문제 해결을 참조하세요.

리소스 컬럼

Network Load Balancer 리소스 맵에는 리소스 유형별로 하나씩 총 3개의 리소스 열이 있습니다. 리소스 그룹은 리스너, 타겟 그룹, 타겟입니다.

리소스 타일

열 내의 각 리소스에는 고유한 타일이 있으며, 이 타일에는 해당 특정 리소스에 대한 세부 정보가 표시됩니다.

- 리소스 타일 위로 마우스를 가져가면 해당 타일과 다른 리소스 간의 관계가 강조 표시됩니다.
- 리소스 타일을 선택하면 해당 타일과 다른 리소스 간의 관계가 강조되고 해당 리소스에 대한 추가 세부 정보가 표시됩니다.
  - 대상 그룹 상태 요약: 각 상태에 등록된 대상의 수.

- 대상 건강 상태: 대상의 현재 건강 상태 및 설명.

> **Note**
>
> 리소스 세부 정보 표시를 끄면 리소스 맵 내에서 추가 세부 정보를 숨길 수 있습니다.

- 각 리소스 타일에는 선택 시 해당 리소스의 세부정보 페이지로 이동하는 링크가 포함되어 있습니다.
  - 리스너 - 리스너 프로토콜:포트를 선택합니다. 예제: `TCP:80`
  - 대상 그룹 - 대상 그룹 이름을 선택합니다. 예제: `my-target-group`
  - 대상 - 대상 ID를 선택합니다. 예제: `i-1234567890abcdef0`

리소스 맵 익스포트

내보내기를 선택하면 네트워크 로드 밸런서 리소스 맵의 현재 보기를 PDF로 내보낼 수 있는 옵션이 제공됩니다.

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 Balancer의 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 이름이 포함됨). 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 Balancing은 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.

고려 사항

- 인터넷 경계 로드 밸런서의 경우, 사용자가 지정하는 서브넷에 사용 가능한 IP 주소가 8개 이상 있어야 합니다. 내부 로드 밸런서의 경우 서브넷에서 프라이빗 IPv4 주소를 AWS 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.
- 자신이 사용자와 공유한 서브넷은 지정할 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 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. Network mapping(네트워크 매핑) 탭에서 Edit subnets(서브넷 편집)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. 변경 사항 저장를 선택합니다.

를 사용하여 가용 영역을 추가하려면 AWS CLI

set-subnets 명령을 사용합니다.

교차 영역 로드 밸런싱

기본적으로 각 로드 밸런서 노드는 해당 가용 영역의 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 켜면 각 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 대상 간에 트래픽을 분산합니다. 대상 그룹 수준으로 교차 영역 로드 밸런싱을 켤 수도 있습니다. 자세한 내용은 the section called “교차 영역 로드 밸런싱” 및 Elastic Load Balancing 사용 설명서의 교차 영역 로드 밸런싱을 참조하세요.

삭제 방지

로드 밸런서가 실수로 삭제되지 않도록 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 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 구성에서 삭제 방지를 켭니다.
6. 변경 사항 저장를 선택합니다.

콘솔을 사용하여 삭제 방지 기능을 비활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 구성에서 삭제 방지를 켭니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 삭제 보호를 활성화 또는 비활성화하려면 AWS CLI

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

연결 유휴 제한 시간

클라이언트가 Network Load Balancer를 통해 보내는 각 TCP 요청에 대해 해당 연결의 상태가 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.

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. TLS 연결을 유지하기 위해 전송된 Keepalive 패킷에는 데이터나 페이로드가 포함될 수 없습니다.

TLS 리스너가 클라이언트 또는 대상으로부터 TCP keepalive 패킷을 수신하면 로드 밸런서는 TCP keepalive 패킷을 생성하여 20초마다 프런트엔드 및 백엔드 연결 모두에 전송합니다. 이 동작은 수정할 수 없습니다.

UDP가 연결이 없는 동안 로드 밸런서는 소스 및 대상 IP 주소와 포트를 기반으로 UDP 흐름 상태를 유지합니다. 따라서 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 Balancing은 UDP 흐름의 유휴 시간 초과 값을 120초로 설정합니다.

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

DNS 이름

각 Network Load Balancer는 다음 구문을 사용하여 기본 DNS(도메인 이름 시스템)을 수신합니다. *name-id*.elb.*region*.amazonaws.com. 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 DNS 레코드를 생성하여 쿼리를 로드 밸런서로 라우팅 요청을 하려면 도메인 등록 대행자와 같은 DNS 서비스를 사용하면 됩니다. 자세한 내용은 DNS 서비스에 대한 설명서를 참조하세요. 예를 들어, DNS 서비스로 Amazon Route 53을 사용하는 경우 로드 밸런서를 지정하는 별칭 레코드를 생성합니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 ELB 로드 밸런서로 트래픽 라우팅을 참조하세요.

로드 밸런서는 활성화된 각 가용 영역에 대하여 하나의 IP 주소를 가집니다. 이는 로드 밸런서 노드의 IP 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. DNS 이름을 다음 구문과 함께 사용하여 로드 밸런서 노드의 IP 주소를 확인할 수 있습니다. *az*.*name*-*id*.elb.*region*.amazonaws.com.

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
```

가용 영역 DNS 친화도

기본 클라이언트 라우팅 정책을 사용하는 경우 Network Load Balancer DNS 이름으로 전송된 요청은 정상적인 로드 밸런서 IP 주소를 수신합니다. 이로 인해 로드 밸런서의 가용 영역 전체에 클라이언트 연결이 분산됩니다. 가용 영역 친화도 라우팅 정책을 사용하면 클라이언트 DNS 쿼리가 자체 가용 영역에 있는 로드 밸런서 IP 주소를 선호합니다. 이렇게 하면 클라이언트가 대상에 연결할 때 가용 영역 경계를 교차할 필요가 없으므로 지연 시간과 복원력을 모두 개선하는 데 도움이 됩니다.

Route 53 Resolver를 사용하는 Network Load Balancer에 사용할 수 있는 클라이언트 라우팅 정책:

- 가용 영역 친화도 — 100% 영역 친화도

  클라이언트 DNS 쿼리는 자체 가용 영역에 있는 로드 밸런서 IP 주소를 선호합니다. 자체 영역에 정상적인 로드 밸런서 IP 주소가 없는 경우 쿼리가 다른 영역에서 확인될 수 있습니다.
- 부분적 가용 영역 친화도 — 85%의 영역 친화도

클라이언트 DNS 쿼리의 85%는 자체 가용 영역의 로드 밸런서 IP 주소를 선호하지만 나머지 쿼리는 정상 영역으로 확인됩니다. 해당 영역에 정상 IP가 없는 경우 쿼리가 다른 정상 영역에서 확인될 수 있습니다. 영역에 정상 IP가 없는 경우 쿼리는 영역에서 확인됩니다.

- 모든 가용 영역(기본값) — 영역 친화도 0%

  모든 로드 밸런서 가용 영역의 정상 로드 밸런서 IP 주소 사이에서 클라이언트 DNS 쿼리가 해결됩니다.

> **Note**
>
> 가용 영역 친화도 라우팅 정책은 Route 53 Resolver를 사용하여 Network Load Balancer의 DNS 이름을 확인하는 클라이언트에만 적용됩니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 Amazon Route 53 Resolver란 무엇인가요?을(를) 참조하세요

가용 영역 친화도는 클라이언트의 요청을 로드 밸런서로 라우팅하는 데 도움이 되며, 교차 영역 로드 밸런싱은 로드 밸런서의 요청을 대상으로 라우팅하는 데 사용됩니다. 가용 영역 어피니티를 사용할 때는 영역 간 로드 밸런싱을 꺼야 합니다. 이렇게 하면 클라이언트에서 타겟으로 가는 로드 밸런서 트래픽이 동일한 가용 영역 내에 유지됩니다. 이 구성을 사용하면 클라이언트 트래픽이 동일한 Network Load Balancer 가용 영역으로 전송되므로 각 가용 영역에서 독립적으로 확장되도록 애플리케이션을 구성하는 것이 좋습니다. 이는 가용 영역당 클라이언트 수 또는 가용 영역당 트래픽이 동일하지 않을 때 중요한 고려 사항입니다. 자세한 정보는 대상 그룹에 대한 교차 영역 로드 밸런싱을 참조하세요.

가용 영역이 비정상으로 간주되거나 영역 전환이 시작된 경우, 실패 오픈이 적용되지 않는 한 영역 IP 주소는 비정상으로 간주되어 클라이언트에 반환되지 않습니다. 가용 영역 친화도는 DNS 레코드 열기에 실패해도 유지됩니다. 이를 통해 가용 영역을 독립적으로 유지하고 잠재적인 교차 영역 장애를 예방할 수 있습니다.

가용 영역 친화도를 사용할 경우 가용 영역 간 불균형이 발생할 것으로 예상됩니다. 각 가용 영역 워크로드를 지원할 수 있도록 대상을 영역 수준으로 확장하는 것이 좋습니다. 이러한 불균형이 심각한 경우에는 가용 영역 친화도를 끄는 것이 좋습니다. 이렇게 하면 60초 이내에 모든 로드 밸런서의 가용 영역 또는 DNS TTL 간에 클라이언트 연결을 균등하게 분배할 수 있습니다.

가용 영역 친화도를 사용하기 전에 다음 사항을 고려하세요.

- 가용 영역 친화도로 인해 Route 53 Resolver를 사용하는 모든 Network Load Balancer 클라이언트가 변경됩니다.

  - 클라이언트는 영역-로컬 및 다중 영역 DNS 해상도 중 하나를 결정할 수 없습니다. 가용 영역 친화도가 해당 사항을 결정합니다.
  - 클라이언트는 언제 가용 영역 선호도의 영향을 받는지, 어떤 IP 주소가 어떤 가용 영역에 있는지 알 수 있는 방법을 확인하는 신뢰할 수 있는 방법을 제공하지 않습니다.
- 클라이언트는 DNS 상태 확에 따라 완전히 비정상으로 간주되어 DNS에서 제거될 때까지 해당 영역-로컬 IP 주소를 계속 할당받습니다.
- 교차 영역 로드 밸런서가 설정된 상태에서 가용 영역 친화도를 사용하면 가용 영역 간 클라이언트 연결이 불균형하게 분산될 수 있습니다. 각 가용 영역에서 독립적으로 확장되도록 애플리케이션 스택을 구성하여 영역의 클라이언트 트래픽을 지원할 수 있도록 하는 것이 좋습니다.
- 교차 영역 로드 밸런서가 켜져 있는 경우 Network Load Balancer는 교차 영역의 영향을 받을 수 있습니다.
- 각 Network Load Balancer 가용 영역의 로드는 클라이언트 요청의 영역 위치에 비례합니다. 어떤 가용 영역에서 실행 중인 클라이언트 수를 구성하지 않으면 각 가용 영역에 반응하여 독립적으로 확장해야 합니다.

모니터링

영역의 로드 밸런서 지표를 사용하여 가용 영역 간 연결 분포를 추적하는 것이 좋습니다. 지표를 사용하여 영역당 신규 및 활성 연결 수를 볼 수 있습니다.

다음과 같이 추적하는 것이 좋습니다.

- **`ActiveFlowCount`** – 클라이언트에서 대상까지의 동시 흐름(또는 연결)의 총 수입니다.
- **`NewFlowCount`** – 해당 기간에 클라이언트에서 대상까지 설정되는 새로운 흐름(또는 연결)의 총 수입니다.
- **`HealthyHostCount`** – 정상 상태로 간주되는 대상 수.
- **`UnHealthyHostCount`** – 비정상 상태로 간주되는 대상 수.

자세한 내용은 CloudWatch 네트워크 로드 밸런서의 지표 섹션을 참조하세요.

가용 영역 친화도 켜기

이 절차의 단계에서는 Amazon EC2 콘솔을 사용하여 가용 영역 친화도를 켜는 방법을 설명합니다.

콘솔을 사용하여 가용 영역 친화도 켜기

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 가용 영역 라우팅 구성의 클라이언트 라우팅 정책(DNS 레코드)에서 가용 영역 친화도 또는 부분적 가용 영역 친화도를 선택합니다.
6. 변경 사항 저장를 선택합니다.

가용 영역 어피니티를 켜려면 다음을 사용하십시오. AWS CLI

`dns_record.client_routing_policy` 속성과 함께 modify-load-balancer-attributes 명령을 사용합니다.

가용 영역 친화도 끄기

이 절차의 단계에서는 Amazon EC2 콘솔을 사용하여 가용 영역 친화도를 끄는 방법을 설명합니다.

콘솔을 사용하여 가용 영역 친화도 끄기

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 가용 영역 라우팅 구성의 클라이언트 라우팅 정책(DNS 레코드)에서 가용 영역을 선택합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 가용 영역 어피니티를 끄려면 AWS CLI

`dns_record.client_routing_policy` 속성과 함께 modify-load-balancer-attributes 명령을 사용합니다.

Network Load Balancer 생성

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 확인하세요. 또한 대상 그룹으로 트래픽을 라우팅하려면 대상 그룹을 구성하고 하나 이상의 대상을 기본값으로 설정해야 합니다.

를 사용하여 로드 밸런서를 만들려면 AWS CLI을 참조하십시오. 자습서: AWS CLI를 사용하여 Network Load Balancer 생성

를 사용하여 로드 밸런서를 만들려면 다음 작업을 완료하세요. AWS Management Console

Tasks

- 1단계: 대상 그룹 구성
- 2단계: 대상 등록
- 3단계: 로드 밸런서 및 리스너 구성
- 4단계: 로드 밸런서 테스트

1단계: 대상 그룹 구성

대상 그룹을 구성하면 EC2 인스턴스와 같은 대상을 등록할 수 있습니다. 이 단계에서 구성하는 대상 그룹은 로드 밸런서를 구성할 때 리스너 규칙의 대상 그룹으로 사용됩니다. 자세한 정보는 Network Load Balancer 대상 그룹을 참조하세요.

콘솔을 사용하여 대상 그룹을 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 대상 그룹을 선택합니다.
3. 대상 그룹 생성을 선택합니다.
4. 기본 구성 창에서 다음을 수행합니다.
    a. Choose a target type(대상 유형 선택)에서 인스턴스 ID로 대상을 등록하려면 Instances(인스턴스)를 선택하고, IP 주소로 대상을 등록하려면 IP addresses(IP 주소)를 선택하고, Application Load Balancer를 대상으로 등록하려면 Application Load Balancer를 선택합니다.
    b. 대상 그룹 이름(Target group name)에 대상 그룹의 이름을 입력합니다.

c. 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.

d. (선택 사항) 포트에서 필요에 따라 기본값을 변경합니다.

e. IP 주소 유형에서 IPv4 또는 IPv6를 선택합니다. 이 옵션은 대상 유형이 인스턴스 또는 IP 주소이고 프로토콜이 TCP 또는 TLS인 경우에 사용할 수 있습니다.

IPv6 대상 그룹은 듀얼스택 로드 밸런서와 연결해야 합니다. 대상 그룹의 모든 대상은 동일한 IP 주소 유형을 가져야 합니다. 대상 그룹을 생성한 후에는 대상 그룹의 IP 주소 유형을 변경할 수 없습니다.

f. VPC에서 등록하려는 대상이 있는 Virtual Private Cloud(VPC)를 선택합니다.

5. 상태 확인 창에서 필요에 따라 기본 설정을 수정합니다. 고급 상태 확인 설정에서 상태 확인 포트, 개수, 시간 초과, 간격 및 성공 코드를 선택합니다. 상태 확인이 비정상 임계값 수를 연속으로 초과하는 경우 로드 밸런서는 대상을 서비스 중단 상태로 만듭니다. 상태 확인이 정상 임계값 수를 연속으로 초과하는 경우 로드 밸런서는 대상을 다시 서비스 상태로 전환합니다. 자세한 정보는 대상 그룹에 대한 상태 확인을 참조하세요.
6. (선택 사항) 태그를 추가하려면 태그를 확장하고 태그 추가를 선택하여 태그 키와 태그 값을 입력합니다.
7. [Next]를 선택합니다.

2단계: 대상 등록

EC2 인스턴스, IP 주소 또는 Application Load Balancer를 대상 그룹에 등록할 수 있습니다. 로드 밸런서를 생성하기 위한 선택적 단계입니다. 그러나 대상을 등록해야 로드 밸런서가 트래픽을 해당 대상으로 라우팅할 수 있습니다.

1. 대상 등록 페이지에서 다음과 같이 하나 이상의 대상을 추가합니다.
   - 대상 유형이 인스턴스인 경우 인스턴스를 선택하고 포트를 입력한 다음 아래에 보류 중인 것으로 포함을 선택합니다.
   - 대상 유형이 IP 주소인 경우 네트워크를 선택하고 IP 주소와 포트를 입력한 다음 아래에 보류 중인 것으로 포함을 선택합니다.
   - 대상 유형이 Application Load Balancer인 경우 Application Load Balancer를 선택합니다.

2. [Create target group]을 선택합니다.

3단계: 로드 밸런서 및 리스너 구성

Network Load Balancer를 생성하려면 먼저 이름, 구성표 및 IP 주소 유형과 같은 로드 밸런서에 대한 기본 구성 정보를 제공해야 합니다. 그런 다음 네트워크와 하나 이상의 리스너에 대한 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 단원을 참조하십시오.

콘솔을 사용하여 로드 밸런서와 리스너를 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 생성을 선택하세요.
4. Network Load Balancer에서 [생성(Create)]을 선택합니다.
5. 기본 구성

   a. 로드 밸런서 이름(Load Balancer name)에 로드 밸런서의 이름을 입력합니다. 예: **`my-nlb`**. Network Load Balancer의 이름은 해당 리전의 Application Load Balancer 및 Network Load Balancer 세트 내에서 고유해야 합니다. 최대 32자여야 하며 영숫자 및 하이픈만 포함할 수 있습니다. 하이픈 또는 `internal-`(으)로 시작하거나 끝나서는 안 됩니다.

   b. 구성표(Scheme)에서 internet-facing 또는 internal을 선택합니다. internet-facing 로드 밸런서는 인터넷을 통해 클라이언트의 요청을 대상으로 라우팅합니다. 내부 로드 밸런서는 프라이빗 IP 주소를 사용하여 요청을 대상으로 라우팅합니다.

   c. IP 주소 유형의 경우, 클라이언트가 IPv4 주소를 사용하여 로드 밸런서와 통신하는 경우 IPv4를 선택하고, 클라이언트가 IPv4 및 IPv6 주소를 둘 다 사용하여 로드 밸런서와 통신하는 경우 듀얼 스택을 선택합니다.
6. 네트워크 매핑

   a. VPC에서는 EC2 인스턴스에 사용한 것과 동일한 VPC를 선택합니다.

      구성표(Scheme)에 대해 Internet-facing을 선택한 경우 인터넷 게이트웨이가 있는 VPC만 선택할 수 있습니다.

b. 매핑(Mappings)에 대해 하나 이상의 가용 영역과 해당 서브넷을 선택합니다. 여러 가용 영역을 활성화하면 애플리케이션의 내결함성이 향상됩니다. 자신이 사용자와 공유한 서브넷은 지정할 수 있습니다.

   internet-facing 로드 밸런서의 경우, 각 가용 영역에 대해 탄력적 IP 주소를 선택할 수 있습니다. 그러면 로드 밸런서에 고정 IP 주소가 제공됩니다. 또는 내부 부하 분산기의 경우 사설 IP 주소를 자동으로 할당하지 않고 각 서브넷의 IPv4 범위에서 사설 IP 주소를 할당할 수 있습니다. AWS

7. 보안 그룹에서 VPC의 기본 보안 그룹을 미리 선택합니다. 필요에 따라 다른 보안 그룹을 선택할 수 있습니다. 적합한 보안 그룹이 없는 경우 새 보안 그룹 생성을 선택하고 보안 요구 사항을 충족하는 보안 그룹을 생성합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 보안 그룹 생성을 참조하세요.

   > **Warning**
   >
   > 지금 보안 그룹을 로드 밸런서와 연결하지 않으면 나중에 연결할 수 없습니다.

8. 리스너 및 라우팅

   a. 기본값은 포트 80에서 TCP 트래픽을 수락하는 리스너입니다. 기본 리스너 설정을 그대로 두거나 필요에 따라 프로토콜 또는 포트를 변경합니다.

   b. 기본 작업(Default action)에서 트래픽을 전달할 대상 그룹을 선택합니다. 이전에 대상 그룹을 생성하지 않은 경우 지금 생성해야 합니다. 리스너 추가(Add listener)를 선택해 다른 리스너(예: TLS 리스너)를 추가할 수도 있습니다.

   c. (선택 사항) 태그를 추가하여 리스너를 분류합니다.

   d. 보안 리스너 설정(TLS 리스너에만 사용 가능)의 경우 다음을 수행합니다.

      i. 보안 정책의 경우 요구 사항을 충족하는 보안 정책을 선택합니다.

      ii. ALPN 정책의 경우 ALPN을 활성화할 정책을 선택하거나 [None]을 선택하여 ALPN을 비활성화합니다.

      iii. 기본 SSL 인증서경우 ACM에서(From ACM)(권장)를 선택하고 인증서를 선택합니다. 사용 가능한 인증서가 없는 경우 인증서를 ACM으로 가져오거나 ACM을 사용하여 인증서를 프로비저닝할 수 있습니다. 자세한 내용은 AWS Certificate Manager 사용자 안내서의 인증서 발급 및 관리를 참조하세요.

9. (선택 사항) 로드 밸런서와 함께 애드온 서비스를 사용할 수 있습니다. 예를 들어, 액셀러레이터를 자동으로 AWS Global Accelerator생성하고 로드 밸런서를 액셀러레이터에 연결하도록 선택할 수

있습니다. 액셀러레이터 이름은 a-z, A-Z, 0-9, 등의 문자 (최대 64자) 를 사용할 수 있습니다. (마침표) 및 - (하이픈). 액셀러레이터를 만든 후 AWS Global Accelerator콘솔로 이동하여 구성을 완료합니다. 자세한 내용은 로드 밸런서 생성 시 가속기 추가를 참조하십시오.

10. 태그

    (선택 사항) 태그를 추가하여 로드 밸런서를 분류합니다. 자세한 내용은 태그를 참조하세요.

11. 요약

    구성을 검토하고 로드 밸런서 생성(Create load balancer)을 선택합니다. 생성 중에 로드 밸런서에 몇 가지 기본 특성이 적용됩니다. 로드 밸런서를 생성한 후 이를 보고 편집할 수 있습니다. 자세한 정보는 로드 밸런서 속성을 참조하세요.

4단계: 로드 밸런서 테스트

로드 밸런서를 생성한 후, EC2 인스턴스가 초기 상태 확인을 통과했는지 확인한 다음 로드 밸런서가 EC2 인스턴스로 트래픽을 전송하고 있는지 검사할 수 있습니다. 로드 밸런서를 삭제하려면 Network Load Balancer 삭제 섹션을 참조하세요.

로드 밸런서 테스트

1. 로드 밸런서가 생성된 후 [Close]를 선택합니다.
2. 탐색 창에서 대상 그룹을 선택합니다.
3. 새로운 대상 그룹을 선택합니다.
4. [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. 자세한 정보는 대상 상태을 참조하세요.
5. 탐색 창에서 로드 밸런서를 선택합니다.
6. 새 로드 밸런서를 선택합니다.
7. 로드 밸런서의 DNS 이름을 복사합니다 (예: my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). DNS 이름을 인터넷에 연결된 웹 브라우저의 주소 필드에 붙여넣습니다. 모든 것이 잘 작동하는 경우 브라우저에 서버 기본 페이지가 표시됩니다.

Network Load Balancer의 IP 주소 유형

클라이언트가 로드 밸런서와 통신할 때 IPv4 주소만 사용하도록 하거나 IPv4 및 IPv6 주소를 둘 다 사용하도록(듀얼스택) Network Load Balancer를 구성할 수 있습니다. 로드 밸런서는 대상 그룹의 IP 주소 유형에 따라 대상과 통신합니다. 자세한 정보는 IP 주소 유형을 참조하세요.

DualStack 요구 사항

- 로드 밸런서를 만들고 업데이트할 때 언제든지 IP 주소 유형을 설정할 수 있습니다.
- 로드 밸런서용으로 지정하는 Virtual Private Cloud(VPC) 및 서브넷에는 연결된 IPv6 CIDR 블록이 있어야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 IPv6 주소를 참조하세요.
- 로드 밸런서에는 TCP 및 TLS 리스너만 있어야 합니다.
- 로드 밸런서 서브넷의 라우팅 테이블은 IPv6 트래픽을 라우팅해야 합니다.
- 로드 밸런서 서브넷의 네트워크 ACL은 IPv6 트래픽을 허용해야 합니다.

생성 시 IP 주소 유형을 설정하려면

로드 밸런서 생성에 설명된 대로 설정을 구성합니다.

콘솔을 사용하여 IP 주소 유형을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서의 확인란을 선택합니다.
4. 작업, IP 주소 유형 편집을 선택합니다.
5. IP 주소 유형에서 IPv4를 선택하여 IPv4 주소만 지원하거나 듀얼 스택을 선택하여 IPv4 주소와 IPv6 주소를 모두 지원합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 IP 주소 유형을 업데이트하려면 AWS CLI

set-ip-address-type 명령을 사용합니다.

Network Load Balancer의 보안 그룹

보안 그룹을 Network Load Balancer와 연결하여 로드 밸런서에 도달하고 나갈 수 있는 트래픽을 제어할 수 있습니다. 인바운드 트래픽을 허용할 포트, 프로토콜 및 소스와 아웃바운드 트래픽을 허용할 포

트, 프로토콜 및 대상을 지정합니다. 로드 밸런서에 보안 그룹을 할당하지 않으면 모든 클라이언트 트래픽이 로드 밸런서 리스너에 도달할 수 있고 모든 트래픽이 로드 밸런서를 벗어날 수 있습니다.

대상과 연결된 보안 그룹에 Network Load Balancer와 연결된 보안 그룹을 참조하는 규칙을 추가할 수 있습니다. 이렇게 하면 클라이언트가 로드 밸런서를 통해 대상으로 트래픽을 전송할 수 있지만 대상으로 직접 트래픽을 전송할 수는 없습니다. 대상과 연결된 보안 그룹에서 Network Load Balancer와 연결된 보안 그룹을 참조하면 로드 밸런서에 대해 클라이언트 IP 보존을 활성화하더라도 대상이 로드 밸런서로부터 트래픽을 허용합니다.

인바운드 보안 그룹 규칙에 의해 차단된 트래픽에 대해서는 요금이 부과되지 않습니다.

내용

고려 사항

- Network Load Balancer를 생성할 때 보안 그룹을 Network Load Balancer와 연결할 수 있습니다. 보안 그룹을 연결하지 않고 Network Load Balancer를 생성하면 나중에 해당 보안 그룹을 로드 밸런서와 연결할 수 없습니다. 로드 밸런서를 생성할 때 보안 그룹을 로드 밸런서와 연결하는 것이 좋습니다.
- 연결된 보안 그룹이 있는 Network Load Balancer를 생성한 후 언제든지 로드 밸런서와 연결된 보안 그룹을 변경할 수 있습니다.
- 상태 확인에는 아웃바운드 규칙이 적용되지만 인바운드 규칙은 적용되지 않습니다. 아웃바운드 규칙이 상태 확인 트래픽을 차단하지 않는지 확인해야 합니다. 그렇지 않으면 로드 밸런서는 대상을 비정상으로 간주합니다.
- PrivateLink 트래픽에 인바운드 규칙이 적용되는지 여부를 제어할 수 있습니다. PrivateLink 트래픽에 인바운드 규칙을 사용하도록 설정하는 경우 트래픽의 소스는 엔드포인트 인터페이스가 아니라 클라이언트의 프라이빗 IP 주소입니다.

예: 클라이언트 트래픽 필터링

Network Load Balancer와 연결된 보안 그룹의 다음 인바운드 규칙은 지정된 주소 범위에서 오는 트래픽만 허용합니다. 내부 로드 밸런서인 경우 VPC CIDR 범위를 소스로 지정하여 특정 VPC로부터 트래픽만 허용할 수 있습니다. 인터넷의 모든 위치에서 오는 트래픽을 수락해야 하는 인터넷 경계 로드 밸런서인 경우 0.0.0.0/0을 소스로 지정할 수 있습니다.

인바운드

프로토콜	소스	포트 범위	설명
protocol	***##### IP ## ##***	***### ##***	리스너 포트에서 소스 CIDR의 인바운드 트래픽 허용
ICMP	0.0.0.0/0	모두	인바운드 ICMP 트래픽이 MTU 또는 경로 MTU 검색을 지원하도록 허용 †

† 자세한 내용은 Amazon EC2 사용 설명서의 경로 MTU 검색을 참조하십시오.

아웃바운드

프로토콜	대상	포트 범위	설명
모두	Anywhere	모두	모든 아웃바운드 트래픽을 허용합니다

예: 로드 밸런서의 트래픽만 수락

Network Load Balancer에 보안 그룹 sg-1111122222233333이 있다고 가정해 보겠습니다. 대상 인스턴스와 연결된 보안 그룹에서 다음 규칙을 사용하여 Network Load Balancer의 트래픽만 허용하도록 합니다. 대상이 대상 포트와 상태 확인 포트 모두에서 로드 밸런서로부터 트래픽을 수락하는지 확인해야 합니다. 자세한 정보는 the section called “대상 보안 그룹”을 참조하세요.

인바운드

프로토콜	소스	포트 범위	설명
protocol	sg-111112222233333	***## ##***	대상 포트에서 로드 밸런서의 인바운드 트래픽 허용

프로토콜	소스	포트 범위	설명
protocol	sg-111112 222233333	*## ##*	상태 확인 포트에서 로드 밸런서의 인바운드 트래픽 허용

아웃바운드

프로토콜	대상	포트 범위	설명
모두	Anywhere	모두	모든 아웃바운드 트래픽을 허용합니다

연결된 보안 그룹 업데이트

로드 밸런서를 생성할 때 하나 이상의 보안 그룹을 로드 밸런서와 연결한 경우 언제든지 해당 로드 밸런서에 대한 보안 그룹을 업데이트할 수 있습니다.

콘솔을 사용하여 보안 그룹을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. 보안 탭에서 편집을 선택합니다.
5. 로드 밸런서에 보안 그룹을 연결하려면 보안 그룹을 선택합니다. 로드 밸런서에서 보안 그룹을 제거하려면 보안 그룹을 선택 취소합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 보안 그룹을 업데이트하려면 AWS CLI

set-security-groups 명령을 사용합니다.

보안 설정 업데이트

기본적으로 로드 밸런서로 전송되는 모든 트래픽에 인바운드 보안 그룹 규칙을 적용합니다. 하지만 로드 밸런서를 통해 AWS PrivateLink전송되는 트래픽에는 이러한 규칙을 적용하지 않는 것이 좋습니다.

이 트래픽은 중복되는 IP 주소에서 발생할 수 있습니다. 이 경우 로드 밸런서를 통해 전송되는 트래픽에 대해 인바운드 규칙을 적용하지 않도록 로드 밸런서를 구성할 수 있습니다. AWS PrivateLink

콘솔을 사용하여 보안 설정 업데이트

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. 보안 탭에서 편집을 선택합니다.
5. 보안 설정에서 트래픽에 인바운드 규칙 적용을 선택 해제합니다. PrivateLink
6. 변경 사항 저장를 선택합니다.

를 사용하여 보안 설정을 업데이트하려면 AWS CLI

set-security-groups 명령을 사용합니다.

로드 밸런서 보안 그룹 모니터링

`SecurityGroupBlockedFlowCount_Inbound`및 `SecurityGroupBlockedFlowCount_Outbound` CloudWatch 지표를 사용하여 로드 밸런서 보안 그룹에 의해 차단된 흐름의 수를 모니터링할 수 있습니다. 차단된 트래픽은 다른 지표에 반영되지 않습니다. 자세한 정보는 the section called “CloudWatch 지표”을 참조하세요.

VPC 흐름 로그를 사용하여 로드 밸런서 보안 그룹에서 수락하거나 거부하는 트래픽을 모니터링합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하세요.

Network Load Balancer에 대한 태그

태그는 로드 밸런서를 다양한 방식으로 분류할 수 있도록 해줍니다. 예를 들어 용도, 소유자 또는 환경별로 리소스를 태깅할 수 있습니다.

각 로드 밸런서에 여러 태그를 추가할 수 있습니다. 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 + - = . _ : / @입니다. 선행 또는 후행 공백을 사용하면 안 됩니다.
- `aws:`접두사는 사용하도록 예약되어 있으므로 태그 이름이나 값에 사용하지 마십시오. AWS 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 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 태그 탭에서 태그 관리를 선택합니다.
5. 태그를 추가하려면 태그 추가를 선택한 다음 태그 키와 태그 값을 입력합니다. 허용되는 문자는 문자, 공백, 숫자(UTF-8 형식) 및 특수 문자 + - = . _ : / @입니다. 선행 또는 후행 공백을 사용하면 안 됩니다. 태그 값은 대소문자를 구분합니다.
6. 태그를 업데이트하려면 키 및 값에 새 값을 입력합니다.
7. 태그를 삭제하려면 태그 옆의 제거(Remove) 버튼을 선택합니다.
8. 작업을 마쳤으면 변경 사항 저장을 선택합니다.

를 사용하여 로드 밸런서의 태그를 업데이트하려면 AWS CLI

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 단원을 참조하세요.

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 단원을 참조하세요.

콘솔을 사용하여 로드 밸런서를 삭제하려면

1. 로드 밸런서를 가리키는 도메인을 위한 DNS 레코드가 있는 경우에는 새로운 위치를 가리키도록 하고 로드 밸런서를 삭제하기 전에 DNS 변경이 적용될 때까지 기다립니다.

   예제

   - 레코드가 300초 TTL(Time To Live)인 CNAME 레코드인 경우 다음 단계를 계속하기 전에 300초 이상 기다려야 합니다.
   - 레코드가 Route 53 Alias(A) 레코드인 경우 60초 이상 기다려야 합니다.
   - Route 53을 사용하는 경우 레코드 변경 사항이 모든 글로벌 Route 53 이름 서버에 전파되는 데 60초가 걸립니다. 업데이트 중인 레코드의 TTL 값에 이 시간을 더합니다.
2. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
3. 탐색 창에서 [Load Balancers]를 클릭합니다.
4. 로드 밸런서의 확인란을 선택합니다.
5. 작업, 로드 밸런서 삭제를 선택합니다.
6. 확인 메시지가 나타나면 **`confirm`**을 입력하고 Delete(삭제)를 선택합니다.

를 사용하여 로드 밸런서를 삭제하려면 AWS CLI

delete-load-balancer 명령을 사용합니다.

영역 전환

영역 전환은 Amazon Route 53 Application Recovery Controller(Route 53 ARC) 내의 기능입니다. 영역 전환을 사용하면 한 번의 작업으로 손상된 가용 영역에서 로드 밸런서 리소스를 다른 곳으로 이동할 수 있습니다. 이러한 방법을 통해 AWS 리전의 다른 정상 가용 영역에서 계속 운영할 수 있습니다.

영역 전환을 시작하면 로드 밸런서가 해당 리소스에 대한 트래픽을 영향을 받는 가용 영역으로 보내는 것을 중단합니다. Route 53 ARC는 영역 전환을 즉시 생성합니다. 그러나 영향을 받는 가용 영역에서 진행 중인 기존 연결을 완료하는 데는 보통 몇 분 정도 소요될 수 있습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller 개발자 안내서의 영역 이동 작동 방식: 상태 확인 및 영역 IP 주소를 참조하세요.

영역 이동은 교차 영역 로드 밸런싱이 꺼진 상태에서 Application Load Balancer 및 Network Load Balancer에서만 지원됩니다. 교차 영역 로드 밸런싱을 켜면 영역 전환을 시작할 수 없습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller 개발자 안내서의 영역 전환에 지원되는 리소스를 참조하세요.

영역 전환을 사용하기 전에 다음을 검토하세요.

- 영역 이동에서는 교차 영역 로드 밸런싱이 지원되지 않습니다. 이 기능을 사용하려면 교차 영역 로드 밸런싱을 꺼야 합니다.
- Application Load Balancer를 AWS Global Accelerator에서 액셀러레이터 엔드포인트로 사용할 때는 영역 전환이 지원되지 않습니다.
- 특정 로드 밸런서에 대한 영역 전환은 단일 가용 영역에 대해서만 시작할 수 있습니다. 여러 가용 영역에 대한 영역 전환은 시작할 수 없습니다.
- AWS 여러 인프라 문제가 서비스에 영향을 미칠 경우 DNS에서 영역 로드 밸런서 IP 주소를 사전에 제거합니다. 영역 전환을 시작하기 전에 항상 현재 가용 영역 용량을 확인하세요. 로드 밸런서의 교차 영역 로드 밸런싱이 꺼져 있으며 영역 전환을 사용하여 영역 로드 밸런서 IP 주소를 제거하는 경우, 영역 전환의 영향을 받는 가용 영역도 대상 용량을 잃게 됩니다.
- Network Load Balancer의 대상인 Application Load Balancer는 항상 Network Load Balancer에서 영역 이동을 시작하세요. Application Load Balancer에서 영역 전환을 시작하는 경우 Network Load Balancer는 이동을 인식하지 못하고 Application Load Balancer로 트래픽을 계속 전송합니다.

자세한 내용은 Amazon Route 53 Application Recovery Controller 개발자 안내서의 Route 53 ARC 영역 전환 모범 사례를 참조하세요.

영역 전환 시작

이 절차의 단계에서는 Amazon EC2 콘솔을 사용하여 영역 이동을 시작하는 방법을 설명합니다. Route 53 ARC 콘솔을 사용하여 영역 전환을 시작하는 단계는 Amazon Route 53 Application Recovery Controller 개발자 안내서의 영역 전환 시작하기를 참조하세요.

콘솔을 사용하여 영역 이동을 시작하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서를 선택합니다.
4. Integrations(통합) 탭의 Route 53 Application Recovery Controller에서 Start zonal shift(영역 이동 시작)을 선택합니다.
5. 트래픽을 이동할 가용 영역을 선택합니다.
6. 영역 이동에 대한 만료를 선택하거나 입력합니다. 영역 이동은 처음에 1분부터 최대 3일(72시간)까지 설정할 수 있습니다.

   모든 영역 이동은 일시적입니다. 만료를 설정해야 하지만 나중에 활성 이동을 업데이트하여 만료를 새로 설정할 수 있습니다.
7. 설명을 입력합니다. 원하는 경우 나중에 영역 전환을 업데이트하여 설명을 편집할 수 있습니다.
8. 영역 전환을 시작하면 트래픽을 해당 가용 영역에서 다른 곳으로 이동하여 애플리케이션의 용량이 줄어든다는 것을 확인하려면 확인란을 선택합니다.
9. 시작을 선택합니다.

다음을 사용하여 영역 전환을 시작하려면 AWS CLI

프로그래밍 방식으로 영역 이동 작업을 수행하려면 영역 이동 API 참조 안내서를 참조하세요

영역 전환 업데이트

이 절차의 단계에서는 Amazon EC2 콘솔을 사용하여 영역 이동을 업데이트하는 방법을 설명합니다. Amazon Route 53 Application Recovery Controller 콘솔을 사용하여 영역 전환을 업데이트하는 단계는 Amazon Route 53 Application Recovery Controller 개발자 안내서의 영역 전환 업데이트를 참조하세요.

콘솔을 사용하여 영역 이동을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 활성 영역 전환이 있는 로드 밸런서 이름을 선택합니다.
4. 통합 탭의 Route 53 Application Recovery Controller에서 영역 전환 업데이트를 선택합니다.

   그러면 Route 53 ARC 콘솔이 열리며 업데이트를 계속할 수 있습니다.

5. 영역 전환 만료 설정에서 만료를 선택하거나 입력할 수 있습니다.
6. Comment(설명)의 경우 기존 설명을 편집하거나 새 설명을 입력할 수 있습니다.
7. 업데이트를 선택합니다.

를 사용하여 영역 이동을 업데이트하려면 AWS CLI

프로그래밍 방식으로 영역 이동 작업을 수행하려면 영역 이동 API 참조 안내서를 참조하세요.

영역 전환 취소

이 절차의 단계에서는 Amazon EC2 콘솔을 사용하여 영역 이동을 취소하는 방법을 설명합니다. Amazon Route 53 Application Recovery Controller 콘솔을 사용하여 영역 전환을 취소하는 단계는 Amazon Route 53 Application Recovery Controller 개발자 안내서의 영역 전환 취소를 참조하세요.

콘솔을 사용하여 영역 이동을 취소하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 활성 영역 전환이 있는 로드 밸런서 이름을 선택합니다.
4. 통합 탭의 Route 53 Application Recovery Controller에서 영역 전환 취소를 선택합니다.

   그러면 Route 53 ARC 콘솔이 열리면서 취소를 계속할 수 있습니다.
5. Cancel zonal shift(영역 이동 취소)를 선택합니다.
6. 확인 대화 상자에서 Confirm(확인)을 선택합니다.

를 사용하여 영역 이동을 취소하려면 AWS CLI

프로그래밍 방식으로 영역 이동 작업을 수행하려면 영역 이동 API 참조 안내서를 참조하세요.

Network Load Balancer를 위한 리스너

리스너는 구성한 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. Network Load Balancer를 사용하기 전에 리스너를 하나 이상 추가해야 합니다. 로드 밸런서에 리스너가 없는 경우 클라이언트로부터 트래픽을 수신할 수 없습니다. 리스너에 대해 정의하는 규칙에 따라 로드 밸런서가 EC2 인스턴스와 같이 등록한 대상으로 요청을 라우팅하는 방법이 결정됩니다.

내용

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 정보는 Network Load Balancer를 위한 TLS 리스너을 참조하세요.

대상이 로드 밸런서 대신 TLS 트래픽을 해독하도록 하려면 TLS 리스너를 생성하는 대신 포트 443에서 수신하는 TCP 리스너를 생성합니다. TCP 리스너를 사용하여 로드 밸런서는 암호화된 트래픽을 해독하지 않고 대상으로 전달합니다.

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

Dualstack Network Load Balancer의 경우 TCP 및 TLS 프로토콜만 지원됩니다.

WebSockets 청취자와 함께 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 대상에 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.

자세한 내용은 Elastic Load Balancing 사용 설명서의 라우팅 요청을 참조하세요.

리스너 규칙

리스너를 생성할 때 라우팅 요청의 규칙을 지정합니다. 이 규칙은 요청을 지정된 대상 그룹으로 전달합니다. 이 규칙을 업데이트하려면 Network Load Balancer를 위한 리스너 업데이트 단원을 참조하십시오.

Network Load Balancer에 대한 리스너 만들기

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

필수 조건

- 리스너 규칙에 대한 대상 그룹을 지정해야 합니다. 자세한 내용은 Network Load Balancer에 대한 대상 그룹 만들기 단원을 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 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 단원을 참조하십시오.

콘솔을 사용하여 리스너를 추가하려면

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

2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. Listeners(리스너) 탭에서 Add listener(리스너 추가)를 선택합니다.
5. Protocol(프로토콜)에서 TCP, UDP, TCP_UDP, 또는 TLS를 선택합니다. 기본 포트를 그대로 두거나 다른 포트를 입력합니다. Dualstack Network Load Balancer의 경우 TCP 및 TLS 프로토콜만 지원됩니다.
6. Default action(기본 작업)에서 사용 가능한 대상 그룹을 선택합니다.
7. [TLS 리스너] Select policy(정책 선택)에서 기본 보안 정책을 유지하는 것이 좋습니다.
8. [TLS 리스너] Default SSL certificate(기본 SSL 인증서)에서 다음 중 한 가지를 수행합니다.
   - 를 사용하여 AWS Certificate Manager인증서를 생성하거나 가져온 경우 [From ACM] 을 선택하고 인증서를 선택합니다.
   - IAM을 사용하여 인증서를 업로드한 경우 [IAM에서(From IAM)]을 선택하고 인증서를 선택합니다.
9. [TLS 리스너] ALPN 정책의 경우 ALPN을 활성화할 정책을 선택하거나 [None]을 선택하여 ALPN을 비활성화합니다. 자세한 정보는 ALPN 정책을 참조하세요.
10. 추가(Add)를 선택합니다.
11. [TLS 리스너] SNI 프로토콜에 사용할 인증서 목록을 추가(선택 사항)하려면 인증서 목록에 인증서 추가 섹션을 참조하세요.

를 사용하여 리스너를 추가하려면 AWS CLI

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. 암호화된 트래픽을 로드 밸런서의 해독 없이 대상으로 전달해야 하는 경우, TLS 리스너를 생성하는 대신 포트 443에서 수신하는 TCP 리스너를 생성합니다. 로드 밸런서는 요청을 해독하지 않고 있는 그대로 대상으로 전달합니다.

Elastic Load Balancing은 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 데이터

를 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 재협상 또는 mTLS(상호 TLS 인증)를 지원하지 않습니다. mTLS를 지원하려면 TLS 리스너 대신 TCP 리스너를 생성합니다. 로드 밸런서는 요청을 있는 그대로 전달하므로 대상에서 mTLS를 구현할 수 있습니다.

TLS 리스너를 생성하려면 리스너 추가 섹션을 참조하세요. 관련 데모는 Network Load Balancer에 대한 TLS 지원 및 Network Load Balancer에 대한 SNI 지원을 참조하세요.

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. 인증서의 도메인 이름은 사용자 지정 도메인 이름 레코드와 일치해야 TLS 연결을 확인할 수 있습니다. 두 값이 일치하지 않는 경우 트래픽이 암호화되지 않습니다.

인증서에 `www.example.com`과 같은 정규화된 도메인 이름(FQDN) 또는 `example.com`과 같은 apex 도메인 이름을 지정해야 합니다. 별표(*)를 와일드카드로 사용하여 동일한 도메인 내에서 여러 사이트 이름을 보호할 수도 있습니다. 와일드카드 인증서를 요청할 때 별표(*)는 도메인 이름의 맨 왼쪽에 와야 하며 하나의 하위 도메인 수준만 보호할 수 있습니다. 예를 들어 `*.example.com`은 `corp.example.com` 및 `images.example.com`은 보호하지만 `test.login.example.com`을 보호할 수는 없습니다. 또한 `*.example.com`은 `example.com`의 하위 도메인만 보호하고 베어 또는 apex 도메인(`example.com`)은 보호하지 못합니다. 와일드카드 이름은 주체 필드와 인증서의 주체 대체 이름 확장에 표시됩니다. 퍼블릭 인증서 요청에 대한 자세한 내용은 AWS Certificate Manager 사용 설명서의 퍼블릭 인증서 요청을 참조하세요.

AWS Certificate Manager (ACM)를 사용해 로드 밸런서를 위한 인증서를 생성하는 것이 좋습니다. ACM은 Elastic Load Balancing과 통합하여 로드 밸런서에 인증서를 배포합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서를 참조하세요.

또는 TLS 도구를 사용하여 인증서 서명 요청 (CSR) 을 생성한 다음 CA의 CSR 서명을 받아 인증서를 생성한 다음 인증서를 ACM으로 가져오거나 (IAM) 에 인증서를 업로드할 수 있습니다. AWS Identity

and Access Management 자세한 내용은 AWS Certificate Manager 사용 설명서의 인증서 가져오기 또는 IAM 사용 설명서의 서버 인증서 작업 단원을 참조하세요.

내용

지원되는 키 알고리즘

- RSA 1024비트
- RSA 2048비트
- RSA 3072비트
- ECDSA 256비트
- ECDA 384비트
- ECDSA 521비트

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 단원을 참조하십시오.

인증서 목록에서 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 여

러 도메인을 지원하고 각 도메인에 대해 다른 인증서를 제공할 수 있습니다. 자세한 내용은 인증서 목록에 인증서 추가 단원을 참조하세요.

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.

- 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 단원을 참조하세요.

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.

- 로드 밸런서에서 AWS Certificate Manager 제공하고 배포한 인증서는 자동으로 갱신할 수 있습니다. ACM은 인증서가 만료되기 전에 갱신을 시도합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서에서 관리형 갱신을 참조하세요.
- ACM에 인증서를 가져온 경우에는 인증서의 만료일을 반드시 모니터링해서 만료되기 전에 인증서를 갱신해야 합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서에서 인증서 가져오기를 참조하세요.
- IAM으로 인증서를 가져온 경우, 새 인증서를 만들어 ACM이나 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 정보는 보안 정책 업데이트을 참조하세요.

고려 사항:

- 정책은 를 사용하여 만든 TLS 수신기의 기본 보안 `ELBSecurityPolicy-TLS13-1-2-2021-06` 정책입니다. AWS Management Console
  - TLS 1.3을 포함하고 TLS 1.2와 이전 버전과 호환되는 `ELBSecurityPolicy-TLS13-1-2-2021-06` 보안 정책을 사용하는 것이 좋습니다.
- 정책은 를 사용하여 만든 TLS 수신기의 기본 보안 `ELBSecurityPolicy-2016-08` 정책입니다. AWS CLI
- 프런트엔드 연결에는 사용할 보안 정책을 선택할 수 있지만 백엔드 연결에는 사용할 수 없습니다.
  - 백엔드 연결의 경우 TLS 리스너가 TLS 1.3 보안 정책을 사용하는 경우, `ELBSecurityPolicy-TLS13-1-0-2021-06` 보안 정책이 사용됩니다. 그렇지 않으면, `ELBSecurityPolicy-2016-08` 보안 정책은 백엔드 연결에 사용됩니다.
- 특정 TLS 프로토콜 버전을 사용하지 않도록 설정해야 하는 규정 준수 및 보안 표준을 충족하거나 더 이상 사용되지 않는 암호가 필요한 레거시 클라이언트를 지원하려면 보안 정책 중 하나를 사용할 수 있습니다. `ELBSecurityPolicy-TLS-` Network Load Balancer로 전송된 TLS 요청에 대한 정보에 대한 액세스 로그를 활성화하고, TLS 트래픽 패턴을 분석하고, 보안 정책 업그레이드를 관리하고, 문제를 해결할 수 있습니다. 로드 밸런서에 대한 액세스 로깅을 활성화하고 해당 액세스 로그 항목을 검사하십시오. 자세한 내용은 액세스 로그 및 Network Load Balancer 예시 쿼리를 참조하세요.
- IAM AWS 계정 및 AWS Organizations 서비스 제어 정책 (SCP) 에서 각각 Elastic Load Balancing 조건 키를 사용하여 전 세계 사용자가 사용할 수 있는 보안 정책을 제한할 수 있습니다. 자세한 내용은 사용 설명서의 서비스 제어 정책 (SCP) 을 참조하십시오.AWS Organizations

TLS 1.3 보안 정책

Elastic Load Balancing은 네트워크 로드 밸런서에 대해 다음과 같은 TLS 1.3 보안 정책을 제공합니다.

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(권장)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06`
- `ELBSecurityPolicy-TLS13-1-1-2021-06`
- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

FIPS 보안 정책

연방 정보 처리 표준 (FIPS) 은 민감한 정보를 보호하는 암호화 모듈의 보안 요구 사항을 지정하는 미국 및 캐나다 정부 표준입니다. 자세한 내용은 AWS 클라우드 보안 규정 준수 페이지에서 연방 정보 처리 표준 (FIPS) 140을 참조하십시오.

모든 FIPS 정책은 AWS-LC FIPS 검증을 거친 암호화 모듈을 활용합니다. 자세한 내용은 NIST 암호화 모듈 검증 프로그램 사이트의 AWS-LC 암호화 모듈 페이지를 참조하십시오.

Elastic Load Balancing은 네트워크 로드 밸런서에 대해 다음과 같은 FIPS 보안 정책을 제공합니다.

- `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`(권장)
- `ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`

FS 지원 정책

Elastic Load Balancing은 네트워크 로드 밸런서에 대해 다음과 같은 FS (순방향 보안) 지원 보안 정책을 제공합니다.

- `ELBSecurityPolicy-FS-1-2-Res-2020-10`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-2018-06`

TLS 1.0 - 1.2 보안 정책

Elastic Load Balancing은 네트워크 로드 밸런서에 대해 다음과 같은 TLS 1.0 - 1.2 보안 정책을 제공합니다.

- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-TLS-1-0-2015-04
- ELBSecurityPolicy-2015-05(와 동일) **ELBSecurityPolicy-2016-08**

TLS 프로토콜 및 암호

TLS 1.3

다음 표에는 사용 가능한 TLS 1.3 보안 정책에 지원되는 TLS 프로토콜 및 암호가 설명되어 있습니다.

참고: 보안 정책 행의 정책 이름에서 ELBSecurityPolicy- 접두사가 제거되었습니다.

예: 보안 정책은 로 ELBSecurityPolicy-TLS13-1-2-2021-06 표시됩니다. TLS13-1-2-2021-06

보안 정책	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
TLS 프로토콜							
Protocol-TLSv1							✓
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓

보안 정책	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
프로토콜-TLSv1.3	✓	✓	✓	✓	✓	✓	✓
TLS 암호							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓

보안 정책	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
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	✓		✓	✓	✓	✓	✓

보안 정책	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-ECDSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓
AES128-GCM-SHA256				✓	✓	✓	✓
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓

보안 정책	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

CLI를 사용하여 TLS 1.3 정책을 사용하는 TLS 리스너를 만들려면

리스너 생성 명령을 모든 TLS 1.3 보안 정책과 함께 사용하십시오.

이 예제에서는 보안 정책을 사용합니다. ELBSecurityPolicy-TLS13-1-2-2021-06

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

CLI를 사용하여 TLS 1.3 정책을 사용하도록 TLS 리스너를 수정하려면

모든 TLS 1.3 보안 정책과 함께 modify-listener 명령을 사용하십시오.

이 예제에서는 보안 정책을 사용합니다. ELBSecurityPolicy-TLS13-1-2-2021-06

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

CLI를 사용하여 리스너가 사용하는 보안 정책을 보려면

리스너의 설명-리스너 명령을 함께 사용하십시오. arn

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

CLI를 사용하여 TLS 1.3 보안 정책의 컨피그레이션을 보려면

모든 TLS 1.3 보안 정책과 함께 describe-ssl-policies명령을 사용하십시오.

이 예에서는 ELBSecurityPolicy-TLS13-1-2-2021-06 보안 정책을 사용합니다.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

> **Important**
>
> 정책은 ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 레거시 호환성을 위해서만 ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 제공됩니다. FIPS140 모듈을 사용하여 FIPS 암호화를 사용하지만 TLS 구성에 대한 최신 NIST 지침을 준수하지 않을 수 있습니다.

다음 표에는 사용 가능한 FIPS 보안 정책에 지원되는 TLS 프로토콜 및 암호가 설명되어 있습니다.

참고: 보안 정책 행의 정책 이름에서 ELBSecurityPolicy- 접두사가 제거되었습니다.

예: 보안 정책은 로 ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 표시됩니다. TLS13-1-2-FIPS-2023-04

보안 정책	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
TLS 프로토콜								
Protocol-TLSv1								✓
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
프로토콜-TLSv1.3	✓	✓	✓	✓	✓	✓	✓	✓
TLS 암호								
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-		✓	✓	✓	✓	✓	✓	✓

보안 정책	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
SHA256								
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓	✓

보안 정책	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384			✓	✓	✓	✓	✓	✓

보안 정책	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓

보안 정책	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

CLI를 사용하여 FIPS 정책을 사용하는 TLS 리스너를 만들려면

모든 FIPS 보안 정책과 함께 create-listener 명령을 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

CLI를 사용하여 FIPS 정책을 사용하도록 TLS 리스너를 수정하려면

모든 FIPS 보안 정책과 함께 modify-listener 명령을 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

CLI를 사용하여 리스너가 사용하는 보안 정책을 보려면

리스너의 설명-리스너 명령을 함께 사용하십시오. arn

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

CLI를 사용하여 FIPS 보안 정책의 컨피그레이션을 보려면

모든 FIPS describe-ssl-policies보안 정책과 함께 명령을 사용하십시오.

이 예에서는 ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 보안 정책을 사용합니다.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

다음 표에서는 사용 가능한 FS 지원 보안 정책에 지원되는 TLS 프로토콜 및 암호를 설명합니다.

참고: 보안 정책 행의 정책 이름에서 ELBSecurityPolicy- 접두사가 제거되었습니다.

예: 보안 정책은 로 ELBSecurityPolicy-FS-2018-06 표시됩니다. FS-2018-06

보안 정책	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
TLS 프로토콜						
Protocol-TLSv1	✓					✓
Protocol-TLSv1.1	✓				✓	✓

보안 정책	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
TLS 암호						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓

보안 정책	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓		✓	✓	✓	✓

보안 정책	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					
AES256-GCM-SHA384	✓					

보안 정책	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-SHA256	✓					
AES256-SHA	✓					

CLI를 사용하여 FS 지원 정책을 사용하는 TLS 리스너를 만들려면

모든 FS 지원 보안 정책과 함께 create-listener 명령을 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-FS-2018-06

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

CLI를 사용하여 FS 지원 정책을 사용하도록 TLS 리스너를 수정하려면

modify-listener 명령을 모든 FS 지원 보안 정책과 함께 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-FS-2018-06

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

CLI를 사용하여 리스너가 사용하는 보안 정책을 보려면

리스너의 설명-리스너 명령을 함께 사용하십시오. arn

```
aws elbv2 describe-listener \
```

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

CLI를 사용하여 FS 지원 보안 정책의 구성을 보려면

모든 FS 지원 보안 정책과 함께 describe-ssl-policies명령을 사용하십시오.

이 예에서는 ELBSecurityPolicy-FS-2018-06 보안 정책을 사용합니다.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

다음 표에서는 사용 가능한 TLS 1.0-1.2 보안 정책에 지원되는 TLS 프로토콜 및 암호를 설명합니다.

참고: 보안 정책 행의 정책 이름에서 ELBSecurityPolicy- 접두사가 제거되었습니다.

예: 보안 정책은 로 ELBSecurityPolicy-TLS-1-2-Ext-2018-06 표시됩니다. TLS-1-2-Ext-2018-06

보안 정책	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
TLS 프로토콜					
Protocol-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓

보안 정책	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
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	✓	✓		✓	✓

보안 정책	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
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	✓	✓	✓	✓	✓

보안 정책	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
AES128-SHA	✓	✓		✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓
DES-CBC3-SHA					✓

* 보안이 약한 DES-CBC3-SHA 암호를 필요로 하는 기존 클라이언트를 지원해야 하는 경우 외에는 한 이 정책을 사용하지 마세요.

CLI를 사용하여 TLS 1.0-1.2 정책을 사용하는 TLS 리스너를 만들려면

리스너 생성 명령을 모든 TLS 1.0-1.2가 지원되는 보안 정책과 함께 사용하십시오.

이 예에서는 보안 정책을 사용합니다. `ELBSecurityPolicy-2016-08`

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

CLI를 사용하여 TLS 1.0-1.2 정책을 사용하도록 TLS 리스너를 수정하려면

modify-listener 명령을 모든 TLS 1.0-1.2가 지원되는 보안 정책과 함께 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-2016-08

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-2016-08
```

CLI를 사용하여 리스너가 사용하는 보안 정책을 보려면

리스너의 설명-리스너 명령을 함께 사용하십시오. arn

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

CLI를 사용하여 TLS 1.0-1.2 보안 정책의 컨피그레이션을 보려면

모든 TLS 1.0-1.2가 지원되는 보안 정책과 함께 describe-ssl-policies명령을 사용하십시오.

이 예에서는 보안 정책을 사용합니다. ELBSecurityPolicy-2016-08

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-2016-08
```

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.

지원되는 ALPN 정책

지원되는 ALPN 정책은 다음과 같습니다.

`HTTP10nly`

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

`HTTP20nly`

HTTP/2만 협상합니다. ALPN 기본 설정 목록은 h2입니다.

`HTTP20ptional`

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 및 ALPN 정책 업데이트 단원을 참조하십시오.

Network Load Balancer를 위한 리스너 업데이트

전달 작업에서 트래픽을 수신하는 리스너 프로토콜, 리리스너 포트 또는 대상 그룹을 업데이트할 수 있습니다. 기본 규칙이라고도 하는 기본 작업은 선택된 대상 그룹에 요청을 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.

리스너의 기본 작업에 대한 대상 그룹이 업데이트되면 새 연결이 새로 구성된 대상 그룹으로 라우팅됩니다. 그러나 이 변경 이전에 생성된 활성 연결에는 영향을 주지 않습니다. 이러한 활성 연결은 트래픽이 전송되는 경우에는 최대 한 시간 동안, 트래픽이 전송되지 않은 경우에는 최대 유휴 제한 시간이 경과할 때까지 원래 대상 그룹의 대상과 연결된 상태로 유지되며, 이 중 먼저 도래하는 시점이 적용됩니다. 매개 변수 `Connection termination on deregistration`은(는) 대상 등록을 취소할 때 적용되므로 리스너를 업데이트할 때는 적용되지 않습니다.

콘솔을 사용하여 리스너를 업데이트하려면

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

2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 편집을 선택합니다.
6. (선택 사항) 필요에 따라 프로토콜 및 포트에 대해 지정된 값을 변경합니다.
7. (선택 사항) 기본 작업에 대한 다른 대상 그룹을 선택합니다.
8. (선택 사항) 필요에 따라 태그를 추가, 업데이트 또는 제거합니다.
9. 변경 사항 저장를 선택합니다.

를 사용하여 리스너를 업데이트하려면 AWS CLI

modify-listener 명령을 사용하세요.

Network Load Balancer를 위한 TLS 리스너 업데이트

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

Tasks

- 기본 인증서 교체
- 인증서 목록에 인증서 추가
- 인증서 목록에서 인증서 제거
- 보안 정책 업데이트
- ALPN 정책 업데이트

기본 인증서 교체

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

콘솔을 사용하여 기본 인증서를 교체하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.

4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 기본 SSL 인증서(Default SSL certificate)에 대해 다음 중 하나를 수행합니다.
   - 를 사용하여 AWS Certificate Manager인증서를 생성하거나 가져온 경우 [From ACM] 을 선택하고 인증서를 선택합니다.
   - IAM을 사용하여 인증서를 업로드한 경우 [IAM에서(From IAM)]을 선택하고 인증서를 선택합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 기본 인증서를 교체하려면 AWS CLI

--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 단원을 참조하세요.

콘솔을 사용하여 인증서 목록에 인증서를 추가하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 리스너의 확인란을 선택하고 작업, SNI용 SSL 인증서 추가를 선택합니다.
6. ACM 또는 IAM에서 이미 관리하는 인증서를 추가하려면 인증서의 확인란을 선택하고 아래 대기 중으로 포함을 선택합니다.
7. ACM 또는 IAM에서 관리하지 않는 인증서가 있는 경우 인증서 가져오기를 선택하고 양식을 작성한 다음 가져오기를 선택합니다.
8. 보류 중인 인증서 추가를 선택합니다.

를 사용하여 인증서 목록에 인증서를 추가하려면 AWS CLI

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 섹션을 참조하세요.

콘솔을 사용하여 인증서 목록에서 인증서를 제거하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 리스너의 확인란을 선택하고 작업, SNI용 SSL 인증서 추가를 선택합니다.
6. 인증서의 확인란을 선택하고 Remove(제거)를 선택합니다.
7. 확인 메시지가 나타나면 **`confirm`**을 입력하고 제거를 선택합니다.

를 사용하여 인증서 목록에서 인증서를 제거하려면 AWS CLI

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 단원을 참조하십시오.

콘솔을 사용하여 보안 정책을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 편집을 선택합니다.
6. Security policy(보안 정책)에서 보안 정책을 선택합니다.
7. 변경 사항 저장를 선택합니다.

를 사용하여 보안 정책을 업데이트하려면 AWS CLI

--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 단원을 참조하십시오.

콘솔을 사용하여 ALPN 정책을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 리스너 탭에서 프로토콜: 포트 열의 텍스트를 선택하여 리스너에 대한 세부 정보 페이지를 엽니다.
5. 편집을 선택합니다.
6. ALPN 정책의 경우 ALPN을 활성화할 정책을 선택하거나 [None]을 선택하여 ALPN을 비활성화합니다.
7. 변경 사항 저장를 선택합니다.

를 사용하여 ALPN 정책을 업데이트하려면 AWS CLI

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

Network Load Balancer의 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 창에서 [Load Balancers]를 클릭합니다.
3. 로드 밸런서의 확인란을 선택합니다.
4. 리스너 탭에서 리스너의 확인란을 선택한 다음 작업, 리스너 삭제를 선택합니다.
5. 확인 메시지가 나타나면 **`confirm`**을 입력하고 Delete(삭제)를 선택합니다.

를 사용하여 리스너를 삭제하려면 AWS CLI

delete-listener 명령을 사용하세요.

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 단원을 참조하세요.

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 단원을 참조하세요.

목차

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 Balancer의 대상 그룹은 다음 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 가상 사설 클라우드 (VPC) 에 있기 때문에 로드 밸런서와 대상 간의 트래픽은 패킷 수준에서 인증되므로 대상의 인증서가 유효하지 않더라도 공격이나 man-in-the-middle 스푸핑의 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
TCP	TCP	alb	HTTP | HTTPS
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.

`alb`

대상이 Application Load Balancer입니다.

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 모든 CIDR 블록을 사용하여 다음 대상을 대상 그룹에 등록할 수 있습니다.

- AWS IP 주소 및 포트로 주소를 지정할 수 있는 리소스 (예: 데이터베이스).
- 사이트 간 VPN 연결 AWS Direct Connect 또는 Site-to-Site VPN 연결을 AWS 통해 연결된 온프레미스 리소스.

대상 그룹에 대해 클라이언트 IP 보존이 비활성화되면 로드 밸런서는 Network Load Balancer IP 주소 및 고유 대상(IP 주소 및 포트)의 각 조합에 대해 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 추가하세요.

공유 Amazon VPC(참가자로)에서 Network Load Balancer를 시작할 때 사용자와 공유된 서브넷에서만 대상을 등록할 수 있습니다.

대상 유형이 `alb`인 경우 단일 Application Load Balancer를 대상으로 등록할 수 있습니다. 자세한 정보는 대상으로의 Application Load Balancer을 참조하세요.

Network Load Balancer는 `lambda` 대상 유형을 지원하지 않습니다. Application Load Balancer는 `lambda` 대상 유형을 지원하는 유일한 로드 밸런서입니다. 자세한 내용은 Application Load Balancer 사용 설명서의 Lambda 함수를 대상으로를 참조하세요.

Network Load Balancer에 등록된 인스턴스에 마이크로서비스가 있는 경우 로드 밸런서가 인터넷에 연결되어 있거나 인스턴스가 IP 주소로 등록되어 있지 않으면 로드 밸런서를 사용하여 이들 간에 통신을 제공할 수 없습니다. 자세한 정보는 대상에서 로드 밸런서로의 요청에서 연결 시간이 초과됨을 참조하세요.

라우팅 및 IP 주소 요청

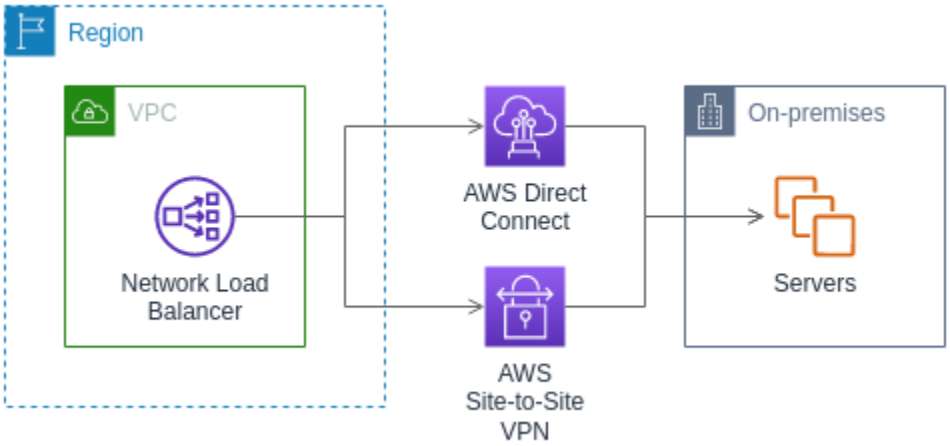
인스턴스 ID를 사용하여 대상을 지정하면 해당 인스턴스의 기본 네트워크 인터페이스에 지정된 기본 프라이빗 IP 주소를 사용하여 트래픽이 인스턴스로 라우팅됩니다. 로드 밸런서는 데이터 패킷의 목적지 IP 주소를 대상 인스턴스로 전송하기 전에 다시 작성합니다.

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 섹션을 참조하세요.

대상으로서의 온프레미스 리소스

대상 유형이 다음과 같은 경우, AWS Direct Connect 또는 Site-to-Site VPN 연결을 통해 연결된 온프레미스 리소스가 대상 역할을 할 수 있습니다. `ip`



온프레미스 리소스를 사용하는 경우 이러한 대상의 IP 주소는 여전히 다음 CIDR 블록 중 하나를 출처로 한 주소여야 합니다.

- 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)

에 대한 자세한 내용은 AWS Direct Connect무엇입니까를 참조하십시오. AWS Direct Connect

에 대한 AWS Site-to-Site VPN자세한 내용은 AWS Site-to-Site VPN무엇입니까를 참조하십시오.

IP 주소 유형

새 대상 그룹 생성 시 대상 그룹의 IP 주소 유형을 선택할 수 있습니다. 이는 대상과 통신하고 상태를 확인하는 데 사용되는 IP 버전을 제어합니다.

네트워크 로드 밸런서는 IPv4 및 IPv6 대상 그룹을 모두 지원합니다. 기본 선택값은 IPv4입니다. IPv6 대상 그룹은 듀얼스택 네트워크 로드 밸런서에만 연결할 수 있습니다.

고려 사항

- 하나의 대상 그룹 내의 모든 IP 주소는 IP 주소 유형이 동일해야 합니다. 예를 들어 IPv6 대상 그룹에 IPv4 대상을 등록할 수 없습니다.
- IPv6 대상 그룹은 TCP 또는 TLS 리스너가 있는 `dualstack` 로드 밸런서와 함께만 사용할 수 있습니다.
- IPv6 대상 그룹은 IP 및 인스턴스 유형 대상을 지원합니다.

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. 로드 밸런서는 등록 프로세스가 완료되고 구성된 임계값에 관계없이 대상이 첫 번째 초기 상태 확인을 통과하는 즉시 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 Scaling은 대상을 시작할 때 대상 그룹에 해당 대상을 등록합니다. 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서에서 로드 밸런서를 Auto Scaling 그룹에 연결을 참조하세요.

요구 사항 및 고려 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.
- IPv6 대상 그룹의 인스턴스 ID로 대상을 등록하는 경우 대상에 할당된 기본 IPv6 주소가 있어야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 IPv6 주소를 참조하십시오.
- 인스턴스 ID로 대상을 등록하는 경우 인스턴스는 Network Load Balancer와 동일한 Amazon VPC에 있어야 합니다. 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.
- 로드 밸런서는 활성화된 가용 영역 내에서만 트래픽을 대상으로 라우팅합니다. 활성화되지 않은 영역에 있는 대상은 사용되지 않습니다.
- 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 마세요. 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 그룹 속성이 지원됩니다. 대상 그룹 유형이 `instance` 또는 `ip`인 경우에만 이러한 속성을 수정할 수 있습니다. 대상 그룹 유형이 `alb`인 경우 이러한 속성은 항상 기본값을 사용합니다.

`deregistration_delay.timeout_seconds`

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

`deregistration_delay.connection_termination.enabled`

등록 취소 시간 제한이 끝날 때 로드 밸런서가 연결을 종료하는지 여부를 나타냅니다. 값은 `true` 또는 `false`입니다. 새 UDP/TCP_UDP 대상 그룹의 경우 기본값은 `true`입니다. 그렇지 않은 경우 기본값은 `false`입니다.

`load_balancing.cross_zone.enabled`

교차 영역 로드 밸런싱의 활성화 여부를 나타냅니다. 값은 `true`, `false` 또는 `use_load_balancer_configuration`입니다. 기본값은 `use_load_balancer_configuration`입니다.

`preserve_client_ip.enabled`

클라이언트 IP 보존이 활성화되었는지를 나타냅니다. 값은 `true` 또는 `false`입니다. 대상 그룹 유형이 IP 주소이고 대상 그룹 프로토콜이 TCP 또는 TLS이면 기본값이 비활성화됩니다. 그렇지 않으면, 기본값이 활성화됩니다. UDP 및 TCP_UDP 대상 그룹에 대해 클라이언트 IP 보존을 비활성화할 수 없습니다.

`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.

`target_group_health.dns_failover.minimum_healthy_targets.count`

정상 상태로 유지되어야 하는 최소 대상 수. 정상 대상 수가 이 값보다 낮으면 DNS에서 영역을 비정상으로 표시하여 트래픽이 정상 영역으로만 라우팅되도록 합니다. 가능한 값은 `off` 또는 1부터 최대 대상 수까지의 정수입니다. `off`, DNS 페일 어웨이가 비활성화되면 각 대상 그룹이 독립적으로 DNS 페일 오버에 기여합니다. 기본 값은 1입니다.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

정상 상태로 유지되어야 하는 대상의 최소 백분율. 정상 대상 백분율이 이 값보다 낮으면 DNS에서 영역을 비정상으로 표시하여 트래픽이 정상 영역으로만 라우팅되도록 합니다. 가능한 값은 `off`, 또는 1부터 100까지의 정수입니다. `off`, DNS 페일 어웨이가 비활성화되면 각 대상 그룹이 독립적으로 DNS 페일 오버에 기여합니다. 기본 값은 1입니다.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

정상 상태로 유지되어야 하는 최소 대상 수. 정상 대상 수가 이 값보다 낮으면 비정상 대상을 포함한 모든 대상으로 트래픽을 전송합니다. 범위는 1에서 최대 대상 수까지입니다. 기본 값은 1입니다.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

정상 상태로 유지되어야 하는 대상의 최소 백분율. 정상 대상의 백분율이 이 값보다 낮으면 비정상 대상을 포함한 모든 대상으로 트래픽을 전송합니다. 가능한 값은 `off` 또는 1부터 100까지의 정수입니다. 기본값은 `off`입니다.

`target_health_state.unhealthy.connection_termination.enabled`

로드 밸런서가 비정상 대상과의 연결을 종료하는지 여부를 나타냅니다. 값은 `true` 또는 `false`입니다. 기본값은 `true`입니다.

`target_health_state.unhealthy.draining_interval_seconds`

Elastic Load Balancing이 비정상 대상의 상태를 에서 로 변경하기 전에 `unhealthy.draining` 대기하는 `unhealthy` 시간입니다. 범위는 0-360000초입니다. 기본값은 0초입니다.

참고: 이 속성은 인 경우에만 구성할 수 있습니다. `target_health_state.unhealthy.connection_termination.enabled` `false`

클라이언트 IP 보존

네트워크 로드 밸런서는 요청을 백엔드 대상으로 라우팅할 때 클라이언트의 소스 IP 주소를 보존할 수 있습니다. 클라이언트 IP 보존을 비활성화하면 Network Load Balancer의 프라이빗 IP 주소가 모든 수신 트래픽에 대한 클라이언트 IP 주소가 됩니다.

기본적으로, 클라이언트 IP 보존은 UDP 및 TCP_UDP 프로토콜을 사용하는 인스턴스와 IP 유형 대상 그룹에 대해 활성화되며, 비활성화할 수 없습니다. 그러나 `preserve_client_ip.enabled` 대상 그룹 속성을 사용하여 TCP 및 TLS 대상 그룹에 대한 클라이언트 IP 보존을 활성화하거나 비활성화할 수 있습니다.

기본 설정

- 인스턴스 유형 대상 그룹: 활성화됨
- IP 유형 대상 그룹(UDP, TCP_UDP): 활성화됨
- IP 유형 대상 그룹(TCP, TLS): 비활성화됨

요구 사항 및 고려 사항

- 클라이언트 IP 보존이 활성화되면 대상은 Network Load Balancer와 동일한 VPC에 있어야 하며 트래픽은 Network Load Balancer에서 대상으로 직접 유입되어야 합니다.
- 대상이 Network Load Balancer와 동일한 Amazon VPC에 있더라도 Gateway Load Balancer 엔드포인트를 통해 Network Load Balancer와 대상(인스턴스 또는 IP) 사이의 트래픽을 검사하면 클라이언트 IP 보존이 지원되지 않습니다.
- 다음 인스턴스 유형, C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, T1은 클라이언트 IP 보존을 지원하지 않습니다. 이러한 인스턴스 유형은 클라이언트 IP 보존이 비활성화된 IP 주소로 등록하는 것이 좋습니다.
- 클라이언트 IP 보존은 인바운드 트래픽의 영향을 받지 않습니다. AWS PrivateLink AWS PrivateLink 트래픽의 소스 IP는 항상 Network Load Balancer의 사설 IP 주소입니다.
- 대상 그룹에 AWS PrivateLink ENI나 다른 Network Load Balancer ENI가 포함된 경우에는 클라이언트 IP 보존이 지원되지 않습니다. 이로 인해 해당 대상과의 통신이 중단됩니다.
- 클라이언트 IP 보존은 IPv6에서 IPv4로 변환된 트래픽에 영향을 주지 않습니다. 이 트래픽 유형의 소스 IP는 항상 Network Load Balancer의 프라이빗 IP 주소입니다.
- Application Load Balancer 유형별로 대상을 지정하면 수신되는 모든 트래픽의 클라이언트 IP가 Network Load Balancer에 의해 보존되고 Application Load Balancer에 전송됩니다. 그런 다음 Application Load Balancer는 클라이언트 IP를 대상으로 보내기 전에 `X-Forwarded-For` 요청 헤더에 첨부합니다.
- 클라이언트 IP 보존의 변경 사항은 새 TCP 연결에만 적용됩니다.
- 헤어피닝이라고도 하는 NAT 루프백은 클라이언트 IP 보존이 활성화된 경우 지원되지 않습니다. 사용하도록 설정한 경우 대상에서 관찰된 소켓 재사용과 관련된 TCP/IP 연결 제한이 발생할 수 있습니다. 이러한 연결 제한은 여러 로드 밸런서 노드에 동시에 연결할 때 클라이언트 또는 클라이언트 앞에 있는 NAT 디바이스가 동일한 소스 IP 주소와 소스 포트를 사용하는 경우에 발생할 수 있습니다. 로드 밸런서가 이러한 연결을 동일한 대상으로 라우팅하는 경우 이 연결은 동일한 소스 소켓에서 온 것처럼 대상에 나타나므로 연결 오류가 발생합니다. 이 경우 (연결이 실패하면) 클라이언트가 다시 시도하거나 (연결이 중단되면) 다시 연결할 수 있습니다. 소스 휘발성 포트 수를 늘리거나 로드 밸런

서에 대한 대상 수를 늘려 이러한 유형의 연결 오류를 줄일 수 있습니다. 클라이언트 IP 보존 혹은 교차 영역 로드 밸런싱을 비활성화하여 이러한 유형의 연결 오류를 방지할 수 있습니다.

- 클라이언트 IP 보존이 비활성화된 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 횟수가 이를 초과할 경우, 포트 할당 오류가 발생할 가능성이 증가하고, 새 연결 구축에 실패할 수 있습니다. 포트 할당 오류는 `PortAllocationErrorCount` 지표를 사용하여 추적할 수 있습니다. 포트 할당 오류를 해결하려면 대상 그룹에 더 많은 대상을 추가하세요. 자세한 정보는 CloudWatch 네트워크 로드 밸런서의 지표을 참조하세요.

콘솔을 사용하여 클라이언트 IP 보존을 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 클라이언트 IP 보존을 활성화하려면 Preserve client IP addresses(클라이언트 IP 주소 보존)를 선택합니다. 클라이언트 IP 보존을 비활성화하려면 Preserve client IP addresses(클라이언트 IP 주소 보존)를 선택 취소합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 클라이언트 IP 보존을 활성화 또는 비활성화하려면 AWS CLI

`preserve_client_ip.enabled` 속성과 함께 modify-target-group-attributes 명령을 사용합니다.

예를 들어, 다음 명령을 사용하여 클라이언트 IP 보존을 비활성화합니다.

```
aws elbv2 modify-target-group-attributes --attributes
 Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

다음 예와 유사하게 출력되어야 합니다.

```
{
    "Attributes": [
      {
        "Key": "proxy_protocol_v2.enabled",
        "Value": "false"
      },
```

```
      {
        "Key": "preserve_client_ip.enabled",
        "Value": "false"
      },
      {
        "Key": "deregistration_delay.timeout_seconds",
        "Value": "300"
      }
    ]
}
```

등록 취소 지연

대상 등록을 취소하면 로드 밸런서가 대상에 대한 새 연결 생성을 중지합니다. 로드 밸런서는 Connection Draining을 사용하여 기존 연결에서 인플라이트 트래픽이 완료되도록합니다. 등록 취소된 대상이 정상 상태를 유지하고 기존 연결이 유휴 상태가 아닌 경우 로드 밸런서는 트래픽을 대상으로 계속 전송할 수 있습니다. 기존 연결을 닫으려면 연결 종료에 대한 대상 그룹 속성을 활성화하거나, 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 업데이트하세요. 요청이 완료될 수 있도록 120초 이상의 값을 지정하는 것이 좋습니다.

연결 종료에 대해 대상 그룹 속성을 활성화하면 등록 취소된 대상에 대한 연결이 등록 취소 시간 제한이 끝나는 즉시 닫힙니다.

콘솔을 사용하여 등록 취소 속성을 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 등록 취소 시간 제한을 변경하려면 등록 취소 지연에 새 값을 입력합니다. 대상을 등록 취소한 후 기존 연결이 닫히게 하려면 Terminate connections on deregistration(등록 취소 시 연결 종료)을 선택합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 등록 취소 속성을 업데이트하려면 AWS CLI

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. TCP리스너와 함께 로드 밸런서는 TCP 데이터에 프록시 프로토콜 헤더를 추가합니다. 로드 밸런서는 클라이언트에서 전송한 모든 수신 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 외부에 대상에 대한 다른 네트워크 경로가 있는 경우 첫 번째 프록시 프로토콜 헤더가 Network Load Balancer의 프록시 프로토콜 헤더가 아닐 수 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.

> **Note**
>
> TLS 리스너는 클라이언트나 다른 프록시가 전송한 프록시 프로토콜 헤더를 통한 수신 연결을 지원하지 않습니다.

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)
	변수(값 길이 -1)	엔드포인트의 ID

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

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 참조하세요.

콘솔을 사용하여 프록시 프로토콜 v2를 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 속성 편집(Edit attributes) 페이지에서 프록시 프로토콜 v2(Proxy protocol v2)를 선택합니다.
6. [Save changes]를 선택합니다.

를 사용하여 프록시 프로토콜 v2를 활성화하려면 AWS CLI

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.
- 대상 그룹에 대해 stickiness 속성이 켜져 있는 경우 수동 상태 확인이 지원되지 않습니다. 자세한 내용은 대상 그룹의 건강 검진을 참조하십시오.
- 스티키 세션은 TLS 리스너에 대해서는 지원되지 않습니다.

콘솔을 사용하여 고정 세션을 활성화하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. Target selection configuration(대상 선택 구성)에서 Stickiness(고정)를 켭니다.
6. 변경 사항 저장를 선택합니다.

고정 세션을 활성화하려면 다음을 사용하십시오. AWS CLI

`stickiness.enabled` 속성과 함께 modify-target-group-attributes 명령을 사용합니다.

Network Load Balancer에 대한 대상 그룹 만들기

Network Load Balancer의 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 정보는 리스너 규칙을 참조하세요. 여러 리스너에서 동일한 대상 그룹을 지정할 수 있지만, 이러한 리스너는 동일한 Network Load Balancer에 속해야 합니다. 대상 그룹을 로드 밸런서와 함께 사용하려면 대상 그룹이 다른 로드 밸런서용으로 리스너에서 사용되고 있지 않은지 확인해야 합니다.

언제든지 대상 그룹에서 대상을 추가하거나 삭제할 수 있습니다. 자세한 정보는 대상 그룹에 대상 등록을 참조하세요. 대상 그룹에 대한 상태 확인 설정을 변경할 수도 있습니다. 자세한 정보는 대상 그룹의 상태 확인 설정 수정을 참조하세요.

콘솔을 사용하여 대상 그룹을 생성하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 대상 그룹을 선택합니다.
3. 대상 그룹 생성을 선택합니다.
4. 기본 구성 창에서 다음을 수행합니다.

    a. Choose a target type(대상 유형 선택)에서 인스턴스 ID로 대상을 등록하려면 Instances(인스턴스)를 선택하고, IP 주소로 대상을 등록하려면 IP addresses(IP 주소)를 선택하고, Application Load Balancer를 대상으로 등록하려면 Application Load Balancer를 선택합니다.

    b. 대상 그룹 이름에 대상 그룹의 이름을 입력합니다. 이 이름은 계정당 리전당 고유해야 하고, 최대 32자여야 하며, 알파벳 문자 또는 하이픈만 포함해야 하고, 하이픈으로 시작하거나 끝나지 않아야 합니다.

    c. 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.

d. (선택 사항) 포트에서 필요에 따라 기본값을 변경합니다.

e. IP 주소 유형에서 IPv4 또는 IPv6를 선택합니다. 이 옵션은 대상 유형이 인스턴스 또는 IP 주소이고 프로토콜이 TCP 또는 TLS인 경우에 사용할 수 있습니다.

   IPv6 대상 그룹은 듀얼스택 로드 밸런서와 연결해야 합니다. 대상 그룹의 모든 대상은 동일한 IP 주소 유형을 가져야 합니다. 대상 그룹을 생성한 후에는 대상 그룹의 IP 주소 유형을 변경할 수 없습니다.

f. VPC에서 등록하려는 대상이 있는 Virtual Private Cloud(VPC)를 선택합니다.

5. 상태 확인 창에서 필요에 따라 기본 설정을 수정합니다. 고급 상태 확인 설정(Advanced health check settings)의 경우 상태 확인 포트, 개수, 시간 초과, 간격을 선택하고 성공 코드를 지정합니다. 상태 확인이 비정상 임계값 수를 연속으로 초과하는 경우 로드 밸런서는 대상을 서비스 중단 상태로 만듭니다. 상태 확인이 정상 임계값 수를 연속으로 초과하는 경우 로드 밸런서는 대상을 다시 서비스 상태로 전환합니다. 자세한 정보는 대상 그룹에 대한 상태 확인을 참조하세요.
6. (선택 사항) 태그를 추가하려면 태그를 확장하고 태그 추가를 선택하여 태그 키와 태그 값을 입력합니다.
7. 다음을 선택합니다.
8. 대상 등록 페이지에서 다음과 같이 하나 이상의 대상을 추가합니다.
   - 대상 유형이 인스턴스인 경우 인스턴스를 선택하고 포트를 입력한 다음 아래에 보류 중인 것으로 포함을 선택합니다.

     참고: IPv6 대상 그룹에 등록하려면 인스턴스에 할당된 기본 IPv6 주소가 있어야 합니다.
   - 대상 유형이 IP 주소인 경우 네트워크를 선택하고 IP 주소와 포트를 입력한 다음 아래에 보류 중인 것으로 포함을 선택합니다.
9. 대상 그룹 생성을 선택합니다.

를 사용하여 대상 그룹을 만들려면 AWS CLI

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 정보는 교차 영역 로드 밸런싱을 참조하세요.

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. UDP 트래픽 및 고정성이 설정된 대상 그룹에는 패시브 상태 확인이 지원되지 않습니다. 자세한 내용은 고정 세션을 참조하십시오.

대상이 비정상 상태이면 비정상 대상이 로드 밸런서의 페일 오픈을 트리거하지 않는 한 로드 밸런서가 대상과 관련된 클라이언트 연결에서 수신된 패킷에 대해 TCP RST를 보냅니다.

대상 그룹이 활성화 가용 영역에서 정상적인 대상이 없는 경우 DNS에서 해당 서브넷의 IP 주소를 제거하여 해당 가용 영역의 대상으로 요청을 라우팅할 수 없습니다. 모든 대상이 활성화된 모든 가용 영역에서 동시에 상태 확인에 실패하면 로드 밸런서가 열리지 않습니다. 대상 그룹이 비어 있는 경우 네트워크 로드 밸런서도 열리지 않습니다. 오류 시 열림이 적용되면 상태에 관계없이 활성화된 모든 가용 영역의 모든 대상에 대한 트래픽이 허용됩니다.

대상 그룹이 HTTPS 상태 확인으로 구성된 경우, 등록된 대상은 TLS 1.3만 지원하는 경우 상태 확인에 실패합니다. 이러한 대상은 TLS 1.2와 같은 이전 버전의 TLS를 지원해야 합니다.

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 추가하는 경우 리스너 연결 테스트를 수행합니다. TLS 종료 시 TCP 연결도 종료되므로 로드 밸런서와 대상 간에 새로운 TCP 연결이 설정됩니다. 따라서 이 테스트의 TCP 연결이 로드 밸런서에서 TLS 수신기에 등록된 대상으로 전송되는 것을 볼 수 있습니다. 이러한 TCP 연결에는 Network Load Balancer의 소스 IP 주소가 있고 연결에 데이터 패킷이 포함되어 있지 않으므로 이러한 연결을 식별할 수 있습니다.

UDP 서비스의 경우, 대상 그룹에서 비 UDP 상태 확인을 사용하여 대상 가용성을 테스트할 수 있습니다. 사용 가능한 모든 상태 확인(TCP, HTTP 또는 HTTPS) 및 대상의 포트를 사용하여 UDP 서비스의 가용성을 확인할 수 있습니다. 상태 확인을 수신하는 서비스가 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 확인에 실패합니다.

상태 확인 설정

다음 설정을 사용하여 대상 그룹에서 대상에 대한 능동 상태 확인을 구성합니다. 상태 확인이 연속 실패 UnhealthyThreshold횟수를 초과할 경우 로드 밸런서는 대상을 서비스 중단시킵니다. 상태 확인의 연속 성공 HealthyThreshold횟수를 초과하면 로드 밸런서는 대상을 다시 서비스 상태로 전환합니다.

설정	설명	기본값
HealthCheck프로토콜	대상에 대한 상태 확인을 수행할 때 로드 밸런서가 사용하는 프로토콜입니다. HTTP, HTTPS, TCP 프로토콜이 여기에 해당됩니다. TCP 프로토콜이 기본 설정값입니다. 대상 유형이 alb인 경우, 지원되는 상태 확인 프로토콜은 HTTP와 HTTPS입니다.	TCP
HealthCheck포트	대상에 대한 상태 확인을 수행할 때 로드 밸런서가 사용하는 포트입니다. 각 대상이 로드 밸런서에서 트래픽을 수신하는 포트를 사용하도록 기본 설정되어 있습니다.	각 대상이 로드 밸런서에서 트래픽을 수신하는 포트입니다.
HealthCheck경로	[HTTP/HTTPS 상태 확인] 상태 확인 대상의 대상이 되는 상태 확인 경로입니다. 기본값은 /입니다.	/
HealthCheckTimeoutSeconds	상태 확인 실패를 의미하는 대상으로부터 응답이 없는 기간(초 단위)입니다. 범위는 2~120초입니다. 기본값은 HTTP의 경우 6초이고 TCP 및 HTTPS 상태 확인의 경우 10초입니다.	HTTP 상태 확인의 경우 6초이고 TCP 및 HTTPS 상태 확인의 경우 10초입니다.
HealthCheckIntervalSeconds	개별 인스턴스의 상태 확인 간의 대략적인 간격(초 단위)입니다. 범위는 5~300초입니다. 기본값은 30초입니다.	30초

설정	설명	기본값
	Important Network Load Balancer에 대한 상태 확인이 배포되고 합의 메커니즘을 사용하여 대상 상태를 확인합니다. 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.	
HealthyThreshold개수	비정상 상태의 대상을 정상으로 간주하기까지 필요한 연속적인 상태 확인 성공 횟수입니다. 범위는 2~10회입니다. 기본값은 5입니다.	5
UnhealthyThreshold카운트	대상을 비정상 상태로 간주하기까지 필요한 연속적인 상태 확인 실패 횟수입니다. 범위는 2~10회입니다. 기본값은 2입니다.	2
Matcher	[HTTP/HTTPS 상태 확인] 대상으로부터 응답 성공을 확인할 때 사용하는 HTTP 코드입니다. 범위는 200~599회입니다. 기본값은 200-399입니다.	200-399

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 실패했거나 대상이 중지된 상태입니다. 관련 사유 코드: Target.FailedHealthChecks
draining	대상이 등록 취소되고 있으며 Connection Draining이 진행 중입니다. 관련 사유 코드: Target.DeregistrationInProgress
unhealthy.draining	대상이 상태 점검에 응답하지 않았거나 상태 점검에 실패하여 유예 기간이 시작됩니다. 대상은 기존 연결을 지원하며 이 유예 기간 동안에는 새 연결을 수락하지 않습니다. 관련 사유 코드: Target.FailedHealthChecks
unavailable	대상 상태를 확인할 수 없습니다. 관련 사유 코드: Elb.InternalError
unused	대상이 대상 그룹에 등록되지 않았거나, 대상 그룹이 수신기 규칙에 사용되지 않거나, 대상이 활성화되지 않은 가용 영역에 있습니다. 관련 사유 코드: Target.NotRegistered | Target.NotInUse | Target.InvalidState | Target.IpUnusable

상태 확인 사유 코드

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

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

콘솔을 사용하여 대상의 상태를 확인하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. Details(세부 정보) 창에는 총 대상 수와 각 상태의 대상 수가 표시됩니다.
5. Targets(대상) 탭에서 Health status(상태) 열은 각 대상의 상태를 나타냅니다.
6. 대상의 상태가 `Healthy` 이외의 값인 경우에는 Health status details(상태 세부 정보) 열에 자세한 정보가 있습니다.

를 사용하여 대상의 상태를 확인하려면 AWS CLI

describe-target-health 명령을 사용합니다. 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 Lambda 함수를 트리거하여 비정상 대상에 대한 세부 정보를 전송합니다. step-by-step 지침은 다음 블로그 게시물을 참조하십시오. 로드 밸런서의 비정상 대상 식별.

대상 그룹의 상태 확인 설정 수정

대상 그룹에 대한 상태 확인 설정을 언제든지 변경할 수도 있습니다.

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 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 상태 확인 탭에서 편집을 선택합니다.
5. 상태 확인 설정 편집(Edit health check settings) 페이지에서 필요에 따라 설정을 수정한 다음 변경 사항 저장(Save changes)을 선택합니다.

를 사용하여 대상 그룹의 상태 점검 설정을 수정하려면 AWS CLI

modify-target-group 명령을 사용합니다.

대상 그룹에 대한 교차 영역 로드 밸런싱

로드 밸런서의 노드는 클라이언트로부터 요청을 가져와서 등록된 대상에 분산합니다. 교차 영역 로드 밸런싱을 켜면 각 로드 밸런서 노드가 등록된 모든 가용 영역에 있는 등록된 대상 간에 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 끄면 각 로드 밸런서 노드가 해당 가용 영역에 있는 등록된 대상 간에만 트래픽을 분산합니다. 지역보다 영역 장애 도메인을 선호하는 경우, 정상 영역이 비정상 영역의 영향을 받지 않도록 하거나 전반적인 지연 시간을 개선하는 데 사용할 수 있습니다.

Network Load Balancer를 사용하면 로드 밸런서 수준에서 기본적으로 교차 영역 로드 밸런싱이 해제되지만, 언제든지 켤 수 있습니다. 대상 그룹의 경우 기본적으로 로드 밸런서 설정을 사용하지만 대상 그룹 수준에서 교차 영역 로드 밸런싱을 명시적으로 켜거나 꺼서 기본값을 재정의할 수 있습니다.

고려 사항

- Network Load Balancer에 대해 영역 간 로드 밸런싱을 활성화하면 EC2 데이터 전송 요금이 적용됩니다. 자세한 내용은 데이터 내보내기 사용 설명서의 데이터 전송 요금 이해를 참조하십시오.AWS
- 대상 그룹 설정은 대상 그룹의 로드 밸런싱 동작을 결정합니다. 예를 들어, 교차 영역 로드 밸런싱이 로드 밸런서 수준에서 활성화되고 대상 그룹 수준에서 비활성화되어 있다면 대상 그룹으로 전송되는 트래픽은 가용 영역 간에 라우팅되지 않습니다.
- 교차 영역 로드 밸런싱이 꺼져 있다면 각 영역에서 관련 워크로드를 처리할 수 있을 만큼 충분한 대상 용량이 각 로드 밸런서 가용 영역에 있는지 확인해야 합니다.
- 교차 영역 로드 밸런싱이 꺼져 있다면 모든 대상 그룹이 동일한 가용 영역에 있어야 합니다. 빈 가용 영역은 비정상인 것으로 간주됩니다.

로드 밸런서의 교차 영역 로드 밸런싱 수정

언제든지 로드 밸런서 수준에서 교차 영역 로드 밸런싱을 켜거나 끌 수 있습니다.

콘솔을 사용하여 로드 밸런서의 교차 영역 로드 밸런싱을 수정하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. 로드 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.

4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. Edit load balancer attributes(로드 밸런서 특성 편집) 페이지에서 Cross-zone load balancing(교차 영역 로드 밸런싱)을 켜거나 끕니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 로드 밸런서의 영역 간 부하 분산을 수정하려면 AWS CLI

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

대상 그룹의 교차 영역 로드 밸런싱 수정

대상 그룹 수준의 교차 영역 로드 밸런싱 설정은 로드 밸런서 수준의 설정을 재정의합니다.

대상 그룹 유형이 `instance` 또는 `ip`인 경우 대상 그룹 수준에서 교차 영역 로드 밸런싱을 켜거나 끌 수 있습니다. 대상 그룹 유형이 `alb`인 경우 대상 그룹은 항상 로드 밸런서로부터 교차 영역 로드 밸런싱 설정을 상속합니다.

콘솔을 사용하여 대상 그룹의 교차 영역 로드 밸런싱을 수정하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing(로드 밸런싱)에서 Target Groups(대상 그룹)을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. Edit target group attributes(대상 그룹 속성 편집) 페이지에서 Cross-zone load balancing(교차 영역 로드 밸런싱)에 대해 On(사용)을 선택합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 대상 그룹의 영역 간 부하 분산을 수정하려면 AWS CLI

`load_balancing.cross_zone.enabled` 속성과 함께 modify-target-group-attributes 명령을 사용합니다.

대상 그룹 상태

기본적으로 대상 그룹은 그룹에 정상 대상이 하나 이상 있는 한 정상 그룹으로 간주됩니다. 플릿이 크면 트래픽을 처리하는 정상 대상이 하나만 있는 것으로는 충분하지 않습니다. 대신, 정상이어야 하는

대상의 최소 개수 또는 백분율을 지정하고 정상 대상이 지정된 임계값 아래로 떨어질 경우 로드 밸런서가 취하는 조치를 지정할 수 있습니다. 이는 가용성을 높입니다.

비정상 상태 작업

다음 작업에 대해 정상 임계값을 구성할 수도 있습니다.

- DNS 장애 조치 - 영역의 정상 대상이 임계값 아래로 떨어지면 DNS에서 영역에 대한 로드 밸런서 노드의 IP 주소를 비정상으로 표시합니다. 따라서 클라이언트가 로드 밸런서 DNS 이름을 확인하면 트래픽이 정상 영역으로만 라우팅됩니다.
- 라우팅 장애 조치 - 영역의 정상 대상이 임계값 아래로 떨어지면 로드 밸런서는 비정상 대상을 포함하여 로드 밸런서 노드에서 사용할 수 있는 모든 대상으로 트래픽을 보냅니다. 이렇게 하면 특히 대상이 일시적으로 상태 확인을 통과하지 못하는 경우 클라이언트 연결이 성공할 가능성이 높아지고 정상 대상에 과부하가 걸릴 위험이 줄어듭니다.

요구 사항 및 고려 사항

- 작업에 대해 두 가지 유형의 임계값(개수 및 백분율)을 모두 지정하는 경우 로드 밸런서는 두 임계값 중 하나가 위반될 때 조치를 취합니다.
- 두 작업 모두에 대해 임계값을 지정하는 경우 DNS 장애 조치의 임계값은 라우팅 장애 조치 임계값보다 크거나 같아야 합니다. 그래야 라우팅 장애 조치 시 또는 라우팅 장애 조치 전에 DNS 장애 조치가 발생할 수 있습니다.
- 임계값을 백분율로 지정하면 대상 그룹에 등록된 총 대상 수를 기준으로 값이 동적으로 계산됩니다.
- 총 대상 수는 교차 영역 로드 밸런싱의 활성화 여부를 기반으로 합니다. 교차 영역 로드 밸런싱이 해제된 경우 각 노드는 자체 영역의 대상에만 트래픽을 전송합니다. 즉, 임계값은 활성화된 각 영역의 대상 수에 개별적으로 적용됩니다. 교차 영역 로드 밸런싱이 해제된 경우 각 노드는 활성화된 모든 영역의 모든 대상에 트래픽을 전송합니다. 즉, 지정된 임계값은 활성화된 모든 영역의 총 대상 수에 적용됩니다. 자세한 정보는 교차 영역 로드 밸런싱을 참조하세요.
- DNS 장애 조치를 사용하면 로드 밸런서의 DNS 호스트 이름에서 비정상 영역의 IP 주소를 제거합니다. 하지만 DNS 레코드의 time-to-live (TTL) 이 만료될 때까지 (60초) 로컬 클라이언트 DNS 캐시에 이러한 IP 주소가 포함될 수 있습니다.
- DNS 장애 조치가 발생하면 로드 밸런서와 연결된 모든 대상 그룹에 영향을 줍니다. 나머지 영역에 이러한 추가 트래픽을 처리할 수 있는 충분한 용량이 있는지 확인하세요. 특히 교차 영역 로드 밸런싱이 꺼져 있는 경우에는 더욱 확인하세요.
- DNS 장애 조치를 사용하면 모든 로드 밸런서 영역이 비정상인 것으로 간주되면 로드 밸런서는 비정상 영역을 포함한 모든 영역으로 트래픽을 전송합니다.

- DNS 장애 조치로 이어질 수 있는 정상 대상이 충분한지 여부와는 다른 요인(예: 영역 상태)이 있습니다.

예

다음 예는 대상 그룹 상태 설정을 적용하는 방법을 보여줍니다.

시나리오

- 두 개의 가용 영역 A와 B를 지원하는 로드 밸런서
- 각 가용 영역에는 10개의 등록된 대상이 포함됨
- 대상 그룹에는 다음과 같은 대상 그룹 상태 설정이 있습니다.
  - DNS 장애 조치 - 50%
  - 라우팅 장애 조치 - 50%
- 가용 영역 B에서 6개의 대상 장애

교차 영역 로드 밸런싱이 꺼져 있는 경우

- 각 가용 영역에 있는 로드 밸런서 노드는 가용 영역에 있는 10개 대상에만 트래픽을 전송할 수 있습니다.
- 가용 영역 A에는 10개의 정상 대상이 있으며, 이는 정상 대상의 필수 백분율을 충족합니다. 로드 밸런서는 10개의 정상 대상 간에 트래픽을 계속 분산합니다.
- 가용 영역 B에는 정상 대상이 4개뿐이며, 이는 가용 영역 B의 로드 밸런서 노드 대상의 40%에 해당합니다. 이는 정상 대상의 필수 백분율보다 적으므로 로드 밸런서는 다음 작업을 수행합니다.
  - DNS 장애 조치 - 가용 영역 B가 DNS에서 비정상으로 표시됩니다. 클라이언트가 가용 영역 B의 로드 밸런서 노드에 대한 로드 밸런서 이름을 확인할 수 없고 가용 영역 A가 정상이므로 클라이언트는 가용 영역 A에 새 연결을 보냅니다.
  - 라우팅 장애 조치 - 새 연결이 가용 영역 B로 명시적으로 전송되면 로드 밸런서는 비정상 대상을 포함하여 가용 영역 B의 모든 대상으로 트래픽을 분산합니다. 이는 나머지 정상 대상 간의 중단을 방지할 수 있습니다.

교차 영역 로드 밸런싱이 켜져 있는 경우

- 각 로드 밸런서 노드는 두 가용 영역에서 등록된 20개 대상 모두에 트래픽을 전송할 수 있습니다.

- 가용 영역 A에는 10개의 정상 대상이 있고 가용 영역 B에는 4개의 정상 대상이 있으므로 총 14개의 정상 대상이 있습니다. 이는 두 가용 영역 모두에 있는 로드 밸런서 노드에 대한 대상의 70%이며, 정상 대상 중 필수 백분율을 충족합니다.
- 로드 밸런서는 두 가용 영역 모두에서 14개의 정상 대상 간에 트래픽을 계속 분산합니다.

대상 그룹 상태 설정 수정

다음과 같이 대상 그룹에 대한 대상 그룹 상태 설정을 변경할 수도 있습니다.

콘솔을 사용하여 대상 그룹의 상태 설정을 변경하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 교차 영역 로드 밸런싱이 켜져 있는지 또는 꺼져 있는지 확인합니다. 필요에 따라 이 설정을 업데이트하여 영역에 장애가 발생할 경우 추가 트래픽을 처리할 수 있는 충분한 용량이 있는지 확인하세요.
6. Target group health requirements(대상 그룹 상태 요구 사항)을 확장합니다.
7. Configuration type(구성 유형)의 경우 두 작업에 대해 동일한 임계값을 설정하는 Unified configuration(통합 구성)을 선택하는 것이 좋습니다.
8. Healthy state requirements(정상 상태 요구 사항)의 경우 다음 중 하나를 실시합니다.
   - Minimum healthy target count(최소 정상 대상 개수)를 선택한 다음 1부터 대상 그룹의 최대 대상 수까지의 숫자를 입력합니다.
   - Minimum healthy target percentage(최소 정상 대상 백분율)을 선택한 다음 1부터 100까지의 숫자를 입력합니다.
9. 변경 사항 저장를 선택합니다.

를 사용하여 대상 그룹 상태 설정을 수정하려면 AWS CLI

modify-target-group-attributes 명령을 사용합니다. 다음 예에서는 두 비정상 상태 동작 모두에 대한 정상 임계값을 50%로 설정합니다.

```
aws elbv2 modify-target-group-attributes \
```

```
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

비정상 대상에 대한 연결 종료

연결 종료는 기본적으로 활성화됩니다. Network Load Balancer의 대상이 구성된 상태 점검에 실패하고 비정상으로 간주되면 로드 밸런서는 설정된 연결을 종료하고 대상으로의 새 연결 라우팅을 중단합니다. 연결 종료가 비활성화된 상태에서도 대상은 여전히 비정상으로 간주되어 새 연결을 수신하지 못하지만 설정된 연결은 활성 상태로 유지되므로 정상적으로 닫힐 수 있습니다.

비정상 대상에 대한 연결 종료는 각 대상 그룹에 대해 개별적으로 설정할 수 있습니다.

콘솔을 사용하여 연결 종료 설정 수정

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 대상: 비정상 상태 관리 아래에서 대상이 비정상 상태가 되면 연결 종료의 활성화 또는 비활성화를 선택합니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 연결 종료 설정을 수정하려면 AWS CLI

`target_health_state.unhealthy.connection_termination.enabled` 속성과 함께 modify-target-group-attributes 명령을 사용합니다.

비정상 배수 간격

> **Important**
>
> 비정상 드레인 간격을 활성화하려면 먼저 연결 종료를 비활성화해야 합니다.

이 unhealthy.draining 상태의 대상은 비정상으로 간주되어 새 연결을 수신하지 않지만 구성된 간격 동안 설정된 연결을 유지합니다. 비정상 연결 간격에 따라 대상이 unhealthy.draining 상태가 되기 전의 상태로 유지되는 시간이 결정됩니다. unhealthy 비정상 연결 간격 동안 대상이 상태 확인을 통과하면 대상이 다시 상태가 됩니다healthy. 등록 취소가 트리거되면 대상 상태가 draining 되고 등록 취소 지연 제한 시간이 시작됩니다.

비정상 드레이닝 간격은 각 대상 그룹에 대해 개별적으로 설정할 수 있습니다.

콘솔을 사용하여 비정상 배수 간격을 수정하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 대상 비정상 상태 관리에서 대상이 비정상이 될 때 연결 종료가 꺼져 있는지 확인합니다.
6. 비정상 드레인 간격에 값을 입력합니다.
7. 변경 사항 저장를 선택합니다.

비정상 배수 간격을 수정하려면 다음을 사용하여 비정상 배수 간격을 수정하십시오. AWS CLI

target_health_state.unhealthy.draining_interval_seconds 속성과 함께 modify-target-group-attributes 명령을 사용합니다.

로드 밸런서에 대한 Route 53 DNS 장애 조치 사용

Route 53을 사용하여 로드 밸런서에 DNS 요청을 라우팅하는 경우, Route 53을 사용하여 로드 밸런서에 대한 DNS 장애 조치를 구성할 수도 있습니다. 장애 조치 구성에서 Route 53은 로드 밸런서에 대한 대상 그룹 대상의 상태를 확인하여 가용 여부를 결정합니다. 로드 밸런서에 정상 상태의 대상이 등록되어 있지 않거나 로드 밸런서 자체가 정상 상태가 아니면 Route 53은 정상 상태 로드 밸런서나 Amazon S3의 정적 웹 사이트 같은 또 다른 가용 리소스로 트래픽을 라우팅합니다.

예를 들어 www.example.com에 대한 웹 사이트가 있고 서로 다른 리전에 상주하는 두 개의 로드 밸런서에서 중복 인스턴스를 실행하고 싶다고 가정합시다. 한 리전의 로드 밸런서에 트래픽을 주로 라우팅하고 다른 리전의 로드 밸런서는 장애 시 백업으로 사용하고 싶을 수 있습니다. DNS 장애 조치를 구성하면 주 및 보조(백업) 로드 밸런서를 지정할 수 있습니다. Route 53은 주 로드 밸런서가 사용 가능한 상태일 때는 여기로 트래픽을 라우팅하고, 그렇지 않으면 보조 로드 밸런서로 라우팅합니다.

대상 상태 평가 사용

- Network Load Balancer 별칭 레코드에서 대상 상태 평가가 `Yes`로 설정된 경우 Route 53은 `alias target` 값으로 지정된 리소스의 상태를 평가합니다. Network Load Balancer 경우 Route 53은 로드 밸런서와 연결된 대상 그룹 상태 확인을 사용합니다.
- Network Load Balancer 밸런서의 모든 타겟 그룹이 정상일 때 Route 53은 별칭 레코드를 정상으로 표시합니다. 대상 그룹에 정상 대상이 하나 이상 있으면 대상 그룹 상태 검사가 통과됩니다. 그러면 Route 53은 라우팅 정책에 따라 레코드를 반환합니다. 장애 조치 라우팅 정책이 사용되는 경우 Route 53는 기본 레코드를 반환합니다.
- Network Load Balancer 밸런서의 대상 그룹 중 하나라도 비정상이면 별칭 레코드가 Route 53 상태 확인(오류 시 열림)에 실패합니다. 대상 상태 평가를 사용하는 경우 장애 조치 라우팅 정책이 실패할 수 있습니다.
- Network Load Balancer의 모든 대상 그룹이 비어 있는 경우(대상 없음), Route 53은 레코드를 비정상(오류 시 열림)으로 간주합니다. 대상 상태 평가를 사용하는 경우 장애 조치 라우팅 정책이 실패할 수 있습니다.

자세한 내용은 Amazon Route 53 개발자 안내서의의 DNS 장애 조치 구성을 참조하세요.

대상 그룹에 대상 등록

대상이 요청을 처리할 준비가 되면 하나 이상의 대상 그룹에 대상을 등록합니다. 대상 그룹의 대상 유형에 따라 대상을 등록하는 방법이 결정됩니다. 예를 들어 인스턴스 ID, IP 주소 또는 Application Load Balancer를 등록할 수 있습니다. Network Load Balancer는 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 단원을 참조하세요.

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 Connection Draining이라고 합니다. Connection Draining이 진행 중인 동안 대상의 상태는

`draining`입니다. 등록 취소가 완료된 후 대상의 상태는 `unused`로 변경됩니다. 자세한 내용은 등록 취소 지연 단원을 참조하세요.

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 오토 스케일링 사용 설명서에서 로드 밸런서를 오토 스케일링 그룹에 연결을 참조하세요.

대상 보안 그룹

대상 그룹에 대상을 추가하기 전에 Network Load Balancer로부터 트래픽을 수락하도록 대상과 연결된 보안 그룹을 구성합니다.

로드 밸런서에 연결된 보안 그룹이 있는 경우 대상 보안 그룹에 대한 권장 사항

- 클라이언트 트래픽 허용: 로드 밸런서와 연결된 보안 그룹을 참조하는 규칙을 추가합니다.
- PrivateLink 트래픽을 허용하려면: 전송된 트래픽의 인바운드 규칙을 평가하도록 로드 밸런서를 구성한 경우 AWS PrivateLink, 로드 밸런서 보안 그룹의 트래픽을 트래픽 포트에 수락하는 규칙을 추가하십시오. 그렇지 않으면 트래픽 포트에서 로드 밸런서 프라이빗 IP 주소로부터 트래픽을 수락하는 규칙을 추가합니다.
- 로드 밸런서 상태 확인 수락: 상태 확인 포트에서 로드 밸런서 보안 그룹의 상태 확인 트래픽을 수락하는 규칙을 추가합니다.

로드 밸런서가 보안 그룹과 연결되지 않은 경우 대상 보안 그룹에 대한 권장 사항

- 클라이언트 트래픽 허용: 로드 밸런서가 클라이언트 IP 주소를 보존하는 경우 트래픽 포트에서 승인된 클라이언트의 IP 주소에서 오는 트래픽을 수락하는 규칙을 추가합니다. 그렇지 않으면 트래픽 포트에서 로드 밸런서 프라이빗 IP 주소로부터 트래픽을 수락하는 규칙을 추가합니다.
- PrivateLink 트래픽을 허용하려면: 트래픽 포트의 로드 밸런서 사설 IP 주소로부터 트래픽을 받는 규칙을 추가하세요.
- 로드 밸런서 상태 확인 수락: 상태 확인 포트에서 로드 밸런서 프라이빗 IP 주소의 상태 확인 트래픽을 수락하는 규칙을 추가합니다.

클라이언트 IP 보존 작동 방식

Network Load Balancer는 `preserve_client_ip.enabled` 속성을 `true`로 설정하지 않는 한 클라이언트 IP 주소를 보존하지 않습니다. 또한 이중 스택 네트워크 로드 밸런서를 사용하면 IPv4 주소를

IPv6으로 변환할 때 클라이언트 IP 주소를 보존합니다. 하지만 IPv6 주소를 IPv4로 변환할 때는 소스 IP가 항상 Network Load Balancer의 사설 IP 주소입니다.

콘솔을 사용하여 로드 밸런서 사설 IP 주소를 찾으려면

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

자세한 정보는 Network Load Balancer의 보안 그룹을 참조하세요.

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
##### 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	프로토콜	포트 범위	Comment
##### 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
##### 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	프로토콜	포트 범위	Comment
##### 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.

공유 서브넷

참여자는 공유 VPC에서 Network Load Balancer를 생성할 수 있습니다. 참여자는 자신과 공유되지 않은 서브넷에서 실행되는 대상을 등록할 수 없습니다.

네트워크 로드 밸런서용 공유 서브넷은 다음을 AWS 제외한 모든 지역에서 지원됩니다.

- 아시아 태평양 (오사카) `ap-northeast-3`
- 아시아 태평양 (홍콩) `ap-east-1`
- 중동 (바레인) `me-south-1`
- AWS 중국 (베이징) `cn-north-1`
- AWS 중국 (닝샤) `cn-northwest-1`

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 정보는 Target type(대상 유형)을 참조하세요.

요구 사항 및 고려 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.
- IPv6 대상 그룹의 인스턴스 ID로 대상을 등록하는 경우 대상에 할당된 기본 IPv6 주소가 있어야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 IPv6 주소를 참조하십시오.

- 인스턴스 ID로 대상을 등록하는 경우 인스턴스는 Network Load Balancer와 동일한 Amazon VPC에 있어야 합니다. 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 마세요. 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

인스턴스를 등록할 때 인스턴스가 `running` 상태여야 합니다.

콘솔을 사용하여 인스턴스 ID별로 대상을 등록 또는 등록 취소하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 대상 탭을 선택합니다.
5. 인스턴스를 등록하려면 대상 등록을 선택합니다. 하나 이상의 인스턴스를 선택하고 필요에 따라 기본 인스턴스 포트를 입력한 다음 아래에 보류 중인 것으로 포함을 선택합니다. 인스턴스 추가를 마쳤으면 보류 중인 대상 등록(Register pending targets)을 선택합니다.

   참고:

   - IPv6 대상 그룹에 등록하려면 인스턴스에 할당된 기본 IPv6 주소가 있어야 합니다.
   - AWS GovCloud (US) Region은 콘솔을 사용하여 기본 IPv6 주소를 할당하는 것을 지원하지 않습니다. API를 사용하여 s에 기본 IPv6 주소를 할당해야 합니다. AWS GovCloud (US) Region
6. 인스턴스의 등록을 취소하려면 인스턴스를 선택한 다음 등록 취소(Deregister)를 선택합니다.

IP 주소로 대상 등록 또는 등록 취소

IPv4 대상

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)

대상 그룹을 생성한 후에는 IP 주소 유형을 변경할 수 없습니다.

공유 Amazon VPC에서 참가자로 Network Load Balancer를 시작할 때 사용자와 공유된 서브넷에서만 대상을 등록할 수 있습니다.

IPv6 대상

- 사용자가 등록하는 IP 주소는 VPC CIDR 블록 내에 있거나 피어링된 VPC CIDR 블록 내에 있어야 합니다.
- 대상 그룹을 생성한 후에는 IP 주소 유형을 변경할 수 없습니다.
- IPv6 대상 그룹은 TCP 또는 TLS 리스너가 있는 듀얼스택 로드 밸런서에만 연결할 수 있습니다.

콘솔을 사용하여 IP 주소로 대상을 등록 또는 등록 취소하는 방법

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 대상 탭을 선택합니다.
5. IP 주소를 등록하려면 대상 등록을 선택합니다. 각 IP 주소에 대해 네트워크, 가용 영역, IP 주소(IPv4 또는 IPv6), 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 취소를 선택합니다. 등록 취소된 IP 주소가 많은 경우 필터를 추가하거나 정렬 순서를 변경하는 것이 유용할 수 있습니다.

AWS CLI를 사용하여 대상 등록 또는 등록 취소

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

대상으로의 Application Load Balancer

단일 Application Load Balancer를 대상으로 사용하여 대상 그룹을 생성하고 트래픽을 전달하도록 Network Load Balancer를 구성할 수 있습니다. 이 시나리오에서는 Application Load Balancer가 트래픽이 도달하는 즉시 로드 밸런싱 결정을 인계합니다. 이 구성은 두 로드 밸런서의 기능을 결합하고 다음과 같은 이점을 제공합니다.

- Application Load Balancer의 계층 7 요청 기반 라우팅 기능을 엔드포인트 서비스(AWS PrivateLink) 및 정적 IP 주소 등의 Network Load Balancer가 지원하는 기능과 함께 사용할 수 있습니다.
- 이 구성은 시그널링을 위해 HTTP를 사용하는 미디어 서비스, 콘텐츠 스트리밍을 위한 RTP와 같이 멀티 프로토콜을 위한 단일 엔드포인트가 필요한 애플리케이션에 대해 이 구성을 사용할 수 있습니다.

내부 또는 인터넷 연결 Application Load Balancer를 내부 또는 인터넷 연결 Network Load Balancer의 대상으로 이 기능을 사용할 수 있습니다.

고려 사항

- 애플리케이션 로드 밸런서를 Network Load Balancer의 대상으로 연결하려면 동일한 계정 내에서 동일한 Amazon VPC에 있어야 합니다.
- Application Load Balancer를 여러 Network Load Balancer의 대상으로 연결할 수 있습니다. 이렇게 하려면 Application Load Balancer를 각 개별 Network Load Balancer를 위한 별도의 대상 그룹에 등록 합니다.
- Network Load Balancer에 등록하는 각 Application Load Balancer는 Network Load Balancer당 가용 영역당 최대 대상 수를 50(교차 영역 로드 밸런싱이 비활성화된 경우) 또는 100(교차 영역 로드 밸런싱이 활성화된 경우)만큼 줄입니다. 지연 시간을 최소화하고 리전 데이터 전송 요금을 방지하기 위해 두 로드 밸런서에 교차 영역 로드 밸런싱을 비활성화할 수 있습니다. 자세한 정보는 Network Load Balancer 할당량을 참조하세요.
- 대상 그룹 유형이 `alb`인 경우 대상 그룹 속성을 수정할 수 없습니다. 이러한 속성은 항상 기본값을 사용합니다.
- Application Load Balancer를 대상으로 등록하면 모든 대상 그룹에서 등록을 취소하기 전까지는 Application Load Balancer Balancer를 삭제할 수 없습니다.

1단계: Application Load Balancer 생성

시작하기 전에 이 Application Load Balancer가 사용할 대상 그룹을 구성합니다. 대상 그룹에 등록할 대상이 있는 Virtual Private Cloud(VPC)가 있는지 확인하세요. 이 VPC에는 대상에서 사용하는 각 가용 영역에 하나 이상의 퍼블릭 서브넷이 있어야 합니다.

콘솔을 사용하여 Application Load Balancer를 만들려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서 생성을 선택하세요.
4. Application Load Balancer 아래에서 생성(Create)을 선택합니다.
5. Create Application Load Balancer(Application Load Balancer 생성) 페이지의 Basic configuration(기본 구성)에서 Load balancer name(로드 밸런서 이름), Scheme(체계), IP address type(IP 주소 유형)을 입력합니다.
6. 리스너의 경우 모든 포트에서 HTTP 또는 HTTPS 리스너를 생성할 수 있습니다. 그러나 이 리스너의 포트 번호가 이 Application Load Balancer가 상주할 대상 그룹의 포트와 일치하는지 확인해야 합니다.
7. 가용 영역에서 다음을 수행합니다.

   a. VPC는 Application Load Balancer의 대상으로 포함한 인스턴스 또는 IP 주소가 있는 Virtual Private Cloud(VPC)를 선택합니다. 3단계: Network Load Balancer를 생성하고 Application Load Balancer를 대상으로 구성에서 Network Load Balancer에 사용할 것과 동일한 VPC를 사용해야 합니다.

   b. 둘 이상의 가용 영역과 해당 서브넷을 선택합니다. 가용성, 확장성 및 성능을 최적화하기 위해 이러한 가용 영역이 Network Load Balancer에 활성화된 가용 영역과 일치하는지 확인합니다.
8. 새 보안 그룹을 생성하거나 기존 보안 그룹을 선택하여 로드 밸런서에 보안 그룹을 할당할 수 있습니다.

   선택하는 보안 그룹에는 이 로드 밸런서에 대한 리스너 포트로 트래픽을 허용하는 규칙이 포함되어 있어야 합니다. 클라이언트 컴퓨터의 CIDR 블록(IP 주소 범위)을 보안 그룹에 대한 인바운드 규칙의 트래픽 소스로 사용합니다. 이렇게 하면 클라이언트가 이 Application Load Balancer를 통해 트래픽을 전송할 수 있습니다. Network Load Balancer의 대상으로 Application Load Balancer에 대한 보안 그룹을 구성하는 방법에 대한 자세한 내용은 Application Load Balancer 사용 설명서의 Application Load Balancer 보안 그룹 섹션을 참조하세요.

9. 라우팅 구성의 경우 이 Application Load Balancer 대해 구성한 대상 그룹을 선택합니다. 사용 가능한 대상 그룹이 없는 상태에서 새 대상 그룹을 구성하려면 Application Load Balancer 사용 설명서의 대상 그룹 생성 단원을 참조하십시오.
10. 구성을 검토하고 로드 밸런서 생성(Create load balancer)을 선택합니다.

를 사용하여 애플리케이션 로드 밸런서를 만들려면 AWS CLI

create-load-balancer 명령을 사용합니다.

2단계: Application Load Balancer를 대상으로 하여 대상 그룹 생성

대상 그룹을 생성하면 새 또는 기존 Application Load Balancer를 대상으로 등록할 수 있습니다. 대상 그룹당 하나의 Application Load Balancer만 추가할 수 있습니다. 동일한 Application Load Balancer를 별도의 대상 그룹에서 최대 2개의 Network Load Balancer의 대상으로 사용할 수도 있습니다.

콘솔을 사용하여 대상 그룹을 생성하고 Application Load Balancer를 대상으로 등록하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱(Load Balancing) 아래에서 대상 그룹(Target Groups)을 선택합니다.
3. [대상 그룹 생성(Create target group)]을 선택합니다.
4. 그룹 세부 정보 지정 페이지의 기본 구성에서 Application Load Balancer를 선택합니다.
5. 대상 그룹 이름은 Application Load Balancer 대상 그룹의 이름을 입력합니다.
6. 프로토콜은 TCP만 허용됩니다. 대상 그룹에 대한 포트를 선택합니다. 이 대상 그룹 포트는 Application Load Balancer의 리스너 포트와 일치해야 합니다. 또는 이 포트와 일치하도록 Application Load Balancer의 리스너 포트를 추가하거나 편집할 수 있습니다.
7. VPC의 경우 대상 그룹에 등록하려는 Application Load Balancer가 있는 Virtual Private Cloud(VPC)를 선택합니다.
8. 상태 확인의 경우 HTTP 또는 HTTPS를 상태 확인 프로토콜로 선택합니다. 상태 확인은 Application Load Balancer로 전송되고 지정된 포트, 프로토콜 및 핑 경로를 사용하여 대상에 전달됩니다. 상태 확인 포트 및 프로토콜과 일치하는 포트 및 프로토콜이 있는 리스너를 사용하여 Application Load Balancer에서 이러한 상태 확인을 수신할 수 있는지 확인합니다.
9. (선택 사항) 필요에 따라 하나 이상의 태그를 추가합니다.
10. 다음을 선택합니다.
11. 대상 등록 페이지에서 대상으로 등록할 Application Load Balancer를 선택합니다. 목록에서 선택한 Application Load Balancer는 생성 중인 대상 그룹과 동일한 포트에 리스너가 있어야 합니다. 대상 그룹의 포트와 일치하도록 이 로드 밸런서에 리스너를 추가 또는 편집하거나 이전 단계로 돌아

가서 대상 그룹에 지정된 포트를 변경할 수 있습니다. 대상으로 추가할 Application Load Balancer가 확실하지 않거나 이 시점에서 추가하지 않으려는 경우 나중에 Application Load Balancer를 추가하도록 선택할 수 있습니다.

12. 대상 그룹 생성을 선택합니다.

AWS CLI를 사용하여 대상 그룹을 생성하고 Application Load Balancer를 대상으로 등록

create-target-group 및 register-targets 명령을 사용합니다.

3단계: Network Load Balancer를 생성하고 Application Load Balancer를 대상으로 구성

다음 단계에 따라 Network Load Balancer를 생성한 다음 콘솔을 사용하여 Application Load Balancer를 대상으로 구성합니다.

콘솔을 사용하여 Network Load Balancer 및 리스너를 만들려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 로드 밸런서를 선택합니다.
3. 로드 밸런서 생성을 선택하세요.
4. Network Load Balancer에서 [생성(Create)]을 선택합니다.
5. 기본 구성

   기본 구성 창에서 로드 밸런서 이름, 체계 및 IP 주소 유형을 구성합니다.
6. 네트워크 매핑

   a. VPC의 경우 Application Load Balancer 대상에 사용한 것과 동일한 VPC 선택합니다. 구성표(Scheme)에 대해 Internet-facing을 선택한 경우 인터넷 게이트웨이가 있는 VPC만 선택할 수 있습니다.

   b. 매핑(Mappings)에 대해 하나 이상의 가용 영역과 해당 서브넷을 선택합니다. 가용성, 확장성 및 성능을 최적화하기 위해 Application Load Balancer 대상과 동일한 가용 영역을 선택하는 것이 좋습니다.

      (선택 사항) 고정 IP 주소를 사용하려면 각 가용 영역에 대해 IPv4 설정에서 탄력적 IP 주소 사용을 선택합니다. 고정 IP 주소를 사용하면 방화벽의 허용 목록에 특정 IP 주소를 추가하거나 클라이언트에 IP 주소를 하드 코딩할 수 있습니다.
7. 리스너 및 라우팅

a. 기본값은 포트 80에서 TCP 트래픽을 수락하는 리스너입니다. TCP 리스너만 트래픽을 Application Load Balancer 대상 그룹으로 전달할 수 있습니다. 프로토콜을 TCP로 유지해야 하지만 필요에 따라 포트를 수정할 수 있습니다.

   이 구성을 사용하면 Application Load Balancer Balancer에서 HTTPS 리스너를 사용하여 TLS 트래픽을 종료할 수 있습니다.

b. 기본 작업에서 트래픽을 전달할 Application Load Balancer 대상 그룹을 선택합니다. 목록에 표시되지 않거나 대상 그룹을 선택할 수 없는 경우(다른 Network Load Balancer에서 이미 사용 중이므로), 2단계: Application Load Balancer를 대상으로 하여 대상 그룹 생성에 표시된 대로 Application Load Balancer 대상 그룹을 생성할 수 있습니다.

8. 태그

   (선택 사항) 태그를 추가하여 로드 밸런서를 분류합니다. 자세한 내용은 태그를 참조하세요.

9. 요약

   구성을 검토하고 로드 밸런서 생성(Create load balancer)을 선택합니다.

를 사용하여 Network Load Balancer를 만들려면 AWS CLI

create-load-balancer 명령을 사용합니다.

4단계: (선택 사항) VPC 엔드포인트 서비스 생성

이전 단계에서 프라이빗 연결을 위한 엔드포인트로 설정한 Network Load Balancer를 사용하려면 AWS PrivateLink을(를) 활성화하면 됩니다. 이렇게 하면 로드 밸런서에 대한 프라이빗 연결이 엔드포인트 서비스로 설정됩니다.

Network Load Balancer를 사용하여 VPC 엔드포인트 서비스를 생성하는 방법

1. 탐색 창에서 로드 밸런서를 선택합니다.
2. Network Load Balancer 이름을 선택하여 세부 정보 페이지를 엽니다.
3. 통합 탭에서 VPC 엔드포인트 서비스(AWS PrivateLink)를 확장합니다.
4. 엔드포인트 서비스 생성을 선택하여 엔드포인트 서비스 페이지를 엽니다. 나머지 단계는 AWS PrivateLink 가이드의 엔드포인트 서비스 생성을 참조하세요.

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 대소문자를 구분합니다. 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 공백 및 숫자와 특수 문자 + - = . _ : / @입니다. 선행 또는 후행 공백을 사용하면 안 됩니다.
- `aws:`접두사는 사용하기 위한 것이므로 태그 이름이나 값에 AWS 사용하지 마십시오. 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다. 이 접두사가 지정된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.

콘솔을 사용하여 대상 그룹의 태그를 업데이트하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 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 및 값에 새 값을 입력합니다.
   b. 태그를 추가하려면 태그 추가를 선택하고 키 및 값에 값을 입력합니다.
   c. 태그를 삭제하려면 태그 옆의 제거를 선택합니다.
5. 태그 업데이트를 마쳤으면 변경 사항 저장(Save changes)을 선택합니다.

를 사용하여 대상 그룹의 태그를 업데이트하려면 AWS CLI

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.

콘솔을 사용하여 대상 그룹을 삭제하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Load Balancing 아래에서 대상 그룹을 선택합니다.
3. 대상 그룹을 선택하고 작업, 삭제를 차례로 선택합니다.
4. 확인 메시지가 나타나면 예, 삭제합니다를 선택합니다.

를 사용하여 대상 그룹을 삭제하려면 AWS CLI

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 측정 항목

CloudWatch Amazon을 사용하여 로드 밸런서 및 대상의 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 가져올 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 CloudWatch 네트워크 로드 밸런서의 지표 단원을 참조하십시오.

VPC 흐름 로그

VPC 흐름 로그를 사용하여 Network Load Balancer로 들어오고 나가는 트래픽에 대한 세부 정보를 캡처할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하세요.

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 Balancer를 통한 각 연결은 두 가지 항목을 가집니다. 프런트엔드 연결은 클라이언트와 로드 밸런서 사이의 연결이고 백엔드 연결은 로드 밸런서와 대상 사이의 연결입니다. 대상 그룹의 클라이언트 IP 보존 특성이 사용된 경우 연결이 클라이언트의 연결로 인스턴스에 표시됩니다. 그렇지 않으면 연결의 소스 IP가 로드 밸런서의 프라이빗 IP 주소입니다. 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.

Network Load Balancer에 연결된 보안 그룹이 있는 경우 보안 그룹에서 허용하거나 거부하는 트래픽에 대한 항목이 흐름 로그에 포함됩니다. TLS 리스너가 있는 Network Load Balancer의 경우 거부된 항목만 흐름 로그 항목에 반영됩니다.

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 Balancer의 액세스 로그 단원을 참조하십시오.

CloudTrail 로그

를 AWS CloudTrail 사용하여 Elastic Load Balancing API에 대한 호출에 대한 세부 정보를 캡처하고 Amazon S3에 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하여 어떤 호출이 이루어졌는지, 어떤 소스 IP 주소를 호출했는지, 누가 전화를 걸었는지 등을 확인할 수 있습니다. 자세한 정보는 AWS CloudTrail을 사용하여 Network Load Balancer에 대한 API 호출 로깅을 참조하세요.

CloudWatch 네트워크 로드 밸런서의 지표

Elastic Load Balancing은 로드 밸런서와 CloudWatch 대상에 대한 데이터 포인트를 Amazon에 게시합니다. CloudWatch이러한 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, 지정된 지표를 모니터링하는 CloudWatch 경보를 만들어 지표가 허용 범위를 벗어나는 경우 이메일 주소로 알림을 보내는 등의 작업을 시작할 수 있습니다.

Elastic Load Balancing은 요청이 로드 밸런서를 통과하는 CloudWatch 경우에만 지표를 보고합니다. 로드 밸런서를 통과하는 요청이 있는 경우 Elastic Load Balancing은 60초 간격으로 지표를 측정하고 전송합니다. 로드 밸런서를 통과하고 있는 요청이 없는 경우나 지표에 대한 데이터가 없는 경우에는 지표가 보고되지 않습니다. 보안 그룹이 있는 Network Load Balancer의 경우 보안 그룹에서 거부한 트래픽은 지표에 캡처되지 않습니다. CloudWatch

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

내용

- Network Load Balancer 지표
- Network Load Balancer의 지표 차원
- Network Load Balancer 지표에 대한 통계
- 로드 밸런서의 CloudWatch 지표 보기

Network Load Balancer 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: 항상 보고. 통계: 가장 유용한 통계는 Average, Maximum 및 Minimum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
ActiveFlowCount_TCP	클라이언트에서 대상까지의 동시 TCP 흐름(또는 연결)의 총 수입니다. 이 지표에는 SYN_SENT 및 ESTABLISHED 상태의 연결이 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 Minimum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
ActiveFlowCount_TLS	클라이언트에서 대상까지의 동시 TLS 흐름(또는 연결)의 총 수입니다. 이 지표에는 SYN_SENT 및 ESTABLISHED 상태의 연결이 포함됩니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Average, Maximum 및 Minimum입니다.

지표	설명
	차원 • LoadBalancer • AvailabilityZone , LoadBalancer
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 Minimum입니다. 차원 • 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 Sum입니다. 차원 • 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 참조하세요. 보고 기준: 항상 보고. 통계: 모두 차원 • LoadBalancer

지표	설명
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 참조하세요. 보고 기준: 0이 아닌 값이 있을 때. 통계: 모두 차원 • LoadBalancer
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 참조하세요. 보고 기준: 0이 아닌 값이 있을 때. 통계: 모두 차원 • 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 참조하세요. 보고 기준: 0이 아닌 값이 있을 때. 통계: 모두 차원 • LoadBalancer

지표	설명
HealthyHostCount	정상 상태로 간주되는 대상 수. 이 지표에는 대상으로 등록된 Application Load Balancer가 포함되지 않습니다. 보고 기준: 상태 확인을 활성화한 경우 보고됩니다. 통계: 가장 유용한 통계는 Maximum 및 Minimum입니다. 차원 • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 흐름(또는 연결)의 총 수입니다. 보고 기준: 항상 보고. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
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. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
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. 차원 • 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. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
PeakPacketsPerSecond	샘플링 기간 동안 10초마다 계산되는 최고 평균 패킷 속도(초당 처리되는 패킷)입니다. 이 지표에는 상태 확인 트래픽이 포함됩니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Maximum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
PortAllocationErrorCount	클라이언트 IP 변환 작업 중 임시 포트 할당 오류의 총 수입니다. 0이 아닌 값은 클라이언트 연결이 끊어졌음을 나타냅니다. 참고: Network Load Balancers는 클라이언트 주소 변환을 수행할 때 각각의 고유 대상(IP 주소 및 포트)에 대해 55,000건의 동시 연결 또는 분당 약 55,000건의 연결을 지원합니다. 포트 할당 오류를 해결하려면 대상 그룹에 더 많은 대상을 추가하세요. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • 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: 항상 보고. 통계: 가장 유용한 통계는 Sum입니다. 차원 • 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. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_TLS	TLS 리스너에서 처리한 총 바이트 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_UDP	UDP 리스너에서 처리한 총 바이트 수입니다. 보고 기준: 0이 아닌 값이 있을 때 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
ProcessedPackets	로드 밸런서에서 처리한 총 패킷 수입니다. 여기에는 대상부터의 트래픽, 대상까지의 트래픽, 상태 확인 트래픽을 포함합니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_ICMP	로드 밸런서 보안 그룹의 인바운드 규칙에서 거부한 새 ICMP 메시지 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_TCP	로드 밸런서 보안 그룹의 인바운드 규칙에서 거부한 새 TCP 흐름 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
SecurityGroupBlockedFlowCount_Inbound_UDP	로드 밸런서 보안 그룹의 인바운드 규칙에서 거부한 새 UDP 흐름 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_ICMP	로드 밸런서 보안 그룹의 아웃바운드 규칙에서 거부한 새 ICMP 메시지 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	로드 밸런서 보안 그룹의 아웃바운드 규칙에서 거부한 새 TCP 흐름 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
SecurityGroupBlockedFlowCount_Outbound_UDP	로드 밸런서 보안 그룹의 아웃바운드 규칙에서 거부한 새 UDP 흐름 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • 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. 차원 • LoadBalancer
TCP_Client_Reset_Count	클라이언트에서 대상까지 전송된 재설정(RST) 패킷의 총 수입니다. 이러한 재설정은 클라이언트에 의해 생성되고 로드 밸런서에 의해 전달됩니다. 보고 기준: 항상 보고. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

지표	설명
TCP_ELB_Reset_Count	로드 밸런서에 의해 생성되는 재설정(RST) 패킷의 총 수입니다. 자세한 내용은 문제 해결을 참조하세요. 보고 기준: 항상 보고. 통계: 가장 유용한 통계는 Sum입니다. 차원 • 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: 항상 보고. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer
UnHealthyHostCount	비정상 상태로 간주되는 대상 수. 이 지표에는 대상으로 등록된 Application Load Balancer가 포함되지 않습니다. 보고 기준: 상태 확인을 활성화한 경우 보고됩니다. 통계: 가장 유용한 통계는 Maximum 및 Minimum입니다. 차원 • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup

지표	설명
UnhealthyRoutingFlowCount	라우팅 장애 조치 작업(페일 오픈)을 사용하여 라우팅된 흐름(또는 연결) 수. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • LoadBalancer • AvailabilityZone , LoadBalancer

Network Load Balancer의 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

CloudWatch Elastic Load Balancing에서 게시한 지표 데이터 포인트를 기반으로 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 말합니

다. 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. 최대 HealthyHostCount 값을 모니터링하여 최대 HealthyHostCount 값이 필요한 최솟값 아래로 떨어지거나 0이 되면 알람을 호출하는 것이 좋습니다. 이렇게 하면 대상이 비정상 상태가 된 시기를 식별하는 데 도움이 될 수 있습니다. 또한 최소 UnHealthyHostCount 값을 모니터링하여 최소 UnHealthyHostCount 값이 0을 초과했을 때 알람을 호출하는 것이 좋습니다. 이렇게 하면 등록된 대상이 더 없을 때 이를 알 수 있습니다.

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

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

로드 밸런서의 CloudWatch 지표 보기

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

또는 콘솔을 사용하여 로드 밸런서에 대한 지표를 볼 수도 있습니다. CloudWatch

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 대상 그룹을 선택합니다.
   b. 대상 그룹을 선택하고 모니터링을 선택합니다.
   c. (선택 사항) 시간을 기준으로 결과를 필터링하려면 다음에 대한 데이터 표시에서 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.

콘솔을 CloudWatch 사용하여 지표를 보려면

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

를 사용하여 지표를 보려면 AWS CLI

사용 가능한 지표의 목록을 표시하려면 아래 list-metrics 명령을 사용하세요.

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

를 사용하여 지표에 대한 통계를 가져오려면 AWS CLI

지정된 지표 및 차원에 대한 통계를 구하려면 아래 get-metric-statistics 명령을 사용하세요. 참고로 각 고유한 측정기준 조합은 별도의 측정항목으로 CloudWatch 취급됩니다. 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 Balancer의 액세스 로그

Elastic Load Balancing은 네트워크 로드 밸런서에 설정된 TLS 연결에 대한 세부 정보를 캡처하는 액세스 로그를 제공합니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

> **Important**
>
> 액세스 로그는 Network Load Balancer에 TLS 리스너가 있고 TLS 연결에 대한 정보만 포함하는 경우에만 생성됩니다.

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

S3 버킷에 대해 Amazon S3 관리형 암호화 키(SSE-S3) 또는 고객 관리형 키(SSE-KMS CMK)와 함께 키 관리 서비스를 사용하여 서버 측 암호화를 활성화할 수 있습니다. 각 액세스 로그 파일은 S3 버킷에 저장되기 전에 자동으로 암호화되고, 액세스할 때 해독됩니다. 암호화된 로그 파일이나 암호화되지 않은 로그 파일을 액세스하는 방식과 다르지 않으므로 별도의 조치가 필요 없습니다. 각 로그 파일은 고유 키로 암호화되며, 이 키 자체는 정기적으로 교체되는 KMS 키로 암호화됩니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 암호화 지정 (SSE-S3) 및 서버 측 암호화 지정 AWS KMS (SSE-KMS) 을 참조하십시오.

액세스 로그에 대한 추가 요금은 없습니다. Amazon S3의 스토리지 비용은 청구되지만, Amazon S3로 로그 파일을 전송하기 위해 Elastic Load Balancing에서 사용하는 대역폭에 대해서는 요금이 부과되지 않습니다. 스토리지 비용에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

액세스 로그 파일

Elastic Load Balancing은 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_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

S3 버킷의 이름.

접두사

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

aws-account-id

소유자의 ID. AWS 계정

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.

다음은 로그 파일 이름의 예제입니다.

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

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 S3 사용 설명서의 스토리지 수명 주기 관리를 참조하세요.

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

필드	설명
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`, `tlsv12` 및 `tlsv13`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.

필드	설명
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.
tls_connection_creation_time	TLS 연결이 시작되면 ISO 8601 형식으로 기록되는 시간입니다.

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
- - - 2018-12-20T02:59:30
```

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" 2020-04-01T08:51:20
```

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 지정하는 버킷 이름과 접두사 뒤에 추가됩니다.
- 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",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        }
    ]
}
```

이전 정책에서 `aws:SourceAccount`에 대해 이 버킷으로 로그를 전달할 계정 번호 목록을 지정합니다. `aws:SourceArn`에 대해 로그를 생성하는 리소스의 ARN 목록을 `arn:aws:logs:`*source-region*`:`*source-account-id*`:*` 형식으로 지정합니다.

암호화(Encryption)

다음 방법 중 하나를 사용하여 Amazon S3 액세스 로그 버킷에 대해 서버 측 암호화를 활성화할 수 있습니다.

- Amazon S3 관리형 키(SSE-S3)
- AWS KMS AWS Key Management Service (SSE-KMS) †에 저장된 키

† Network Load Balancer 액세스 로그에서는 AWS 관리 키를 사용할 수 없으며 고객 관리 키를 사용해야 합니다.

자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 암호화 지정 (SSE-S3) 및 서버 측 암호화 지정 AWS KMS (SSE-KMS) 을 참조하십시오.

키 정책은 서비스가 로그를 암호화하고 해독할 수 있도록 허용해야 합니다. 다음은 정책 예제입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

액세스 로그 활성화

로드 밸런서에 대한 액세스 로그를 활성화할 때는 로드 밸런서가 로그를 저장할 S3 버킷을 지정해야 합니다. 해당 버킷을 소유하고 있으며 필요한 이 버킷에 필요한 버킷 정책을 구성했는지 확인하세요. 자세한 정보는 버킷 요구 사항을 참조하세요.

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 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. [Edit load balancer attributes] 페이지에서 다음 작업을 수행합니다.
   a. 모니터링에서 액세스 로그를 켭니다.
   b. S3 찾아보기를 선택하고 사용할 버킷을 선택합니다. 또는 접두사를 포함하여 S3 버킷의 위치를 입력합니다.
   c. 변경 사항 저장를 선택합니다.

다음을 사용하여 액세스 로깅을 활성화하려면 AWS CLI

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 사용 설명서의 버킷 작업을 참조하세요.

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 밸런서 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 속성성(Attributes) 탭에서 편집(Edit)을 선택합니다.
5. 모니터링에서 액세스 로그를 끕니다.
6. 변경 사항 저장를 선택합니다.

를 사용하여 액세스 로깅을 비활성화하려면 AWS CLI

modify-load-balancer-attributes 명령을 사용합니다.

액세스 로그 파일 처리

액세스 로그 파일은 압축이 됩니다. Amazon S3 콘솔을 사용하여 파일을 열면 파일이 압축되지 않고 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. line-by-line 프로세싱을 사용하여 이렇게 많은 양의 데이터를 처리하지 못할 수도 있습니다. 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 Athena는 표준 SQL을 사용해 Amazon S3에 저장된 데이터를 간편하게 분석할 수 있는 대화식 쿼리 서비스입니다. 자세한 내용은 Amazon Athena 사용 설명서의 Network Load Balancer 로그 쿼리 방법을 참조하세요.
- Loggly
- Splunk
- Sumo Logic

AWS CloudTrail을 사용하여 Network Load Balancer에 대한 API 호출 로깅

Elastic Load Balancing은 Elastic Load AWS 서비스 Balancing에서 사용자, 역할 또는 담당자가 수행한 작업에 대한 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Elastic Load Balancing에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Elastic Load Balancing API 작업에 대한 AWS Management Console 및 코드 호출이 포함됩니다. 트레일을 생성하면 Elastic Load Balancing을 위한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Elastic Load Balancing에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Elastic Load Balancing 정보 참조 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. Elastic Load Balancing에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Elastic Load Balancing을 위한 이벤트를 포함하여 귀하의 AWS 계정이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 트레일을 생성하면 트레일이 모든 AWS 지역에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 AWS 서비스 취하도록 기타를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

네트워크 로드 밸런서에 대한 모든 Elastic Load Balancing 작업은 Elastic Load Balancing API 참조 버전 2015-12-01에 CloudTrail 기록되고 문서화되어 있습니다. 예를 들어, `CreateLoadBalancer` 및 `DeleteLoadBalancer` 작업에 대한 호출은 로그 파일에 항목을 생성합니다. CloudTrail

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

- 요청을 루트로 했는지 아니면 사용자 자격 증명으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail사용자 ID 요소를 참조하십시오.

Elastic Load Balancing 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

로그 파일에는 Elastic Load Balancing AWS API 호출뿐 아니라 사용자에 대한 모든 API 호출에 대한 이벤트가 포함됩니다. AWS 계정`eventSource` 값이 있는 `elasticloadbalancing.amazonaws.com` 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 Network Load Balancer를 생성한 후 를 사용하여 삭제한 사용자에 대한 Elastic Load Balancing의 예제 CloudTrail 로그 기록입니다. AWS CLI`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 단원을 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 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 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 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 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 확인이 배포되고 합의 메커니즘을 사용하여 대상 상태를 확인합니다. 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

이는 등록된 모든 대상이 비정상일 때 발생합니다. 정상 상태의 대상이 한 개 이상 등록되어 있으면 Network Load Balancer는 정상 상태의 등록 대상으로만 요청을 라우팅합니다.

비정상 상태의 대상만 등록되어 있으면 Network Load Balancer는 모든 등록 대상에 요청을 라우팅합니다(오류 시 열림 모드라고 함). 모든 대상이 비정상이고 각 가용 영역에 요청을 보낼 정상 대상이 없는 경우 Network Load Balancer는 DNS에서 모든 IP 주소를 제거하는 대신 이 작업을 수행합니다.

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.

보안 그룹을 로드 밸런서와 연결할 수 없음

Network Load Balancer가 보안 그룹 없이 생성된 경우 생성 후에는 보안 그룹을 지원할 수 없습니다. 보안 그룹은 생성 중 로드 밸런서에 연결하거나 원래 보안 그룹으로 생성된 기존 로드 밸런서에만 연결할 수 있습니다.

모든 보안 그룹을 제거할 수 없음

Network Load Balancer가 보안 그룹과 함께 생성된 경우 항상 하나 이상의 보안 그룹이 연결되어 있어야 합니다. 로드 밸런서에서 모든 보안 그룹을 동시에 제거할 수는 없습니다.

TCP_ELB_Reset_Count 지표 증가

클라이언트가 Network Load Balancer를 통해 보내는 각 TCP 요청에 대해 해당 연결의 상태가 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. 또한, 대상이 비정상 상태이면 비정상 대상이 로드 밸런서의 페일 오픈을 트리거하지 않는 한 로드 밸런서가 대상과 관련된 클라이언트 연결에서 수신된 패킷에 대해 TCP RST를 보냅니다.

`UnhealthyHostCount` 메트릭이 증가하기 직전에 또는 증가함과 동시에 `TCP_ELB_Reset_Count` 지표가 급증하는 것이 보이는 것은 대상이 실패하기 시작했지만 비정상으로 표시되지 않았기 때문에 TCP RST 패킷이 전송되는 것일 수 있습니다. 대상이 비정상적으로 표시되지 않았지만 `TCP_ELB_Reset_Count`에서 지속적인 증가가 보이는 경우, VPC 흐름 로그에서 만료된 흐름에 데이터를 전송하는 클라이언트가 있는지 확인할 수 있습니다.

대상에서 로드 밸런서로의 요청에서 연결 시간이 초과됨

대상 그룹에서 클라이언트 IP 보존이 활성화되어 있는지 확인합니다. 헤어피닝이라고도 하는 NAT 루프백은 클라이언트 IP 보존이 활성화된 경우 지원되지 않습니다. 인스턴스가 등록된 로드 밸런서의 클라이언트이고 클라이언트 IP 보존이 활성화된 경우 요청이 다른 인스턴스로 라우팅된 경우에만 연결이 성공합니다. 요청이 전송된 동일한 인스턴스로 라우팅되는 경우 소스 및 목적지 IP 주소가 동일하기 때문에 연결 시간이 초과됩니다.

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

- 클라이언트 IP 보존을 사용하지 않도록 설정합니다.
- 통신해야 하는 컨테이너가 다른 컨테이너 인스턴스에 있는지 확인합니다.

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 Balancer를 기반으로 더 많은 TCP 연결을 수신할 수 있습니다. 대상이 수신할 수 있는 연결 요청 볼륨을 처리할 준비가 되었는지 확인하십시오.

연결 시 포트 할당 오류가 발생했습니다. AWS PrivateLink

Network Load Balancer가 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 오류는 `PortAllocationErrorCount` 지표를 사용하여 추적할 수 있습니다. 포트 할당 오류를 해결하려면 대상 그룹에 더 많은 대상을 추가하세요. 자세한 정보는 CloudWatch 네트워크 로드 밸런서의 지표을 참조하세요.

클라이언트 IP 보존 사용 시 간헐적인 연결 실패

클라이언트 IP 보존을 사용하도록 설정한 경우 대상에서 관찰된 소켓 재사용과 관련된 TCP/IP 연결 제한이 발생할 수 있습니다. 이러한 연결 제한은 여러 로드 밸런서 노드에 동시에 연결할 때 클라이언트 또는 클라이언트 앞에 있는 NAT 디바이스가 동일한 소스 IP 주소와 소스 포트를 사용하는 경우에 발생할 수 있습니다. 로드 밸런서가 이러한 연결을 동일한 대상으로 라우팅하는 경우 이 연결은 동일한 소스 소켓에서 온 것처럼 대상에 나타나므로 연결 오류가 발생합니다. 이러한 경우(연결이 실패하면) 클라이언트가 다시 시도하거나 (연결이 중단되면) 다시 연결할 수 있습니다. 소스 휘발성 포트 수를 늘리거나 로드 밸런서에 대한 대상 수를 늘려 이러한 유형의 연결 오류를 줄일 수 있습니다. 클라이언트 IP 보존 혹은 교차 영역 로드 밸런싱을 비활성화하여 이러한 유형의 연결 오류를 방지할 수 있습니다.

또한 클라이언트 IP 보존을 사용하도록 설정한 경우 Network Load Balancer에 연결하는 클라이언트가 로드 밸런서를 기반으로 대상에도 연결되어 있으면 연결이 실패할 수 있습니다. 이 문제를 해결하려면 영향을 받는 대상 그룹에서 클라이언트 IP 보존을 비활성화할 수 있습니다. 또는, 클라이언트가 Network Load Balancer에만 연결하거나 대상에만 연결하도록 하고 둘 다에는 연결하지 않도록 합니다.

TCP 연결 지연

교차 영역 로드 밸런싱과 클라이언트 IP 보존이 모두 활성화된 경우, 동일한 로드 밸런서의 다른 IP에 연결하는 클라이언트가 동일한 대상으로 라우팅될 수 있습니다. 클라이언트가 이러한 두 연결 모두에

대해 동일한 소스 포트를 사용하는 경우, 대상은 중복 연결인 것으로 보이는 데이터를 수신하여 새 연결을 설정할 때 연결 오류와 TCP 지연이 발생할 수 있습니다. 교차 영역 로드 밸런싱을 비활성화하면 이러한 유형의 연결 오류를 방지할 수 있습니다. 자세한 정보는 교차 영역 로드 밸런싱을 참조하세요.

로드 밸런서가 프로비저닝되고 있을 때 발생할 수 있는 오류

프로비저닝될 때 Network Load Balancer가 실패할 수 있는 이유 중 하나는 이미 할당되었거나 다른 곳에 할당된 IP 주소(예: EC2 인스턴스의 보조 IP 주소로 할당됨)를 사용하는 경우입니다. 이 IP 주소는 로드 밸런서가 설정되지 않도록 하며 상태는 `failed`입니다. 연결된 IP 주소의 할당을 해제하고 생성 프로세스를 다시 시도하면 이 문제를 해결할 수 있습니다.

DNS 이름 확인에 포함된 IP 주소가 활성화된 가용 영역보다 적음

가용 영역에 하나 이상의 정상 호스트가 있는 경우 Network Load Balancer가 활성화된 가용 영역당 하나의 IP 주소를 제공하는 것이 가장 좋습니다. 특정 가용 영역에 정상 호스트가 없고 영역 간 로드 밸런싱이 비활성화된 경우 해당 AZ와 관련된 Network Load Balancer IP 주소가 DNS에서 제거됩니다.

예를 들어 Network Load Balancer Balancer에 세 개의 가용 영역이 활성화되어 있고 모든 가용 영역에 하나 이상의 정상 등록된 대상 인스턴스가 있다고 가정해 보겠습니다.

- 가용 영역 A에 등록된 대상 인스턴스가 비정상 상태가 되면 Network Load Balancer 가용 영역 A의 해당 IP 주소가 DNS에서 제거됩니다.
- 활성화된 가용 영역 중 두 개 영역에 정상 등록된 대상 인스턴스가 없는 경우 Network Load Balancer 밸런서의 해당 두 IP 주소가 DNS에서 제거됩니다.
- 활성화된 모든 가용 영역에 정상 등록된 대상 인스턴스가 없는 경우 오류 시 열림 모드가 활성화되고 DNS는 세 개의 활성화된 AZ의 모든 IP 주소를 결과에 제공합니다.

리소스 맵을 사용하여 비정상 대상 문제 해결

Network Load Balancer 대상의 상태 확인이 실패하는 경우 리소스 맵을 사용하여 비정상 대상을 찾고 실패 원인 코드에 따라 조치를 취할 수 있습니다. 자세한 정보는 Network Load Balancer 리소스 맵을 참조하세요.

리소스 맵은 개요 및 비정상 대상 맵이라는 두 가지 보기를 제공합니다. 개요는 기본적으로 선택되며 로드 밸런서의 모든 리소스를 표시합니다. 비정상 대상 맵 보기를 선택하면 Network Load Balancer와 관련된 각 대상 그룹의 비정상 대상만 표시됩니다.

> **Note**
>
> 리소스 맵 내의 모든 해당 리소스에 대한 상태 점검 요약 및 오류 메시지를 보려면 리소스 세부 정보 표시를 활성화해야 합니다. 활성화되지 않은 경우 각 리소스를 선택하여 해당 세부 정보를 확인해야 합니다.

목표 그룹 열에는 각 대상 그룹의 정상 및 비정상 대상 요약이 표시됩니다. 이를 통해 모든 대상이 상태 점검에 실패했는지 아니면 특정 대상만 실패했는지 확인할 수 있습니다. 대상 그룹의 모든 대상이 상태 점검에 실패하는 경우 대상 그룹의 상태 점검 설정을 확인하십시오. 대상 그룹의 이름을 선택하면 새 탭에서 해당 세부 정보 페이지가 열립니다.

Targets 열에는 TargetId와 각 대상의 현재 상태 점검 상태가 표시됩니다. 대상이 비정상인 경우 상태 점검 실패 사유 코드가 표시됩니다. 단일 대상이 상태 점검에 실패하는 경우 대상에 충분한 리소스가 있는지 확인하십시오. 대상의 ID를 선택하여 새 탭에서 해당 세부 정보 페이지를 엽니다.

내보내기를 선택하면 네트워크 로드 밸런서 리소스 맵의 현재 보기를 PDF로 내보낼 수 있습니다.

인스턴스의 상태 확인이 실패했는지 확인한 다음 실패 이유 코드를 기반으로 다음 문제를 확인하십시오.

- 비정상: 요청 제한 시간이 초과되었습니다.
  - 대상 및 Network Load Balancer와 관련된 보안 그룹 및 네트워크 액세스 제어 목록 (ACL) 이 연결을 차단하지 않는지 확인하십시오.
  - 대상에 Network Load Balancer의 연결을 수락할 수 있는 충분한 용량이 있는지 확인합니다.
  - Network Load Balancer의 상태 점검 응답은 각 대상의 애플리케이션 로그에서 볼 수 있습니다. 자세한 내용은 건강 진단 사유 코드를 참조하십시오.
- 비정상: FailedHealthChecks
  - 대상이 상태 점검 포트에서 트래픽을 수신하고 있는지 확인하십시오.

> **TLS 리스너를 사용하는 경우**
>
> 프런트 엔드 연결에 사용할 보안 정책을 선택합니다. 백엔드 연결에 사용되는 보안 정책은 사용 중인 프런트 엔드 보안 정책에 따라 자동으로 선택됩니다.
>
> - TLS 수신기가 프런트 엔드 연결에 TLS 1.3 보안 정책을 사용하는 경우 보안 정책은 백엔드 연결에 사용됩니다. `ELBSecurityPolicy-TLS13-1-0-2021-06`

  - TLS 수신기가 프런트 엔드 연결에 TLS 1.3 보안 정책을 사용하지 않는 경우 보안 정책은 백엔드 연결에 사용됩니다. `ELBSecurityPolicy-2016-08`

  자세한 내용은 보안 정책을 참조하십시오.

- 대상이 보안 정책에 지정된 올바른 형식의 서버 인증서 및 키를 제공하고 있는지 확인하십시오.
- 대상이 하나 이상의 일치하는 암호와 TLS 핸드셰이크를 설정하기 위해 Network Load Balancer에서 제공하는 프로토콜을 지원하는지 확인합니다.

Network Load Balancer 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 서비스를 선택하고 Elastic Load Balancing을 선택합니다. Elastic Load Balancing에 대해 describe-account-limits(AWS CLI) 명령을 사용할 수도 있습니다.

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

로드 밸런서

AWS 계정에는 Network Load Balancer와 관련하여 다음과 같은 할당량이 있습니다.

이름	기본값	조정 가능
Network Load Balancer당 인증서	25	예
Network Load Balancer당 리스너	50	아니요
VPC당 Network Load Balancer ENI	1,200 [1]	예
리전당 Network Load Balancer	50	예
Network Load Balancer별 작업당 대상 그룹	1	아니요
Network Load Balancer별 가용 영역당 대상	500 [2, 3]	예
Network Load Balancer당 대상	3,000 [3]	예

[1] 각 Network Load Balancer는 영역당 하나의 네트워크 인터페이스를 사용합니다. 할당량은 VPC 수준에서 설정됩니다. 서브넷이나 VPC를 공유할 때 사용량은 모든 테넌트에 대해 계산됩니다.

[2] 대상이 N개의 대상 그룹에 등록된 경우, 이 한도에 대해 N개의 대상으로 계산됩니다. Network Load Balancer의 대상인 각 Application Load Balancer는 교차 영역 로드 밸런싱이 비활성화된 경우 50개의 대상으로 계산되고 교차 영역 로드 밸런싱이 활성화된 경우 100개의 대상으로 계산됩니다.

[3] 교차 영역 로드 밸런싱이 활성화되어 있는 경우, 가용 영역의 수에 관계없이 로드 밸런서당 최대 값은 대상 500개입니다.

대상 그룹

다음 할당량은 대상 그룹용입니다.

이름	기본값	조정 가능
리전당 대상 그룹	3,000 [1]	예
리전별 대상 그룹당 대상(인스턴스 또는 IP 주소)	1,000	예
리전별 대상 그룹당 대상(Application Load Balancer)	1	아니요

[1] 이 할당량은 Application Load Balancer 및 Network Load Balancer에서 공유됩니다.

Network Load Balancer에 대한 문서 기록

다음 표에서는 Network Load Balancer의 릴리스에 대해 설명합니다.

변경 사항	설명	날짜
RSA 3072비트 및 ECDSA 256/384/521비트 인증서	이 릴리스에는 (ACM) 을 통한 RSA 3072비트 인증서와 타원 곡선 디지털 서명 알고리즘 (ECDSA) 256, 384 및 521비트 인증서에 대한 지원이 추가되었습니다. AWS Certificate Manager	2024년 1월 19일
FIPS 140-3 TLS 터미네이션	이 릴리스에는 TLS 연결을 종료할 때 FIPS 140-3 암호화 모듈을 사용하는 보안 정책이 추가되었습니다.	2023년 11월 20일
영역 DNS 어피니티	이번 릴리스에는 로드 밸런서 DNS를 확인하는 클라이언트가 속해 있는 동일한 가용 영역 (AZ) 에서 IP 주소를 수신하도록 지원하는 기능이 추가되었습니다.	2023년 10월 12일
비정상 대상 연결 종료를 비활성화합니다.	이 릴리스에는 상태 확인에 실패한 대상에 대한 활성 연결을 유지하기 위한 지원이 추가되었습니다.	2023년 10월 12일
기본 UDP 연결 종료	이 릴리스에는 기본적으로 등록 취소 제한 시간 종료 시 UDP 연결을 종료하는 지원이 추가되었습니다.	2023년 10월 12일
IPv6를 사용하여 대상을 등록합니다.	이번 릴리스에는 IPv6 주소 지정 시 인스턴스를 대상으로 등	2023년 10월 2일

	록하는 지원이 추가되었습니다.	
Network Load Balancer의 보안 그룹	이 릴리스에는 생성 시 보안 그룹을 Network Load Balancer와 연결할 수 있는 지원이 추가되었습니다.	2023년 8월 10일
대상 그룹 상태	이 릴리스에는 정상이어야 하는 대상의 최소 개수 또는 백분율, 임계값이 충족되지 않은 경우 로드 밸런서가 취하는 작업을 구성할 수 있는 지원이 추가되었습니다.	2022년 11월 17일
상태 확인 구성	이 릴리스에서는 상태 확인 구성이 개선되었습니다.	2022년 11월 17일
교차 영역 로드 밸런싱	이번 릴리스에는 대상 그룹 수준에서 영역 간 부하 분산을 구성하는 지원이 추가되었습니다.	2022년 11월 17일
IPv6 대상 그룹	이 릴리스에는 네트워크 로드 밸런서를 위한 IPv6 대상 그룹 구성 지원이 추가되었습니다.	2021년 11월 23일
IPv6 내부 부하 분산기	이번 릴리스에는 네트워크 로드 밸런서를 위한 IPv6 대상 그룹 구성 지원이 추가되었습니다.	2021년 11월 23일
TLS 1.3	이 릴리스는 TLS 버전 1.3을 지원하는 보안 정책을 추가합니다.	2021년 10월 14일

대상으로의 Application Load Balancer	이 릴리스는 Network Load Balancer의 대상으로서 Application Load Balancer를 구성하는 지원을 추가합니다.	2021년 9월 27일
클라이언트 IP 보존	이 릴리스에서는 클라이언트 IP 보존 구성에 대한 지원이 추가되었습니다.	2021년 2월 4일
TLS 버전 1.2를 지원하는 FS에 대한 보안 정책	이 릴리스에는 TLS 버전 1.2를 지원하는 FS(Forward Secrecy)에 대한 보안 정책이 추가되었습니다.	2020년 11월 24일
듀얼 스택 모드	이 릴리스에는 클라이언트가 IPv4 주소와 IPv6 주소를 모두 사용하여 로드 밸런서에 연결하게 할 수 있는 듀얼 스택 모드에 대한 지원이 추가되었습니다.	2020년 11월 13일
등록 취소 시 연결 종료	이 릴리스에는 등록 취소 시간 제한이 끝난 후 등록 취소된 대상에 대한 연결을 종료하는 지원이 추가되었습니다.	2020년 11월 13일
ALPN 정책	이 릴리스에는 ALPN(Application-Layer Protocol Negotiation) 기본 설정 목록에 대한 지원이 추가되었습니다.	2020년 5월 27일
고정 세션	이 릴리스에서는 소스 IP 주소 및 프로토콜을 기반으로 고정 세션에 대한 지원이 추가되었습니다.	2020년 2월 28일

공유 서브넷	이 릴리스는 다른 AWS 계정에 의해 사용자와 공유된 서브넷을 지정하는 지원을 추가합니다.	2019년 11월 26일
프라이빗 IP 주소	이 릴리스에서는 내부 로드 밸런서에 대해 가용 영역을 활성화할 때 지정하는 서브넷의 IPv4 주소 범위에서 프라이빗 IP 주소를 제공할 수 있습니다.	2019년 11월 25일
서브넷 추가	이 릴리스에는 로드 밸런서를 생성한 후 추가 가용 영역 활성화에 대한 지원이 추가되었습니다.	2019년 11월 25일
FS의 보안 정책	이 릴리스에는 사전 정의된 순방향 보안 정책 3개에 대한 지원이 추가로 추가되었습니다.	2019년 10월 8일
SNI 지원	이번 릴리스에는 SNI(Server Name Indication)에 대한 지원이 추가되었습니다.	2019년 9월 12일
UDP 프로토콜	이 릴리스에서는 UDP 프로토콜을 추가로 지원합니다.	2019년 6월 24일
새 지역에서 사용 가능	이번 릴리스에는 아시아 태평양 (오사카) 지역의 네트워크 로드 밸런서에 대한 지원이 추가되었습니다.	2019년 6월 12일
TLS 프로토콜	이 릴리스에서는 TLS 프로토콜을 추가로 지원합니다.	2019년 1월 24일
교차 영역 로드 밸런싱	이 릴리스에서는 교차 영역 로드 밸런싱을 활성화하기 위한 지원이 추가되었습니다.	2018년 2월 22일

프록시 프로토콜	이번 릴리스에서는 프록시 프로토콜 활성화에 대한 지원을 추가합니다.	2017년 11월 17일
IP 주소를 대상으로 사용	이 릴리스에서는 IP 주소를 대상으로 등록에 대한 지원이 추가되었습니다.	2017년 9월 21일
새로운 로드 밸런서 유형	이번 Elastic Load Balancing 릴리스에는 Network Load Balancer가 도입되었습니다.	2017년 9월 7일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.