AWS Global Accelerator

개발자 가이드

AWS Global Accelerator: 개발자 가이드

Table of Contents

AWS Global Accelerator 무엇입니까?

AWS Global Accelerator 사용자가액셀러레이터를 사용하여 로컬 및 글로벌 사용자를 위한 애플리케이션의 성능을 향상시킬 수 있습니다. 선택한 액셀러레이터의 유형에 따라 추가 혜택을 얻을 수 있습니다.

- 표준 액셀러레이터를 사용하면 전 세계 사용자가 이용하는 인터넷 애플리케이션의 가용성을 향상시킬 수 있습니다. 글로벌 액셀러레이터는 표준 가속기를 사용하여 AWS 글로벌 네트워크를 통한 트래픽을 클라이언트와 가장 가까운 리전의 엔드포인트로 보냅니다.
- 사용자 지정 라우팅 가속기를 사용하여 하나 이상의 사용자를 여러 대상 중에서 특정 대상에 매핑할 수 있습니다.

글로벌 액셀러레이터는 여러 AWS 리전의 엔드포인트를 지원하는 글로벌 서비스로,AWS 리전 테이블.

기본적으로 글로벌 가속기는 가속기와 연결하는 두 개의 정적 IP 주소를 제공합니다. 표준 가속기를 사용하면 글로벌 가속기가 제공하는 IP 주소를 사용하는 대신 글로벌 가속기로 가져오는 고유한 IP 주소 범위의 IPv4 주소로 이러한 진입점을 구성할 수 있습니다. 정적 IP 주소는 AWS 엣지 네트워크에서 애니캐스트됩니다.

> Important
>
> 액셀러레이터를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않더라도 고정 IP 주소는 액셀러레이터에 할당된 상태로 유지됩니다. 그러나, 때삭제가속기를 사용하면 할당된 고정 IP 주소가 손실되므로 더 이상 트래픽을 라우팅할 수 없습니다. 글로벌 가속기와 함께 태그 기반 권한과 같은 IAM 정책을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

표준 가속기의 경우 Global Accelerator는 AWS 글로벌 네트워크를 사용하여 사용자가 구성한 상태, 클라이언트 위치 및 정책을 기반으로 트래픽을 최적의 리전 엔드포인트로 라우팅하므로 애플리케이션의 가용성이 향상됩니다. 표준 가속기의 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 하나의 AWS 리전 또는 여러 리전에 위치한 엘라스틱 IP 주소일 수 있습니다. 이 서비스는 상태 또는 구성의 변화에 즉시 반응하여 클라이언트의 인터넷 트래픽이 항상 정상적인 엔드포인트로 전달되도록 합니다.

사용자 지정 라우팅 가속기는 VPC (가상 프라이빗 클라우드) 서브넷 엔드포인트 유형만 지원하고 트래픽을 해당 서브넷의 프라이빗 IP 주소로 라우팅합니다.

현재 글로벌 액셀러레이터를 지원하는 AWS 리전 목록은AWS 리전 테이블.

주제

AWS Global Accelerator

AWS Global Accelerator 는 다음 구성 요소를 포함합니다

고정 IP 주소

글로벌 액셀러레이터는 AWS 엣지 네트워크에서 캐스트된 두 개의 정적 IP 주소 집합을 제공합니다. 고유한 IP 주소 범위를 AWS (BYOIP) 액셀러레이터에서 사용할 수 있도록 가져오는 경우 (BYOIP) 액셀러레이터에서 사용할 사용자 풀에서 IP 주소를 할당할 수 있습니다. 자세한 내용은 AWS Global Accelerator 고유 IP 주소 가져오기 (p. 49) 섹션을 참조하세요.

IP 주소는 클라이언트의 단일 고정 진입점 역할을 합니다. 애플리케이션에 대해 Elastic Load Balancing 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소 리소스가 이미 설정되어 있는 경우 글로벌 가속기의 표준 가속기에 이러한 리소스를 쉽게 추가할 수 있습니다. 이렇게 하면 글로벌 가속기가 정적 IP 주소를 사용하여 리소스에 액세스할 수 있습니다.

액셀러레이터를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않더라도 고정 IP 주소는 액셀러레이터에 할당된 상태로 유지됩니다. 그러나, 때삭제가속기를 사용하면 할당된 고정 IP 주소가 손실되므로 더 이상 트래픽을 라우팅할 수 없습니다. 글로벌 가속기와 함께 태그 기반 권한과 같은 IAM 정책을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

가속기

가속기는 AWS 글로벌 네트워크를 통해 엔드포인트로 트래픽을 전송하여 인터넷 애플리케이션의 성능을 향상시킵니다. 각 가속기에는 하나 이상의 수신기가 포함됩니다.

액셀러레이터에는 두 가지 유형이 있습니다.

- A표준가속기는 사용자의 위치, 엔드포인트의 상태, 구성하는 엔드포인트 가중치 등 여러 요소를 기반으로 최적의 AWS 엔드포인트로 트래픽을 전달합니다. 이렇게 하면 애플리케이션의 가용성과 성능이 향상됩니다. 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다.
- A사용자 지정 라우팅가속기를 사용하면 일부 사용 사례에 따라 여러 사용자를 가속기 뒤의 특정 EC2 대상으로 결정적으로 라우팅할 수 있습니다. 이렇게 하려면 글로벌 가속기가 대상에 매핑된 가속기의 고유한 IP 주소 및 포트로 사용자를 안내합니다.

자세한 내용은 액셀러레이터의 종류 (p. 6) 섹션을 참조하세요.

DNS 이름

글로벌 액셀러레이터별로 기본 DNS (Domain Name System) 이름을 할당합니다.`a1234567890abcdef.awsglobalaccelerator.com`로 설정하면 글로벌 가속기가 사용자에게 할당하거나 사용자가 자신의 IP 주소 범위에서 선택하는 고정 IP 주소를 가리킵니다. 사용 사례에 따라 가속기의 고정 IP 주소 또는 DNS 이름을 사용하여 트래픽을 가속기로 라우팅하거나 DNS 레코드를 설정하여 사용자 지정 도메인 이름을 사용하여 트래픽을 라우팅할 수 있습니다.

네트워크 존

네트워크 영역은 고유한 IP 서브넷에서 가속기에 대한 고정 IP 주소를 제공합니다. AWS 가용 영역과 마찬가지로 네트워크 영역은 자체 물리적 인프라 세트가 있는 격리된 단위입니다. 가속기를 구성하면 기본적으로 글로벌 가속기에서 두 개의 IPv4 주소를 할당합니다. 특정 클라이언트 네트워크에 의한 IP 주소 차단 또는 네트워크 중단으로 인해 네트워크 영역의 IP 주소 하나를 사용할 수 없게 되면 클라이언트 응용 프로그램은 격리된 다른 네트워크 영역에서 정상 정적 IP 주소를 다시 시도할 수 있습니다.

Listener

수신기는 사용자가 구성하는 포트 (또는 포트 범위) 및 프로토콜 (또는 프로토콜) 에 따라 클라이언트에서 글로벌 가속기로의 인바운드 연결을 처리합니다. 리스너는 TCP, UDP 또는 TCP 및 UDP 프로토콜 모두에 대해 구성할 수 있습니다. 각 수신기에는 하나 이상의 끝점 그룹이 연결되어 있으며 트래픽은 그룹 중 하나의 끝점으로 전달됩니다. 트래픽을 분산할 지역을 지정하여 엔드포인트 그룹을 리스너와 연결합니다. 표준 가속기를 사용하면 트래픽이 수신기와 연결된 끝점 그룹 내의 최적 끝점에 분산됩니다.

엔드포인트 그룹

각 엔드포인트 그룹은 특정 AWS 리전과 연결되어 있습니다. 끝점 그룹에는 리전에 하나 이상의 끝점이 포함됩니다. 표준 가속기를 사용하면 끝점 그룹에 전달되는 트래픽의 비율을 늘리거나 줄일 수 있습니다.트래픽 다이얼. 트래픽 다이얼을 사용하면 성능 테스트 또는 파란색/녹색 배포 테스트를 쉽게 수행할 수 있습니다 (예: 여러 AWS 리전의 새 릴리스에 대해).

Endpoint

엔드포인트는 글로벌 액셀러레이터가 트래픽을 전달하는 리소스입니다.

표준 가속기의 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다. Application Load Balancer 엔드포인트는 인터넷 연결 또는 내부일 수 있습니다. 표준 가속기의 트래픽은 엔드포인트 가중치와 같은 사용자가 선택한 구성 옵션과 함께 엔드포인트의 상태에 따라 엔드포인트로 라우팅됩니다. 각 엔드포인트에 대해 가중치를 구성할 수 있습니다. 가중치는 각 엔드포인트로 라우팅할 트래픽 비율을 지정하는 데 사용할 수 있습니다. 예를 들어 지역 내에서 성능 테스트를 수행하는 데 유용 할 수 있습니다.

사용자 지정 라우팅 가속기를 위한 엔드포인트는 트래픽의 대상인 하나 이상의 Amazon EC2 인스턴스가 있는 가상 프라이빗 클라우드 (VPC) 서브넷입니다.

AWS Global Accelerator

AWS Global Accelerator 터가 제공하는 고정 IP 주소는 고객의 단일 고정 진입점 역할을 합니다. 글로벌 액셀러레이터를 사용하여 가속기를 설정하면 하나 이상의 AWS 리전에 있는 리전 엔드포인트에 고정 IP 주소를 연결합니다. 표준 가속기의 경우 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소입니다. 사용자 지정 라우팅 가속기의 경우 엔드포인트는 하나 이상의 EC2 인스턴스가 있는 가상 프라이빗 클라우드 (VPC) 서브넷입니다. 고정 IP 주소는 사용자와 가장 가까운 엣지 로케이션에서 AWS 글로벌 네트워크로 들어오는 트래픽을 허용합니다.

Note

고유한 IP 주소 범위를 AWS (BYOIP) 로 가져와 Global Accelerator에 사용할 경우 (BYOIP) 액셀러레이터에서 사용할 사용자 풀에서 고정 IP 주소를 할당할 수 있습니다. 자세한 내용은 AWS Global Accelerator 고유 IP 주소 가져오기 (p. 49) 섹션을 참조하세요.

엣지 로케이션에서 응용 프로그램의 트래픽은 구성하는 가속기 유형에 따라 라우팅됩니다.

- 표준 가속기의 경우 트래픽은 사용자의 위치, 엔드포인트의 상태, 구성하는 엔드포인트 가중치 등 여러 요소를 기반으로 최적의 AWS 엔드포인트로 라우팅됩니다.
- 사용자 지정 라우팅 가속기의 경우, 각 클라이언트는 사용자가 제공한 외부 고정 IP 주소 및 수신기 포트를 기반으로 VPC 서브넷의 특정 Amazon EC2 인스턴스 및 포트로 라우팅됩니다.

트래픽은 잘 모니터링되고 정체 없는 중복 AWS 글로벌 네트워크를 통해 엔드포인트로 이동합니다. 글로벌 액셀러레이터는 트래픽이 AWS 네트워크에 걸리는 시간을 극대화함으로써 트래픽이 항상 최적의 네트워크 경로를 통해 라우팅되도록 합니다.

일부 엔드 포인트 유형 (일부 AWS 리전 (p. 58)) 를 사용하는 경우 클라이언트 IP 주소를 보존하고 액세스할 수 있는 옵션이 있습니다. 두 가지 유형의 끝점은 들어오는 패킷에서 클라이언트의 원본 IP 주소를 보존할 수 있습니다. 애플리케이션 로드 밸런서 및 Amazon EC2 인스턴스 글로벌 가속기는 Network Load Balancer 및 엘라스틱 IP 주소 끝점에 대한 클라이언트 IP 주소 보존을 지원하지 않습니다. 사용자 지정 라우팅 가속기의 끝점에는 항상 클라이언트 IP 주소가 유지됩니다.

글로벌 액셀러레이터는 AWS 엣지 로케이션의 클라이언트에서 TCP 연결을 종료하고 거의 동시에 엔드포인트와 새 TCP 연결을 설정합니다. 따라서 클라이언트의 응답 시간 단축 (지연 시간 단축) 및 처리량 증가가 가능합니다.

표준 가속기에서 Global Accelerator 는 모든 끝점의 상태를 지속적으로 모니터링하고 활성 끝점이 비정상이라고 판단되면 사용 가능한 다른 끝점으로 트래픽을 즉시 전달하기 시작합니다. 이를 통해 AWS 에서 애플리케이션을 위한 고가용성 아키텍처를 생성할 수 있습니다. Health 확인은 사용자 지정 라우팅 가속기와 함께 사용되지 않으며 트래픽을 라우팅할 대상을 지정하므로 장애 조치가 없습니다.

액셀러레이터를 추가하면 이미 구성한 보안 그룹 및 AWS WAF 규칙은 액셀러레이터를 추가하기 전과 동일하게 작동합니다.

글로벌 트래픽을 세밀하게 제어하려면 표준 가속기에서 엔드포인트에 대한 가중치를 구성할 수 있습니다. 또한 성능 테스트 또는 스택 업그레이드를 위해 특정 엔드포인트 그룹에 대한 트래픽 비율을 증가 (다이얼 업) 또는 감소 (다이얼 다운) 할 수 있습니다.

Global Accelerator를 사용하는 경우에는 다음 사항에 유의하십시오.

- AWS Direct Connect 는 퍼블릭 가상 인터페이스를 통해 AWS Global Accelerator 터에 대한 IP 주소 접두사를 알리지 않습니다. AWS Direct Connect 퍼블릭 가상 인터페이스를 통해 글로벌 액셀러레이터와 통신하는 데 사용하는 IP 주소는 광고하지 않는 것이 좋습니다. AWS Direct Connect 퍼블릭 가상 인터페이스를 통해 글로벌 액셀러레이터와 통신하는 데 사용하는 IP 주소를 광고하는 경우 비대칭적인 트래픽 흐름이 발생합니다. 글로벌 액셀러레이터로 향하는 트래픽은 인터넷을 통해 글로벌 액셀러레이터로 이동하지만 온프레미스로 들어오는 트래픽은 반환합니다.네트워크는 AWS Direct Connect 퍼블릭 가상 인터페이스를 통해 제공됩니다.
- 글로벌 액셀러레이터는 다른 AWS 계정에 속한 리소스를 엔드포인트로 추가하는 것을 지원하지 않습니다.

주제

AWS Global Accelerator 에

AWS Global Accelerator 에 해당 연결에 적용되는 유휴 제한 시간 기간을 설정합니다. 유휴 제한 시간이 경과할 때까지 데이터가 전송되거나 전송 또는 수신되지 않으면 Global Accelerator에서 연결을 종료합니다. 연결이 계속 유지되도록 하려면 유휴 시간 초과 기간이 경과하기 전에 클라이언트 또는 끝점이 최소 1바이트 이상의 데이터를 전송해야 합니다.

네트워크 연결에 대한 글로벌 가속기 유휴 시간 초과는 연결 유형에 따라 다릅니다.

- TCP 연결의 시간 초과는 340 초입니다.
- UDP 연결의 경우 30초입니다.

글로벌 액셀러레이터는 끝점이 비정상으로 표시된 경우에도 유휴 시간 초과가 충족될 때까지 엔드포인트로 트래픽을 계속 보냅니다. 글로벌 가속기는 새 연결이 시작되거나 유휴 시간 초과 이후에만 필요한 경우 새 끝점을 선택합니다.

AWS Global Accelerator 에 사용되는

글로벌 액셀러레이터가 가속기에 할당하거나 표준 가속기의 경우 자체 IP 주소 풀에서 지정한 고정 IP 주소를 사용하여 사용자의 위치에 관계없이 사용자의 위치에 가까운 AWS 글로벌 네트워크로 인터넷 트래픽을 라우팅합니다. 표준 가속기의 경우 단일 AWS 리전 또는 여러 리전에서 실행되는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소와 주소를 연결합니다. 사용자 지정 라우팅 가속기의 경우 하나 이상의 리전에 있는 VPC 서브넷에 있는 EC2 대상으로 트래픽을 보냅니다. AWS 글로벌 네트워크를 통해 트래픽을 라우팅하면 트래픽이 퍼블릭 인터넷을 통해 여러 홉을 수행할 필요가 없으

므로 가용성과 성능이 향상됩니다. 또한 고정 IP 주소를 사용하면 수신 애플리케이션 트래픽을 여러 AWS 리전의 여러 엔드포인트 리소스에 분산할 수 있습니다.

또한 고정 IP 주소를 사용하면 애플리케이션을 더 많은 지역에 추가하거나 지역 간에 애플리케이션을 마이그레이션할 수 있습니다. 고정 IP 주소를 사용한다는 것은 사용자가 변경 시 애플리케이션에 일관된 방식으로 연결할 수 있음을 의미합니다.

원하는 경우 사용자 지정 도메인 이름을 가속기의 고정 IP 주소와 연결할 수 있습니다. 자세한 내용은 사용자 지정 도메인 트래픽을 가속기로 라우팅 (p. 48) 섹션을 참조하세요.

글로벌 액셀러레이터는 자체 IP 주소 범위를 AWS 로 가져온 다음 해당 풀에서 고정 IP 주소를 지정하지 않는 한 Amazon IP 주소 풀에서 정적 IP 주소를 제공합니다. (자세한 내용은 AWS Global Accelerator 고유 IP 주소 가져오기 (p. 49) 섹션을 참조하십시오.) 콘솔에서 가속기를 만들려면 첫 번째 단계는 가속기의 이름을 입력하거나 고정 IP 주소를 선택하여 글로벌 가속기에 정적 IP 주소를 프로비저닝하라는 메시지를 표시합니다. 가속기를 만드는 단계를 보려면AWS Global Accelerator 시작하기 (p. 11).

액셀러레이터를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않더라도 고정 IP 주소는 액셀러레이터에 할당된 상태로 유지됩니다. 그러나, 때삭제가속기를 사용하면 할당된 고정 IP 주소가 손실되므로 더 이상 트래픽을 라우팅할 수 없습니다. 글로벌 가속기와 함께 태그 기반 권한과 같은 IAM 정책을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

트래픽 다이얼 및 엔드포인트 가중치를 사용한 트래픽 흐름 관리

AWS 글로벌 액셀러레이터가 표준 액셀러레이터를 사용하여 엔드포인트로 트래픽을 전송하는 방법을 사용자 지정할 수 있는 두 가지 방법이 있습니다.

- 하나 이상의 끝점 그룹에 대한 트래픽을 제한하도록 트래픽 다이얼 변경
- 가중치를 지정하여 그룹의 엔드포인트에 대한 트래픽 비율을 변경합니다.

트래픽 다이얼의 작동 방식

표준 가속기의 각 끝점 그룹에 대해 트래픽 다이얼을 설정하여 끝점 그룹으로 전송되는 트래픽의 비율을 제어할 수 있습니다. 이 비율은 모든 수신기 트래픽이 아니라 이미 끝점 그룹으로 전달된 트래픽에만 적용됩니다.

트래픽 다이얼은 엔드포인트 그룹이 허용하는 트래픽 부분을 제한합니다. 이 부분은 해당 엔드포인트 그룹에 전달되는 트래픽의 백분율로 표시됩니다. 예를 들어, 끝점 그룹에 대한 트래픽 다이얼을`us-east-1`를 50 (즉, 50%) 으로 설정하고 가속기가 100개의 사용자 요청을 해당 끝점 그룹에 보내면 그룹에서 50개의 요청만 수락됩니다. 가속기는 나머지 50개의 요청을 다른 지역의 끝점 그룹으로 보냅니다.

자세한 내용은 트래픽 다이얼로 트래픽 흐름 조정 (p. 27) 섹션을 참조하세요.

분동 작동 방식

표준 가속기의 각 끝점에 대해 가중치를 지정할 수 있습니다. 가중치는 가속기가 각 끝점으로 라우팅하는 트래픽의 비율을 변경하는 숫자입니다. 예를 들어 지역 내에서 성능 테스트를 수행하는 데 유용 할 수 있습니다.

가중치는 가속기가 엔드포인트로 보내는 트래픽의 비율을 결정하는 값입니다. 기본적으로 끝점의 가중치는 128입니다. 즉, 가중치에 대한 최대값의 절반인 255입니다.

가속기는 끝점 그룹의 끝점에 대한 가중치 합계를 계산한 다음 각 끝점의 가중치 대 총 가중치의 비율에 따라 트래픽을 끝점으로 보냅니다. 가중치가 작동하는 방식에 대한 예는 단원을 참조하십시오. 엔드포인트 가중치 (p. 32).

트래픽 다이얼과 가중치는 표준 가속기가 다양한 방식으로 트래픽을 제공하는 방식에 영향을 줍니다.

- 당신은에 대한 트래픽 다이얼을 구성엔드포인트 그룹. 트래픽 다이얼을 사용하면 가속기가 근접성과 같은 다른 요소를 기반으로 이미 전달한 트래픽을 “전화 걸기”하여 그룹에 대한 트래픽 비율 (또는 모든 트래픽)을 차단할 수 있습니다.
- 반면에 가중치를 사용하여 값을 설정합니다.개별 엔드포인트엔드포인트 그룹을 포함합니다. 가중치는 엔드포인트 그룹 내에서 트래픽을 분할하는 방법을 제공합니다. 예를 들어 가중치를 사용하여 지역의 특정 엔드포인트에 대한 성능 테스트를 수행할 수 있습니다.

  Note

  트래픽 다이얼과 가중치가 장애 조치 (failover) 에 미치는 영향에 대한 자세한 내용은 단원을 참조하십시오비정상 엔드포인트에 대한 장애 조치 (p. 32).

AWS Global Accelerator Health 확인

표준 가속기의 경우 AWS Global Accelerator는 정적 IP 주소와 연결된 엔드포인트의 상태를 자동으로 확인한 다음 사용자 트래픽을 정상 엔드포인트로만 보냅니다.

글로벌 가속기에는 자동으로 실행되는 기본 상태 확인이 포함되어 있지만 검사 및 기타 옵션에 대한 타이밍을 구성할 수 있습니다. 사용자 지정 상태 확인 설정을 구성한 경우 전역 가속기는 구성에 따라 특정 방식으로 이러한 설정을 사용합니다. Amazon EC2 용 글로벌 액셀러레이터 인스턴스 또는 엘라스틱 IP 주소 엔드포인트에서 이러한 설정을 구성하거나 네트워크 로드 밸런서 또는 애플리케이션 로드 밸런서에 대한 엘라스틱 로드 밸런싱 콘솔에서 설정을 구성합니다. 자세한 내용은 상태 확인 옵션 (p. 28) 섹션을 참조하세요.

표준 가속기에 엔드포인트를 추가하는 경우 트래픽이 전달되기 전에 상태 확인을 통과해야 정상으로 간주됩니다. 글로벌 액셀러레이터는 표준 액셀러레이터에서 트래픽을 라우팅할 정상 엔드포인트가 없는 경우 요청을 모든 엔드포인트로 라우팅합니다.

액셀러레이터의 종류

AWS Global Accelerator 액셀러레이터와 함께 사용할 수 있는 액셀러레이터에는 다음 두 가지 유형이 있습니다.표준 액셀러레이터및사용자 정의 라우팅 가속기. 두 가지 유형의 가속기 모두 AWS 글로벌 네트워크를 통해 트래픽을 라우팅하여 성능과 안정성을 향상시키지만 각 가속기는 서로 다른 애플리케이션 요구 사항에 맞게 설계되었습니다.

표준 액셀러레이터

표준 가속기를 사용하면 애플리케이션 로드 밸런서, 네트워크 로드 밸런서 또는 Amazon EC2 인스턴스에서 실행되는 애플리케이션의 가용성과 성능을 향상시킬 수 있습니다. 표준 가속기를 사용하는 글로벌 액셀러레이터는 지리적 근접성 및 엔드포인트 상태에 따라 리전 엔드포인트 간에 클라이언트 트래픽을 라우팅합니다. 또한 고객은 트래픽 다이얼 및 엔드포인트 가중치와 같은 제어를 기반으로 엔드포인트 간에 클라이언트 트래픽을 이동할 수 있습니다. 이 기능은 파란색/녹색 배포, A/B 테스트 및 다중 지역 배포를 비롯한 다양한 사용 사례에서 사용할 수 있습니다. 더 많은 사용 사례를 보려면 AWS Global Accelerator 사용 (p. 7).

자세한 내용은 AWS 글로벌 액셀러레이터의 표준 액셀러레이터 사용 (p. 20) 단원을 참조하십시오.

사용자 라우팅 액셀러레이터

사용자 지정 라우팅 가속기는 사용자 지정 응용 프로그램 논리를 사용하여 한 명 이상의 사용자를 특정 대상 및 포트로 안내하는 동시에 글로벌 가속기의 성능 이점을 얻고자 하는 시나리오에 적합합니다. 한 가지 예는 음성, 비디오 및 메시징 세션을 시작하기 위해 특정 미디어 서버에 여러 발신자를 할당하는 VoIP 응용 프로그램입니다. 또 다른 예는 지리적 위치, 플레이어 기술 및 게임 모드와 같은 요소를 기반으로 게임 서버의 단일 세션에 여러 플레이어를 할당하려는 온라인 실시간 게임 응용 프로그램입니다.

자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기 사용 (p. 36) 단원을 참조하십시오.

특정 요구 사항에 따라 이러한 유형의 가속기 중 하나를 만들어 고객 트래픽을 가속화합니다.

Global Accelerator 엣지 서버의 위치 및 IP 주소 범위

Global Accelerator 엣지 서버 위치 목록은 단원을 참조하십시오.현재 AWS Global Accelerator 터는 어디에 배포됩니까?단원을 참조하십시오.AWS Global Accelerator FAQ페이지를 참조하십시오.

AWS 는 현재 IP 주소 범위를 JSON 형식으로 게시합니다. 현재 범위를 보려면json의 IP 범위입니다.. 자세한 내용은 단원을 참조하십시오.AWS IP 주소 범위의Amazon Web Services 일반 참조.

AWS Global Accelerator 엣지 서버와 연결된 IP 주소 범위를 찾으려면`ip-ranges.json`를 다음 문자열에 추가합니다.

```
"service": "GLOBALACCELERATOR"
```

다음을 포함하는 글로벌 액셀러레이터 항목`"region": "GLOBAL"`은 가속기에 할당된 고정 IP 주소를 나타냅니다. 한 영역의 현재 위치 (POP) 에서 오는 가속기를 통해 트래픽을 필터링하려면 다음과 같은 특정 지리적 영역을 포함하는 항목을 필터링합니다.`us-*`또는`eu-*`. 예를 들어,`us-*`을 선택하면 미국 (미국) 의 POP를 통해 들어오는 트래픽만 표시됩니다.

AWS Global Accelerator 사용

AWS Global Accelerator 를 사용하면 다양한 목표를 달성할 수 있습니다. 이 섹션에는 글로벌 액셀러레이터를 사용하여 요구 사항을 충족하는 방법을 알려 주는 몇 가지 목록이 나와 있습니다.

애플리케이션 활용도 향상을 위한 확장성

애플리케이션 사용량이 증가하면 관리해야 하는 IP 주소 및 엔드포인트 수도 증가합니다. 글로벌 액셀러레이터를 사용하면 네트워크를 확장하거나 축소할 수 있습니다. 로드 밸런서 및 Amazon EC2 인스턴스와 같은 리전 리소스를 두 개의 정적 IP 주소에 연결할 수 있습니다. 이러한 주소는 클라이언트 응용 프로그램, 방화벽 및 DNS 레코드에 한 번만 허용 목록에 포함시킵니다. 글로벌 액셀러레이터를 사용하면 클라이언트 애플리케이션에서 IP 주소를 업데이트하지 않고도 AWS 리전에서 엔드포인트를 추가 또는 제거하고, 청색/녹색 배포를 실행하고, A/B 테스트를 수행할 수 있습니다. 이 기능은 클라이언트 응용 프로그램을 자주 업데이트할 수 없는 IoT, 소매, 미디어, 자동차 및 의료 사용 사례에 특히 유용합니다.

지연 시간에 민감한 애플리케이션을 위한 가속화

특히 게임, 미디어, 모바일 앱 및 재무 등의 분야에서 많은 응용 프로그램은 뛰어난 사용자 환경을 위해 대기 시간이 매우 짧아야 합니다. 사용자 환경을 개선하기 위해 글로벌 액셀러레이터는 클라이언트와 가장 가까운 애플리케이션 엔드포인트로 사용자 트래픽을 전달하여 인터넷 지연 시간과 지터를 줄입니다. 글로벌 액셀러레이터는 애니캐스트를 사용하여 트래픽을 가장 가까운 엣지 로케이션으로 라우팅한 다음 AWS 글로벌 네트워크를 통해 가장 가까운 리전 엔드포인트로 라우팅합니다. 글로벌 액셀러레이터는 네트워크 성능의 변화에 빠르게 반응하여 사용자의 애플리케이션 성능을 향상시킵니다.

재해 복구 및 다중 지역 복원력

사용 가능하려면 네트워크에 의존할 수 있어야 합니다. 재해 복구, 가용성 향상, 지연 시간 단축 또는 규정 준수를 지원하기 위해 여러 AWS 지역에서 애플리케이션을 실행하고 있을 수 있습니다. 글로벌 액셀러레이터는 애플리케이션 엔드포인트가 기본 AWS 리전에서 실패하고 있음을 감지하면 사용 가능한 가장 가까운 다음 AWS 리전에서 애플리케이션 엔드포인트로 트래픽 재라우팅이 즉시 트리거됩니다.

애플리케이션 보호

애플리케이션 로드 밸런서 또는 Amazon EC2 인스턴스와 같은 AWS 오리진을 퍼블릭 인터넷 트래픽에 노출하면 악의적인 공격이 발생할 수 있습니다. 글로벌 가속기는 두 개의 정적 진입점 뒤에 오리진을 마스킹하여 공격 위험을 줄입니다. 이러한 진입점은 기본적으로 AWS Shield를 통한 DDoS (분산 서비스

거부) 공격으로부터 보호됩니다. 글로벌 액셀러레이터는 프라이빗 IP 주소를 사용하여 Amazon Virtual Private Cloud 와의 피어링 연결을 생성하여 퍼블릭 인터넷 외부의 내부 애플리케이션 로드 밸런서 또는 프라이빗 EC2 인스턴스에 대한 연결을 유지합니다.

VoIP 또는 온라인 게임 애플리케이션의 성능 향상

사용자 지정 라우팅 가속기를 사용하면 VoIP 또는 게임 응용 프로그램에 글로벌 가속기의 성능 이점을 활용할 수 있습니다. 예를 들어 단일 게임 세션에 여러 플레이어를 할당하는 온라인 게임 응용 프로그램에 글로벌 가속기를 사용할 수 있습니다. 글로벌 액셀러레이터를 사용하면 멀티플레이어 게임 또는 VoIP 호출과 같은 특정 엔드포인트에 사용자를 매핑하기 위해 사용자 지정 논리가 필요한 애플리케이션의 지연 시간과 지터를 전체적으로 줄일 수 있습니다. 단일 가속기를 사용하여 클라이언트를 단일 또는 여러 AWS 리전에서 실행 중인 수천 개의 Amazon EC2 인스턴스에 연결할 수 있으며, 어떤 클라이언트가 어떤 EC2 인스턴스와 포트로 전달되는지 완벽하게 제어할 수 있습니다.

AWS Global Accelerator 속도 비교

AWS Global Accelerator 속도 비교 도구를 사용하여 AWS 리전에서 직접 인터넷 다운로드와 비교하여 글로벌 가속기 다운로드 속도를 확인할 수 있습니다. 이 도구를 사용하면 글로벌 가속기를 사용하여 데이터를 전송할 때 브라우저를 사용하여 성능 차이를 확인할 수 있습니다. 다운로드할 파일 크기를 선택하면 도구가 HTTPS/TCP를 통해 다른 지역의 애플리케이션 로드 밸런서에서 브라우저로 파일을 다운로드합니다. 각 지역에 대해 다운로드 속도를 직접 비교할 수 있습니다.

속도 비교 도구에 액세스하려면 브라우저에 다음 URL을 복사합니다.

```
https://speedtest.globalaccelerator.aws
```

Important

테스트를 여러 번 실행할 때 결과가 다를 수 있습니다. 다운로드 시간은 사용 중인 라스트 마일 네트워크의 연결 품질, 용량, 거리 등 글로벌 액셀러레이터 외부의 요인에 따라 달라질 수 있습니다.

AWS Global Accelerator 시작하는 방법

API를 사용하거나 AWS Global Accelerator 콘솔을 사용하여 AWS Global Accelerator 설정을 시작할 수 있습니다. 글로벌 액셀러레이터는 글로벌 서비스이므로 특정 AWS 리전과 연결되지 않습니다. 글로벌 액셀러레이터는 여러 AWS 리전의 엔드포인트를 지원하는 글로벌 서비스이지만 액셀러레이터를 생성하거나 업데이트하려면 미국 서부 (오레곤) 리전을 지정해야 합니다.

글로벌 액셀러레이터 사용을 시작하려면 다음과 같은 일반적인 단계를 따르십시오.

1. 생성하려는 액셀러레이터의 유형을 선택합니다. 표준 액셀러레이터 또는 사용자 지정 라우팅 액셀러레이터
2. 글로벌 가속기에 대한 초기 설정을 구성합니다. 액셀러레이터의 이름을 제공합니다. 그런 다음 지정한 프로토콜 및 포트 (또는 포트 범위) 를 기반으로 클라이언트의 인바운드 연결을 처리하도록 하나 이상의 수신기를 구성합니다.
3. 가속기에 대한 지역별 끝점 그룹을 구성합니다. 리스너에 추가할 리전 엔드포인트 그룹을 하나 이상 선택할 수 있습니다. 수신기는 엔드포인트 그룹에 추가한 엔드포인트로 요청을 라우팅합니다.

   표준 가속기의 경우 글로벌 가속기는 각 끝점에 대해 정의된 상태 확인 설정을 사용하여 그룹 내 끝점의 상태를 모니터링합니다. 표준 가속기의 각 끝점 그룹에 대해트래픽 다이얼백분율을 사용하여 끝점 그룹이 수락할 트래픽의 백분율을 제어합니다. 이 비율은 모든 수신기 트래픽이 아니라 이미 끝점 그룹으로 전달된 트래픽에만 적용됩니다. 기본적으로 트래픽 다이얼은 모든 지역별 끝점 그룹에 대해 100% 로 설정됩니다.

사용자 지정 라우팅 가속기의 경우 트래픽이 수신되는 수신기 포트를 기반으로 VPC 서브넷의 특정 대상으로 트래픽이 결정적으로 라우팅됩니다.

4. 끝점 그룹에 끝점 추가: 추가하는 엔드포인트는 액셀러레이터의 유형에 따라 달라집니다.
   - 표준 가속기의 경우 각 엔드포인트 그룹에 하나 이상의 지역 리소스 (예: 로드 밸런서 또는 EC2 인스턴스 엔드포인트) 를 추가할 수 있습니다. 다음으로 엔드포인트 가중치를 설정하여 각 엔드포인트로 라우팅할 트래픽의 양을 결정할 수 있습니다.
   - 사용자 지정 라우팅 가속기의 경우 최대 수천 개의 Amazon EC2 인스턴스 대상을 포함하는 가상 프라이빗 클라우드 (VPC) 서브넷을 하나 이상 추가합니다.

AWS Global Accelerator 가속기 콘솔을 사용하여 표준 가속기 또는 사용자 지정 라우팅 가속기를 만드는 방법에 대한 자세한 단계는AWS Global Accelerator 시작하기 (p. 11). API 작업을 사용하려면 단원을 참조하십시오.AWS 글로벌 액셀러레이터와 함께 사용할 수 있는 일반적인 작업 (p. 18)및AWS Global Accelerator API.

AWS Global Accelerator

태그는 AWS 리소스를 식별하고 정리할 때 사용하는 단어 또는 구 (메타데이터) 입니다. 각 리소스에 태그를 여러 개 추가할 수 있고, 각 태그는 사용자가 정의한 키와 값을 포함할 수 있습니다. 예를 들어 키는`environment`값이 될 수 있습니다`production`. 추가하는 태그에 따라 리소스를 검색하고 필터링할 수 있습니다. AWS 글로벌 액셀러레이터에서는 가속기에 태그를 지정할 수 있습니다.

다음은 이 기능이 Global Accelerator 액셀러레이터

- 태그를 사용하여 다양한 범주에서 청구 정보를 추적합니다. 이렇게 하려면 가속기 또는 기타 AWS 리소스 (예: 네트워크 로드 밸런서, 애플리케이션 로드 밸런서 또는 Amazon EC2 인스턴스) 에 태그를 적용하고 태그를 활성화합니다. 그런 다음, AWS 에서 사용 내역 및 비용이 활성 태그 기준으로 집계된 CSV 파일 형식으로 만듭니다. 비즈니스 범주를 나타내는 태그(예: 비용 센터, 애플리케이션 이름 또는 소유자)를 적용하여 여러 서비스에 대한 비용을 정리할 수 있습니다. 자세한 내용은 단원을 참조하십시오.비용 할당 태그 사용의AWS Billing and Cost Management 사용 설명서.
- 태그를 사용하여 Accelerator 액셀러레이터에 대한 태그 기반 권한을 적용합니다. 이렇게 하려면 작업을 허용하거나 허용하지 않도록 태그 및 태그 값을 지정하는 IAM 정책을 생성합니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

사용 규칙 및 태깅에 대한 다른 리소스에 대한 링크는AWS 리소스에 태그 지정의AWS 일반 참조. 태그 사용에 대한 팁은태그 지정 모범 사례 AWS 리소스 태깅 전략의AWS 백서블로그를 참조하십시오.

Global Accelerator 액셀러레이터에서 리소스에 추가할 수 있는 최대 태그 수는 단원을 참조하십시오.AWS Global Accelerator 할당량 (p. 104).

AWS 콘솔, AWS CLI 또는 Global Accelerator API를 사용하여 태그를 추가하고 업데이트할 수 있습니다. 이 장에는 콘솔에서 태그 지정 작업을 수행하는 단계가 포함되어 있습니다. CLI 예제를 포함하여 AWS CLI 및 글로벌 액셀러레이터 API를 사용한 태그 작업에 대한 자세한 내용은AWS Global Accelerator:

- 액셀러레이터 만들기
- TagResource
- UntagResource
- ListTagsForResource

글로벌 가속기의 태그 지정 지원

AWS 글로벌 액셀러레이터는 가속기에 대한 태그 지정을 지원합니다.

AWS Identity and Access Management (IAM) 의 태그 기반 액세스 제어 기능을 지원합니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

Global Accelerator 액셀러레이터

다음 절차는 Global Accelerator 콘솔에서 액셀러레이터 태그를 추가, 편집 및 삭제하는 방법을 설명합니다.

Note

콘솔, AWS CLI 또는 Global Accelerator API 작업을 사용하여 태그를 추가하거나 제거할 수 있습니다. CLI 예제를 포함한 자세한 내용은 단원을 참조하십시오.TagResource의AWS Global Accelerator.

전역 Accelerator 에서 태그를 추가, 편집 또는 삭제하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 태그를 추가하거나 업데이트하려는 Accelerator 를 선택합니다.
3. 에서태그섹션에서 다음 작업을 수행할 수 있습니다.

   태그 추가

   선택태그 추가을 선택한 다음 키와 태그 값 (선택 사항) 을 입력합니다.

   태그 편집

   키, 값 또는 둘 다에 대한 텍스트를 업데이트합니다. 태그의 값은 지울 수 있지만 키는 필요합니다.

   태그 삭제

   선택제거값 필드 오른쪽에 있습니다.
4. [Save changes]를 선택합니다.

AWS Global Accelerator 요금

AWS Global Accelerator 사용하면 사용한 만큼만 지불하면 됩니다. 계정의 각 액셀러레이터별로 시간당 요금 및 데이터 전송 비용이 청구됩니다. 자세한 내용은 단원을 참조하십시오.AWS Global Accelerator.

AWS Global Accelerator 시작하기

이 자습서에서는 콘솔을 사용하여 AWS Global Accelerator 시작하는 단계를 제공합니다. AWS Global Accelerator API 작업을 사용하여 액셀러레이터를 만들고 사용자 지정할 수도 있습니다. 이 자습서의 각 단계에는 프로그래밍 방식으로 작업을 완료하기 위한 해당 API 작업에 대한 링크가 있습니다. 사용자 지정 라우팅 가속기를 설정할 때는 특정 구성 단계에 API를 사용해야 합니다. AWS Global Accelerator API 작업에 대한 자세한 내용은 단원을 참조하십시오.AWS Global Accelerator API.

> Tip
>
> 글로벌 액셀러레이터를 사용하여 웹 응용 프로그램의 성능 및 가용성을 개선하는 방법을 알아보려면 다음 자습형 워크샵을 참조하십시오. AWS Global Accelerator.

글로벌 액셀러레이터는 여러 AWS 리전의 엔드포인트를 지원하는 글로벌 서비스로,AWS 리전 표.

이 장에는 표준 가속기 작성용 튜토리얼과 사용자 지정 라우팅 가속기 작성용 튜토리얼이 포함되어 있습니다. 두 가지 유형의 액셀러레이터에 대한 자세한 내용은 단원을 참조하세요.AWS 글로벌 액셀러레이터의 표준 액셀러레이터 사용 (p. 20)및AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기 사용 (p. 36).

주제

표준 액셀러레이터 시작하기

이 단원에서는 트래픽을 최적의 엔드포인트로 라우팅하는 표준 액셀러레이터를 생성하는 단계에 대해 설명합니다.

작업

시작하기 전에

가속기를 만들기 전에 트래픽을 전달하기 위해 끝점으로 추가할 수 있는 리소스를 하나 이상 만듭니다. 예를 들어 다음 중 하나를 생성합니다.

- 엔드포인트로 추가할 Amazon EC2 인스턴스를 하나 이상 시작합니다. 자세한 내용은 단원을 참조하십시오.EC2 리소스를 생성하고 EC2 인스턴스를 시작합니다.의Linux 인스턴스용 Amazon EC2 사용 설명서.
- 필요에 따라 EC2 인스턴스가 포함된 네트워크 로드 밸런서 또는 애플리케이션 로드 밸런서를 하나 이상 생성합니다. 자세한 내용은 단원을 참조하십시오.Network Load Balancer Application Load Balancer 생성의Network Load Balancer 사용 설명서.

Global Accelerator 액셀러레이터에 추가할 리소스를 생성할 때 다음 사항을 인식하십시오.

- 글로벌 액셀러레이터에서 내부 Application Load Balancer 또는 EC2 인스턴스 엔드포인트를 추가하면 프라이빗 서브넷에서 가상 프라이빗 클라우드 (VPC) 의 엔드포인트로 인터넷 트래픽이 직접 전송되도록 할 수 있습니다. 로드 밸런서 또는 EC2 인스턴스를 포함하는 VPC인터넷 게이트웨이를 추가하여 VPC가 인터넷 트래픽을 허용함을 나타냅니다. 자세한 내용은 AWS Global Accelerator 터의 보안 VPC 연결 (p. 101) 섹션을 참조하세요.
- 글로벌 액셀러레이터를 사용하려면 Route 53 상태 확인 프로그램과 연결된 IP 주소로부터의 인바운드 트래픽이 EC2 인스턴스 또는 엘라스틱 IP 주소 엔드포인트에 대한 상태 확인을 완료할 수 있도록 라우터 및 방화벽 규칙이 필요합니다. Amazon Route 53 상태 확인 프로그램과 연결된 IP 주소 범위에 대한 정보는대상 그룹에 대한 상태 확인의Amazon Route 53 개발자 가이드.

단계 1: 액셀러레이터 생성

가속기를 만들려면 이름을 입력합니다.

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.액셀러레이터 만들기의AWS Global Accelerator API.

액셀러레이터를 생성하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 선택액셀러레이터 생성.
3. 액셀러레이터의 이름을 제공합니다.
4. 필요한 경우 Global Accelerator 리소스를 식별하는 데 도움이 되는 태그를 하나 이상 추가합니다.
5. [Next]를 선택합니다.

단계 2: 리스너 추가

사용자로부터 Global Accelerator 로의 인바운드 연결을 처리하는 수신기를 생성합니다.

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.CreateListener의AWS Global Accelerator.

리스너 생성

1. 에서리스너 추가페이지에서 리스너와 연결할 포트 또는 포트 범위를 입력합니다. 리스너 포트 1-65535에 대해 지원합니다.
2. 입력한 포트에 대한 프로토콜을 하나 이상 선택합니다.
3. 선택적으로 클라이언트 선호도를 사용하도록 선택합니다. 수신기에 대한 클라이언트 선호도는 글로벌 액셀러레이터가 특정 소스 (클라이언트) IP 주소의 연결이 항상 동일한 엔드포인트로 라우팅되도록 보장한다는 것을 의미합니다. 이 동작을 사용하려면 드롭다운 목록에서소스 IP.

   기본값은 입니다.없음로 설정되어 있습니다. 즉, 클라이언트 선호도가 활성화되지 않고 글로벌 가속기가 수신기의 끝점 그룹에 있는 끝점 간에 트래픽을 균등하게 분배합니다.

   자세한 내용은 클라이언트 선호도 (p. 25) 섹션을 참조하세요.
4. 필요에 따라리스너 추가를 클릭하여 추가 리스너를 추가합니다.
5. 리스너 추가를 마치면 [] 를 선택합니다.다음.

단계 3: 엔드포인트 그룹을 추가합니다.

하나 이상의 엔드포인트 그룹을 추가합니다. 각 그룹은 특정 AWS 리전과 연결됩니다.

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.만들기끝점 그룹의AWS Global Accelerator.

엔드포인트 그룹을 추가하려면

1. 에서엔드포인트 그룹을 추가합니다.페이지의 리스너의 섹션에서리전를 드롭 다운 목록에서 선택합니다.
2. 필요에 따라전화 걸기에 0에서 100 사이의 숫자를 입력하여 이 끝점 그룹에 대한 트래픽 비율을 설정합니다. 이 비율은 모든 수신기 트래픽이 아닌 이 끝점 그룹으로 이미 전달된 트래픽에만 적용됩니다. 기본적으로 끝점 그룹의 트래픽 다이얼은 100 (즉, 100%) 으로 설정됩니다.
3. 필요에 따라 사용자 지정 상태 확인 값의 경우상태 확인 구성. 상태 확인 설정을 구성하면 글로벌 액셀러레이터는 EC2 인스턴스 및 엘라스틱 IP 주소 엔드포인트에 대한 상태 확인에 대한 설정을 사용합니다. Network Load Balancer 및 Application Load Balancer 끝점의 경우 글로벌 가속기는 부하 분산 장치 자체에 대해 이미 구성한 상태 확인 설정을 사용합니다. 자세한 내용은 상태 확인 옵션 (p. 28) 섹션을 참조하세요.
4. 필요에 따라엔드포인트 그룹을 추가합니다.이 리스너 또는 다른 리스너의 엔드포인트 그룹을 추가할 수 있습니다.
5. [Next]를 선택합니다.

단계 4: 끝점 추가

특정 끝점 그룹과 연결된 하나 이상의 끝점을 추가합니다. 이 단계는 필요하지 않지만 끝점이 끝점 그룹에 포함되어 있지 않으면 리전의 끝점으로 트래픽이 전달되지 않습니다.

> Note
>
> 프로그래밍 방식으로 가속기를 만드는 경우 끝점 그룹 추가의 일부로 끝점을 추가합니다. 자세한 내용은 단원을 참조하십시오.만들기끝점 그룹의AWS Global Accelerator.

엔드포인트를 추가하려면

1. 에서엔드포인트 생성페이지의 엔드포인트 섹션에서엔드포인트.
2. 필요에 따라Weight에 0에서 255 사이의 숫자를 입력하여 이 엔드포인트로 트래픽을 라우팅하기 위한 가중치를 설정합니다. 엔드포인트에 가중치를 추가할 경우 지정한 비율에 따라 트래픽을 라우팅하도록 Global Accelerator를 구성합니다. 기본적으로 모든 끝점의 가중치는 128입니다. 자세한 내용은 엔드포인트 가중치 (p. 32) 섹션을 참조하세요.
3. 필요에 따라 Application Load Balancer 엔드포인트의 경우클라이언트 IP 주소 보존를 선택한 다음주소 보존. 자세한 내용은 AWS Global Accelerator 클라이언트 IP 주소 보존 (p. 55) 섹션을 참조하세요.
4. 필요에 따라엔드포인트 추가를 클릭하여 더 많은 엔드포인트를 추가합니다.
5. [Next]를 선택합니다.

선택한 후다음을 클릭하면 글로벌 액셀러레이터 대시보드에 가속기가 진행 중이라는 메시지가 표시됩니다. 프로세스가 완료되면 대시보드의 액셀러레이터 상태는활성 상태.

단계 5: 액셀러레이터 테스트

액셀러레이터를 테스트하여 트래픽이 엔드포인트로 전달되는지 확인합니다. 예를 들어 액셀러레이터의 정적 IP 주소 중 하나를 대체하여 다음과 같은 curl 명령을 실행하여 요청이 처리되는 AWS 리전을 표시합니다.

이 기능은 끝점에 대해 서로 다른 가중치를 설정하거나 끝점 그룹의 트래픽 다이얼을 조정하는 경우에 특히 유용합니다.

가속기의 정적 IP 주소 중 하나를 대체하여 다음과 같은 curl 명령을 실행하여 IP 주소를 100 번 호출 한 다음 각 요청이 처리 된 위치를 출력합니다.

```
for ((i=0;i<100;i++)); do  curl http://198.51.100.0/ >> output.txt; done; cat output.txt |
 sort | uniq -c ; rm output.txt;
```

끝점 그룹에서 트래픽 다이얼을 조정한 경우 이 명령을 사용하면 가속기가 올바른 트래픽 비율을 다른 그룹으로 전달하는지 확인할 수 있습니다. 자세한 내용은 다음 블로그 게시물의 자세한 예제를 참조하세요.AWS Global Accelerator 를.

단계 6 (선택 사항): 액셀러레이터 삭제

테스트로 가속기를 만들었거나 가속기를 더 이상 사용하지 않는 경우 해당 가속기를 삭제할 수 있습니다. 콘솔에서 가속기를 비활성화한 다음 삭제할 수 있습니다. 가속기에서 수신기 및 끝점 그룹을 제거할 필요가 없습니다.

콘솔 대신 API 작업을 사용하여 가속기를 삭제하려면 먼저 가속기와 연결된 모든 수신기 및 끝점 그룹을 제거하고 비활성화해야 합니다. 자세한 내용은 단원을 참조하십시오.삭제액셀러레이터에서 하는 작업을AWS Global Accelerator.

끝점 또는 끝점 그룹을 제거하거나 가속기를 삭제할 때 다음 사항에 유의하십시오.

- 가속기를 만들면 글로벌 가속기에서 두 개의 고정 IP 주소 집합을 제공합니다. 가속기를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않는 경우에도 IP 주소가 있는 동안 가속기에 할당됩니다. 그러나, 때삭제가속기를 사용하는 경우 가속기에 할당된 고정 IP 주소가 손실되므로 더 이상 이 주소를 사용하여 트래픽을 라우팅할 수 없습니다. 실수로 가속기를 삭제하지 않도록 권한이 있는지 확인하는 것이 좋습니다. 글로벌 가속기와 함께 IAM 정책 (예: 태그 기반 권한) 을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.
- 글로벌 가속기의 엔드포인트 그룹에서 EC2 인스턴스를 제거하기 전에 EC2 인스턴스를 종료한 다음 동일한 프라이빗 IP 주소로 다른 인스턴스를 생성하고 상태 확인을 통과하면 글로벌 액셀러레이터는 트래픽을 새 엔드포인트로 라우팅합니다. 이런 일이 발생하지 않도록 하려면 인스턴스를 종료하기 전에 엔드포인트 그룹에서 EC2 인스턴스를 제거합니다.

액셀러레이터를 삭제하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 삭제하려는 액셀러레이터를 선택합니다.
3. [Edit]를 선택합니다.
4. 선택액셀러레이터 비활성화를 선택한 다음Save.
5. 삭제하려는 액셀러레이터를 선택합니다.
6. 선택액셀러레이터 삭제.
7. 확인 대화 상자에서 삭제를 선택합니다.

사용자 지정 라우팅 액셀러레이터 시작하기

이 섹션에서는 가상 프라이빗 클라우드 (VPC) 서브넷 엔드포인트의 Amazon EC2 인스턴스 대상으로 트래픽을 확정적으로 라우팅하는 사용자 지정 라우팅 가속기를 생성하는 단계를 제공합니다.

작업

시작하기 전에

사용자 지정 라우팅 가속기를 만들기 전에 트래픽을 전달하기 위해 끝점으로 추가할 수 있는 리소스를 만듭니다. 사용자 지정 라우팅 가속기 엔드포인트는 가상 프라이빗 클라우드 (VPC) 서브넷이어야 하며, 여기에는 여러 Amazon EC2 인스턴스가 포함될 수 있습니다. 리소스 생성 지침은 다음을 참조하십시오.

- VPC 서브넷을 생성합니다. 자세한 내용은 단원을 참조하십시오.VPC 생성 및 구성의AWS Directory Service 관리 가이드.
- VPC 하나 이상의 Amazon EC2 인스턴스를 시작합니다. 자세한 내용은 단원을 참조하십시오.EC2 리소스를 생성하고 EC2 인스턴스를 시작합니다.의Linux 인스턴스용 Amazon EC2 사용 설명서.

Global Accelerator 액셀러레이터에 추가할 리소스를 생성할 때 다음 사항을 인식하십시오.

- 글로벌 액셀러레이터에서 EC2 인스턴스 엔드포인트를 추가하면 프라이빗 서브넷에서 해당 엔드포인트를 대상으로 VPC의 엔드포인트에서 직접 송수신할 수 있습니다. EC2 인스턴스를 포함하는 VPC인터넷 게이트웨이를 추가하여 VPC 가 인터넷 트래픽을 허용함을 나타냅니다. 자세한 내용은 AWS Global Accelerator 터의 보안 VPC 연결 (p. 101) 섹션을 참조하세요.

단계 1: 사용자 지정 라우팅 액셀러레이터 생성

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.사용자 정의 라우팅가속기 만들기의AWS Global Accelerator.

액셀러레이터를 생성하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 액셀러레이터의 이름을 제공합니다.
3. 용액셀러레이터 유형를 선택한 다음사용자 지정 라우팅.
4. 필요한 경우 Accelerator 리소스를 쉽게 식별할 수 있도록 하나 이상의 태그를 추가합니다.
5. 선택다음를 사용하여 리스너, 엔드포인트 그룹 및 VPC 서브넷 엔드포인트를 추가합니다.

단계 2: 리스너 추가

사용자로부터 Global Accelerator 로의 인바운드 연결을 처리하는 수신기를 생성합니다.

리스너를 생성할 때 지정하는 범위는 사용자 지정 라우팅 가속기와 함께 사용할 수 있는 리스너 포트 및 대상 IP 주소 조합 수를 정의합니다. 유연성을 극대화하려면 큰 포트 범위를 지정하는 것이 좋습니다. 지정하는 각 리스너 포트 범위에는 최소 16개의 포트가 포함되어야 합니다.

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.사용자 정의 라우팅 리스너 생성의AWS Global Accelerator.

리스너 생성

1. 에서리스너 추가페이지에서 리스너와 연결할 포트 또는 포트 범위를 입력합니다. 리스너 포트 1-65535에 대해 지원합니다.
2. 입력한 포트에 대한 프로토콜을 하나 이상 선택합니다.
3. 필요에 따라리스너 추가를 클릭하여 추가 리스너를 추가합니다.
4. 리스너 추가를 마치면 [] 를 선택합니다.다음.

단계 3: 엔드포인트 그룹을 추가합니다.

하나 이상의 엔드포인트 그룹을 추가합니다. 각 그룹은 특정 AWS 리전과 연결됩니다. 각 끝점 그룹에 대해 포트 범위 및 프로토콜 집합을 하나 이상 지정합니다. 글로벌 액셀러레이터는 이를 사용하여 해당 지역의 서브넷에 있는 Amazon EC2 인스턴스로 트래픽을 보냅니다.

제공하는 각 포트 범위에 대해 사용할 프로토콜도 지정합니다. UDP, TCP 또는 UDP 및 TCP 둘 다 사용할 수 있습니다.

> Note
>
> 콘솔 대신 API 작업을 사용하여 이 작업을 완료하려면 단원을 참조하십시오.사용자 지정 라우팅끝점 그룹 만들기의AWS Global Accelerator.

엔드포인트 그룹을 추가하려면

1. 에서엔드포인트 그룹을 추가합니다.페이지의 리스너의 섹션에서리전.
2. 용포트 및 프로토콜에 Amazon EC2 인스턴스의 포트 범위 및 프로토콜을 입력합니다.

   - a를 입력합니다.포트및포트를 사용하여 포트 범위를 지정할 수 있습니다.
   - 각 포트 범위에 대해 해당 범위의 프로토콜을 지정합니다.

   포트 범위는 리스너 포트 범위의 하위 집합일 필요는 없지만 리스너 포트 범위에 지정한 총 포트 수를 지원하기에 충분한 총 포트가 있어야 합니다.
3. 저장을 선택합니다.
4. 필요에 따라엔드포인트 그룹을 추가합니다.이 리스너 또는 다른 리스너의 엔드포인트 그룹을 추가할 수 있습니다.
5. [Next]를 선택합니다.

단계 4: VPC 서브넷 엔드포인트 추가

이 리전 엔드포인트 그룹에 하나 이상의 VPC (가상 프라이빗 클라우드) 서브넷 엔드포인트를 추가합니다. 사용자 지정 라우팅 가속기의 끝점은 사용자 지정 라우팅 가속기를 통해 트래픽을 수신할 수 있는 VPC 서브넷을 정의합니다. 각 서브넷에는 하나 이상의 Amazon EC2 인스턴스 대상이 포함될 수 있습니다.

VPC 서브넷 엔드포인트를 추가하면 글로벌 액셀러레이터는 서브넷의 대상 EC2 인스턴스 IP 주소로 트래픽을 라우팅하는 데 사용할 수 있는 새 포트 매핑을 생성합니다. 그런 다음 글로벌 액셀러레이터 API를 사용하여 서브넷에 대한 모든 포트 매핑의 정적 목록을 가져오고 매핑을 사용하여 특정 EC2 인스턴스로 트래픽을 결정적으로 전달할 수 있습니다.

> Note
>
> 이 단계에서는 콘솔에 끝점을 추가하는 방법을 보여 줍니다. 프로그래밍 방식으로 가속기를 만드는 경우 끝점 그룹이 있는 끝점을 추가합니다. 자세한 내용은 단원을 참조하십시오.사용자 지정 라우팅끝점 그룹 만들기의AWS Global Accelerator.

엔드포인트를 추가하려면

1. 에서끝점 추가페이지의 엔드포인트를 추가할 엔드포인트 그룹에 대한 섹션에서엔드포인트.
2. 선택적으로 다음 중 하나를 수행하여 서브넷의 EC2 인스턴스 대상에 대한 트래픽을 활성화합니다.

   - 트래픽이 서브넷의 모든 EC2 엔드포인트 및 포트로 전달되도록 허용하려면모든 트래픽 허용
   - 서브넷의 특정 EC2 엔드포인트 및 포트에 대한 트래픽을 허용하려면특정 대상 소켓 주소에 대한 트래픽 허용. 그런 다음 허용할 IP 주소와 포트 또는 포트 범위를 지정합니다. 마지막으로, Select다음 목적지 허용.

   기본적으로 서브넷 끝점에 대한 트래픽은 허용되지 않습니다. 트래픽을 허용하는 옵션을 선택하지 않으면 서브넷의 모든 대상에 대한 트래픽이 거부됩니다.

   Note

   서브넷의 특정 EC2 인스턴스 및 포트에 대한 트래픽을 활성화하려는 경우 프로그래밍 방식으로 이를 수행할 수 있습니다. 자세한 내용은 단원을 참조하십시오.사용자 지정 라우팅 트래픽 허용의AWS Global Accelerator.
3. [Next]를 선택합니다.

선택한 후다음의 글로벌 가속기 대시보드에서 가속기가 진행 중이라는 메시지가 표시됩니다. 프로세스가 완료되면 대시보드의 액셀러레이터 상태는활성 상태.

5단계 (선택 사항): 액셀러레이터 삭제

테스트로 가속기를 만들었거나 가속기를 더 이상 사용하지 않는 경우 해당 가속기를 삭제할 수 있습니다. 콘솔에서 가속기를 비활성화한 다음 삭제할 수 있습니다. 가속기에서 수신기 및 끝점 그룹을 제거할 필요가 없습니다.

콘솔 대신 API 작업을 사용하여 가속기를 삭제하려면 먼저 가속기와 연결된 모든 수신기 및 끝점 그룹을 제거하고 비활성화해야 합니다. 자세한 내용은 단원을 참조하십시오.삭제사용자 정의 라우팅가속기에서 하는 작업을AWS Global Accelerator.

액셀러레이터를 삭제할 때는 다음 사항을 인식하십시오.

- 가속기를 만들면 글로벌 가속기에서 두 개의 고정 IP 주소 집합을 제공합니다. 가속기를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않는 경우에도 IP 주소가 있는 동안 가속기에 할당됩니다. 그러나, 때삭제가속기를 사용하는 경우 가속기에 할당된 고정 IP 주소가 손실되므로 더 이상 이 주소를 사용하여 트래픽을 라우팅할 수 없습니다. 실수로 가속기를 삭제하지 않도록 권한이 있는지 확인하는 것이 좋습니다. 글로벌 가속기와 함께 태그 기반 권한과 같은 IAM 정책을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

액셀러레이터를 삭제하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 삭제하려는 액셀러레이터를 선택합니다.
3. [Edit]를 선택합니다.
4. 선택액셀러레이터 비활성화를 선택한 다음Save.
5. 삭제하려는 액셀러레이터를 선택합니다.
6. 선택액셀러레이터 삭제.
7. 확인 대화 상자에서 삭제를 선택합니다.

AWS 글로벌 액셀러레이터와 함께 사용할 수 있는 일반적인 작업

이 섹션에서는 글로벌 액셀러레이터 리소스와 함께 사용할 수 있는 일반적인 AWS Global Accelerator 작업과 관련 문서 링크를 나열합니다.

표준 리소스와 함께 사용할 작업

다음 표에는 글로벌 액셀러레이터 표준 액셀러레이터와 함께 사용할 수 있는 일반적인 글로벌 액셀러레이터 작업과 관련 문서에 대한 링크가 나와 있습니다.

작업	글로벌 가속기 콘솔 사용	Global Accelerator API 사용
표준 액셀러레이터 만들기	표준 액셀러레이터 시작하기 (p. 11)섹션을 참조하십시오.	`CreateAccelerator`섹션을 참조하십시오.
표준 액셀러레이터를 위한 수신기 생성	AWS 글로벌 액셀러레이터의 표준 액셀러레이터 수신기 (p. 24)섹션을 참조하십시오.	`CreateListener`섹션을 참조하십시오.
표준 가속기에 대한 끝점 그룹 만들기	AWS Global Accelerator 표준 가속기에 대한 엔드포인트 그룹 (p. 25)섹션을 참조하십시오.	`CreateEndpointGroup`섹션을 참조하십시오.
표준 가속기 업데이트	AWS Global Accelerator의 표준 액셀러레이터 (p. 20)섹션을 참조하십시오.	`UpdateAccelerator`섹션을 참조하십시오.
액셀러레이터 나열	액셀러레이터 보기 (p. 22)섹션을 참조하십시오.	`ListAccelerator`섹션을 참조하십시오.
액셀러레이트에 대한 모든 정보 보기	액셀러레이터 보기 (p. 22)섹션을 참조하십시오.	`DescribeAccelerator`섹션을 참조하십시오.
액셀러레이터 삭제	표준 액셀러레이터 만들기 또는 업데이트 (p. 21)섹션을 참조하십시오.	`DeleteAccelerator`섹션을 참조하십시오.

사용자 지정 라우팅 리소스와 함께 사용할 작업

다음 표에는 사용자 지정 라우팅 가속기와 함께 사용할 수 있는 일반적인 글로벌 액셀러레이터 작업과 관련 문서에 대한 링크가 나와 있습니다.

작업	글로벌 가속기 콘솔 사용	Global Accelerator API 사용
사용자 지정 라우팅 액셀러레이터 생성	사용자 지정 라우팅 액셀러레이터 시작하기 (p. 14)섹션을 참조하십시오.	`CreateCustomRoutingAccelerator`섹션을 참조하십시오.

작업	글로벌 가속기 콘솔 사용	Global Accelerator API 사용
사용자 지정 라우팅 액셀러레이터를 위한 수신기 생성	AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 위한 리스너 (p. 43)섹션을 참조하십시오.	CreateCustomRoutingListener섹션을 참조하십시오.
사용자 지정 라우팅 액셀러레이터를 위한 엔드포인트 그룹 생성	AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 위한 엔드포인트 그룹 (p. 44)섹션을 참조하십시오.	CreateCustomRoutingEndpointGroup섹션을 참조하십시오.
사용자 지정 라우팅 가속기 업데이트	AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기 (p. 41)섹션을 참조하십시오.	UpdateCustomRoutingAccelerator섹션을 참조하십시오.
사용자 지정 라우팅 가속기 나열	사용자 지정 라우팅 가속기 보기 (p. 42)섹션을 참조하십시오.	ListCustomRoutingAccelerator섹션을 참조하십시오.
사용자 지정 라우팅 액셀러레이기에 대한 모든 정보 보기	사용자 지정 라우팅 가속기 보기 (p. 42)섹션을 참조하십시오.	DescribeCustomRoutingAccelerator섹션을 참조하십시오.
사용자 지정 라우팅 가속기 삭제	사용자 지정 라우팅 액셀러레이터 만들기 또는 업데이트 (p. 41)섹션을 참조하십시오.	DeleteCustomRoutingAccelerator섹션을 참조하십시오.
사용자 지정 라우팅 액셀러레이터를 위한 정적 포트 매핑 가져오기	해당 사항 없음	ListCustomRoutingPortMappings섹션을 참조하십시오.
사용자 지정 라우팅 가속기에서 서브넷에 대한 모든 대상 트래픽 허용	VPC 서브넷 엔드포인트 추가, 편집 또는 제거 (p. 46)섹션을 참조하십시오.	AllowCustomRoutingTraffic섹션을 참조하십시오.
사용자 지정 라우팅 가속기에서 서브넷에 대한 모든 대상 트래픽 거부	VPC 서브넷 엔드포인트 추가, 편집 또는 제거 (p. 46)섹션을 참조하십시오.	DenyCustomRoutingTraffic섹션을 참조하십시오.
사용자 지정 라우팅 가속기에서 특정 대상에 대한 트래픽 허용	VPC 서브넷 엔드포인트 추가, 편집 또는 제거 (p. 46)섹션을 참조하십시오.	AllowCustomRoutingTraffic섹션을 참조하십시오.
사용자 지정 라우팅 가속기에서 특정 대상에 대한 트래픽 거부	VPC 서브넷 엔드포인트 추가, 편집 또는 제거 (p. 46)섹션을 참조하십시오.	DenyCustomRoutingTraffic섹션을 참조하십시오.

AWS 글로벌 액셀러레이터의 표준 액셀러레이터 사용

이 장에는 AWS 글로벌 액셀러레이터에서 표준 가속기를 만들기 위한 절차와 권장 사항이 포함되어 있습니다. 글로벌 액셀러레이터는 표준 가속기를 사용하여 트래픽에 가장 가까운 정상 엔드포인트를 선택합니다.

사용자 지정 응용 프로그램 논리를 사용하여 한 명 이상의 사용자를 여러 끝점 중에서 특정 끝점으로 안내하려면 사용자 지정 라우팅 가속기를 만듭니다. 자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기 사용 (p. 36) 섹션을 참조하세요.

표준 가속기를 설정하려면 다음 작업을 수행합니다.

1. 가속기를 만들고 표준 가속기 옵션을 선택합니다.
2. 특정 포트 또는 포트 범위 집합이 있는 리스너를 추가하고 수락할 프로토콜을 선택합니다. TCP, UDP 또는 둘 다를 사용할 수 있습니다.
3. 엔드포인트 리소스가 있는 각 AWS 리전마다 하나씩, 하나 이상의 엔드포인트 그룹을 추가합니다.
4. 끝점 그룹에 끝점을 하나 이상 추가합니다. 필수 사항은 아니지만 엔드포인트가 없으면 트래픽이 라우팅되지 않습니다. 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다.

다음 섹션에서는 표준 가속기, 수신기, 끝점 그룹 및 끝점 작업에 대해 단계별로 설명합니다.

주제

AWS Global Accelerator의 표준 액셀러레이터

A표준 AcceleratorAWS Global Accelerator 가 트래픽을 AWS Accelerator에 최적의 엔드포인트로 유도하여 전 세계 사용자가 있는 인터넷 애플리케이션의 가용성과 성능을 향상시킵니다. 각 가속기에는 하나 이상의 수신기가 포함됩니다. 리스너는 구성하는 프로토콜 (또는 프로토콜) 및 포트 (또는 포트 범위) 에 따라 클라이언트에서 글로벌 가속기로의 인바운드 연결을 처리합니다.

가속기를 만들면 기본적으로 글로벌 가속기에서 두 개의 고정 IP 주소 집합을 제공합니다. AWS (BYOIP) 에 고유한 IP 주소 범위를 가져오는 경우 액셀러레이터와 함께 사용할 사용자 풀에서 고정 IP 주소를 할당할 수 있습니다. 자세한 내용은 AWS Global Accelerator 고유 IP 주소 가져오기 (p. 49) 섹션을 참조하세요.

> Important
>
> 가속기를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않는 경우에도 IP 주소가 있는 동안 가속기에 할당됩니다. 그러나, 때삭제가속기를 사용하는 경우 가속기에 할당된 글로벌 가속기 고정 IP 주소가 손실되므로 더 이상 이 주소를 사용하여 트래픽을 라우팅할 수 없습니다. 실수로 가속기를 삭제하지 않도록 권한이 있는지 확인하는 것이 좋습니다. 글로벌 가속기와 함께 IAM 정책 (예: 태그 기반 권한) 을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

이 섹션에서는 글로벌 가속기 콘솔에서 표준 가속기를 만들거나 편집하거나 삭제하는 방법에 대해 설명합니다. Global Accelerator에 API 작업을 사용하려면AWS Global Accelerator API.

주제

표준 액셀러레이터 만들기 또는 업데이트

이 단원에서는 본체에서 표준 액셀러레이터를 만들거나 업데이트하는 방법에 대해 설명합니다. 전역 가속기를 프로그래밍 방식으로 사용하려면AWS Global Accelerator API.

표준 액셀러레이터를 생성하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 선택액셀러레이터 만들기.
3. 액셀러레이터의 이름을 제공합니다.
4. 용액셀러레이터 유형를 선택한 다음표준.
5. 필요에 따라 자체 IP 주소 범위를 AWS (BYOIP) 로 가져온 경우 가속기의 고정 IP 주소를 각 주소 풀에서 하나씩 지정할 수 있습니다. 가속기에 대한 두 개의 정적 IP 주소 각각에 대해 이 옵션을 선택합니다.
   - 각 고정 IP 주소에 대해 사용할 IP 주소 풀을 선택합니다.

     Note

     각 고정 IP 주소에 대해 다른 IP 주소 풀을 선택해야 합니다. 글로벌 액셀러레이터는 고가용성을 위해 각 주소 범위를 다른 네트워크 영역에 할당하기 때문입니다.
   - 고유한 IP 주소 풀을 선택한 경우 풀에서 특정 IP 주소도 선택합니다. 기본 Amazon IP 주소 풀을 선택하면 글로벌 가속기가 가속기에 특정 IP 주소를 할당합니다.
6. 필요에 따라 액셀러레이터 리소스를 쉽게 식별할 수 있도록 태그를 하나 이상 추가합니다.
7. 선택다음를 사용하여 수신기, 끝점 그룹 및 끝점을 추가합니다.

표준 액셀러레이터를 편집하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 액셀러레이터 목록에서 액셀러레이터를 선택한 다음Edit.
3. 에서액셀러레이터 편집페이지에서 원하는 대로 변경합니다. 예를 들어 가속기가 더 이상 트래픽을 허용하거나 라우팅하지 않도록 하거나 삭제할 수 있도록 가속기를 비활성화할 수 있습니다. 또는 가속기가 비활성화되어 있으면 활성화할 수 있습니다.
4. [Save changes]를 선택합니다.

액셀러레이터를 삭제하려면

테스트로 가속기를 만들었거나 가속기를 더 이상 사용하지 않는 경우 해당 가속기를 삭제할 수 있습니다. 콘솔에서 가속기를 비활성화한 다음 삭제할 수 있습니다. 가속기에서 수신기 및 끝점 그룹을 제거할 필요가 없습니다.

콘솔 대신 API 작업을 사용하여 가속기를 삭제하려면 먼저 가속기와 연결된 모든 수신기 및 끝점 그룹을 제거한 다음 비활성화해야 합니다. 자세한 내용은 단원을 참조하십시오.삭제액셀러레이터작업 매니저에서AWS Global Accelerator API.

액셀러레이터를 비활성화하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 목록에서 사용하지 않도록 설정할 액셀러레이터를 선택합니다.
3. [Edit]를 선택합니다.
4. 선택액셀러레이터 비활성화를 선택한 다음Save.

액셀러레이터를 삭제하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 목록에서 삭제할 액셀러레이터를 선택합니다.
3. 삭제를 선택합니다.

   Note

   액셀러레이터를 사용하지 않도록 설정하지 않았으면삭제를 사용할 수 없음.
4. 확인 대화 상자에서 삭제를 선택합니다.

   Important

   가속기를 삭제하면 가속기에 할당된 고정 IP 주소가 손실되므로 더 이상 해당 가속기를 사용하여 트래픽을 라우팅할 수 없습니다.

액셀러레이터 보기

콘솔에서 액셀러레이터에 대한 정보를 볼 수 있습니다. 프로그래밍 방식으로 가속기에 대한 설명을 보려면목록 가속기및DescribeAccelerator의AWS Global Accelerator API.

액셀러레이터에 대한 정보를 보려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 가속기에 대한 세부 정보를 보려면 목록에서 가속기를 선택한 다음보기:.

로드 밸런서를 만들 때 가속기 추가

AWS Management Console에서 Application Load Balancer 서를 생성할 때 필요에 따라액셀러레이터를 동시에 추가. Elastic Load Balancing 과 글로벌 가속기가 함께 작동하여 가속기를 투명하게 추가합니다. 부하 분산 장치를 엔드포인트로 사용하여 계정에 가속기가 생성됩니다. 액셀러레이터를 사용하면 고정 IP 주소가 제공되며 응용 프로그램의 가용성과 성능이 향상됩니다.

Important

액셀러레이터를 만들려면 올바른 권한이 있어야 합니다. 자세한 내용은 콘솔 액세스, 인증 관리 및 액세스 제어에 필요한 권한 (p. 79) 섹션을 참조하세요.

가속기 구성 및 보기

트래픽을 가속기의 고정 IP 주소 또는 DNS 이름으로 보내려면 DNS 구성을 업데이트해야 합니다. 트래픽은 구성 변경이 완료될 때까지 가속기를 통해 로드 밸런서로 이동하지 않습니다.

Amazon EC2 콘솔에서 글로벌 액셀러레이터 추가 기능을 선택하여 로드 밸런서를 생성한 후통합 서비스탭을 클릭하여 액셀러레이터의 고정 IP 주소와 Domain Name System (DNS) 이름을 확인합니다. 이 정보를 사용하여 AWS 글로벌 네트워크를 통해 로드 밸런서로 사용자 트래픽을 라우팅합니다. 액셀러레이터에 할당된 DNS 이름에 대한 자세한 내용은AWS Global Accelerator 터의 DNS 주소 지정 및 사용자 지정 도메인 (p. 48).

다음과 같이 가속기를 보고 구성할 수 있습니다.Global Accelerator 로 이동AWS Management Console에서. 예를 들어 계정과 연결된 가속기를 보거나 가속기에 부하 분산 장치를 추가할 수 있습니다. 자세한 내용은 액셀러레이터 보기 (p. 22) 및 표준 액셀러레이터 만들기 또는 업데이트 (p. 21) 섹션을 참조하세요.

요금

AWS Global Accelerator 를 사용하면 사용한 만큼만 지불하면 됩니다. 계정의 각 액셀러레이터별로 시간당 요금 및 데이터 전송 비용이 청구됩니다. 자세한 내용은 단원을 참조하십시오.AWS Global Accelerator 가.

액셀러레이터 사용 중지

글로벌 액셀러레이터를 통해 로드 밸런서로 트래픽 라우팅을 중지하려면 다음을 수행합니다.

1. 트래픽을 로드 밸런서로 직접 가리키도록 DNS 구성을 업데이트합니다.
2. 가속기에서 로드 밸런서를 삭제합니다. 자세한 내용은 단원을 참조하십시오.끝점을 제거하려면in표준 끝점 추가, 편집 또는 제거 (p. 30).
3. 액셀러레이터를 삭제합니다. 자세한 내용은 액셀러레이터를 삭제하려면 (p. 21) 섹션을 참조하세요.

지역 정적 IP 주소 대신 전역 정적 IP 주소 사용

Amazon EC2 인스턴스와 같은 AWS 리소스 앞에 고정 IP 주소를 사용하려는 경우 몇 가지 옵션이 있습니다. 예를 들어 단일 AWS 리전의 Amazon EC2 인스턴스 또는 네트워크 인터페이스와 연결할 수 있는 고정 IPv4 주소인 엘라스틱 IP 주소를 할당할 수 있습니다.

글로벌 오디언스가 있는 경우 글로벌 액셀러레이터를 사용하여 액셀러레이터를 만들어 전 세계의 AWS 엣지 로케이션에서 발표되는 두 개의 글로벌 고정 IP 주소를 받을 수 있습니다. Amazon EC2 인스턴스, 네트워크 로드 밸런서 및 애플리케이션 로드 밸런서를 비롯한 하나 또는 여러 리전에서 애플리케이션에 대해 이미 AWS 리소스를 설정한 경우 글로벌 액셀러레이터를 글로벌 고정 IP 주소로 쉽게 추가할 수 있습니다.

글로벌 액셀러레이터에서 프로비저닝한 글로벌 정적 IP 주소를 사용하도록 선택하면 애플리케이션의 가용성과 성능을 향상시킬 수도 있습니다. 글로벌 액셀러레이터를 사용하면 정적 IP 주소가 사용자와 가장 가까운 에지에서 AWS 글로벌 네트워크로 들어오는 트래픽을 허용합니다. AWS 네트워크에서 트래픽이 발생하는 시간을 최대화하면 더 빠르고 더 나은 고객 경험을 제공할 수 있습니다. 자세한 내용은 AWS Global Accelerator (p. 3) 섹션을 참조하세요.

AWS 관리 콘솔에서 액셀러레이터를 추가하거나 AWS CLI 또는 SDK에서 API 작업을 사용하여 액셀러레이터를 추가할 수 있습니다. 자세한 내용은 표준 액셀러레이터 만들기 또는 업데이트 (p. 21) 섹션을 참조하세요.

액셀러레이터를 추가할 때 다음 사항에 유의하십시오.

- 가속기를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않더라도 글로벌 가속기에서 프로비저닝한 글로벌 정적 IP 주소는 가속기가 존재하는 한 사용자에게 할당된 상태로 유지됩니다. 그러나 가속기를 삭제하면 할당된 고정 IP 주소가 손실됩니다. 자세한 내용은 액셀러레이터를 삭제하려면 (p. 21) 섹션을 참조하세요.
- Global Accelerator를 사용하면 사용한 만큼만 지불하면 됩니다. 계정의 각 액셀러레이터별로 시간당 요금 및 데이터 전송 비용이 청구됩니다. 자세한 내용은 단원을 참조하십시오.AWS Global Accelerator 가.

AWS 글로벌 액셀러레이터의 표준 액셀러레이터 수신기

AWS Global Accelerator 사용하면 지정한 포트 및 프로토콜을 기반으로 클라이언트의 인바운드 연결을 처리하는 리스너를 추가할 수 있습니다. 리스너는 TCP, UDP 또는 TCP 및 UDP 프로토콜을 모두 지원합니다.

표준 액셀러레이터를 생성할 때 표준 리스너를 정의하면 언제라도 더 많은 리스너를 추가할 수 있습니다. 각 리스너를 하나 이상의 엔드포인트 그룹과 연결하고 각 엔드포인트 그룹을 하나의 AWS 리전에 연결합니다.

주제

표준 리스너 추가, 편집 또는 제거

이 단원에서는 AWS Global Accelerator 에서 리스너를 사용하는 방법에 대해 설명합니다. 콘솔 대신 API 작업을 사용하여 이러한 작업을 수행하려면`CreateListener`,`UpdateListener`, 및`DeleteListener`의AWS Global Accelerator.

리스너를 추가하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 리스너 추가를 선택합니다.
4. 에리스너 추가페이지에서 리스너와 연결할 포트 또는 포트 범위를 입력합니다. 리스너는 포트 1-65535을 지원합니다.
5. 입력한 포트에 대한 프로토콜을 선택합니다.
6. 선택적으로 클라이언트 선호도를 사용하도록 선택합니다. 수신기에 대한 클라이언트 선호도는 글로벌 가속기를 통해 특정 소스 (클라이언트) IP 주소의 연결이 항상 동일한 끝점으로 라우팅됩니다. 이 동작을 사용하려면 드롭다운 목록에서소스 IP.

   기본값은 입니다.없음로 설정되어 있습니다. 즉, 클라이언트 선호도가 활성화되지 않고 글로벌 가속기가 수신기의 끝점 그룹에 있는 끝점 간에 트래픽을 균등하게 분배합니다.

   자세한 내용은 클라이언트 선호도 (p. 25) 섹션을 참조하세요.
7. 리스너 추가를 선택합니다.

표준 리스너를 편집하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 리스너를 선택한 다음리스너 편집.
4. 에리스너 편집페이지에서 리스너와 연결할 포트, 포트 범위 또는 프로토콜을 변경합니다.
5. 선택적으로 클라이언트 선호도를 사용하도록 선택합니다. 수신기에 대한 클라이언트 선호도는 글로벌 가속기를 통해 특정 소스 (클라이언트) IP 주소의 연결이 항상 동일한 끝점으로 라우팅됩니다. 이 동작을 사용하려면 드롭다운 목록에서소스 IP.

   기본값은 입니다.없음로 설정되어 있습니다. 즉, 클라이언트 선호도가 활성화되지 않고 글로벌 가속기가 수신기의 끝점 그룹에 있는 끝점 간에 트래픽을 균등하게 분배합니다.

자세한 내용은 클라이언트 선호도 (p. 25) 섹션을 참조하세요.

6. 저장을 선택합니다.

리스너를 제거하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 리스너를 선택한 다음제거.
4. 확인 대화 상자에서제거.

클라이언트 선호도

표준 가속기와 함께 사용하는 상태 저장 응용 프로그램이 있는 경우 글로벌 가속기가 특정 소스 (클라이언트) IP 주소에 있는 사용자의 모든 요청을 동일한 끝점 리소스로 보내도록 선택하여 클라이언트 선호도를 유지할 수 있습니다.

기본적으로 표준 리스너에 대한 클라이언트 선호도는없음및 글로벌 가속기는 수신기에 대한 끝점 그룹의 끝점 간에 트래픽을 균등하게 분산합니다.

Global Accelerator는 일관된 흐름 해싱 알고리즘을 사용하여 사용자 연결에 가장 적합한 엔드포인트를 선택합니다. 글로벌 액셀러레이터 리소스에 대한 클라이언트 선호도를없음에서 Global Accelerator는 5튜플 속성 (소스 IP, 소스 포트, 소스 포트, 대상 포트 및 프로토콜) 을 사용하여 해시 값을 선택합니다. 다음으로 최상의 성능을 제공하는 엔드포인트를 선택합니다. 지정된 클라이언트가 다른 포트를 사용하여 Global Accelerator에 연결하는 경우 이 설정을 지정한 경우 Global Accelerator는 항상 동일한 엔드포인트로 라우팅되도록 할 수 없습니다.

소스 IP 주소로 식별되는 특정 사용자를 연결할 때마다 동일한 엔드포인트로 라우팅하여 클라이언트 선호도를 유지하려면 클라이언트 선호도를소스 IP. 이 옵션을 지정하면 Global Accelerator는 2튜플 속성 (소스 IP 및 대상 IP) 을 사용하여 해시 값을 선택하고 사용자가 연결할 때마다 동일한 엔드포인트로 라우팅합니다. 전역 가속기는 선택한 끝점 그룹 다음에 클라이언트 선호도를 적용합니다.

AWS Global Accelerator 표준 가속기에 대한 엔드포인트 그룹

엔드포인트 그룹은 AWS Global Accelerator 에 등록된 엔드포인트로 요청을 라우팅합니다. 표준 가속기에 수신기를 추가할 때 글로벌 가속기에서 트래픽을 전달하기 위한 끝점 그룹을 지정합니다. 엔드포인트 그룹과 이 그룹의 모든 엔드포인트는 하나의 AWS 리전에 속해야 합니다. 파란색/녹색 배포 테스트와 같이 다른 목적을 위해 서로 다른 끝점 그룹을 추가할 수 있습니다.

글로벌 액셀러레이터는 클라이언트의 위치 및 엔드포인트 그룹의 상태에 따라 표준 가속기의 엔드포인트 그룹으로 트래픽을 보냅니다. 원하는 경우 엔드포인트 그룹에 전송할 트래픽의 비율을 설정할 수도 있습니다. 트래픽 다이얼을 사용하여 그룹에 대한 트래픽을 증가 (전화 접속) 또는 감소 (다이얼 다운) 하면 됩니다. 백분율은 글로벌 액셀러레이터가 이미 끝점 그룹으로 전달하고 있는 트래픽에만 적용되며 수신기로 들어오는 모든 트래픽은 적용되지 않습니다.

각 끝점 그룹에 대해 전역 가속기에 대한 상태 확인 설정을 정의할 수 있습니다. 상태 확인 설정을 업데이트하면 Amazon EC2 인스턴스 및 엘라스틱 IP 주소 엔드포인트의 폴링 및 상태 확인 요구 사항을 변경할 수 있습니다. Network Load Balancer 및 Application Load Balancer 엔드포인트의 경우 Elastic Load Balancing 콘솔에서 상태 확인 설정을 구성합니다.

글로벌 액셀러레이터는 표준 끝점 그룹에 포함된 모든 끝점의 상태를 지속적으로 모니터링하고 정상적인 활성 끝점에만 요청을 라우팅합니다. 트래픽을 라우팅할 정상 엔드포인트가 없는 경우 글로벌 액셀러레이터는 요청을 모든 엔드포인트로 라우팅합니다.

이 섹션에서는 AWS Global Accelerator 콘솔에서 표준 가속기에 대한 엔드포인트 그룹을 사용하는 방법에 대해 설명합니다. AWS Global Accelerator 에서 API 작업을 사용하려면 단원을 참조하십시오.AWS Global Accelerator.

주제

표준 끝점 그룹 추가, 편집 또는 제거

AWS Global Accelerator 콘솔에서 엔드포인트 그룹을 사용하거나 API 작업을 사용하여 작업을 수행합니다. 언제든지 엔드포인트를 추가하거나 엔드포인트 그룹에서 엔드포인트를 제거할 수 있습니다.

이 단원에서는 AWS Global Accelerator 콘솔에서 표준 엔드포인트 그룹을 사용하는 방법에 대해 설명합니다. AWS Global Accelerator에서 API 작업을 사용하려면AWS Global Accelerator.

표준 엔드포인트 그룹을 추가하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 을 선택합니다.리스너 ID에서 엔드포인트 그룹을 추가할 리스너의 ID를 선택합니다.
4. 선택엔드포인트 그룹을 추가합니다..
5. 리스너 섹션에서 드롭다운 목록에서 하나를 선택하여 끝점 그룹의 Region을 지정합니다.
6. 필요에 따라트래픽 다이얼에 0에서 100 사이의 숫자를 입력하여 이 끝점 그룹에 대한 트래픽 비율을 설정합니다. 이 비율은 모든 수신기 트래픽이 아닌 이 끝점 그룹으로 이미 전달된 트래픽에만 적용됩니다. 기본적으로 트래픽 다이얼은 100으로 설정됩니다.
7. 선택적으로 트래픽을 엔드포인트로 라우팅하는 데 사용되는 리스너 포트를 재정의하고 트래픽을 엔드포인트의 특정 포트로 다시 라우팅하려면포트 재지정 구성. 자세한 내용은 포트 재정의 (p. 27) 섹션을 참조하세요.
8. 필요에 따라 EC2 인스턴스 및 엘라스틱 IP 주소 엔드포인트에 적용할 사용자 지정 상태 확인 값을 지정하려면상태 확인 구성. 자세한 내용은 상태 확인 옵션 (p. 28) 섹션을 참조하세요.
9. 필요에 따라엔드포인트 그룹을 추가합니다.을 클릭하여 이 리스너 또는 다른 엔드포인트에 대한 그룹을 추가합니다.
10. 선택엔드포인트 그룹을 추가합니다..

엔드포인트 그룹을 편집하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 을 선택합니다.리스너 ID에서 엔드포인트 그룹이 연결된 리스너의 ID를 선택합니다.

4. 선택엔드포인트 그룹을 편집합니다..
5. 에서엔드포인트 그룹을 편집합니다.페이지에서 지역을 변경하거나 트래픽 다이얼 비율을 조정하거나상태 확인 구성을 클릭하여 상태 확인 설정을 수정합니다.
6. 저장을 선택합니다.

표준 엔드포인트 그룹을 제거하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 리스너를 선택한 다음제거.
4. 에서엔드포인트 그룹섹션에서 엔드포인트 그룹을 선택한 다음제거.
5. 확인 대화 상자에서 을 선택합니다.제거.

트래픽 다이얼로 트래픽 흐름 조정

각 표준 끝점 그룹에 대해 트래픽 다이얼을 설정하여 그룹에 전달되는 트래픽의 비율을 제어할 수 있습니다. 이 비율은 모든 수신기 트래픽이 아니라 이미 끝점 그룹으로 전달된 트래픽에만 적용됩니다.

기본적으로 트래픽 다이얼은 가속기의 모든 지역 끝점 그룹에 대해 100 (즉, 100%) 으로 설정됩니다. 트래픽 다이얼을 사용하면 여러 AWS 리전의 새 릴리스에 대한 성능 테스트 또는 파란색/녹색 배포 테스트를 쉽게 수행할 수 있습니다.

다음은 트래픽 다이얼을 사용하여 트래픽 흐름을 엔드포인트 그룹으로 변경하는 방법을 보여 주는 몇 가지 예입니다.

지역별 애플리케이션 업그레이드

리전에서 애플리케이션을 업그레이드하거나 유지 관리를 수행하려면 먼저 트래픽 다이얼을 0으로 설정하여 해당 지역의 트래픽을 차단합니다. 작업을 완료하고 지역을 다시 사용할 준비가 되면 트래픽 다이얼을 100으로 조정하여 트래픽에 다시 전화를 겁니다.

두 지역 간 트래픽 혼합

이 예에서는 두 지역 끝점 그룹에 대한 트래픽 다이얼을 동시에 변경할 때 트래픽 흐름이 작동하는 방식을 보여 줍니다. 가속기에 대해 두 개의 끝점 그룹이 있다고 가정해 보겠습니다. 하나는`us-west-2`지역에 대한 하나 및`us-east-1`지역 및 각 엔드포인트 그룹에 대해 트래픽 다이얼을 50% 로 설정했습니다.

이제 가속기에 100개의 요청이 있고 미국 동부 해안에서 50개, 서해안에서 50개의 요청이 있다고 가정해 보겠습니다. 가속기는 다음과 같이 트래픽을 전달합니다.

- 각 해안에서 처음 25개의 요청 (총 50개의 요청) 이 가까운 엔드포인트 그룹에서 제공됩니다. 즉, 25개의 요청이`us-west-2`에서 끝점 그룹으로 전달되고 25는`us-east-1`.
- 다음 50개의 요청은 반대 지역으로 전달됩니다. 즉, 동부 해안의 다음 25 요청은`us-west-2`, 다음 25 웨스트 코스트에서 요청에 의해 제공됩니다`us-east-1`.

이 시나리오의 결과는 두 끝점 그룹이 동일한 양의 트래픽을 처리한다는 것입니다. 그러나 각 리전은 두 리전에서 혼합된 트래픽을 수신합니다.

포트 재정의

기본적으로 가속기는 리스너를 생성할 때 지정한 프로토콜 및 포트 범위를 사용하여 사용자 트래픽을 AWS 리전의 엔드포인트로 라우팅합니다. 예를 들어 포트 80 및 443에서 TCP 트래픽을 허용하는 수신기를 정의하는 경우 가속기는 트래픽을 엔드포인트의 해당 포트로 라우팅합니다.

그러나 엔드포인트 그룹을 추가하거나 업데이트할 경우 트래픽을 엔드포인트로 라우팅하는 데 사용되는 리스너 포트를 재정의할 수 있습니다. 예를 들어 수신기가 포트 80 및 443에서 사용자 트래픽을 수신하지만 가속기가 해당 트래픽을 각각 끝점의 포트 1080 및 1443으로 라우팅하는 포트 재정의를 만들 수 있습니다.

포트 재정의를 사용하면 제한된 포트에서 수신 대기 문제를 방지할 수 있습니다. 엔드포인트에서 수퍼 유저 (루트) 권한이 필요하지 않은 애플리케이션을 실행하는 것이 더 안전합니다. 그러나 Linux 및 기타 유닉스 계열 시스템에서는 제한된 포트 (TCP 또는 UDP 포트 1024 이하) 에서 수신 대기하려면 수퍼 유저 권한이 있어야합니다. 수신기의 제한된 포트를 끝점의 제한되지 않은 포트에 매핑하면 포트 재정의를 통해 이 문제를 방지할 수 있습니다. 글로벌 액셀러레이터 뒤의 엔드포인트에 대한 루트 액세스 없이 애플리케이션을 실행하는 동안 제한된 포트에서 트래픽을 허용할 수 있습니다. 예를 들어 리스너 포트 443을 끝점 포트 8443으로 재정의할 수 있습니다.

각 포트 재정의에 대해 사용자의 트래픽을 허용하는 수신기 포트와 글로벌 액셀러레이터가 해당 트래픽을 라우팅할 끝점 포트를 지정합니다. 자세한 내용은 표준 끝점 그룹 추가, 편집 또는 제거 (p. 26) 섹션을 참조하세요.

포트 재정의 를 만들 경우 다음 사항에 유의해야 합니다.

- 끝점 포트는 수신기 포트 범위를 겹칠 수 없습니다. 포트 재정의에서 지정한 끝점 포트는 가속기에 대해 구성한 리스너 포트 범위에 포함될 수 없습니다. 예를 들어 가속기에 대해 두 개의 리스너가 있고 해당 리스너의 포트 범위를 각각 100-199 및 200-299로 정의했다고 가정해 보겠습니다. 예를 들어, 엔드포인트 포트 (210) 가 정의한 리스너 포트 범위 (200-299) 에 포함되어 있기 때문에 포트 재정의를 생성할 때 리스너 포트 100에서 끝점 포트 210까지 하나를 정의할 수 없습니다.
- 중복된 끝점 포트가 없습니다. 가속기의 한 포트 재정의가 끝점 포트를 지정하는 경우 다른 리스너 포트의 포트 재정의를 사용하여 동일한 끝점 포트를 지정할 수 없습니다. 예를 들어 리스너 포트 81에서 끝점 포트 90까지의 재정의와 함께 리스너 포트 80에서 끝점 포트 90까지의 포트 재정의를 지정할 수 없습니다.
- Health 확인은 계속해서 원래 포트를 사용합니다. 상태 확인 포트로 구성된 포트에 대해 포트 재정의를 지정하면 상태 확인은 재정의 포트가 아닌 원래 포트를 계속 사용합니다. 예를 들어 리스너 포트 80에서 상태 확인을 지정하고 리스너 포트 80에서 끝점 포트 480까지 포트 재정의도 지정한다고 가정합니다. Health 확인은 끝점 포트 80을 계속 사용합니다. 그러나 포트 80을 통해 들어오는 사용자 트래픽은 끝점의 포트 480으로 이동합니다.

  이 동작은 Network Load Balancer, Application Load Balancer, EC2 인스턴스 및 엘라스틱 IP 주소 엔드포인트 간의 일관성을 유지합니다. 글로벌 가속기에서 포트 재정의를 지정할 때 네트워크 로드 밸런서와 애플리케이션 로드 밸런서는 상태 확인 포트를 다른 엔드포인트 포트에 매핑하지 않으므로 글로벌 가속기가 상태 확인 포트를 EC2 인스턴스 및 엘라스틱 IP의 다른 엔드포인트 포트에 매핑하는 것은 일관되지 않습니다.주소 끝점.
- 보안 그룹 설정은 포트 액세스를 허용해야 합니다. 보안 그룹이 포트 재정의에서 지정한 엔드포인트 포트에 트래픽이 도달하도록 허용하는지 확인합니다. 예를 들어 리스너 포트 443을 엔드포인트 포트 1433으로 재정의하는 경우 해당 Application Load Balancer 또는 Amazon EC2 엔드포인트에 대해 보안 그룹에 설정된 포트 제한이 포트 1433에서 인바운드 트래픽을 허용하는지 확인합니다.

상태 확인 옵션

AWS Global Accelerator 는 표준 엔드포인트로 요청을 전송하여 상태를 확인합니다. 이러한 상태 확인은 자동으로 실행됩니다. 각 끝점의 상태 및 상태 확인 타이밍을 결정하기 위한 지침은 끝점 리소스의 유형에 따라 다릅니다.

> Important
>
> 글로벌 액셀러레이터를 사용하려면 Route 53 상태 확인 프로그램과 연결된 IP 주소로부터의 인바운드 트래픽이 EC2 인스턴스 또는 엘라스틱 IP 주소 엔드포인트에 대한 상태 확인을 완료할 수 있도록 라우터 및 방화벽 규칙이 필요합니다. Amazon Route 53 상태 확인 프로그램과 연결된 IP 주소 범위에 대한 정보는대상 그룹에 대한 상태 확인의Amazon Route 53 개발자 가이드.

끝점 그룹에 대해 다음과 같은 상태 확인 옵션을 구성할 수 있습니다. 상태 확인 옵션을 지정하는 경우 글로벌 가속기는 EC2 인스턴스 또는 엘라스틱 IP 주소 상태 확인에 대한 설정을 사용하지만 네트워크 로드 밸런서나 애플리케이션 로드 밸런서는 사용하지 않습니다.

- Application Load Balancer 또는 Network Load Balancer 엔드포인트의 경우 Elastic Load Balancing 구성 옵션을 사용하여 리소스에 대한 상태 확인을 구성합니다. 자세한 내용은 단원을 참조하십시오.대상 그룹에 대한 상태 확인. 글로벌 가속기에서 선택한 Health 확인 옵션은 엔드포인트로 추가한 애플리케이션 로드 밸런서 또는 네트워크 로드 밸런서에 영향을 주지 않습니다.

  Note

  여러 대상 그룹을 포함하는 Application Load Balancer 또는 네트워크 로드 밸런서가 있는 경우 글로벌 액셀러레이터는각각의대상 그룹에는 하나 이상의 정상 대상이 있습니다. 로드 밸런서의 단일 대상 그룹에 비정상 대상만 있는 경우 글로벌 가속기는 엔드포인트를 비정상으로 간주합니다.
- TCP로 구성된 리스너에 추가되는 EC2 인스턴스 또는 엘라스틱 IP 주소 엔드포인트의 경우 상태 확인에 사용할 포트를 지정할 수 있습니다. 기본적으로 상태 확인에 사용할 포트를 지정하지 않으면 글로벌 가속기는 가속기에 대해 지정한 수신기 포트를 사용합니다.
- EC2 인스턴스 또는 UDP 리스너가 있는 엘라스틱 IP 주소 엔드포인트의 경우 글로벌 액셀러레이터는 상태 확인에 리스너 포트와 TCP 프로토콜을 사용하므로 엔드포인트에 TCP 서버가 있어야 합니다.

  Note

  각 끝점의 TCP 서버에 대해 구성한 포트가 글로벌 가속기의 상태 확인에 대해 지정한 포트와 동일한지 확인해야 합니다. 포트 번호가 동일하지 않거나 엔드포인트에 대해 TCP 서버를 설정하지 않은 경우 글로벌 가속기는 엔드포인트의 상태에 관계없이 엔드포인트를 비정상으로 표시합니다.

Health 확인 포트

Global Accelerator가 이 엔드포인트 그룹의 일부인 엔드포인트에 대한 상태 확인을 수행할 때 사용할 포트입니다.

Note

상태 확인 포트에 대해 포트 재정의를 설정할 수 없습니다.

상태 확인 프로토콜

Global Accelerator가 이 엔드포인트 그룹의 일부인 엔드포인트에 대한 상태 확인을 수행할 때 사용할 프로토콜입니다.

Health 확인 간격

엔드포인트에 대한 각 상태 확인 간격 (초) 입니다.

임계값 개수

비정상 상태의 대상을 정상으로 간주하기까지 필요한 연속적 상태 확인 횟수입니다.

각 수신기는 정상적인 끝점으로만 요청을 라우팅합니다. 엔드포인트를 추가한 후에는 상태 확인을 통과해야 정상으로 간주됩니다. 각 상태 확인이 완료되면 리스너는 상태 확인을 위해 설정된 연결을 닫습니다.

AWS 글로벌 가속기의 표준 가속기에 대한 엔드포인트

AWS 글로벌 가속기의 표준 가속기에 대한 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다. 표준 가속기를 사용하면 고정 IP 주소가 클라이언트에 대한 단일 접점의 역할을 하며 Global Accelerator를 통해 정상적인 엔드포인트로 들어오는 트래픽을 분산합니다. 글로벌 액셀러레이터는 엔드포인트의 끝점 그룹이 속한 수신기에 대해 지정한 포트 (또는 포트 범위) 를 사용하여 트래픽을 끝점으로 보냅니다.

각 엔드포인트 그룹은 여러 엔드포인트를 포함할 수 있습니다. 각 끝점을 여러 끝점 그룹에 추가할 수 있지만 끝점 그룹은 서로 다른 수신기와 연결되어야 합니다. 리소스는 엔드포인트로 추가할 때 유효하고 활성 상태여야 합니다.

글로벌 가속기는 표준 끝점 그룹에 포함된 모든 끝점의 상태를 지속적으로 모니터링합니다. 정상적인 활성 끝점으로만 트래픽을 라우팅합니다. 글로벌 액셀러레이터는 트래픽을 라우팅할 정상 엔드포인트가 없는 경우 트래픽을 모든 엔드포인트로 라우팅합니다.

특정 유형의 글로벌 가속기 표준 끝점에 대해서는 다음 사항에 유의하십시오.

로드 밸런서 엔드포인트

- Application Load Balancer 엔드포인트는 인터넷 연결이나 내부일 수 있습니다. Network Load Balancer 끝점은 인터넷에 연결되어야 합니다.

Amazon EC2 인스턴스 엔드포인트

- EC2 인스턴스 엔드포인트 (표준 및 사용자 지정 라우팅 가속기 모두) 는 다음 유형 중 하나일 수 없습니다. C1, G1, G1, G1, G1, G1, G1, G1, G2, G2, G2, M1, M1, M2, M3, M2, M3, M2, M3, M2, M2, M3,
- EC2 인스턴스는 일부 AWS 리전에서만 엔드포인트로 지원됩니다. 지원되는 리전 목록은 클라이언트 IP 주소 보존을 위해 지원되는 AWS 리전 (p. 58) 단원을 참조하십시오.
- 인스턴스를 종료하기 전에 글로벌 액셀러레이터 엔드포인트 그룹에서 EC2 인스턴스를 제거하는 것이 좋습니다. 글로벌 액셀러레이터의 엔드포인트 그룹에서 EC2 인스턴스를 제거하기 전에 EC2 인스턴스를 종료한 다음 동일한 VPC 동일한 프라이빗 IP 주소를 사용하여 다른 인스턴스를 생성하고 상태 확인을 통과하면 글로벌 액셀러레이터는 트래픽을 새 엔드포인트로 라우팅합니다.

주제

표준 끝점 추가, 편집 또는 제거

트래픽이 리소스로 전달될 수 있도록 엔드포인트를 엔드포인트 그룹에 추가합니다. 표준 끝점을 편집하여 끝점의 가중치를 변경할 수 있습니다. 또는 끝점 그룹에서 끝점을 제거하여 가속기에서 끝점을 제거할 수 있습니다. 엔드포인트를 제거해도 엔드포인트 자체에는 영향을 주지 않지만 글로벌 액셀러레이터는 더 이상 트래픽을 해당 리소스로 보낼 수 없습니다.

글로벌 가속기의 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다. 먼저 이러한 리소스 중 하나를 만든 다음 글로벌 액셀러레이터에서 끝점으로 추가할 수 있습니다. 리소스는 엔드포인트로 추가할 때 유효하고 활성 상태여야 합니다.

사용량에 따라 엔드포인트 그룹에 엔드포인트를 추가하거나 제거할 수 있습니다. 예를 들어 응용 프로그램에 대한 수요가 증가하면 리소스를 더 만든 다음 하나 이상의 끝점 그룹에 끝점을 추가하여 증가된 트래픽을 처리할 수 있습니다. Global Accelerator를 추가하고 엔드포인트에 초기 상태 확인을 통과하자마자 해당 엔드포인트로 라우팅하기 시작합니다. 엔드포인트의 가중치를 조정하여 엔드포인트에 대한 트래픽을 비례적으로 더 많거나 적은 트래픽을 엔드포인트로 전송하도록 관리할 수 있습니다.

클라이언트 IP 주소 보존이 있는 엔드포인트를 추가하는 경우 먼저클라이언트 IP 주소 보존을 위해 지원되는 AWS 리전 (p. 58)및AWS Global Accelerator 클라이언트 IP 주소 보존 (p. 55).

예를 들어 엔드포인트를 서비스해야 하는 경우 엔드포인트 그룹에서 엔드포인트를 제거할 수 있습니다. 엔드포인트를 제거하면 엔드포인트 그룹에서 제거되지만 엔드포인트에 영향을 미치지는 않습니다. 글로벌 액셀러레이터는 엔드포인트 그룹에서 트래픽을 제거하는 즉시 엔드포인트로 트래픽을 전달하는 것을 중지합니다. 끝점은 현재 모든 요청이 완료될 때까지 기다리는 상태로 전환되므로 진행 중인 클라이언트 트래픽에 대한 중단이 없습니다. 요청 수신을 다시 시작할 준비가 되면 엔드포인트에 엔드포인트를 다시 추가할 수 있습니다.

이 단원에서는 AWS Global Accelerator 콘솔에서 엔드포인트로 작업하는 방법에 대해 설명합니다. AWS Global Accelerator 터에 API 작업을 사용하려면 단원을 참조하십시오.AWS Global Accelerator API 참조.

표준 끝점을 추가하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서엔드포인트 그룹섹션에서엔드포인트 ID에서 엔드포인트를 추가할 엔드포인트 그룹의 ID를 선택합니다.
5. 에서엔드포인트섹션에서엔드포인트 추가.
6. 에서끝점 추가페이지의 드롭다운 목록에서 리소스를 선택합니다.

   AWS 리소스가 없는 경우 목록에 항목이 없습니다. 계속하려면 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소와 같은 AWS 리소스를 생성합니다. 그런 다음 여기로 돌아와 목록에서 리소스를 선택합니다.
7. 필요에 따라Weight에 0에서 255 사이의 숫자를 입력하여 이 엔드포인트로 트래픽을 라우팅하기 위한 가중치를 설정합니다. 엔드포인트에 가중치를 추가할 경우 지정한 비율에 따라 트래픽을 라우팅하도록 글로벌 가속기를 구성합니다. 기본적으로 모든 끝점의 가중치는 128입니다. 자세한 내용은 엔드포인트 가중치 (p. 32) 섹션을 참조하세요.
8. 선택적으로 인터넷 연결 Application Load Balancer 엔드포인트에 대해 클라이언트 IP 주소 보존을 활성화합니다. 언더클라이언트 IP 주소 보존를 선택하려면주소 보존.

   이 옵션은 내부 Application Load Balancer 및 EC2 인스턴스 엔드포인트에 대해 항상 선택되며 Network Load Balancer 및 엘라스틱 IP 주소 엔드포인트에는 선택되지 않습니다. 자세한 내용은 AWS Global Accelerator 클라이언트 IP 주소 보존 (p. 55) 섹션을 참조하세요.

   Note

   클라이언트 IP 주소를 보존하는 끝점으로 트래픽을 추가하고 라우팅하기 전에 보안 그룹과 같은 모든 필수 보안 구성이 허용 목록에 사용자 클라이언트 IP 주소를 포함하도록 업데이트되었는지 확인합니다.
9. Add endpoint(엔드포인트 추가)를 선택합니다.

표준 끝점을 편집하려면

엔드포인트 구성을 편집하여 가중치를 변경할 수 있습니다. 자세한 내용은 엔드포인트 가중치 (p. 32) 섹션을 참조하세요.

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서엔드포인트 그룹섹션에서엔드포인트 ID에서 엔드포인트 그룹의 ID를 선택합니다.
5. 선택엔드포인트 편집.
6. 에서엔드포인트 편집페이지에서 업데이트를 수행한 다음Save.

끝점을 제거하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.

3. 에서리스너섹션에서리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서엔드포인트 그룹섹션에서엔드포인트 ID에서 엔드포인트 그룹의 ID를 선택합니다.
5. 선택엔드포인트 제거.
6. 확인 대화 상자에서제거.

엔드포인트 가중치

가중치는 글로벌 액셀러레이터가 표준 가속기의 엔드포인트로 전송하는 트래픽의 비율을 결정하는 값입니다. 엔드포인트는 네트워크 로드 밸런서, 애플리케이션 로드 밸런서, Amazon EC2 인스턴스 또는 엘라스틱 IP 주소일 수 있습니다. 글로벌 액셀러레이터는 엔드포인트 그룹의 엔드포인트에 대한 가중치 합계를 계산한 다음 각 엔드포인트의 가중치 대 총 가중치의 비율에 따라 트래픽을 엔드포인트로 보냅니다.

가중치 기반 라우팅을 사용하면 엔드포인트 그룹의 리소스로 라우팅되는 트래픽 양을 선택할 수 있습니다. 이 방법은 로드 밸런싱, 새 버전의 응용 프로그램 테스트 등을 비롯한 여러 가지 방법으로 유용할 수 있습니다.

엔드포인트 가중치 작동 방식

가중치를 사용하려면 엔드포인트 그룹의 각 엔드포인트에 전송하려는 트래픽 양에 해당하는 상대적 가중치를 할당합니다. 기본적으로 끝점의 가중치는 128입니다. 즉, 가중치에 대한 최대값의 절반인 255입니다. Global Accelerator는 그룹 내 전체 엔드포인트에 대한 비율로 그룹에 할당된 가중치를 기반으로 엔드포인트로 트래픽을 전송합니다.

$$\frac{\text{Weight for a specified endpoint}}{\text{Sum of the weights for all endpoints}}$$

예를 들어 한 엔드포인트로 일부 트래픽만 전송하고 나머지를 다른 엔드포인트로 전송하려는 경우 가중치 1과 255를 지정할 수 있습니다. 가중치 1이 할당된 엔드포인트에는 트래픽의 1/256 (1/1+255) 이 전송되고, 다른 엔드포인트에는 트래픽의 255/256 (255/1+255) 이 전송됩니다. 가중치를 변경하여 점진적으로 균형을 조정할 수 있습니다. 엔드포인트로 트래픽 전송을 중단하려면 해당 리소스의 가중치를 0으로 변경할 수 있습니다.

비정상 엔드포인트에 대한 장애 조치

가중치가 0보다 큰 끝점이 끝점 그룹에 없는 경우 글로벌 가속기는 다른 끝점 그룹에서 가중치가 0보다 큰 정상 끝점으로 장애 조치를 시도합니다. 이 장애 조치의 경우 글로벌 가속기는 트래픽 다이얼 설정을 무시합니다. 따라서 예를 들어 끝점 그룹에 트래픽 다이얼이 0으로 설정된 경우 글로벌 가속기는 여전히 장애 조치 시도에 해당 끝점 그룹을 포함합니다.

글로벌 액셀러레이터는 세 개의 추가 엔드포인트 그룹 (즉, 세 개의 AWS 리전) 을 시도한 후 가중치가 0보다 큰 정상 엔드포인트를 찾지 못하면 트래픽을 클라이언트와 가장 가까운 엔드포인트 그룹의 임의 엔드포인트로 라우팅합니다. 즉,열기 실패.

다음을 참조하십시오.

- 장애 조치를 위해 선택한 끝점 그룹은 트래픽 다이얼이 0으로 설정된 끝점 그룹일 수 있습니다.
- 가장 가까운 끝점 그룹은 원래 끝점 그룹이 아닐 수 있습니다. 이는 글로벌 가속기가 원래 끝점 그룹을 선택할 때 계정 트래픽 다이얼 설정을 고려하기 때문입니다.

예를 들어 구성에 두 개의 끝점 (정상 및 비정상) 이 있고 각 끝점의 가중치를 0보다 크게 설정했다고 가정해 보겠습니다. 이 경우 글로벌 액셀러레이터는 트래픽을 정상 엔드포인트로 라우팅합니다. 그러나 이제 유일한 정상 끝점의 가중치를 0으로 설정한다고 가정 해보십시오. 그런 다음 글로벌 액셀러레이터는 가중치가 0보다 큰 정상 끝점을 찾기 위해 세 개의 추가 끝점 그룹을 시도합니다. 글로벌 액셀러레이터는 클라이언트에 가장 가까운 끝점 그룹의 임의 끝점으로 트래픽을 라우팅합니다.

클라이언트 IP 주소 보존을 사용하여 엔드포인트 추가

일부 엔드포인트 유형 (일부 지역에서는) 과 함께 사용할 수 있는 기능은클라이언트 IP 주소 보존. 이 기능을 사용하면 끝점에 도착하는 패킷에 대해 원본 클라이언트의 원본 IP 주소를 보존할 수 있습니다. 이 기능은 Application Load Balancer 및 Amazon EC2 인스턴스 엔드포인트에서 사용할 수 있습니다. 사용자 지정 라우팅 가속기의 끝점에는 항상 클라이언트 IP 주소가 유지됩니다. 자세한 내용은 AWS Global Accelerator 클라이언트 IP 주소 보존 (p. 55) 섹션을 참조하세요.

클라이언트 IP 주소 보존 기능을 사용하려는 경우 글로벌 가속기에 끝점을 추가할 때 다음 사항에 유의하십시오.

탄력적 네트워크 인터페이스

클라이언트 IP 주소 보존을 지원하기 위해 글로벌 액셀러레이터는 AWS 계정에 엔드포인트가 있는 각 서브넷에 대해 하나씩 엘라스틱 네트워크 인터페이스를 만듭니다. 글로벌 액셀러레이터가 탄력적 네트워크 인터페이스로 작동하는 방법에 대한 자세한 내용은 단원을 참조하십시오.클라이언트 IP 주소 보존에 대한 모범 사례 (p. 57).

프라이빗 서브넷의 엔드포인트

AWS Global Accelerator 사용하여 프라이빗 서브넷의 Application Load Balancer 또는 EC2 인스턴스를 대상으로 지정할 수 있지만인터넷 게이트웨이엔드포인트가 포함된 VPC 연결되어 있습니다. 자세한 내용은 AWS Global Accelerator 터의 보안 VPC 연결 (p. 101) 섹션을 참조하세요.

클라이언트 IP 주소를 허용 목록에 추가합니다.

클라이언트 IP 주소를 보존하는 끝점으로 트래픽을 추가하고 라우팅하기 전에 보안 그룹과 같은 모든 필수 보안 구성이 허용 목록에 사용자 클라이언트 IP 주소를 포함하도록 업데이트되었는지 확인합니다. 네트워크 액세스 제어 목록 (ACL) 은 송신 (아웃바운드) 트래픽에만 적용됩니다. 수신 (인바운드) 트래픽을 필터링해야 하는 경우 보안 그룹을 사용해야 합니다.

네트워크 액세스 제어 목록 (ACL) 구성

가속기에서 클라이언트 IP 주소 보존이 활성화된 경우 VPC 서브넷과 연결된 네트워크 ACL은 송신 (아웃바운드) 트래픽에 적용됩니다. 그러나 트래픽이 글로벌 가속기를 통해 종료되도록 허용하려면 ACL을 인바운드 및 아웃바운드 규칙으로 구성해야 합니다.

예를 들어 임시 소스 포트를 사용하는 TCP 및 UDP 클라이언트가 글로벌 가속기를 통해 끝점에 연결할 수 있도록 하려면 끝점의 서브넷을 임시 TCP 또는 UDP 포트 (포트 범위 1024-65535, 대상 0.0.0.0/0) 로 향하는 아웃바운드 트래픽을 허용하는 네트워크 ACL과 연결합니다. 또한 일치하는 인바운드 규칙 (포트 범위 1024-65535, 소스 0.0.0.0/0) 을 생성합니다.

Note

보안 그룹 및 AWS WAF 규칙은 리소스를 보호하기 위해 적용할 수 있는 추가 기능 집합입니다. 예를 들어 Amazon EC2 인스턴스 및 애플리케이션 로드 밸런서와 연결된 인바운드 보안 그룹 규칙을 사용하면 클라이언트가 글로벌 가속기를 통해 연결할 수 있는 대상 포트 (예: HTTP의 경우 포트 80, HTTPS의 경우 포트 443) 를 제어할 수 있습니다. Amazon EC2 인스턴스 보안 그룹은 글로벌 액셀러레이터로부터의 트래픽과 인스턴스에 할당된 퍼블릭 또는 엘라스틱 IP 주소를 포함하여 인스턴스에 도착하는 모든 트래픽에 적용됩니다. 글로벌 액셀러레이터에서만 트래픽을 전송하려면 프라이빗 서브넷을 사용하는 것이 좋습니다. 또한 인바운드 보안 그룹 규칙이 응용 프로그램의 트래픽을 올바르게 허용하거나 거부하도록 적절하게 구성되어 있는지 확인합니다.

클라이언트 IP 주소 보존을 사용하기 위해 끝점 전환

이 섹션의 지침에 따라 가속기에 있는 하나 이상의 끝점을 사용자의 클라이언트 IP 주소를 유지하는 끝점으로 전환합니다. Application Load Balancer 엔드포인트 또는 엘라스틱 IP 주소 엔드포인트를 클라이언트 IP

주소 보존이 있는 해당 엔드포인트 (Application Load Balancer 또는 EC2 인스턴스) 로 전환하도록 선택할 수 있습니다. 자세한 내용은 AWS Global Accelerator 클라이언트 IP 주소 보존 (p. 55) 섹션을 참조하세요.

클라이언트 IP 주소 보존을 느리게 사용하는 것으로 전환하는 것이 좋습니다. 먼저 클라이언트 IP 주소를 보존하기 위해 사용하도록 설정한 새 Application Load Balancer 또는 EC2 인스턴스 엔드포인트를 추가합니다. 그런 다음 엔드포인트에 가중치를 구성하여 기존 엔드포인트에서 새 엔드포인트로 트래픽을 천천히 이동합니다.

> Important
>
> 클라이언트 IP 주소를 보존하는 끝점으로 트래픽을 라우팅하기 전에 허용 목록에 글로벌 액셀러레이터 클라이언트 IP 주소를 포함하는 모든 구성이 사용자 클라이언트 IP 주소를 포함하도록 업데이트되었는지 확인하십시오.

클라이언트 IP 주소 보존은 특정 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 클라이언트 IP 주소 보존을 위해 지원되는 AWS 리전 (p. 58) 섹션을 참조하세요.

이 단원에서는 AWS Global Accelerator 에서 엔드포인트 그룹을 사용하는 방법에 대해 설명합니다. Global Accelerator 액셀러레이터를 사용하려면AWS Global Accelerator API 참조.

클라이언트 IP 주소 보존을 사용하여 소량의 트래픽을 새 끝점으로 이동한 후 구성이 예상대로 작동하는지 테스트합니다. 그런 다음 해당 끝점의 가중치를 조정하여 새 끝점에 대한 트래픽 비율을 점차 늘립니다.

클라이언트 IP 주소를 보존하는 끝점으로 전환하려면 다음 단계에 따라 새 끝점을 추가하고 인터넷 연결 Application Load Balancer 끝점의 경우 클라이언트 IP 주소 보존을 사용하도록 설정합니다. 내부 애플리케이션 로드 밸런서 및 EC2 인스턴스에 대해 클라이언트 IP 주소 보존 옵션이 항상 선택됩니다.

클라이언트 IP 주소 보존을 사용하여 끝점을 추가하려면

1. 글로벌 액셀러레이터 콘솔을 다음 위치에서 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 리스너를 선택합니다.
4. 에서엔드포인트 그룹섹션에서 엔드포인트 그룹을 선택합니다.
5. 에서엔드포인트섹션에서엔드포인트 추가.
6. 에서끝점 추가페이지의엔드포인트드롭다운 목록에서 Application Load Balancer 엔드포인트 또는 EC2 인스턴스 엔드포인트를 선택합니다.
7. 에서Weight필드에서 기존 엔드포인트에 대해 설정된 가중치에 비해 낮은 수를 선택합니다. 예를 들어 해당 Application Load Balancer 서의 가중치가 255인 경우 새 애플리케이션 로드 밸런서의 가중치를 5로 입력하여 시작할 수 있습니다. 자세한 내용은 엔드포인트 가중치 (p. 32) 섹션을 참조하세요.
8. 외부 연결 Application Load Balancer 끝점의 경우클라이언트 IP 주소 보존를 선택하려면주소 보존. (이 옵션은 내부 애플리케이션 로드 밸런서 및 EC2 인스턴스에 대해 항상 선택됩니다.)
9. [Save changes]를 선택합니다.

그런 다음, 클라이언트 IP 주소 보존을 사용하여 새 끝점으로 대체하는 기존 끝점을 편집하여 기존 끝점의 가중치를 줄여 더 적은 트래픽이 전달되도록 합니다.

기존 엔드포인트의 트래픽을 줄이려면

1. 에서엔드포인트 그룹페이지에서 클라이언트 IP 주소 보존이 없는 기존 끝점을 선택합니다.
2. [Edit]를 선택합니다.
3. 에서엔드포인트 편집페이지의Weight필드에 현재 숫자보다 낮은 숫자를 입력합니다. 예를 들어 기존 끝점의 가중치가 255인 경우 새 끝점에 대해 가중치를 220으로 입력할 수 있습니다 (클라이언트 IP 주소 보존).
4. [Save changes]를 선택합니다.

새 끝점의 가중치를 낮은 수로 설정하여 원래 트래픽의 일부를 테스트한 후에는 원래 끝점과 새 끝점의 가중치를 계속 조정하여 모든 트래픽을 천천히 전환할 수 있습니다.

예를 들어 가중치가 200으로 설정된 기존 Application Load Balancer 시작하고 가중치가 5로 설정된 클라이언트 IP 주소 보존이 활성화된 새 Application Load Balancer 끝점을 추가한다고 가정합니다. 새로운 Application Load Balancer 가중치를 늘리고 원래 Application Load Balancer 가중치를 줄임으로써 원래 애플리케이션 로드 밸런서에서 새로운 애플리케이션 로드 밸런서로 트래픽을 점진적으로 이동합니다. 예:

- 원래 무게 190/새로운 무게 10
- 원래 무게 180/새로운 무게 20
- 원래 무게 170/새로운 무게 30 등등.

원래 끝점의 가중치를 0으로 줄이면 모든 트래픽 (이 예제 시나리오에서) 은 클라이언트 IP 주소 보존을 포함하는 새로운 Application Load Balancer 끝점으로 이동합니다.

클라이언트 IP 주소 보존을 사용하도록 전환하려는 추가 엔드포인트 (애플리케이션 로드 밸런서 또는 EC2 인스턴스) 가 있는 경우 이 섹션의 단계를 반복하여 전환하십시오.

엔드포인트에 대한 트래픽이 클라이언트 IP 주소를 보존하지 않도록 엔드포인트에 대한 구성을 되돌려야 하는 경우 언제든지이를 수행할 수 있습니다.하지클라이언트 IP 주소를 원래 값으로 보존하고 엔드포인트의 가중치를 줄입니다.다음으로 바꿉니다.클라이언트 IP 주소 보존을 0으로 설정합니다.

AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기 사용

이 장에는 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기를 만들기 위한 절차와 권장 사항이 포함되어 있습니다. 사용자 지정 라우팅 가속기를 사용하면 애플리케이션 로직을 사용하여 여러 대상 간에 한 명 이상의 사용자를 특정 Amazon EC2 인스턴스로 직접 매핑하는 동시에 글로벌 액셀러레이터를 통해 트래픽을 라우팅하는 성능을 향상시킬 수 있습니다. 이 기능은 게임 애플리케이션 또는 VoIP (Voice over IP) 세션과 같이 특정 EC2 인스턴스 및 포트에서 실행되는 동일한 세션에서 사용자 그룹이 서로 상호 작용해야 하는 애플리케이션이 있는 경우에 유용합니다.

사용자 지정 라우팅 가속기의 엔드포인트는 가상 프라이빗 클라우드 (VPC) 서브넷이어야 하며, 사용자 지정 라우팅 가속기는 트래픽을 해당 서브넷의 Amazon EC2 인스턴스로만 라우팅할 수 있습니다. 사용자 지정 라우팅 가속기를 생성할 때 단일 또는 여러 VPC 서브넷에서 실행 중인 수천 개의 Amazon EC2 인스턴스를 포함할 수 있습니다. 자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식 (p. 37) 단원을 참조하십시오.

대신 글로벌 액셀러레이터가 클라이언트에 가장 가까운 정상 엔드포인트를 자동으로 선택하도록 하려면 표준 액셀러레이터를 생성합니다. 자세한 내용은 AWS 글로벌 액셀러레이터의 표준 액셀러레이터 사용 (p. 20) 섹션을 참조하세요.

사용자 지정 라우팅 액셀러레이터를 설정하려면 다음 작업을 수행합니다.

1. 사용자 지정 라우팅 액셀러레이터를 만들기 위한 지침과 요구 사항을 검토합니다. 사용자 지정 라우팅 가속기에 대한 지침 및 제한 사항 (p. 39) 단원을 참조하십시오.
2. VPC 서브넷을 생성합니다. 글로벌 가속기에 서브넷을 추가한 후 언제든지 EC2 인스턴스를 서브넷에 추가할 수 있습니다.
3. 액셀러레이터를 생성하고 사용자 지정 라우팅 액셀러레이터를 위한 옵션을 선택합니다.
4. 수신기를 추가하고 글로벌 가속기가 수신할 포트 범위를 지정합니다. 글로벌 액셀러레이터를 사용할 것으로 예상되는 모든 대상에 매핑할 수 있는 충분한 포트가 있는 넓은 범위를 포함해야 합니다. 이러한 포트는 다음 단계에서 지정하는 대상 포트와 구별됩니다. 수신기 포트 요구 사항에 대한 자세한 내용은 단원을 참조하십시오.사용자 지정 라우팅 가속기에 대한 지침 및 제한 사항 (p. 39).
5. VPC 서브넷이 있는 AWS 리전용 엔드포인트 그룹을 하나 이상 추가합니다. 각 엔드포인트 그룹에 대해 다음을 지정합니다.
   - 트래픽을 수신할 수 있는 대상 EC2 인스턴스의 포트를 나타내는 엔드포인트 포트 범위
   - 각 대상 포트 범위에 대한 프로토콜: UDP, TCP 또는 UDP 및 TCP 둘 다 사용할 수 있습니다.
6. 끝점 서브넷의 경우 서브넷 ID를 선택합니다. 각 끝점 그룹에 여러 서브넷을 추가할 수 있으며 서브넷의 크기가 다를 수 있습니다 (최대 /17).

다음 섹션에서는 사용자 지정 라우팅 가속기, 수신기, 끝점 그룹 및 끝점에 대한 작업을 단계별로 설명합니다.

주제

AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식

AWS Global Accelerator에서 사용자 지정 라우팅 가속기를 사용하면 애플리케이션 로직을 사용하여 한 명 이상의 사용자를 여러 대상 중에서 특정 대상에 직접 매핑하는 동시에 글로벌 액셀러레이터의 성능 이점을 누릴 수 있습니다. 사용자 지정 라우팅 가속기는 수신기 포트 범위를 VPC (가상 프라이빗 클라우드) 서브넷의 EC2 인스턴스 대상으로 매핑합니다. 이를 통해 글로벌 액셀러레이터는 트래픽을 서브넷의 특정 Amazon EC2 프라이빗 IP 주소 및 포트 대상으로 결정적으로 라우팅할 수 있습니다.

예를 들어, 온라인 실시간 게임 애플리케이션과 함께 사용자 지정 라우팅 가속기를 사용할 수 있습니다. 이 애플리케이션은 지리적 위치, 플레이어 기술, 게임 모드 등 사용자가 선택한 요소에 따라 Amazon EC2 게임 서버의 단일 세션에 여러 플레이어를 할당할 수 있습니다. 또는 음성, 비디오 및 메시징 세션을 위해 특정 미디어 서버에 여러 사용자를 할당하는 VoIP 또는 소셜 미디어 응용 프로그램이 있을 수 있습니다.

응용 프로그램에서 글로벌 가속기 API를 호출하고 글로벌 가속기 포트와 연결된 대상 IP 주소 및 포트에 대한 전체 정적 매핑을 수신할 수 있습니다. 정적 매핑을 저장한 다음 매치메이킹 서비스에서 이를 사용하여 사용자를 특정 대상 EC2 인스턴스로 라우팅할 수 있습니다. 응용 프로그램에서 Global Accelerator 를 사용하기 위해 클라이언트 소프트웨어를 수정하지 않아도 됩니다.

사용자 지정 라우팅 가속기를 구성하려면 VPC 서브넷 끝점을 선택합니다. 그런 다음 들어오는 연결이 매핑될 대상 포트 범위를 정의하여 소프트웨어가 모든 인스턴스에서 동일한 포트 세트에서 수신 대기할 수 있도록 합니다. 글로벌 액셀러레이터 (Global Accelerator) 는 매치메이킹 서비스에서 세션의 대상 IP 주소와 포트 번호를 사용자가 사용자에게 제공하는 외부 IP 주소 및 포트로 변환할 수 있도록 하는 정적 매핑을 만듭니다.

응용 프로그램의 네트워크 스택은 단일 전송 프로토콜을 통해 작동하거나 빠른 전송을 위해 UDP를 사용하고 신뢰할 수 있는 전송을 위해 TCP를 사용할 수 있습니다. 각 대상 포트 범위에 대해 UDP, TCP 또는 UDP 및 TCP를 모두 설정하여 각 프로토콜에 대한 구성을 복제하지 않고도 유연성을 극대화할 수 있습니다.

> Note
>
> 기본적으로 사용자 지정 라우팅 가속기의 모든 VPC 서브넷 대상은 트래픽을 수신할 수 없습니다. 이는 기본적으로 안전하며, 서브넷에서 트래픽을 수신할 수 있는 프라이빗 EC2 인스턴스 대상을 세부적으로 제어할 수 있도록 하기 위한 것입니다. 서브넷 또는 특정 IP 주소 및 포트 조합 (대상 소켓)에 대한 트래픽을 허용하거나 거부할 수 있습니다. 자세한 내용은 VPC 서브넷 엔드포인트 추가, 편집 또는 제거 (p. 46) 섹션을 참조하세요. 글로벌 액셀러레이터 API를 사용하여 대상을 지정할 수도 있습니다. 자세한 내용은 단원을 참조하십시오.사용자 지정 라우팅 트래픽 허용및사용자 지정 라우팅 트래픽.

글로벌 액셀러레이터에서 사용자 지정 라우팅의 작동 방식 예

예를 들어 글로벌 액셀러레이터 뒤에 있는 1,000개의 Amazon EC2 인스턴스에서 게임 세션이나 VoIP 호출 세션과 같은 사용자 그룹이 상호 작용하는 10,000개의 세션을 지원한다고 가정해 보겠습니다. 이 예에서는 수신기 포트 범위를 10001-20040으로 지정하고 대상 포트 범위를 81-90으로 지정합니다. 서브넷 -1, 서브넷 2, 서브넷 3 및 서브넷 4의 네 개의 VPC 서브넷이 있다고 말할 수 있습니다.

예제 구성에서는 각 VPC 서브넷의 블록 크기가 /24이므로 251개의 Amazon EC2 인스턴스를 지원할 수 있습니다. (5개 주소는 예약되어 있고 각 서브넷에서 사용할 수 없으며 이러한 주소는 매핑되지 않습니다.) 각 EC2 인스턴스에서 실행되는 각 서버는 엔드포인트 그룹의 대상 포트에 대해 지정한 다음 10개의 포트를 제공합니다. 81-90 즉, 각 서브넷과 연결된 2510 개의 포트 (10 x 251) 가 있습니다. 각 포트는 세션과 연관될 수 있습니다.

서브넷의 각 EC2 인스턴스에서 대상 포트를 10개 지정했으므로 글로벌 액셀러레이터는 내부적으로 EC2 인스턴스에 액세스하는 데 사용할 수 있는 10개의 수신기 포트와 연결합니다. 간단히 설명하기 위해 첫 번째 10개 집합에 대한 끝점 서브넷의 첫 번째 IP 주소로 시작한 다음 10개의 수신기 포트 집합에 대해 다음 IP 주소로 이동하는 수신기 포트 블록이 있다고 가정합니다.

Note

매핑은 실제로 이와 같이 예측할 수 없지만 여기서 순차적 매핑을 사용하여 포트 매핑이 어떻게 작동하는지 보여줍니다. 리스너 포트 범위에 대한 실제 매핑을 확인하려면 다음 API 작업을 사용합니다. 목록 사용자 지정 라우팅포트매핑및목록사용자 지정 라우팅포트매핑대상별.

이 예에서 첫 번째 리스너 포트는 10001입니다. 이 포트는 첫 번째 서브넷 IP 주소 192.0.2.4 및 첫 번째 EC2 포트 81과 연결됩니다. 다음 수신기 포트인 10002는 첫 번째 서브넷 IP 주소 192.0.2.4 및 두 번째 EC2 포트 82와 연결됩니다. 다음 표에서는 이 예제 매핑이 첫 번째 VPC 서브넷의 마지막 IP 주소를 거쳐 두 번째 VPC 서브넷의 첫 번째 IP 주소로 계속되는 방법을 보여 줍니다.

Global Accelerator	VPC 서브넷	EC2 인스턴스 포트
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84
10005	192.0.2.4	85
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81

Global Accelerator	VPC 서브넷	EC2 인스턴스 포트
12502	192.0.2.244	82
12503	192.0.2.244	83
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89
12520	192.0.3.4	90

사용자 지정 라우팅 가속기에 대한 지침 및 제한 사항

AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기를 생성하고 작업할 때는 다음 지침과 제한 사항에 유의하십시오.

Amazon EC2 인스턴스 대상

사용자 지정 라우팅 액셀러레이터에서 가상 퍼블릭 클라우드 (VPC) 서브넷 엔드포인트는 EC2 인스턴스만 포함할 수 있습니다. 로드 밸런서와 같은 다른 리소스는 사용자 지정 라우팅 가속기에 지원되지 않습니다.

글로벌 액셀러레이터에서 지원되는 EC2 인스턴스 유형은AWS 글로벌 가속기의 표준 가속기에 대한 엔드포인트 (p. 29).

포트 매핑

VPC 서브넷을 추가하면 Global Accelerator는 서브넷에서 지원하는 포트 범위에 대한 리스너 포트 범위의 정적 포트 매핑을 생성합니다. 특정 서브넷에 대한 포트 매핑은 변경되지 않습니다.

프로그래밍 방식으로 사용자 지정 라우팅 액셀러레이터를 위한 포트 매핑 목록을 볼 수 있습니다. 자세한 내용은 `ListCustomRoutingPortMappings` 섹션을 참조하세요.

VPC 서브넷 크기

사용자 지정 라우팅 가속기에 추가하는 VPC 서브넷은 최소 /28이고 최대 /17이어야 합니다.

리스너 포트 범위

리스너 포트 범위를 지정하여 사용자 지정 라우팅 가속기에 추가할 서브넷에 포함된 대상 수를 수용할 수 있도록 충분한 리스너 포트를 지정해야 합니다. 리스너를 생성할 때 지정하는 범위에 따라 사용자 지정 라우팅 가속기와 함께 사용할 수 있는 리스너 포트 및 대상 IP 주소 조합 수가 결정됩니다. 유연성을 극대화하고 사용 가능한 리스너 포트가 충분하지 않다는 오류 발생 가능성을 줄이려면 큰 포트 범위를 지정하는 것이 좋습니다.

글로벌 가속기는 사용자 지정 라우팅 가속기에 서브넷을 추가할 때 블록 단위로 포트 범위를 할당합니다. 리스너 포트 범위를 선형으로 할당하고 원하는 대상 포트 수를 지원할 수 있을 만큼 범위를 크게 만드는 것이 좋습니다. 즉, 할당해야 하는 포트 수는 최소한 서브넷 크기에 서브넷에 있을 대상 포트 및 프로토콜 (대상 구성) 수를 곱한 값이어야 합니다.

Note

글로벌 액셀러레이터가 포트 매핑을 할당하는 데 사용하는 알고리즘에 대해서는 이 합계 이상의 수신기 포트를 추가해야 할 수 있습니다.

리스너를 만든 후에는 리스너를 편집하여 포트 범위 및 연결된 프로토콜을 추가할 수 있지만 기존 포트 범위를 줄일 수는 없습니다. 예를 들어 수신기 포트 범위가 5,000~10,000인 경우 포트 범위를 5900—10,000으로 변경할 수 없으며 포트 범위를 5,000—9,900으로 변경할 수 없습니다.

각 리스너 포트 범위에는 최소 16개의 포트가 포함되어야 합니다. 리스너 포트 1-65535를 지원합니다.

대상 포트 범위

사용자 지정 라우팅 가속기의 포트 범위는 리스너를 추가할 때 지정하는 포트 범위와 끝점 그룹에 대해 지정하는 대상 포트 범위 및 프로토콜의 두 가지가 있습니다.

- 리스너 포트 범위입니다. 클라이언트가 연결하는 글로벌 가속기 정적 IP 주소의 수신기 포트입니다. 글로벌 가속기는 각 포트를 가속기 뒤에 있는 VPC 서브넷의 고유한 대상 IP 주소 및 포트에 매핑합니다.
- 대상 포트 범위입니다. 엔드포인트 그룹에 대해 지정하는 대상 포트 범위 집합 (대상 구성이라고도 함)은 트래픽을 수신하는 EC2 인스턴스 포트입니다. 대상 포트에서 트래픽을 수신하려면 EC2 인스턴스와 연결된 보안 그룹에서 트래픽을 허용해야 합니다.

Health 확인 및 페일오버

글로벌 가속기는 사용자 지정 라우팅 가속기에 대한 상태 확인을 수행하지 않으며 정상 끝점으로 장애 조치하지 않습니다. 사용자 지정 라우팅 가속기의 트래픽은 대상 리소스의 상태에 관계없이 결정적으로 라우팅됩니다.

모든 트래픽은 기본적으로 거부됩니다.

기본적으로 사용자 지정 라우팅 가속기를 통해 전달되는 트래픽은 서브넷의 모든 대상으로 거부됩니다. 대상 인스턴스가 트래픽을 수신할 수 있도록 하려면 서브넷에 대한 모든 트래픽을 특별히 허용하거나 서브넷의 특정 인스턴스 IP 주소 및 포트에 대한 트래픽을 허용해야 합니다.

서브넷이나 특정 대상을 업데이트하여 트래픽을 허용하거나 거부하면 인터넷을 통해 전파되는 데 시간이 걸립니다. 변경 사항이 전파되었는지 확인하려면`DescribeCustomRoutingAccelerator`API 작업을 사용하여 가속기 상태를 확인합니다. 자세한 내용은 단원을 참조하십시오.설명워크스톰 라우팅 가속기.

AWS CloudFormation 션은 지원되지 않습니다.

AWS CloudFormation 은 사용자 지정 라우팅 가속기에 대해 지원되지 않습니다.

AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기

A사용자 지정 라우팅를 사용하면 사용자 지정 애플리케이션 로직을 사용하여 여러 대상 중 한 명 이상의 사용자를 특정 대상으로 안내하는 한편, AWS 글로벌 네트워크를 사용하여 애플리케이션의 가용성과 성능을 향상시킬 수 있습니다.

사용자 지정 라우팅 가속기는 가상 프라이빗 클라우드 (VPC) 서브넷에서 실행 중인 Amazon EC2 인스턴스의 포트로만 트래픽을 라우팅합니다. 사용자 지정 라우팅 가속기를 사용하는 경우 글로벌 가속기는 끝점의 지리적 근접성 또는 상태를 기반으로 트래픽을 라우팅하지 않습니다. 자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식 (p. 37) 단원을 참조하십시오.

가속기를 만들면 기본적으로 글로벌 가속기에서 두 개의 고정 IP 주소 집합을 제공합니다. AWS (BYOIP) 액셀러레이터와 함께 사용할 사용자 풀에서 고정 IP 주소를 할당할 수 있습니다. 자세한 내용은 AWS Global Accelerator 고유 IP 주소 가져오기 (p. 49) 섹션을 참조하세요.

> Important
>
> 가속기를 사용하지 않도록 설정하고 트래픽을 더 이상 허용하거나 라우팅하지 않는 경우에도 IP 주소가 있는 동안 가속기에 할당됩니다. 그러나, 때삭제가속기를 사용하는 경우 가속기에 할당된 글로벌 가속기 고정 IP 주소가 손실되므로 더 이상 이 주소를 사용하여 트래픽을 라우팅할 수 없습니다. 실수로 가속기를 삭제하지 않도록 권한이 있는지 확인하는 것이 좋습니다. 글로벌 가속기와 함께 태그 기반 권한과 같은 IAM 정책을 사용하여 가속기를 삭제할 권한이 있는 사용자를 제한할 수 있습니다. 자세한 내용은 태그 기반 정책 (p. 83) 섹션을 참조하세요.

이 섹션에서는 글로벌 가속기 콘솔에서 사용자 지정 라우팅 가속기를 생성, 편집 또는 삭제하는 방법에 대해 설명합니다. 글로벌 액셀러레이터에서 API 작업을 사용하는 방법에 대한 자세한 내용은AWS Global Accelerator.

주제

사용자 지정 라우팅 액셀러레이터 만들기 또는 업데이트

사용자 지정 라우팅 액셀러레이터를 작성하려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 선택액셀러레이터 만들기.
3. 액셀러레이터의 이름을 제공합니다.
4. 용액셀러레이터 유형를 선택하려면사용자 지정 라우팅.
5. 필요에 따라 자체 IP 주소 범위를 AWS (BYOIP) 로 가져온 경우 해당 주소 풀에서 가속기에 대한 고정 IP 주소를 지정할 수 있습니다. 가속기에 대한 두 개의 정적 IP 주소 각각에 대해 이 옵션을 선택합니다.
   - 각 고정 IP 주소에 대해 사용할 IP 주소 풀을 선택합니다.
   - IP 주소 풀을 선택한 경우 풀에서 특정 IP 주소를 선택합니다. 기본 Amazon IP 주소 풀을 선택한 경우 글로벌 가속기는 가속기에 특정 IP 주소를 할당합니다.
6. 필요에 따라 액셀러레이터 리소스를 쉽게 식별할 수 있도록 하나 이상의 태그를 추가합니다.
7. 선택다음를 클릭하여 마법사의 다음 페이지로 이동하여 리스너, 엔드포인트 그룹 및 VPC 서브넷 엔드포인트를 추가합니다.

사용자 지정 라우팅 액셀러레이터를 편집하려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 사용자 지정 라우팅 액셀러레이터 목록에서 하나를 선택한 다음Edit.
3. 에액셀러레이터 편집페이지에서 원하는 대로 변경합니다. 예를 들어 액셀러레이터를 비활성화하여 삭제할 수 있습니다.
4. 저장을 선택합니다.

사용자 지정 라우팅 가속기 보기

콘솔에서 사용자 지정 라우팅 액셀러레이터에 대한 정보를 볼 수 있습니다. 프로그래밍 방식으로 사용자 지정 라우팅 가속기에 대한 설명을 보려면목록 사용자 지정 라우팅가속기및설명과정라우팅 가속기AWS Global Accelerator API 참조의.

사용자 지정 라우팅 가속기 정보를 보려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 액셀러레이터에 대한 세부 정보를 보려면 액셀러레이터를 선택한 다음보기:.

사용자 지정 라우팅 가속기 삭제

테스트로 사용자 지정 라우팅 가속기를 만들었거나 더 이상 가속기를 사용하지 않는 경우 삭제할 수 있습니다. 콘솔에서 가속기를 비활성화한 다음 삭제할 수 있습니다. 가속기에서 수신기 및 끝점 그룹을 제거할 필요가 없습니다.

콘솔 대신 API 작업을 사용하여 사용자 지정 라우팅 가속기를 삭제하려면 먼저 가속기와 연결된 모든 수신기 및 끝점 그룹을 제거한 다음 비활성화해야 합니다. 자세한 내용은 단원을 참조하십시오.삭제액셀러레이터에서 하는 작업을AWS Global Accelerator.

사용자 지정 라우팅 액셀러레이터를 사용하지 않으려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 목록에서 사용하지 않도록 설정할 액셀러레이터를 선택합니다.
3. [Edit]를 선택합니다.
4. 선택액셀러레이터 비활성화를 선택한 다음Save.

사용자 지정 라우팅 액셀러레이터를 삭제하려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 목록에서 삭제할 액셀러레이터를 선택합니다.
3. 삭제를 선택합니다.

   Note

   액셀러레이터를 비활성화하지 않았다면삭제를 사용할 수 없습니다. 액셀러레이터를 비활성화하려면 이전 절차를 참조하십시오.
4. 확인 대화 상자에서 삭제를 선택합니다.

   Important

   가속기를 삭제하면 가속기에 할당된 고정 IP 주소가 손실되므로 더 이상 해당 가속기를 사용하여 트래픽을 라우팅할 수 없습니다.

AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 위한 리스너

AWS 글로벌 가속기의 사용자 지정 라우팅 가속기의 경우, 글로벌 액셀러레이터가 VPC 서브넷 엔드포인트의 특정 대상 Amazon EC2 인스턴스에 매핑하는 연결된 프로토콜과 함께 수신기 포트 범위를 지정하는 리스너를 구성합니다. VPC 서브넷 엔드포인트를 추가하면 Global Accelerator는 리스너에 대해 정의한 포트 범위와 서브넷의 대상 IP 주소 및 포트 간에 정적 포트 매핑을 생성합니다. 그런 다음 포트 매핑을 사용하여 액셀러레이터 고정 IP 주소를 리스너 포트 및 프로토콜과 함께 지정하여 사용자 트래픽을 VPC 서브넷의 특정 대상 Amazon EC2 인스턴스 IP 주소 및 포트로 보낼 수 있습니다.

사용자 지정 라우팅 액셀러레이터를 생성할 때 리스너를 정의하면 언제라도 언제라도 언제라도 정의하면 언제라도 언제라도 언제라도 언제든지 정의할 수 있습니다. 각 리스너는 VPC 서브넷 엔드포인트가 있는 각 AWS 리전에 대해 하나씩, 하나 이상의 엔드포인트 그룹을 가질 수 있습니다. 사용자 지정 라우팅 가속기의 수신기는 TCP 및 UDP 프로토콜을 모두 지원합니다. 정의하는 각 대상 포트 범위에 대해 프로토콜을 지정합니다. UDP, TCP 또는 UDP 및 TCP 둘 다 사용할 수 있습니다.

자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식 (p. 37) 섹션을 참조하세요.

사용자 지정 라우팅 리스너 추가, 편집 또는 제거

이 단원에서는 AWS Global Accelerator 콘솔에서 사용자 지정 라우팅 리스너를 사용하는 방법에 대해 설명합니다. AWS Global Accelerator API 작업을 사용하는 방법에 대한 자세한 내용은AWS Global Accelerator API.

사용자 지정 라우팅 액셀러레이터를 추가하려면

리스너를 생성할 때 지정하는 범위는 사용자 지정 라우팅 가속기와 함께 사용할 수 있는 리스너 포트 및 대상 IP 주소 조합 수를 정의합니다. 유연성을 극대화하려면 큰 포트 범위를 지정하는 것이 좋습니다. 지정하는 각 리스너 포트 범위에는 최소 16개의 포트가 포함되어야 합니다.

> **Note**
>
> 리스너를 만든 후에는 리스너를 편집하여 포트 범위 및 연결된 프로토콜을 추가할 수 있지만 기존 포트 범위를 줄일 수는 없습니다.

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 리스너 추가를 선택합니다.
4. 에리스너 추가페이지에서 가속기와 연결할 리스너 포트 범위를 입력합니다.

   리스너는 포트 1-65535를 지원합니다. 사용자 지정 라우팅 가속기를 사용하여 유연성을 극대화하려면 큰 포트 범위를 지정하는 것이 좋습니다.
5. 리스너 추가를 선택합니다.

사용자 지정 라우팅 액셀러레이터를 편집하려면

사용자 지정 라우팅 가속기에 대한 리스너를 편집할 때 포트 범위 및 연결된 프로토콜을 추가하거나 기존 포트 범위를 늘리거나 프로토콜을 변경할 수 있지만 기존 포트 범위를 줄일 수는 없습니다.

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 리스너를 선택한 다음리스너 편집.

4. 에리스너 편집페이지에서 기존 포트 범위 또는 프로토콜을 변경하거나 새 포트 범위를 추가합니다.

   기존 포트 범위의 범위를 줄일 수 없습니다.
5. 저장을 선택합니다.

리스너를 제거하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 리스너를 선택한 다음제거.
4. 확인 대화 상자에서제거.

AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 위한 엔드포인트 그룹

엔드포인트 그룹은 AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 사용하여 가상 프라이빗 클라우드 (VPC) 서브넷의 대상 Amazon EC2 인스턴스가 트래픽을 허용하는 포트와 프로토콜을 정의합니다.

VPC 서브넷과 EC2 인스턴스가 위치한 각 AWS 리전에 대한 사용자 지정 라우팅 가속기에 대한 엔드포인트 그룹을 생성합니다. 사용자 지정 라우팅 가속기의 각 엔드포인트 그룹은 여러 VPC 서브넷 엔드포인트를 가질 수 있습니다. 마찬가지로 각 VPC 여러 엔드포인트 그룹에 추가할 수 있지만 엔드포인트 그룹은 서로 다른 리스너와 연결되어야 합니다.

각 엔드포인트 그룹에 대해 리전의 EC2 인스턴스에서 트래픽을 전달하려는 포트가 포함된 하나 이상의 포트 범위 집합을 지정합니다. 각 끝점 그룹 포트 범위에 대해 사용할 프로토콜을 지정합니다. UDP, TCP 또는 UDP 및 TCP 둘 다 사용할 수 있습니다. 따라서 각 프로토콜에 대해 포트 범위 집합을 복제하지 않고도 유연성을 극대화할 수 있습니다. 예를 들어 포트 8080-8090에서 UDP를 통해 게임 트래픽이 실행되는 게임 서버가 있고 포트 80에서 TCP를 통해 채팅 메시지를 수신하는 서버가 있을 수 있습니다.

자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식 (p. 37) 단원을 참조하십시오.

사용자 지정 라우팅 액셀러레이터를 위한 엔드포인트 그룹 추가, 편집 또는 제거

AWS Global Accelerator 콘솔에서 또는 API 작업을 사용하여 사용자 지정 라우팅 가속기에 대한 엔드포인트 그룹으로 작업합니다. 언제든지 엔드포인트 그룹에서 VPC 서브넷 엔드포인트를 추가하거나 엔드포인트 그룹에서 제거할 수 있습니다.

이 섹션에서는 AWS Global Accelerator 콘솔에서 사용자 지정 라우팅 가속기에 대한 엔드포인트 그룹을 사용하는 방법에 대해 설명합니다. 글로벌 액셀러레이터에서 API 작업을 사용하는 방법에 대한 자세한 내용은AWS Global Accelerator API 참조.

사용자 지정 라우팅 액셀러레이터를 위한 엔드포인트 그룹을 추가하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 을 선택합니다.리스너 ID에서 엔드포인트 그룹을 추가할 리스너의 ID를 선택합니다.
4. 선택엔드포인트 그룹을 추가합니다..

5. 리스너 섹션에서 끝점 그룹에 대한 Region을 지정합니다.
6. 용포트 및 프로토콜 세트에 Amazon EC2 인스턴스의 포트 범위 및 프로토콜을 입력합니다.

   - 를 입력합니다.포트에서및대상 포트를 입력하여 포트 범위를 지정합니다.
   - 각 포트 범위에 대해 해당 범위의 프로토콜을 지정합니다.

   포트 범위는 리스너 포트 범위의 하위 집합일 필요는 없지만 리스너 포트 범위에 사용자 지정 라우팅 가속기의 끝점 그룹에 대해 지정한 총 포트 수를 지원할 수 있는 충분한 총 포트가 있어야 합니다.
7. 저장을 선택합니다.
8. 필요에 따라엔드포인트 그룹을 추가합니다.를 클릭하여 이 리스너의 엔드포인트 그룹을 추가합니다. 다른 수신기를 선택하고 끝점 그룹을 추가할 수도 있습니다.
9. 선택엔드포인트 그룹을 추가합니다..

사용자 지정 라우팅 액셀러레이터를 위한 엔드포인트 그룹을 편집하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 을 선택합니다.리스너 ID에서 엔드포인트 그룹이 연결된 리스너의 ID를 선택합니다.
4. 선택엔드포인트 그룹 편집.
5. 에서엔드포인트 그룹 편집페이지에서 Region, 포트 범위 또는 포트 범위에 대한 프로토콜을 변경합니다.
6. 저장을 선택합니다.

사용자 지정 라우팅 액셀러레이터를 제거하려면

1. 글로벌 액셀러레이터 콘솔을https://console.aws.amazon.com/globalaccelerator/home.
2. 에서액셀러레이터페이지에서 액셀러레이터를 선택합니다.
3. 에서리스너섹션에서 리스너를 선택한 다음제거.
4. 에서엔드포인트 그룹섹션에서 엔드포인트 그룹을 선택한 다음제거.
5. 확인 대화 상자에서 을 선택합니다.제거.

AWS 글로벌 액셀러레이터의 사용자 지정 라우팅 가속기를 위한 VPC 서브넷 엔드포인트

사용자 지정 라우팅 가속기의 끝점은 가속기를 통해 트래픽을 수신할 수 있는 VPC (가상 프라이빗 클라우드) 서브넷입니다. 각 서브넷에는 하나 이상의 Amazon EC2 인스턴스 대상이 포함될 수 있습니다. 서브넷 끝점을 추가하면 글로벌 가속기가 새 포트 매핑을 생성합니다. 그런 다음 글로벌 액셀러레이터 API를 사용하여 서브넷에 대한 모든 포트 매핑의 정적 목록을 가져올 수 있습니다. 이 목록을 사용하여 서브넷의 대상 EC2 인스턴스 IP 주소로 트래픽을 라우팅할 수 있습니다. 자세한 내용은 단원을 참조하십시오.목록 사용자 지정 라우팅포트매핑.

서브넷의 EC2 인스턴스로만 트래픽을 보낼 수 있으며 로드 밸런서와 같은 다른 리소스는 보낼 수 없습니다 (표준 가속기와 달리). 지원되는 EC2 인스턴스 유형은AWS 글로벌 가속기의 표준 가속기에 대한 엔드포인트 (p. 29).

자세한 내용은 AWS 글로벌 액셀러레이터에서 사용자 지정 라우팅 가속기의 작동 방식 (p. 37) 단원을 참조하십시오.

사용자 지정 라우팅 가속기에 VPC 서브넷을 추가할 때는 다음 사항에 유의하십시오.

- 기본적으로 사용자 지정 라우팅 가속기를 통해 전달되는 트래픽은 서브넷의 어떤 목적지에도 도착할 수 없습니다. 대상 인스턴스가 트래픽을 수신하도록 하려면 서브넷에 대한 모든 트래픽을 허용하도록 선택하거나 서브넷의 특정 인스턴스 IP 주소 및 포트 (대상 소켓) 에 대한 트래픽을 활성화해야 합니다.

  Important

  서브넷이나 특정 대상을 업데이트하여 트래픽을 허용하거나 거부하면 인터넷을 통해 전파되는 데 시간이 걸립니다. 변경 사항이 전파되었는지 확인하려면`DescribeCustomRoutingAccelerator`API 작업을 사용하여 가속기 상태를 확인할 수 있습니다. 자세한 내용은 단원을 참조하십시오.설명컴포트라우팅액셀러레이터.
- VPC 서브넷은 클라이언트 IP 주소를 보존하므로 서브넷을 사용자 지정 라우팅 가속기의 엔드포인트로 추가할 때 관련 보안 및 구성 정보를 검토해야 합니다. 자세한 내용은 클라이언트 IP 주소 보존을 사용하여 엔드포인트 추가 (p. 33) 섹션을 참조하세요.

VPC 서브넷 엔드포인트 추가, 편집 또는 제거

사용자 지정 라우팅 가속기의 엔드포인트 그룹에 가상 프라이빗 클라우드 (VPC) 서브넷 엔드포인트를 추가하여 서브넷의 대상 Amazon EC2 인스턴스로 사용자 트래픽을 보낼 수 있습니다.

서브넷에서 EC2 인스턴스를 추가 및 제거하거나 EC2 대상에 대한 트래픽을 활성화 또는 비활성화할 때 해당 대상이 트래픽을 수신할 수 있는지 여부를 변경합니다. 그러나 전역 가속기 포트 매핑은 변경되지 않습니다.

서브넷의 일부 대상으로의 트래픽 (전부는 아님) 을 허용하려면 허용할 각 EC2 인스턴스의 IP 주소와 트래픽을 수신할 인스턴스의 포트를 입력합니다. 지정하는 IP 주소는 서브넷의 EC2 인스턴스용이어야 합니다. 서브넷에 대해 매핑된 포트에서 포트 또는 포트 범위를 지정할 수 있습니다.

엔드포인트 그룹에서 VPC 서브넷을 제거하여 가속기에서 VPC 서브넷을 제거할 수 있습니다. 서브넷을 제거해도 서브넷 자체에는 영향을 주지 않지만 글로벌 액셀러레이터는 더 이상 서브넷이나 서브넷의 Amazon EC2 인스턴스로 트래픽을 보낼 수 없습니다. 또한 글로벌 액셀러레이터는 VPC 서브넷에 대한 포트 매핑을 회수하여 추가한 새 서브넷에 사용할 수 있습니다.

이 섹션의 단계에서는 AWS Global Accelerator 콘솔에서 VPC 서브넷 엔드포인트를 추가, 편집 또는 제거하는 방법에 대해 설명합니다. AWS Global Accelerator API 작업을 사용하는 방법에 대한 자세한 내용은AWS Global Accelerator API 참조 참조.

VPC 서브넷 엔드포인트를 추가하려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션,리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서그룹 그룹섹션,엔드포인트 그룹 ID에서 VPC 서브넷 엔드포인트를 추가할 엔드포인트 그룹 (AWS 리전) 의 ID를 선택합니다.
5. 에서엔드포인트섹션에서엔드포인트 추가.
6. 에끝점 추가페이지에 대한엔드포인트에서 VPC 서브넷을 선택합니다.

   VPC가 없는 경우 목록에 항목이 없는 것입니다. 계속하려면 하나 이상의 VPC 추가한 다음 여기로 돌아와 목록에서 VPC를 선택합니다.
7. 추가하는 VPC 서브넷 엔드포인트의 경우 서브넷의 모든 대상에 대한 트래픽을 허용 또는 거부하도록 선택하거나 특정 EC2 인스턴스 및 포트에 대한 트래픽만 허용할 수 있습니다. 기본값은 서브넷의 모든 대상에 대한 트래픽을 거부하는 것입니다.
8. Add endpoint(엔드포인트 추가)를 선택합니다.

특정 대상에 대한 트래픽을 허용하거나 거부하려면

엔드포인트의 VPC 서브넷 포트 매핑을 편집하여 서브넷의 특정 EC2 인스턴스 및 포트 (대상 소켓) 로의 트래픽을 허용하거나 거부할 수 있습니다.

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션,리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서그룹 그룹섹션,엔드포인트 그룹 ID에서 편집할 VPC 서브넷 엔드포인트의 엔드포인트 그룹 (AWS 리전) ID를 선택합니다.
5. 엔드포인트 서브넷을 선택한 후세부 정보 보기.
6. 에엔드포인트페이지의포트 매핑를 선택하고 IP 주소를 선택한 다음Edit.
7. 트래픽을 활성화할 포트를 입력한 후대상 허용.

서브넷에 대한 모든 트래픽을 허용하거나 거부하려면

엔드포인트를 업데이트하여 VPC 서브넷의 모든 대상에 대한 트래픽을 허용하거나 거부할 수 있습니다.

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션,리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서그룹 그룹섹션,엔드포인트 그룹 ID에서 업데이트할 VPC 서브넷 엔드포인트의 엔드포인트 그룹 (AWS 리전) ID를 선택합니다.
5. 선택허용/거부.
6. 옵션을 선택하여 모든 트래픽을 허용하거나 모든 트래픽을 거부한 다음Save.

끝점을 제거하려면

1. 다음 위치에서 글로벌 가속기 콘솔을 엽니다.https://console.aws.amazon.com/globalaccelerator/home.
2. 에액셀러레이터페이지에서 사용자 지정 라우팅 액셀러레이터를 선택합니다.
3. 에서리스너섹션,리스너 ID에서 리스너의 ID를 선택합니다.
4. 에서그룹 그룹섹션,엔드포인트 그룹 ID에서 제거하려는 VPC 서브넷 엔드포인트의 엔드포인트 그룹 (AWS 리전) ID를 선택합니다.
5. 선택엔드포인트 제거.
6. 확인 대화 상자에서 [] 를 선택합니다.제거.

AWS Global Accelerator 터의 DNS 주소 지정 및 사용자 지정 도메인

이 장에서는 AWS Global Accelerator 터가 DNS 라우팅을 수행하는 방법에 대해 설명하고 글로벌 액셀러레이터에서 사용자 지정 도메인을 사용하는 방법에 대한 정보를 제공합니다.

주제

글로벌 액셀러레이터에서 DNS 주소 지정 Support

사용자 지정 라우팅 또는 표준 가속기를 만들 때 글로벌 가속기는 두 개의 정적 IP 주소를 프로비저닝합니다. 가속기에 기본 설정된 DNS (Domain Name System) 이름을 할당합니다.`a1234567890abcdef.awsglobalaccelerator.com`, 정적 IP 주소를 가리키는. 정적 IP 주소는 AWS 엣지 네트워크에서 엔드포인트까지 anycast를 사용하여 전역적으로 광고됩니다. 가속기의 고정 IP 주소 또는 DNS 이름을 사용하여 트래픽을 가속기로 라우팅할 수 있습니다. DNS 서버와 DNS 확인자는 라운드 로빈을 사용하여 가속기의 DNS 이름을 확인합니다. 따라서 이름은 가속기의 정적 IP 주소로 확인되고 Amazon Route 53에서 임의의 순서로 반환됩니다. 일반적으로 클라이언트는 반환되는 첫 번째 IP 주소를 사용합니다.

> Note
>
> 글로벌 가속기는 역방향 DNS 조회를 지원하기 위해 가속기의 정적 IP 주소를 글로벌 가속기에서 생성된 해당 DNS 이름에 매핑하는 두 개의 PTR (포인터) 레코드를 만듭니다. 이를 역방향 호스팅 영역이라고도 합니다. 글로벌 액셀러레이터가 생성하는 DNS 이름은 구성할 수 없으며 사용자 지정 도메인 이름을 가리키는 PTR 레코드를 만들 수 없습니다. 글로벌 액셀러레이터는 AWS (BYOIP) 로 가져오는 IP 주소 범위에서 고정 IP 주소에 대한 PTR 레코드도 생성하지 않습니다.

사용자 지정 도메인 트래픽을 가속기로 라우팅

대부분의 시나리오에서는 사용자 지정 도메인 이름을 사용하도록 DNS를 구성할 수 있습니다 (예:`www.example.com`) 을 할당된 정적 IP 주소 또는 기본 DNS 이름을 사용하는 대신 가속기로 연결합니다. 먼저 Amazon Route 53 또는 다른 DNS 공급자를 사용하여 도메인 이름을 생성한 다음 글로벌 액셀러레이터 IP 주소로 DNS 레코드를 추가하거나 업데이트합니다. 또는 사용자 지정 도메인 이름을 가속기의 DNS 이름과 연결할 수 있습니다. DNS 구성을 완료하고 변경 사항이 인터넷을 통해 전파될 때까지 기다립니다. 이제 클라이언트가 사용자 지정 도메인 이름을 사용해 요청을 하면 DNS 서버는 이를 임의의 순서로 IP 주소 또는 가속기의 DNS 이름으로 해석합니다.

Route 53을 DNS 서비스로 사용할 때 글로벌 가속기와 함께 사용자 지정 도메인 이름을 사용하려면 사용자 지정 도메인 이름을 가속기에 할당된 DNS 이름으로 가리키는 별칭 레코드를 생성합니다. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는 루트 도메인 (예: 루트 도메인) 에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하고, CNAME 레코드와 유사합니다.`example.com`및 하위 도메인 (예:`www.example.com`. 자세한 내용은 단원을 참조하십시오.별칭 또는 비 별칭 레코드 선택Amazon Route 53 개발자 안내서에 나와 있습니다.

가속기에 대한 별칭 레코드로 Route 53을 설정하려면 다음 항목에 포함된 지침을 따르십시오. 별칭 대상Amazon Route 53 개발자 안내서에 나와 있습니다. 글로벌 가속기에 대한 정보를 보려면별칭 대상페이지를 참조하십시오.

AWS Global Accelerator 고유 IP 주소 가져오기

AWS Global Accelerator 터는 고정 IP 주소를 액셀러레이터의 진입점으로 사용합니다. 이러한 IP 주소는 AWS 엣지 로케이션의 애니 캐스트입니다. 기본적으로 글로벌 가속기는Amazon IP 주소 풀. 글로벌 액셀러레이터가 제공하는 IP 주소를 사용하는 대신 고유한 주소 범위의 IPv4 주소로 이러한 진입점을 구성할 수 있습니다. 이 항목에서는 글로벌 가속기에서 고유한 IP 주소 범위를 사용하는 방법에 대해 설명합니다.

온프레미스 네트워크에서 AWS 계정으로 모든 퍼블릭 IPv4 주소 범위의 일부 또는 전체를 가져와 글로벌 액셀러레이터와 함께 사용할 수 있습니다. 주소 범위는 계속해서 소유할 수 있지만 AWS 인터넷에서 이러한 주소 범위를 알립니다.

한 AWS 서비스에 대해 AWS 로 가져온 IP 주소는 다른 서비스와 함께 사용할 수 없습니다. 이 장의 단계에서는 AWS Global Accelerator 기에서만 사용할 IP 주소 범위를 가져오는 방법에 대해 설명합니다. Amazon EC2 2에서 사용할 고유 IP 주소 범위를 가져오는 단계는 단원을 참조하십시오.고유 IP 주소 가져오기 (BYOIP)Amazon EC2 사용 설명서의 내용을 참조하십시오.

> Important
>
> AWS 를 통해 알리기 전에 다른 위치에서 IP 주소 범위 알리기를 중지해야 합니다. IP 주소 범위가 멀티홈인 경우 (즉, 범위를 여러 서비스 제공업체가 동시에 광고하는 경우) 주소 범위로의 트래픽이 당사 네트워크에 들어가거나 BYOIP 광고 워크플로가 성공적으로 완료된다고 보장할 수 없습니다.

AWS 로 주소 범위를 가져오면 해당 주소가 계정에 주소 풀로 나타납니다. 가속기를 만들 때 범위에서 하나의 IP 주소를 할당할 수 있습니다. 글로벌 액셀러레이터는 Amazon IP 주소 범위에서 두 번째 고정 IP 주소를 할당합니다. 두 개의 IP 주소 범위를 AWS 로 가져오는 경우 각 범위에서 하나의 IP 주소를 가속기에 할당할 수 있습니다. 글로벌 액셀러레이터는 고가용성을 위해 각 주소 범위를 다른 네트워크 영역에 할당하기 때문입니다.

글로벌 액셀러레이터에서 고유한 IP 주소 범위를 사용하려면 요구 사항을 검토한 다음 이 항목에 제공된 단계를 따릅니다.

주제

Requirements

AWS 계정당 AWS Global Accelerator 터로 최대 두 개의 적격 IP 주소 범위를 가져올 수 있습니다.

자격을 얻으려면 IP 주소 범위가 다음 요구 사항을 충족해야 합니다.

- IP 주소 범위를 ARIN (미국 인터넷 번호 등록 기관), RIPE (Réseaux IP Européens Network Coordination Centre) 또는 APNIC (아시아 태평양 지역 네트워크 정보 센터) 와 같은 RIR (지역 인터넷 등록 기관) 에 등록해야 합니다. 주소 범위는 사업체 또는 기관에 등록되어야 합니다. 개인에게는 등록할 수 없습니다.
- 가져올 수 있는 가장 구체적인 주소 범위는 /24입니다. IP 주소의 처음 24비트는 네트워크 번호를 지정합니다. 예를 들어 198.51.100은 IP 주소 198.51.100.0의 네트워크 번호입니다.
- 주소 범위의 IP 주소에는 명확한 기록이 있어야 합니다. 즉, 그들은 평판이 좋지 않거나 악의적 인 행동과 연관 될 수 없습니다. 당사는 IP 주소 범위의 평판을 조사할 수 있으며, 깨끗한 기록이 없는 IP 주소가 포함된 것으로 판단되는 경우 IP 주소 범위를 거부할 권한을 보유합니다.

또한 IP 주소 범위를 등록한 위치에 따라 다음과 같은 할당 및 할당 네트워크 유형 또는 상태가 필요합니다.

- 아린:`Direct Allocation`및`Direct Assignment`네트워크 유형
- 익은:`ALLOCATED PA`,`LEGACY`, 및`ASSIGNED PI`할당 상태
- APNIC:`ALLOCATED PORTABLE`및`ASSIGNED PORTABLE`할당 상태

AWS 계정으로 IP 주소 범위를 가져오기 위해 준비하려면 다음 단계를 따르세요. 승인

귀하 만 아마존에 IP 주소 공간을 가져올 수 있도록 하려면 다음 두 가지 승인이 필요합니다.

- 귀하는 아마존에 IP 주소 범위를 광고하도록 승인해야 합니다.
- IP 주소 범위를 소유하고 있다는 증거를 제공해야 하며, 이를 AWS 로 가져올 권한이 있어야 합니다.

  Note

  BYOIP를 사용하여 IP 주소 범위를 AWS 로 가져오는 경우 광고하는 동안 해당 주소 범위의 소유권을 다른 계정 또는 회사로 이전할 수 없습니다. 또한 한 AWS 계정에서 다른 계정으로 IP 주소 범위를 직접 전송할 수는 없습니다. 소유권을 이전하거나 AWS 계정 간에 이전하려면 주소 범위를 프로비저닝 해제해야 합니다. 그런 다음 새 소유자는 단계에 따라 주소 범위를 AWS 계정에 추가해야 합니다.

아마존에 IP 주소 범위를 광고하도록 승인하려면 아마존에 서명된 승인 메시지를 제공해야 합니다. ROA (경로 원본 권한 부여) 를 사용하여 이 권한을 제공합니다. ROA는 RIR (지역 인터넷 등록 기관) 를 통해 생성하는 경로 알림에 대한 암호화 설명입니다. ROA는 IP 주소 범위, IP 주소 범위를 알리도록 허용된 자율 시스템 번호 (ASN) 와 만료 날짜가 포함되어 있습니다. ROA는 Amazon에 특정 자율 시스템 (AS) 에서 IP 주소 범위를 알리도록 권한을 부여합니다.

ROA는 AWS 계정에 IP 주소 범위를 AWS로 가져올 수 있는 권한을 부여하지 않습니다. 이 권한을 제공하려면 IP 주소 범위에 대한 등록 데이터 액세스 프로토콜 (R) 설명에 자체 서명된 X.509 인증서를 게시해야 합니다. 이 인증서에는 제공한 권한 부여-컨텍스트 서명을 확인하기 위해 AWS이(가) 사용하는 퍼블릭 키가 포함되어 있습니다. 프라이빗 키는 안전하게 보관하고, 권한 부여-컨텍스트 메시지에 서명하는 데 사용하십시오.

다음 섹션에서는 이러한 권한 부여 작업을 완료하기 위한 자세한 단계를 제공합니다. 이 단계의 명령은 Linux에서 지원됩니다. Windows를 사용하는 경우Windows Subsystem for Linux를 사용하여 Linux 명령을 실행할 수 있습니다.

권한 부여를 제공하는 단계

- 단계 1: ROA 객체 생성 (p. 50)
- 단계 2: 자체 서명된 X.509 인증서 생성 (p. 51)
- 단계 3: 서명된 권한 부여 메시지 생성 (p. 51)

단계 1: ROA 객체 생성

ROA 객체를 생성하여 Amazon ASN 16509가 IP 주소 범위를 공급하도록 권한을 부여하고 현재 IP 주소 범위의 공급 권한이 있는 ASN이 IP 주소 범위를 공급하도록 권한을 부여합니다. ROA는 AWS 로 가져올 /24 IP 주소를 포함해야 하며, 최대 길이를 /24로 설정해야 합니다.

ROA 요청 생성에 대한 자세한 내용은 IP 주소 범위를 등록한 위치에 따라 다음 섹션을 참조하십시오.

- 아린: ROA 요청
- 익은: ROAS 관리
- APNIC: 라우팅 관리

단계 2: 자체 서명된 X.509 인증서 생성

key pair 어와 자체 서명된 X.509 인증서를 만들고 RIR에 대한 R레코드에 인증서를 추가합니다. 다음 단계에서는 이러한 작업을 수행하는 방법을 설명합니다.

> Note
>
> 이`openssl`명령에는 OpenSSL 버전 1.0.2 이상이 필요합니다.

X.509 인증서를 만들고 추가하려면

1. 다음 명령을 사용하여 RSA 2048비트 key pair 생성합니다.

```
openssl genrsa -out private.key 2048
```

2. 다음 명령을 사용하여 key pair 어에서 퍼블릭 X.509 인증서를 생성합니다.

```
openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
```

   이 예제에서 인증서는 365일이 지나면 만료되므로, 이 기간이 지난 후에는 신뢰할 수 없습니다. 명령을 실행할 때는`-days`옵션을 올바른 만료에 대해 원하는 값으로 설정합니다. 다른 정보를 입력하라는 메시지가 표시되면 기본값을 수락할 수 있습니다.

3. RIR에 따라 다음 단계를 사용하여 RIR에 대한 R레코드를 업데이트합니다.

   1. 다음 명령을 사용하여 인증서를 봅니다.

```
cat publickey.cer
```

   2. 다음을 수행하여 인증서를 추가합니다.

      > Important
      >
      > 반드시 포함해야 합니다.`-----BEGIN CERTIFICATE-----`및`-----END CERTIFICATE-----`인증서로부터.

      - ARIN의 경우`Public Comments`IP 주소 범위 섹션을 참조하십시오.
      - RIPE의 경우 인증서를 새`descr`IP 주소 범위의 필드를 선택합니다.
      - APNIC의 경우 전자 메일의 공개 키를`helpdesk@apnic.net`에서 IP 주소의 APNIC 공인 연락처를 사용하여`remarks`필드를 선택합니다.

단계 3: 서명된 권한 부여 메시지 생성

아마존이 귀하의 IP 주소 범위를 광고할 수 있도록 서명된 인증 메시지를 생성합니다.

메시지 형식은 다음과 같으며`YYYYMMDD`date는 메시지의 만료 날짜입니다.

```
1|aws|aws-account|address-range|YYYYMMDD|SHA256|RSAPSS
```

서명된 권한 부여 메시지를 만들려면

1. 일반 텍스트 권한 부여 메시지를 만들고 라는 변수에 저장합니다.`text_message`다음 예제와 같이. 예제 계정 번호, IP 주소 범위 및 만료 날짜를 해당 값으로 바꿉니다.

```
text_message="1|aws|123456789012|203.0.113.0/24|20191201|SHA256|RSAPSS"
```

2. 인증 메시지에 서명하십시오.`text_message`이전 섹션에서 생성한 key pair 사용합니다.

3. 라는 변수에 메시지를 저장`signed_message`다음 예제와 같이.

```
signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt
      rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform PEM |
 openssl base64 |
      tr -- '+=/' '-_~' | tr -d "\n")
```

AWS Global Accelerator 사용할 수 있도록 주소 범위 프로비저닝

AWS 에서 사용할 수 있도록 주소 범위를 프로비저닝하는 경우 주소 범위를 소유하고 있는지 확인하고 Amazon에 해당 주소 범위를 알리도록 권한을 부여합니다. 주소 범위를 소유하고 있는지는 확인합니다.

CLI 또는 글로벌 액셀러레이터 API 작업을 사용하여 주소 범위를 프로비저닝해야 합니다. AWS 콘솔에서 이 기능을 사용할 수 없습니다.

주소 범위를 프로비저닝하려면 다음을 사용합니다.ProvisionByoipCidr명령입니다. `--cidr-authorization-context` 파라미터는 ROA 메시지가 아니라 이전 섹션에서 생성한 변수를 사용합니다.

```
aws globalaccelerator provision-byoip-cidr --cidr address-range --cidr-authorization-
context Message="$text_message",Signature="$signed_message"
```

다음은 주소 범위를 프로비저닝하는 예입니다.

```
aws globalaccelerator provision-byoip-cidr
    --cidr 203.0.113.25/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

주소 범위 프로비저닝은 비동기 작업이므로 호출이 즉시 반환됩니다. 그러나 주소 범위는 상태가 변경될 때까지 사용할 준비가 되지 않았습니다.`PENDING_PROVISIONING`to`READY`. 프로비저닝 프로세스를 완료하는 데 최대 3주까지 걸릴 수 있습니다. 프로비저닝한 주소 범위의 상태를 모니터링하려면 다음목록보IPCIDR명령:

```
aws globalaccelerator list-byoip-cidrs
```

IP 주소 범위에 대한 상태 목록을 보려면바이아이프씨더.

IP 주소 범위가 프로비저닝되면`State`에서 반환한`list-byoip-cidrs`확장하는 데`READY`. 예:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "READY"
        }
    ]
}
```

AWS을(를) 통해 주소 범위 알리기

주소 범위가 프로비저닝되면 알릴 준비가 된 것입니다. 프로비저닝한 정확한 주소 범위를 알려야 합니다. 프로비저닝한 주소 범위의 일부만 알릴 수 없습니다. 또한 AWS 를 통해 알리기 전에 다른 위치에서 IP 주소 범위 알리기를 중지해야 합니다.

CLI 또는 글로벌 액셀러레이터 API 작업을 사용하여 주소 범위를 광고하거나 광고를 중지해야 합니다. AWS 콘솔에서 이 기능을 사용할 수 없습니다.

> Important
>
> 글로벌 액셀러레이터를 사용하여 풀의 IP 주소를 사용하기 전에 AWS 에서 IP 주소 범위를 알려야 합니다.

주소 범위를 알리려면 다음을 사용합니다.광고바이오익시더명령입니다.

```
aws globalaccelerator advertise-byoip-cidr --cidr address-range
```

다음은 주소 범위를 광고하도록 글로벌 액셀러레이터를 요청하는 예입니다.

```
aws globalaccelerator advertise-byoip-cidr --cidr 203.0.113.0/24
```

알린 주소 범위의 상태를 모니터링하려면 다음목록보IPCIDR명령입니다.

```
aws globalaccelerator list-byoip-cidrs
```

IP 주소 범위가 보급되면State에서 반환한list-byoip-cidrs확장하는 데ADVERTISING. 예:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "ADVERTISING"
        }
    ]
}
```

주소 범위 알리기를 중지하려면 다음withdraw-byoip-cidr명령입니다.

> Important
>
> 주소 범위 광고를 중지하려면 먼저 주소 풀에서 할당된 고정 IP 주소가 있는 가속기를 제거해야 합니다. 콘솔 또는 API 작업을 사용하여 가속기를 삭제하려면 액셀러레이터를 삭제하려면 (p. 21).

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

다음은 글로벌 액셀러레이터에 주소 범위를 철회하도록 요청하는 예입니다.

```
aws globalaccelerator withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

주소 범위 프로비저닝 취소

AWS 에서 주소 범위 사용을 중지하려면 먼저 주소 풀에서 할당되는 고정 IP 주소가 있는 가속기를 모두 제거하고 주소 범위 알리기를 중지해야 합니다. 이러한 단계를 완료한 후 주소 범위를 프로비저닝 해제할 수 있습니다.

CLI 또는 글로벌 액셀러레이터 API 작업을 사용하여 광고를 중지하고 주소 범위를 프로비저닝 해제해야 합니다. AWS 콘솔에서 이 기능을 사용할 수 없습니다.

단계 1: 연결된 액셀러레이터를 모두 삭제합니다. 콘솔 또는 API 작업을 사용하여 가속기를 삭제하려면 액셀러레이터를 삭제하려면 (p. 21).

단계 2. 주소 범위 알리기를 중지합니다. 범위 알리기를 중지하려면 다음을 사용합니다.바이오익시더명령입니다.

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

단계 3. 주소 범위 프로비저닝을 취소하십시오. 범위를 프로비저닝 해제하려면 다음을 사용하십시오.디프로비전 바이오익시더명령입니다.

```
aws globalaccelerator deprovision-byoip-cidr --cidr address-range
```

IP 주소로 가속기 만들기

이제 IP 주소로 가속기를 만들 수 있습니다. 하나의 주소 범위를 AWS 로 가져온 경우 가속기에 하나의 IP 주소를 할당할 수 있습니다. 두 개의 주소 범위를 가져온 경우 각 주소 범위에서 하나의 IP 주소를 가속기에 할당할 수 있습니다.

고정 IP 주소에 대해 사용자 고유의 IP 주소를 사용하여 가속기를 만드는 몇 가지 옵션이 있습니다.

- 글로벌 가속기 콘솔을 사용하여 가속기를 만듭니다. 자세한 내용은 표준 액셀러레이터 만들기 또는 업데이트 (p. 21) 및 사용자 지정 라우팅 액셀러레이터 만들기 또는 업데이트 (p. 41) 섹션을 참조하세요.
- 글로벌 가속기 API를 사용하여 가속기를 만듭니다. CLI 사용 예제를 포함하여 자세한 내용을 보려면 단원을 참조하십시오.액셀러레이터 만들기및사용자 정의 라우팅가속기 만들기AWS Global Accelerator API 참조의.

AWS Global Accelerator 클라이언트 IP 주소 보존

AWS 글로벌 액셀러레이터의 클라이언트 IP 주소를 보존하고 액세스하는 옵션은 가속기를 사용하여 설정한 엔드포인트에 따라 다릅니다. 들어오는 패킷에서 클라이언트의 원본 IP 주소를 보존할 수 있는 끝점에는 두 가지 유형이 있습니다. 애플리케이션 로드 밸런서 및 Amazon EC2 인스턴스

- 글로벌 가속기를 사용하여 인터넷 연결 Application Load Balancer 엔드포인트로 사용하는 경우 새 가속기에 대해 클라이언트 IP 주소 보존이 기본적으로 활성화됩니다. 즉, 로드 밸런서에 도착하는 패킷에 대해 원본 클라이언트의 원본 IP 주소가 보존됩니다. 가속기를 만들 때 또는 나중에 가속기를 편집하여 이 옵션을 비활성화하도록 선택할 수 있습니다.
- 글로벌 액셀러레이터와 함께 내부 Application Load Balancer 또는 EC2 인스턴스를 사용하는 경우 엔드포인트에 항상 클라이언트 IP 주소 보존이 활성화됩니다.

> **Note**
>
> 글로벌 가속기는 Network Load Balancer 및 엘라스틱 IP 주소 끝점에 대한 클라이언트 IP 주소 보존을 지원하지 않습니다.

클라이언트 IP 주소 보존을 추가할 계획인 경우 다음 사항을 숙지해야 합니다.

- 클라이언트 IP 주소를 보존하는 끝점으로 트래픽을 추가하고 라우팅하기 전에 보안 그룹과 같은 모든 필수 보안 구성이 허용 목록에 사용자 클라이언트 IP 주소를 포함하도록 업데이트되었는지 확인합니다.
- 클라이언트 IP 주소 보존은 특정 AWS 리전에서만 지원됩니다. 자세한 내용은 클라이언트 IP 주소 보존을 위해 지원되는 AWS 리전 (p. 58) 섹션을 참조하세요.

주제

클라이언트 IP 주소 보존을 사용하도록 설정하는 방법

새 가속기를 만들면 지원되는 끝점에 대해 기본적으로 클라이언트 IP 주소 보존이 활성화됩니다.

다음에 유의하십시오.

- 내부 애플리케이션 로드 밸런서 및 EC2 인스턴스에는 항상 클라이언트 IP 주소 보존이 활성화되어 있습니다. 이러한 엔드포인트에 대해서는 옵션을 비활성화할 수 없습니다.
- AWS 콘솔을 사용하여 새 가속기를 생성하는 경우 Application Load Balancer 엔드포인트에 대해 클라이언트 IP 주소 보존 옵션이 기본적으로 활성화됩니다. 인터넷 연결 Application Load Balancer 끝점에 대해 클라이언트 IP 주소를 보존하지 않으려면 언제든지 이 옵션을 비활성화할 수 있습니다.
- AWS CLI 또는 API 작업을 사용하여 새 가속기를 생성하고 클라이언트 IP 주소 보존 옵션을 지정하지 않으면 인터넷 연결 Application Load Balancer 엔드포인트에 클라이언트 IP 주소 보존이 기본적으로 활성화되어 있습니다.

- 글로벌 가속기는 Network Load Balancer 및 엘라스틱 IP 주소 끝점에 대한 클라이언트 IP 주소 보존을 지원하지 않습니다.

기존 가속기의 경우 클라이언트 IP 주소를 보존하지 않고 끝점을 클라이언트 IP 주소를 보존하는 끝점으로 전환할 수 있습니다. 기존 Application Load Balancer 엔드포인트를 새로운 Application Load Balancer 엔드포인트로 전환할 수 있으며, 기존 엘라스틱 IP 주소 엔드포인트를 EC2 인스턴스 엔드포인트로 전환할 수 있습니다. Network Load Balancer 끝점은 클라이언트 IP 주소 보존을 지원하지 않습니다. 새 끝점으로 전환하려면 다음을 수행하여 기존 끝점에서 클라이언트 IP 주소가 보존된 새 끝점으로 트래픽을 느리게 이동하는 것이 좋습니다.

- 기존 Application Load Balancer 엔드포인트의 경우 먼저 글로벌 가속기에 동일한 백엔드를 대상으로 하는 중복 Application Load Balancer 끝점을 추가하고, 인터넷 연결 애플리케이션 로드 밸런서인 경우 클라이언트 IP 주소 보존을 활성화합니다. 그런 다음 엔드포인트의 가중치를 조정하여하지로드 밸런서에 클라이언트 IP 주소 보존이 활성화되어 있어야 합니다.다음으로 바꿉니다.클라이언트 IP 주소
- 기존 엘라스틱 IP 주소 엔드포인트의 경우 클라이언트 IP 주소를 보존하여 EC2 인스턴스 엔드포인트로 트래픽을 이동할 수 있습니다. 먼저 EC2 인스턴스 엔드포인트를 글로벌 액셀러레이터에 추가한 다음 엔드포인트의 가중치를 조정하여 엘라스틱 IP 주소 엔드포인트에서 EC2 인스턴스 엔드포인트로 트래픽을 느리게 이동합니다.

단계별 전환 지침은 클라이언트 IP 주소 보존을 사용하기 위해 끝점 전환 (p. 33).

클라이언트 IP 주소

클라이언트 IP 주소 보존이 활성화되지 않은 끝점의 경우 에지 네트워크의 글로벌 가속기 서비스에서 사용하는 IP 주소가 요청하는 사용자의 IP 주소를 도착하는 패킷의 원본 주소로 바꿉니다. 클라이언트의 IP 주소 및 클라이언트 포트와 같은 원래 클라이언트의 연결 정보는 액셀러레이터 뒤의 시스템으로 트래픽이 이동해도 보존되지 않습니다. 이것은 많은 응용 프로그램, 특히 공용 웹 사이트와 같은 모든 사용자가 사용할 수있는 응용 프로그램에서 잘 작동합니다.

그러나 다른 응용 프로그램의 경우 클라이언트 IP 주소가 보존된 끝점을 사용하여 원래 클라이언트 IP 주소에 액세스할 수 있습니다. 예를 들어 클라이언트 IP 주소가 있는 경우 클라이언트 IP 주소를 기반으로 통계를 수집할 수 있습니다. 다음과 같은 IP 주소 기반 필터를 사용할 수도 있습니다.애플리케이션 로드 밸런서의 보안 그룹를 사용하여 트래픽을 필터링합니다. 해당 Application Load Balancer 끝점 뒤에 있는 웹 계층 서버에서 실행되는 애플리케이션의 사용자 IP 주소에 특정한 논리를 적용할 수 있습니다.`X-Forwarded-For`헤더입니다. 이 헤더는 원래 클라이언트 IP 주소 정보를 포함합니다. Application Load Balancer 서와 연결된 보안 그룹의 보안 그룹 규칙에서 클라이언트 IP 주소 보존을 사용할 수도 있습니다. 자세한 내용은 AWS Global Accelerator 터에서 클라이언트 IP 주소를 보존하는 방법 (p. 56) 섹션을 참조하세요. EC2 인스턴스 엔드포인트의 경우 원래 클라이언트 IP 주소가 보존됩니다.

클라이언트 IP 주소 보존이 없는 끝점의 경우 글로벌 가속기가 에지에서 트래픽을 전달할 때 사용하는 원본 IP 주소를 필터링할 수 있습니다. 글로벌 액셀러레이터 흐름 로그를 검토하여 들어오는 패킷의 원본 IP 주소(클라이언트 IP 주소 보존이 활성화된 경우 클라이언트 IP 주소) 에 대한 정보를 볼 수 있습니다. 자세한 내용은 Global Accelerator 엣지 서버의 위치 및 IP 주소 범위 (p. 7) 및 AWS Global Accelerator (p. 60) 섹션을 참조하세요.

AWS Global Accelerator 터에서 클라이언트 IP 주소를 보존하는 방법

AWS Global Accelerator Amazon EC2 인스턴스 및 애플리케이션 로드 밸런서에 대해 클라이언트의 소스 IP 주소를 다르게 유지합니다.

- EC2 인스턴스 엔드포인트의 경우 클라이언트의 IP 주소는 모든 트래픽에 대해 보존됩니다.

- 클라이언트 IP 주소 보존이 있는 Application Load Balancer 엔드포인트의 경우 글로벌 가속기는 Application Load Balancer 함께 작동하여`X-Forwarded`헤더`X-Forwarded-For`, 웹 티어가 액세스 할 수 있도록 원래 클라이언트의 IP 주소를 포함합니다.

HTTP 요청 및 HTTP 응답은 헤더 필드를 사용하여 HTTP 메시지에 대한 정보를 전송합니다. 헤더 필드는 콜론으로 구분된 이름-값 페어이며 CR(캐리지 리턴) 및 LF(줄 바꿈)로 구분됩니다. HTTP 헤더 필드의 표준 집합은 RFC 2616에 정의되어 있습니다.메시지 헤더. 애플리케이션에서 널리 사용되는 비표준 HTTP 헤더도 제공되고 있습니다. 일부 비표준 HTTP 헤더는`X-Forwarded`접두사.

Application Load Balancer 들어오는 TCP 연결을 종료하고 백엔드 대상에 대한 새 연결을 생성하기 때문에 클라이언트 IP 주소를 대상 코드 (예: 인스턴스, 컨테이너 또는 Lambda 코드) 까지 유지하지는 않습니다. 대상이 TCP 패킷에 표시되는 소스 IP 주소는 Application Load Balancer 서의 IP 주소입니다. 그러나 Application Load Balancer 원래 패킷의 응답 주소에서 클라이언트 IP 주소를 제거하고 새 TCP 연결을 통해 백엔드로 요청을 보내기 전에 HTTP 헤더에 삽입하여 원래 클라이언트 IP 주소를 보존합니다.

이`X-Forwarded-For`요청 헤더의 형식은 다음과 같습니다.

```
X-Forwarded-For: client-ip-address
```

다음 예제에서는`X-Forwarded-For`IP 주소가 203.0.113.7인 클라이언트의 요청 헤더를 사용합니다.

```
X-Forwarded-For: 203.0.113.7
```

클라이언트 IP 주소 보존에 대한 모범 사례

AWS Global Accelerator 클라이언트 IP 주소 보존을 사용하는 경우 엘라스틱 네트워크 인터페이스 및 보안 그룹에 대한 이 섹션의 정보와 모범 사례에 유의하십시오.

클라이언트 IP 주소 보존을 지원하기 위해 글로벌 액셀러레이터는 AWS 계정에 엔드포인트가 있는 각 서브넷에 대해 하나씩 엘라스틱 네트워크 인터페이스를 만듭니다. 탄력적 네트워크 인터페이스는 VPC에서 가상 네트워크 카드를 나타내는 논리적 네트워킹 구성 요소입니다. 글로벌 액셀러레이터는 이러한 엘라스틱 네트워크 인터페이스를 사용하여 액셀러레이터 뒤에 구성된 엔드포인트로 트래픽을 라우팅합니다. 이러한 방식으로 트래픽을 라우팅하기 위해 지원되는 엔드포인트는 애플리케이션 로드 밸런서 (내부 및 인터넷 연결) 및 Amazon EC2 인스턴스입니다.

> **Note**
>
> 글로벌 액셀러레이터에서 내부 Application Load Balancer 또는 EC2 인스턴스 엔드포인트를 추가하면 프라이빗 서브넷에서 VPC (가상 프라이빗 클라우드) 의 엔드포인트로 인터넷 트래픽이 직접 전송되도록 할 수 있습니다. 자세한 내용은 AWS Global Accelerator 터의 보안 VPC 연결 (p. 101) 섹션을 참조하세요.

글로벌 액셀러레이터에서 엘라스틱 네트워크 인터페이스

클라이언트 IP 주소 보존이 활성화된 Application Load Balancer 있는 경우 로드 밸런서가 속한 서브넷 수에 따라 글로벌 가속기가 계정에 생성하는 엘라스틱 네트워크 인터페이스 수가 결정됩니다. 글로벌 액셀러레이터는 각 서브넷에 대해 하나의 탄력적 네트워크 인터페이스를 만듭니다. 여기에는 Application Load Balancer 엘라스틱 네트워크 인터페이스가 하나 이상 있고 계정의 가속기가 앞에 있습니다.

다음 예에서는 이 계정의 작동 방식을 설명합니다.

- 예 1: Application Load Balancer 서브넷 A와 서브넷 B에 엘라스틱 네트워크 인터페이스가 있는 경우 로드 밸런서를 가속기 끝점으로 추가하면 글로벌 가속기는 각 서브넷에 하나씩 두 개의 엘라스틱 네트워크 인터페이스를 만듭니다.
- 예 2: 예를 들어, 서브넷A에서 탄력적 네트워크 인터페이스가 있는 ALB1을 가속기1에 추가한 다음 서브넷 A에 엘라스틱 네트워크 인터페이스가 있고 서브넷 B가 Accelerator2에 있는 ALB2를 추가하는

경우 글로벌 가속기는 두 개의 탄력적 네트워크 인터페이스만 만듭니다. 하나는 서브넷A와 서브넷 B에 하나씩 두 개의 탄력적 네트워크 인터페이스만 만듭니다.

- 예 3 서브넷A와 서브넷B에 탄력적 네트워크 인터페이스가 있는 ALB1을 가속기1에 추가한 다음 서브넷A에서 탄력적 네트워크 인터페이스가 있는 ALB2를 가속기2에 추가하는 경우 글로벌 가속기는 세 개의 탄력적 네트워크 인터페이스를 만듭니다. 하나는 서브넷A에, 하나는 서브넷B에 있고 다른 하나는 서브넷에 있고 다른 하나는 서브넷에 있습니다. 서브넷A의 elastic network interface 가속기1 및 가속기2 모두에 대한 트래픽을 전달합니다.

예제 3에서 볼 수 있듯이 동일한 서브넷의 끝점이 여러 가속기 뒤에 배치된 경우 탄력적 네트워크 인터페이스가 가속기 간에 재사용됩니다.

Global Accelerator 에서 생성하는 논리적 엘라스틱 네트워크 인터페이스는 단일 호스트, 처리량 병목 현상 또는 단일 장애 지점을 나타내지 않습니다. 가용 영역이나 서브넷에서 단일 elastic network interface 나타나는 다른 AWS 서비스와 마찬가지로, NAT (네트워크 주소 변환) 게이트웨이 또는 네트워크 로드 밸런서와 같은 서비스도 글로벌 액셀러레이터는 수평적으로 확장되고 가용성이 뛰어난 서비스로 구현됩니다.

가속기의 끝점에서 사용하는 서브넷 수를 평가하여 글로벌 액셀러레이터가 만들 엘라스틱 네트워크 인터페이스의 수를 결정합니다. 가속기를 만들기 전에 필요한 탄력적 네트워크 인터페이스에 충분한 IP 주소 공간 용량 (관련 서브넷당 하나 이상의 사용 가능한 IP 주소) 이 있는지 확인합니다. 사용 가능한 IP 주소 공간이 충분하지 않은 경우 Application Load Balancer 및 연결된 글로벌 액셀러레이터 엘라스틱 네트워크 인터페이스에 적합한 사용 가능한 IP 주소 공간이 있는 서브넷을 만들거나 사용해야 합니다.

글로벌 액셀러레이터가 계정의 액셀러레이터에 있는 엔드포인트에서 엘라elastic network interface 사용하고 있지 않다고 판단하면 글로벌 액셀러레이터가 인터페이스를 삭제합니다.

글로벌 액셀러레이터에서 만든 보안 그룹

글로벌 액셀러레이터 및 보안 그룹으로 작업할 때 다음 정보와 모범 사례를 검토하십시오.

- 글로벌 액셀러레이터는 엘라스틱 네트워크 인터페이스와 연결된 보안 그룹을 만듭니다. 시스템이 이러한 작업을 방해하지는 않지만 이러한 그룹에 대한 보안 그룹 설정을 편집하면 안 됩니다.
- 글로벌 액셀러레이터는 만든 보안 그룹을 삭제하지 않습니다. 그러나 글로벌 액셀러레이터는 계정의 액셀러레이터에 있는 엔드포인트에서 사용하지 않는 경우 엘라elastic network interface 삭제합니다.
- 글로벌 액셀러레이터에서 생성한 보안 그룹을 유지 관리하는 다른 보안 그룹의 소스 그룹으로 사용할 수 있지만 글로벌 액셀러레이터는 VPC PC에서 지정한 대상으로만 트래픽을 전달합니다.
- 글로벌 액셀러레이터에서 만든 보안 그룹 규칙을 수정하면 엔드포인트가 비정상 상태가 될 수 있습니다. 이런 일이 발생하면AWS Support에서 지원을 받으십시오.
- 글로벌 액셀러레이터는 각 VPC 대해 특정 보안 그룹을 생성합니다. 특정 VPC 내의 엔드포인트에 대해 생성된 엘라스틱 네트워크 인터페이스는 elastic network interface 연결된 서브넷에 관계없이 모두 동일한 보안 그룹을 사용합니다.

클라이언트 IP 주소 보존을 위해 지원되는 AWS 리전

다음 AWS 리전에서 AWS Global Accelerator 터에 대한 클라이언트 IP 주소 보존을 활성화할 수 있습니다.

리전 이름	Region
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`
US West (N. California)	`us-west-1 (except AZ usw1-az2)`

리전 이름	Region
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1 (except AZ apne1-az3)
Asia Pacific (Seoul)	ap-northeast-2
Canada (Central)	ca-central-1 (except AZ cac1-az3)
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1

AWS Global Accelerator 로깅 및 모니터링

흐름 로그와 AWS CloudTrail을 사용하여 AWS 글로벌 액셀러레이터에서 가속기를 모니터링하고 트래픽 패턴을 분석하며 리스너 및 엔드포인트의 문제를 해결할 수 있습니다.

주제

AWS Global Accelerator

흐름 로그를 사용하면 AWS Global Accelerator 액셀러레이터의 액셀러레이터의 네트워크 인터페이스에서 전송되고 수신되는 IP 주소 트래픽에 대한 정보를 수집할 수 있습니다. 흐름 로그 데이터는 Amazon S3 게시되며, 여기서 플로우 로그를 생성한 다음 데이터를 가져와 확인할 수 있습니다.

흐름 로그는 여러 작업에 도움이 될 수 있습니다. 예를 들어 특정 트래픽이 엔드포인트에 도달하지 않는 문제를 해결할 수 있습니다. 이렇게 하면 과도하게 제한적인 보안 그룹 규칙을 진단할 수 있게 도와줍니다. 흐름 로그를 엔드포인트에 액세스하는 트래픽을 모니터링하기 위한 보안 도구로 사용할 수도 있습니다.

흐름 로그 레코드는 흐름 로그에 네트워크 흐름을 나타냅니다. 각 레코드는 특정 캡처 기간 중 특정 5 튜플의 네트워크 흐름을 캡처합니다. 5 튜플은 IP 흐름의 소스, 대상 및 프로토콜을 지정하는 5가지 값의 집합입니다. 캡처 기간은 흐름 로그 서비스에서 로그 레코드를 게시하기 전에 데이터를 집계하는 시간 기간입니다. 캡처 기간은 약 10초이지만 최대 1분까지 걸릴 수 있습니다.

흐름 로그를 사용할 때 CloudWatch Logs의 요금은 로그가 Amazon S3 직접 게시되더라도 적용됩니다. 자세한 내용은 단원을 참조하십시오.S3로 로그 전송atAmazon CloudWatch 요금.

주제

Amazon S3에 플로우 로그 게시

AWS Global Accelerator 에 대한 플로우 로그는 지정된 기존 S3 버킷에 Amazon S3 S3에 게시됩니다. 흐름 로그 레코드는 버킷에 저장된 일련의 로그 파일 객체에 게시됩니다.

플로우 로그와 함께 사용할 Amazon S3 버킷을 생성하려면버킷 만들기의Amazon Simple Storage Service 시작 안내서.

흐름 로그 파일

플로우 로그는 플로우 로그 레코드를 수집하여 로그 파일로 통합한 다음 해당 로그 파일을 5분 간격으로 Amazon S3 버킷에 게시합니다. 각 로그 파일에는 이전 5분 동안 기록된 IP 주소 트래픽에 대한 플로우 로그 레코드가 포함됩니다.

로그 파일의 최대 크기는 75MB입니다. 로그 파일이 5분 내에 파일 크기 한도에 도달하는 경우, 플로우 로그는 플로우 로그 레코드의 로그 파일로의 추가를 중단하고 Amazon S3 버킷에 게시한 다음 새로운 로그 파일을 생성합니다.

로그 파일은 플로우 로그의 ID, 리전 및 생성된 날짜에 따라 결정된 폴더 구조를 사용하여 지정된 Amazon S3 버킷에 저장됩니다. 버킷 폴더 구조는 다음 형식을 사용합니다.

```
s3-bucket_name/s3-bucket-prefix/AWSLogs/aws_account_id/globalaccelerator/region/yyyy/mm/dd/
```

마찬가지로 로그 파일 이름은 플로우 로그의 ID, 리전 및 생성된 날짜 및 시간에 따라 결정됩니다. 파일 이름은 다음의 형식을 사용합니다.

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

로그 파일의 폴더 및 파일 이름 구조에 대한 다음 사항에 유의하십시오.

- 타임스탬프는 `YYYYMMDDTHHmmZ` 형식을 사용합니다.
- S3 버킷 접두사에 슬래시 (/) 를 지정하면 로그 파일 버킷 폴더 구조에 다음과 같이 이중 슬래시 (//) 가 포함됩니다.

  ```
  s3-bucket_name//AWSLogs/aws_account_id
  ```

다음 예에서는 AWS 계정에서 생성한 플로우 로그에 대한 로그 파일의 폴더 구조 및 파일 이름을 보여줍니다.`123456789012`ID가 인 가속기의 경우`1234abcd-abcd-1234-abcd-1234abcdefgh`, 2018년 11월 23일, UTC:

```
my-s3-bucket/prefix1/AWSLogs/123456789012/globalaccelerator/us-
west-2/2018/11/23/123456789012_globalaccelerator_1234abcd-abcd-1234-
abcd-1234abcdefgh_20181123T0005Z_1fb1234.log.gz
```

단일 흐름 로그 파일에는 여러 5개의 튜플 레코드가 있는 인터리브된 항목이 들어 있습니다. 즉,`client_ip`,`client_port`,`accelerator_ip`,`accelerator_port`,`protocol`. 가속기에 대한 모든 흐름 로그 파일을 보려면`accelerator_id`및 귀하의`account_id`.

Amazon S3 플로우 로그를 게시하기 위한 IAM 역할

IAM 사용자와 같은 IAM 보안 주체에는 Amazon S3 버킷에 플로우 로그를 게시할 충분한 권한이 있어야 합니다. IAM 정책에 다음 권한이 포함되어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeliverLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGlobalAcceleratorService",
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "s3Perms",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon S3 버킷의 플로우 로그에 대한 권한

기본적으로 Amazon S3 버킷과 버킷에 포함된 객체는 비공개입니다. 버킷 소유자만이 해당 버킷과 그 안에 저장된 객체에 액세스할 수 있습니다. 그러나 버킷 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

흐름 로그를 생성하는 사용자가 버킷을 소유한 경우, 서비스는 다음 정책을 버킷에 자동으로 연결하여 로그를 버킷에 게시할 플로우 로그 권한을 부여합니다.

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

플로우 로그를 생성하는 사용자가 버킷을 소유하지 않거나 해당 버킷에 대한 `GetBucketPolicy`와 `PutBucketPolicy`가 없는 경우, 플로우 로그 생성이 실패합니다. 이 경우 버킷 소유자는 이전 정책을 버킷에 수동으로 추가하고 플로우 로그 생성자의 AWS 계정 ID를 지정해야 합니다. 자세한 내용은 단원을 참조하십시오.S3 버킷 정책을 추가하려면 어떻게 해야 합니까?의Amazon Simple Storage Service 시작 안내서. 버킷이 여러 계정으로부터 플로우 로그를 수신하는 경우, `Resource` 요소 입력 내용을 각 계정의 `AWSLogDeliveryWrite` 정책 설명에 추가합니다.

예를 들어 다음 버킷 정책에 따라 AWS 계정 12312312123123 및 456456456456456456456456456456666456666456은 플로우 로그를`flow-logs`이라는 버킷에`log-bucket`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
```

```
            ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

Note

부여 하는 것이 좋습니다.`AWSLogDeliveryAclCheck`및`AWSLogDeliveryWrite`권한을 개별 AWS 계정 ARN 대신 로그 전송 서비스 보안 주체에게 할당합니다.

SSE-KMS 버킷에 사용할 경우 필요한 CMK 키 정책

고객 관리형 고객 마스터 키 (CMK) 와 함께 AWS KMS 관리형 키 (SSE-KMS) 를 사용하여 Amazon S3 버킷에 대하여 서버 측 암호화를 활성화한 경우, 플로우 로그가 로그 파일을 버킷에 쓸 수 있도록 CMK의 키 정책에 다음을 추가해야 합니다.

```
{
    "Sid": "Allow AWS Global Accelerator Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Amazon S3 로그 파일 권한

필요한 버킷 정책 외에도, Amazon S3는 ACL(액세스 제어 목록)을 사용하여 플로우 로그에서 생성한 로그 파일에 대한 액세스를 관리합니다. 기본적으로 버킷 소유자는 각 로그 파일에 대한 `FULL_CONTROL` 권한을 보유합니다. 로그 전송 소유자가 버킷 소유자와 다른 경우에는 권한이 없습니다. 로그 전송 계정에는 `READ` 및 `WRITE` 권한이 부여됩니다. 자세한 내용은 단원을 참조하십시오.ACL(액세스 통제 목록) 개요의Amazon Simple Storage Service 시작 안내서.

Amazon S3 플로우 로그 게시

AWS Global Accelerator 흐름 로그를 활성화하려면 이 절차의 단계를 따릅니다.

AWS Global Accelerator 흐름 로그를 활성화하려면

1. AWS 계정에 플로우 로그용 Amazon S3 버킷을 생성합니다.
2. 흐름 로그를 활성화하는 AWS 사용자에 대해 필요한 IAM 정책을 추가합니다. 자세한 내용은 Amazon S3 플로우 로그를 게시하기 위한 IAM 역할 (p. 61) 섹션을 참조하세요.
3. 로그 파일에 사용할 Amazon S3 버킷 이름과 접두사를 사용하여 다음 AWS CLI 명령을 실행합니다.

```
aws globalaccelerator update-accelerator-attributes
       --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
       --region us-west-2
```

```
    --flow-logs-enabled
    --flow-logs-s3-bucket s3-bucket-name
    --flow-logs-s3-prefix s3-bucket-prefix
```

Amazon S3에서 플로우 로그 레코드 처리

로그 파일은 압축된 상태입니다. Amazon S3 콘솔을 사용해 로그 파일을 열면 압축이 해제되고 플로우 로그 레코드가 표시됩니다. 파일을 다운로드하는 경우, 압축을 해제해야 플로우 로그 레코드를 볼 수 있습니다.

로그 파일 전송 타이밍

AWS Global Accelerator 는 구성된 액셀러레이터에 대한 로그 파일을 1시간 동안 여러 번 전송합니다. 일반적으로 로그 파일에는 지정된 기간 중에 액셀러레이터가 수신한 요청에 대한 정보가 들어 있습니다. 일반적으로 Global Accelerator 는 로그에 표시된 이벤트가 발생한 후 한 시간 이내에 로그 파일을 Amazon S3 버킷으로 전송합니다. 특정 기간 동안의 일부 또는 전체 로그 파일 항목이 때때로 최대 24시간까지 지연되기도 합니다. 로그 항목이 지연되는 경우 Global Accelerator 는 파일 이름에 파일이 전송된 날짜 및 시간이 아니라 요청이 발생한 기간의 날짜 및 시간이 로그 파일에 이러한 로그 항목을 저장합니다.

로그 파일을 생성할 때 Global Accelerator 는 로그 파일에 포함되는 기간 중에 요청을 받은 모든 엣지 로케이션의 액셀러레이터 관련 정보를 통합합니다.

로깅을 활성화하고 약 4시간이 지나면 로그 파일이 안정적으로 전송되기 시작합니다. 그 전에는 일부 로그 파일이 가져올 수 있습니다.

> Note
>
> 해당 기간 중에 액셀러레이터에 연결하는 사용자가 없으면 해당 기간 동안 로그 파일이 수신되지 않습니다.

흐름 로그 레코드 구문

흐름 로그 레코드는 공백으로 구분된 문자열로, 다음과 같은 형식입니다.

```
<version> <aws_account_id> <accelerator_id> <client_ip> <client_port>
<accelerator_ip> <accelerator_port> <endpoint_ip> <endpoint_port> <protocol>
<ip_address_type> <packets> <bytes> <start_time> <end_time> <action> <log-
status> <globalaccelerator_source_ip> <globalaccelerator_source_port>
<endpoint_region> <globalaccelerator_region> <direction> <vpc_id>
```

버전 1.0 형식에는 VPC 식별자,vpc_id. 버전 2.0 형식.vpc_id는 글로벌 액셀러레이터가 클라이언트 IP 주소를 보존하여 엔드포인트로 트래픽을 전송할 때 생성됩니다.

다음 표에서는 플로우 로그 레코드의 필드를 설명합니다.

필드	설명
version	흐름 로그 버전입니다.
aws_account_id	흐름 로그의 AWS 계정 ID.
accelerator_id	트래픽이 기록되는 액셀러레이터의 ID.
client_ip	소스 IPv4 주소입니다.
client_port	소스 포트.
accelerator_ip	가속기의 IP 주소입니다.

필드	설명
accelerator_port	가속기의 포트.
endpoint_ip	트래픽의 대상 IP 주소입니다.
endpoint_port	트래픽의 대상 포트
protocol	트래픽의 IANA 프로토콜 번호. 자세한 정보는 지정된 인터넷 프로토콜 번호 단원을 참조하십시오.
ip_address_type	IPv4입니다.
packets	캡처 기간 중 전송된 패킷 수.
bytes	캡처 기간 중 전송된 바이트 수.
start_time	캡처 기간의 시작 시간(단위: Unix 초)
end_time	캡처 기간의 종료 시간(단위: Unix 초)
action	트래픽과 연결된 작업 • ACCEPT: 보안 그룹 또는 네트워크 ACL에서 허용한 트래픽입니다. 값은 현재 항상 수락입니다.
log-status	흐름 로그의 로깅 상태: • OK: 데이터가 선택된 대상에 정상적으로 로깅됩니다. • NODATA: 캡처 기간 중 네트워크 인터페이스에서 전송하거나 수신된 네트워크 트래픽이 없었습니다. • SKIPDATA: 캡처 기간 중 일부 흐름 로그 레코드를 건너뛰었습니다. 내부 용량 제한 또는 내부 오류가 원인일 수 있습니다.
globalaccelerator_source_ip	글로벌 가속기 네트워크 인터페이스에서 사용하는 IP 주소입니다.
globalaccelerator_source_port	글로벌 액셀러레이터 네트워크 인터페이스에서 사용하는 포트입니다.
endpoint_region	엔드포인트가 위치한 AWS 리전입니다.
globalaccelerator_region	요청을 처리한 엣지 로케이션 (현재 위치) 입니다. 각 엣지 로케이션에는 3자 코드와 임의 배정된 번호가 있습니다 (예: DFW3). 3자 코드는 일반적으로 엣지 로케이션 부근의 공항을 나타내는 국제 항공 수송 협회 공항 코드에 상응합니다. 이러한 약어는 향후에 변경될 수 있습니다.
direction	트래픽의 방향입니다. 글로벌 액셀러레이터 네트워크로 들어오는 트래픽을 나타냅니다 (INGRESS) 또는 클라이언트로 돌아 가기 (EGRESS).
vpc_id	VPC 식별자. 글로벌 액셀러레이터가 클라이언트 IP 주소를 보존하여 엔드포인트로 트래픽을 전송할 때 버전 2.0 흐름 로그에 포함됩니다.

필드가 특정 레코드에 적용되지 않을 경우 레코드에 '-' 기호가 표시됩니다.

AWS Global Accelerator Amazon CloudWatch 사용

AWS Global Accelerator 는 가속기를 위해 Amazon CloudWatch 에 데이터 포인트를 게시합니다. CloudWatch 를 사용하면 이러한 데이터 요소에 대한 통계를 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 통계를지표. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅

니다. 예를 들어 지정된 기간 동안 가속기를 통해 트래픽을 모니터링할 수 있습니다. 각 데이터 요소에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

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

Global Accelerator 는 요청이 가속기를 통과하는 경우에만 CloudWatch 에 지표를 보고합니다. 요청이 가속기를 통과하고 있는 경우 Global Accelerator 는 60초마다 지표를 측정하여 전송합니다. Accelerator 를 통과하는 요청이 없는 경우나 지표에 대한 데이터가 없는 경우에는 지표가 보고되지 않습니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

목차

전역 Accelerator 지표

`AWS/GlobalAccelerator` 네임스페이스에는 다음 지표가 포함되어 있습니다.

지표	설명
`NewFlowCount`	해당 기간 동안 클라이언트에서 엔드포인트로 설정되는 새로운 TCP 및 UDP 흐름 (또는 연결) 의 총 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 유일하게 유용한 통계는`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	TCP/IP 헤더를 포함하여 가속기가 처리하는 총 수신 바이트 수. 이 수에는 엔드포인트에 대한 모든 트래픽이 포함됩니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 유일하게 유용한 통계는`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion`

지표	설명
	• Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesOut	TCP/IP 헤더를 포함하여 가속기가 처리하는 나가는 총 바이트 수. 이 수는 엔드포인트의 트래픽, 마이너스 상태 확인 트래픽을 포함합니다. 보고 기준: 0이 아닌 값이 있을 때. 통계: 유일하게 유용한 통계는Sum. Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

Accelerator에 대한 지표 차원

Accelerator 에 대한 지표를 필터링하려면 다음 차원을 사용하십시오.

차원	설명
Accelerator	Accelerator 를 기준으로 지표 데이터를 필터링합니다. 가속기 id (가속기 ARN 의 마지막 부분) 로 가속기를 지정합니다. 예를 들어 ARN 이arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh에서 다음을 지정할 수 있습니다.**1234abcd-abcd-1234-abcd-1234abcdefgh**.
Listener	리스너를 기준으로 지표 데이터를 필터링합니다. 리스너 ID (리스너 ARN 의 마지막 부분) 로 리스너를 지정합니다. 예를 들어 ARN 이arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz에서 다음을 지정할 수 있습니다.**0123wxyz**.
EndpointGroup	엔드포인트 그룹을 기준으로 지표 데이터를 필터링합니다. AWS 리전별로 엔드포인트 그룹을 지정합니다 (예:**us-east-1**(모두 소문자).
SourceRegion	애플리케이션 엔드포인트가 실행 중인 AWS 리전의 지리적 영역인 소스 리전별로 메트릭 데이터를 필터링합니다. 출처 영역은 다음 중 하나입니다. • NA — 미국 및 캐나다 • EU — 유럽 • AP — 아시아 태평양* • KR — 대한민국 • INA — 인도 • AU — 오스트레일리아

차원	설명
	• ME — 중동 • SA — 남아메리카 *한국 및 인도 제외
`DestinationEdge`	클라이언트 트래픽을 처리하는 AWS 엣지 로케이션의 지리적 영역인 대상 에지별로 메트릭 데이터를 필터링합니다. 대상 가장자리는 다음 중 하나입니다. • NA — 미국 및 캐나다 • EU — 유럽 • AP — 아시아 태평양* • KR — 대한민국 • INA — 인도 • AU — 오스트레일리아 • ME — 중동 • SA — 남아메리카 • ZA — 남아프리카 *한국 및 인도 제외
`TransportProtocol`	전송 프로토콜을 기준으로 지표 데이터를 필터링합니다. UDP 또는 TCP
`AcceleratorIPAddress`	가속기의 IP 주소, 즉 가속기에 할당된 정적 IP 주소 중 하나를 기준으로 지표 데이터를 필터링합니다.

전역 Accelerator 지표에 대한 통계

CloudWatch 는 Global Accelerator 가 게시한 지표 데이터 요소에 따라 통계를 제공합니다. 통계는 지정된 기간 동안 지표 데이터를 집계한 것입니다. 통계를 요청하면 지표 이름 및 차원으로 반환된 데이터 스트림이 식별됩니다. 차원이란 지표를 고유하게 식별하는 데 도움이 되는 이름/값 쌍을 말합니다. 예를 들어 유럽의 AWS 엣지 로케이션에서 바이트가 제공되는 가속기에 대해 처리된 바이트를 요청할 수 있습니다 (대상 에지는 “EU”).

다음은 유용할 수 있는 메트릭/차원 조합의 예입니다.

- 두 가속기 IP 주소 각각에 의해 제공된 트래픽 양 (예: ProcessedBytesout) 을 확인하여 DNS 구성이 올바른지 확인합니다.
- 사용자 트래픽의 지리적 분포를 보고 로컬 (예: 북미에서 북미) 또는 글로벌 (예: 호주 또는 인도에서 북미) 의 양을 모니터링합니다. 이를 확인하려면 특정 값으로 설정된 대상 가장자리 및 SourceRegion 차원을 사용하여 처리되는 바이트 입력 또는 처리바이트 출력 측정 단위를 봅니다.

Accelerator에 대한 CloudWatch 지표를 확인합니다.

CloudWatch 콘솔 또는 AWS CLI를 사용하여 가속기에 대한 CloudWatch 지표를 확인할 수 있습니다. 콘솔에서 지표가 모니터링 그래프로 표시됩니다. 모니터링 그래프는 가속기가 활성 상태로 요청을 수신하는 경우에만 데이터 요소를 보여 줍니다.

콘솔에서 또는 AWS CLI를 사용할 때 미국 서부 (오레곤) 리전의 글로벌 Accelerator 에 대한 CloudWatch 지표를 확인해야 합니다. AWS CLI를 사용하는 경우 다음 매개 변수를 포함하여 명령에 대한 미국 서부 (오레곤) 리전을 지정합니다.`--region us-west-2`.

CloudWatch 콘솔을 사용하여 지표를 보려면

1. 다음 위치에서 CloudWatch 콘솔을 엽니다.https://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2.
2. 탐색 창에서 지표를 선택합니다.
3. SelectGlobalAcceleratorNamespace.
4. (선택 사항) 모든 차원의 지표를 보려면 검색 필드에 이름을 입력합니다.

AWS CLI를 사용하여 측정치를 보려면

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

```
aws cloudwatch list-metrics --namespace AWS/GlobalAccelerator --region us-west-2
```

AWS CLI를 사용하여 지표에 대한 통계를 구하려면

다음을 사용하십시오.통계를 구하려면명령을 사용하여 지정된 지표 및 차원에 대한 통계를 가져올 수 있습니다. CloudWatch는 각각의 고유한 차원의 조합을 별도의 지표로 처리합니다. 게시가 되지 않은 차원의 조합을 사용해 통계를 검색할 수는 없습니다. 지표 생성 시 사용한 것과 동일하게 차원을 지정해야 합니다.

다음 예에서는 북미 (NA) 대상 에지에서 제공하는 가속기에 대해 처리된 총 바이트 수 (분당) 를 나열합니다.

```
aws cloudwatch get-metric-statistics --namespace AWS/GlobalAccelerator \
--metric-name ProcessedBytesIn \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=Accelerator,Value=1234abcd-abcd-1234-abcd-1234abcdefgh
 Name=DestinationEdge,Value=NA \
--start-time 2019-12-18T20:00:00Z --end-time 2019-12-18T21:00:00Z
```

다음은 명령의 출력 예제입니다.

```
{
    "Label": "ProcessedBytesIn",
    "Datapoints": [
        {
            "Timestamp": "2019-12-18T20:45:00Z",
            "Sum": 2410870.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:47:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:46:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:42:00Z",
            "Sum": 1560.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:48:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
```

```
        },
        {
            "Timestamp": "2019-12-18T20:43:00Z",
            "Sum": 1343.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:49:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:44:00Z",
            "Sum": 35791560.0,
            "Unit": "Bytes"
        }
    ]
}
```

AWS CloudTrail 을 사용하여 AWS Global Accelerator API 호출 기록

AWS Global Accelerator 는 Global Accelerator 에서 사용자, 역할, AWS 서비스가 수행한 작업의 레코드를 제공하는 서비스인 AWS AWS CloudTrail 과 통합됩니다. CloudTrail 은 글로벌 Accelerator 콘솔의 호출 및 글로벌 Accelerator API에 대한 코드 호출을 포함하여 글로벌 Accelerator 액셀러레이션에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면, 글로벌 Accelerator 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 전달할 수 있습니다. 추적을 구성하지 않은 경우 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail User Guide을 참조하십시오.

CloudTrail 의 글로벌 Accelerator 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Global Accelerator 에서 활동이 발생하면, 해당 활동이이벤트 기록. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하십시오.

AWS 계정의 이벤트 기록 (Global Accelerator 이벤트 포함) 을 보려면 추적을 생성하십시오. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있도록 합니다. 콘솔에서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로그하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 주제를 참조하십시오.

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

모든 글로벌 Accelerator 작업은 CloudTrail 에서 로깅되며AWS Global Accelerator API 참조. 예를 들어,`CreateAccelerator`,`ListAccelerators`및`UpdateAccelerator`작업은 CloudTrail 로그 파일에 항목을 생성합니다.

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

- 요청을 루트로 했는지 아니면 IAM 사용자 자격 증명으로 했는지 여부
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 요청이 다른 AWS 서비스에 의해 이루어졌는지

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

전역 Accelerator 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. 각 JSON 형식의 CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 로그 항목은 어떤 소스로부터의 단일 요청을 나타내며 모든 매개 변수, 작업 날짜와 시간 등 요청한 작업에 대한 정보가 포함됩니다. 로그 항목은 특정 순서를 유지하지 않으며, API 호출의 정렬된 스택 추적 정보가 아닙니다.

다음 예에 이러한 글로벌 Accelerator 작업이 포함된 CloudTrail 로그 항목이 나와 있습니다.

- 계정에 대한 가속기 나열:`eventName`확장하는 데`ListAccelerators`.
- 리스너 생성`eventName`확장하는 데`CreateListener`.
- 리스너 업데이트:`eventName`확장하는 데`UpdateListener`.
- 리스너 설명`eventName`확장하는 데`DescribeListener`.
- 계정의 리스너 나열:`eventName`확장하는 데`ListListeners`.
- 리스너 삭제`eventName`확장하는 데`DeleteListener`.


```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:14Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListAccelerators",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "083cae81-28ab-4a66-862f-096e1example",
      "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
```

```
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:04:49Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample/
listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
"arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
```

```
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample/
listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
            "fromPort": 81,
            "toPort": 81
          }
        ]
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample/
listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            },
            {
              "fromPort": 81,
              "toPort": 81
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "008ef93c-b3a3-44b4-afb3-768example",
      "eventID": "85958f0d-63ff-4a2c-99e3-6ffbexample",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
```

```
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:05Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DescribeListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample/
listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListListeners",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample"
      },
      "responseElements": null,
      "requestID": "08e4b0f7-689b-4c84-af2d-47619example",
      "eventID": "f4fb8e41-ed21-404d-af9d-037c4example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:24Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DeleteListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-a114-5d7fexample/
listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

AWS Global Accelerator

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 – AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호해야 합니다. 또한 AWS는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 AWS 규정 준수 프로그램의 일환으로 정기적으로 보안 효과를 테스트하고 검증합니다. 글로벌 액셀러레이터에 적용되는 규정 준수 프로그램에 대해 알아보려면규정 준수 프로그램 제공 AWS 범위 내 서비스.
- 클라우드 내 보안 – 사용자의 책임은 사용하는 AWS 서비스에 의해 결정됩니다. 또한 데이터의 민감도, 조직의 요구 사항 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 글로벌 액셀러레이터를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 목표를 충족하도록 글로벌 액셀러레이터를 구성하는 방법을 보여줍니다.

주제

AWS Global Accelerator 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM) 는 AWS 글로벌 액셀러레이터 리소스를 비롯한 AWS 리소스에 대한 관리자의 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. 관리자는 IAM을 사용하여 사용자 제어인증(로그인) 및Auth(권한 있음) 을 사용하여 글로벌 가속기 리소스를 사용할 수 있습니다. IAM은 추가 비용 없이 AWS 계정에 제공되는 기능입니다.

> **Important**
>
> IAM에 대해 잘 모르는 경우 이 페이지에 나와 있는 기본 정보를 검토한 다음IAM 시작하기 (p. 94). 인증 및 액세스 제어에 대한 자세한 내용은 를 참조하십시오.인증이란 무엇입니까? (p. 88),액세스 제어란 무엇입니까? (p. 89), 및정책이란 무엇입니까? (p. 91).

주제

개념 및 용어

인증— AWS 에 로그인하려면 루트 사용자 자격 증명 (권장 안 됨), IAM 사용자 자격 증명 또는 IAM 역할을 사용하는 임시 자격 증명 중 하나를 사용해야 합니다. 이러한 엔터티에 대한 자세한 내용은 인증이란 무엇입니까? (p. 88) 단원을 참조하십시오.

액세스 제어— AWS 관리자는 정책을 사용해 글로벌 액셀러레이터의 액셀러레이터와 같은 AWS 리소스에 대한 액세스를 제어합니다. 자세한 내용은 액세스 제어란 무엇입니까? (p. 89) 및 정책이란 무엇입니까? (p. 91) 단원을 참조하십시오.

> Important
>
> 리소스를 누가 생성했든 상관 없이 계정 내 모든 리소스를 해당 계정이 소유합니다. 리소스를 생성할 수 있는 권한을 부여 받아야 합니다. 그러나 리소스를 생성했다는 이유만으로 해당 리소스에 대한 모든 액세스 권한이 자동으로 부여되지는 않습니다. 수행하려는 각 작업에 대한 권한을 관리자가 명시적으로 부여해야 합니다. 또한 관리자는 언제든지 권한을 취소할 수 있습니다.

IAM 작동 방식에 대한 기본적인 내용을 알아보려면 다음 용어를 살펴보십시오.

리소스

글로벌 액셀러레이터 및 IAM 같은 AWS 서비스에는 일반적으로 리소스라는 객체가 포함됩니다. 대부분의 경우 이러한 리소스는 이러한 서비스에서 생성, 관리 및 삭제할 수 있습니다. IAM 리소스에는 사용자, 그룹, 역할 및 정책이 포함됩니다.

Users

IAM 사용자는 AWS와 상호 작용하는 자격 증명을 사용해 AWS 를 조작하는 개인 또는 애플리케이션을 나타냅니다. 사용자는 이름, AWS Management Console 에 로그인하기 위한 암호 그리고 AWS CLI 또는 AWS API와 함께 사용할 수 있는 2개의 액세스 키로 이루어져 있습니다.

그룹

IAM 그룹은 IAM 사용자에 대한 컬렉션입니다. 관리자는 그룹을 사용하여 멤버 사용자에 대한 권한을 지정할 수 있습니다. 그러면 관리자가 여러 사용자의 권한을 보다 쉽게 관리할 수 있습니다.

Roles

IAM 역할은 그와 연관된 표준 장기 자격 증명 (암호 또는 액세스 키) 이 없습니다. 역할은 역할이 필요하고 권한이 있는 사용자라면 누구나 맡을 수 있습니다. IAM 사용자는 한 가지 역할을 맡음으로써 특정 작업을 위해 다른 권한을 임시로 얻을 수 있습니다. 연합된 사용자는 역할에 매핑된 외부 자격 증명 공급자를 사용하여 역할을 맡을 수 있습니다. 일부 AWS 서비스는서비스 역할에서 AWS 리소스에 대신 액세스하도록 허용합니다.

정책

정책은 연결된 객체에 대한 권한을 정의하는 JSON 문서입니다. AWS 지원합니다.자격 증명 기반 정책자격 증명 (사용자, 그룹 또는 역할) 에 연결합니다. 일부 AWS 서비스에서는리소스 기반 정책리소스에 연결해 해당 리소스에 대해 작업을 수행할 수 있는 보안 주체 (개인 또는 애플리케이션) 를 제어할 수 있습니다. Global Accelerator는 리소스 기반 정책을 지원하지 않습니다.

ID

자격 증명 자격 증명은 권한을 정의할 수 있는 IAM 리소스입니다. 여기에는 사용자, 그룹 및 역할이 포함됩니다.

엔터티

엔터티 엔터티는 인증에 사용하는 IAM 리소스입니다. 여기에는 사용자 및 역할이 포함됩니다.

Principal

AWS 에서 보안 주체는 AWS에 로그인하여 AWS에 요청을 생성하기 위해 엔터티를 사용하는 개인 또는 애플리케이션입니다. 보안 주체는 AWS Management Console, AWS CLI 또는 AWS API를 사용하여 작업 (예: 액셀러레이터 삭제) 을 수행할 수 있습니다. 그러면 작업에 대한 요청이 생성됩니다. 요청은 작업, 리소스, 보안 주체, 보안 주체 계정 및 요청에 대한 모든 추가 정보를 지정합니다. 이러한 모든 정보는

AWS 에서context요청을 참조하십시오. AWS 요청 콘텍스트에 적용되는 모든 정책을 확인합니다. AWS 는 정책이 요청의 각 부분을 허용한 경우에만 요청을 승인합니다.

인증 및 액세스 제어 프로세스의 다이어그램을 보려면IAM 작동 방식 이해의IAM 사용 설명서. AWS 에서 요청이 허용되는지 여부를 결정하는 방법에 대한 자세한 내용은 를 참조하십시오.정책 평가 로직의IAM 사용 설명서.

콘솔 액세스, 인증 관리 및 액세스 제어에 필요한 권한

글로벌 액셀러레이터를 사용하거나 자신 또는 다른 사람에 대한 권한 부여 및 액세스 제어를 관리하려면 올바른 권한이 있어야 합니다.

글로벌 액셀러레이터 가속기를 만드는 데 필요한 권한

AWS Global Accelerator 가속기를 만들려면 사용자에게 글로벌 액셀러레이터와 연결된 서비스 연결 역할을 생성할 권한이 있어야 합니다.

사용자에게 글로벌 액셀러레이터에서 액셀러레이터를 만들 수 있는 올바른 권한이 있는지 확인하려면 다음과 같은 정책을 사용자에게 연결합니다.

Note

더 제한적인 자격 증명 기반 권한 정책을 만들면 해당 정책이 있는 사용자는 액셀러레이터를 생성할 수 없습니다.

```
{
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "globalaccelerator.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/globalaccelerator.amazonaws.com/
AWSServiceRoleForGlobalAccelerator*"
    }
```

Global Accelerator 콘솔 사용에 필요한 권한

AWS Global Accelerator 콘솔에 액세스하려면 AWS 계정의 글로벌 액셀러레이터 리소스에 대한 세부 정보를 나열하고 볼 수 있는 최소 권한이 있어야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 권한 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티에 대해 의도대로 작동하지 않습니다.

해당 개체가 글로벌 액셀러레이터 콘솔 또는 API 작업을 여전히 사용할 수 있도록 하려면 다음과 같은 AWS 관리형 정책 중 하나도 사용자에게 연결합니다.JSON 탭에서 정책 만들기:

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

첫 번째 정책인`GlobalAcceleratorReadOnlyAccess`, 사용자가 콘솔에서 정보를 보거나 AWS CLI 또는`List*`또는`Describe*`작업을 지원합니다.

두 번째 정책인GlobalAcceleratorFullAccess를 통해 가속기를 생성하거나 업데이트해야 하는 사용자에게 제공할 수 있습니다. 전체 액세스 정책에는 다음이 포함됩니다.풀전역 가속기에 대한 권한뿐만 아니라describe권한과 Elastic Load Balancing 에 대한 권한을 제공합니다.

> **Note**
>
> Amazon EC2 및 Elastic Load Balancing 에 필요한 권한을 포함하지 않는 ID 기반 권한 정책을 생성하는 경우 해당 정책을 사용하는 사용자는 Amazon EC2 및 엘라스틱 로드 밸런싱 리소스를 가속기에 추가할 수 없습니다.

다음은 전체 액세스 정책입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
```

```
        }
    ]
}
```

인증 관리에 필요한 권한

자신의 자격 증명(예: 암호, 액세스 키 및 멀티 팩터 인증(MFA) 디바이스)을 관리하려면 관리자가 필요한 권한을 부여해야 합니다. 이러한 권한이 포함된 정책을 보려면 사용자가 자격 증명을 자체 관리할 수 있게 하려면 (p. 97) 단원을 참조하십시오.

AWS 관리자는 IAM에서 사용자, 그룹, 역할 및 정책을 생성하고 관리할 수 있도록 IAM에 대한 모든 액세스 권한이 필요합니다. 를 사용해야 합니다.AdministratorAccess모든 AWS에 대한 모든 액세스 권한을 포함하는 AWS 관리형 정책입니다. 이 정책은 AWS BBilling and Cost Management 콘솔에 대한 액세스 권한을 제공하지 않거나 AWS 계정 루트 사용자 자격 증명을 필요로 하는 작업은 허용하지 않습니다. 자세한 내용은 단원을 참조하십시오.AWS 계정 루트 사용자 자격 증명이 필요한 AWS 작업의AWS 일반 참조.

> Warning
>
> 관리자 사용자만 AWS 에 대한 모든 액세스 권한을 가져야 합니다. 이 정책을 가진 사용자는 누구나 AWS 의 모든 리소스를 수정할 수 있는 권한 이외에 인증 및 액세스 제어를 완전히 관리할 수 있는 권한을 가지고 있습니다. 이 사용자를 생성하는 방법에 대한 자세한 내용은 IAM 관리 사용자를 생성합니다. (p. 95) 단원을 참조하십시오.

액세스 제어에 필요한 권한

관리자가 IAM 사용자 자격 증명을 제공한 경우 여러분이 액세스할 수 있는 리소스를 제어할 수 있도록 IAM 사용자에게 정책을 연결합니다. AWS Management Console에서 사용자 자격 증명에 연결된 정책을 보려면 다음 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "ListUsersViewGroupsAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

추가 권한이 필요한 경우 관리자에게 필요한 작업에 액세스할 수 있도록 정책을 업데이트해 달라고 요청하십시오.

IAM에서 글로벌 액셀러레이터 작동 방식 이해

서비스는 다음과 같은 여러 가지 방식으로 IAM을 사용할 수 있습니다.

Actions

Global Accelerator 는 정책에서 작업 사용을 지원합니다. 따라서 관리자가 글로벌 액셀러레이터에서 엔터티가 작업을 완료할 수 있는지 제어할 수 있습니다. 예를 들어 엔터티가`GetPolicy`정책을 보려면 AWS API 작업을 수행하려면 관리자가`iam:GetPolicy`action.

다음 예제 정책에서는 사용자가`CreateAccelerator`작업을 사용하여 AWS 계정에 대한 가속기를 프로그래밍 방식으로 생성할 수 있습니다.

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "globalaccelerator:CreateAccelerator"
         ],
         "Resource":"*"
      }
   ]
}
```

리소스 수준 권한

Global Acceleratorは리소스 수준 권한을 지원합니다. 리소스 수준 권한이 있으면 ARN을 사용하여 정책에서 개별 리소스를 지정할 수 있습니다.

리소스 기반 정책

Global Acceleratorは리소스 기반 정책을 지원하지 않습니다. 리소스 기반 정책을 사용하면 서비스 내 리소스에 정책을 연결할 수 있습니다. 리소스 기반 정책에는`Principal`요소를 사용하여 해당 리소스에 액세스할 수 있는 IAM 자격 증명을 지정합니다.

태그 기반 권한 부여

글로벌 액셀러레이터는 권한 기반 태그를 지원합니다. 이 기능을 사용하면 정책 조건에서 리소스 태그를 사용할 수 있습니다.

2013년 5월 22일

글로벌 액셀러레이터는 임시 자격 증명을 지원합니다 임시 자격 증명을 사용하여 페더레이션을 사용해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AWS STS API 작업을 호출하면 임시 보안 자격 증명을 얻을 수 있습니다.`AssumeRole`또는`GetFederationToken`.

서비스 연결 역할

Global Accelerator 는 서비스 연결 역할을 지원합니다. 이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 연결 역할을 맡을 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 역할

Global Accelerator 는 서비스 역할을 지원하지 않습니다. 이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스

해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

인증 및 액세스 제어

다음 정보를 사용하여 IAM으로 작업할 때 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

Global Accelerator에서 작업을 수행할 권한이 없음

AWS Management Console에서 작업을 수행할 권한이 없다는 메시지가 나타나는 경우 사용자 이름 및 암호를 제공한 관리자에게 연락해야 합니다.

다음 예는 IAM 사용자가`my-user-name`에서 콘솔을 사용하여`globalaccelerator:CreateAccelerator`작업을 수행하지만 사용 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/my-user-name is not authorized to perform: aws-globalaccelerator:CreateAccelerator on resource: my-example-accelerator
```

이 경우에는 관리자에게 정책을 업데이트해달라고 요청하여`my-example-accelerator`리소스를 사용하여`aws-globalaccelerator:CreateAccelerator`action.

관리자이며 다른 사용자가 글로벌 액셀러레이터에 액세스하도록 허용하려고 함

다른 사용자가 글로벌 액셀러레이터에 액세스하도록 허용하려면 액세스 권한이 필요한 사용자 또는 애플리케이션에 대한 IAM 엔터티 (사용자 또는 역할) 를 생성해야 합니다. 다른 사용자들은 해당 개체에 대한 자격 증명을 사용해 AWS에 액세스합니다. 그런 다음 글로벌 액셀러레이터에서 올바른 권한을 부여하는 정책을 엔터티에 연결해야 합니다.

바로 시작하려면 IAM 시작하기 (p. 94) 단원을 참조하십시오.

전문가가 되지 않고 IAM을 이해하길 원함

IAM 용어, 개념 및 절차에 대해 자세히 알아보려면 다음 주제를 참조하십시오.

태그 기반 정책

IAM 정책을 설계할 때 특정 리소스에 대한 액세스 권한을 부여하여 세부적인 권한을 설정할 수 있습니다. 관리하는 리소스의 개수가 늘어날수록 이 작업은 더 어려워집니다. 가속기에 태그를 지정하고 정책 문 조건에서 태그를 사용하면 이러한 작업이 더 간단해질 수 있습니다. 특정 태그가 있는 모든 가속기에 대량으로 액세스 권한을 부여합니다. 그런 다음 액셀러레이터를 만들거나 나중에 액셀러레이터를 업데이트할 때 관련 액셀러레이터에 반복해서 적용합니다.

Note

조건에 태그를 사용하는 것은 리소스 및 요청에 대한 액세스를 제어하는 하나의 방법입니다. Global Accelerator에서 태그 지정에 대한 자세한 내용은AWS Global Accelerator (p. 9).

리소스에 태그가 연결되거나 태그 지정을 지원하는 서비스에 대한 요청에서 전달될 수 있습니다. 전역 가속기에서는 가속기만 태그를 포함할 수 있습니다. IAM 정책을 생성하면 태그 조건 키를 사용하여 다음을 제어할 수 있습니다.

- 이미 가지고 있는 태그를 기반으로 액셀러레이터에 대해 작업을 수행할 수 있는 사용자
- 어떤 태그가 작업의 요청에서 전달될 수 있는지 제어합니다.
- 요청에서 특정 키를 사용할 수 있는지 여부

태그 조건 키의 전체 구문 및 의미는 단원을 참조하십시오.IAM 태그를 사용하여 액세스 제어의IAM 사용 설명서.

예를 들어 글로벌 가속기`GlobalAcceleratorFullAccess`관리형 사용자 정책은 사용자에게 모든 리소스에서 모든 글로벌 액셀러레이터 작업을 수행할 수 있는 무제한적인 권한을 제공합니다. 다음 정책은 이러한 기능을 제한하고 권한이 없는 사용자의 모든 글로벌 액셀러레이터 작업 수행 권한을 거부합니다.프로덕션액셀러레이터 고객의 관리자는 권한이 없는 IAM 사용자에게 관리형 사용자 정책 이외에 이 IAM 정책도 연결해야 합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:RequestTag/stage":"prod"
            }
         }
      },
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:ResourceTag/stage":"prod"
            }
         }
      }
   ]
}
```

글로벌 액셀러레이터를 위한 서비스 연결 역할

AWS 글로벌 액셀러레이터 (IAM) 를 사용하는 AWS Global Accelerator서비스 연결 역할. 서비스 연결 역할은 서비스에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 해당 서비스에서 사전 정의하며 서비스에서 사용자를 대신하여 다른 AWS 서비스를 호출하기 위해 필요한 모든 권한을 포함합니다.

Global Accelerator는 다음 IAM 서비스 연결 역할을 사용합니다.

- AWS서비스역할글로벌 가속기- 글로벌 액셀러레이터는 이 역할을 사용하여 글로벌 액셀러레이터가 클라이언트 IP 주소 보존에 필요한 리소스를 만들고 관리할 수 있도록 합니다.

글로벌 액셀러레이터 API 작업을 지원하기 위해 역할이 먼저 필요한 경우 글로벌 액셀러레이터는 AWSServiceRoleForGlobalAccelerator 라는 역할을 자동으로 생성합니다. AWSServiceRoleForGlobalAccelerator 역할을 사용하면 글로벌 가속기가 클라이언트 IP 주소 보존에 필요한 리소스를 만들고 관리할 수 있습니다. 이 역할은 글로벌 가속기에서 가속기를 사용하는 데 필요합니다. AWSServiceRoleFor글로벌 가속기 역할에 대한 ARN 의 모양은 다음과 같습니다.

```
arn:aws:iam::123456789012:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator
```

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 글로벌 액셀러레이터를 더 쉽게 설정하고 사용할 수 있습니다. 글로벌 액셀러레이터는 서비스 연결 역할의 권한을 정의하므로 글로벌 액셀러레이터만이 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

서비스 연결 역할을 삭제하려면 먼저 연결된 글로벌 액셀러레이터 리소스를 제거해야 합니다. 이렇게 하면 활성 리소스에 액세스하는 데 필요한 서비스 연결 역할을 제거할 필요가 없어 글로벌 액셀러레이터 리소스를 보호할 수 있습니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 를 참조하십시오.IAM과 함께 작동하는 AWS 서비스가지고 있는 서비스를 찾아보세요.예의서비스 연결 역할열을 선택합니다.

글로벌 Accelerator에 대한 서비스 연결 역할 권한

Global Accelerator는 서비스 연결 역할을 사용합니다.AWS서비스역할글로벌 가속기. 다음 단원에서는 역할에 대한 권한을 설명합니다.

서비스 연결 역할 권한

글로벌 액셀러레이터는 이 서비스 연결 역할을 통해 EC2 엘라스틱 네트워크 인터페이스 및 보안 그룹을 관리하고 오류를 진단할 수 있습니다.

AWSServiceRoleForGlobalAccelerator 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `globalaccelerator.amazonaws.com`

역할 권한 정책은 글로벌 액셀러레이터가 정책에 표시된 것처럼 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

IAM 엔터티 (예: 사용자, 그룹 또는 역할) 가 글로벌 액셀러레이터 서비스 연결 역할을 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 단원을 참조하십시오.서비스 연결 역할 권한의IAM 사용 설명서.

Global Accelerator에 대한 서비스 연결 역할 생성

글로벌 액셀러레이터에 대한 서비스 연결 역할은 수동으로 생성하지 않습니다. 이 서비스는 사용자가 가속기를 처음 생성할 때 자동으로 사용자를 대신하여 역할을 생성합니다. 글로벌 액셀러레이터 리소스를 제거하고 서비스 연결 역할을 삭제한 경우 새 액셀러레이터를 생성할 때 서비스가 자동으로 다시 생성합니다.

Global Accelerator 서비스 연결 역할 편집

글로벌 액셀러레이터는 AWSServiceRoleFor글로벌 액셀러레이터 서비스 연결 역할을 편집할 수 없습니다. 서비스에서 서비스 연결 역할을 만든 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 단원을 참조하십시오.서비스 연결 역할 편집의IAM 사용 설명서.

Global Accelerator 서비스 연결 역할 삭제

글로벌 액셀러레이터를 더 이상 사용할 필요가 없는 경우에는 서비스 연결 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하지 않거나 유지하지 않는 미사용 개체가 없도록 합니다. 단, 계정에서 글로벌 액셀러레이터 리소스를 먼저 정리해야 역할을 수동으로 삭제할 수 있습니다.

가속기를 비활성화하고 삭제한 후에는 서비스 연결 역할을 삭제할 수 있습니다. 가속기 삭제에 대한 자세한 내용은 단원을 참조하십시오. 표준 액셀러레이터 만들기 또는 업데이트 (p. 21).

> **Note**
>
> 액셀러레이터를 비활성화하고 삭제했지만 글로벌 액셀러레이터가 업데이트를 완료하지 않으면 서비스 연결 역할이 삭제되지 않습니다. 이 문제가 발생하면 몇 분 기다렸다가 서비스 연결 역할 삭제 단계를 다시 시도하십시오.

AWSServiceRoleFor글로벌 액셀러레이터 서비스 연결 역할을 수동으로 삭제하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택합니다. 그런 다음 삭제할 역할의 이름이나 행이 아닌 이름 옆에 있는 확인란을 선택합니다.
3. 페이지 상단의 역할 작업에서 역할 삭제를 선택합니다.
4. 확인 대화 상자가 나타나면 서비스 마지막 액세스 데이터를 검토합니다. 이 데이터는 선택한 각 역할이 AWS 서비스를 마지막으로 액세스한 일시를 보여줍니다. 이를 통해 역할이 현재 활동 중인지 여부를 확인할 수 있습니다. 계속 진행하려면 [Yes, Delete]을 선택하여 삭제할 서비스 연결 역할을 제출합니다.
5. IAM 콘솔 알림을 보고 서비스 연결 역할 삭제 진행 상황을 모니터링합니다. IAM 서비스 연결 역할 삭제는 비동기이므로 삭제할 역할을 제출한 후에 삭제 작업이 성공하거나 실패할 수 있습니다. 자세한 내용은 단원을 참조하십시오.서비스 연결 역할 삭제의IAM 사용 설명서.

글로벌 액셀러레이터 서비스 연결 역할 (AWS 관리형 정책) 에 대한 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후 에 대한 서비스 연결 역할 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 보려면 AWS Global Accelerator RSS 피드를 구독하십시오.문서 기록 (p. 107)페이지를 참조하십시오.

변경 사항	설명	날짜
AWS서비스역할글로벌 가속기—정책 업데이트	글로벌 액셀러레이터는 글로벌 액셀러레이터에서 오류를 진단하는 데 도움이 되는 새로운 권한을 추가했습니다. 글로벌 액셀러레이터`ec2:DescribeRegions`를 사용하여 고객이 속한 AWS 리전을 확인하면 글로벌 액셀러레이터가 오류를 해결하는 데 도움이 될 수 있습니다.	2021년 5월 18일
글로벌 액셀러레이터 변경 내용 추적 시작	글로벌 액셀러레이터는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 5월 18일

Global Accelerator 서비스 연결 역할이 지원되는 리전

글로벌 액셀러레이터는 글로벌 액셀러레이터가 지원되는 AWS 리전에서 서비스 연결 역할 사용을 지원합니다.

현재 글로벌 액셀러레이터 및 기타 서비스가 지원되는 AWS 리전 목록은AWS 리전 테이블.

액세스 및 인증 개요

IAM을 처음 사용하는 경우 AWS 에서 권한 부여 및 액세스를 시작하려면 다음 단원을 참조하십시오.

주제

- 인증이란 무엇입니까? (p. 88)

인증이란 무엇입니까?

인증은 자격 증명을 사용하여 AWS 에 로그인하는 방식입니다.

> Note
>
> 빠르게 시작하려면 이 섹션을 무시할 수 있습니다. 먼저 에 대한 소개 정보를 살펴보십시오.AWS Global Accelerator 자격 증명 및 액세스 관리 (p. 77), 다음 단원을 참조하십시오.IAM 시작하기 (p. 94).

주체로서, 당신은인증AWS 에 로그인) 을 엔터티 (루트 사용자, IAM 사용자 또는 IAM 역할) 를 사용해 AWS 로 요청을 보냅니다. IAM 사용자에게 사용자 이름과 암호 또는 액세스 키 세트와 같은 장기 자격 증명이 있을 수 있습니다. IAM 역할을 맡으면 임시 보안 자격 증명이 주어집니다.

AWS Management Console에서 사용자로 인증하려면 사용자 이름 및 암호를 사용하여 로그인해야 합니다. AWS CLI 또는 AWS API에서 인증을 받으려면 액세스 키와 보안 키 또는 임시 자격 증명을 제공해야 합니다. AWS 는 자격 증명을 사용해 암호화 방식으로 요청에 서명할 수 있는 SDK 및 CLI 도구를 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS는 Multi-Factor Authentication(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다.

보안 주체로서 다음 엔터티 (사용자 또는 역할) 를 사용하여 AWS 에 로그인할 수 있습니다.

AWS 계정 루트 사용자

AWS 계정을 처음 생성하는 경우에는 계정의 모든 AWS 서비스 및 리소스에 대해 완전한 액세스 권한을 지닌 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 마실 것을 강력히 권장합니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수합니다. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 사용합니다.

IAM 사용자

한IAM 사용자은 특정 권한을 가지고 있는 AWS 계정 내 엔터티입니다. 글로벌 액셀러레이터 지원서명 버전 4이는 인바운드 API 요청을 인증하기 위한 프로토콜입니다. 요청 인증에 대한 자세한 내용은 단원을 참조하십시오.서명 버전 4 서명 프로세스의AWS 일반 참조.

IAM 역할

한IAM 역할은 특정 권한을 가지고 있는 계정에 생성할 수 있는 IAM 자격 증명입니다. AWS에서 자격 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책을 갖춘 AWS 자격 증명이라는 점에서 IAM 역할은 IAM 사용자와 유사합니다. 그러나 역할은 한 사람과만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 대신에 역할을 맡은 사람에게는 해당 역할 세션을 위한 임시 보안 자격 증명이 제공됩니다. 임시 자격 증명이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

연합된 사용자 액세스

IAM 사용자를 생성하는 대신 AWS Directory Service의 기존 자격 증명, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이러한 사용자를 연동 사용자라고 합니다. 자격 증명 공급자를 통해 액세스를 요청하면 AWS가 연합된 사용자에게 역할을 할당합니다. 페더레이션 사용자에 대한 자세한 내용은연동 사용자 및 역할의IAM 사용 설명서.

임시 사용자 권한

IAM 사용자는 한 가지 역할을 맡음으로써 특정 작업을 위해 다른 권한을 임시로 얻을 수 있습니다.

교차 계정 액세스

IAM 역할을 사용하여 다른 계정의 신뢰할 수 있는 보안 주체가 내 계정의 리소스에 액세스하도록 할 수 있습니다. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스에서는 역할을 프록시로 사용하는 대신 리소스에 정책을 직접 연결할 수 있습니다. 글로벌 액셀러레이터는 이러한 리소스 기반 정책을 지원하지 않습니다. 교차 계정 액세스를 허용하기 위해 역할 또는 리소스 기반 정책을 사용할지 여부에 대한 자세한 내용은 다른 계정에서 보안 주체에 대한 액세스 제어 (p. 91) 단원을 참조하십시오.

AWS 서비스 액세스

서비스 역할은IAM 역할서비스가 사용자를 대신하여 작업을 수행하기 위해 수임한 것으로 가정합니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 단원을 참조하십시오.AWS 서비스에 대한 권한을 위임할 역할 생성의IAM 사용 설명서.

Amazon EC2에서 실행 중인 애플리케이션

IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 그 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 만들어야 합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 단원을 참조하십시오.IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여의IAM 사용 설명서.

액세스 제어란 무엇입니까?

AWS에 로그인하면 (인증되면) AWS 리소스 및 작업에 대한 액세스는 정책에 의해 관리됩니다. 액세스 제어는 권한 부여라고도 합니다.

Note

빠르게 시작하려면 이 페이지를 무시할 수 있습니다. 먼저 에 대한 소개 정보를 살펴보십시오.AWS Global Accelerator 자격 증명 및 액세스 관리 (p. 77), 다음 단원을 참조하십시오.IAM 시작하기 (p. 94).

권한 부여 동안 AWS 는요청 컨텍스트을 선택하여 적용되는 정책을 확인합니다. 그런 다음 이것은 정책을 사용하여 요청을 허용하거나 거부할지 여부를 결정합니다. 대부분의 정책은 AWS 에 JSON 문서로 저장되며 보안 주체에 대해 허용되거나 거부되는 권한을 지정합니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 정책이란 무엇입니까? (p. 91) 단원을 참조하십시오.

정책을 사용하여 관리자는 AWS 리소스에 액세스할 수 있는 대상과 액세스한 사용자가 해당 리소스에서 수행할 수 있는 작업을 지정할 수 있습니다. 모든 IAM 개체(사용자 또는 역할)는 처음에는 권한이 없습니다. 다시 말해, 기본적으로 사용자는 아무 작업도 할 수 없으며, 심지어 자신의 액세스 키를 볼 수도 없습니다. 사용자에게 작업을 수행할 권한을 부여하기 위해 관리자는 사용자에게 권한 정책을 연결해야 합니다. 의도한 권한을 보유한 그룹에 사용자를 추가할 수 있습니다. 그런 다음 관리자가 그룹에 권한을 부여하면 그룹의 모든 사용자가 해당 권한을 얻습니다.

요청을 인증하는 데 유효한 자격 증명이 있더라도 관리자가 권한을 부여하지 않으면 AWS Global Accelerator 리소스를 생성하거나 액세스할 수 없습니다. 예를 들어 AWS Global Accelerator 가속기를 생성할 명시적인 권한이 있어야 합니다.

관리자는 다음에 대한 액세스를 제어하는 정책을 작성할 수 있습니다.

- Principal (p. 90)— 사용자 또는 애플리케이션이 요청하는 사항을 제어합니다 (보안 주체) 가 허용됩니다.
- IAM 자격 증명 (p. 90)IAM 자격 증명 (그룹, 사용자 및 역할) 에 액세스할 수 있는 및 그 방법을 제어합니다.

- IAM 정책 (p. 90)— 고객 관리형 정책을 생성, 편집 및 삭제할 수 있는 대상과 모든 관리형 정책을 연결하고 분리할 수 있는 대상을 제어합니다.
- AWS 리소스 (p. 90)— 자격 증명 기반 정책 또는 리소스 기반 정책을 사용하여 리소스에 액세스할 수 있는 대상을 제어할 수 있습니다.
- AWS 계정 (p. 91)- 특정 계정의 멤버에만 요청이 허용되는지 여부를 제어합니다.

보안 주체에 대한 액세스 제어

권한 정책은 보안 주체가 수행할 수 있는 작업을 제어합니다. 관리자는 자격 증명(사용자, 그룹 또는 역할)에 권한을 제공하는 자격 증명 기반 권한 정책을 연결해야 합니다. 권한 정책은 AWS 에 대한 액세스를 허용하거나 거부합니다. 또한 관리자는 IAM 엔터티 (사용자 또는 역할) 에 대한 권한 경계를 설정해 해당 엔터티가 가질 수 있는 최대 권한을 정의할 수 있습니다. 권한 경계는 고급 기능입니다. 권한 경계에 대한 자세한 내용은 단원을 참조하십시오.IAM 자격 증명에 대한 권한 경계의IAM 사용 설명서.

보안 주체에 대한 AWS 액세스를 제어하는 방법에 대한 자세한 내용과 예는보안 주체에 대한 액세스 제어의IAM 사용 설명서.

자격 증명에 대한 액세스 제어

관리자는 자격 증명에 대해 수행할 수 있는 작업과 자격 증명에 액세스할 수 있는 사람을 제한하는 정책을 생성하여 IAM 자격 증명 (사용자, 그룹 또는 역할) 에 대해 수행할 수 있는 작업을 제어합니다. 그런 다음 자격 증명에 권한을 제공하는 정책을 연결합니다.

예를 들어, 관리자가 여러분이 사용자 3명에 대해 암호를 재설정할 수 있도록 허용할 수 있습니다. 이렇게 하기 위해 관리자는 자신과 지정된 사용자 3명의 ARN 가진 사용자에 대한 암호만 재설정할 수 있도록 허용하는 정책을 여러분의 IAM 사용자에게 연결합니다. 그러면 팀원의 암호를 재설정할 수 있지만 다른 IAM 사용자는 재설정할 수 없습니다.

자격 증명에 대한 AWS 액세스를 제어하는 정책을 사용하는 방법에 대한 자세한 내용과 예는자격 증명에 대한 액세스 제어의IAM 사용 설명서.

정책에 대한 액세스 제어

관리자는 누가 고객 관리형 정책을 생성, 편집 및 삭제할 수 있고, 누가 모든 관리형 정책을 연결하고 분리할 수 있는지 제어합니다. 정책을 보면 그 정책 안에서 각 서비스에 대한 액세스 레벨의 요약이 들어 있는 정책 요약을 확인할 수 있습니다. AWS 는 각 서비스 작업을 네 가지 중 하나로 분류합니다.액세스 레벨각 작업이 수행하는 작업에 따라:`List`,`Read`,`Write`또는`Permissions management`. 이러한 액세스 레벨을 사용하여 어떤 작업을 정책에 포함할지 결정할 수 있습니다. 자세한 내용은 단원을 참조하십시오.정책 요약 내의 액세스 수준 요약 이해의IAM 사용 설명서.

> Warning
>
> 제한해야 합니다.`Permissions Management`계정에서 액세스 레벨 권한을 부여합니다. 그렇지 않으면 계정 멤버가 가지고 있어야 하는 것보다 더 많은 권한을 가지고 직접 정책을 생성할 수 있습니다. 또는 AWS 에 대한 모든 액세스 권한을 가진 별도의 사용자를 생성할 수 있습니다.

정책에 대한 AWS 액세스를 제어하는 방법에 대한 자세한 내용과 예는정책에 대한 액세스 제어의IAM 사용 설명서.

리소스에 대한 액세스 제어

관리자는 자격 증명 기반 정책 또는 리소스 기반 정책을 사용하여 리소스에 대한 액세스를 제어할 수 있습니다. 자격 증명 기반 정책에서 자격 증명에 정책을 연결하고 자격 증명이 액세스할 수 있는 리소스를 지정합니다. 리소스 기반 정책에서 제어하려는 리소스에 정책을 연결합니다. 정책에서 해당 리소스에 액세스할 수 있는 보안 주체를 지정합니다.

자세한 내용은 단원을 참조하십시오.리소스에 대한 액세스 제어의IAM 사용 설명서.

리소스 작성자가 자동으로 사용 권한을 갖지 않음

리소스를 누가 생성했든 상관 없이 계정 내 모든 리소스를 해당 계정이 소유합니다. AWS 계정 루트 사용자는 계정 소유자이므로는 계정의 모든 리소스에 대해 작업을 수행할 권한이 있습니다.

> **Important**
>
> 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 마십시 것을 강력히 권장합니다. 그 대신,IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 사용합니다. 루트 사용자로 로그인해야 하는 작업을 보려면루트 사용자가 필요한 AWS 작업.

AWS 계정의 엔터티 (사용자 또는 역할) 에 리소스를 생성할 수 있는 액세스 권한을 부여해야 합니다. 그러나 리소스를 생성했다는 이유만으로 해당 리소스에 대한 모든 액세스 권한이 자동으로 부여되지는 않습니다. 관리자는 각 작업에 대해 권한을 명시적으로 부여해야 합니다. 또한 관리자는 사용자 및 역할 권한을 관리할 수 있는 액세스 권한이 있는 한 언제든지 권한을 취소할 수 있습니다.

다른 계정에서 보안 주체에 대한 액세스 제어

관리자는 AWS 리소스 기반 정책, IAM 리소스 교차 계정 역할 또는 AWS Organizations 서비스를 사용하여 다른 계정의 보안 주체가 내 리소스에 액세스하도록 할 수 있습니다.

일부 AWS 서비스의 경우 관리자는 리소스에 대한 교차 계정 액세스 권한을 부여할 수 있습니다. 이렇게 하려면 관리자는 역할을 프록시로 사용하는 대신 공유하고자 하는 리소스에 정책을 직접 연결합니다. 서비스에서 이 정책 유형을 지원하는 경우 관리자가 공유하는 리소스는 리소스 기반 정책을 지원해야 합니다. 사용자 기반 정책과 달리 리소스 기반 정책은 해당 리소스에 액세스할 수 있는 사용자 (AWS 계정 ID 번호 목록의 형태) 를 지정합니다. Global Accelerator는 리소스 기반 정책을 지원하지 않습니다.

리소스 기반 정책을 사용한 교차 계정 액세스는 역할에 비해 몇 가지 이점이 있습니다. 리소스 기반 정책을 통해 액세스한 리소스로 인해 보안 주체(개인 또는 애플리케이션)는 여전히 신뢰받는 계정에서 작업을 할 수 있고 역할 권한 대신에 자신의 사용자 권한을 포기할 필요가 없습니다. 다시 말해서 보안 주체는 자신이 신뢰하는 계정과 자신을 신뢰하는 계정의 리소스에 동시에 액세스할 수 있습니다. 이는 한 계정에서 다른 계정으로 정보를 복사하는 등의 작업에서 특히 유용합니다. 교차 계정 역할 사용에 대한 자세한 내용은 단원을 참조하십시오.자신이 소유한 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공의IAM 사용 설명서.

AWS Organizations 소유한 여러 AWS 계정에 정책 기반 관리를 제공합니다. Organizations 사용하면 계정 그룹을 생성하고 계정 생성을 자동화하며 해당 그룹에 정책을 적용하고 관리할 수 있습니다. 또한 사용자 지정 스크립트와 수동 프로세스 없이도 여러 계정의 정책을 중앙에서 관리할 수 있습니다. AWS Organizations 사용하면 여러 AWS 계정의 AWS 서비스 사용을 중앙에서 제어하는 SCP (서비스 제어 정책) 를 생성할 수 있습니다. 자세한 내용은 단원을 참조하십시오.AWS Organizations 이란 무엇입니까?의AWS Organizations 사용 설명서.

정책이란 무엇입니까?

정책을 생성하고 IAM 자격 증명 또는 AWS 리소스에 연결하여 AWS 액세스를 제어합니다.

> **Note**
>
> 빠르게 시작하려면 이 페이지를 무시할 수 있습니다. 먼저 에 대한 소개 정보를 살펴보십시오.AWS Global Accelerator 자격 증명 및 액세스 관리 (p. 77), 다음 단원을 참조하십시오.IAM 시작하기 (p. 94).

정책은 엔터티 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS 의 객체입니다. AWS는 사용자와 같은 보안 주체가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지 여부를 결정합니다. 대부분의 정책은 AWS에 JSON 문서로 저장됩니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어 정책에서GetUser작업을 수행하면 해당 정책이 있는 사용자는 AWS Management Console, AWS CLI 또는 AWS API에서 사용자 정보를 얻을 수 있습니다. IAM 사용자를 생성할 경우 사용자가 콘솔 또는 프로그래밍

방식 액세스를 허용하도록 설정할 수 있습니다. IAM 사용자는 사용자 이름 및 암호를 사용하는 콘솔에 로그인할 수 있습니다. 또는 CLI 또는 API를 사용해 액세스 키를 사용할 수 있습니다.

빈도수에 따라 나열된 다음 정책 유형에 따라 요청의 허가 여부가 달라질 수 있습니다. 자세한 내용은 단원을 참조하십시오.정책 유형의IAM 사용 설명서.

자격 증명 기반 정책

관리형 및 인라인 정책을 IAM 자격 증명 (사용자, 사용자가 속한 사용자 그룹 및 역할) 에 연결할 수 있습니다.

리소스 기반 정책

인라인 정책을 일부 AWS 서비스의 리소스에 연결할 수 있습니다. 리소스 기반 정책의 가장 일반적인 예제는 Amazon S3 버킷 정책 및 IAM 역할 신뢰 정책입니다. Global Accelerator는 리소스 기반 정책을 지원하지 않습니다.

Organizations CP

AWS Organizations 서비스 제어 정책 (SCP) 을 사용하여 AWS Organizations 조직 조직 또는 조직 단위 (OU) 에 권한 경계를 적용할 수 있습니다. 이러한 권한은 멤버 계정 내 모든 엔터티에 적용됩니다.

ACL(액세스 제어 목록)

ACL을 사용하여 보안 주체의 리소스 액세스를 제어할 수 있습니다. ACL는 리소스 기반 정책과 비슷합니다. 다만 JSON 정책 문서 구조를 사용하지 않은 유일한 정책 유형입니다. Global Accelerator는 ACL을 지원하지 않습니다.

이런 정책 유형은 권한 정책 또는 권한 경계로 분류할 수 있습니다.

권한 정책

AWS 의 리소스에 권한 정책을 연결해 해당 객체에 대한 권한을 정의할 수 있습니다. AWS 단일 계정 내에서 모든 권한 정책을 같이 평가합니다. 권한 정책은 가장 범용 정책입니다. 다음 권한 유형을 권한 정책으로 사용할 수 있습니다.

자격 증명 기반 정책

관리형 또는 인라인 정책을 IAM 사용자, 그룹 또는 역할에 연결하면 정책은 해당 엔터티에 대한 권한을 정의합니다.

리소스 기반 정책

JSON 정책 문서를 리소스로 연결할 경우, 그 리소스에 대한 권한을 정의할 수 있습니다. 서비스는 리소스 기반 정책을 지원해야 합니다.

ACL(액세스 제어 목록)

ACL을 리소스로 연결할 경우, 그 리소스에 대한 액세스 권한의 보안 주체 목록을 정의할 수 있습니다. 리소스는 ACL을 지원해야 합니다.

권한 경계

정책을 사용하여 엔터티 (사용자 또는 역할) 에 대한 권한 경계를 정의할 수 있습니다. 이 권한 경계는 엔터티가 가질 수 있는 최대 권한을 제어합니다. 권한 경계는 AWS 기능입니다. 두 개 이상의 권한 경계를 요청에 적용할 경우 AWS 는 권한 경계를 각각 평가합니다. 다음 상황에서 권한 경계를 적용할 수 있습니다.

Organizations

AWS Organizations 서비스 제어 정책 (SCP) 을 사용하여 AWS Organizations 조직 조직 또는 조직 단위 (OU) 에 권한 경계를 적용할 수 있습니다.

IAM 사용자 또는 역할

관리형 정책을 사용자 또는 역할의 권한 경계용 사용할 수 있습니다. 자세한 내용은 단원을 참조하십시오.IAM 엔터티에 대한 권한 경계의IAM 사용 설명서.

주제

자격 증명 기반 정책

정책을 IAM 자격 증명에 연결할 수 있습니다. 예를 들면,

계정 내 사용자 또는 그룹에 권한 정책 연결

AWS Global Accelerator 리소스 (예:) 생성 권한을 해당 사용자에게 부여하려면 해당 사용자 또는 사용자가 속한 그룹에 권한 정책을 연결할 수 있습니다.

역할에 권한 정책 연결 (교차 계정 권한 부여)

자격 증명 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어, 계정 A의 관리자는 다음과 같이 다른 AWS 계정(예: 계정 B) 또는 AWS 서비스에 교차 계정 권한을 부여할 역할을 생성할 수 있습니다.

1. 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 역할에 권한 정책을 연결합니다.
2. 계정 A 관리자는 계정 B를 역할을 수임할 보안 주체로 식별하는 역할에 신뢰 정책을 연결합니다.
3. 계정 B 관리자는 계정 B의 사용자에게 역할을 수임할 권한을 위임할 수 있습니다. 그러면 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스할 수 있습니다. AWS 서비스에 역할 수임 권한을 부여할 경우 신뢰 정책의 보안 주체가 AWS 서비스 보안 주체이기도 합니다.

IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 를 참조하십시오.액세스 관리의IAM 사용 설명서.

사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 를 참조하십시오.자격 증명(사용자, 그룹, 및 역할)의IAM 사용 설명서.

다음은 글로벌 액셀러레이터와 함께 사용할 수 있는 두 가지 정책의 예입니다. 첫 번째 예제 정책은 사용자에게 AWS 계정의 가속기에 대한 모든 List 및 Describe 작업에 대한 프로그래밍 방식의 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

다음 예제에서는 프로그래밍 방식으로`ListAccelerators`작업:

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

```
            "Action": [
                "globalaccelerator:ListAccelerators",
            ],
            "Resource": "*"
        }
    ]
}
```

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 이러한 정책은 지정된 보안 주체가 해당 리소스에 대해 수행할 수 있는 작업 및 이에 관한 조건을 지정하도록 허용합니다. 가장 일반적인 리소스 기반 정책은 Amazon S3 버킷입니다. 리소스 기반 정책은 리소스에만 존재하는 인라인 정책입니다. 관리형 리소스 기반 정책은 없습니다.

리소스 기반 정책을 사용해 다른 AWS 계정의 멤버에게 권한을 부여하는 것은 IAM 역할에 비해 몇 가지 이점이 있습니다. 자세한 내용은 단원을 참조하십시오.IAM 역할과 리소스 기반 정책의 차이의IAM 사용 설명서.

정책 액세스 수준 분류

IAM 콘솔에서 작업은 다음 액세스 레벨 분류를 사용하여 그룹화됩니다.

나열

서비스 내의 리소스를 나열하여 객체가 존재하는지 판단할 수 있는 권한을 제공합니다. 이 액세스 레벨의 작업은 객체를 나열할 수 있으나 리소스의 내용을 확인할 수 없습니다. 액세스 레벨이 나열인 대부분의 작업은 특정 리소스에 대해 수행할 수 없습니다. 이러한 작업에 관련한 정책 설명을 생성할 때 모든 리소스(`"*"`)를 지정해야 합니다.

Read

읽기 서비스에서 리소스 내용과 속성을 읽을 수 있으나 편집할 수 없는 권한을 제공합니다. 예를 들어 Amazon S3 작업`GetObject`및`GetBucketLocation`를 가지고Read액세스 레벨

쓰기

쓰기 서비스에서 리소스를 생성, 삭제 또는 수정할 수 있는 권한을 제공합니다. 예를 들어 Amazon S3 작업`CreateBucket`,`DeleteBucket`, 및`PutObject`를 가지고쓰기액세스 레벨

권한 관리

권한 서비스에서 리소스 권한을 부여하거나 수정할 수 있는 권한을 제공합니다. 예를 들어, 대부분의 IAM 및 AWS Organizations 정책 작업에는권한 관리액세스 레벨

Tip

AWS 계정의 보안을 개선하려면권한 관리액세스 수준 분류입니다.

태그 지정

작성, 삭제 또는 서비스의 리소스에 연결된 태그를 생성, 삭제하거나 수정할 수 있는 권한을 제공합니다. 예를 들어 Amazon EC2`CreateTags`및`DeleteTags`작업에는태그 지정액세스 레벨

IAM 시작하기

AWS Identity and Access Management (IAM) 는 서비스 및 리소스에 대한 사용자의 액세스를 안전하게 관리할 수 있게 해주는 AWS 서비스입니다. IAM은 추가 비용 없이 AWS 계정의 기능입니다.

Note

IAM으로 시작하기 전에 에 대한 기본 정보를 살펴보십시오.AWS Global Accelerator 자격 증명 및 액세스 관리 (p. 77).

AWS 계정을 처음 생성하는 경우에는 계정의 모든 AWS 서비스 및 리소스에 대해 완전한 액세스 권한을 지닌 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 마실 것을 강력히 권장합니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수합니다. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 사용합니다.

IAM 관리 사용자를 생성합니다.

관리자 사용자를 직접 생성하여 관리자 그룹에 추가하려면(콘솔)

1. 에 로그인합니다.IAM 콘솔를 선택하여 계정 소유자로루트 사용자를 클릭하고 AWS 계정 이메일 주소를 입력합니다. 다음 페이지에서 암호를 입력합니다.

   Note

   를 사용하는 모범 사례를 준수하는 것이 좋습니다.**`Administrator`**IAM 사용자를 팔로우하고, 루트 사용자 자격 증명을 안전하게 보관합니다. 몇 가지 계정 및 서비스 관리 태스크를 수행하려면 반드시 루트 사용자로 로그인해야 합니다.
2. 탐색 창에서 사용자와 사용자 추가를 차례로 선택합니다.
3. 사용자 이름에 **`Administrator`**를 입력합니다.
4. AWS Management Console 액세스(AWS Management Console access)옆에 있는 확인란을 선택합니다. 그런 다음 Custom password(사용자 지정 암호)를 선택하고 텍스트 상자에 새 암호를 입력합니다.
5. (선택 사항) 기본적으로 AWS에서는 새 사용자가 처음 로그인할 때 새 암호를 생성해야 합니다. User must create a new password at next sign-in(사용자가 다음에 로그인할 때 새 암호를 생성해야 합니다) 옆에 있는 확인란의 선택을 취소하면 새 사용자가 로그인한 후 암호를 재설정할 수 있습니다.
6. 선택다음: 권한.
7. 권한 설정 아래에서 그룹에 사용자 추가를 선택합니다.
8. 그룹 생성을 선택합니다.
9. 그룹 생성 대화 상자의 그룹 이름에 **`Administrators`**를 입력합니다.
10. 선택정책 필터링을 선택한 다음AWS 관리형 - 직무 기능를 클릭하여 테이블 내용을 필터링합니다.
11. 정책 목록에서 AdministratorAccess 확인란을 선택합니다. 그런 다음 Create group을 선택합니다.

    Note

    `AdministratorAccess` 권한을 사용하여 AWS 결제 및 비용 관리 콘솔에 액세스하려면 먼저 결제에 대한 IAM 사용자 및 역할 액세스를 활성화해야 합니다. 이를 위해 결제 콘솔에 액세스를 위임하기 위한 자습서 1단계의 지침을 따르십시오.
12. 그룹 목록으로 돌아가 새로 만든 그룹 옆의 확인란을 선택합니다. 목록에서 그룹을 확인하기 위해 필요한 경우 Refresh(새로 고침)를 선택합니다.
13. 선택다음: 태그.
14. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 단원을 참조하십시오.IAM 엔터티 태그 지정의IAM 사용 설명서.
15. 선택다음: 검토새 사용자에게 추가할 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 Create user를 선택합니다.

이제 동일한 절차에 따라 그룹이나 사용자를 추가 생성하여 AWS 계정 리소스에 액세스할 수 있는 권한을 사용자에게 부여할 수 있게 되었습니다. 특정 AWS 리소스에 대한 사용자 권한을 제한하는 정책을 사용하는 방법을 알아보려면 액세스 관리 및 정책 예제를 참조하십시오.

글로벌 액셀러레이터를 위한 위임된 사용자 만들기

AWS 계정에서 여러 사용자를 지원하려면 다른 사용자가 허용된 작업만 수행할 수 있도록 권한을 위임해야 합니다. 이렇게 하려면 해당 사용자에게 필요한 권한이 있는 IAM 그룹을 생성한 다음 필요에 따라 필요한 그

룹에 IAM 사용자를 추가합니다. 이 프로세스를 사용하여 전체 AWS 계정에 대한 그룹, 사용자 및 권한을 설정할 수 있습니다. 이 솔루션은 AWS 관리자가 수동으로 사용자 및 그룹을 관리할 수 있는 중소 규모 조직에서 가장 적합합니다. 대규모 조직의 경우 다음을 사용할 수 있습니다.사용자 지정 IAM 역할,연합또는Single Sign-On.

다음 절차에서는 세 명의 사용자를 만듭니다.**arnav**,**carlos**, 및**martha**라는 액셀러레이터를 만들 수 있는 권한을 부여하는 정책을 첨부합니다.**my-example-accelerator**, 그러나 다음 30 일 이내에 만. 여기 제공된 단계에 따라 다른 권한을 가진 사용자를 추가할 수 있습니다.

다른 사용자에 대해 위임 사용자를 생성하려면(콘솔)

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Users와 Add user를 차례대로 선택합니다.
3. 사용자 이름에 **arnav**를 입력합니다.
4. 다른 사용자 추가를 선택하고 두 번째 사용자로 **carlos**을 입력합니다. 다른 사용자 추가를 선택하고 세 번째 사용자로 **martha**를 입력합니다.
5. 옆의 확인란을 선택합니다.AWS Management Console 액세스을 선택한 다음자동 생성된 암호.
6. 새로운 사용자가 로그인한 후 암호를 재설정할 수 있도록 사용자가 다음에 로그인할 때 새 암호를 생성해야 합니다 확인란의 선택을 취소합니다.
7. 선택다음: 권한.
8. Attach existing policies directly(기존 정책 직접 연결)를 선택합니다. 사용자에 대해 새 관리형 정책을 생성합니다.
9. 정책 생성을 선택합니다.

   새 탭 또는 브라우저 창에서 정책 생성 마법사가 열립니다.
10. Visual editor(시각적 편집기) 탭에서 Choose a service(서비스 선택)을 선택합니다. 그런 다음 Global Accelerator 상단의 검색 상자를 사용하여 서비스 목록 결과를 제한할 수 있습니다.

    이서비스섹션이 닫히고작업섹션이 자동으로 열립니다.
11. 허용할 Global Accelerator 작업을 선택합니다. 예를 들어, 액셀러레이터를 생성할 권한을 부여하려면**globalaccelerator:CreateAccelerator**의작업 필터텍스트 상자에 로그인합니다. 전역 가속기 작업 목록이 필터링되면 옆에 있는 확인란을 선택합니다.**globalaccelerator:CreateAccelerator**.

    글로벌 액셀러레이터 작업은 액세스 레벨 분류에 따라 그룹화되어 각 작업이 제공하는 액세스 레벨을 빠르고 쉽게 확인할 수 있습니다. 자세한 내용은 정책 액세스 수준 분류 (p. 94) 섹션을 참조하세요.
12. 이전 단계에서 선택한 작업이 특정 리소스 선택을 지원하지 않는 경우모든 리소스가 선택됩니다. 이러한 경우 이 섹션을 편집할 수 없습니다.

    리소스 수준 권한을 지원하는 작업을 하나 이상 선택하면 시각적 편집기의 리소스 섹션에 해당 리소스 유형이 나열됩니다. 선택필요한 작업을 선택했습니다.액셀러레이터리소스 유형을 선택하여 정책에 특정 액셀러레이터를 입력할지 여부를 선택합니다.
13. 모든 리소스에 대해 `globalaccelerator:CreateAccelerator` 작업을 허용하려는 경우 모든 리소스를 선택합니다.

    리소스를 지정하려는 경우 ARN 추가를 선택합니다. 리전 및 계정 ID (또는 계정 ID) 를 지정하거나 (모두 선택) 을 입력한 다음**my-example-accelerator**리소스의 그런 다음 추가를 선택합니다.
14. 요청 조건 지정(선택 사항)을 선택합니다.
15. 선택조건 추가액셀러레이터를 만들 수 있는 권한을 부여합니다.다음 7일 이내에 합니다. 오늘 날짜가 2019년 1월 1일이라고 가정합니다.
16. 조건 키로 aws:CurrentTime을 선택합니다. 이 조건 키는 사용자가 요청을 생성한 날짜 및 시간을 확인합니다. true를 반환하므로 날짜 및 시간이 지정된 범위에 속하는 경우에만 **globalaccelerator:CreateAccelerator** 작업을 허용합니다.

17. 용Qualifier기본값을 그대로 둡니다.
18. 허용되는 시간 및 날짜 범위의 시작 부분을 지정하려면 연산자로 DateGreaterThan을 선택합니다. 그런 다음 값으로 **`2019-01-01T00:00:00Z`**를 입력합니다.
19. 추가를 선택하여 조건을 저장합니다.
20. 다른 조건 추가를 선택하여 종료 날짜를 지정합니다.
21. 유사한 단계를 수행해 허용되는 날짜 및 시간 범위의 종료 부분을 지정합니다. 조건 키로 aws:CurrentTime을 선택합니다. 연산자로 DateLessThan을 선택합니다. 값으로 첫 번째 날짜 7일 후인 **`2019-01-06T23:59:59Z`**를 입력합니다. 그런 다음 추가를 선택하여 조건을 저장합니다.
22. (선택 사항) 생성한 정책에 대한 JSON 정책 문서를 보려면JSON탭을 선택합니다. 언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경하거나검토 정책의Visual editor(시각적 편집기)탭에서 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 단원을 참조하십시오.정책 재구성의IAM 사용 설명서.
23. 작업이 완료되면 [Review policy]를 선택합니다.
24. 에서검토 정책페이지에 대해이름를 입력하고**`globalaccelerator:CreateAcceleratorPolicy`**. 설명에 **`Policy to grants permission to create an accelerator`**을 입력합니다. 정책 요약을 검토하여 의도한 권한이 부여되었는지 확인한 다음 정책 생성을 선택하여 새 정책을 저장합니다.
25. 원래 탭 또는 창으로 돌아가 정책 목록을 새로 고칩니다.
26. 검색 상자에 **`globalaccelerator:CreateAcceleratorPolicy`**를 입력합니다. 새 정책 옆의 확인란을 선택합니다. 그런 다음 [Next Step]을 선택합니다.
27. 선택다음: 검토을 선택하여 새 사용자를 미리 봅니다. 계속 진행할 준비가 되었으면 사용자 생성을 선택합니다.
28. 새 사용자의 암호를 다운로드하거나 복사하여 사용자에게 안전하게 전달합니다. 이와 별도로 사용자에게IAM 사용자 콘솔 페이지로 연결되는 링크및 방금 생성한 사용자 이름을 입력합니다.

사용자가 자격 증명을 자체 관리할 수 있게 하려면

MFA를 구성하려면 사용자의 가상 MFA 디바이스가 호스팅되는 하드웨어에 대한 물리적 액세스가 필요합니다. 예를 들어, 스마트폰에서 가상 MFA 디바이스를 실행하는 사용자에게 MFA를 구성할 수 있습니다. 이 경우 마법사를 완료하기 위해 스마트폰을 사용할 수 있어야 합니다. 이러한 이유로 사용자가 자신의 가상 MFA 디바이스를 직접 구성 및 관리할 수 있도록 허용하는 것이 좋습니다. 이 경우에는 사용자에게 필요한 IAM 작업을 수행할 수 있는 권한을 부여해야 합니다.

자격 증명 자기 관리를 허용하는 정책을 생성하려면(콘솔)

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
3. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 이 텍스트를 JSON 텍스트 상자에 붙여 넣습니다.

   Important

   이 정책 예제에서는 사용자가 로그인과 암호 재설정을 한 번에 할 수 없습니다. 새 사용자와 암호가 만료된 사용자는 이 작업을 시도할 수 있습니다. `iam:ChangePassword` 및 `iam:CreateLoginProfile`을 `BlockMostAccessUnlessSignedInWithMFA` 문에 추가하여 이를 허용할 수 있습니다. 그러나 IAM에서는 이 방식을 권장하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
```

```
            "iam:ListAccountAliases",
            "iam:ListUsers",
            "iam:ListVirtualMFADevices",
            "iam:GetAccountPasswordPolicy",
            "iam:GetAccountSummary"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation",
        "Effect": "Allow",
        "Action": [
            "iam:ChangePassword",
            "iam:CreateAccessKey",
            "iam:CreateLoginProfile",
            "iam:DeleteAccessKey",
            "iam:DeleteLoginProfile",
            "iam:GetLoginProfile",
            "iam:ListAccessKeys",
            "iam:UpdateAccessKey",
            "iam:UpdateLoginProfile",
            "iam:ListSigningCertificates",
            "iam:DeleteSigningCertificate",
            "iam:UpdateSigningCertificate",
            "iam:UploadSigningCertificate",
            "iam:ListSSHPublicKeys",
            "iam:GetSSHPublicKey",
            "iam:DeleteSSHPublicKey",
            "iam:UpdateSSHPublicKey",
            "iam:UploadSSHPublicKey"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowIndividualUserToViewAndManageTheirOwnMFA",
        "Effect": "Allow",
        "Action": [
            "iam:CreateVirtualMFADevice",
            "iam:DeleteVirtualMFADevice",
            "iam:EnableMFADevice",
            "iam:ListMFADevices",
            "iam:ResyncMFADevice"
        ],
        "Resource": [
            "arn:aws:iam::*:mfa/${aws:username}",
            "arn:aws:iam::*:user/${aws:username}"
        ]
    },
    {
        "Sid": "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
        "Effect": "Allow",
        "Action": [
            "iam:DeactivateMFADevice"
        ],
        "Resource": [
            "arn:aws:iam::*:mfa/${aws:username}",
            "arn:aws:iam::*:user/${aws:username}"
        ],
        "Condition": {
            "Bool": {
                "aws:MultiFactorAuthPresent": "true"
            }
        }
    },
    {
        "Sid": "BlockMostAccessUnlessSignedInWithMFA",
```

```
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:ListVirtualMFADevices",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice",
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListSSHPublicKeys",
                "iam:ListAccessKeys",
                "iam:ListServiceSpecificCredentials",
                "iam:ListMFADevices",
                "iam:GetAccountSummary",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

이 정책이 하는 일은 무엇입니까?

- 이`AllowAllUsersToListAccounts`문은 사용자가 IAM 콘솔에서 계정 및 하위 사용자에 관한 기본 정보를 볼 수 있도록 허용합니다. 이러한 권한은 구체적인 리소스 ARN을 지원하지 않거나, 리소스 ARN을 지정하는 대신 `"Resource" : "*"`를 지정하면 되기 때문에 권한별로 각각의 문에 포함되어 있어야 합니다.
- 이`AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation`문은 사용자가 IAM 콘솔에서 자신의 사용자, 암호, 액세스 키, 서명 인증서, SSH 퍼블릭 키 및 MFA 정보를 관리할 수 있도록 합니다. 사용자가 처음으로 관리자에 로그인할 수 있도록 허용하여 첫 암호를 설정할 수 있도록 합니다. 리소스 ARN 은 사용자의 IAM 사용자 개체만 이러한 권한을 사용할 수 있도록 제한합니다.
- `AllowIndividualUserToViewAndManageTheirOwnMFA` 설명문은 사용자가 자신의 MFA 디바이스를 보거나 관리할 수 있도록 허용합니다. 이 문의 리소스 ARN은 현재 로그인한 사용자와 이름이 정확히 똑같은 MFA 디바이스나 사용자에게만 액세스를 허용한다는 점에 유의하십시오. 사용자들은 자신의 것이 아닌 어떤 MFA 디바이스도 생성 또는 변경할 수 없습니다.
- `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA` 문은 사용자가 MFA를 사용하여 로그인한 경우에만 자신의 MFA 디바이스를 비활성화할 수 있도록 허용합니다. 이를 통해 액세스 키만 있는 다른 사용자(MFA 디바이스가 없음)가 MFA 디바이스를 비활성화하고 계정에 액세스할 수 있습니다.
- 이`BlockMostAccessUnlessSignedInWithMFA`문의 조합을 사용 하는`"Deny"`및`"NotAction"`를 사용하여 IAM 및 기타 AWS 서비스에서 일부 작업을 제외한 모든 작업에 대한 액세스를 거부할 수 있습니다.다음과 같은 경우사용자가 MFA 로 로그인되지 않았습니다. 이 문의 로직에 대한 자세한 내용은 단원을 참조하십시오.NotAction 및 Deny의IAM 사용 설명서. 사용자가 MFA로 로그인한 경우에는 `"Condition"` 테스트가 실패하여 마지막 "deny" 문은 효과가 없습니다. 따라서 사용자의 기타 정책 또는 문이 해당 사용자의 권한을 결정합니다. 이 문은 MFA로 로그인하지 않은 사용자가 나열된 작업 또는 이들 작업에 액세스할 수 있는 기타 문 또는 정책일 경우에만 수행할 수 있도록 합니다.

  `...IfExists` 키를 분실했을 경우 `Bool` 연산자의 `aws:MultiFactorAuthPresent` 버전은 조건이 true로 반환됩니다. 즉, 액세스 키와 같은 장기 자격 증명으로 API에 액세스하는 사용자는 비 IAM API 작업에 대한 액세스가 거부됩니다.

4. 작업이 완료되면 [Review policy]를 선택합니다.
5. 검토 페이지에서 정책 이름에 **`Force_MFA`**를 입력합니다. 정책 설명에 을 입력합니다.**`This policy allows users to manage their own passwords and MFA devices but nothing else`**

`unless they authenticate with MFA.`정책을 검토합니다.요약을 클릭하여 정책에 의해 부여된 권한을 확인한 다음정책 생성를 선택하여 작업을 저장합니다.

새로운 정책이 관리형 정책 목록에 나타나며 연결 준비가 완료됩니다.

사용자에 정책을 연결하려면(콘솔)

1. 탐색 창에서 사용자를 선택합니다.
2. 편집하려는 사용자의 이름(확인란 아님)을 선택합니다.
3. 권한 탭에서 권한 추가를 선택합니다.
4. Attach existing policies directly(기존 정책 직접 연결)를 선택합니다.
5. 검색 상자에 **`Force`**를 입력한 다음, 목록에서 Force_MFA 옆에 있는 확인란을 선택합니다. 다음을 선택합니다. 검토.
6. 변경 사항을 검토한 후 권한 추가를 선택합니다.

IAM 사용자에 대해 MFA 활성화

보안 강화를 위해 모든 IAM 사용자는 멀티 팩터 인증 (MFA) 을 구성하여 글로벌 액셀러레이터 리소스를 보호하는 것이 좋습니다. MFA는 사용자의 정규 로그인 자격 증명 외에도 AWS 지원 MFA 디바이스의 고유 인증을 제출하라고 요청함으로써 보안을 더욱 강화합니다. 가장 안전한 AWS MFA 디바이스는 U2F 보안 키입니다. 회사에 U2F 디바이스가 이미 있는 경우 AWS 에서 해당 디바이스를 활성화하는 것이 좋습니다. 그렇지 않으면 각 사용자에 대해 디바이스를 구입하고 해당 하드웨어가 도착할 때까지 기다려야 합니다. 자세한 내용은 단원을 참조하십시오.U2F 보안 키 활성화의IAM 사용 설명서.

U2F 디바이스가 아직 없는 경우 가상 MFA 디바이스를 활성화하여 저렴한 비용으로 빠르게 시작할 수 있습니다. 이렇게 하려면 기존 휴대폰 또는 다른 모바일 디바이스에 소프트웨어 앱이 설치되어 있어야 합니다. 디바이스가 동기화된 1회 암호 알고리즘에 따라 여섯 자리 숫자 코드를 생성합니다. AWS 에 로그인하면 디바이스에서 코드를 입력하라는 메시지가 표시됩니다. 사용자에게 할당된 각 가상 MFA 디바이스는 고유해야 합니다. 사용자는 다른 사용자의 가상 MFA 디바이스의 코드를 입력하여 인증할 수 없습니다. 가상 MFA 디바이스로 사용할 수 있도록 지원되는 몇 가지 앱의 목록은 멀티 팩터 인증 단원을 참조하십시오.

Note

IAM 사용자에 대해 MFA를 구성하려면 사용자의 가상 MFA 디바이스가 호스팅되는 모바일 디바이스에 대한 물리적 액세스가 필요합니다.

IAM 사용자에 대한 가상 MFA 디바이스를 활성화하려면 (콘솔)

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 이름 목록에서 원하는 MFA 사용자 이름을 선택합니다.
4. Security credentials(보안 자격 증명) 탭을 선택합니다. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA Device(할당된 MFA 디바이스) 마법사에서 Virtual MFA device(가상 MFA 디바이스 비활성화)를 선택한 후 계속을 선택합니다.

   IAM은 QR 코드 그래픽을 포함하여 가상 MFA 디바이스의 구성 정보를 생성 및 표시합니다. 그래픽은 QR 코드를 지원하지 않는 디바이스 상에서 수동 입력할 수 있는 '보안 구성 키'를 표시한 것입니다.
6. 가상 MFA 앱을 엽니다.

   가상 MFA 디바이스의 호스팅에 사용되는 앱 목록은 멀티 팩터 인증을 참조하십시오. 가상 MFA 앱이 다수의 계정(다수의 가상 MFA 디바이스)을 지원하는 경우 옵션을 선택하여 새로운 계정(새로운 가상 MFA 디바이스)을 생성합니다.

7. MFA 앱의 QR 코드 지원 여부를 결정한 후 다음 중 한 가지를 실행합니다.

   - 마법사에서 Show QR code(QT 코드 표시)를 선택한 다음 해당 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어 카메라 모양의 아이콘을 선택하거나 코드 스캔(Scan code)과 비슷한 옵션을 선택한 다음, 디바이스의 카메라를 사용하여 코드를 스캔합니다.
   - MFA 디바이스 관리 마법사에서 보안 키 표시를 선택한 다음 MFA 앱에 보안 키를 입력합니다.

   모든 작업을 마치면 가상 MFA 디바이스가 일회용 암호 생성을 시작합니다.
8. MFA 디바이스 관리 마법사의 MFA 코드 1 상자에 현재 가상 MFA 디바이스에 표시된 일회용 암호를 입력합니다. 디바이스가 새로운 일회용 암호를 생성할 때까지 최대 30초 기다립니다. 그런 다음 두 번째 일회용 암호를 MFA 코드 2 상자에 입력합니다. Assign MFA(MFA 할당)을 선택합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화할 수 있습니다. 자세한 내용은 단원을 참조하십시오.가상 및 하드웨어 MFA 디바이스 재동기화의IAM 사용 설명서.

   이제 AWS 에서 가상 MFA 디바이스를 사용할 준비가 끝났습니다.

AWS Global Accelerator 터의 보안 VPC 연결

AWS Global Accelerator 내부 Application Load Balancer 또는 Amazon EC2 인스턴스 엔드포인트를 추가하면 프라이빗 서브넷에서 VPC (가상 프라이빗 클라우드) 의 엔드포인트로 인터넷 트래픽이 직접 전송되도록 할 수 있습니다. 로드 밸런서 또는 EC2 인스턴스가 포함된 VPC인터넷 게이트웨이를 추가하여 VPC 가 인터넷 트래픽을 허용함을 나타냅니다. 그러나 로드 밸런서 또는 EC2 인스턴스에는 퍼블릭 IP 주소가 필요하지 않습니다. 또한 서브넷에 연결된 인터넷 게이트웨이 경로가 필요하지 않습니다.

이는 인터넷 트래픽이 VPC 인스턴스 또는 로드 밸런서로 흐르기 위해 퍼블릭 IP 주소와 인터넷 게이트웨이 경로가 모두 필요한 일반적인 인터넷 게이트웨이 사용 사례와는 다릅니다. 대상의 탄력적 네트워크 인터페이스가 퍼블릭 서브넷 (즉, 인터넷 게이트웨이 경로가 있는 서브넷) 에 있더라도 인터넷 트래픽에 글로벌 액셀러레이터를 사용하면 글로벌 액셀러레이터는 일반적인 인터넷 경로와 글로벌또한 가속기는 인터넷 게이트웨이가 아닌 글로벌 가속기를 통해 반환됩니다.

Note

퍼블릭 IP 주소를 사용하고 Amazon EC2 인스턴스에 퍼블릭 서브넷을 사용하는 것은 일반적이지는 않지만 이 주소를 사용하여 구성을 설정할 수도 있습니다. 보안 그룹은 글로벌 액셀러레이터로부터의 트래픽과 인스턴스 ENI에 할당된 퍼블릭 또는 엘라스틱 IP 주소를 포함하여 인스턴스에 도착하는 모든 트래픽에 적용됩니다. 글로벌 액셀러레이터에 의해서만 트래픽이 전송되도록 하려면 프라이빗 서브넷을 사용합니다.

네트워크 경계 문제를 고려하고 인터넷 액세스 관리와 관련된 IAM 권한을 구성할 때 이 정보를 염두에 두십시오. VPC 대한 인터넷 액세스 제어에 대한 자세한 내용은 를 참조하십시오.서비스 제어 정책 예제.

AWS Global Accelerator 에서 로깅

모니터링은 글로벌 액셀러레이터와 AWS 솔루션의 가용성 및 성능을 유지하는 데 중요한 부분입니다. 발생하는 다중 지점 실패를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분으로부터 모니터링 데이터를 수집해야 합니다. AWS 는 다음과 같이 글로벌 액셀러레이터 리소스 및 활동을 모니터링하고 잠재적 인시던트에 대응할 수 있는 몇 가지 도구를 제공합니다.

AWS Global Accelerator 흐름

서버 흐름 로그는 가속기를 통해 끝점으로 이동하는 트래픽에 대한 자세한 레코드를 제공합니다. 서버 흐름 로그는 많은 애플리케이션에 있어 유용합니다. 예를 들어 흐름 로그 정보는 보안 및 액세스 감사에 유용할 수 있습니다. 자세한 내용은 AWS Global Accelerator (p. 60) 섹션을 참조하세요.

Amazon CloudWatch 지표 및 경보

CloudWatch 를 사용하면 AWS에서 실행하는 AWS 리소스 및 애플리케이션을 실시간으로 모니터링할 수 있습니다. CloudWatch 는 사용자가 시간 경과에 따라 측정하는 변수인 지표를 수집하고 추적합니다. 특정 지표를 감시해 알림을 보내거나 일정 기간 동안 특정 임계값을 초과한 경우 모니터링 중인 리소스를 자동으로 변경하는 경보를 생성할 수 있습니다. 자세한 내용은 AWS Global Accelerator Amazon CloudWatch 사용 (p. 65) 섹션을 참조하세요.

AWS CloudTrail 로그

CloudTrail 은 글로벌 액셀러레이터에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공합니다. CloudTrail 은 글로벌 액셀러레이터 콘솔, 글로벌 액셀러레이터 API 호출 코드를 비롯한 글로벌 액셀러레이터 API에 대한 호출을 비롯한 모든 API 호출을 이벤트로 캡처합니다. 자세한 내용은 AWS CloudTrail 을 사용하여 AWS Global Accelerator API 호출 기록 (p. 70) 섹션을 참조하세요.

AWS Global Accelerator 규정 준수

타사 감사자는 여러 AWS 규정 준수 프로그램의 일환으로 AWS Global Accelerator cerator의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, HIPAA, GDPR, ISO 및 ENS High가 포함됩니다.

글로벌 액셀러레이터를 포함하여 특정 규정 준수 프로그램 범위에 속하는 AWS 서비스의 목록은 단원을 참조하십시오.규정 준수 프로그램 제공 AWS 범위 내 서비스 제공. 일반적인 내용은 AWS 규정 준수 프로그램을 참조하십시오.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 단원을 참조하십시오.AWS Artifact t에서 보고서 다운로드.

글로벌 액셀러레이터 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. AWS는 규정 준수에 도움이 되도록 다음 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS 환경을 배포하기 위한 단계를 제공합니다.
- HIPAA 보안 및 규정 준수 기술 백서 설계 – 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 만드는 방법을 설명합니다.
- AWS 규정 준수 리소스 – 이 워크북 및 안내서 모음은 귀사가 속한 업계 및 위치에 적용될 수 있습니다.
- 규칙을 사용하여 리소스 평가의AWS Config 개발자 안내서— AWS Config 서비스는 사용자의 리소스 구성이 내부 관례, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub – 이 AWS 제품으로 보안 업계 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되는 AWS 내 보안 상태에 대한 포괄적인 관점을 제공합니다.

AWS Global Accelerator 에서

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 지역에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하십시오.

글로벌 액셀러레이터는 AWS 글로벌 인프라를 지원할 뿐만 아니라 데이터 복원성을 지원하는 데 도움이 되는 다음과 같은 기능을 제공합니다.

- 네트워크 영역은 고유한 IP 서브넷에서 가속기에 대한 고정 IP 주소를 제공합니다. AWS 가용 영역과 마찬가지로 네트워크 영역은 자체 물리적 인프라 세트가 있는 격리된 단위입니다. 가속기를 구성하면 글로벌 가속기에서 두 개의 IPv4 주소를 할당합니다. 특정 클라이언트 네트워크에 의한 IP 주소 차단으로 인해 네트워크 영역의 IP 주소 하나를 사용할 수 없게 되거나 네트워크 중단으로 인해 클라이언트 응용 프로그램이 격리된 다른 네트워크 영역에서 정상 정적 IP 주소를 다시 시도할 수 있습니다.
- 글로벌 액셀러레이터는 모든 엔드포인트의 상태를 지속적으로 모니터링합니다. 활성 엔드포인트가 비정상이라고 판단되면 글로벌 액셀러레이터는 즉시 트래픽을 사용 가능한 다른 엔드포인트로 보내기 시작합니다. 이를 통해 AWS 에서 애플리케이션을 위한 고가용성 아키텍처를 생성할 수 있습니다.

AWS Global Accelerator

관리형 서비스인 AWS Global Accelerator 터는Amazon Web Services: 보안 프로세스 개요백서를 참조하십시오.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 글로벌 액셀러레이터에 액세스합니다. 클라이언트가 TLS(전송 계층 보안) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다. 또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Global Accelerator 할당량

AWS 계정에는 AWS Global Accelerator 와 관련된 특정 할당량 (제한이라고도 함) 이 있습니다.

Service Quotas 콘솔은 Global Accelerator 할당량에 대한 정보를 제공합니다. 기본 할당량을 보는 것 외에도, Service Quotas 콘솔을 사용하여 다음을 수행할 수 있습니다.요청 할당량 증가- 조정 가능한 할당량. 글로벌 액셀러레이터의 할당량 증가를 요청할 때는 미국 동부 (버지니아 북부) 에 있어야 합니다.

주제

일반 할당량

다음은 글로벌 액셀러레이터의 전체 할당량입니다.

엔터티	Quota
AWS 계정당 액셀러레이터	20 다음을 할 수 있습니다할당량 증가를 요청하려면.
액셀러레이터 당 리스너	10 다음을 할 수 있습니다할당량 증가를 요청하려면.
리스너당 포트 범위	10
끝점 그룹당 포트 재지정	10 다음을 할 수 있습니다할당량 증가를 요청하려면.

끝점 그룹당 끝점에 대한 할당량

다음은 끝점 그룹의 끝점 수에 적용되는 글로벌 가속기 할당량입니다.

엔터티	설명	Quota
엔드포인트 유형이 하나 이상 있는 엔드포인트 그룹	둘 이상의 끝점 유형을 포함하는 끝점 그룹의 끝점 수입니다.	10
애플리케이션 로드 밸런서만 있는 엔드포인트 그룹	Application Load Balancer 끝점만 포함하는 엔드포인트 그룹의 애플리케이션 로드 밸런서 수입니다.	10
네트워크 부하 분산 장치만 있는 끝점 그룹	Network Load Balancer 끝점만 포함하는 끝점 그룹의 네트워크 로드 밸런서 수입니다.	10

엔터티	설명	Quota
Amazon EC2 인스턴스만 있는 엔드포인트 그룹	EC2 인스턴스 엔드포인트만 포함된 엔드포인트 그룹의 EC2 인스턴스 수입니다.	10 다음을 할 수 있습니다할당량 증가를 요청하려면.
엘라스틱 IP 주소만 있는 엔드포인트 그룹	엘라스틱 IP 주소 끝점만 포함하는 끝점 그룹의 엘라스틱 IP 주소 수입니다.	10 다음을 할 수 있습니다할당량 증가를 요청하려면.
Amazon Virtual Private Cloud 서브넷만 있는 엔드포인트 그룹	서브넷 엔드포인트만 포함하는 엔드포인트 그룹의 Amazon VPC 서브넷 수입니다.	10 다음을 할 수 있습니다할당량 증가를 요청하려면.

관련 할당량

Global Accelerator에 할당량 외에도 액셀러레이터용 엔드포인트로 사용하는 리소스에 적용되는 할당량 또한 있습니다. 자세한 내용은 다음 섹션을 참조하세요.

- 탄력적 IP 주소 할당량의Amazon EC2 사용 설명서.
- Amazon EC2 Service 할당량의Amazon EC2 사용 설명서.
- Network Load Balancer에 대한 할당량의Network Load Balancer 사용 설명서.
- Application Load Balancer에 대한 할당량의Application Load Balancer 사용 설명서.
- Amazon VPC 할당량의Amazon VPC 사용 설명서.

AWS Global Accelerator

Global Accelerator 에 대해 자세히 알아보는 데 도움이 될 수 있습니다.

주제

AWS Global Accelerator

다음 표에는 이 서비스를 이용할 때 참조할 수 있는 관련 리소스가 나와 있습니다.

- AWS Global Accelerator- API 작업, 파라미터, 데이터 형식에 대한 전체 설명과 서비스가 반환하는 오류 목록을 제공합니다.
- AWS Global Accelerator- 기능 및 요금 정보를 비롯해 Global Accelerator 에 대한 정보를 얻을 수 있는 기본 웹 페이지입니다.
- 서비스 약관- 저작권 및 상표, 사용자 계정, 라이선스 및 사이트 액세스와 기타 주제에 대한 세부 정보.

지원 받기

글로벌 가속기에 대한 Support 여러 가지 형태로 제공됩니다.

- 토론 포럼— Global Accelerator 관련 기술적 질문을 논의할 수 있는 개발자를 위한 커뮤니티 기반 포럼입니다.
- AWS 지원 센터 - 이 사이트에서는 최근 지원 사례에 대한 정보와 AWS Trusted Advisor 및 상태 확인의 결과를 함께 제공합니다. 또한 토론 포럼, 기술 FAQ, 서비스 상태 대시보드에 대한 링크와 AWS 지원 계획에 대한 정보를 제공합니다.
- AWS Premium Support 정보 - 1:1 신속 대응 지원 채널을 통해 AWS Infrastructure Services에서 애플리케이션을 구축하고 실행할 수 있도록 지원하는 AWS Premium Support 관련 정보의 기본 웹 페이지입니다.
- 문의처 - 결제 또는 계정과 관련하여 문의할 수 있는 링크입니다. 기술적인 질문의 경우 토론 포럼이나 위의 지원 링크를 이용하십시오.

Amazon Web Services 블로그의 팁

AWS 블로그에는 AWS 서비스 사용에 도움이 되는 여러 게시물이 올라와 있습니다. 예를 들어 Global Accelerator 에 대한 다음 블로그 게시물을 참조하십시오.

- 가용성 및 성능을 위한 AWS Global Accelerator
- AWS Global Accelerator
- 아마존 아테네 및 Amazon QuickSight 를 사용하여 AWS Global Accelerator 흐름 로그 분석 및 시각화

AWS Global Accelerator 블로그의 전체 목록은 단원을 참조하십시오.AWS Global AcceleratorAWS 블로그 게시물의 네트워킹 및 콘텐츠 전송 범주에 있습니다.

문서 기록

다음 항목은 AWS Global Accelerator 설명서의 중요한 변경 사항을 설명합니다.

- API 버전: 최신
- 최신 설명서 업데이트: 2020년 12월 9일

변경 사항	설명	날짜
글로벌 액셀러레이터 기존 서비스 연결 역할에 대한 업데이트	글로벌 액셀러레이터에서 새로운 권한을 추가했습니다.`ec2:DescribeRegions`를 통해 글로벌 액셀러레이터가 오류를 진단하는 데 도움이 되는 AWS 리전 정보를 얻을 수 있습니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html 섹션을 참조하세요.	2021년 5월 7일
사용자 지정 라우팅 가속기 추가	글로벌 액셀러레이터는 새로운 유형의 액셀러레이터 사용자 지정 라우팅 가속기를 도입했습니다. 사용자 지정 라우팅 가속기는 사용자 지정 응용 프로그램 논리를 사용하여 한 명 이상의 사용자를 특정 대상 및 포트로 안내하는 동시에 글로벌 가속기의 성능 이점을 얻고자 하는 시나리오에 적합합니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html 섹션을 참조하세요.	2020년 12월 9일
포트 재정의 지원 추가	이제 글로벌 액셀러레이터는 트래픽을 엔드포인트로 라우팅하는 데 사용되는 수신기 포트 재정의를 지원하므로 트래픽을 엔드포인트의 특정 포트로 다시 라우팅할 수 있습니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html 섹션을 참조하세요.	2020년 10월 21일
는 두 개의 새로운 영역을 추가했습니다	이제 아프리카 (케이프타운) 및 유럽 (밀라노) 를 지원합니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html 섹션을 참조하세요.	2020년 5월 20일

변경 사항	설명	날짜
태그 지정 및 BYOIP	이 릴리스에서는 가속기에 태그를 추가하고 자체 IP 주소를 AWS Global Accelerator (BYOIP)로 가져오는 기능이 추가되었습니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html 및 https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html 섹션을 참조하세요.	2020년 2월 27일
보안 장 업데이트	규정 준수, 복원력 및 인프라 보안을 위한 컨텐츠가 추가되었습니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html 섹션을 참조하세요.	2019년 12월 20일
EC2 인스턴스 및 기본 DNS 이름 Support	AWS Global Accelerator 터는 이제 지원되는 AWS 리전에서 EC2 인스턴스 추가를 지원합니다. 또한 글로벌 가속기는 가속기의 고정 IP 주소에 매핑되는 기본 DNS 이름을 만듭니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html 및 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing 섹션을 참조하세요.	2019년 10월 29일
애플리케이션 로드 밸런서에 대한 클라이언트 IP 주소 보존	이제 AWS 글로벌 액셀러레이터가 지원되는 AWS 리전에서 애플리케이션 로드 밸런서에 대한 클라이언트 IP 주소를 보존하도록 선택할 수 있습니다. 자세한 내용은 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html 섹션을 참조하세요.	2019년 8월 28일
AWS Global Accelerator 서비스 출시	AWS Global Accelerator 개발자 안내서에서는 네트워크 계층 트래픽 관리자인 가속기를 설정하고 사용하는 방법에 대한 정보를 제공합니다. 이 안내서는 전 세계 사용자가 있는 인터넷 애플리케이션의 가용성과 성능을 향상시킵니다.	2018년 11월 26일

AWS 용어집

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.

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