AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

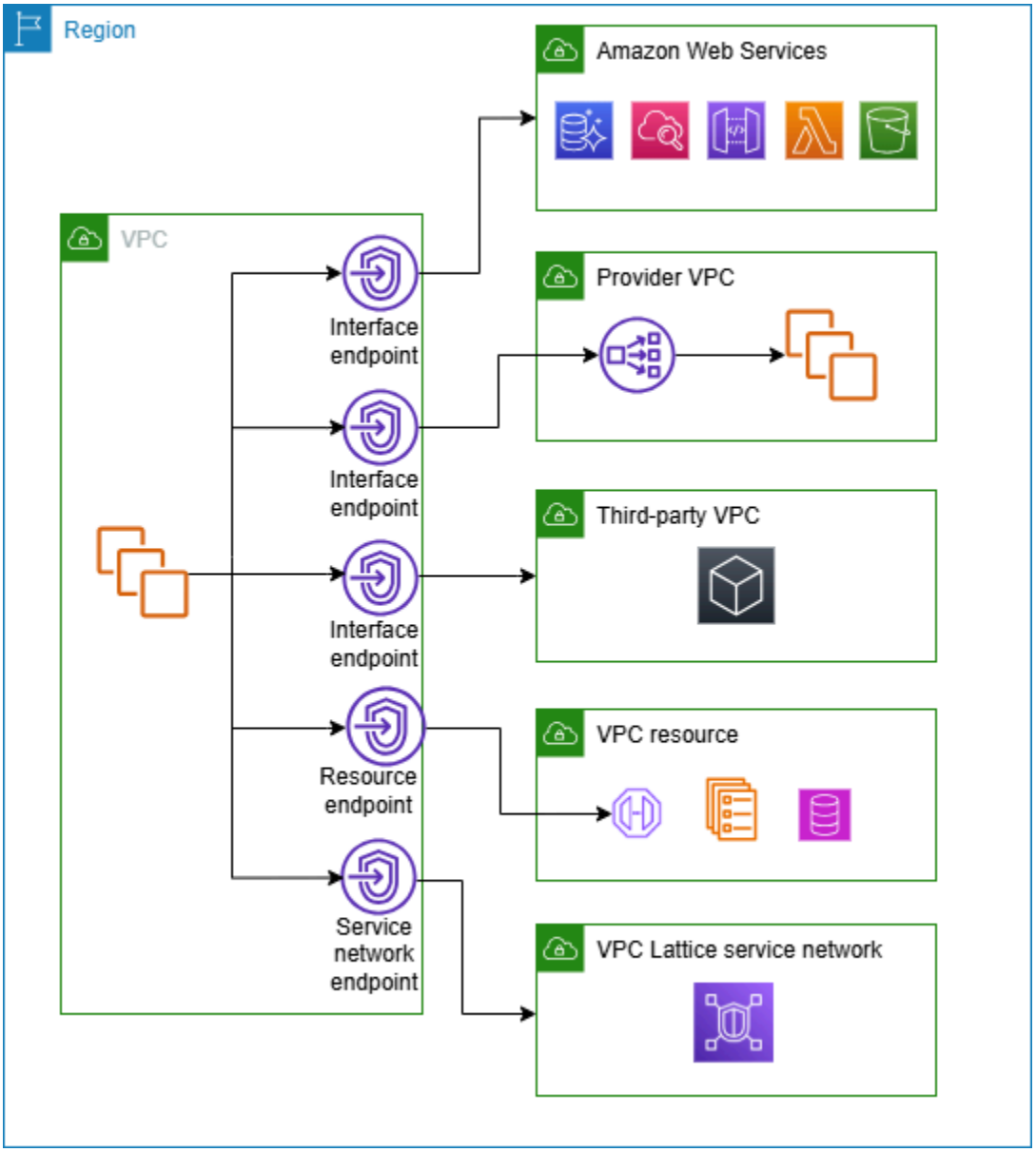
AWS PrivateLink란 무엇인가요?

AWS PrivateLink 는 VPC에 있는 것처럼 VPC를 서비스 및 리소스에 비공개로 연결하는 데 사용할 수 있는 가용성과 확장성이 뛰어난 기술입니다. 프라이빗 서브넷에서 서비스 또는 AWS Site-to-Site VPN 리소스와의 통신을 허용하기 위해 인터넷 게이트웨이, NAT 디바이스, 퍼블릭 IP 주소, Direct Connect 연결 또는 연결을 사용할 필요가 없습니다. 따라서 VPC에서 연결할 수 있는 특정 API 엔드포인트, 사이트, 서비스 및 리소스를 제어할 수 있습니다.

사용 사례

VPC 엔드포인트를 생성하여 VPC의 클라이언트를와 통합되는 서비스 및 리소스에 연결할 수 있습니다 AWS PrivateLink. 자체 VPC 엔드포인트 서비스를 생성하여 다른 AWS 고객이 사용할 수 있도록 할 수 있습니다. 자세한 내용은 the section called “개념” 단원을 참조하십시오.

다음 다이어그램에서 왼쪽의 VPC에는 프라이빗 서브넷 내 여러 Amazon EC2 인스턴스와 5개의 VPC 엔드포인트가 있으며, 이 VPC 엔드포인트는 3개의 인터페이스 VPC 엔드포인트, 하나의 리소스 VPC 엔드포인트, 그리고 하나의 서비스 네트워크 VPC 엔드포인트로 구성되어 있습니다. 첫 번째 인터페이스 VPC 엔드포인트는 AWS 서비스에 연결합니다. 두 번째 인터페이스 VPC 엔드포인트는 다른 AWS 계정에서 호스팅하는 서비스(VPC 엔드포인트 서비스)에 연결합니다. 세 번째 인터페이스 VPC 엔드포인트는 AWS Marketplace 파트너 서비스에 연결합니다. 리소스 VPC 엔드포인트는 데이터베이스에 연결합니다. 서비스 네트워크 VPC 엔드포인트는 서비스 네트워크에 연결합니다.



자세히 알아보기

- 개념
- AWS 서비스액세스
- SaaS 제품 액세스
- 가상 어플라이언스 액세스
- 서비스 공유

VPC 엔드포인트 작업

다음 중 하나를 사용하여 VPC 엔드포인트를 생성하고 액세스하고 관리할 수 있습니다.

- AWS Management Console - AWS PrivateLink 리소스에 액세스하는 데 사용할 수 있는 웹 인터페이스를 제공합니다. Amazon VPC 콘솔을 열고 엔드포인트 또는 엔드포인트 서비스를 선택합니다.
- AWS Command Line Interface (AWS CLI) - 다음을 AWS 서비스포함한 광범위한에 대한 명령을 제공합니다 AWS PrivateLink. 명령에 대한 자세한 내용은 명령 AWS PrivateLink참조의 ec2를 AWS CLI 참조하세요.
- CloudFormation - AWS 리소스를 설명하는 템플릿을 생성합니다. 템플릿을 사용하여 이러한 리소스를 하나의 단위로 프로비저닝하고 관리할 수 있습니다. 자세한 내용은 다음 AWS PrivateLink 리소스를 참조하세요.
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs- 언어별 APIs 제공합니다. SDK는 서명 계산, 요청 재시도 처리 및 오류 처리와 같은 많은 연결 세부 정보를 관리합니다. 자세한 내용은 AWS기반의 도구를 참조하세요.
- 쿼리 API — HTTPS 요청을 사용하여 호출하는 하위 수준의 API 작업을 제공합니다. 쿼리 API 사용은 Amazon VPC에 액세스하는 가장 직접적인 방법입니다. 하지만 이를 사용하려면 애플리케이션에서 요청에 서명할 해시 생성 및 오류 처리와 같은 하위 수준의 세부 정보를 처리해야 합니다. 자세한 내용은 Amazon EC2 API 참조의 AWS PrivateLink 작업을 참조하세요.

가격 책정

VPC 엔드포인트 요금에 대한 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

AWS PrivateLink 개념

Amazon VPC를 사용하면 논리적으로 분리된 가상 네트워크인 가상 프라이빗 클라우드(VPC)를 정의할 수 있습니다. 또한 VPC 내의 클라이언트가 해당 VPC 외부의 대상에 연결하도록 허용할 수 있습니다. 예를 들어 VPC에 인터넷 게이트웨이를 추가하여 인터넷 액세스를 허용하거나 VPN 연결을 추가하여 온프레미스 네트워크 액세스를 허용할 수 있습니다. 또는 VPC의 클라이언트가 VPC에서 직접 호

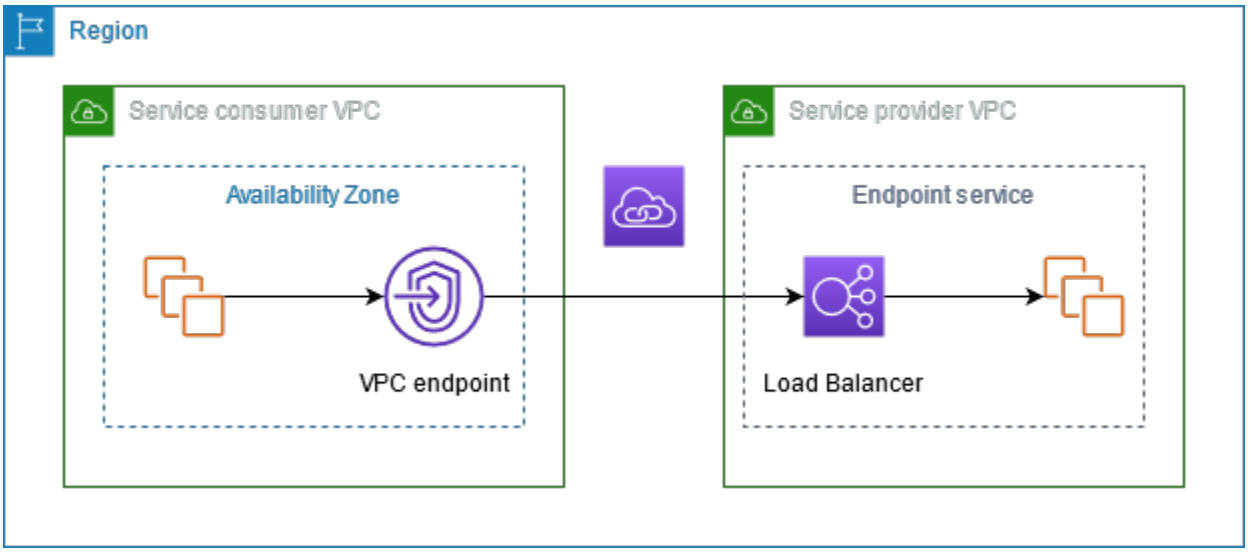
스팅된 것처럼 프라이빗 IP 주소를 사용하여 다른 VPCs의 서비스 및 리소스에 연결할 수 있도록 AWS PrivateLink 하려면를 사용합니다.

다음은 AWS PrivateLink사용을 시작하려면 알아야 하는 중요한 개념입니다.

내용

아키텍처 다이어그램

다음 다이어그램은 AWS PrivateLink 작동 방식에 대한 개략적인 개요를 제공합니다. 소비자는 VPC 엔드포인트를 생성하여 공급자가 호스팅하는 엔드포인트 서비스와 리소스에 연결합니다.



공급자

공급자와 관련된 개념을 이해합니다.

서비스 공급자

서비스 소유자가 서비스 공급자입니다. 서비스 제공업체에는 AWS AWS 파트너 등이 포함됩니다 AWS 계정. 서비스 공급자는 EC2 인스턴스와 같은 AWS 리소스를 사용하거나 온프레미스 서버를 사용하여 서비스를 호스팅할 수 있습니다.

리소스 공급자

데이터베이스 또는 Amazon EC2 인스턴스와 같은 리소스의 소유자가 리소스 공급자입니다. 리소스 공급자에는 AWS 서비스, AWS 파트너 및 기타 AWS 계정이 포함됩니다. 리소스 공급자는 VPC 또는 온프레미스에서 리소스를 호스팅할 수 있습니다.

개념

- 엔드포인트 서비스
- 서비스 이름
- 서비스 상태
- 리소스 구성
- 리소스 게이트웨이

엔드포인트 서비스

서비스 공급자는 서비스를 리전에서 사용할 수 있도록 하기 위해 엔드포인트 서비스를 생성합니다. 서비스 공급자는 엔드포인트 서비스를 생성할 때 로드 밸런서를 지정해야 합니다. 로드 밸런서는 서비스 소비자의 요청을 받아 서비스로 전달합니다.

기본적으로 엔드포인트 서비스는 서비스 소비자가 사용할 수 없습니다. 특정 AWS 보안 주체가 엔드포인트 서비스에 연결할 수 있도록 허용하는 권한을 추가해야 합니다.

서비스 이름

각 엔드포인트 서비스는 서비스 이름으로 식별됩니다. 서비스 소비자는 VPC 엔드포인트를 생성할 때 서비스 이름을 지정해야 합니다. 서비스 소비자는 서비스 이름을 쿼리할 수 있습니다 AWS 서비스. 서비스 공급자는 제공하는 서비스의 이름을 서비스 소비자와 공유해야 합니다.

서비스 상태

엔드포인트 서비스의 가능한 상태는 다음과 같습니다.

- 보류 중 - 엔드포인트 서비스를 생성하는 중입니다.
- 사용 가능 - 엔드포인트 서비스를 사용할 수 있습니다.
- 실패 - 엔드포인트 서비스를 생성할 수 없습니다.
- 삭제 중 - 서비스 공급자가 엔드포인트 서비스를 삭제했으며 삭제가 진행 중입니다.
- 삭제됨 - 엔드포인트 서비스가 삭제되었습니다.

리소스 구성

리소스 공급자는 리소스를 공유하기 위해 리소스 구성을 생성합니다. 리소스 구성은 데이터베이스와 같은 단일 리소스나 리소스 그룹을 나타내는 논리적 객체입니다. 리소스는 IP 주소, 도메인 이름 대상 또는 Amazon Relational Database Service(Amazon RDS) 데이터베이스일 수 있습니다.

다른 계정과 공유할 때 리소스 공급자는 다른 계정의 특정 보안 AWS 주체가 리소스 VPC 엔드포인트를 통해 리소스에 연결할 수 있도록 AWS Resource Access Manager (AWS RAM) 리소스 공유를 통해 리소스를 공유해야 합니다.

리소스 구성은 보안 주체가 서비스 네트워크 VPC 엔드포인트를 통해 연결하는 서비스 네트워크와 연결할 수 있습니다.

리소스 게이트웨이

리소스 게이트웨이는 리소스가 공유되는 VPC로 들어오는 진입 지점입니다. 공급자는 VPC에서 리소스를 공유하기 위해 리소스 게이트웨이를 생성합니다.

서비스 또는 리소스 소비자

서비스 또는 리소스의 사용자를 소비자라고 합니다. 소비자는 자신의 VPC 또는 온프레미스 환경에서 엔드포인트 서비스와 리소스에 액세스할 수 있습니다.

개념

- VPC 엔드포인트
- 엔드포인트 네트워크 인터페이스
- 엔드포인트 정책
- 엔드포인트 상태

VPC 엔드포인트

소비자는 VPC 엔드포인트를 생성하여 VPC를 엔드포인트 서비스나 리소스에 연결합니다. 소비자는 VPC 엔드포인트를 생성할 때 엔드포인트 서비스, 리소스 또는 서비스 네트워크를 지정해야 합니다. VPC 엔드포인트는 여러 유형이 있습니다. 필요한 VPC 엔드포인트 유형을 생성해야 합니다.

- `Interface` - TCP 또는 UDP 트래픽을 엔드포인트로 전송하는 인터페이스 엔드포인트를 생성합니다. 엔드포인트 서비스로 전송되는 트래픽은 DNS를 사용하여 확인됩니다.

- `GatewayLoadBalancer` - 프라이빗 IP 주소를 사용하여 가상 어플라이언스 플릿에 트래픽을 보내는 Gateway Load Balancer 엔드포인트를 생성합니다. 라우팅 테이블을 사용하여 VPC의 트래픽을 Gateway Load Balancer 엔드포인트로 라우팅합니다. Gateway Load Balancer는 트래픽을 가상 어플라이언스로 분산하며 수요에 맞게 확장될 수 있습니다.
- `Resource` - 공유 받았고 다른 VPC에 있는 리소스에 액세스하기 위해 리소스 엔드포인트를 생성합니다. 리소스 엔드포인트를 사용하면 데이터베이스, Amazon EC2 인스턴스, 애플리케이션 엔드포인트, 도메인 이름 대상 또는 다른 VPC의 프라이빗 서브넷이나 온프레미스 환경에 있을 수도 있는 IP 주소와 같은 리소스에 비공개로 안전하게 액세스할 수 있습니다. 리소스 엔드포인트는 로드 밸런서를 필요로 하지 않으며, 리소스에 직접 액세스할 수 있습니다.
- `Service network` - 생성했거나 다른 사용자로부터 공유받은 서비스 네트워크에 액세스하기 위해 서비스 네트워크 엔드포인트를 생성합니다. 단일 서비스 네트워크 엔드포인트를 사용하면 해당 서비스 네트워크에 연결된 여러 리소스 및 서비스에 비공개로 안전하게 액세스할 수 있습니다.

트래픽을 Amazon S3 또는 DynamoDB로 전송하는 게이트웨이 엔드포인트를 생성하는 다른 유형의 VPC 엔드포인트 `Gateway`이(가) 있습니다. 게이트웨이 엔드포인트는 다른 유형의 VPC 엔드포인트와 AWS PrivateLink달리를 사용하지 않습니다. 자세한 내용은 the section called “게이트웨이 엔드포인트” 단원을 참조하십시오.

엔드포인트 네트워크 인터페이스

엔드포인트 네트워크 인터페이스는 요청자가 관리하는 네트워크 인터페이스로, 엔드포인트 서비스, 리소스 또는 서비스 네트워크로 향하는 트래픽의 진입점 역할을 합니다. VPC 엔드포인트를 생성할 때 지정하는 각 서브넷에 대해 엔드포인트 네트워크 인터페이스가 서브넷에 생성됩니다.

VPC 엔드포인트가 IPv4를 지원하는 경우 해당 엔드포인트 네트워크 인터페이스에 IPv4 주소가 있습니다. VPC 엔드포인트가 IPv6를 지원하는 경우 해당 엔드포인트 네트워크 인터페이스에 IPv6 주소가 있습니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이(가) 활성화됩니다.

엔드포인트 정책

VPC 엔드포인트 정책은 VPC 엔드포인트에 연결할 수 있는 IAM 리소스 정책입니다. 이 정책에 따라 VPC 엔드포인트를 사용하여 엔드포인트 서비스에 액세스할 수 있는 보안 주체가 결정됩니다. 기본 VPC 엔드포인트 정책을 사용하면 VPC 엔드포인트를 통해 모든 리소스에 대해 모든 보안 주체의 모든 작업이 허용됩니다.

엔드포인트 상태

인터페이스 VPC 엔드포인트를 생성할 때 엔드포인트 서비스는 연결 요청을 수신합니다. 서비스 공급자는 이 요청을 수락하거나 거부할 수 있습니다. 서비스 공급자가 요청을 수락하면, 서비스 소비자는 VPC 엔드포인트가 사용 가능 상태가 된 후에 이를 사용할 수 있습니다.

VPC 엔드포인트의 가능한 상태는 다음과 같습니다.

- 수락 대기 중 – 연결 요청이 대기 중입니다. 요청을 수동으로 수락하는 경우의 초기 상태입니다.
- 대기 중 - 서비스 공급자가 연결 요청을 수락했습니다. 요청이 자동으로 수락되는 경우의 초기 상태입니다. 서비스 소비자가 VPC 엔드포인트를 수정하면 VPC 엔드포인트가 이 상태로 돌아갑니다.
- 사용 가능 - VPC 엔드포인트를 사용할 수 있습니다.
- 거부됨 – 서비스 공급자가 연결 요청을 거부했습니다. 서비스 공급자는 서비스를 사용할 수 있게 된 후 연결을 거부할 수도 있습니다.
- 만료됨 - 연결 요청이 만료되었습니다.
- 실패 - VPC 엔드포인트를 사용하도록 설정할 수 없습니다.
- 삭제 중 - 서비스 소비자가 VPC 엔드포인트를 삭제했으며 삭제가 진행 중입니다.
- 삭제됨 - VPC 엔드포인트가 삭제되었습니다.

AWS PrivateLink API는 카멜 사례를 사용하여 가능한 상태를 반환합니다.

AWS PrivateLink 연결

VPC의 트래픽은 VPC 엔드포인트와 엔드포인트 서비스 또는 리소스 간 연결을 사용하여 엔드포인트 서비스 또는 리소스로 전송됩니다. VPC 엔드포인트와 엔드포인트 서비스 또는 리소스 간 트래픽은 공개 인터넷을 통과하지 않고 AWS 네트워크 내에 머무릅니다.

서비스 공급자는 서비스 소비자가 엔드포인트 서비스에 액세스할 수 있도록 권한을 추가합니다. 서비스 소비자가 연결을 시작하고 서비스 공급자는 연결 요청을 수락하거나 거부합니다. 리소스 소유자 또는 서비스 네트워크 소유자는를 통해 리소스 구성 또는 서비스 네트워크를 소비자와 공유 AWS Resource Access Manager 하여 소비자가 리소스 또는 서비스 네트워크에 액세스할 수 있도록 합니다.

인터페이스 VPC 엔드포인트의 경우, 소비자는 엔드포인트 정책을 사용하여 어떤 IAM 보안 주체가 VPC 엔드포인트를 통해 엔드포인트 서비스나 리소스에 액세스할 수 있는지 제어할 수 있습니다.

프라이빗 호스팅 영역

호스팅 영역은 도메인 또는 하위 도메인에 대한 트래픽 라우팅 방식을 정의하는 DNS 레코드의 컨테이너입니다. 퍼블릭 호스팅 영역의 레코드에서는 트래픽을 인터넷에서 라우팅하는 방법을 지정합니다. 프라이빗 호스팅 영역의 레코드에서는 트래픽을 VPC에서 라우팅하는 방법을 지정합니다.

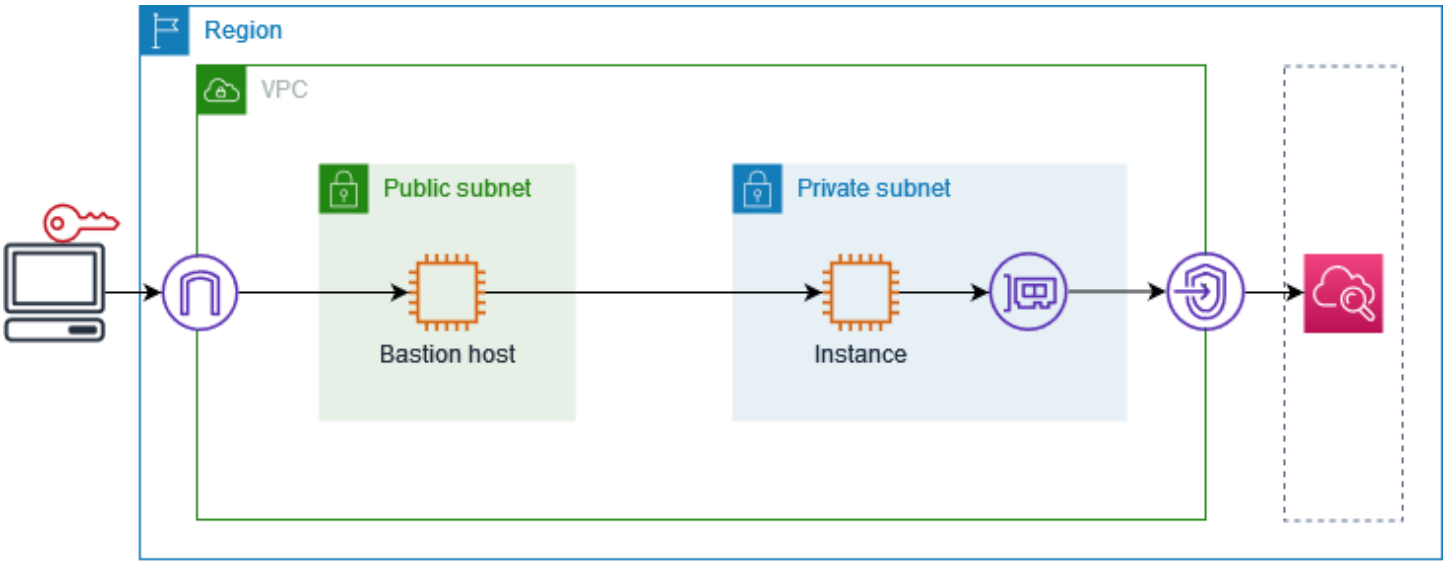
도메인 트래픽을 VPC 엔드포인트로 라우팅하도록 Amazon Route 53을 구성할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 VPC 엔드포인트로 트래픽 라우팅을 참조하세요.

Route 53을 사용하여 퍼블릭 웹 사이트와 기반 엔드포인트 서비스 모두에 동일한 도메인 이름을 사용하는 분할 영역 DNS를 구성할 수 있습니다 AWS PrivateLink. 소비자 VPC의 퍼블릭 호스트 이름에 대한 DNS 요청은 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인되지만, VPC 외부에서 들어오는 요청은 계속해서 퍼블릭 엔드포인트로 확인됩니다. 자세한 내용은 AWS PrivateLink 배포를 위한 트래픽 라우팅 및 페일오버 활성화에 대한 DNS 메커니즘을 참조하세요.

AWS PrivateLink 시작하기

이 자습서에서는 AWS PrivateLink를 사용하여 프라이빗 서브넷의 EC2 인스턴스에서 Amazon CloudWatch로 요청을 보내는 방법을 설명합니다.

다음 다이어그램은 이 시나리오의 개요를 제공합니다. 컴퓨터에서 프라이빗 서브넷의 인스턴스에 연결하려면 먼저 퍼블릭 서브넷의 Bastion 호스트에 연결해야 합니다. Bastion 호스트와 인스턴스 모두 동일한 키 페어를 사용해야 합니다. 프라이빗 키의 `.pem` 파일은 Bastion 호스트가 아닌 컴퓨터에 있으므로 SSH 키 전달을 사용하게 됩니다. 그러면 ssh 명령에서 `.pem` 파일을 지정하지 않고 Bastion 호스트에서 인스턴스에 연결할 수 있습니다. CloudWatch에 대한 VPC 엔드포인트를 설정하면 CloudWatch로 향하는 인스턴스의 트래픽이 엔드포인트 네트워크 인터페이스로 확인된 다음 VPC 엔드포인트를 사용하여 CloudWatch로 전송됩니다.



테스트 목적으로 하나의 가용 영역을 사용할 수 있습니다. 프로덕션 환경에서는 낮은 지연 시간과 높은 가용성을 위해 적어도 두 개의 가용 영역을 사용하는 것이 좋습니다.

Tasks

- 1단계: 서브넷이 있는 VPC 생성
- 2단계: 인스턴스 시작
- 3단계: CloudWatch 액세스 테스트
- 4단계: CloudWatch에 액세스하기 위한 VPC 엔드포인트 생성
- 5단계: VPC 엔드포인트 테스트
- 6단계: 정리

1단계: 서브넷이 있는 VPC 생성

다음 절차를 따라 퍼블릭 서브넷 및 프라이빗 서브넷이 있는 VPC를 생성합니다.

VPC를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. VPC 생성을 선택합니다.
3. Resources to create(생성할 리소스)에서 VPC and more(VPC 등)를 선택합니다.
4. Name tag auto-generation(이름 태그 자동 생성)에 VPC의 이름을 입력합니다.
5. 서브넷을 구성하려면 다음을 수행합니다.
   a. Number of Availability Zones(가용 영역 수)에서 필요에 따라 1 또는 2를 선택합니다.
   b. Number of public subnets(퍼블릭 서브넷 수)에서 가용 영역당 하나의 퍼블릭 서브넷이 있는지 확인합니다.
   c. Number of private subnets(프라이빗 서브넷 수)에서 가용 영역당 하나의 프라이빗 서브넷이 있는지 확인합니다.
6. VPC 생성을 선택합니다.

2단계: 인스턴스 시작

이전 단계에서 생성한 VPC를 사용하여 퍼블릭 서브넷에서 Bastion 호스트를 시작하고 프라이빗 서브넷에서 인스턴스를 시작합니다.

사전 조건

- .pem 형식을 사용하여 키 페어를 생성합니다. Bastion 호스트와 인스턴스를 모두 시작할 때 이 키 페어를 선택해야 합니다.
- 컴퓨터의 CIDR 블록으로부터의 인바운드 SSH 트래픽을 허용하는 Bastion 호스트의 보안 그룹을 생성합니다.
- Bastion 호스트의 보안 그룹으로부터의 인바운드 SSH 트래픽을 허용하는 인스턴스의 보안 그룹을 생성합니다.
- IAM 인스턴스 프로파일을 생성한 다음 CloudWatchReadOnlyAccess 정책을 연결합니다.

Bastion 호스트를 시작하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 인스턴스 시작을 선택합니다.
3. Name(이름)에 Bastion 호스트의 이름을 입력합니다.
4. 기본 이미지 및 인스턴스 유형을 유지합니다.
5. Key pair(키 페어)에서 키 페어를 선택합니다.
6. Network settings(네트워크 설정)에서 다음을 수행합니다.
   a. VPC에서 VPC를 선택합니다.
   b. Subnet(서브넷)에서 퍼블릭 서브넷을 선택합니다.
   c. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.
   d. Firewall(방화벽)에서 Select existing security group(기존 보안 그룹 선택)을 선택한 다음 Bastion 호스트의 보안 그룹을 선택합니다.
7. 인스턴스 시작을 선택합니다.

인스턴스를 시작하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 인스턴스 시작을 선택합니다.
3. Name(이름)에 인스턴스의 이름을 입력합니다.
4. 기본 이미지 및 인스턴스 유형을 유지합니다.
5. Key pair(키 페어)에서 키 페어를 선택합니다.
6. Network settings(네트워크 설정)에서 다음을 수행합니다.
   a. VPC에서 VPC를 선택합니다.
   b. Subnet(서브넷)에서 프라이빗 서브넷을 선택합니다.
   c. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Disable(비활성화)을 선택합니다.
   d. Firewall(방화벽)에서 Select existing security group(기존 보안 그룹 선택)을 선택한 다음 인스턴스의 보안 그룹을 선택합니다.
7. Advanced details(고급 세부 정보)를 확장합니다. IAM instance profile(IAM 인스턴스 프로파일)에서 IAM 인스턴스 프로파일을 선택합니다.
8. 인스턴스 시작을 선택합니다.

3단계: CloudWatch 액세스 테스트

다음 절차를 따라 인스턴스가 CloudWatch에 액세스할 수 없는지 확인합니다. CloudWatch의 읽기 전용 AWS CLI 명령을 사용하여 이 작업을 수행합니다.

CloudWatch 액세스를 테스트하려면

1. 컴퓨터에서 다음 명령을 사용하여 SSH 에이전트에 키 페어를 추가합니다. 여기서 *key.pem*은 .pem 파일의 이름입니다.

   ```
   ssh-add ./key.pem
   ```

   키 페어에 대한 권한이 너무 개방되어 있다는 오류 메시지가 표시되면 다음 명령을 실행한 다음 이전 명령을 다시 시도하세요.

   ```
   chmod 400 ./key.pem
   ```

2. 컴퓨터에서 Bastion 호스트에 연결합니다. `-A` 옵션, 인스턴스 사용자 이름(예:`ec2-user`) 및 Bastion 호스트의 퍼블릭 IP 주소를 지정해야 합니다.

   ```
   ssh -A ec2-user@bastion-public-ip-address
   ```

3. Bastion 호스트에서 인스턴스에 연결합니다. 인스턴스 사용자 이름(예: `ec2-user`) 및 인스턴스의 프라이빗 IP 주소를 지정해야 합니다.

   ```
   ssh ec2-user@instance-private-ip-address
   ```

4. 다음과 같이 인스턴스에서 CloudWatch list-metrics 명령을 실행합니다. `--region` 옵션에서 VPC를 생성한 리전을 지정합니다.

   ```
   aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
   ```

5. 몇 분 후 명령 시간이 초과됩니다. 이는 현재 VPC 구성으로는 인스턴스에서 CloudWatch에 액세스할 수 없음을 보여 줍니다.

   ```
   Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
   ```

6. 인스턴스와 연결 상태를 유지합니다. VPC 엔드포인트를 생성한 후 이 list-metrics 명령을 다시 시도합니다.

4단계: CloudWatch에 액세스하기 위한 VPC 엔드포인트 생성

다음 절차를 따라 CloudWatch에 연결하는 VPC 엔드포인트를 생성합니다.

전제 조건

CloudWatch에 대한 트래픽을 허용하는 VPC 엔드포인트의 보안 그룹을 생성합니다. 예를 들어 VPC CIDR 블록의 HTTPS 트래픽을 허용하는 규칙을 추가합니다.

CloudWatch에 대한 VPC 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Create endpoint(엔드포인트 생성)을 선택합니다.
4. Name tag(이름 태그)에 엔드포인트의 이름을 입력합니다.
5. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
6. Service(서비스)에서 com.amazonaws.***region***.monitoring을 선택합니다.
7. VPC에서 해당 VPC를 선택합니다.
8. Subnet(서브넷)에서 가용 영역을 선택한 다음 프라이빗 서브넷을 선택합니다.
9. Security group(보안 그룹)에서 VPC 엔드포인트의 보안 그룹을 선택합니다.
10. 정책(Policy)에서 모든 액세스(Full access)를 선택하여 VPC 엔드포인트를 통한 모든 리소스에 대한 모든 보안 주체의 모든 작업을 허용합니다.
11. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
12. Create endpoint(엔드포인트 생성)을 선택합니다. 초기 상태는 Pending(대기 중)입니다. 다음 단계로 이동하기 전에 상태가 Available(사용 가능)이 될 때까지 기다립니다. 몇 분 정도 소요될 수 있습니다.

5단계: VPC 엔드포인트 테스트

VPC 엔드포인트가 인스턴스에서 CloudWatch로 요청을 보내고 있는지 확인합니다.

VPC 엔드포인트를 테스트하려면

인스턴스에서 다음 명령을 실행합니다. `--region` 옵션에 VPC 엔드포인트를 생성한 리전을 지정합니다.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

결과가 비어 있는 응답이라도 응답을 받으면 AWS PrivateLink를 사용하여 CloudWatch에 연결된 것입니다.

`UnauthorizedOperation` 오류가 발생하는 경우 인스턴스에 CloudWatch에 대한 액세스를 허용하는 IAM 역할이 있는지 확인합니다.

요청 시간이 초과되면 다음을 확인합니다.

- 엔드포인트의 보안 그룹이 CloudWatch에 대한 트래픽을 허용합니다.
- `--region` 옵션이 VPC 엔드포인트를 생성한 리전을 지정합니다.

6단계: 정리

이 자습서용으로 생성한 Bastion 호스트 및 인스턴스가 더 이상 필요하지 않은 경우 종료할 수 있습니다.

인스턴스를 종료하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택합니다.
3. 테스트 인스턴스를 모두 선택하고 Instance state(인스턴스 상태), Terminate instance(인스턴스 종료)를 선택합니다.
4. 확인 메시지가 나타나면 종료를 선택합니다.

VPC 엔드포인트가 더 이상 필요하지 않으면 삭제할 수 있습니다.

VPC 엔드포인트를 삭제하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. VPC 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 나타나면 **`delete`**을 입력한 다음 삭제를 선택합니다.

를 AWS 서비스 통한 액세스 AWS PrivateLink

엔드포인트를 AWS 서비스 사용하여에 액세스합니다. 기본 서비스 엔드포인트는 퍼블릭 인터페이스이므로 트래픽이 VPC에서 AWS 서비스로 이동할 수 있도록 VPC에 인터넷 게이트웨이를 추가해야 합니다. 이 구성이 네트워크 보안 요구 사항과 호환되지 않는 경우 AWS PrivateLink 를 사용하여 인터넷 게이트웨이를 사용하지 않고 VPC에 있는 AWS 서비스 것처럼 VPC를에 연결할 수 있습니다.

VPC 엔드포인트를 AWS PrivateLink 사용하여와 통합 AWS 서비스 되는에 비공개로 액세스할 수 있습니다. 이 경우 인터넷 게이트웨이를 사용하지 않고도 애플리케이션 스택의 모든 계층을 구축하고 관리할 수 있습니다.

가격 책정

인터페이스 VPC 엔드포인트가 각 가용 영역에 프로비저닝되는 시간에 대해 시간당 요금이 청구됩니다. 또한 처리된 데이터의 GB당 요금이 청구됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

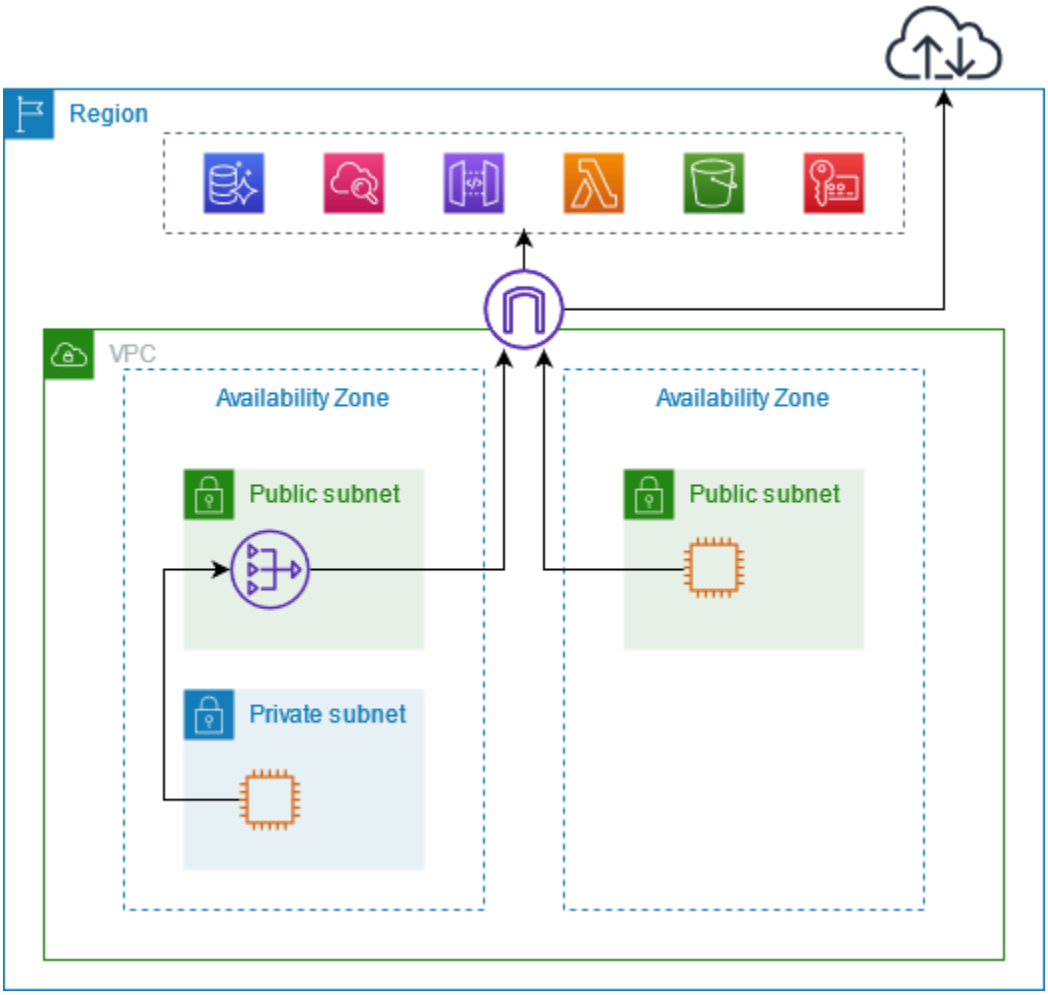
내용

개요

퍼블릭 서비스 엔드포인트를 AWS 서비스 통해에 액세스하거나를 AWS 서비스 사용하여 지원되는에 연결할 수 있습니다 AWS PrivateLink. 이 개요에서는 두 방법을 비교합니다.

퍼플릭 서비스 엔드포인트를 통한 액세스

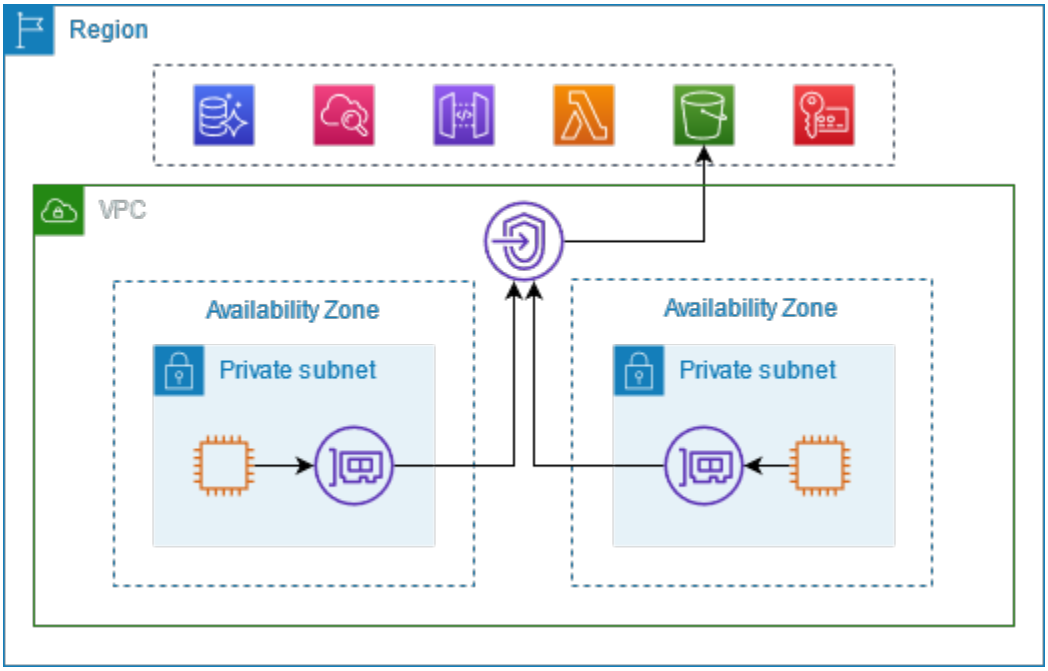
다음 다이어그램은 인스턴스가 퍼블릭 서비스 엔드포인트를 AWS 서비스 통해 액세스하는 방법을 보여줍니다. 퍼블릭 서브넷의 인스턴스 AWS 서비스 에서 로 가는 트래픽은 VPC의 인터넷 게이트웨이로 라우팅된 다음 로 라우팅됩니다 AWS 서비스. 프라이빗 서브넷의 인스턴스에서 AWS 서비스 로의 트래픽은 차례로 NAT 게이트웨이, VPC의 인터넷 게이트웨이, AWS 서비스로 라우팅됩니다. 이 트래픽은 인터넷 게이트웨이를 통과하지만 AWS 네트워크를 벗어나지 않습니다.



를 통해 연결 AWS PrivateLink

다음 다이어그램은 인스턴스가를 AWS 서비스 통해 액세스하는 방법을 보여줍니다 AWS PrivateLink. 먼저 네트워크 인터페이스를 AWS 서비스 사용하여 VPC의 서브넷과 간에 연결을 설정하는 인터페이

스 VPC 엔드포인트를 생성합니다. 로 향하는 트래픽 AWS 서비스 은 DNS를 사용하여 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인된 다음 VPC 엔드포인트와 간의 연결을 AWS 서비스 사용하여 로 전송됩니다 AWS 서비스.



AWS 서비스 연결 요청을 자동으로 수락합니다. 서비스에서는 VPC 엔드포인트를 통해 리소스에 대한 요청을 시작할 수 없습니다.

DNS 호스트 이름

대부분은 다음 구문을 가진 퍼블릭 리전 엔드포인트를 AWS 서비스 제공합니다.

```
protocol://service_code.region_code.amazonaws.com
```

예를 들어 us-east-2에서 Amazon CloudWatch의 퍼블릭 엔드포인트는 다음과 같습니다.

```
https://monitoring.us-east-2.amazonaws.com
```

를 사용하면 프라이빗 엔드포인트를 사용하여 서비스로 트래픽을 AWS PrivateLink전송합니다. 인터페이스 VPC 엔드포인트를 생성하면 VPC AWS 서비스 에서와 통신하는 데 사용할 수 있는 리전 및 영역 DNS 이름이 생성됩니다.

인터페이스 VPC 엔드포인트의 리전 DNS 이름은 구문이 다음과 같습니다.

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

영역 DNS 이름의 구문은 다음과 같습니다.

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

에 대한 인터페이스 VPC 엔드포인트를 생성할 때 프라이빗 DNS를 활성화 AWS 서비스할 수 있습니다. 프라이빗 DNS를 사용하면 인터페이스 VPC 엔드포인트를 통한 프라이빗 연결을 활용하면서 퍼블릭 엔드포인트의 DNS 이름을 사용하여 서비스에 계속 요청할 수 있습니다. 자세한 내용은 the section called “DNS 확인” 단원을 참조하십시오.

다음 describe-vpc-endpoints 명령은 인터페이스 엔드포인트의 DNS 항목을 표시합니다.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

다음은 프라이빗 DNS 이름이 활성화된 Amazon CloudWatch의 인터페이스 엔드포인트에 대한 출력 예입니다. 첫 번째 항목은 프라이빗 리전 엔드포인트입니다. 다음 세 개 항목은 프라이빗 영역 엔드포인트입니다. 마지막 항목은 숨겨진 프라이빗 호스팅 영역의 엔드포인트로, 퍼블릭 엔드포인트에 대한 요청을 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인합니다.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
```

```
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

DNS 확인

인터페이스 VPC 엔드포인트에 대해 생성되는 DNS 레코드는 퍼블릭입니다. 따라서 해당 DNS 이름은 공개적으로 확인할 수 있습니다. 하지만 VPC 외부의 DNS 요청은 여전히 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소를 반환하므로 VPC에 액세스할 수 없는 경우 이러한 IP 주소를 사용하여 엔드포인트 서비스에 액세스할 수 없습니다.

프라이빗 DNS

인터페이스 VPC 엔드포인트에 대해 프라이빗 DNS를 활성화하고 VPC에 DNS 호스트 이름과 DNS 확인이 모두 활성화된 경우 숨겨진 AWS관리형 프라이빗 호스팅 영역이 생성됩니다. 호스팅 영역에는 VPC에 있는 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인되는 서비스에 대한 기본 DNS 이름의 레코드 세트가 포함됩니다. 따라서 퍼블릭 리전 엔드포인트를 AWS 서비스 사용하여에 요청을 보내는 기존 애플리케이션이 있는 경우 이제 해당 애플리케이션을 변경할 필요 없이 해당 요청이 엔드포인트 네트워크 인터페이스를 통과합니다.

AWS 서비스용 VPC 엔드포인트에 프라이빗 DNS 이름을 사용하는 것이 좋습니다. 이렇게 하면 AWS SDK를 통한 요청과 같이 퍼블릭 서비스 엔드포인트를 사용하는 요청이 VPC 엔드포인트로 확인됩니다.

Amazon은 Route 53 Resolver라고 하는 VPC용 DNS 서버를 제공합니다. Route 53 Resolver는 프라이빗 호스팅 영역의 로컬 VPC 도메인 이름 및 레코드를 자동으로 확인합니다. 하지만 VPC 외부에서는 Route 53 Resolver를 사용할 수 없습니다. 온프레미스 네트워크에서 VPC 엔드포인트에 액세스하려는 경우 Route 53 Resolver 엔드포인트 및 Resolver 규칙을 사용할 수 있습니다. 자세한 내용은 AWS PrivateLink 및 AWS Transit Gateway 와 통합을 참조하세요 Amazon Route 53 Resolver.

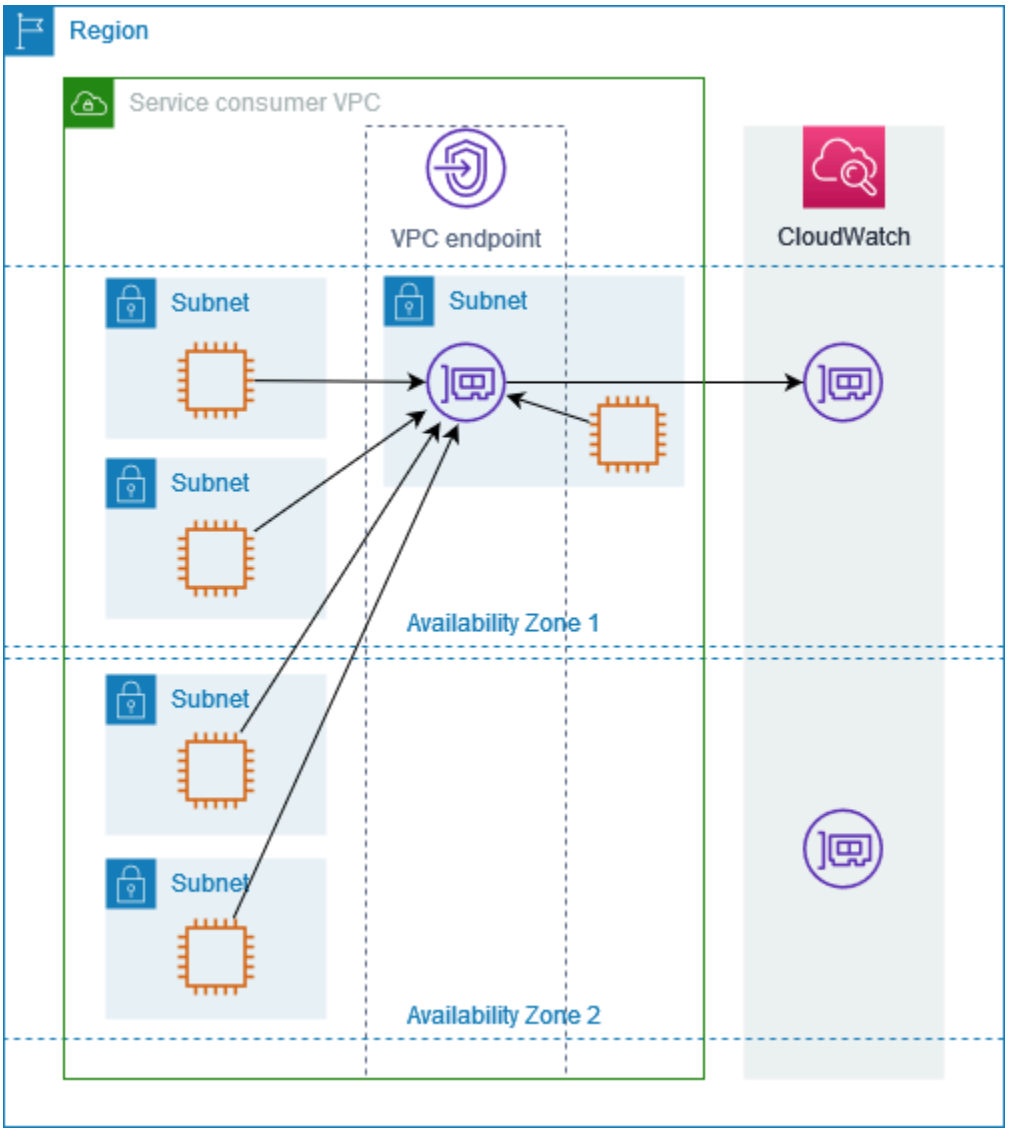
서브넷 및 가용 영역

가용 영역당 1개의 서브넷으로 VPC 엔드포인트를 구성할 수 있습니다. 서브넷의 VPC 엔드포인트에 대한 엔드포인트 네트워크 인터페이스가 생성됩니다. VPC 엔드포인트의 IP 주소 유형에 따라 서브넷의 각 엔드포인트 네트워크 인터페이스에 IP 주소가 할당됩니다. 엔드포인트 네트워크 인터페이스의 IP 주소는 VPC 엔드포인트의 수명 기간 동안 변경되지 않습니다.

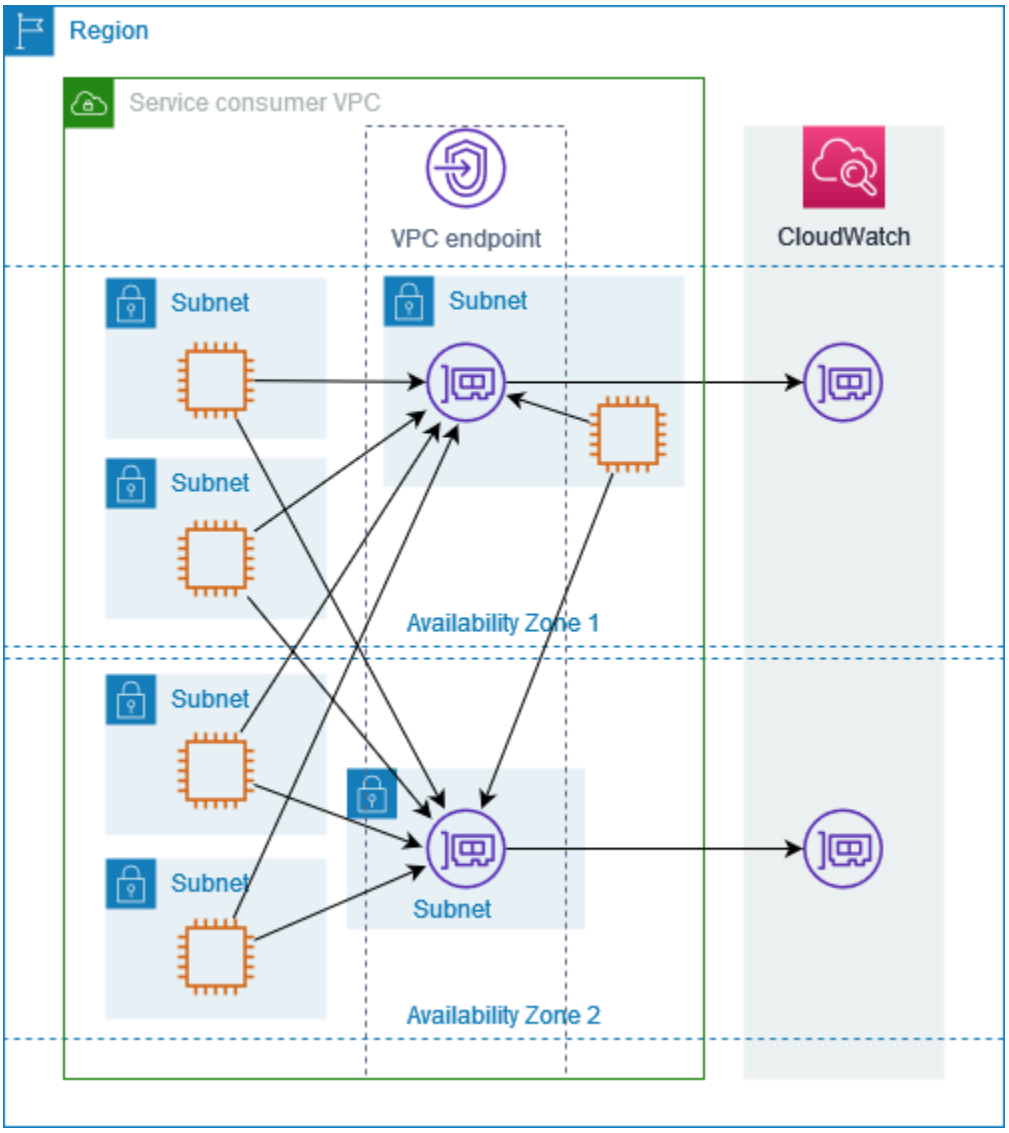
프로덕션 환경에서는 고가용성 및 복원력을 위해 다음과 같이 진행하는 것이 좋습니다.

- VPC 엔드포인트당 최소 두 개의 가용 영역을 구성하고 이러한 가용 영역에서 AWS 서비스 에 액세스해야 하는 리소스를 배포 AWS 합니다.
- VPC 엔드포인트의 프라이빗 DNS 이름을 구성합니다.
- 퍼블릭 엔드포인트라고도 하는 리전 DNS 이름을 AWS 서비스 사용하여에 액세스합니다.

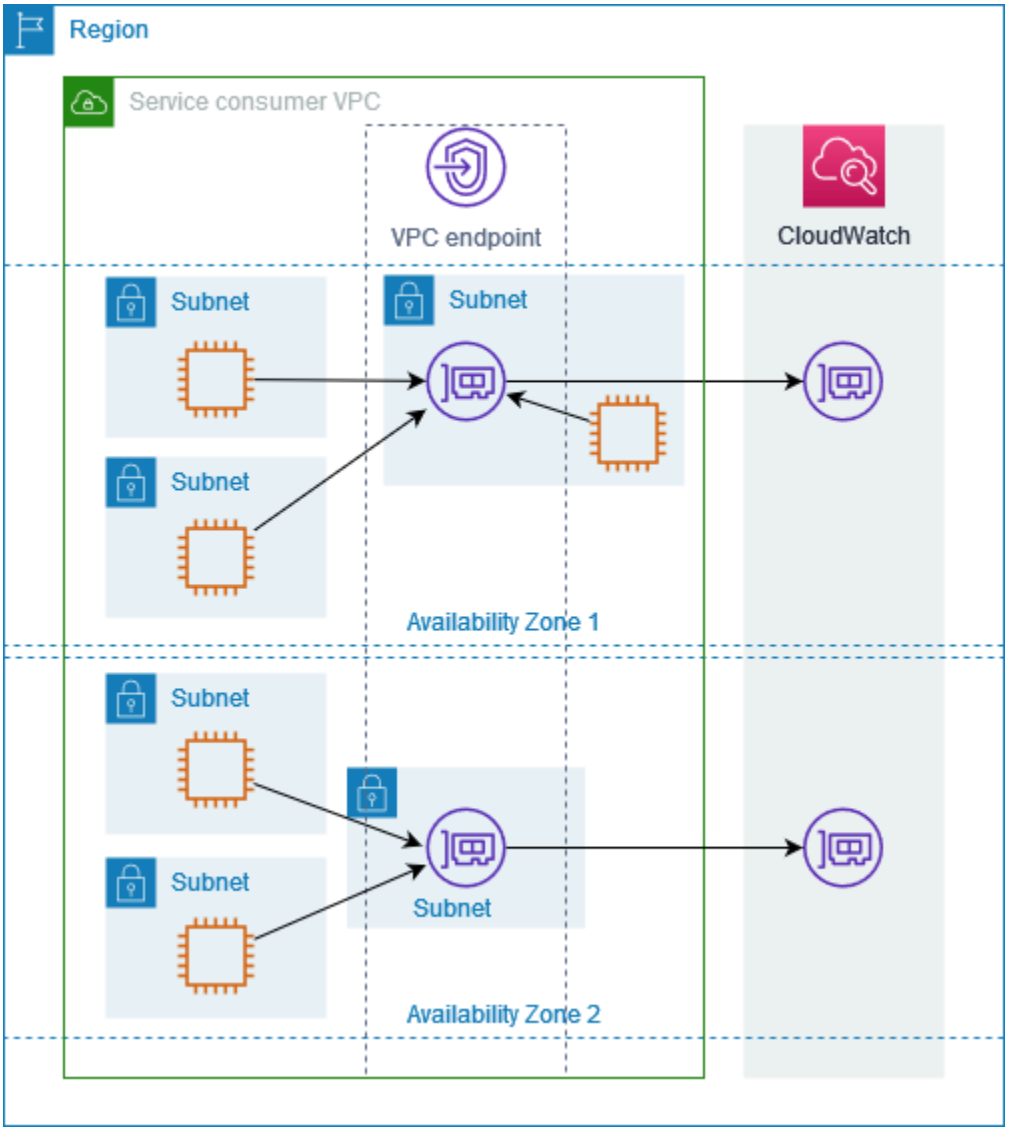
다음 다이어그램에서는 1개의 가용 영역에 엔드포인트 네트워크 인터페이스가 있는 Amazon CloudWatch용 VPC 엔드포인트를 보여줍니다. VPC의 서브넷에 있는 리소스에서 퍼블릭 엔드포인트를 사용하여 Amazon CloudWatch에 액세스하면 엔드포인트 네트워크 인터페이스의 IP 주소로 트래픽이 확인됩니다. 여기에는 다른 가용 영역에 있는 서브넷의 트래픽도 포함됩니다. 그러나 가용 영역 1이 손상되면 가용 영역 2의 리소스의 Amazon CloudWatch 액세스 권한이 손실됩니다.



다음 다이어그램에서는 2개의 가용 영역에 엔드포인트 네트워크 인터페이스가 있는 Amazon CloudWatch용 VPC 엔드포인트를 보여줍니다. VPC의 서브넷에 있는 리소스에서 퍼블릭 엔드포인트를 사용하여 Amazon CloudWatch에 액세스하면 두 가지를 번갈아 사용하는 라운드 로빈 알고리즘을 통해 정상 엔드포인트 네트워크 인터페이스가 선택됩니다. 그런 다음에 선택된 엔드포인트 네트워크 인터페이스의 IP 주소로 트래픽이 확인됩니다.



사용 사례에 더 적합한 경우 동일한 가용 영역의 엔드포인트 네트워크 인터페이스를 사용하여 리소스에서 AWS 서비스 로 트래픽을 보낼 수 있습니다. 이렇게 하려면 엔드포인트 네트워크 인터페이스의 프라이빗 영역별 엔드포인트 또는 IP 주소를 사용하세요.



IP 주소 유형

AWS 서비스 는 퍼블릭 엔드포인트를 통해 IPv6를 지원하지 않더라도 프라이빗 엔드포인트를 통해 IPv6를 지원할 수 있습니다. IPv6를 지원하는 엔드포인트는 AAAA 레코드를 사용하여 DNS 쿼리에 응답할 수 있습니다.

인터페이스 엔드포인트에 대해 IPv6를 활성화하기 위한 요구 사항

- 는 IPv6를 통해 서비스 엔드포인트를 사용할 수 있도록 해야 AWS 서비스 합니다. 자세한 내용은 the section called “IPv6 지원 보기” 단원을 참조하십시오.
- 인터페이스 엔드포인트의 IP 주소 유형이 여기에 설명된 대로 인터페이스 엔드포인트의 서브넷과 호환되어야 합니다.

- IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.
- IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
- 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

인터페이스 VPC 엔드포인트가 IPv4를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv4 주소가 있습니다. 인터페이스 VPC 엔드포인트가 IPv6를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv6 주소가 있습니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이 활성화됩니다.

DNS 레코드 IP 유형

IP 주소 유형에 따라 VPC 엔드포인트를 호출할 때 AWS 서비스는 A 레코드, AAAA 레코드 또는 A 레코드와 AAAA 레코드를 모두 반환할 수 있습니다. DNS 레코드 IP 유형을 수정하여 AWS 서비스가 반환하는 레코드 유형을 사용자 지정할 수 있습니다. 다음 표에는 지원되는 DNS 레코드 IP 유형과 반환된 레코드 유형이 나와 있습니다.

DNS 레코드 IP 유형	반환된 레코드 유형
IPv4	A
IPv6	AAAA
듀얼 스택	A 및 AAAA

기본적으로 DNS 레코드 유형은 IP 주소 유형과 동일합니다. 다른 DNS 레코드 IP 유형을 선택할 수도 있지만, 엔드포인트 서비스에 호환되는 IP 주소 유형을 사용해야 합니다. 다음 표는 인터페이스 엔드포인트의 각 IP 주소 유형에 대해 지원되는 DNS 레코드 IP 유형을 보여줍니다.

IP 주소 유형	지원되는 DNS 레코드 IP 유형
IPv4	IPv4

IP 주소 유형	지원되는 DNS 레코드 IP 유형
IPv6	IPv6
듀얼 스택	듀얼 스택*, IPv4, IPv6, 서비스 정의형

* 기본 DNS 레코드 IP 유형을 나타냅니다.

서비스 정의형 DNS 레코드 IP 유형은 호출하는 서비스 엔드포인트에 따라 DNS 레코드를 반환합니다. 서비스 정의형 DNS 레코드 IP 유형을 사용하는 경우, 서비스가 다양한 서비스 엔드포인트에서의 호출을 처리할 수 있는지 확인해야 합니다. 인터페이스 엔드포인트에서 지원하는 DNS 레코드를 보려면에서 VPC 엔드포인트의 DNS 이름을 참조 AWS Management Console하거나 DescribeVpcEndpoints를 사용합니다.

DNS 레코드 IP 유형의 동작은 게이트웨이 엔드포인트의 경우 다릅니다. 자세한 내용은 게이트웨이 엔드포인트의 DNS 레코드 IP 유형을 참조하세요.

AWS 서비스 와 통합되는 AWS PrivateLink

다음은와 AWS 서비스 통합됩니다 AWS PrivateLink. VPC 엔드포인트를 생성하면 이러한 서비스에 비공개로 연결하여 자체 VPC에서 실행 중인 것처럼 서비스를 이용할 수 있습니다.

AWS 서비스 열에서 링크를 선택하면와 통합되는 서비스에 대한 설명서를 볼 수 있습니다 AWS PrivateLink. 서비스 이름 열에는 인터페이스 VPC 엔드포인트를 생성할 때 지정하는 서비스 이름을 포함하거나, 서비스가 해당 엔드포인트를 관리함을 가리킵니다.

AWS 서비스	서비스 이름
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
	com.amazonaws.*region*.apigateway
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfig-fips
	com.amazonaws.*region*.appconfigdata

AWS 서비스	서비스 이름
	com.amazonaws.*region*.appconfigdata-fips
AWS App Mesh	com.amazonaws.*region*.appmesh
	com.amazonaws.*region*.appmesh-envoy-management
AWS 앱 실행기	com.amazonaws.*region*.apprunner
AWS App Runner 서비스	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS Application Discovery Service	com.amazonaws.*region*.discovery
	com.amazonaws.*region*.arsenal-discovery
AWS 애플리케이션 마이그레이션 서비스	com.amazonaws.*region*.mgn
Amazon WorkSpaces Applications	com.amazonaws.*region*.appstream.api
	com.amazonaws.*region*.appstream.streaming
AWS AppSync	com.amazonaws.*region*.appsync-api
Amazon Athena	com.amazonaws.*region*.athena
AWS Audit Manager	com.amazonaws.*region*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
	com.amazonaws.*region*.rds-fips
Amazon Aurora DSQL	com.amazonaws.*region*.dsql
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS B2B Data Interchange	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup

AWS 서비스	서비스 이름
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*region*.bedrock
	com.amazonaws.*region*.bedrock-agent
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-data-automation
	com.amazonaws.*region*.bedrock-data-automation-fips
	com.amazonaws.*region*.bedrock-data-automation-runtime
	com.amazonaws.*region*.bedrock-data-automation-runtime-fips
	com.amazonaws.*region*.bedrock-runtime
AWS 결제 및 비용 관리	com.amazonaws.*region*.billing
	com.amazonaws.*region*.freetier
	com.amazonaws.*region*.tax
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.braket
AWS Certificate Manager	com.amazonaws.*region*.acm
	com.amazonaws.*region*.acm-fips
AWS 클린 룸	com.amazonaws.*region*.cleanrooms
	com.amazonaws.*region*.cleanrooms-fips

AWS 서비스	서비스 이름
AWS Clean Rooms ML	com.amazonaws.*region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
	com.amazonaws.*region*.cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
AWS CloudHSM	com.amazonaws.*region*.cloudhsmv2
AWS Cloud Map	com.amazonaws.*region*.servicediscovery
	com.amazonaws.*region*.servicediscovery-fips
	com.amazonaws.*region*.data-servicediscovery
	com.amazonaws.*region*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*.cloudtrail
AWS 클라우드 WAN	com.amazonaws.*region*.networkmanager
Amazon CloudWatch	com.amazonaws.*region*.application-signals
	com.amazonaws.*region*.applicationinsights
	com.amazonaws.*region*.internetmonitor
	com.amazonaws.*region*.internetmonitor-fips
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.networkflowmonitor

AWS 서비스	서비스 이름
	com.amazonaws.*region*.networkflowmonitorreports
	com.amazonaws.*region*.networkmonitor
	com.amazonaws.*region*.observabilityadmin
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics
	com.amazonaws.*region*.synthetics-fips
	com.amazonaws.*region*.oam
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws.*region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws.*region*.codeconnections.api
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy

AWS 서비스	서비스 이름
	amazonaws*region*.codedeploy-commands-secure
	com.amazonaws.*region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws.*region*.codeguru-profiler
Amazon CodeGuru Reviewer	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Compute Optimizer	com.amazonaws.*region*.compute-optimizer
AWS Config	com.amazonaws.*region*.config
	com.amazonaws.*region*.config-fips
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws.*region*.cases
	com.amazonaws.*region*.connect-campaigns
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
AWS 제어 기능 카탈로그	com.amazonaws.*region*.controlcatalog
AWS Cost Explorer	com.amazonaws.*region*.ce
AWS Cost Optimization Hub	com.amazonaws.*region*.cost-optimization-hub

AWS 서비스	서비스 이름
AWS Control Tower	com.amazonaws.*region*.controltower
	com.amazonaws.*region*.controltower-fips
AWS Data Exchange	com.amazonaws.*region*.dataexchange
AWS Data Exports	aws.api.*region*.bcm-data-exports
	com.amazonaws.*region*.bcm-pricing-calculator
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
Amazon Data Lifecycle Manager	com.amazonaws.*region*.dlm
	com.amazonaws.*region*.dlm-fips
AWS Database Migration Service	com.amazonaws.*region*.dms
	com.amazonaws.*region*.dms-fips
AWS DataSync	com.amazonaws.*region*.datasync
Amazon DataZone	com.amazonaws.*region*.datazone
	com.amazonaws.*region*.datazone-fips
AWS Deadline Cloud	com.amazonaws.*region*.deadline.management
	com.amazonaws.*region*.deadline.scheduling
Amazon Detective	com.amazonaws.*region*.detective
	com.amazonaws.*region*.detective-fips
Amazon DevOps Guru	com.amazonaws.*region*.devops-guru
AWS Direct Connect	com.amazonaws.*region*.directconnect
	com.amazonaws.*region*.directconnect-fips

AWS 서비스	서비스 이름
AWS Directory Service	com.amazonaws.*region*.ds
	com.amazonaws.*region*.ds-data
	com.amazonaws.*region*.ds-data-fips
Amazon DocumentDB	com.amazonaws.*region*.rds
Amazon DynamoDB	com.amazonaws.*region*.dynamodb
	com.amazonaws.*region*.dynamodb-fips
	com.amazonaws.*region*.dynamodb-streams
Amazon EBS 다이렉트 API	com.amazonaws.*region*.ebs
	com.amazonaws.*region*.ebs-fips
Amazon EC2	com.amazonaws.*region*.ec2
	com.amazonaws.*region*.ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
	com.amazonaws.*region*.autoscaling-fips
EC2 Image Builder	com.amazonaws.*region*.imagebuilder
Amazon ECR	com.amazonaws.*region*.ecr.api
	com.amazonaws.*region*.ecr.dkr
Amazon ECS	com.amazonaws.*region*.ecs
	com.amazonaws.*region*.ecs-agent
	com.amazonaws.*region*.ecs-telemetry
Amazon EKS	com.amazonaws.*region*.eks

AWS 서비스	서비스 이름
	com.amazonaws.*region*.eks-auth
	com.amazonaws.*region*.eks-fips
	com.amazonaws.*region*.eks-proxy
AWS Elastic Beanstalk	com.amazonaws.*region*.elasticbeanstalk
	com.amazonaws.*region*.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.*region*.drs
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
	com.amazonaws.*region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon Elastic VMware Service	com.amazonaws.*region*.evs
	com.amazonaws.*region*.evs-fips
Amazon ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
AWS Elemental MediaConvert	com.amazonaws.*region*.mediaconvert
	com.amazonaws.*region*.mediaconvert-fips
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
	com.amazonaws.*region*.elasticmapreduce-fips
Amazon EMR on EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless

AWS 서비스	서비스 이름
	com.amazonaws.*region*.emr-serverless-services.livy
	com.amazonaws.*region*.emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws.*region*.emrwal.prod
AWS 최종 사용자 메시징 소셜	com.amazonaws.*region*.social-messaging
	com.amazonaws.*region*.social-messaging-fips
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
	com.amazonaws.*region*.entityresolution-fips
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws.*region*.events-fips
	com.amazonaws.*region*.pipes
	com.amazonaws.*region*.pipes-data
	com.amazonaws.*region*.pipes-fips
	com.amazonaws.*region*.schemas
Amazon EventBridge Scheduler	com.amazonaws.*region*.scheduler
AWS Fault Injection Service	com.amazonaws.*region*.fis
	com.amazonaws.*region*.fis-fips
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
AWS Firewall Manager	com.amazonaws.*region*.fms
	com.amazonaws.*region*.fms-fips

AWS 서비스	서비스 이름
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips
Amazon GameLift Servers	com.amazonaws.*region*.gamelift
Amazon GameLift Streams	com.amazonaws.*region*.gameliftstreams
Transit Gateway용 AWS 글로벌 네트워크	com.amazonaws.*region*.networkmanager
AWS Glue	com.amazonaws.*region*.glue
	com.amazonaws.*region*.glue.dashboard
AWS Glue DataBrew	com.amazonaws.*region*.databrew
	com.amazonaws.*region*.databrew-fips
Amazon Managed Grafana	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
	com.amazonaws.*region*.groundstation-fips
Amazon GuardDuty	com.amazonaws.*region*.guardduty
	com.amazonaws.*region*.guardduty-data

AWS 서비스	서비스 이름
	com.amazonaws.*region*.guardduty-data-fips
	com.amazonaws.*region*.guardduty-fips
AWS HealthImaging	com.amazonaws.*region*.dicom-medical-imaging
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws.*region*.analytics-omics-fips
	com.amazonaws.*region*.control-storage-omics
	com.amazonaws.*region*.control-storage-omics-fips
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.tags-omics-fips
	com.amazonaws.*region*.workflows-omics
	com.amazonaws.*region*.workflows-omics-fips
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAM Access Analyzer	com.amazonaws.*region*.access-analyzer
	com.amazonaws.*region*.access-analyzer-fips
IAM Identity Center	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere

AWS 서비스	서비스 이름
	com.amazonaws.*region*.rolesanywhere-fips
Amazon Inspector –	com.amazonaws.*region*.inspector2
	com.amazonaws.*region*.inspector2-fips
	com.amazonaws.*region*.inspector-scan
	com.amazonaws.*region*.inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws.*region*.ivs.contribute
AWS IoT Core	com.amazonaws.*region*.iot.api
	com.amazonaws.*region*.iot-fips.api
	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials
AWS IoT Device Management 보안 터널링	com.amazonaws.*region*.iot.tunneling.api
	com.amazonaws.*region*.iot-fips.tunneling.api
	com.amazonaws.*region*.iot.tunneling.data
	com.amazonaws.*region*.iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws.*region*.deviceadvisor.iot
에 대한 관리형 통합 AWS IoT Device Management	com.amazonaws.*region*.iotmanagedintegrations.api
	com.amazonaws.*region*.iotmanagedintegrations-fips.api
AWS IoT Core for LoRaWAN	com.amazonaws.*region*.iotwireless.api
	com.amazonaws.*region*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns

AWS 서비스	서비스 이름
AWS IoT FleetWise	com.amazonaws.*region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws.*region*.greengrass
AWS IoT RoboRunner	com.amazonaws.*region*.iotroborunner
AWS IoT SiteWise	com.amazonaws.*region*.iotsitewise.api
	com.amazonaws.*region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws.*region*.iottwinmaker.api
	com.amazonaws.*region*.iottwinmaker.data
Amazon Kendra	com.amazonaws.*region*.kendra
	aws.api.*region*.kendra-ranking
AWS Key Management Service	com.amazonaws.*region*.kms
	com.amazonaws.*region*.kms-fips
Amazon Keyspaces(Apache Cassandra용)	com.amazonaws.*region*.cassandra
	com.amazonaws.*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
	com.amazonaws.*region*.kinesis-streams-fips
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
AWS Launch Wizard	com.amazonaws.*region*.launchwizard
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex

AWS 서비스	서비스 이름
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-linux-subscriptions
	com.amazonaws.*region*.license-manager-linux-subscriptions-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
	com.amazonaws.*region*.license-manager-user-subscriptions-fips
Amazon Lightsail	com.amazonaws.*region*.lightsail
Amazon Location Service	com.amazonaws.*region*.geo.maps
	com.amazonaws.*region*.geo.places
	com.amazonaws.*region*.geo.routes
	com.amazonaws.*region*.geo.geofencing
	com.amazonaws.*region*.geo.tracking
	com.amazonaws.*region*.geo.metadata
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
	com.amazonaws.*region*.macie2-fips
AWS Mainframe Modernization	com.amazonaws.*region*.apptest

AWS 서비스	서비스 이름
	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
AWS Marketplace Metering Service	com.amazonaws.*region*.metering-marketplace
– Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Streaming for Apache Kafka(MSK)	com.amazonaws.*region*.kafka
	com.amazonaws.*region*.kafka-fips
Amazon Managed Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.api-fips
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.env-fips
	com.amazonaws.*region*.airflow.ops
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	aws.api.us-east-2.route53globalresolver
	aws.api.us-east-2.route53globalresolver-fips
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin

AWS 서비스	서비스 이름
Amazon MemoryDB	com.amazonaws.*region*.memory-db
	com.amazonaws.*region*.memorydb-fips
AWS Migration Hub Orchestrator	com.amazonaws.*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws.*region*.refactor-spaces
Migration Hub Strategy Recommendations	com.amazonaws.*region*.migrationhub-strategy
Amazon MQ	com.amazonaws.*region*.mq
	com.amazonaws.*region*.mq-fips
Amazon Neptune Analytics	com.amazonaws.*region*.neptune-graph
	com.amazonaws.*region*.neptune-graph-data
	com.amazonaws.*region*.neptune-graph-fips
AWS Network Firewall	com.amazonaws.*region*.network-firewall
	com.amazonaws.*region*.network-firewall-fips
Amazon OpenSearch Service	이러한 엔드포인트는 서비스 관리형입니다.
Amazon OpenSearch Ingestion	com.amazonaws.*region*.osis
AWS Organizations	com.amazonaws.*region*.organizations
	com.amazonaws.*region*.organizations-fips
AWS Outposts	com.amazonaws.*region*.outposts
AWS Panorama	com.amazonaws.*region*.panorama
AWS 결제 암호화	com.amazonaws.*region*.payment-cryptography.controlplane

AWS 서비스	서비스 이름
	com.amazonaws.*region*.payment-cryptography.datap lane
AWS PCS	com.amazonaws.*region*.pcs
	com.amazonaws.*region*.pcs-fips
Amazon Personalize	com.amazonaws. *##*.개인화
	com.amazonaws. *##*.개인화-이벤트
	com.amazonaws. *##*.개인화-런타임
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
	com.amazonaws.*region*.polly-fips
AWS 가격표	com.amazonaws.*region*.pricing.api
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.acm-pca-fips
	com.amazonaws.*region*.pca-connector-ad
	com.amazonaws.*region*.pca-connector-scep
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api.*region*.qbusiness
Amazon Q Developer	com.amazonaws.*region*.codewhisperer
	com.amazonaws.*region*.q
	com.amazonaws.*region*.qapps

AWS 서비스	서비스 이름
Amazon Q 사용자 구독	com.amazonaws.*region*.service.user-subscriptions
빠른	com.amazonaws.*region*.quicksight-website
Amazon RDS	com.amazonaws.*region*.rds
	com.amazonaws.*region*.rds-fips
Amazon RDS Data API	com.amazonaws.*region*.rds-data
Amazon RDS 성능 개선 도우미	com.amazonaws.*region*.pi
	com.amazonaws.*region*.pi-fips
AWS re:Post 프라이빗	com.amazonaws.*region*.repostspace
휴지통	com.amazonaws.*region*.rbin
	com.amazonaws.*region*.rbin-fips
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
	com.amazonaws.*region*.redshift-serverless
	com.amazonaws.*region*.redshift-serverless-fips
Amazon Redshift 데이터 API	com.amazonaws.*region*.redshift-data
	com.amazonaws.*region*.redshift-data-fips
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips

AWS 서비스	서비스 이름
AWS Resource Access Manager	com.amazonaws.*region*.ram
	com.amazonaws.*region*.ram-fips
AWS 리소스 탐색기	com.amazonaws.*region*.resource-explorer-2
	com.amazonaws.*region*.resource-explorer-2-fips
AWS Resource Groups	com.amazonaws.*region*.resource-groups
	com.amazonaws.*region*.resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws.*region*.tagging
Amazon S3	com.amazonaws.*region*.s3
	com.amazonaws.*region*.s3tables
Amazon S3 다중 리전 액세스 포인트	com.amazonaws.s3-global.accesspoint
Outposts에서의 Amazon S3	com.amazonaws.*region*.s3-outposts
Amazon SageMaker AI	aws.sagemaker.*region*.experiments
	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.partner-app
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker-data-science-assistant
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.api-fips
	com.amazonaws.*region*.sagemaker.featurestore-runtime

AWS 서비스	서비스 이름
	com.amazonaws.*region*.sagemaker.featurestore-runtime-fips
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
절감형 플랜	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub CSPM	com.amazonaws.*region*.securityhub
	com.amazonaws.*region*.securityhub-fips
Amazon Security Lake	com.amazonaws.*region*.securitylake
	com.amazonaws.*region*.securitylake-fips
AWS Security Token Service	com.amazonaws.*region*.sts
	com.amazonaws.*region*.sts-fips
AWS Serverless Application Repository	com.amazonaws.*region*.serverlessrepo
Service Catalog	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry
Service Quotas	com.amazonaws.*region*.servicequotas
Amazon SES	com.amazonaws.*region*.email-smtp
	com.amazonaws.*region*.mail-manager
	com.amazonaws.*region*.mail-manager-fips

AWS 서비스	서비스 이름
	com.amazonaws.*region*.mail-manager-smtp.auth.fips
	com.amazonaws.*region*.mail-manager-smtp.open.fips
AWS SimSpace Weaver	com.amazonaws.*region*.simspaceweaver
AWS Snowball Edge Device Management	com.amazonaws.*region*.snow-device-management
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
	com.amazonaws.*region*.sqs-fips
Amazon SWF	com.amazonaws.*region*.swf
	com.amazonaws.*region*.swf-fips
AWS Step Functions	com.amazonaws.*region*.states
	com.amazonaws.*region*.sync-states
AWS Storage Gateway	com.amazonaws.*region*.storagegateway
AWS Supply Chain	com.amazonaws.*region*.scn
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssm-incidents-fips
	com.amazonaws.*region*.ssm-quicksetup
	com.amazonaws.*region*.ssmmessages

AWS 서비스	서비스 이름
AWS Systems Manager for SAP	com.amazonaws.*region*.ssm-sap
	com.amazonaws.*region*.ssm-sap-fips
AWS 통신 네트워크 빌더	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
Amazon Timestream for InfluxDB	com.amazonaws.*region*.timestream-influxdb
	com.amazonaws.*region*.timestream-influxdb-fips
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
	com.amazonaws.*region*.transcribestreaming-fips
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
AWS Transform	com.amazonaws.*region*.transform
AWS Transform 사용자 지정	com.amazonaws.*region*.transform-custom
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor

AWS 서비스	서비스 이름
AWS 사용자 알림	com.amazonaws.*region*.notifications
	com.amazonaws.*region*.notifications-contacts
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
	com.amazonaws.*region*.verifiedpermissions-fips
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
AWS WAFV2	com.amazonaws.*region*.wafv2
	com.amazonaws.*region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws.*region*.wellarchitected
Amazon WorkMail	com.amazonaws.*region*.workmail
	com.amazonaws.*region*.workmailmessageflow
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Secure Browser	com.amazonaws.*region*.workspaces-web
	com.amazonaws.*region*.workspaces-web-fips
WorkSpaces streaming	com.amazonaws.*region*.highlander
Amazon WorkSpaces Thin Client	com.amazonaws.*region*.thinclient.api
AWS X-Ray	com.amazonaws.*region*.xray
Amazon Managed Service for Apache Flink	com.amazonaws.*region*.kinesisanalytics
	com.amazonaws.*region*.kinesisanalytics-fips

사용 가능한 AWS 서비스 이름 보기

describe-vpc-endpoint-services 명령을 사용하여 VPC 엔드포인트를 지원하는 서비스 이름을 볼 수 있습니다.

다음 예제에서는 지정된 리전에서 인터페이스 엔드포인트를 AWS 서비스 지원하는를 표시합니다. 이 `--query` 옵션은 출력을 서비스 이름으로 제한합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

다음은 예제 출력입니다. 전체 출력은 표시되지 않습니다.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    . . .
     "com.amazonaws.us-east-1.xray"
]
```

서비스에 대한 정보 보기

서비스 이름이 있으면 describe-vpc-endpoint-services 명령을 사용하여 각 엔드포인트 서비스에 대한 세부 정보를 볼 수 있습니다.

다음 예는 지정된 리전의 Amazon CloudWatch 인터페이스 엔드포인트에 대한 정보를 표시합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

출력의 예는 다음과 같습니다. `VpcEndpointPolicySupported`는 엔드포인트 정책이 지원되는지 여부를 나타냅니다. `SupportedIpAddressTypes`는 지원되는 IP 주소 유형을 나타냅니다.

```
{
```

```
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring.us-east-1.api.aws"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
                }           ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv6",
                "ipv4"
            ]
```

```
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

엔드포인트 정책 지원 보기

서비스가 엔드포인트 정책을 지원하는지 확인하려면 describe-vpc-endpoint-services 명령을 호출하고 VpcEndpointPolicySupported의 값을 확인합니다. 가능한 값은 true와 false입니다.

다음 예는 지정된 리전에서 지정된 서비스가 엔드포인트 정책을 지원하는지 확인합니다. --query 옵션은 출력을 VpcEndpointPolicySupported의 값으로 제한합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

다음은 예제 출력입니다.

```
True
```

다음 예제에서는 지정된 리전에서 엔드포인트 정책을 AWS 서비스 지원하는를 나열합니다. 이 --query 옵션은 출력을 서비스 이름으로 제한합니다. Windows 명령 프롬프트를 사용하여 이 명령을 실행하려면 쿼리 문자열 앞뒤의 작은따옴표를 제거하고 줄 연속 문자를 \에서 ^으로 변경합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

다음은 예제 출력입니다. 전체 출력은 표시되지 않습니다.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
```

```
    "aws.api.us-east-1.kendra-ranking",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

다음 예제에서는 지정된 리전에서 엔드포인트 정책을 지원하지 AWS 서비스 않는를 나열합니다. 이 `--query` 옵션은 출력을 서비스 이름으로 제한합니다. Windows 명령 프롬프트를 사용하여 이 명령을 실행하려면 쿼리 문자열 앞뒤의 작은따옴표를 제거하고 줄 연속 문자를 \에서 ^으로 변경합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

다음은 예제 출력입니다. 전체 출력은 표시되지 않습니다.

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    . . .
    "com.amazonaws.us-east-1.transfer.server"
]
```

IPv6 지원 보기

AWS 서비스에 대한 IPv6 지원을 보려면 AWS IPv6를 지원하는 서비스를 참조하세요. 다음 describe-vpc-endpoint-services 명령을 사용하여 지정된 리전에서 IPv6를 통해 액세스할 수 AWS 서비스 있는를 볼 수도 있습니다. 이 `--query` 옵션은 출력을 서비스 이름으로 제한합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

다음은 예제 출력입니다. 전체 출력은 표시되지 않습니다.

```
[
```

```
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "aws.api.us-east-1.resource-explorer-2",
    "aws.api.us-east-1.resource-explorer-2-fips",
    "aws.sagemaker.us-east-1.experiments",
    "aws.sagemaker.us-east-1.partner-app",
    "com.amazonaws.iam",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

교차 리전 활성화된 AWS 서비스

다음은 교차 리전과 AWS 서비스 통합됩니다 AWS PrivateLink. 인터페이스 엔드포인트를 생성하여 자체 VPC에서 실행 중인 것처럼 다른 AWS 리전의 이러한 서비스에 비공개로 연결할 수 있습니다.

AWS 서비스 열에서 링크를 선택하면 서비스 설명서를 볼 수 있습니다. 서비스 이름 열에는 인터페이스 엔드포인트를 생성할 때 지정하는 서비스 이름이 포함됩니다.

AWS 서비스	서비스 이름
Amazon S3	com.amazonaws.*region*.s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Amazon ECR	com.amazonaws.*region*.ecr.api
	com.amazonaws.*region*.ecr.dkr
AWS Key Management Service	com.amazonaws.*region*.kms
	com.amazonaws.*region*.kms-fips
Amazon ECS	com.amazonaws.*region*.ecs

AWS 서비스	서비스 이름
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
Amazon Managed Service for Apache Flink	com.amazonaws.*region*.kinesisanalytics
	com.amazonaws.*region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

사용 가능한 AWS 서비스 이름 보기

describe-vpc-endpoint-services 명령을 사용하여 리전 간 지원 서비스를 볼 수 있습니다.

다음 예제에서는 us-east-1 리전의 사용자가 인터페이스 엔드포인트를 통해 지정된 (us-west-2) 서비스 리전에 액세스할 수 AWS 서비스 있는를 표시합니다. 이 --query 옵션은 출력을 서비스 이름으로 제한합니다.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

다음은 예제 출력입니다. 전체 출력은 표시되지 않습니다.

```
[
    "com.amazonaws.us-west-2.ecr.api",
    "com.amazonaws.us-west-2.ecr.dkr",
    "com.amazonaws.us-west-2.ecs",
    "com.amazonaws.us-west-2.ecs-fips",
    ...
    "com.amazonaws.us-west-2.s3"
]
```

> **Note**
>
> 리전 DNS를 사용해야 합니다. 다른 리전 AWS 서비스 에서에 액세스할 때는 영역 DNS가 지원되지 않습니다. 자세한 내용은 Amazon VPC 사용 설명서의 DNS 속성 보기 및 업데이트를 참조하세요.

권한 및 고려 사항

- 기본적으로 IAM 엔터티에는 다른 리전의 AWS 서비스 에 액세스할 수 있는 권한이 없습니다. 리전 간 액세스에 필요한 권한을 부여하기 위해 IAM 관리자는 `vpce:AllowMultiRegion` 권한 전용 작업을 허용하는 IAM 정책을 생성할 수 있습니다.
- 서비스 제어 정책(SCP)이 `vpce:AllowMultiRegion` 권한 전용 작업을 거부하지 않는지 확인합니다. AWS PrivateLink의 교차 리전 연결 기능을 사용하려면 자격 증명 정책과 SCP가 모두이 작업을 허용해야 합니다.
- VPC 엔드포인트를 생성할 때 IAM 엔터티가 지정할 수 있는 서비스 리전을 제어하려면 `ec2:VpceServiceRegion` 조건 키를 사용합니다.
- 서비스 소비자는 엔드포인트의 서비스 리전으로 선택하기 전에 해당 옵트인 리전에 참여해야 합니다. 가능한 경우, 서비스 소비자는 리전 내 연결을 통해 서비스를 액세스하는 것이 교차 리전 연결보다 권장됩니다. 리전 내 연결은 지연 시간이 짧고 비용이 적게 듭니다.
- IAM의 새로운 `aws:SourceVpcArn` 전역 조건 키를 사용하여 리소스에 액세스할 수 있는 리전 AWS 계정 및 VPCs 보호할 수 있습니다. 이 키는 데이터 레지던시 및 리전 기반 액세스 제어를 구현하는 데 도움이 됩니다.
- 고가용성을 위해 두 개 이상의 가용 영역에 교차 리전 지원 인터페이스 엔드포인트를 생성합니다. 이 경우 공급자와 소비자가 동일한 가용 영역을 사용할 필요는 없습니다.
- 교차 리전 액세스를 통해는 서비스 및 소비자 리전 모두에서 가용 영역 간의 장애 조치를 AWS PrivateLink 관리합니다. 교차 리전 장애 조치는 관리하지 않습니다.
- 리전 간 액세스는 `use1-az3`, , `usw1-az2`, 및 가용 영역에서 지원되지 않습니다`apne1-az3``apne2-az2``apne2-az4`.
- AWS Fault Injection Service 를 사용하여 리전 내 및 리전 간 활성화 인터페이스 엔드포인트에 대한 리전 이벤트 및 모델 장애 시나리오를 시뮬레이션할 수 있습니다. 자세한 내용은 AWS FIS 설명서를 참조하세요.

다른 리전 AWS 서비스 의에 대한 인터페이스 엔드포인트 생성

콘솔을 사용하여 인터페이스 엔드포인트를 생성하려면 VPC 엔드포인트 생성 섹션을 참조하세요.

CLI에서 create-vpc-endpoint 명령을 사용하여 다른 리전의 AWS 서비스 에 대한 VPC 엔드포인트를 생성할 수 있습니다. 다음 예제에서는의 VPC`us-west-2`에서의 Amazon S3에 대한 인터페이스 엔드포인트를 생성합니다`us-east-1`.

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-id \
  --service-name com.amazonaws.us-west-2.s3 \
  --vpc-endpoint-type Interface \
  --subnet-ids subnet-id-1 subnet-id-2 \
  --region us-east-1 \
  --service-region us-west-2
```

인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여에 액세스

인터페이스 VPC 엔드포인트를 생성하여 여러를 AWS PrivateLink포함하여 기반 서비스에 연결할 수 있습니다 AWS 서비스. 개요는 the section called “개념” and AWS 서비스액세스을(를) 참조하세요.

VPC에서 지정하는 각 서브넷에 대해 서브넷에 엔드포인트 네트워크 인터페이스가 생성되고 해당 인터페이스에 서브넷 주소 범위의 프라이빗 IP 주소가 할당됩니다. 엔드포인트 네트워크 인터페이스는 요청자가 관리하는 네트워크 인터페이스로, AWS 계정에서 확인할 수 있지만 직접 관리할 수는 없습니다.

이용 시 시간당 사용 요금 및 데이터 처리 요금이 청구됩니다. 자세한 내용은 인터페이스 엔드포인트 요금을 참조하세요.

내용

- 사전 조건
- VPC 엔드포인트 생성
- 공유 서브넷
- ICMP

사전 조건

- VPC에서 AWS 서비스 에 액세스할 리소스를 배포합니다.
- 프라이빗 DNS를 사용하려면 VPC에 대해 DNS 호스트 이름 및 DNS 확인을 활성화해야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 DNS 속성 보기 및 업데이트를 참조하세요.
- 인터페이스 엔드포인트에 대해 IPv6를 활성화하려면가 IPv6를 통한 액세스를 지원 AWS 서비스 해야 합니다. 자세한 내용은 the section called “IP 주소 유형” 단원을 참조하십시오.
- VPC의 리소스에서 예상되는 트래픽을 허용하도록 엔드포인트 네트워크 인터페이스에 대한 보안 그룹 규칙을 생성합니다. 예를 들어가에 HTTPS 요청을 보낼 AWS CLI 수 있도록 하려면 AWS 서비스 보안 그룹이 인바운드 HTTPS 트래픽을 허용해야 합니다.
- 리소스가 네트워크 ACL를 사용하는 서브넷에 있는 경우 네트워크 ACL에서 VPC의 리소스와 엔드포인트 네트워크 인터페이스 간 트래픽을 허용하는지 확인합니다.
- AWS PrivateLink 리소스에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 단원을 참조하십시오.

VPC 엔드포인트 생성

다음 절차에 따라 AWS 서비스에 연결하는 인터페이스 VPC 엔드포인트를 생성합니다.

에 대한 인터페이스 엔드포인트를 생성하려면 AWS 서비스

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 유형에서 AWS 서비스를 선택합니다.
5. (선택 사항) 다른 리전 AWS 서비스 의에 대한 엔드포인트를 생성하는 경우 교차 리전 엔드포인트 활성화 확인란을 선택한 다음 드롭다운에서 서비스 리전을 선택합니다.
6. 서비스 이름(Service name)에서 서비스를 선택합니다. 자세한 내용은 the section called “통합되는 서비스” 단원을 참조하십시오.
7. VPC에서 AWS 서비스에 액세스하는 데 사용할 VPC를 선택합니다.
8. 5단계에서 Amazon S3 서비스 이름을 선택한 경우 프라이빗 DNS 지원을 구성하려면 추가 설정인 DNS 이름 활성화를 선택합니다. 이 옵션을 선택하면 인바운드 엔드포인트에 대해서만 프라이빗 DNS 활성화도 자동으로 선택됩니다. Amazon S3 인터페이스 엔드포인트에 대해서만 인바운드 Resolver 엔드포인트를 사용하여 프라이빗 DNS를 구성할 수 있습니다. Amazon S3용 게이트웨이

엔드포인트가 없는 상태에서 인바운드 엔드포인트에 프라이빗 DNS만 활성화를 선택하면 이 절차의 마지막 단계를 시도할 때 오류가 발생합니다.

5단계에서 Amazon S3가 아닌 다른 서비스의 서비스 이름을 선택한 경우 추가 설정인 DNS 이름 활성화가 이미 선택되어 있습니다. 기본값을 그대로 유지하는 것이 좋습니다. 이렇게 하면 AWS SDK를 통한 요청과 같이 퍼블릭 서비스 엔드포인트를 사용하는 요청이 VPC 엔드포인트로 확인됩니다.

9. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다. 가용 영역당 서브넷 한 개를 선택할 수 있습니다. 동일한 가용 영역에서 여러 서브넷을 선택할 수 없습니다. 자세한 내용은 the section called “서브넷 및 가용 영역” 단원을 참조하십시오.

   기본적으로 서브넷 IP 주소 범위의 IP 주소를 선택하고 엔드포인트 네트워크 인터페이스에 할당합니다. IP 주소를 직접 선택하려면 IP 주소 지정을 선택합니다. 서브넷 CIDR 블록의 처음 4개의 IP 주소와 마지막 IP 주소는 내부용으로 예약되어 있으므로 엔드포인트 네트워크 인터페이스에 지정할 수 없습니다.

10. IP 주소 유형에서 다음 옵션 중에서 선택합니다.

    - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있으며 서비스가 IPv4 요청을 수락하는 경우에만 지원됩니다.
    - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷이며 서비스가 IPv6 요청을 수락하는 경우에만 지원됩니다.
    - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있으며 서비스가 IPv4 및 IPv6 요청을 모두 수락하는 경우에만 지원됩니다.

11. 보안 그룹에서 엔드포인트 네트워크 인터페이스에 연결할 보안 그룹을 선택합니다. 기본적으로 VPC에 대한 기본 보안 그룹이 연결됩니다.
12. 정책에서 인터페이스 엔드포인트를 통해 모든 보안 주체가 모든 리소스에 대해 모든 작업을 수행할 수 있도록 허용하려면 전체 액세스를 선택합니다. 액세스를 제한하려면 사용자 지정을 선택하고 정책을 입력합니다. 이 옵션은 서비스에서 VPC 엔드포인트 정책을 지원하는 경우에만 사용할 수 있습니다. 자세한 내용은 엔드포인트 정책 단원을 참조하십시오.
13. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
14. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)

- New-EC2VpcEndpoint(Windows PowerShell용 도구)

공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다.

ICMP

인터페이스 엔드포인트는 ping 요청에 응답하지 않습니다. 대신 nc 또는 nmap 명령을 사용할 수 있습니다.

인터페이스 엔드포인트 구성

인터페이스 VPC 엔드포인트를 생성한 후 해당 구성을 업데이트할 수 있습니다.

작업

- 서브넷 추가 또는 제거
- 보안 그룹 연결
- VPC 엔드포인트 정책 편집
- 프라이빗 DNS 이름 활성화
- 태그 관리

서브넷 추가 또는 제거

인터페이스 엔드포인트에 대해 가용 영역당 1개의 서브넷만 선택할 수 있습니다. 서브넷을 추가하면 서브넷에 엔드포인트 네트워크 인터페이스가 생성되고 해당 인터페이스에 서브넷 IP 주소 범위의 프라이빗 IP 주소가 할당됩니다. 서브넷을 제거하면 엔드포인트 네트워크 인터페이스가 삭제됩니다. 자세한 내용은 the section called “서브넷 및 가용 영역” 단원을 참조하십시오.

콘솔을 사용하여 서브넷 변경하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.

4. 작업(Actions), 서브넷 관리(Manage subnets)를 선택합니다.
5. 필요에 따라 가용 영역을 선택하거나 선택 취소합니다. 가용 영역마다 서브넷을 하나씩 선택합니다. 기본적으로 서브넷 IP 주소 범위의 IP 주소를 선택하고 엔드포인트 네트워크 인터페이스에 할당합니다. 엔드포인트 네트워크 인터페이스에 대한 IP 주소를 선택하려면 IP 주소 지정을 선택하고 서브넷 주소 범위의 IPv4 주소를 입력합니다. 엔드포인트 서비스에서 IPv6를 지원하는 경우 서브넷 주소 범위의 IPv6 주소를 입력할 수도 있습니다.

   이 VPC 엔드포인트에 대한 엔드포인트 네트워크 인터페이스가 이미 있는 서브넷의 IP 주소를 지정하면 엔드포인트 네트워크 인터페이스가 새 엔드포인트 네트워크 인터페이스로 바뀝니다. 이 프로세스는 일시적으로 서브넷과 VPC 엔드포인트 연결을 해제합니다.
6. 서브넷 수정(Modify subnets)을 선택합니다.

명령줄을 사용하여 서브넷 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

보안 그룹 연결

인터페이스 엔드포인트의 네트워크 인터페이스와 연결된 보안 그룹을 변경할 수 있습니다. 보안 그룹 규칙은 VPC의 리소스에서 엔드포인트 네트워크 인터페이스 간에 허용되는 트래픽을 제어합니다.

콘솔을 사용하여 보안 그룹 변경하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 작업(Actions), 보안 그룹 관리(Manage security groups)를 선택합니다.
5. 필요에 따라 보안 그룹을 선택하거나 선택 취소합니다.
6. 보안 그룹 수정(Modify security groups)을 선택합니다.

명령줄을 사용하여 보안 그룹 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

VPC 엔드포인트 정책 편집

가 엔드포인트 정책을 AWS 서비스 지원하는 경우 엔드포인트에 대한 엔드포인트 정책을 편집할 수 있습니다. 엔드포인트 정책을 업데이트할 경우 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다. 자세한 내용은 엔드포인트 정책 단원을 참조하십시오.

콘솔을 사용하여 엔드포인트 정책 변경

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 작업(Actions), 정책 관리(Manage policy)를 선택합니다.
5. 모든 액세스(Full Access)를 선택하여 서비스에 대한 전체 액세스를 허용하거나 사용자 지정(Custom)을 선택하고 사용자 지정 정책을 연결합니다.
6. 저장을 선택합니다.

명령줄을 사용하여 엔드포인트 정책 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

프라이빗 DNS 이름 활성화

AWS 서비스용 VPC 엔드포인트에 프라이빗 DNS 이름을 사용하는 것이 좋습니다. 이렇게 하면 AWS SDK를 통한 요청과 같이 퍼블릭 서비스 엔드포인트를 사용하는 요청이 VPC 엔드포인트로 확인됩니다.

프라이빗 DNS를 사용하려면 VPC에 대해 DNS 호스트 이름 및 DNS 확인을 모두 활성화해야 합니다. 프라이빗 DNS를 활성화하면 프라이빗 IP 주소를 사용할 수 있게 되기까지 몇 분 정도 걸릴 수 있습니다. 프라이빗 DNS 이름을 활성화할 때 생성되는 DNS 레코드는 프라이빗입니다. 따라서 프라이빗 DNS 이름은 공개적으로 확인할 수 없습니다.

콘솔을 사용하여 프라이빗 DNS 이름 옵션 변경하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.

4. 작업(Actions), 프라이빗 DNS 이름 수정(Modify private DNS name)을 차례로 선택합니다.
5. 필요에 따라 이 엔드포인트에 대해 활성화(Enable for this endpoint)를 선택하거나 선택 취소합니다.
6. 서비스가 Amazon S3인 경우 이전 단계에서 이 엔드포인트에 대해 활성화를 선택하면 인바운드 엔드포인트에 대해서만 프라이빗 DNS 활성화도 선택됩니다. 표준 프라이빗 DNS 기능을 선호하는 경우 인바운드 엔드포인트에 프라이빗 DNS만 활성화를 선택 해제하세요. Amazon S3용 인터페이스 엔드포인트 외에 Amazon S3용 게이트웨이 엔드포인트가 없는 경우 인바운드 엔드포인트에 대해서만 프라이빗 DNS 활성화를 선택하면 다음 단계에서 변경 사항을 저장할 때 오류가 발생합니다. 자세한 내용은 the section called “프라이빗 DNS” 단원을 참조하십시오.
7. 변경 사항 저장을 선택합니다.

명령줄을 사용하여 프라이빗 DNS 이름 옵션 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

태그 관리

인터페이스 엔드포인트에 태그를 지정하면 조직의 요구에 따라 엔드포인트를 식별하거나 분류하는 데 도움을 얻을 수 있습니다.

콘솔을 사용하여 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 작업, 태그 관리를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장을 선택합니다.

명령줄을 사용하여 태그 관리하기

- create-tags 및 delete-tags(AWS CLI)
- New-EC2Tag 및 Remove-EC2Tag(Windows PowerShell용 도구)

인터페이스 엔드포인트 이벤트에 대한 알림 받기

인터페이스 엔드포인트와 관련된 특정 이벤트에 대한 알림을 받도록 알림을 생성할 수 있습니다. 연결 요청이 수락되거나 거부될 때 이메일을 수신할 수 있습니다.

작업

- SNS 알림 생성
- 액세스 정책 추가
- 키 정책 추가

SNS 알림 생성

다음 절차를 활용하여 알림을 위한 Amazon SNS 주제를 생성하고 해당 주제를 구독합니다.

콘솔을 사용하여 인터페이스 엔드포인트에 대한 알림 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 알림(Notifications) 탭에서 알림 생성(Create notification)을 선택합니다.
5. 알림 ARN에서 생성한 SNS 토픽의 Amazon 리소스 이름(ARN)을 선택합니다.
6. 이벤트를 구독하려면 Events(이벤트)에서 이벤트를 선택합니다.
   - Connect(연결) - 서비스 소비자가 인터페이스 엔드포인트를 생성했습니다. 이 경우 연결 요청이 서비스 공급자에 전송됩니다.
   - 허용(Accept) - 서비스 공급자가 연결 요청을 수락했습니다.
   - Reject(거부) – 서비스 공급자가 연결 요청을 거부했습니다.
   - Delete(삭제) – 서비스 소비자가 인터페이스 엔드포인트를 삭제했습니다.
7. 알림 생성(Create notification)을 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트에 대한 알림 생성하기

- create-vpc-endpoint-connection-notification(AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Windows PowerShell용 도구)

액세스 정책 추가

가 다음과 같이 사용자를 대신하여 알림을 AWS PrivateLink 게시할 수 있도록 허용하는 액세스 정책을 Amazon SNS 주제에 추가합니다. 자세한 내용은 내 Amazon SNS 주제의 액세스 정책을 편집하려면 어떻게 해야 합니까?를 참조하세요. 혼동된 대리자 문제를 방지하기 위해 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 키를 사용합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

키 정책 추가

암호화된 SNS 주제를 사용하는 경우 KMS 키의 리소스 정책은 AWS KMS API 작업을 호출 AWS PrivateLink 하기 위해를 신뢰해야 합니다. 다음은 예제 키 정책입니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

인터페이스 엔드포인트 삭제

VPC 엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다. 인터페이스 엔드포인트를 삭제하면 해당 엔드포인트 네트워크 인터페이스도 삭제됩니다.

콘솔을 사용하여 인터페이스 엔드포인트 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.

5. 확인 메시지가 표시되면 **delete**를 입력합니다.
6. 삭제를 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(Windows PowerShell용 도구)

게이트웨이 엔드포인트

게이트웨이 VPC 엔드포인트를 사용하면 VPC용 인터넷 게이트웨이 또는 NAT 디바이스가 없어도 Amazon S3 및 DynamoDB에 안정적으로 연결할 수 있습니다. 게이트웨이 엔드포인트는 다른 유형의 VPC 엔드포인트와 AWS PrivateLink달리를 사용하지 않습니다.

Amazon S3와 DynamoDB는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다. 옵션에 대한 비교는 다음을 참조하세요.

- Amazon S3용 VPC 엔드포인트의 유형
- Amazon DynamoDB용 VPC 엔드포인트의 유형

가격 책정

게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다.

내용

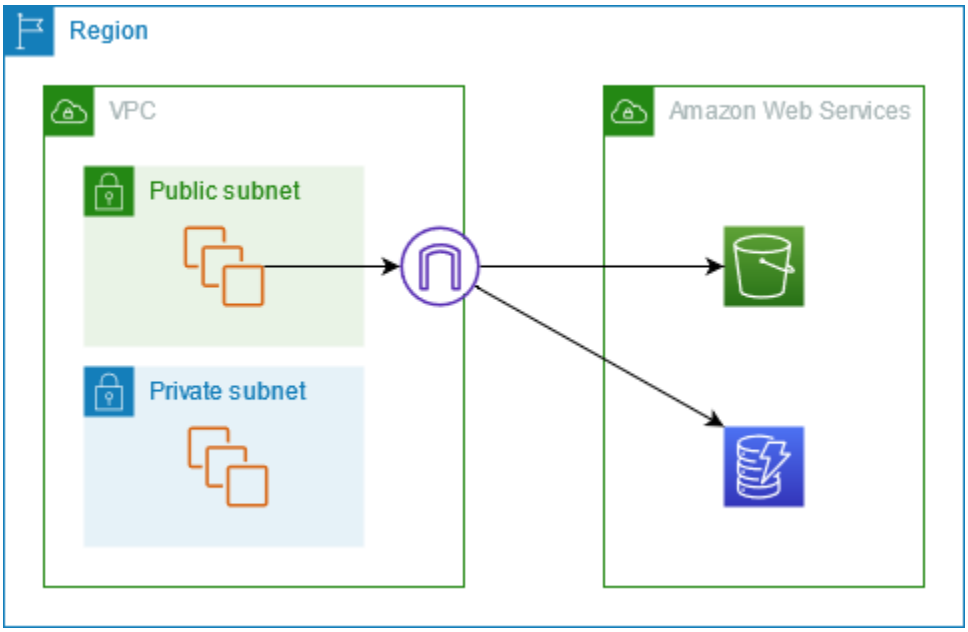
- 개요
- 라우팅
- 보안
- IP 주소 유형
- DNS 레코드 IP 유형
- Amazon S3에 대한 게이트웨이 엔드포인트
- Amazon DynamoDB에 대한 게이트웨이 엔드포인트

개요

Amazon S3와 DynamoDB는 퍼블릭 서비스 엔드포인트나 게이트웨이 엔드포인트를 통해 액세스할 수 있습니다. 이 개요에서는 두 방법을 비교합니다.

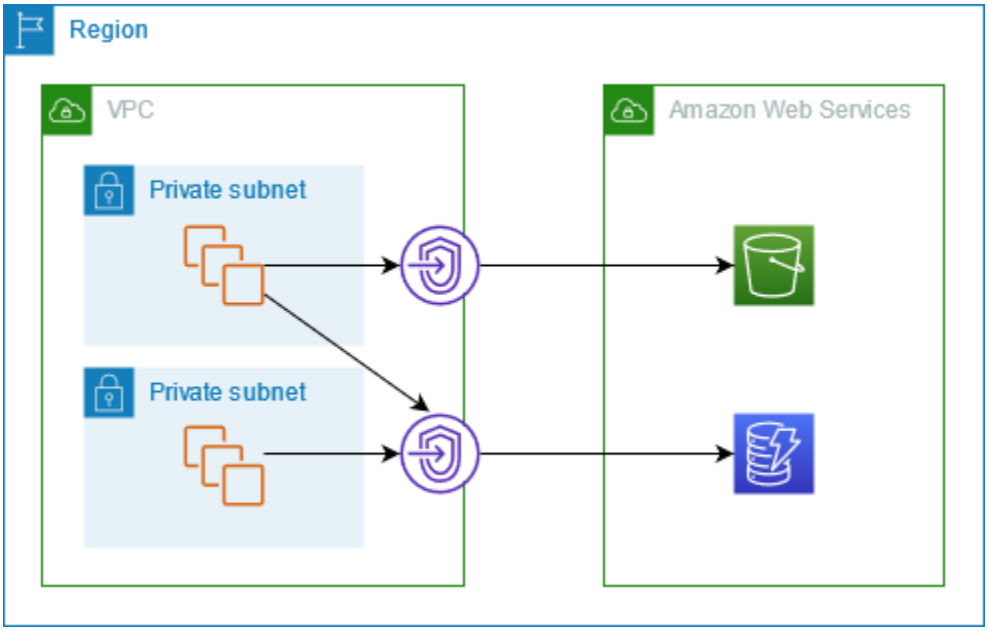
인터넷 게이트웨이를 통한 액세스

다음 다이어그램은 인스턴스에서 퍼블릭 서비스 엔드포인트를 통해 Amazon S3 및 DynamoDB에 액세스하는 방법을 보여줍니다. 퍼블릭 서브넷의 인스턴스에서 Amazon S3 또는 DynamoDB로의 트래픽은 VPC의 인터넷 게이트웨이를 거쳐 서비스로 라우팅됩니다. 프라이빗 서브넷의 인스턴스는 Amazon S3 또는 DynamoDB로 트래픽을 전송할 수 없습니다. 기본적으로 프라이빗 서브넷에는 인터넷 게이트웨이에 대한 라우팅이 없기 때문입니다. 프라이빗 서브넷의 인스턴스에서 Amazon S3 또는 DynamoDB로 트래픽을 보내려면 퍼블릭 서브넷에 NAT 디바이스를 추가하고 프라이빗 서브넷의 트래픽을 NAT 디바이스로 라우팅합니다. Amazon S3 또는 DynamoDB로의 트래픽은 인터넷 게이트웨이를 통과하지만 AWS 네트워크를 벗어나지 않습니다.



게이트웨이 엔드포인트를 통한 액세스

다음 다이어그램은 인스턴스에서 게이트웨이 엔드포인트를 통해 Amazon S3 및 DynamoDB에 액세스하는 방법을 보여줍니다. VPC에서 Amazon S3 또는 DynamoDB로의 트래픽은 게이트웨이 엔드포인트로 라우팅됩니다. 각 서브넷 라우팅 테이블에는 서비스로 전송되는 트래픽을 서비스의 접두사 목록을 사용하여 게이트웨이 엔드포인트로 보내는 라우팅이 있어야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 AWS관리형 접두사 목록을 참조하세요.



라우팅

게이트웨이 엔드포인트를 생성할 때 활성화하는 서브넷의 VPC 라우팅 테이블을 선택합니다. 선택하는 각 라우팅 테이블에는 다음 라우팅이 자동으로 추가됩니다. 대상은가 소유한 서비스의 접두사 목록 AWS 이고 대상은 게이트웨이 엔드포인트입니다.

Destination	대상
prefix_list_id	*gateway_endpoint_id*

고려 사항

- 라우팅 테이블에 추가된 엔드포인트 라우팅을 확인할 수 있지만 수정하거나 삭제할 수는 없습니다. 라우팅 테이블에 엔드포인트 라우팅을 추가하려면 테이블을 게이트웨이 엔드포인트와 연결합니다. 라우팅 테이블과 게이트웨이 엔드포인트의 연결을 해제하거나 게이트웨이 엔드포인트를 삭제하면 엔드포인트 라우팅이 삭제됩니다.
- 게이트웨이 엔드포인트와 연결된 라우팅 테이블에 연결된 서브넷의 모든 인스턴스는 자동으로 해당 게이트웨이 엔드포인트를 사용하여 서비스에 액세스합니다. 이러한 라우팅 테이블과 연결되지 않은 서브넷의 인스턴스는 게이트웨이 엔드포인트가 아니라 퍼블릭 서비스 엔드포인트를 사용합니다.
- 라우팅 테이블에는 Amazon S3에 대한 엔드포인트 라우팅과 DynamoDB에 대한 엔드포인트 라우팅이 모두 있을 수 있습니다. 동일한 서비스(Amazon S3 또는 DynamoDB)에 대한 엔드포인트 라우팅

을 여러 라우팅 테이블에 추가할 수 있습니다. 하지만 동일한 서비스(Amazon S3 또는 DynamoDB)에 대한 여러 엔드포인트 라우팅을 하나의 라우팅 테이블에 추가할 수는 없습니다.

- Amazon은 LPM(Longest Prefix Match)을 통해 트래픽과 일치하는 고도로 구체적인 라우팅을 사용하여 트래픽의 라우팅 방법을 결정합니다. 엔드포인트 라우팅이 포함된 라우팅 테이블의 경우 다음을 의미합니다.
  - 모든 인터넷 트래픽(0.0.0.0/0)을 인터넷 게이트웨이로 보내는 라우팅이 있는 경우 현재 리전에서 서비스(Amazon S3 또는 DynamoDB)로 전송되는 트래픽에 대해 엔드포인트 라우팅이 우선 적용됩니다. 다른 로 향하는 트래픽은 인터넷 게이트웨이를 AWS 서비스 사용합니다.
  - 접두사 목록은 리전에 따라 다르므로 다른 리전의 서비스(Amazon S3 또는 DynamoDB)로 전송되는 트래픽은 인터넷 게이트웨이로 이동됩니다.
  - 동일한 리전에서 서비스(Amazon S3 또는 DynamoDB)의 정확한 IP 주소 범위를 지정하는 라우팅이 있는 경우에는 해당 라우팅이 엔드포인트 라우팅보다 우선 적용됩니다.

보안

인스턴스에서 게이트웨이 엔드포인트를 통해 Amazon S3 또는 DynamoDB에 액세스하는 경우 인스턴스에서 퍼블릭 엔드포인트를 사용하여 서비스에 액세스합니다. 이러한 인스턴스를 위한 보안 그룹은 로드 밸런서에서 이동하는 트래픽을 허용해야 합니다. 다음은 아웃바운드 예제입니다. 서비스의 접두사 목록 ID를 참조합니다.

Destination	프로토콜	포트 범위
prefix_list_id	TCP	443

이러한 인스턴스의 서브넷에 대한 네트워크 ACL은 서비스에서 이동하는 트래픽을 허용해야 합니다. 다음은 아웃바운드 예제입니다. 네트워크 ACL 규칙에서 접두사 목록을 참조할 수는 없지만 접두사 목록에서 서비스의 IP 주소 범위를 가져올 수 있습니다.

Destination	프로토콜	포트 범위
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

IP 주소 유형

IP 주소 유형은 라우팅 테이블에 연결되는 접두사 목록을 결정합니다.

게이트웨이 엔드포인트에서 IPv6을 활성화하기 위한 요구 사항

- 게이트웨이 엔드포인트의 IP 주소 유형은 다음과 같이 엔드포인트에 사용할 서브넷과 호환되어야 합니다.
  - IPv4 - 라우팅 테이블에 서비스의 IPv4 접두사 목록을 추가합니다.
  - IPv6 - 라우팅 테이블에 서비스의 IPv6 접두사 목록을 추가합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
  - 듀얼 스택 - 라우팅 테이블에 서비스의 IPv4 접두사 목록과 IPv6 접두사 목록을 모두 추가합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

DNS 레코드 IP 유형

기본적으로 게이트웨이 엔드포인트는 호출하는 서비스 엔드포인트를 기반으로 DNS 레코드를 반환합니다. 와 같은 IPv4 서비스 엔드포인트를 사용하여 게이트웨이 엔드포인트를 생성하는 경우 `s3.us-east-2.amazonaws.com` Amazon S3는 클라이언트에 A 레코드를 반환하고 라우팅 테이블의 모든 서브넷은 IPv4를 사용합니다.

반대로와 같은 듀얼 스택 서비스 엔드포인트를 사용하여 게이트웨이 엔드포인트를 생성하는 경우 `s3.dualstack.us-east-2.amazonaws.com` Amazon S3는 클라이언트에 A 및 AAAA 레코드를 모두 반환하고 라우팅 테이블의 서브넷은 IPv4 및 IPv6를 사용합니다.

> **Note**
>
> 디렉터리 버킷 또는 S3 Express One Zone의 경우 데이터 영역의 게이트웨이 엔드포인트는 `s3express-use2-az1.dualstack.us-east-2.amazonaws.com` 각각 `s3express-use2-az1.us-east-2.amazonaws.com` 및 입니다.

DNS 레코드 IP 유형은 트래픽이 클라이언트로 라우팅되는 방식에 영향을 줍니다. IPv4 서비스 엔드포인트를 사용하여 게이트웨이 엔드포인트를 생성한 다음 듀얼 스택 서비스 엔드포인트를 호출하는 경우 AAAA 레코드를 사용하는 트래픽은 게이트웨이 엔드포인트를 통해 라우팅되지 않습니다. 트래픽이 있는 경우 IPv6-compatible 경로를 통해 트래픽이 삭제되거나 라우팅됩니다. 서비스 정의 DNS 레코드 IP 유형을 사용하는 경우 서비스가 여러 서비스 엔드포인트의 가변 호출을 처리할 수 있는지 확인합니다.

서비스 정의의 기본 DNS 레코드 IP 유형 설정 대신 DNS 레코드 IP 유형을 사용자 지정하여 특정 엔드포인트에 대해 반환되는 레코드를 선택할 수 있습니다. 다음 표에는 지원되는 DNS 레코드 IP 유형과 반환된 레코드 유형이 나와 있습니다.

DNS 레코드 IP 유형	반환된 레코드 유형
IPv4	A
IPv6	AAAA
듀얼 스택	A 및 AAAA
서비스 정의	레코드는 서비스 엔드포인트에 따라 다릅니다.

DNS 레코드 IP 유형을 선택하려면 엔드포인트 서비스에 호환되는 IP 주소 유형을 사용해야 합니다. 다음 표에는 게이트웨이 엔드포인트의 각 IP 주소 유형에 대해 지원되는 DNS 레코드 IP 유형이 나와 있습니다.

IP 주소 유형	지원되는 DNS 레코드 IP 유형
IPv4	IPv4, 서비스 정의형*
IPv6	IPv6, 서비스 정의형*
듀얼 스택	IPv4, IPv6, 듀얼 스택, 서비스 정의형*

* 기본 DNS 레코드 IP 유형을 나타냅니다.

> **Note**
>
> 게이트웨이 엔드포인트에 대해 서비스 정의 이외의 DNS 레코드 IP 유형을 사용하려면 VPC 설정에서 `enableDnsSupport` 및 `enableDnsHostnames` 속성을 허용해야 합니다.

DynamoDB 게이트웨이 엔드포인트의 DNS 레코드 IP 유형은 변경할 수 없습니다. DynamoDB는 서비스 정의의 DNS 레코드 IP 유형만 지원합니다.

DNS 레코드 IP 유형의 동작은 인터페이스 엔드포인트의 경우 다릅니다. 자세한 내용은 인터페이스 엔드포인트의 DNS 레코드 IP 유형을 참조하세요.

Amazon S3에 대한 게이트웨이 엔드포인트

VPC에서 게이트웨이 VPC 엔드포인트를 사용하여 Amazon S3에 액세스할 수 있습니다. 게이트웨이 엔드포인트를 생성한 후 VPC에서 Amazon S3로 전송되는 트래픽에 대해 해당 엔드포인트를 라우팅 테이블의 대상으로 추가할 수 있습니다.

게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다.

Amazon S3는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다. 게이트웨이 엔드포인트를 사용하면 VPC 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고 추가 비용 없이 VPC에서 Amazon S3에 액세스할 수 있습니다. 그러나 게이트웨이 엔드포인트는 온프레미스 네트워크, 다른 AWS 리전의 피어링된 VPCs 또는 전송 게이트웨이를 통한 액세스를 허용하지 않습니다. 이러한 시나리오에서는 추가 비용을 지불한 후 사용할 수 있는 인터페이스 엔드포인트를 사용해야 합니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3용 VPC 엔드포인트 유형을 참조하세요.

내용

고려 사항

- 게이트웨이 엔드포인트는 해당 엔드포인트를 생성한 리전에서만 사용할 수 있습니다. S3 버킷과 동일한 리전에서 게이트웨이 엔드포인트를 생성해야 합니다.
- Amazon DNS 서버를 사용 중인 경우 VPC에 대해 DNS 호스트 이름 및 DNS 확인을 모두 활성화해야 합니다. 자체 DNS 서버를 사용하는 경우 Amazon S3에 대한 요청이 AWS에서 유지 관리하는 IP 주소로 올바르게 확인되어야 합니다.

- 게이트웨이 엔드포인트를 통해 Amazon S3에 액세스하는 인스턴스의 보안 그룹에 대한 규칙은 Amazon S3에서 이동하는 트래픽을 허용해야 합니다. 보안 그룹 규칙에서 Amazon S3의 접두사 목록 ID를 참조할 수 있습니다.
- 게이트웨이 엔드포인트를 통해 Amazon S3에 액세스하는 인스턴스의 서브넷에 대한 네트워크 ACL에서 Amazon S3로 이동하는 트래픽을 허용해야 합니다. 네트워크 ACL 규칙에서 접두사 목록을 참조할 수는 없지만 Amazon S3의 접두사 목록에서 Amazon S3의 IP 주소 범위를 가져올 수 있습니다.
- S3 버킷에 액세스해야 AWS 서비스 하는를 사용하고 있는지 확인합니다. 예를 들어, 서비스에서 로그 파일이 포함된 버킷에 액세스해야 하거나 EC2 인스턴스에 드라이버 또는 에이전트를 다운로드해야 할 수 있습니다. 그렇다면 엔드포인트 정책에서 AWS 서비스 또는 리소스가 `s3:GetObject` 작업을 사용하여 이러한 버킷에 액세스하도록 허용하는지 확인합니다.
- VPC 엔드포인트를 통과하는 Amazon S3에 대한 요청에 대한 자격 증명 정책 또는 버킷 정책의 `aws:SourceIp` 조건은 사용할 수 없습니다. 대신 `aws:VpcSourceIp` 조건을 사용합니다. 또는 라우팅 테이블을 사용하여 VPC 엔드포인트를 통해 Amazon S3에 액세스할 수 있는 EC2 인스턴스를 제어할 수 있습니다.
- Amazon S3에서 수신한 영향을 받는 서브넷의 인스턴스에서 가져온 소스 IPv4 또는 IPv6 주소가 퍼블릭 주소에서 VPC의 프라이빗 주소로 변경됩니다. 엔드포인트는 네트워크 라우팅을 스위칭하고 열린 TCP 연결을 끊습니다. 퍼블릭 주소를 사용한 이전 연결은 재개되지 않습니다. 따라서 엔드포인트를 만들거나 수정할 때는 중요한 작업을 실행하지 않는 것이 좋으며 연결이 끊어진 후에는 소프트웨어가 자동으로 Amazon S3에 다시 연결할 수 있는지 테스트해야 합니다.
- 엔드포인트 연결은 VPC 외부로 확장할 수 없습니다. VPN 연결, VPC 피어링 연결, 전송 게이트웨이 또는 VPC Direct Connect 연결의 반대쪽에 있는 리소스는 게이트웨이 엔드포인트를 사용하여 Amazon S3와 통신할 수 없습니다.
- 계정의 기본 할당량은 리전당 게이트웨이 엔드포인트 20개이며 조정 가능합니다. 또한 VPC당 게이트웨이 엔드포인트는 255개로 제한됩니다.

프라이빗 DNS

Amazon S3용 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 생성할 때 비용을 최적화하도록 프라이빗 DNS를 구성할 수 있습니다.

Route 53 Resolver

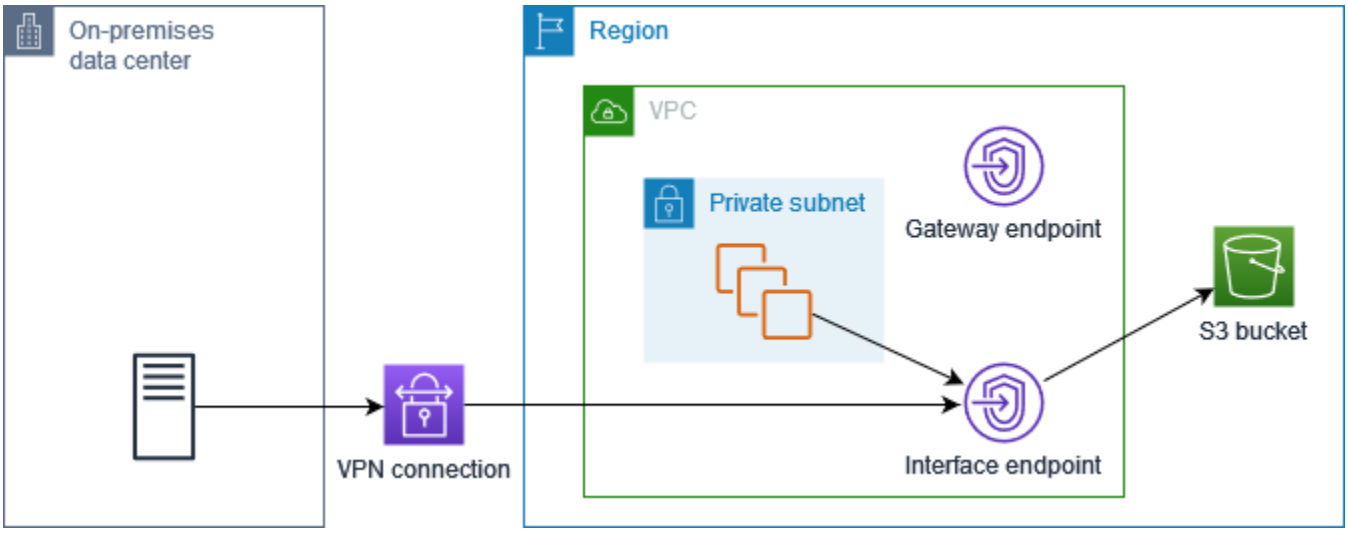
Amazon은 Route 53 Resolver라고 하는 VPC용 DNS 서버를 제공합니다. Route 53 Resolver는 프라이빗 호스팅 영역의 로컬 VPC 도메인 이름 및 레코드를 자동으로 확인합니다. 하지만 VPC 외부에서는 Route 53 Resolver를 사용할 수 없습니다. Route 53은 사용자가 VPC 외부에서 Route 53 Resolver를 사용할 수 있도록 Resolver 엔드포인트와 Resolver 규칙을 제공합니다. 인바운드 Resolver 엔드포인

트는 온프레미스 네트워크 상의 DNS 쿼리를 Route 53 Resolver로 전달합니다. 아웃바운드 Resolver 엔드포인트는 Route 53 Resolver의 DNS 쿼리를 온프레미스 네트워크로 전달합니다.

인바운드 Resolver 엔드포인트에 프라이빗 DNS만 사용하도록 Amazon S3용 인터페이스 엔드포인트를 구성하면 인바운드 Resolver 엔드포인트가 생성됩니다. 인바운드 Resolver 엔드포인트는 온프레미스에서 인터페이스 엔드포인트의 프라이빗 IP 주소로 전송되는 Amazon S3에 대한 DNS 쿼리를 해결합니다. 또한 VPC의 DNS 쿼리가 트래픽을 게이트웨이 엔드포인트로 라우팅하는 Amazon S3 퍼블릭 IP 주소로 확인되도록 Route 53 Resolver의 ALIAS 레코드를 Amazon S3 퍼블릭 호스팅 영역에 추가합니다.

프라이빗 DNS

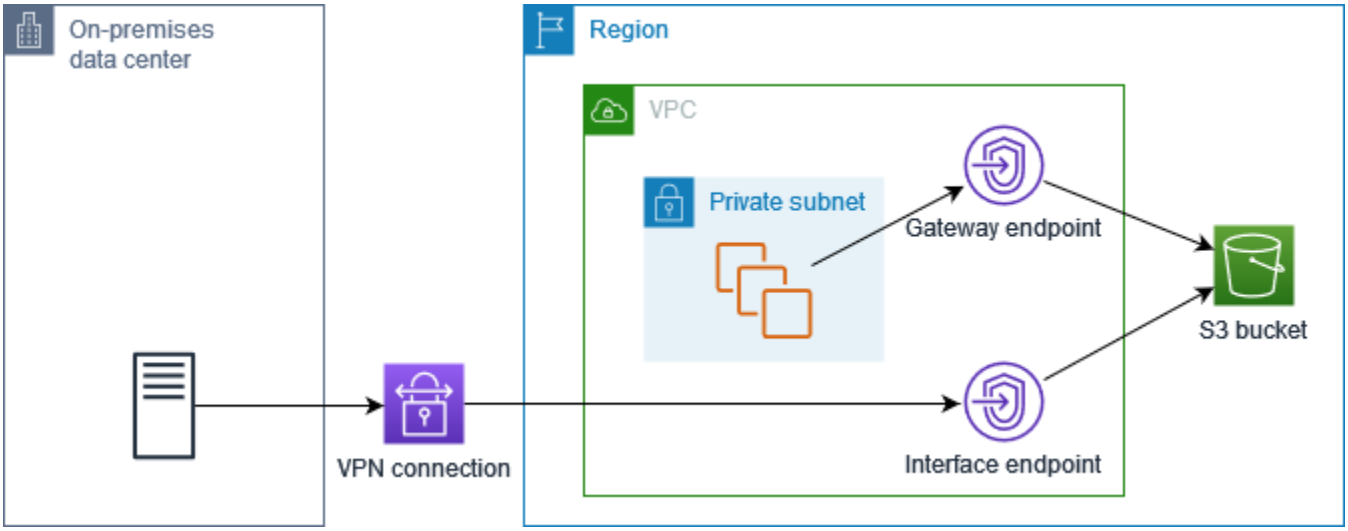
Amazon S3용 인터페이스 엔드포인트에 프라이빗 DNS를 구성하지만 인바운드 Resolver 엔드포인트에 대해서만 프라이빗 DNS를 구성하지 않는 경우, 온프레미스 네트워크와 VPC 모두의 요청이 인터페이스 엔드포인트를 사용하여 Amazon S3에 액세스합니다. 따라서 추가 요금 없이 게이트웨이 엔드포인트를 사용하는 대신 VPC의 트래픽에 인터페이스 엔드포인트를 사용하려면 비용을 지불해야 합니다.



인바운드 Resolver 엔드포인트 전용 프라이빗 DNS

인바운드 Resolver 엔드포인트에 대해서만 프라이빗 DNS를 구성하는 경우, 온프레미스 네트워크의 요청은 인터페이스 엔드포인트를 사용하여 Amazon S3에 액세스하고, VPC의 요청은 게이트웨이 엔드포인트를 사용하여 Amazon S3에 액세스합니다. 따라서 게이트웨이 엔드포인트를 사용할 수 없는 트래픽에 대해서만 인터페이스 엔드포인트를 사용하기 위해 비용을 지불하므로 비용을 최적화할 수 있습니다.

이를 구성하려면 게이트웨이 엔드포인트의 DNS 레코드 IP 유형이 인터페이스 엔드포인트와 일치하거나 이어야 합니다`service-defined`. AWS PrivateLink 다른 조합을 지원하지 않습니다. 자세한 내용은 the section called “DNS 레코드 IP 유형” 단원을 참조하십시오.



프라이빗 DNS 설정

Amazon S3용 인터페이스 엔드포인트를 생성할 때 또는 생성한 후에 Amazon S3용 인터페이스 엔드포인트에 대한 프라이빗 DNS를 구성할 수 있습니다. 자세한 내용은 the section called “VPC 엔드포인트 생성”(생성 중 구성) 또는 the section called “프라이빗 DNS 이름 활성화”(생성 후 구성)을 참조하세요.

게이트웨이 엔드포인트 생성

다음 절차에 따라 Amazon S3에 연결하는 게이트웨이 엔드포인트를 생성합니다.

콘솔을 사용하여 게이트웨이 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
5. 서비스에 유형 = 게이트웨이 필터를 추가합니다.

   Amazon S3 데이터가 범용 버킷에 저장되어 있는 경우 com.amazonaws.*region*.s3를 선택합니다.

Amazon S3 데이터가 디렉터리 버킷에 저장되어 있는 경우 com.amazonaws.*region*.s3express를 선택합니다.

6. VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
7. IP 주소 유형에서 다음 옵션 중에서 선택합니다.
   - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있으며 서비스가 IPv4 요청을 수락하는 경우에만 지원됩니다.
   - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷이며 서비스가 IPv6 요청을 수락하는 경우에만 지원됩니다.
   - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있으며 서비스가 IPv4 및 IPv6 요청을 모두 수락하는 경우에만 지원됩니다.
8. 라우팅 테이블(Route tables)에서 엔드포인트에서 사용할 라우팅 테이블을 선택합니다. 서버로 전송되는 트래픽을 가리키는 라우팅이 엔드포인트 네트워크 인터페이스에 자동으로 추가됩니다.
9. 정책(Policy)에서 모든 액세스(Full access)를 선택하여 VPC 엔드포인트를 통한 모든 리소스에 대한 모든 보안 주체의 모든 작업을 허용합니다. 또는 사용자 지정(Custom)을 선택하여 VPC 엔드포인트를 통해 리소스에 대한 작업을 수행하기 위해 보안 주체에 필요한 권한을 제어하는 VPC 엔드포인트 정책을 연결합니다.
10. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
11. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(Windows PowerShell용 도구)

버킷 정책을 사용한 액세스 제어

버킷 정책을 사용하여 특정 엔드포인트, VPCs, IP 주소 범위 및에서 버킷에 대한 액세스를 제어할 수 있습니다 AWS 계정. 이러한 예에서는 해당 사용 사례에 필요한 액세스 권한을 허용하는 정책 명령문도 있다고 가정합니다.

Example예: 특정 엔드포인트에 대한 액세스 제한

aws:sourceVpce 조건 키를 사용하여 특정 엔드포인트에 대한 액세스를 제한하는 버킷 정책을 생성할 수 있습니다. 다음 정책은 지정된 게이트웨이 엔드포인트가 사용되지 않는 한 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 거부합니다. 이 정책은 AWS Management Console을 통해 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 차단한다는 점에 유의하세요.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example예: 특정 VPC에 대한 액세스 제한

aws:sourceVpc 조건 키를 사용하여 특정 VPC에 대한 액세스를 제한하는 버킷 정책을 생성할 수 있습니다. 이 정적은 같은 VPC에 여러 엔드포인트가 구성되어 있는 경우 유용합니다. 다음 정책은 요청이 지정된 VPC에서 시작되지 않는 한 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 거부합니다. 이 정책은 AWS Management Console을 통해 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 차단한다는 점에 유의하세요.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

Example예: 특정 IP 주소 범위에 대한 액세스 제한

aws:VpcSourceIp 조건 키를 사용하여 특정 IP 주소 범위에 대한 액세스를 제한하는 버킷 정책을 생성할 수 있습니다. 다음 정책은 지정된 IP 주소에서 시작되지 않는 한 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 거부합니다. 이 정책은 AWS Management Console을 통해 지정된 작업을 사용하여 지정된 버킷에 대한 액세스를 차단한다는 점에 유의하세요.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
```

```
      }
    }
  ]
}
```

Example예: 특정의 버킷에 대한 액세스 제한 AWS 계정

`s3:ResourceAccount` 조건을 사용하여 특정 AWS 계정 의 S3 버킷에 대한 액세스를 제한하는 정책을 생성할 수 있습니다. 다음 정책은 지정된 AWS 계정에서 소유하지 않는 한 지정된 작업을 사용한 S3 버킷에 대한 액세스를 거부합니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

라우팅 테이블 연결

게이트웨이 엔드포인트와 연결된 라우팅 테이블을 변경할 수 있습니다. 라우팅 테이블을 연결하면 서비스로 전송되는 트래픽을 가리키는 라우팅이 엔드포인트 네트워크 인터페이스에 자동으로 추가됩니다. 라우팅 테이블의 연결을 해제하면 라우팅 테이블에서 엔드포인트 라우팅이 자동으로 제거됩니다.

콘솔을 사용하여 라우팅 테이블 연결하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), 라우팅 테이블 관리(Manage route tables)를 차례로 선택합니다.
5. 필요에 따라 라우팅 테이블을 선택하거나 선택 취소합니다.
6. 라우팅 테이블 수정(Modify route tables)을 선택합니다.

명령줄을 사용하여 라우팅 테이블 연결하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

VPC 엔드포인트 정책 편집

게이트웨이 엔드포인트에 대한 엔드포인트 정책을 편집하여 VPC에서 엔드포인트를 통해 Amazon S3에 대한 액세스를 제어할 수 있습니다. 엔드포인트 정책을 업데이트할 경우 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다. 기본 정책에서는 모든 액세스를 허용합니다. 자세한 내용은 엔드포인트 정책 단원을 참조하십시오.

콘솔을 사용하여 엔드포인트 정책 변경

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), 정책 관리(Manage policy)를 선택합니다.
5. 모든 액세스(Full Access)를 선택하여 서비스에 대한 전체 액세스를 허용하거나 사용자 지정(Custom)을 선택하고 사용자 지정 정책을 연결합니다.
6. 저장을 선택합니다.

다음은 Amazon S3에 액세스하기 위한 엔드포인트 정책의 예입니다.

Example예: 특정 버킷에 대한 액세스 제한

특정 S3 버킷에 대해서만 액세스를 제한하는 정책을 생성할 수 있습니다. 이는 VPC AWS 서비스 에 S3 버킷을 사용하는 다른이 있는 경우에 유용합니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example예: 특정 IAM 역할에 대한 액세스 제한

특정 IAM 역할에 대한 액세스를 제한하는 정책을 생성할 수 있습니다. `aws:PrincipalArn`을 사용하여 보안 주체에 액세스 권한을 부여해야 합니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
```

```
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example예: 특정 계정의 사용자에 대한 액세스 제한

특정 계정에 대한 액세스를 제한하는 정책을 생성할 수 있습니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

게이트웨이 엔드포인트 삭제

게이트웨이 엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다. 게이트웨이 엔드포인트를 삭제하면 서브넷 라우팅 테이블에서 엔드포인트 라우팅이 제거됩니다.

프라이빗 DNS가 활성화되어 있으면 게이트웨이 엔드포인트를 삭제할 수 없습니다.

콘솔을 사용하여 게이트웨이 엔드포인트 삭제

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 표시되면 **delete**를 입력합니다.
6. 삭제를 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(Windows PowerShell용 도구)

Amazon DynamoDB에 대한 게이트웨이 엔드포인트

VPC에서 게이트웨이 VPC 엔드포인트를 사용하여 Amazon DynamoDB에 액세스할 수 있습니다. 게이트웨이 엔드포인트를 생성한 후 VPC에서 DynamoDB로 전송되는 트래픽에 대해 해당 엔드포인트를 라우팅 테이블의 대상으로 추가할 수 있습니다.

게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다.

DynamoDB는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다. 게이트웨이 엔드포인트를 사용하면 VPC 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고 추가 비용 없이 VPC에서 DynamoDB에 액세스할 수 있습니다. 그러나 게이트웨이 엔드포인트는 온프레미스 네트워크, 다른 AWS 리전의 피어링된 VPCs 또는 전송 게이트웨이를 통한 액세스를 허용하지 않습니다. 이러한 시나리오에서는 추가 비용을 지불한 후 사용할 수 있는 인터페이스 엔드포인트를 사용해야 합니다. 자세한 내용은 Amazon DynamoDB 개발자 가이드의 DynamoDB용 VPC 엔드포인트 유형을 참조하세요.

내용

- 고려 사항
- 게이트웨이 엔드포인트 생성
- IAM 정책을 사용하여 액세스 제어
- 라우팅 테이블 연결
- VPC 엔드포인트 정책 편집

- 게이트웨이 엔드포인트 삭제

고려 사항

- 게이트웨이 엔드포인트는 해당 엔드포인트를 생성한 리전에서만 사용할 수 있습니다. DynamoDB 테이블과 동일한 리전에서 게이트웨이 엔드포인트를 생성해야 합니다.
- Amazon DNS 서버를 사용 중인 경우 VPC에 대해 DNS 호스트 이름 및 DNS 확인을 모두 활성화해야 합니다. 또한 자체 DNS 서버를 사용하는 경우 DynamoDB에 대한 요청이 AWS에서 유지 관리하는 IP 주소로 올바르게 확인되어야 합니다.
- 게이트웨이 엔드포인트를 통해 DynamoDB에 액세스하는 인스턴스의 보안 그룹에 대한 규칙은 DynamoDB에서 이동하는 트래픽을 허용해야 합니다. 보안 그룹 규칙에서 DynamoDB 접두사 목록의 ID를 참조할 수 있습니다.
- 게이트웨이 엔드포인트를 통해 DynamoDB에 액세스하는 인스턴스의 서브넷에 대한 네트워크 ACL은 DynamoDB에서 이동하는 트래픽을 허용해야 합니다. 네트워크 ACL 규칙의 접두사 목록은 참조할 수 없지만 DynamoDB의 접두사 목록에서 DynamoDB의 IP 주소 범위를 가져올 수 있습니다.
- AWS CloudTrail 를 사용하여 DynamoDB 작업을 로깅하는 경우 로그 파일에는 서비스 소비자 VPC에 있는 EC2 인스턴스의 프라이빗 IP 주소와 엔드포인트를 통해 수행된 모든 요청에 대한 게이트웨이 엔드포인트의 ID가 포함됩니다.
- 게이트웨이 엔드포인트는 IPv4 트래픽만 지원합니다.
- 해당 서브넷에 있는 인스턴스의 원본 IPv4 주소는 퍼블릭 IPv4 주소에서 VPC의 프라이빗 IPv4 주소로 변경됩니다. 엔드포인트는 네트워크 라우팅을 스위칭하고 열린 TCP 연결을 끊습니다. 퍼블릭 IPv4 주소를 사용한 이전 연결은 다시 시작되지 않습니다. 따라서 게이트웨이 엔드포인트를 생성하거나 수정할 때는 중요한 작업을 실행하지 않는 것이 좋습니다. 또는 연결이 끊어질 경우 소프트웨어에서 DynamoDB에 자동으로 다시 연결할 수 있는지 테스트하세요.
- 엔드포인트 연결은 VPC 외부로 확장할 수 없습니다. VPN 연결, VPC 피어링 연결, 전송 게이트웨이 또는 VPC 연결의 반대쪽 Direct Connect 에 있는 리소스는 게이트웨이 엔드포인트를 사용하여 DynamoDB와 통신할 수 없습니다.
- 계정의 기본 할당량은 리전당 게이트웨이 엔드포인트 20개이며 조정 가능합니다. 또한 VPC당 게이트웨이 엔드포인트는 255개로 제한됩니다.

게이트웨이 엔드포인트 생성

다음 절차에 따라 DynamoDB에 연결하는 게이트웨이 엔드포인트를 생성합니다.

콘솔을 사용하여 게이트웨이 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
5. 서비스에서 유형 = 게이트웨이 필터를 추가하고 com.amazonaws.*region*.dynamodb를 선택합니다.
6. VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
7. 라우팅 테이블(Route tables)에서 엔드포인트에서 사용할 라우팅 테이블을 선택합니다. 서버로 전송되는 트래픽을 가리키는 라우팅이 엔드포인트 네트워크 인터페이스에 자동으로 추가됩니다.
8. 정책(Policy)에서 모든 액세스(Full access)를 선택하여 VPC 엔드포인트를 통한 모든 리소스에 대한 모든 보안 주체의 모든 작업을 허용합니다. 또는 사용자 지정(Custom)을 선택하여 VPC 엔드포인트를 통해 리소스에 대한 작업을 수행하기 위해 보안 주체에 필요한 권한을 제어하는 VPC 엔드포인트 정책을 연결합니다.
9. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
10. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(Windows PowerShell용 도구)

IAM 정책을 사용하여 액세스 제어

특정 VPC 엔드포인트를 사용하여 DynamoDB 테이블에 액세스할 수 있는 IAM 보안 주체를 제어하는 IAM 정책을 생성할 수 있습니다.

Example예: 특정 엔드포인트에 대한 액세스 제한

aws:sourceVpce 조건 키를 사용하여 특정 VPC 엔드포인트에 대한 액세스를 제한하는 정책을 생성할 수 있습니다. 다음 정책은 지정된 VPC 엔드포인트를 사용하지 않는 경우 계정의 DynamoDB 테이블에 대한 액세스를 거부합니다. 이 예제에서는 해당 사용 사례에 필요한 액세스를 허용하는 정책 문도 있다고 가정합니다.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example예: 특정 IAM 역할의 액세스 허용

특정 IAM 역할을 사용한 액세스를 허용하는 정책을 생성할 수 있습니다. 다음 정책은 지정된 IAM 역할에 액세스 권한을 부여합니다.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
```

```
      }
   ]
}
```

Example예: 특정 계정의 액세스 허용

특정 계정의 액세스만 허용하는 정책을 생성할 수 있습니다. 다음 정책은 지정된 계정의 사용자에 액세스 권한을 부여합니다.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

라우팅 테이블 연결

게이트웨이 엔드포인트와 연결된 라우팅 테이블을 변경할 수 있습니다. 라우팅 테이블을 연결하면 서비스로 전송되는 트래픽을 가리키는 라우팅이 엔드포인트 네트워크 인터페이스에 자동으로 추가됩니다. 라우팅 테이블의 연결을 해제하면 라우팅 테이블에서 엔드포인트 라우팅이 자동으로 제거됩니다.

콘솔을 사용하여 라우팅 테이블 연결하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.

3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), 라우팅 테이블 관리(Manage route tables)를 차례로 선택합니다.
5. 필요에 따라 라우팅 테이블을 선택하거나 선택 취소합니다.
6. 라우팅 테이블 수정(Modify route tables)을 선택합니다.

명령줄을 사용하여 라우팅 테이블 연결하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

VPC 엔드포인트 정책 편집

게이트웨이 엔드포인트에 대한 엔드포인트 정책을 편집하여 VPC에서 엔드포인트를 통해 DynamoDB에 대한 액세스를 제어할 수 있습니다. 엔드포인트 정책을 업데이트할 경우 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다. 기본 정책에서는 모든 액세스를 허용합니다. 자세한 내용은 엔드포인트 정책 단원을 참조하십시오.

콘솔을 사용하여 엔드포인트 정책 변경

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), 정책 관리(Manage policy)를 선택합니다.
5. 모든 액세스(Full Access)를 선택하여 서비스에 대한 전체 액세스를 허용하거나 사용자 지정(Custom)을 선택하고 사용자 지정 정책을 연결합니다.
6. 저장을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 수정하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

다음은 DynamoDB에 액세스하기 위한 엔드포인트 정책의 예입니다.

Example예제: 읽기 전용 액세스 허용

액세스를 읽기 전용 액세스로 제한하는 정책을 생성할 수 있습니다. 다음 정책은 DynamoDB 테이블을 열거하고 설명할 수 있는 권한을 부여합니다.

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

Example예: 특정 테이블에 대한 액세스 제한

특정 DynamoDB 테이블에 대한 액세스를 제한하는 정책을 생성할 수 있습니다. 다음 정책은 지정된 DynamoDB 테이블에 대한 액세스를 허용합니다.

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
```

```
}
```

게이트웨이 엔드포인트 삭제

게이트웨이 엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다. 게이트웨이 엔드포인트를 삭제하면 서브넷 라우팅 테이블에서 엔드포인트 라우팅이 제거됩니다.

콘솔을 사용하여 게이트웨이 엔드포인트 삭제

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 표시되면 **`delete`**를 입력합니다.
6. 삭제를 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(Windows PowerShell용 도구)

AWS PrivateLink를 통한 SaaS 제품 액세스

AWS PrivateLink를 사용하면 SaaS 제품에 비공개로 액세스하여 해당 제품을 자체 VPC에서 실행하는 것처럼 이용할 수 있습니다.

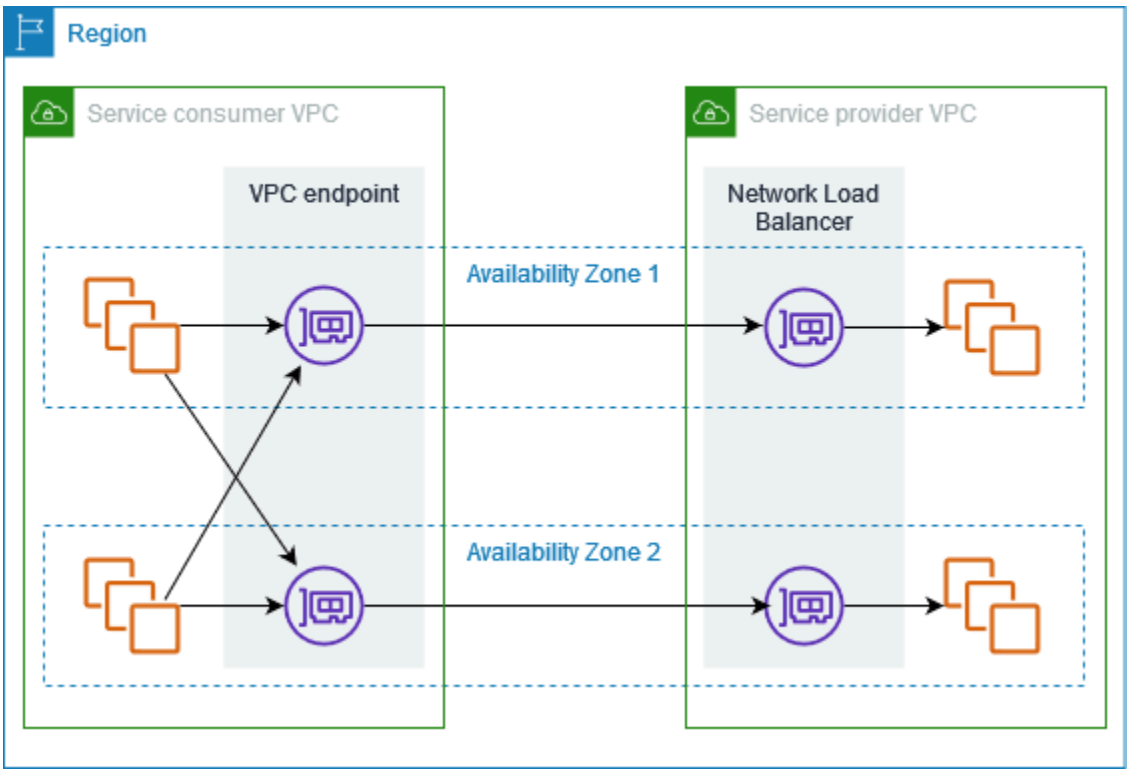
내용

개요

AWS Marketplace를 통해 AWS PrivateLink 기반의 SaaS 제품을 검색, 구매 및 프로비저닝할 수 있습니다. 자세한 내용은 AWS PrivateLink를 사용하여 SaaS 애플리케이션에 안전하게 비공개로 액세스를 참조하세요.

AWS 파트너를 통해 AWS PrivateLink 기반 SaaS 제품을 찾을 수도 있습니다. 자세한 내용은 AWS PrivateLink 파트너를 참조하세요.

다음 다이어그램은 VPC 엔드포인트를 사용하여 SaaS 제품에 연결하는 방법을 보여줍니다. 서비스 공급자는 엔드포인트 서비스를 생성하고 고객에게 엔드포인트 서비스에 대한 액세스 권한을 부여합니다. 서비스 소비자는 VPC의 서브넷 하나 이상과 엔드포인트 서비스 간에 연결을 설정하는 인터페이스 VPC 엔드포인트를 생성합니다.



인터페이스 엔드포인트 생성

다음 절차에 따라 SaaS 제품에 연결하는 인터페이스 VPC 엔드포인트를 생성합니다.

요구 사항

서비스를 구독합니다.

파트너 서비스에 대한 인터페이스 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. AWS Marketplace에서 서비스를 구매한 경우 다음을 수행합니다.
   a. 유형에서 AWS Marketplace 서비스를 선택합니다.
   b. 이 서비스를 선택합니다.
5. AWS Service Ready 지정이 있는 서비스를 구독한 경우 다음을 수행합니다.
   a. 유형에서 PrivateLink Ready 파트너 서비스를 선택합니다.

b. 서비스 이름을 입력한 후 서비스 확인을 선택합니다.

6. VPC에서 제품에 액세스하는 데 사용할 VPC를 선택합니다.
7. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다.
8. 보안 그룹에서 엔드포인트 네트워크 인터페이스에 연결할 보안 그룹을 선택합니다. 보안 그룹 규칙에서 VPC의 리소스와 엔드포인트 네트워크 인터페이스 간의 트래픽을 허용해야 합니다.
9. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
10. 엔드포인트 생성을 선택합니다.

인터페이스 엔드포인트 구성하기

인터페이스 엔드포인트를 구성하는 방법에 대한 자세한 내용은 the section called “인터페이스 엔드포인트 구성” 섹션을 참조하세요.

AWS PrivateLink를 통해 가상 어플라이언스 액세스

Gateway Load Balancer를 사용하여 네트워크 가상 어플라이언스 플릿에 트래픽을 분산할 수 있습니다. 어플라이언스는 보안 검사, 규정 준수, 정책 제어 및 기타 네트워킹 서비스에 사용할 수 있습니다. VPC 엔드포인트 서비스를 생성할 때 Gateway Load Balancer를 지정합니다. 다른 AWS 보안 주체는 Gateway Load Balancer 엔드포인트를 생성하여 엔드포인트 서비스에 액세스합니다.

요금

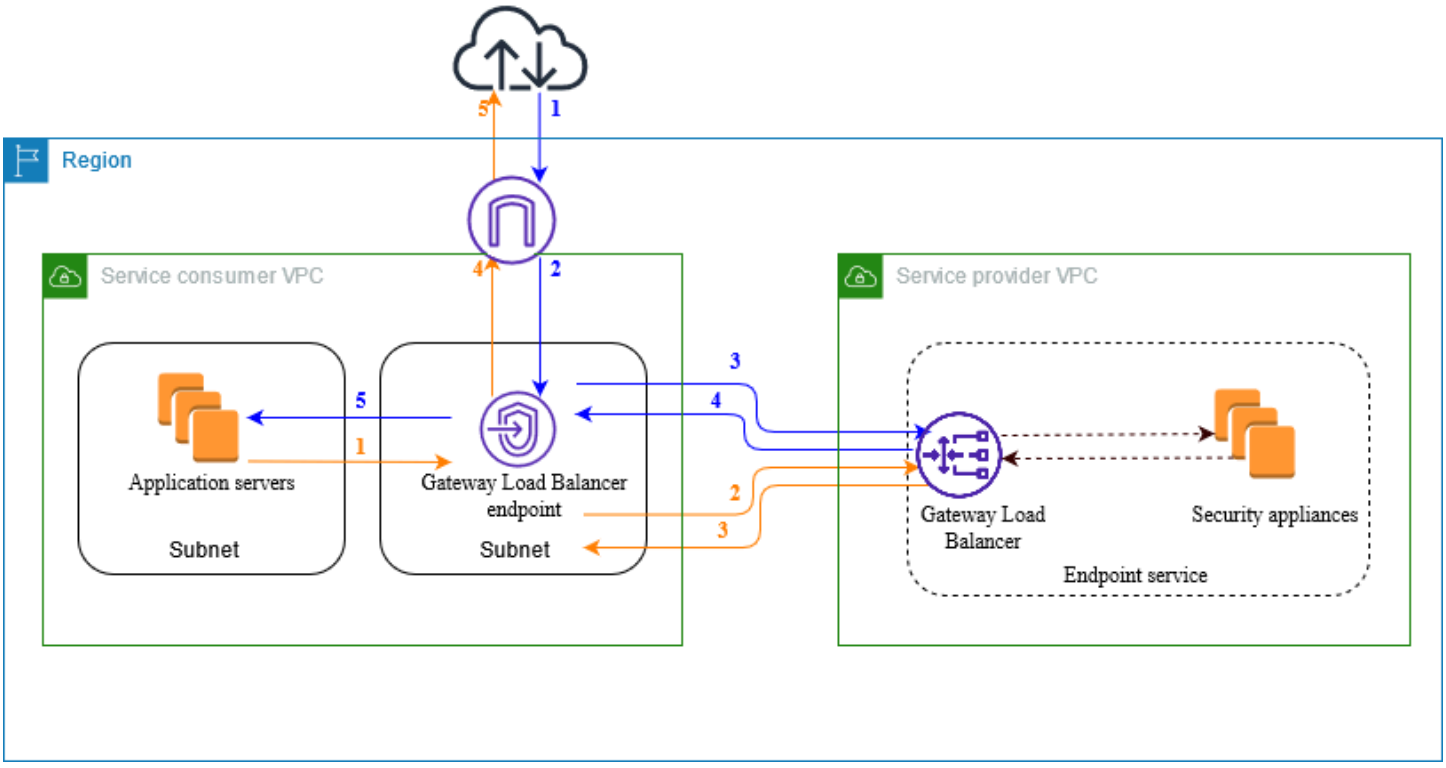
Gateway Load Balancer 엔드포인트가 각 가용 영역에 프로비저닝되는 시간에 대해 시간당 요금이 청구됩니다. 또한 처리된 데이터의 GB당 요금이 청구됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

내용

자세한 내용은 Gateway Load Balancers를 참조하세요.

개요

다음 다이어그램은 애플리케이션 서버가 AWS PrivateLink를 통해 보안 어플라이언스에 액세스하는 방법을 보여줍니다. 애플리케이션 서버는 서비스 소비자 VPC의 서브넷에서 실행됩니다. 동일한 VPC의 다른 서브넷에서 Gateway Load Balancer 엔드포인트를 생성합니다. 인터넷 게이트웨이를 통해 서비스 소비자 VPC로 들어오는 모든 트래픽은 먼저 검사를 위해 Gateway Load Balancer 엔드포인트로 라우팅된 후 대상 서브넷으로 라우팅됩니다. 마찬가지로 애플리케이션 서버에서 나가는 모든 트래픽은 검사할 수 있도록 먼저 Gateway Load Balancer 엔드포인트로 라우팅된 후 인터넷 게이트웨이로 라우팅됩니다.



인터넷에서 애플리케이션 서버로의 트래픽(파란색 화살표):

1. 트래픽이 인터넷 게이트웨이를 통해 서비스 소비자 VPC로 들어갑니다.
2. 라우팅 테이블 구성에 따라 트래픽이 Gateway Load Balancer 엔드포인트로 전송됩니다.
3. 보안 어플라이언스를 통한 검사를 위해 트래픽이 Gateway Load Balancer로 전송됩니다.
4. 검사 후 트래픽이 Gateway Load Balancer 엔드포인트로 다시 전송됩니다.
5. 라우팅 테이블 구성에 따라 트래픽이 애플리케이션 서버로 전송됩니다.

애플리케이션 서버에서 인터넷으로의 트래픽(주황색 화살표):

1. 라우팅 테이블 구성에 따라 트래픽이 Gateway Load Balancer 엔드포인트로 전송됩니다.
2. 보안 어플라이언스를 통한 검사를 위해 트래픽이 Gateway Load Balancer로 전송됩니다.
3. 검사 후 트래픽이 Gateway Load Balancer 엔드포인트로 다시 전송됩니다.
4. 라우팅 테이블 구성에 따라 트래픽이 인터넷 게이트웨이로 전송됩니다.
5. 트래픽이 인터넷으로 다시 라우팅됩니다.

IP 주소 유형

서비스 공급자는 보안 어플라이언스가 IPv4만 지원하는 경우에도 IPv4, IPv6 또는 IPv4 및 IPv6 모두를 통해 서비스 소비자에게 서비스 엔드포인트를 제공할 수 있습니다. 듀얼 스택 지원을 활성화하는 경우 기존 소비자는 계속 IPv4를 사용하여 서비스에 액세스할 수 있고 새 소비자는 IPv6를 사용하여 서비스에 액세스할 수 있습니다.

Gateway Load Balancer 엔드포인트가 IPv4를 지원하는 경우 엔드포인트 네트워크 인터페이스는 IPv4 주소를 갖습니다. Gateway Load Balancer 엔드포인트가 IPv6를 지원하는 경우 엔드포인트 네트워크 인터페이스는 IPv6 주소를 갖습니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이 활성화됩니다.

엔드포인트 서비스에 대해 IPv6를 활성화하기 위한 요구 사항

- 엔드포인트 서비스의 VPC와 서브넷에는 연결된 IPv6 CIDR 블록이 있어야 합니다.
- 엔드포인트 서비스의 Gateway Load Balancer는 듀얼 스택 IP 주소 유형을 사용해야 합니다. 보안 어플라이언스는 IPv6 트래픽을 지원할 필요가 없습니다.

Gateway Load Balancer 엔드포인트에 대해 IPv6를 활성화하기 위한 요구 사항

- 엔드포인트 서비스에는 IPv6 지원이 포함된 IP 주소 유형이 있어야 합니다.
- Gateway Load Balancer 엔드포인트의 IP 주소 유형이 다음에 설명된 대로 Gateway Load Balancer 엔드포인트의 서브넷과 호환되어야 합니다.
  - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.
  - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
  - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.
- 서비스 소비자 VPC의 서브넷에 대한 라우팅 테이블은 IPv6 트래픽을 라우팅해야 하며 이러한 서브넷의 네트워크 ACL은 IPv6 트래픽을 허용해야 합니다.

라우팅

트래픽을 엔드포인트 서비스로 라우팅하려면 Gateway Load Balancer 엔드포인트를 해당 ID를 사용하여 라우팅 테이블에서 대상으로 지정합니다. 위 다이어그램의 경우 다음과 같이 라우팅 테이블에 라우팅을 추가합니다. Gateway Load Balancer 엔드포인트를 대상으로 사용하는 경우 접두사 목록을 대상으로 지정할 수 없습니다. 이 표에서는 듀얼 스택 구성의 경우 IPv6 라우트가 포함됩니다.

인터넷 게이트웨이의 라우팅 테이블

이 라우팅 테이블에는 애플리케이션 서버로 전송되는 트래픽을 Gateway Load Balancer 엔드포인트로 보내는 라우팅이 있어야 합니다.

대상 주소	대상
VPC IPv4 CIDR	로컬
VPC IPv6 CIDR	로컬
###### ### IPv4 CIDR	*vpc-endpoint-id*
###### ### IPv6 CIDR	*vpc-endpoint-id*

애플리케이션 서버가 있는 서브넷의 라우팅 테이블

이 라우팅 테이블에는 모든 트래픽을 애플리케이션 서버에서 Gateway Load Balancer 엔드포인트로 보내는 라우팅이 있어야 합니다.

대상 주소	대상
VPC IPv4 CIDR	로컬
VPC IPv6 CIDR	로컬
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Gateway Load Balancer 엔드포인트가 있는 서브넷의 라우팅 테이블

이 라우팅 테이블에서는 검사에서 반환되는 트래픽을 최종 대상 주소로 전송해야 합니다. 인터넷에서 시작된 트래픽의 경우 로컬 라우팅은 트래픽을 애플리케이션 서버로 보냅니다. 애플리케이션 서버에서 시작된 트래픽의 경우 모든 트래픽을 인터넷 게이트웨이로 전송하는 라우팅을 추가합니다.

대상 주소	대상
VPC IPv4 CIDR	로컬
VPC IPv6 CIDR	로컬
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

검사 시스템을 Gateway Load Balancer 엔드포인트 서비스로 생성

엔드포인트 서비스라고 하는 AWS PrivateLink 기반 자체 서비스를 생성할 수 있습니다. 서비스를 생성하면 서비스 공급자이고 해당 서비스에 대한 연결을 생성하는 AWS 보안 주체는 서비스 소비자입니다.

엔드포인트 서비스에는 Network Load Balancer나 Gateway Load Balancer가 필요합니다. 여기서는 Gateway Load Balancer를 사용하여 엔드포인트 서비스를 생성합니다. Network Load Balancer를 사용하여 엔드포인트 서비스를 생성하는 방법에 대한 자세한 내용은 엔드포인트 서비스 생성 섹션을 참조하세요.

내용

- 고려 사항
- 사전 조건
- 엔드포인트 서비스 생성
- 엔드포인트 서비스를 사용할 수 있도록 설정

고려 사항

- 엔드포인트 서비스는 해당 서비스를 생성한 리전에서 사용할 수 있습니다.
- 서비스 소비자가 엔드포인트 서비스에 대한 정보를 검색할 때 서비스 공급자와 공통되는 가용 영역만 볼 수 있습니다. 서비스 공급자와 서비스 소비자가 다른 계정에 있는 경우 각 AWS 계정의 다른 물리적 가용 영역에 `us-east-1a`와 같은 가용 영역 이름이 매핑될 수 있습니다. AZ ID를 사용하여 서

비스의 가용 영역을 일관되게 식별할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 AZ ID를 참조하세요.

- AWS PrivateLink 리소스에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 섹션을 참조하세요.

사전 조건

- 서비스를 제공할 가용 영역에서 둘 이상의 서브넷을 사용하여 서비스 공급자 VPC를 생성합니다. 하나의 서브넷은 보안 어플라이언스 인스턴스용이고 다른 하나는 Gateway Load Balancer용입니다.
- 서비스 공급자 VPC에서 Gateway Load Balancer Balancer를 생성합니다. 엔드포인트 서비스에서 IPv6 지원을 활성화하려는 경우 Gateway Load Balancer 듀얼 스택 지원을 활성화해야 합니다. 자세한 내용은 Gateway Load Balancer 시작하기를 참조하세요.
- 서비스 공급자 VPC에서 보안 어플라이언스를 시작하고 로드 밸런서 대상 그룹에 등록합니다.

엔드포인트 서비스 생성

Gateway Load Balancer를 사용하여 엔드포인트 서비스를 생성하려면 다음 절차를 따르세요.

콘솔을 사용하여 엔드포인트 서비스 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스 생성(Create endpoint service)을 선택합니다.
4. 로드 밸런서 유형(Load balancer type)에서 게이트웨이(Gateway)를 선택합니다.
5. Available load balancers(사용 가능한 로드 밸런서)에서 Gateway Load Balancer를 선택합니다.
6. Require acceptance for endpoint(엔드포인트 수락 필요)에서 엔드포인트 서비스에 대한 연결 요청을 수동으로 수락하도록 하려면 Acceptance required(수락 필요)를 선택합니다. 그러지 않으면 자동으로 요청이 수락됩니다.
7. Supported IP address types(지원되는 IP 주소 유형)에서 다음 중 하나를 수행합니다.
   - IPv4 선택 - IPv4 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.
   - IPv6 선택 - IPv6 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.
   - IPv4 및 IPv6 선택 - IPv4 및 IPv6 요청을 모두 수락하도록 엔드포인트 서비스를 활성화합니다.
8. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.

9. 생성(Create)을 선택합니다.

명령줄을 사용하여 엔드포인트 서비스 생성하기

- create-vpc-endpoint-service-configuration(AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

엔드포인트 서비스를 사용할 수 있도록 설정

서비스 공급자는 서비스를 서비스 소비자가 사용할 수 있도록 하려면 다음을 수행해야 합니다.

- 각 서비스 소비자가 엔드포인트 서비스에 연결할 수 있도록 권한을 추가합니다. 자세한 내용은 the section called “권한 관리” 섹션을 참조하세요.
- 서비스 소비자가 인터페이스 엔드포인트를 생성하여 서비스에 연결할 수 있도록 서비스 소비자에게 서비스의 이름과 지원되는 가용 영역을 제공합니다. 자세한 내용은 아래 절차를 참조하세요.
- 서비스 소비자의 엔드포인트 연결 요청을 수락합니다. 자세한 내용은 the section called “연결 요청 수락 또는 거부”을 참조하세요.

AWS 보안 주체는 Gateway Load Balancer 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Gateway Load Balancer 엔드포인트 생성 섹션을 참조하세요.

Gateway Load Balancer 엔드포인트를 사용하여 검사 시스템 액세스

Gateway Load Balancer 엔드포인트를 생성하여 AWS PrivateLink 기반 엔드포인트 서비스에 연결할 수 있습니다.

VPC에서 지정하는 각 서브넷에 대해 서브넷에 엔드포인트 네트워크 인터페이스가 생성되고 해당 인터페이스에 서브넷 주소 범위의 프라이빗 IP 주소가 할당됩니다. 엔드포인트 네트워크 인터페이스는 요청자가 관리하는 네트워크 인터페이스로, AWS 계정에서 확인할 수 있지만 직접 관리할 수는 없습니다.

이용 시 시간당 사용 요금 및 데이터 처리 요금이 청구됩니다. 자세한 내용은 Gateway Load Balancer 엔드포인트 요금을 참조하세요.

내용

고려 사항

- 서비스 소비자 VPC에서는 가용 영역을 하나만 선택할 수 있습니다. 나중에 이 서브넷을 변경할 수 없습니다. 다른 서브넷에서 Gateway Load Balancer 엔드포인트를 사용하려면 새 Gateway Load Balancer 엔드포인트를 생성해야 합니다.
- 서비스별로 가용 영역당 하나의 Gateway Load Balancer 엔드포인트를 생성할 수 있고 Gateway Load Balancer가 지원하는 가용 영역을 선택해야 합니다. 서비스 공급자와 서비스 소비자가 다른 계정에 있는 경우 각 AWS 계정의 다른 물리적 가용 영역에 `us-east-1a`와 같은 가용 영역 이름이 매핑될 수 있습니다. AZ ID를 사용하여 서비스의 가용 영역을 일관되게 식별할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 AZ ID를 참조하세요.
- 엔드포인트 서비스를 사용하려면 먼저 서비스 공급자가 연결 요청을 수락해야 합니다. 서비스에서는 VPC 엔드포인트를 통해 VPC의 리소스에 대한 요청을 시작할 수 없습니다. 엔드포인트는 VPC의 리소스에서 시작된 트래픽에 대한 응답만 반환합니다.
- 각 Gateway Load Balancer 엔드포인트는 가용 영역당 최대 10Gbps의 대역폭을 지원하고 최대 100Gbps까지 자동으로 조정됩니다.
- 엔드포인트 서비스가 여러 Gateway Load Balancer에 연결되어 있는 경우 Gateway Load Balancer 엔드포인트는 가용 영역당 한 개의 로드 밸런서에만 연결을 설정합니다.
- 트래픽을 동일한 가용 영역 내에 유지하려면 트래픽을 전송할 각 가용 영역에 Gateway Load Balancer 엔드포인트를 생성하는 것이 좋습니다.
- 대상이 Network Load Balancer와 동일한 VPC 있더라도 트래픽이 Gateway Load Balancer 엔드포인트를 통해 라우팅되면 네트워크 로드 밸런서 클라이언트 IP 보존이 지원되지 않습니다.
- 애플리케이션 서버와 Gateway Load Balancer 엔드포인트가 동일한 서브넷에 있는 경우 애플리케이션 서버에서 Gateway Load Balancer 엔드포인트로의 트래픽에 대해 NACL 규칙이 평가됩니다.
- 송신 전용 인터넷 게이트웨이와 함께 Gateway Load Balancer를 사용하는 경우 IPv6 트래픽이 삭제됩니다. 대신 인터넷 게이트웨이와 인바운드 방화벽 규칙을 사용하세요.

- AWS PrivateLink 리소스에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 섹션을 참조하세요.

사전 조건

- 서비스에 액세스할 가용 영역에서 2개 이상의 서브넷이 있는 서비스 소비자 VPC 생성합니다. 하나의 서브넷은 애플리케이션 서버용이고 다른 하나는 Gateway Load Balancer 엔드포인트용입니다.
- 엔드포인트 서비스에서 지원하는 가용 영역을 확인하려면 콘솔이나 describe-vpc-endpoint-services 명령을 사용하여 엔드포인트 서비스를 설명합니다.
- 리소스가 네트워크 ACL를 사용하는 서브넷에 있는 경우 네트워크 ACL에서 엔드포인트 네트워크 인터페이스와 VPC의 리소스 간 트래픽을 허용하는지 확인합니다.

엔드포인트 생성

다음 절차에 따라 검사 시스템용 엔드포인트 서비스에 연결하는 Gateway Load Balancer 엔드포인트를 생성합니다.

콘솔을 사용하여 Gateway Load Balancer 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 유형에서 NLBs 및 GWLBs를 사용하는 엔드포인트 서비스를 선택합니다.
5. Service name(서비스 이름)에 서비스의 이름을 입력한 다음 Verify service(서비스 확인)를 선택합니다.
6. VPC에서 엔드포인트 서비스에 액세스할 서브넷을 선택합니다.
7. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다.
8. IP 주소 유형에서 다음 옵션 중에서 선택합니다.

    - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.
    - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
    - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

9. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
10. 엔드포인트 생성을 선택합니다. 초기 상태는 `pending acceptance`입니다.

명령줄을 사용하여 Gateway Load Balancer 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(Windows PowerShell용 도구)

라우팅 구성

다음 절차에 따라 서비스 소비자 VPC의 라우팅 테이블을 구성합니다. 이 테이블을 사용하여 보안 어플라이언스에서 애플리케이션 서버로 전송되는 인바운드 트래픽에 대한 보안 검사를 수행할 수 있습니다. 자세한 내용은 the section called “라우팅” 섹션을 참조하세요.

콘솔을 사용하여 라우팅 구성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 라우팅 테이블(Route Tables)을 선택합니다.
3. 인터넷 게이트웨이의 라우팅 테이블을 선택하고 다음을 수행합니다.
   a. 작업(Actions), 라우팅 편집(Edit routes)을 선택합니다.
   b. IPv4를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상(Destination)에 애플리케이션 서버에 대한 서브넷의 IPv4 CIDR 블록을 입력합니다. 대상(Target)에서 VPC 엔드포인트를 선택합니다.
   c. IPv6를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상(Destination)에 애플리케이션 서버에 대한 서브넷의 IPv6 CIDR 블록을 입력합니다. 대상(Target)에서 VPC 엔드포인트를 선택합니다.
   d. 변경 사항 저장을 선택합니다.
4. 애플리케이션 서버가 있는 서브넷의 라우팅 테이블을 선택하고 다음을 수행합니다.
   a. 작업(Actions), 라우팅 편집(Edit routes)을 선택합니다.
   b. IPv4를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상 주소(Destination)에 **`0.0.0.0/0`**을 입력합니다. 대상(Target)에서 VPC 엔드포인트를 선택합니다.
   c. IPv6를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상 주소(Destination)에 **`::/0`**을 입력합니다. 대상(Target)에서 VPC 엔드포인트를 선택합니다.

d. 변경 사항 저장을 선택합니다.

5. Gateway Load Balancer 엔드포인트가 있는 서브넷의 라우팅 테이블을 선택하고 다음을 수행합니다.

   a. 작업(Actions), 라우팅 편집(Edit routes)을 선택합니다.
   b. IPv4를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상 주소(Destination)에 **`0.0.0.0/0`**을 입력합니다. 대상(Target)에서 인터넷 게이트웨이를 선택합니다.
   c. IPv6를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. 대상 주소(Destination)에 **`::/0`**을 입력합니다. 대상(Target)에서 인터넷 게이트웨이를 선택합니다.
   d. 변경 사항 저장을 선택합니다.

명령줄을 사용하여 라우팅 구성하기

- create-route(AWS CLI)
- New-EC2Route(Windows PowerShell용 도구)

태그 관리

Gateway Load Balancer 엔드포인트에 태그를 지정하면 조직의 요구에 따라 이를 식별 또는 분류할 수 있습니다.

콘솔을 사용하여 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택합니다.
4. 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그 키와 태크 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장을 선택합니다.

명령줄을 사용하여 태그 관리하기

- create-tags 및 delete-tags(AWS CLI)
- New-EC2Tag 및 Remove-EC2Tag(Windows PowerShell용 도구)

Gateway Load Balancer 엔드포인트 삭제

엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다. Gateway Load Balancer 엔드포인트를 삭제하면 엔드포인트 네트워크 인터페이스도 삭제됩니다. 라우팅 테이블에 엔드포인트를 가리키는 라우팅이 있으면 Gateway Load Balancer 엔드포인트를 삭제할 수 없습니다.

Gateway Load Balancer 엔드포인트 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트(Endpoints)를 선택한 후 엔드포인트를 선택합니다.
3. 작업(Actions), 엔드포인트 삭제(Delete Endpoint)를 차례로 선택합니다.
4. 확인 화면에서 예, 삭제(Yes, Delete)를 선택합니다.

Gateway Load Balancer 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(AWS Tools for Windows PowerShell)

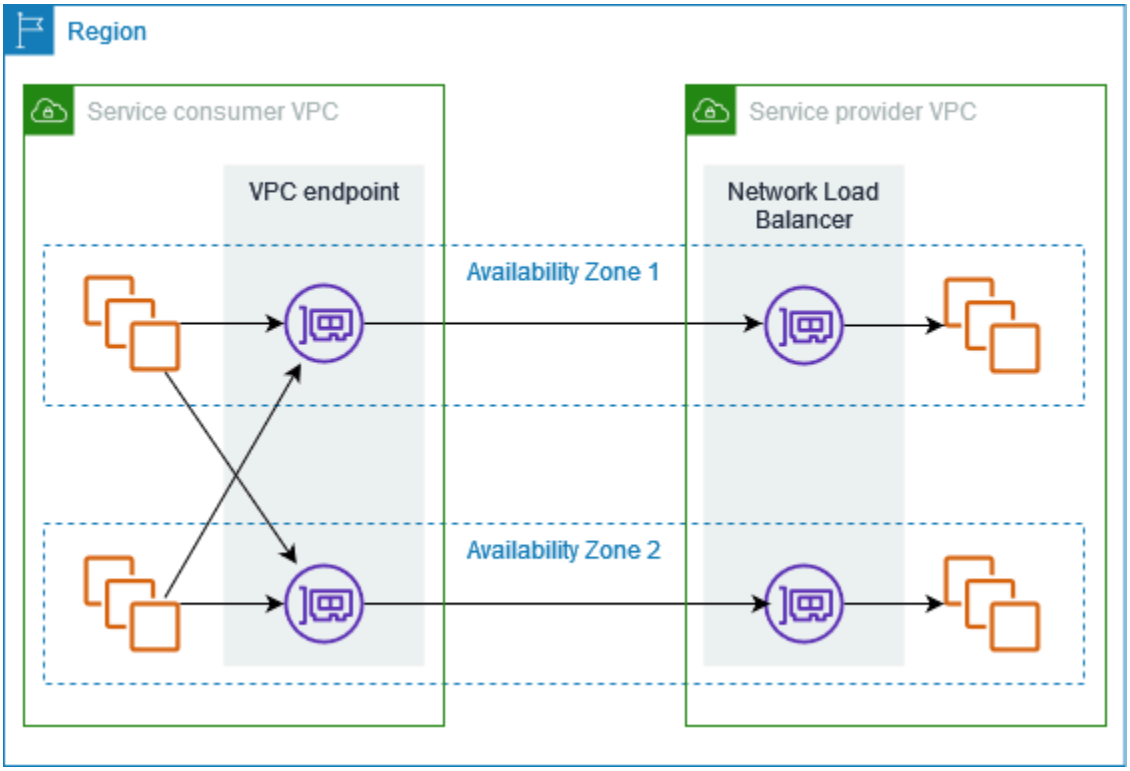
를 통해 서비스 공유 AWS PrivateLink

엔드포인트 서비스라고 하는 자체 AWS PrivateLink 구동 서비스를 호스팅하고 다른 AWS 고객과 공유할 수 있습니다.

내용

개요

다음 다이어그램은에서 호스팅되는 서비스를 AWS 다른 AWS 고객과 공유하는 방법과 해당 고객이 서비스에 연결하는 방법을 보여줍니다. 서비스 공급자는 Network Load Balancer를 VPC에 서비스 프런트 엔드로 생성합니다. 그런 다음 VPC 엔드포인트 서비스 구성을 생성할 때 이 로드 밸런서를 선택합니다. 서비스에 연결할 수 있도록 특정 AWS 보안 주체에 권한을 부여합니다. 서비스 소비자는 VPC에서 선택한 서브넷과 엔드포인트 서비스 간에 연결을 설정하는 인터페이스 VPC 엔드포인트를 생성합니다. 로드 밸런서는 서비스 소비자의 요청을 받아 서비스를 호스팅하는 대상으로 전달합니다.



낮은 지연 시간과 높은 가용성을 위해 적어도 두 개의 가용 영역에 서비스를 제공하는 것이 좋습니다.

DNS 호스트 이름

서비스 공급자가 VPC 엔드포인트 서비스를 생성하면는 서비스에 대한 엔드포인트별 DNS 호스트 이름을 AWS 생성합니다. 이러한 이름의 구문은 다음과 같습니다.

```
endpoint_service_id.region.vpce.amazonaws.com
```

다음은 us-east-2 리전의 VPC 엔드포인트 서비스에 대한 DNS 호스트 이름의 예입니다.

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

서비스 소비자가 인터페이스 VPC 엔드포인트를 생성하면 서비스 소비자가 엔드포인트 서비스와 통신하는 데 사용할 수 있는 리전 및 영역 DNS 이름이 생성됩니다. 리전 이름의 구문은 다음과 같습니다.

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

영역 이름의 구문은 다음과 같습니다.

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

프라이빗 DNS

또한 서비스 공급자는 엔드포인트 서비스의 프라이빗 DNS 이름을 연결하여 서비스 소비자가 기존 DNS 이름을 사용하여 서비스에 계속 액세스할 수 있도록 할 수 있습니다. 서비스 공급자가 프라이빗 DNS 이름을 엔드포인트 서비스에 연결한 경우 서비스 소비자는 인터페이스 엔드포인트의 프라이빗 DNS 이름을 활성화할 수 있습니다. 서비스 공급자가 프라이빗 DNS를 활성화하지 않는 경우 서비스 소비자는 VPC 엔드포인트 서비스의 퍼블릭 DNS 이름을 사용하도록 애플리케이션을 업데이트해야 할 수 있습니다. 자세한 내용은 DNS 이름 관리 단원을 참조하십시오.

서브넷 및 가용 영역

엔드포인트 서비스는 Network Load Balancer에 대해 활성화한 가용 영역에서 사용할 수 있습니다. 고가용성과 복원력을 확보하기 위해, 로드 밸런서를 최소 두 개 이상의 가용 영역에서 활성화하고 활성화된 각 영역에 EC2 인스턴스를 배포한 뒤 이러한 인스턴스를 로드 밸런서의 대상 그룹에 등록하는 것이 좋습니다.

엔드포인트 서비스를 여러 가용 영역에 호스팅하는 대신 교차 영역 로드 밸런싱을 활성화할 수도 있습니다. 그러나 엔드포인트 서비스를 호스팅하는 영역에 장애가 발생하면, 소비자는 두 영역 모두에서 엔드포인트 서비스에 액세스할 수 없게 됩니다. 또한 Network Load Balancer에 대해 교차 영역 로드 밸런싱을 활성화하면 EC2 데이터 전송 요금이 부과된다는 점도 고려해야 합니다.

소비자는 엔드포인트 서비스가 제공되는 가용 영역 내에서 인터페이스 VPC 엔드포인트를 생성할 수 있습니다. VPC 엔드포인트에 대해 소비자가 구성한 각 서브넷에는 엔드포인트 네트워크 인터페이스가 생성됩니다. VPC 엔드포인트의 IP 주소 유형에 따라 서브넷의 각 엔드포인트 네트워크 인터페이스에 IP 주소가 할당됩니다. 요청에 따라 VPC 엔드포인트 서비스에 리전 엔드포인트를 사용할 경우, 시스템은 정상 상태인 엔드포인트 네트워크 인터페이스를 선택하며, 서로 다른 가용 영역의 네트워크 인터페이스 간에 라운드 로빈 알고리즘을 사용해 순차적으로 트래픽을 분배합니다. 그런 다음에 선택된 엔드포인트 네트워크 인터페이스의 IP 주소로 트래픽을 라우팅합니다.

소비자는 트래픽을 동일한 가용 영역 내에 유지하는 것이 사용 사례에 더 적합할 경우 VPC 엔드포인트의 영역별 엔드포인트를 사용할 수도 있습니다.

교차 리전 액세스

서비스 공급자는 하나의 리전에서 서비스를 호스팅하고, 지원되는 여러 리전에서 해당 서비스를 제공할 수 있습니다. 서비스 소비자는 엔드포인트를 생성할 때 서비스 리전을 선택합니다.

권한

- 기본적으로 IAM 엔터티는 엔드포인트 서비스를 여러 리전에서 제공하거나 리전을 넘어 엔드포인트 서비스에 액세스할 권한이 없습니다. 리전 간 액세스 권한을 부여하려면, IAM 관리자가 `vpce:AllowMultiRegion` 권한만 허용하는 IAM 정책을 생성해야 합니다.
- 엔드포인트 서비스를 생성할 때 IAM 엔터티가 지정할 수 있는 지원 리전을 제어하려면 `ec2:VpceSupportedRegion` 조건 키를 사용합니다.
- VPC 엔드포인트를 생성할 때 IAM 엔터티가 지정할 수 있는 서비스 리전을 제어하려면 `ec2:VpceServiceRegion` 조건 키를 사용합니다.

고려 사항

- 서비스 공급자는 엔드포인트 서비스의 지원 리전으로 추가하기 전에 해당 옵트인 리전에 참여해야 합니다.
- 엔드포인트 서비스는 호스트 리전에서 액세스할 수 있어야 합니다. 호스트 리전은 지원 리전 목록에서 제거할 수 없습니다. 중복성을 위해 엔드포인트 서비스를 여러 리전에 배포하고 각 엔드포인트 서비스에 대해 교차 리전 액세스를 활성화할 수 있습니다.
- 서비스 소비자는 엔드포인트의 서비스 리전으로 선택하기 전에 해당 옵트인 리전에 참여해야 합니다. 가능한 경우, 서비스 소비자는 리전 내 연결을 통해 서비스를 액세스하는 것이 교차 리전 연결보다 권장됩니다. 리전 내 연결은 지연 시간이 짧고 비용이 적게 듭니다.
- 서비스 공급자가 지원 리전 목록에서 특정 리전을 제거하면, 서비스 소비자는 새 엔드포인트를 생성할 때 해당 리전을 서비스 리전으로 선택할 수 없습니다. 단, 기존 엔드포인트가 해당 리전을 서비스 리전으로 사용 중인 경우에는 기존 엔드포인트 액세스에 영향이 없습니다.
- 고가용성을 위해 공급자는 최소 2개의 가용 영역을 사용해야 합니다. 교차 리전 액세스에서는 공급자와 소비자가 반드시 동일한 가용 영역을 사용해야 하는 것은 아닙니다.
- `use1-az3`, `usw1-az2`, `apne1-az3`, `apne2-az2` 및 `apne2-az4` 가용 영역에서는 교차 리전 액세스가 지원되지 않습니다
- 리전 간 액세스를 통해 가용 영역 간의 장애 조치를 AWS PrivateLink 관리합니다. 교차 리전 장애 조치는 관리하지 않습니다.
- TCP 유휴 제한 시간에 사용자 지정 값을 설정한 Network Load Balancer에는 교차 리전 액세스가 지원되지 않습니다.
- UDP 조각화를 사용하는 경우 교차 리전 액세스는 지원되지 않습니다.
- 리전 간 액세스는 공유하는 서비스에 대해서만 지원됩니다 AWS PrivateLink.

IP 주소 유형

서비스 공급자는 백엔드 서버가 IPv4만 지원하는 경우에도 서비스 엔드포인트를 IPv4, IPv6 또는 IPv4와 IPv6 모두를 통해 서비스 소비자에 제공할 수 있습니다. 듀얼 스택 지원을 활성화하는 경우 기존 소비자는 계속 IPv4를 사용하여 서비스에 액세스할 수 있고 새 소비자는 IPv6를 사용하여 서비스에 액세스할 수 있습니다.

인터페이스 VPC 엔드포인트가 IPv4를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv4 주소가 있습니다. 인터페이스 VPC 엔드포인트가 IPv6를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv6 주소가 있습니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이 활성화됩니다.

엔드포인트 서비스에 대해 IPv6를 활성화하기 위한 요구 사항

- 엔드포인트 서비스의 VPC와 서브넷에는 연결된 IPv6 CIDR 블록이 있어야 합니다.
- 엔드포인트 서비스의 모든 Network Load Balancer는 듀얼 스택 IP 주소 유형을 사용해야 합니다. 대상에서 IPv6 트래픽을 지원할 필요는 없습니다. 서비스에서 프록시 프로토콜 버전 2 헤더의 소스 IP 주소를 처리하는 경우 IPv6 주소를 처리해야 합니다.

인터페이스 엔드포인트에 대해 IPv6를 활성화하기 위한 요구 사항

- 엔드포인트 서비스에서 IPv6 요청을 지원해야 합니다.
- 인터페이스 엔드포인트의 IP 주소 유형이 여기에 설명된 대로 인터페이스 엔드포인트의 서브넷과 호환되어야 합니다.
  - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.
  - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
  - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

인터페이스 엔드포인트에 대한 DNS 레코드 IP 주소 유형

인터페이스 엔드포인트에서 지원하는 DNS 레코드 IP 주소 유형에 따라 생성되는 DNS 레코드가 결정됩니다. 인터페이스 엔드포인트의 DNS 레코드 IP 주소 유형이 여기에 설명된 대로 인터페이스 엔드포인트의 IP 주소와 호환되어야 합니다.

- IPv4 - 프라이빗, 리전 및 영역 DNS 이름에 대해 A 레코드를 생성합니다. IP 주소 유형은 IPv4 또는 Dualstack(듀얼 스택)이어야 합니다.
- IPv6 - 프라이빗, 리전 및 영역 DNS 이름에 대해 AAAA 레코드를 생성합니다. IP 주소 유형은 IPv6 또는 듀얼 스택이어야 합니다.
- 듀얼 스택 - 프라이빗, 리전 및 영역 DNS 이름에 대해 A 및 AAAA 레코드를 생성합니다. IP 주소 유형은 듀얼 스택이어야 합니다.

에서 제공하는 서비스 생성 AWS PrivateLink

엔드포인트 서비스라고 AWS PrivateLink하는에서 제공하는 자체 서비스를 생성할 수 있습니다. 서비스를 생성하면 서비스 공급자이고 해당 서비스에 대한 연결을 생성하는 AWS 보안 주체는 서비스 소비자입니다.

엔드포인트 서비스에는 Network Load Balancer나 Gateway Load Balancer가 필요합니다. 로드 밸런서는 서비스 소비자의 요청을 받아 서비스로 전달합니다. 여기서는 Network Load Balancer를 사용하여 엔드포인트 서비스를 생성합니다. Gateway Load Balancer를 사용하여 엔드포인트 서비스를 생성하는 방법에 대한 자세한 내용은 가상 어플라이언스 액세스 섹션을 참조하세요.

내용

고려 사항

- 엔드포인트 서비스는 해당 서비스를 생성한 리전에서 사용할 수 있습니다. 소비자는 교차 리전 액세스를 활성화한 경우 또는 VPC 피어링이나 전송 게이트웨이를 사용하는 경우, 다른 리전에서도 서비스에 액세스할 수 있습니다.
- 서비스 소비자가 엔드포인트 서비스에 대한 정보를 검색할 때 서비스 공급자와 공통되는 가용 영역만 볼 수 있습니다. 서비스 공급자와 서비스 소비자가 다른 계정에 있는 경우 각 AWS 계정의 다른 물리적 가용 영역에 `us-east-1a`와 같은 가용 영역 이름이 매핑될 수 있습니다. AZ ID를 사용하여 서비스의 가용 영역을 일관되게 식별할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 AZ ID를 참조하세요.

- 서비스 소비자가 인터페이스 엔드포인트를 통해 서비스로 트래픽을 전송할 때 애플리케이션에 제공된 원본 IP 주소는 서비스 소비자의 IP 주소가 아니라 로드 밸런서 노드의 프라이빗 IP 주소입니다. 로드 밸런서에서 프록시 프로토콜을 활성화하는 경우 프록시 프로토콜 헤더에서 서비스 소비자의 주소와 인터페이스 엔드포인트의 ID를 확인할 수 있습니다. 자세한 내용은 Network Load Balancer 사용 설명서의 프록시 프로토콜을 참조하세요.
- Network Load Balancer는 단일 엔드포인트 서비스에 연결될 수 있지만 엔드포인트 서비스는 여러 Network Load Balancer에 연결될 수 있습니다.
- 엔드포인트 서비스가 여러 Network Load Balancer에 연결되어 있는 경우 각 엔드포인트 네트워크 인터페이스는 하나의 로드 밸런서와만 연결됩니다. 엔드포인트 네트워크 인터페이스에서 첫 번째 연결이 시작되면 엔드포인트 네트워크 인터페이스와 동일한 가용 영역에 있는 Network Load Balancer 중 하나를 임의로 선택합니다. 이 엔드포인트 네트워크 인터페이스의 모든 후속 연결 요청은 선택한 로드 밸런서를 사용합니다. 어떤 로드 밸런서를 선택하든 소비자가 엔드포인트 서비스를 사용할 수 있도록 엔드포인트 서비스의 모든 로드 밸런서에 동일한 리스너 및 대상 그룹 구성을 사용하는 것이 좋습니다.
- AWS PrivateLink 리소스에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 단원을 참조하십시오.

사전 조건

- 서비스를 제공할 각 가용 영역에서 하나 이상의 서브넷을 사용하여 엔드포인트 서비스의 VPC를 생성합니다.
- 서비스 소비자가 엔드포인트 서비스의 IPv6 인터페이스 VPC 엔드포인트를 생성할 수 있도록 하려면 VPC와 서브넷에는 연결된 IPv6 CIDR 블록이 있어야 합니다.
- VPC에서 Network Load Balancer를 생성합니다. 서비스 소비자에게 서비스를 제공할 가용 영역당 하나의 서브넷을 선택합니다. 낮은 지연 시간과 내결함성을 지원하기 위해 리전에서 두 개 이상의 가용 영역에 서비스를 제공하는 것이 좋습니다.
- Network Load Balancer에 보안 그룹이 있는 경우 클라이언트의 IP 주소에서 오는 인바운드 트래픽을 허용해야 합니다. 또는 트래픽에 대한 인바운드 보안 그룹 규칙의 평가를 끌 수 있습니다 AWS PrivateLink. 자세한 내용은 Network Load Balancer 사용 설명서의 보안 그룹을 참조하세요.
- 엔드포인트 서비스에서 IPv6 요청을 수락할 수 있도록 하려면 해당 Network Load Balancer가 듀얼스택 IP 주소 유형을 사용해야 합니다. 대상에서 IPv6 트래픽을 지원할 필요는 없습니다. 자세한 내용은 Network Load Balancer 사용 설명서의 IP 주소 유형을 참조하세요.

  프록시 프로토콜 버전 2 헤더의 소스 IP 주소를 처리하는 경우 IPv6 주소를 처리할 수 있는지 확인합니다.

- 서비스를 제공할 각 가용 영역에서 인스턴스를 시작하고 로드 밸런서 대상 그룹에 등록합니다. 활성화된 가용 영역 일부에서 인스턴스를 시작하지 않는 경우 교차 영역 로드 밸런싱을 활성화하여 영역 DNS 호스트 이름을 사용해 서비스에 액세스하는 서비스 소비자를 지원할 수 있습니다. 교차 영역 로드 밸런싱을 활성화하는 경우 리전 데이터 전송 요금이 부과될 수 있습니다. 자세한 내용은 Network Load Balancer 사용 설명서의 교차 영역 로드 밸런싱을 참조하세요.

엔드포인트 서비스 생성

Network Load Balancer를 사용하여 엔드포인트 서비스를 생성하려면 다음 절차를 따르세요.

콘솔을 사용하여 엔드포인트 서비스 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스 생성(Create endpoint service)을 선택합니다.
4. 로드 밸런서 유형(Load balancer type)에서 네트워크(Network)를 선택합니다.
5. 사용 가능한 로드 밸런서(Available load balancers)에서 엔드포인트 서비스에 연결할 Network Load Balancer를 선택합니다. 선택한 로드 밸런서에 대해 활성화된 가용 영역을 보려면 선택한 로드 밸런서의 세부 정보, 포함된 가용 영역을 참조하세요. 엔드포인트 서비스는 이러한 가용 영역에서 사용할 수 있습니다.
6. (선택 사항) 엔드포인트 서비스가 호스팅된 리전 외의 다른 리전에서도 사용 가능하도록 하려면, 서비스 리전에서 해당 리전을 선택합니다. 자세한 내용은 the section called “교차 리전 액세스” 단원을 참조하십시오.
7. Require acceptance for endpoint(엔드포인트 수락 필요)에서 엔드포인트 서비스에 대한 연결 요청을 수동으로 수락하도록 하려면 Acceptance required(수락 필요)를 선택합니다. 그러지 않으면 요청이 자동으로 수락됩니다.
8. 프라이빗 DNS 이름 활성화(Enable private DNS name)에서 프라이빗 DNS 이름을 서비스에 연결(Associate a private DNS name with the service)을 선택하여 서비스 소비자가 서비스에 액세스하는 데 사용할 수 있는 프라이빗 DNS 이름을 연결한 다음 프라이빗 DNS 이름을 입력합니다. 그렇지 않으면 서비스 소비자는에서 제공하는 엔드포인트별 DNS 이름을 사용할 수 있습니다 AWS. 서비스 소비자가 프라이빗 DNS 이름을 사용할 수 있으려면 서비스 공급자가 소비자의 도메인 소유 사실을 증명해야 합니다. 자세한 내용은 DNS 이름 관리 단원을 참조하십시오.
9. Supported IP address types(지원되는 IP 주소 유형)에서 다음 중 하나를 수행합니다.

   - IPv4 선택 - IPv4 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.

- IPv6 선택 - IPv6 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.
- IPv4 및 IPv6 선택 - IPv4 및 IPv6 요청을 모두 수락하도록 엔드포인트 서비스를 활성화합니다.

10. (선택 사항) 태그를 추가하려면 새로운 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
11. 생성(Create)을 선택합니다.

명령줄을 사용하여 엔드포인트 서비스 생성하기

- create-vpc-endpoint-service-configuration(AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

서비스 소비자가 엔드포인트 서비스를 사용할 수 있도록 설정

AWS 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 서비스 공급자는 서비스를 서비스 소비자가 사용할 수 있도록 하려면 다음을 수행해야 합니다.

- 각 서비스 소비자가 엔드포인트 서비스에 연결할 수 있도록 권한을 추가합니다. 자세한 내용은 the section called “권한 관리” 단원을 참조하십시오.
- 서비스 소비자가 인터페이스 엔드포인트를 생성하여 서비스에 연결할 수 있도록 서비스 소비자에게 서비스의 이름과 지원되는 가용 영역을 제공합니다. 자세한 내용은 the section called “서비스 소비자로 엔드포인트 서비스에 연결” 단원을 참조하십시오.
- 서비스 소비자의 엔드포인트 연결 요청을 수락합니다. 자세한 내용은 the section called “연결 요청 수락 또는 거부” 단원을 참조하십시오.

서비스 소비자로 엔드포인트 서비스에 연결

서비스 소비자는 다음 절차에 따라 인터페이스 엔드포인트를 생성하여 엔드포인트 서비스에 연결합니다.

콘솔을 사용하여 인터페이스 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.

4. 유형에서 NLB 및 GWLB를 사용하는 엔드포인트 서비스를 선택합니다.
5. 서비스 이름에서 서비스의 이름(예: `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`)을 입력한 다음 서비스 확인을 선택합니다.
6. (선택 사항) 엔드포인트 리전과 다른 리전에 있는 엔드포인트 서비스에 연결하려면, 서비스 리전, 교차 리전 엔드포인트 활성화를 선택한 후 해당 리전을 선택합니다. 자세한 내용은 the section called “교차 리전 액세스” 단원을 참조하십시오.
7. VPC에서 엔드포인트 서비스에 액세스할 서브넷을 선택합니다.
8. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다.
9. IP 주소 유형에서 다음 옵션 중에서 선택합니다.

   - IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있으며 엔드포인트 서비스가 IPv4 요청을 수락하는 경우에만 지원됩니다.
   - IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷이며 엔드포인트 서비스가 IPv6 요청을 수락하는 경우에만 지원됩니다.
   - 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있으며 엔드포인트 서비스가 IPv4 및 IPv6 요청을 수락하는 경우에만 지원됩니다.

10. DNS 레코드 IP 유형(DNS record IP type)에서 다음 옵션 중에서 선택합니다.

    - IPv4 - 프라이빗, 리전 및 영역 DNS 이름에 대해 A 레코드를 생성합니다. IP 주소 유형은 IPv4 또는 Dualstack(듀얼 스택)이어야 합니다.
    - IPv6 - 프라이빗, 리전 및 영역 DNS 이름에 대해 AAAA 레코드를 생성합니다. IP 주소 유형은 IPv6 또는 듀얼 스택이어야 합니다.
    - 듀얼 스택 - 프라이빗, 리전 및 영역 DNS 이름에 대해 A 및 AAAA 레코드를 생성합니다. IP 주소 유형은 듀얼 스택이어야 합니다.
    - Service defined(서비스 정의) - 프라이빗, 리전 및 영역 DNS 이름에 대해 A 레코드, 리전 및 영역 DNS 이름에 대해 AAAA 레코드를 생성합니다. IP 주소 유형은 듀얼 스택이어야 합니다.

11. 보안 그룹(Security group)에서 엔드포인트 네트워크 인터페이스에 연결할 보안 그룹을 선택합니다.
12. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)

- New-EC2VpcEndpoint(Windows PowerShell용 도구)

엔드포인트 서비스 구성

엔드포인트 서비스를 생성한 후 해당 구성을 업데이트할 수 있습니다.

작업

- 권한 관리
- 연결 요청 수락 또는 거부
- 로드 밸런서 관리
- 프라이빗 DNS 이름 연결
- 지원되는 리전 수정
- 지원되는 IP 주소 유형 수정
- 태그 관리

권한 관리

권한과 수락 설정을 조합하면 엔드포인트 서비스에 액세스할 수 있는 서비스 소비자(AWS 보안 주체)를 제어할 수 있습니다. 예를 들어 신뢰할 수 있고 자동으로 모든 연결 요청을 수락하는 특정 보안 주체에 권한을 부여하거나, 더 넓은 범위의 보안 주체 그룹에 권한을 부여하고 신뢰할 수 있는 특정 연결 요청을 수동으로 수락할 수 있습니다.

기본적으로 엔드포인트 서비스는 서비스 소비자가 사용할 수 없습니다. 특정 AWS 보안 주체가 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 연결할 수 있도록 허용하는 권한을 추가해야 합니다. AWS 보안 주체에 대한 권한을 추가하려면 Amazon 리소스 이름(ARN)이 필요합니다. 다음 목록에는 지원되는 AWS 보안 주체의 ARN 예시가 포함되어 있습니다.

AWS 보안 주체ARNs

AWS 계정 (계정의 모든 보안 주체 포함)

    arn:aws:iam::*account_id*:root

Role

    arn:aws:iam::*account_id*:role/*role_name*

User

arn:aws:iam::*account_id*:user/*user_name*

모든의 모든 보안 주체 AWS 계정

*

고려 사항

- 모든 사용자에게 엔드포인트 서비스에 액세스할 수 있는 권한을 부여하고 모든 요청을 수락하도록 엔드포인트 서비스를 구성하는 경우 로드 밸런서는 퍼블릭 IP 주소가 없더라도 퍼블릭으로 설정됩니다.
- 권한을 제거해도 엔드포인트와 이전에 수락된 서비스 간의 기존 연결에는 영향을 미치지 않습니다.

콘솔을 사용해 엔드포인트 서비스에 대한 권한 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택하고 보안 주체 허용(Allow principals) 탭을 선택합니다.
4. 권한을 추가하려면 보안 주체 허용(Allow principals)을 선택합니다. Principals to add(추가할 보안 주체)에 보안 주체의 ARN을 입력합니다. 다른 보안 주체를 추가하려면 보안 주체 추가(Add principal)를 선택합니다. 보안 주체를 추가했다면 보안 주체 허용(Allow principals)을 선택합니다.
5. 권한을 제거하려면 위탁자를 선택하고 작업(Actions), 삭제(Delete)를 선택합니다. 확인 메시지가 나타나면 **delete**을 입력한 다음 삭제를 선택합니다.

명령줄을 사용하여 엔드포인트 서비스에 대한 권한 추가하기

- modify-vpc-endpoint-service-permissions(AWS CLI)
- Edit-EC2EndpointServicePermission(Windows PowerShell용 도구)

연결 요청 수락 또는 거부

권한과 수락 설정을 조합하면 엔드포인트 서비스에 액세스할 수 있는 서비스 소비자(AWS 보안 주체)를 제어할 수 있습니다. 예를 들어 신뢰할 수 있고 자동으로 모든 연결 요청을 수락하는 특정 보안 주체에 권한을 부여하거나, 더 넓은 범위의 보안 주체 그룹에 권한을 부여하고 신뢰할 수 있는 특정 연결 요청을 수동으로 수락할 수 있습니다.

연결 요청을 자동으로 수락하도록 엔드포인트 서비스를 구성할 수 있습니다. 그러지 않으면 요청을 수동으로 수락하거나 거부해야 합니다. 연결 요청을 수락하지 않으면 서비스 소비자가 엔드포인트 서비스에 액세스할 수 없습니다.

모든 사용자에게 엔드포인트 서비스에 액세스할 수 있는 권한을 부여하고 모든 요청을 수락하도록 엔드포인트 서비스를 구성하는 경우 로드 밸런서는 퍼블릭 IP 주소가 없더라도 퍼블릭으로 설정됩니다.

연결 요청이 수락되거나 거부될 때 알림을 받을 수 있습니다. 자세한 내용은 the section called “엔드포인트 서비스 이벤트에 대한 알림 받기” 단원을 참조하십시오.

콘솔을 사용하여 수락 설정 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), 엔드포인트 수락 설정 수정(Modify endpoint acceptance setting)을 차례로 선택합니다.
5. Acceptance required(수락 필요)를 선택하거나 선택 취소합니다.
6. 변경 사항 저장을 선택합니다

명령줄을 사용하여 수락 설정 수정하기

- modify-vpc-endpoint-service-configuration(AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

콘솔을 사용하여 연결 요청 수락 또는 거부하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 엔드포인트 연결(Endpoint connections) 탭에서 엔드포인트 연결을 선택합니다.
5. 연결 요청을 수락하려면 작업(Actions), 엔드포인트 연결 요청 수락(Accept endpoint connection request)을 차례로 선택합니다. 확인 메시지가 나타나면 **accept**를 입력한 다음 수락(Accept)을 선택합니다.

6. 연결 요청을 거부하려면 작업(Actions), 엔드포인트 연결 요청 거부(Reject endpoint connection request)를 차례로 선택합니다. 확인 메시지가 나타나면 **reject**를 입력한 다음 거부(Reject)를 선택합니다.

명령줄을 사용하여 연결 요청 수락 또는 거부하기

- accept-vpc-endpoint-connections 또는 reject-vpc-endpoint-connections(AWS CLI)
- Approve-EC2EndpointConnection 또는 Deny-EC2EndpointConnection(Windows PowerShell용 도구)

로드 밸런서 관리

엔드포인트 서비스에 연결된 로드 밸런서를 관리할 수 있습니다. 엔드포인트 서비스에 연결된 엔드포인트가 있는 경우에는 로드 밸런서를 연결 해제할 수 없습니다.

로드 밸런서에 다른 가용 영역을 활성화하면, 엔드포인트 서비스 페이지의 로드 밸런서 탭에 해당 가용 영역이 표시됩니다. 하지만 그 가용 영역은 엔드포인트 서비스에 자동으로 활성화되지 않으며, AWS Management Console의 엔드포인트 서비스 세부 정보 탭에도 나타나지 않습니다 새 가용 영역에 대한 엔드포인트 서비스를 활성화해야 합니다.

로드 밸런서의 새 가용 영역이 엔드포인트 서비스에서 사용할 준비가 되기까지 몇 분이 걸릴 수 있습니다. 자동화 과정을 사용 중이라면, 새 가용 영역을 엔드포인트 서비스에서 활성화하기 전에 대기 시간을 추가하는 것이 좋습니다.

콘솔을 사용하여 엔드포인트 서비스에 대한 로드 밸런서 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), 로드 밸런서 연결 또는 연결 해제(Associate or disassociate load balancers)를 선택합니다.
5. 엔드포인트 서비스 구성을 필요에 따라 변경합니다. 예제:
   - 로드밸런서를 엔드포인트 서비스에 연결하려면 확인란을 선택합니다.
   - 로드 밸런서를 엔드포인트 서비스에서 연결 해제하려면 확인란의 선택을 취소합니다. 로드 밸런서는 하나 이상 선택되어 있어야 합니다.
6. 변경 사항 저장을 선택합니다

엔드포인트 서비스는 로드 밸런서에 새로 추가한 모든 가용 영역에 대해 활성화됩니다. 새 가용 영역은 엔드포인트 서비스의 로드 밸런서 탭과 세부 정보 탭에 표시됩니다.

엔드포인트 서비스에 대해 가용 영역을 활성화한 후 서비스 소비자는 해당 가용 영역의 서브넷을 인터페이스 VPC 엔드포인트에 추가할 수 있습니다.

명령줄을 사용하여 엔드포인트 서비스에 대한 로드 밸런서 관리하기

- modify-vpc-endpoint-service-configuration(AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

최근에 로드 밸런서에 대해 활성화된 가용 영역에서 엔드포인트 서비스를 활성화하려면 엔드포인트 서비스의 ID를 사용하여 명령을 호출하면 됩니다.

프라이빗 DNS 이름 연결

프라이빗 DNS 이름을 엔드포인트 서비스에 연결할 수 있습니다. 프라이빗 DNS 이름을 연결한 후에는 DNS 서버에서 도메인에 대한 항목을 업데이트해야 합니다. 서비스 소비자가 프라이빗 DNS 이름을 사용할 수 있으려면 서비스 공급자가 소비자의 도메인 소유 사실을 증명해야 합니다. 자세한 내용은 DNS 이름 관리 단원을 참조하십시오.

콘솔을 사용하여 엔드포인트 서비스 프라이빗 DNS 이름 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), 프라이빗 DNS 이름 수정(Modify private DNS name)을 차례로 선택합니다.
5. 프라이빗 DNS 이름을 서비스에 연결(Associate a private DNS name with the service)을 선택하고 프라이빗 DNS 이름을 입력합니다.
   - 도메인 이름에는 소문자를 사용해야 합니다.
   - 도메인 이름에 와일드카드를 사용할 수 있습니다(예: **`*.myexampleservice.com`**).
6. 변경 사항 저장을 선택합니다.
7. 프라이빗 DNS 이름은 확인 상태가 verified(확인됨)인 경우 서비스 소비자가 사용할 수 있습니다. 확인 상태가 변경되는 경우 새 연결 요청이 거부되지만 기존 연결은 영향을 받지 않습니다.

명령줄을 사용하여 엔드포인트 서비스 프라이빗 DNS 이름 수정하기

- modify-vpc-endpoint-service-configuration(AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

콘솔을 사용하여 도메인 확인 시작하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. Actions(작업), Verify domain ownership for private DNS name(프라이빗 DNS 이름에 대한 도메인 소유권 확인)을 차례로 선택합니다.
5. 확인 메시지가 나타나면 **`verify`**를 입력한 다음 확인(Verify)을 선택합니다.

명령줄을 사용하여 도메인 확인 시작하기

- start-vpc-endpoint-service-private-dns-verification(AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification(Windows PowerShell용 도구)

지원되는 리전 수정

엔드포인트 서비스의 지원 리전 집합을 수정할 수 있습니다. 옵트인 리전을 추가하려면 먼저 해당 리전에 옵트인해야 합니다. 엔드포인트 서비스를 호스팅하는 리전은 제거할 수 없습니다.

리전을 제거한 후에는 서비스 소비자가 새 엔드포인트를 생성할 때 해당 리전을 서비스 리전으로 지정할 수 없습니다. 기존 엔드포인트에서 해당 리전을 서비스 리전으로 사용하는 경우에는 영향이 없습니다. 리전을 제거할 때는 해당 리전에서 연결된 기존 엔드포인트를 거부하는 것이 좋습니다.

엔드포인트 서비스에 대해 지원되는 리전 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업, 지원 리전 수정을 선택합니다.
5. 필요에 따라 리전을 선택하거나 선택 해제합니다.
6. 변경 사항 저장을 선택합니다.

지원되는 IP 주소 유형 수정

엔드포인트 서비스에서 지원하는 IP 주소 유형을 변경할 수 있습니다.

고려 사항

엔드포인트 서비스에서 IPv6 요청을 수락할 수 있도록 하려면 해당 Network Load Balancer가 듀얼 스택 IP 주소 유형을 사용해야 합니다. 대상에서 IPv6 트래픽을 지원할 필요는 없습니다. 자세한 내용은 Network Load Balancer 사용 설명서의 IP 주소 유형을 참조하세요.

콘솔을 사용하여 지원되는 IP 주소 유형 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. VPC 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), Modify supported IP address types(지원되는 IP 주소 유형 수정)을 차례로 선택합니다.
5. Supported IP address types(지원되는 IP 주소 유형)에서 다음 중 하나를 수행합니다.
   - IPv4 선택 - IPv4 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.
   - IPv6 선택 - IPv6 요청을 수락하도록 엔드포인트 서비스를 활성화합니다.
   - IPv4 및 IPv6 선택 - IPv4 및 IPv6 요청을 모두 수락하도록 엔드포인트 서비스를 활성화합니다.
6. 변경 사항 저장을 선택합니다.

명령줄을 사용하여 지원되는 IP 주소 유형 수정하기

- modify-vpc-endpoint-service-configuration(AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Windows PowerShell용 도구)

태그 관리

리소스에 태그를 지정하면 조직의 요구에 따라 리소스를 식별하거나 분류하는 데 유용할 수 있습니다.

콘솔을 사용해 엔드포인트 서비스에 대한 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.

3. VPC 엔드포인트 서비스를 선택합니다.
4. 작업, 태그 관리를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장을 선택합니다.

콘솔을 사용해 엔드포인트 연결에 대한 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. VPC 엔드포인트 서비스를 선택한 다음 엔드포인트 연결(Endpoint connections) 탭을 선택합니다.
4. 엔드포인트 연결을 선택한 다음 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장을 선택합니다.

콘솔을 사용해 엔드포인트 서비스 권한에 대한 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. VPC 엔드포인트 서비스를 선택한 다음 보안 주체 허용(Allow principals) 탭을 선택합니다.
4. 위탁자를 선택한 다음 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장을 선택합니다.

명령줄을 사용하여 태그 추가 또는 제거하기

- create-tags 및 delete-tags(AWS CLI)
- New-EC2Tag 및 Remove-EC2Tag(Windows PowerShell용 도구)

VPC 엔드포인트 서비스의 DNS 이름 관리

서비스 공급자는 엔드포인트 서비스의 프라이빗 DNS 이름을 구성할 수 있습니다. 예를 들어, 서비스 공급자가 서비스를 퍼블릭 엔드포인트와 엔드포인트 서비스 형태로 모두 제공한다고 가정합니다. 이때 서비스 공급자가 퍼블릭 엔드포인트의 DNS 이름을 엔드포인트 서비스의 프라이빗 DNS 이름으로 사용하면, 서비스 소비자는 클라이언트 애플리케이션을 수정하지 않고도 퍼블릭 엔드포인트 또는 엔드포인트 서비스에 동일하게 액세스할 수 있습니다. 요청이 서비스 소비자 VPC에서 오는 경우, 프라이빗 DNS 서버가 DNS 이름을 엔드포인트 네트워크 인터페이스의 IP 주소로 확인합니다. 그러지 않으면 퍼블릭 DNS 서버가 DNS 이름을 퍼블릭 엔드포인트로 확인합니다.

엔드포인트 서비스의 프라이빗 DNS 이름을 구성하려면 먼저 도메인 소유권 확인 검사를 수행하여 도메인 소유 사실을 증명해야 합니다.

고려 사항

- 엔드포인트 서비스당 프라이빗 DNS 이름은 하나만 있을 수 있습니다.
- 소비자가 서비스에 연결하기 위해 인터페이스 엔드포인트를 생성하면, 프라이빗 호스팅 영역을 생성하고 이를 서비스 소비자 VPC와 연결합니다. 프라이빗 호스팅 영역에는 엔드포인트 서비스의 프라이빗 DNS 이름을 VPC 엔드포인트의 리전 DNS 이름에 매핑하는 CNAME 레코드를 생성합니다. 소비자가 서비스의 퍼블릭 DNS 이름으로 요청을 보내면, 프라이빗 DNS 서버가 요청을 엔드포인트 네트워크 인터페이스의 IP 주소로 확인합니다.
- 도메인을 확인하려면 퍼블릭 호스트 이름 또는 퍼블릭 DNS 공급자가 있어야 합니다.
- 하위 도메인의 도메인은 확인할 수 있습니다. 예를 들어, a.example.com 대신 example.com을 확인할 수 있습니다. 각 DNS 레이블은 최대 63자일 수 있으며 전체 도메인 이름은 총 길이 255자를 초과할 수 없습니다.

  하위 도메인을 추가하는 경우 하위 도메인 또는 도메인을 확인해야 합니다. 예를 들어, a.example.com이 있었고 example.com을 확인했다고 가정합시다. 이제 b.example.com을 프라이빗 DNS 이름으로 추가하는 경우 example.com 또는 b.example.com을 확인해야만 서비스 소비자가 해당 이름을 사용할 수 있습니다.
- Gateway Load Balancer 엔드포인트에는 프라이빗 DNS 이름이 지원되지 않습니다.

도메인 소유권 확인

도메인은 DNS 공급자를 통해 관리하는 도메인 이름 시스템(DNS) 레코드의 집합과 연결되어 있습니다. TXT 레코드는 DNS 레코드의 한 유형으로 도메인에 대한 추가 정보를 제공하며 이름과 값으로 구

성되어 있습니다. 확인 프로세스의 일부로 퍼블릭 도메인의 DNS 서버에 TXT 레코드를 추가해야 합니다.

도메인의 DNS 설정에 TXT 레코드가 있다는 것이 확인되면 도메인 소유권 확인이 완료됩니다.

레코드를 추가한 후에는 Amazon VPC 콘솔을 사용하여 도메인 확인 프로세스의 상태를 확인할 수 있습니다. 탐색 창에서 엔드포인트 서비스를 선택합니다. 엔드포인트 서비스를 선택하고 Details(세부 정보) 탭에서 Domain verification status(도메인 확인 상태)의 값을 확인합니다. 도메인 확인이 보류 중인 경우 몇 분 더 기다렸다가 화면을 새로 고칩니다. 필요한 경우 확인 프로세스를 수동으로 시작할 수 있습니다. Actions(작업), Verify domain ownership for private DNS name(프라이빗 DNS 이름에 대한 도메인 소유권 확인)을 차례로 선택합니다.

프라이빗 DNS 이름은 확인 상태가 verified(확인됨)인 경우 서비스 소비자가 사용할 수 있습니다. 확인 상태가 변경되는 경우 새 연결 요청이 거부되지만 기존 연결은 영향을 받지 않습니다.

확인 상태가 failed(실패)인 경우 the section called “도메인 확인 문제 해결” 섹션을 참조하세요.

이름 및 값 가져오기

TXT 레코드에 사용하는 이름과 값은 제공됩니다. 예를 들어 AWS Management Console에서 이 정보를 사용할 수 있습니다. 엔드포인트 서비스를 선택하고 엔드포인트 서비스의 Details(세부 정보) 탭에서 Domain verification name(도메인 확인 이름) 및 Domain verification value(도메인 확인 값)를 확인합니다. 다음 describe-vpc-endpoint-service-configurations AWS CLI 명령을 사용하여 지정된 엔드포인트 서비스의 프라이빗 DNS 이름 구성에 대한 정보를 검색할 수도 있습니다.

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

출력의 예는 다음과 같습니다. `Value` 및 `Name`은 TXT 레코드를 생성할 때 사용합니다.

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

예를 들어 도메인 이름이 example.com이고 `Value` 및 `Name`이 앞의 출력 예와 같다고 가정합니다. TXT 레코드 설정의 예는 다음 표와 같습니다.

이름	Type	값
_6e86v84tqgqubxbwii1m.example.com	TXT	vpce:l6p0ERxlTt45jevFwOCp

기본 도메인 이름은 이미 사용 중일 수 있으므로 `Name`을 레코드 하위 도메인으로 사용하는 것이 좋습니다. 그러나 DNS 공급자가 DNS 레코드 이름에 밑줄 사용을 허용하지 않는 경우에는 TXT 레코드에서 "_6e86v84tqgqubxbwii1m"을 생략하고 "example.com"만 사용할 수 있습니다.

"_6e86v84tqgqubxbwii1m.example.com"이 확인되면 서비스 소비자는 "example.com"이나 하위 도메인(예: "service.example.com" 또는 "my.service.example.com")을 사용할 수 있습니다.

도메인의 DNS 서버에 TXT 레코드 추가

도메인의 DNS 서버에 TXT 레코드를 추가하는 절차는 DNS 서비스를 누가 제공하는지에 따라 다릅니다. DNS 공급자가 Amazon Route 53 또는 다른 도메인 이름 등록자일 수 있습니다.

Amazon Route 53

퍼블릭 호스팅 영역에 대해 단순 라우팅 정책을 사용하여 레코드를 생성합니다. 다음 값을 사용합니다.

- Record name(레코드 이름)에 도메인 또는 하위 도메인을 입력합니다.
- 레코드 유형(Record type)에 대해 TXT를 선택합니다.
- 값/트래픽 라우팅 대상(Value/Route traffic to)에 도메인 확인 값을 입력합니다.
- TTL(초)(TTL (seconds))에 **`1800`**을 입력합니다.

자세한 내용은 Amazon Route 53 개발자 가이드에서 콘솔을 사용하여 레코드 생성을 참조하세요.

일반 절차

DNS 공급자의 웹 사이트로 이동하여 계정에 로그인합니다. 도메인의 DNS 레코드를 업데이트할 페이지를 찾습니다. AWS에서 제공한 이름과 값이 포함된 TXT 레코드를 추가합니다. DNS 레코드 업데이트가 적용되려면 최대 48시간이 걸릴 수 있지만, 대개는 이보다 훨씬 더 빨리 적용됩니다.

더 구체적인 지침은 DNS 공급자의 설명서를 참조하세요. 다음 표에는 몇몇 일반적인 DNS 공급자의 설명서 링크가 나와 있습니다. 이 목록은 전체를 포함하지도 않으며 해당 회사에서 제공하는 제품이나 서비스를 추천하기 위한 것도 아닙니다.

DNS/호스팅 공급자	설명서 링크
GoDaddy	TXT 레코드 추가
Dreamhost	사용자 지정 DNS 레코드 추가
Cloudflare	DNS 레코드 관리
HostGator	HostGator/eNom을 통한 DNS 레코드 관리
Namecheap	도메인의 TXT/SPF/DKIM/DMARC 레코드를 추가하는 방법
Names.co.uk	도메인 DNS 설정 변경
Wix	Wix 계정에서 TXT 레코드 추가 또는 업데이트

TXT 레코드가 게시되었는지 확인

다음 단계에 따라 프라이빗 DNS 이름 도메인 소유권 확인 TXT 레코드가 DNS 서버에 올바르게 게시되었는지 확인할 수 있습니다. 여기서는 Windows 및 Linux에서 사용 가능한 nslookup 명령을 실행합니다.

도메인에 서비스하는 DNS 서버를 쿼리하는 이유는 이들 서버가 도메인에 대한 최신 정보를 포함하고 있기 때문입니다. 도메인 정보가 다른 DNS 서버로 전파되는 데에는 시간이 걸립니다.

TXT 레코드가 DNS 서버에 게시되었는지 확인하기

1. 다음 명령을 사용하여 도메인의 이름 서버를 찾습니다.

   ```
   nslookup -type=NS example.com
   ```

   도메인에 서비스하는 이름 서버가 출력에 나열됩니다. 다음 단계에서 이들 서버 중 하나를 쿼리합니다.
2. 다음 명령을 사용하여 TXT 레코드가 올바로 게시되었는지 확인합니다. 여기서 *name_server*는 이전 단계에서 찾은 이름 서버 중 하나입니다.

```
nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
```

3. 이전 단계의 출력에서 `text =` 다음의 문자열이 TXT 값과 일치하는지 확인합니다.

   여기 예제에서는 레코드가 올바로 게시된 경우 출력에 다음이 포함됩니다.

```
_6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
```

도메인 확인 문제 해결

도메인 확인 프로세스가 실패하는 경우 다음 정보를 참조하여 문제를 해결할 수 있습니다.

- DNS 공급자가 TXT 레코드 이름에 밑줄 사용을 허용하지는 확인합니다. DNS 공급자가 밑줄을 허용하지 않는 경우 TXT 레코드에서 도메인 확인 이름(예: “_6e86v84tqgqubxbwii1m”)을 생략할 수 있습니다.
- DNS 공급자가 TXT 레코드 끝에 도메인 이름을 추가했는지 확인합니다. 일부 DNS 공급자는 도메인 이름을 TXT 레코드의 속성 이름에 자동으로 추가합니다. 이와 같은 도메인 이름 중복을 방지하려면 TXT 레코드를 생성할 때 도메인 이름의 끝에 마침표를 추가합니다. 그러면 DNS 공급자가 TXT 레코드에 도메인 이름을 추가할 필요가 없음을 알게 됩니다.
- DNS 공급자가 소문자만 사용하도록 DNS 레코드 값을 수정했는지 확인합니다. 제공된 값과 정확히 일치하는 속성 값이 포함된 확인 레코드가 있는 경우에만 도메인이 확인됩니다. DNS 공급자가 소문자만 사용하도록 TXT 레코드 값을 변경한 경우 DNS 공급자에게 연락하여 지원을 요청하세요.
- 여러 리전이나 여러 AWS 계정을 지원하므로 도메인을 두 번 이상 확인해야 할 수 있습니다. DNS 공급자가 속성 이름이 같은 TXT 레코드가 두 개 이상인 것을 허용하지 않는 경우 DNS 공급자가 동일한 TXT 레코드에 여러 속성 값을 할당하도록 허용하는지 확인합니다. 예를 들어 DNS가 Amazon Route 53을 통해 관리되는 경우 다음 절차를 사용할 수 있습니다.

  1. Amazon Route 53 콘솔에서 첫 번째 리전에서 도메인을 확인할 때 생성한 TXT 레코드를 선택합니다.
  2. 값(Value)에서 기존 속성 값의 끝으로 이동한 다음 Enter 키를 누릅니다.
  3. 추가 리전에 대한 속성 값을 추가한 다음 레코드 세트를 저장합니다.

  DNS 공급자가 동일한 TXT 레코드에 여러 값을 할당하도록 허용하지 않는 경우에는 한 번은 TXT 레코드 속성 이름의 값으로 도메인을 확인하고 또 한 번은 속성 이름에서 값을 제거하고 도메인을 확인할 수 있습니다. 하지만 동일한 도메인을 두 번만 확인할 수 있습니다.

엔드포인트 서비스 이벤트에 대한 알림 받기

엔드포인트 서비스와 관련된 특정 이벤트에 대한 알림을 받도록 알림을 생성할 수 있습니다. 연결 요청이 수락되거나 거부될 때 이메일을 수신할 수 있습니다.

작업

- SNS 알림 생성
- 액세스 정책 추가
- 키 정책 추가

SNS 알림 생성

다음 절차를 활용하여 알림을 위한 Amazon SNS 주제를 생성하고 해당 주제를 구독합니다.

콘솔을 사용하여 엔드포인트 서비스에 대한 알림 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 알림(Notifications) 탭에서 알림 생성(Create notification)을 선택합니다.
5. Notification ARN(알림 ARN)에서 생성한 SNS 주제의 ARN을 선택합니다.
6. 이벤트를 구독하려면 Events(이벤트)에서 이벤트를 선택합니다.
   - Connect(연결) - 서비스 소비자가 인터페이스 엔드포인트를 생성했습니다. 이 경우 연결 요청이 서비스 공급자에 전송됩니다.
   - 허용(Accept) - 서비스 공급자가 연결 요청을 수락했습니다.
   - Reject(거부) – 서비스 공급자가 연결 요청을 거부했습니다.
   - Delete(삭제) – 서비스 소비자가 인터페이스 엔드포인트를 삭제했습니다.
7. 알림 생성(Create notification)을 선택합니다.

명령줄을 사용하여 엔드포인트 서비스에 대한 알림 생성하기

- create-vpc-endpoint-connection-notification(AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Windows PowerShell용 도구)

액세스 정책 추가

가 사용자를 대신하여 다음과 같은 알림을 AWS PrivateLink 게시할 수 있도록 허용하는 액세스 정책을 SNS 주제에 추가합니다. 자세한 내용은 내 Amazon SNS 주제의 액세스 정책을 편집하려면 어떻게 해야 합니까?를 참조하세요. 혼동된 대리자 문제를 방지하기 위해 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 키를 사용합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

키 정책 추가

암호화된 SNS 주제를 사용하는 경우 KMS 키에 대한 리소스 정책은 AWS KMS API 작업을 호출 AWS PrivateLink 하기 위해를 신뢰해야 합니다. 다음은 예제 키 정책입니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

엔드포인트 서비스 삭제

엔드포인트 서비스 사용을 마치면 서비스를 삭제할 수 있습니다. 엔드포인트 서비스에 연결되어 있고 상태가 `available` 또는 `pending-acceptance`인 엔드포인트가 있는 경우 엔드포인트 서비스를 삭제할 수 없습니다.

엔드포인트 서비스를 삭제해도 연결된 로드 밸런서는 삭제되지 않으며 로드 밸런서 대상 그룹에 등록된 애플리케이션 서버는 영향을 받지 않습니다.

콘솔을 사용하여 엔드포인트 서비스 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), 엔드포인트 삭제(Delete Endpoint)를 차례로 선택합니다.
5. 확인 메시지가 나타나면 **delete**을 입력한 다음 삭제를 선택합니다.

명령줄을 사용하여 엔드포인트 서비스 삭제하기

- delete-vpc-endpoint-service-configurations(AWS CLI)
- Remove-EC2EndpointServiceConfiguration(Windows PowerShell용 도구)

를 통해 VPC 리소스에 액세스 AWS PrivateLink

리소스 VPC 엔드포인트(리소스 엔드포인트)를 사용하면 다른 VPC의 VPC 리소스에 비공개로 액세스할 수 있습니다. 리소스 엔드포인트를 사용하면 데이터베이스, Amazon EC2 인스턴스, 애플리케이션 엔드포인트, 도메인 이름 대상, 또는 다른 VPC의 프라이빗 서브넷이나 온프레미스 환경에 있을 수도 있는 IP 주소와 같은 VPC 리소스에 비공개로 안전하게 액세스할 수 있습니다. 리소스 엔드포인트가 없으면 VPC에 인터넷 게이트웨이를 추가하거나 AWS PrivateLink 인터페이스 엔드포인트 및 Network Load Balancer를 사용하여 리소스에 액세스해야 합니다. 리소스 엔드포인트에는 로드 밸런서가 필요하지 않으므로, 사용자가 VPC 리소스에 직접 액세스할 수 있습니다. VPC 리소스는 리소스 구성으로 표시되며, 리소스 구성은 리소스 게이트웨이와 연결됩니다.

요금

리소스 엔드포인트를 사용하여 리소스에 액세스하면, 리소스 VPC 엔드포인트가 프로비저닝된 시간 단위로 요금이 청구됩니다. 또한 리소스에 액세스할 때 처리된 데이터량(GB 단위)에도 요금이 부과됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하십시오. 리소스 구성과 리소스 게이트웨이를 통해 리소스 액세스를 활성화하면, 리소스 게이트웨이가 처리한 데이터량(GB 단위)에 따라 요금이 청구됩니다. 자세한 내용은 Amazon VPC Lattice 요금을 참조하십시오.

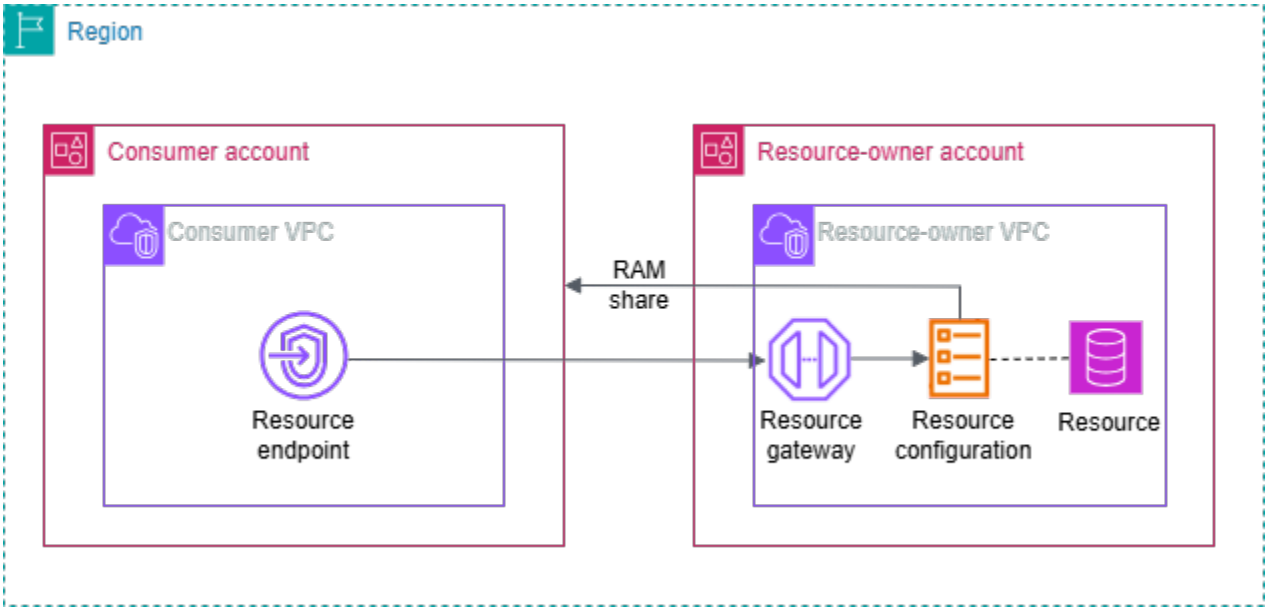
내용

개요

자신의 계정에 있는 리소스 또는 다른 계정에서 공유받은 리소스에 액세스할 수 있습니다. 리소스에 액세스하려면 리소스 VPC 엔드포인트를 생성해야 하며, 이를 통해 VPC 내 서브넷과 리소스 간에 네트워

크 인터페이스를 이용한 연결이 설정됩니다. 리소스로 향하는 트래픽은 DNS를 사용하여 리소스 엔드포인트의 네트워크 인터페이스 프라이빗 IP 주소로 확인됩니다. 이후 리소스 게이트웨이를 통해 VPC 엔드포인트와 리소스 간의 연결을 사용하여 트래픽이 전송됩니다.

다음 이미지는 다른 계정이 소유하고를 통해 공유되는 리소스에 액세스하는 소비자 계정의 리소스 엔드포인트를 보여줍니다 AWS RAM.



고려 사항

- TCP 트래픽만 지원되며, UDP 트래픽은 지원되지 않습니다.
- 네트워크 연결은 리소스가 있는 VPC가 아닌 리소스 엔드포인트가 있는 VPC에서 시작해야 합니다. 리소스의 VPC에서는 엔드포인트 VPC로 네트워크 연결을 시작할 수 없습니다.
- ARN 기반 리소스 중 지원되는 것은 Amazon RDS 리소스뿐입니다.
- VPC 엔드포인트와 리소스 게이트웨이는 최소 한 개 이상 가용 영역이 겹쳐야 합니다.

DNS 호스트 이름

를 사용하면 프라이빗 엔드포인트를 사용하여 리소스로 트래픽을 AWS PrivateLink보냅니다. 리소스 VPC 엔드포인트를 생성하면, VPC 및 온프레미스에서 리소스와 통신할 때 사용할 수 있는 리전별 DNS 이름(기본 DNS 이름)이 생성됩니다. 따라서 리소스에 연결할 때는 엔드포인트 IP 대신 DNS를 사용하는 것이 좋습니다. 리소스 VPC 엔드포인트의 기본 DNS 이름 구문은 다음과 같습니다.

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

ARN을 사용하는 일부 리소스 구성에 대해 리소스 VPC 엔드포인트를 생성할 때 프라이빗 DNS를 활성화할 수 있습니다. 프라이빗 DNS를 사용하면 리소스 VPC 엔드포인트를 통한 프라이빗 연결을 활용하면서 AWS 서비스에서 리소스에 프로비저닝된 DNS 이름을 사용하여 리소스에 계속 요청할 수 있습니다. 자세한 내용은 the section called “DNS 확인” 단원을 참조하십시오.

다음 describe-vpc-endpoint-associations 명령을 사용하면 리소스 엔드포인트의 DNS 항목을 확인할 수 있습니다.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].*'
```

다음은 프라이빗 DNS가 활성화된 Amazon RDS 데이터베이스용 리소스 엔드포인트의 예시 출력입니다. 첫 번째 DNS 이름은 기본 DNS 이름입니다. 두 번째 DNS 이름은 숨겨진 프라이빗 호스팅 영역의 엔드포인트로, 퍼블릭 엔드포인트에 대한 요청을 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인합니다.

```
[
    [
        "vpce-rsc-asc-abcd1234abcd",
        "vpce-123456789abcdefgh",
        "Accessible",
        {
            "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
            "HostedZoneId": "ABCDEFGH123456789000"
        },
        {
            "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
            "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
        },
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefg",
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
    ]
]
```

DNS 확인

리소스 VPC 엔드포인트에 대해 생성되는 DNS 레코드는 공개 상태입니다. 따라서 해당 DNS 이름은 공개적으로 확인할 수 있습니다. 그러나 VPC 외부에서의 DNS 요청은 여전히 리소스 엔드포인트의 네트워크 인터페이스가 가진 비공개 IP 주소를 반환합니다. 따라서 VPN 또는 Direct Connect를 통해 리소스 엔드포인트가 속한 VPC에 액세스할 수 있다면, 온프레미스에서도 이 DNS 이름을 사용하여 리소스에 액세스할 수 있습니다.

프라이빗 DNS

ARNs을 사용하는 일부 리소스 구성에 대해 리소스 VPC 엔드포인트에 대해 프라이빗 DNS를 활성화하고 VPC에 DNS 호스트 이름과 DNS 확인이 모두 활성화된 경우 사용자 지정 DNS 이름을 사용하여 리소스 구성을 위한 숨겨진 AWS관리형 프라이빗 호스팅 영역을 생성합니다. 이 호스팅 영역에는 VPC 내 리소스 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인되는 리소스에 대한 기본 DNS 이름의 레코드 세트가 포함됩니다.

Amazon은 Route 53 Resolver라고 하는 VPC용 DNS 서버를 제공합니다. Route 53 Resolver는 프라이빗 호스팅 영역의 로컬 VPC 도메인 이름 및 레코드를 자동으로 확인합니다. 하지만 VPC 외부에서는 Route 53 Resolver를 사용할 수 없습니다. 온프레미스 네트워크에서 VPC 엔드포인트에 액세스하려는 경우 사용자 지정 DNS 이름을 사용하거나 Route 53 Resolver 엔드포인트 및 Resolver 규칙을 사용할 수 있습니다. 자세한 내용은 AWS PrivateLink 및 AWS Transit Gateway 와 통합을 참조하세요 Amazon Route 53 Resolver.

서브넷 및 가용 영역

가용 영역당 1개의 서브넷으로 VPC 엔드포인트를 구성할 수 있습니다. 서브넷의 VPC 엔드포인트에 대한 엔드포인트 네트워크 인터페이스가 생성됩니다. VPC 엔드포인트의 IP 주소 유형에 따라 서브넷의 각 엔드포인트 네트워크 인터페이스에 IP 주소가 할당됩니다. 프로덕션 환경에서는 고가용성과 복원력을 위해 각 VPC 엔드포인트에 대해 최소 2개의 가용 영역을 구성하는 것이 좋습니다.

IP 주소 유형

리소스 엔드포인트는 IPv4, IPv6 또는 듀얼 스택 주소를 지원할 수 있습니다. IPv6를 지원하는 엔드포인트는 AAAA 레코드를 사용하여 DNS 쿼리에 응답할 수 있습니다. 리소스 엔드포인트의 IP 주소 유형은 여기에 설명된 대로 인터페이스 엔드포인트의 서브넷과 호환되어야 합니다.

- IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.

- IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
- 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

리소스 VPC 엔드포인트가 IPv4를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv4 주소가 있습니다. 리소스 VPC 엔드포인트가 IPv6를 지원하는 경우 엔드포인트 네트워크 인터페이스에 IPv6 주소가 있습니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이 활성화됩니다.

리소스 VPC 엔드포인트를 통해 리소스에 액세스

리소스 VPC 엔드포인트를 사용하면 도메인 이름, IP 주소 또는 Amazon RDS 데이터베이스와 같은 VPC 리소스에 액세스할 수 있습니다. 리소스 엔드포인트는 리소스에 대한 프라이빗 액세스를 제공합니다. 리소스 엔드포인트를 생성할 때는 단일, 그룹 또는 ARN 유형의 리소스 구성을 지정해야 합니다. 하나의 리소스 엔드포인트는 하나의 리소스 구성과만 연결될 수 있으며, 리소스 구성은 단일 리소스 또는 리소스 그룹을 나타낼 수 있습니다.

사전 조건

리소스 엔드포인트를 생성하려면 다음 사전 조건을 충족해야 합니다.

- 자신이 생성했거나 다른 계정에서 AWS RAM을 통해 공유받은 리소스 구성이 있어야 합니다.
- 다른 계정에서 공유받은 리소스 구성인 경우, 해당 리소스 구성을 포함하는 리소스 공유를 검토하고 수락해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 초대 수락 및 거부를 참조하세요.

VPC 리소스 엔드포인트 생성

다음 절차에 따라 VPC 리소스 엔드포인트를 생성합니다. 리소스 엔드포인트를 생성한 후에는 해당 보안 그룹 또는 태그만 수정할 수 있습니다.

VPC 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.

3. 엔드포인트 생성을 선택합니다.
4. 엔드포인트를 쉽게 찾고 관리할 수 있도록 이름을 지정할 수 있습니다.
5. 유형에서 리소스를 선택합니다.
6. 리소스 구성에서 리소스 구성을 선택합니다.
7. 네트워크 설정에서 리소스에 액세스할 VPC를 선택합니다.
8. 리소스 구성에 대한 프라이빗 DNS 지원을 구성하려면 추가 설정, DNS 이름 활성화를 선택합니다. 이 기능을 사용하려면 VPC에서 DNS 호스트 이름 활성화와 DNS 지원 활성화 속성이 활성화되어 있어야 합니다. 자세한 내용은 the section called “리소스 소비자의 사용자 지정 도메인 이름” 단원을 참조하십시오.
9. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다.

   프로덕션 환경에서는 고가용성과 복원력을 위해 각 VPC 엔드포인트에 대해 최소 2개의 가용 영역을 구성하는 것이 좋습니다.
10. 보안 그룹에서 보안 그룹을 선택합니다.

    보안 그룹을 지정하지 않은 경우 VPC에 대한 기본 보안 그룹이 연결됩니다.
11. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(Windows PowerShell용 도구)

리소스 엔드포인트 관리

리소스 엔드포인트를 생성한 후에는 해당 보안 그룹 또는 태그를 관리할 수 있습니다.

태스크

- 엔드포인트 삭제
- 엔드포인트 업데이트

엔드포인트 삭제

VPC 엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다.

콘솔을 사용하여 엔드포인트 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 표시되면 **delete**를 입력합니다.
6. 삭제를 선택합니다.

명령줄을 사용하여 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(Windows PowerShell용 도구)

엔드포인트 업데이트

VPC 엔드포인트를 업데이트할 수 있습니다.

콘솔을 사용하여 엔드포인트 업데이트하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트를 선택합니다.
4. 작업과 적절한 옵션을 선택합니다.
5. 콘솔 단계에 따라 업데이트를 제출합니다.

명령줄을 사용하여 엔드포인트 업데이트하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

VPC 리소스에 대한 리소스 구성

리소스 구성은 다른 VPC 및 계정의 클라이언트가 액세스할 수 있는 리소스 또는 리소스 그룹을 나타냅니다. 리소스 구성을 정의하면, 다른 VPC 및 계정의 클라이언트가 사용자 VPC의 리소스에 대한 안전

한 프라이빗 단방향 네트워크 연결을 허용할 수 있습니다. 리소스 구성은 트래픽을 수신하는 리소스 게이트웨이와 연결됩니다.

내용

리소스 구성 유형

리소스 구성은 여러 유형이 있을 수 있습니다. 서로 다른 유형은 다양한 종류의 리소스를 표현하는 데 사용됩니다. 다음과 같은 유형이 있습니다.

- 단일 리소스 구성: IP 주소 또는 도메인 이름. 독립적으로 공유할 수 있습니다.
- 그룹 리소스 구성: 하위 리소스 구성의 모음. 독립적으로 공유할 수 있습니다.
- 하위 리소스 구성: 그룹 리소스 구성의 구성원. IP 주소 또는 도메인 이름을 나타냅니다. 독립적으로 공유할 수 없으며 그룹의 일부로만 공유할 수 있습니다. 자유롭게 그룹에 추가하거나 그룹에서 제거할 수 있습니다. 추가하면 해당 그룹에 액세스할 수 있는 모든 사람이 자동으로 액세스할 수 있게 됩니다.
- ARN 리소스 구성: AWS 서비스에 의해 프로비저닝되는 지원되는 리소스 유형을 나타냅니다. 예를 들면 Amazon RDS 데이터베이스입니다. 하위 리소스 구성은 AWS에서 자동으로 관리합니다.

리소스 게이트웨이

리소스 구성은 리소스 게이트웨이와 연결됩니다. 리소스 게이트웨이는 해당 리소스가 위치한 VPC로 들어오는 진입 지점 역할을 하는 탄력적 네트워크 인터페이스(ENI)의 집합입니다. 여러 리소스 구성을 동일한 리소스 게이트웨이에 연결할 수 있습니다. 다른 VPC 또는 계정의 클라이언트가 사용자 VPC에 있는 리소스에 액세스하면 해당 리소스는 트래픽이 그 VPC 내의 리소스 게이트웨이에서 로컬로 들어오는 것처럼 인식합니다.

리소스 공급자의 사용자 지정 도메인 이름

리소스 공급자는 리소스 소비자가 리소스 구성에 액세스하는 데 사용할 수 `example.com`있는와 같은 리소스 구성에 사용자 지정 도메인 이름을 연결할 수 있습니다. 사용자 지정 도메인 이름은 리소스 공급자가 소유 및 확인하거나 타사 또는 AWS 도메인일 수 있습니다. 리소스 공급자는 리소스 구성을 사용하여 캐시 클러스터 및 Kafka 클러스터, TLS 기반 애플리케이션 또는 기타 AWS 리소스를 공유할 수 있습니다.

리소스 구성 공급자에는 다음 고려 사항이 적용됩니다.

- 리소스 구성에는 사용자 지정 도메인이 하나만 있을 수 있습니다.
- 리소스 구성의 사용자 지정 도메인 이름은 변경할 수 없습니다.
- 사용자 지정 도메인 이름은 모든 리소스 구성 소비자에게 표시됩니다.
- VPC Lattice의 도메인 이름 확인 프로세스를 사용하여 사용자 지정 도메인 이름을 확인할 수 있습니다. 자세한 내용은 단원을 참조하십시오https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html.
- 유형 그룹 및 하위 유형의 리소스 구성의 경우 먼저 그룹 리소스 구성에서 그룹 도메인을 지정해야 합니다. 이후 하위 리소스 구성에는 그룹 도메인의 하위 도메인인 사용자 지정 도메인이 있을 수 있습니다. 그룹에 그룹 도메인이 없는 경우 하위에 대한 사용자 지정 도메인 이름을 사용할 수 있지만 VPC Lattice는 리소스 소비자의 VPC에서 하위 도메인 이름에 대한 호스팅 영역을 프로비저닝하지 않습니다.

리소스 소비자의 사용자 지정 도메인 이름

리소스 소비자가 사용자 지정 도메인 이름이 있는 리소스 구성에 대한 연결을 활성화하면 VPC Lattice가 VPC에서 Route 53 프라이빗 호스팅 영역을 관리하도록 허용할 수 있습니다. 리소스 소비자는 VPC Lattice가 프라이빗 호스팅 영역을 관리할 수 있도록 허용할 도메인에 대해 세분화된 옵션이 있습니다.

리소스 소비자는 리소스 엔드포인트, 서비스 네트워크 엔드포인트 또는 서비스 네트워크 VPC 연결을 통해 리소스 구성에 대한 연결을 활성화할 때 `private-dns-enabled` 파라미터를 설정할 수 있습니다. `private-dns-enabled` 파라미터와 함께 소비자는 DNS 옵션을 사용하여 VPC Lattice가 프라이빗 호스팅 영역을 관리할 도메인을 지정할 수 있습니다. 소비자는 다음 프라이빗 DNS 기본 설정 중에서 선택할 수 있습니다.

`ALL_DOMAINS`

VPC Lattice는 모든 사용자 지정 도메인 이름에 프라이빗 호스팅 영역을 프로비저닝합니다.

`VERIFIED_DOMAINS_ONLY`

VPC Lattice는 공급자가 사용자 지정 도메인 이름을 확인한 경우에만 프라이빗 호스팅 영역을 프로비저닝합니다.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

VPC Lattice는 확인된 모든 사용자 지정 도메인 이름 및 리소스 소비자가 지정하는 기타 도메인 이름에 대해 프라이빗 호스팅 영역을 프로비저닝합니다. 리소스 소비자는 `private DNS specified domains` 파라미터에 도메인 이름을 지정합니다.

`SPECIFIED_DOMAINS_ONLY`

VPC Lattice는 리소스 소비자가 지정한 도메인 이름에 대해 프라이빗 호스팅 영역을 프로비저닝합니다. 리소스 소비자는 `private DNS specified domains` 파라미터에 도메인 이름을 지정합니다.

프라이빗 DNS를 활성화하면 VPC Lattice는 리소스 구성과 연결된 사용자 지정 도메인 이름에 대한 프라이빗 호스팅 영역을 VPC에 생성합니다. 기본적으로 프라이빗 DNS 기본 설정은 로 설정됩니다`VERIFIED_DOMAINS_ONLY`. 즉, 리소스 공급자가 사용자 지정 도메인 이름을 확인한 경우에만 프라이빗 호스팅 영역이 생성됩니다. 프라이빗 DNS 기본 설정을 `ALL_DOMAINS` 또는 로 설정하면 `SPECIFIED_DOMAINS_ONLY` VPC Lattice는 사용자 지정 도메인 이름의 확인 상태에 관계없이 프라이빗 호스팅 영역을 생성합니다. 지정된 도메인에 대해 프라이빗 호스팅 영역이 생성되면 VPC에서 해당 도메인으로 가는 모든 트래픽이 VPC Lattice를 통해 라우팅됩니다. 이러한 사용자 지정 도메인 이름에 대한 트래픽이 VPC Lattice를 통과하도록 하려는 경우에만 `ALL_DOMAINS`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS, 또는 `SPECIFIED_DOMAINS_ONLY` 기본 설정을 사용하는 것이 좋습니다.

리소스 소비자는 프라이빗 DNS 기본 설정을 로 설정하는 것이 좋습니다`VERIFIED_DOMAINS_ONLY`. 이를 통해 소비자는 VPC Lattice만 리소스 소비자 계정의 확인된 도메인에 프라이빗 호스팅 영역을 프로비저닝하도록 허용하여 보안 경계를 좁힐 수 있습니다.

프라이빗 DNS 지정 도메인에서 도메인을 선택하기 위해 리소스 소비자는와 같은 정규화된 도메인 이름을 입력my.example.com하거나와 같은 와일드카드를 사용할 수 있습니다*.example.com.

리소스 구성 소비자에게는 다음 고려 사항이 적용됩니다.

- 프라이빗 DNS 활성화 파라미터는 변경할 수 없습니다.
- VPC에서 프라이빗 호스팅을 생성하려면 서비스 네트워크 리소스 연결에서 프라이빗 DNS를 활성화해야 합니다. 리소스 구성의 경우 서비스 네트워크 리소스 연결의 프라이빗 DNS 활성화 상태는 서비스 네트워크 엔드포인트 또는 서비스 네트워크 VPC 연결의 프라이빗 DNS 활성화 상태를 재정의합니다.

서비스 네트워크 소유자의 사용자 지정 도메인 이름

서비스 네트워크 리소스 연결의 프라이빗 DNS 지원 속성은 서비스 네트워크 엔드포인트 및 서비스 네트워크 VPC 연결의 프라이빗 DNS 지원 속성을 재정의합니다.

서비스 네트워크 소유자가 서비스 네트워크 리소스 연결을 생성하고 프라이빗 DNS를 활성화하지 않는 경우 VPC Lattice는 서비스 네트워크 엔드포인트 또는 서비스 네트워크 VPCs 연결에서 프라이빗 DNS가 활성화되어 있더라도 서비스 네트워크가 연결된 VPC에서 해당 리소스 구성에 대한 프라이빗 호스팅 영역을 프로비저닝하지 않습니다.

ARN 유형의 리소스 구성의 경우 프라이빗 DNS 플래그는 true이고 변경할 수 없습니다.

리소스 정의

리소스 구성에서 리소스를 다음 방법 중 하나로 식별할 수 있습니다.

- Amazon 리소스 이름(ARN) 기준: AWS 서비스에서 프로비저닝하는 지원되는 리소스 유형은 해당 ARN으로 식별할 수 있습니다. 지원되는 리소스는 Amazon RDS 데이터베이스뿐입니다. 공개적으로 액세스할 수 있는 클러스터에 대한 리소스 구성은 생성할 수 없습니다.
- 도메인 이름 대상으로 식별: 공개적으로 확인할 수 있는 도메인 이름을 지정할 수 있습니다 도메인 이름이 VPC 외부의 IP를 가리키는 경우, VPC 내에 NAT 게이트웨이가 있어야 합니다.
- IP 주소로 식별: IPv4의 경우 10.0.0.0/8, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16 범위 내의 프라이빗 IP를 지정합니다. IPv6의 경우 VPC 내의 IP를 지정합니다. 퍼블릭 IP는 지원되지 않습니다.

프로토콜

리소스 구성을 생성할 때 리소스가 지원할 프로토콜을 정의할 수 있습니다. 현재는 TCP 프로토콜만 지원됩니다.

포트 범위

리소스 구성을 생성할 때 요청을 수락할 포트를 정의할 수 있습니다. 다른 포트에 대한 클라이언트 액세스는 허용되지 않습니다.

리소스 액세스

소비자는 VPC 엔드포인트를 사용하거나 서비스 네트워크를 통해 리소스 구성을 직접 액세스할 수 있습니다. 소비자로서, 자신의 VPC에서 동일 계정 내 리소스 구성이나 다른 계정에서 AWS RAM을 통해 공유된 리소스 구성에 대한 액세스를 활성화할 수 있습니다.

- 리소스 구성에 직접 액세스

  AWS PrivateLink VPC에서 리소스 유형의 VPC 엔드포인트(리소스 엔드포인트)를 생성하여 VPC에서 리소스 구성에 비공개로 액세스할 수 있습니다. 리소스 엔드포인트를 생성하는 방법에 대한 자세한 내용은 AWS PrivateLink사용 설명서의 VPC 리소스 액세스를 참조하세요.
- 서비스 네트워크를 통한 리소스 구성 액세스

  리소스 구성을 서비스 네트워크에 연결하고 VPC를 서비스 네트워크에 연결할 수 있습니다. 연결을 통해 또는 서비스 네트워크 VPC 엔드포인트를 사용하여 VPC를 AWS PrivateLink 서비스 네트워크에 연결할 수 있습니다.

  서비스 네트워크 연결에 대한 자세한 내용은 VPC Lattice 서비스 네트워크 연결 관리를 참조하세요.

  서비스 네트워크 VPC 엔드포인트에 대한 자세한 내용은 AWS PrivateLink 사용 설명서의 서비스 네트워크 액세스를 참조하세요.

VPC에서 프라이빗 DNS가 활성화된 경우, 동일한 리소스 구성에 대해 리소스 엔드포인트와 서비스 네트워크 엔드포인트를 동시에 생성할 수 없습니다.

서비스 네트워크 유형과의 연결

Account-B와 같은 소비자 계정과 리소스 구성을 공유하는 경우 Account AWS RAM-B는 리소스 VPC 엔드포인트 또는 서비스 네트워크를 통해 리소스 구성에 직접 액세스할 수 있습니다.

서비스 네트워크를 통해 리소스 구성에 액세스하려면, Account-B가 해당 리소스 구성을 서비스 네트워크에 연결해야 합니다. 서비스 네트워크는 계정 간에 공유할 수 있습니다. 따라서 Account-B는 (리소스 구성이 연결된) 자신의 서비스 네트워크를 Account-C와 공유하여 Account-C에서도 해당 리소스에 액세스할 수 있습니다.

이러한 전이적 공유를 방지하려면, 리소스 구성을 계정 간 공유가 가능한 서비스 네트워크에 추가할 수 없도록 지정할 수 있습니다. 이 설정을 하면 Account-B는 해당 리소스를 앞으로 다른 계정과 공유되거나 공유 가능한 서비스 네트워크에 추가할 수 없습니다.

서비스 네트워크 유형

Account-B와 같은 다른 계정과 리소스 구성을 공유할 때 Account AWS RAM-B는 다음 세 가지 방법 중 하나로 리소스에 액세스할 수 있습니다.

- 리소스 유형의 VPC 엔드포인트 사용(리소스 VPC 엔드포인트).
- 서비스 네트워크 유형의 VPC 엔드포인트 사용(서비스 네트워크 VPC 엔드포인트).
- 서비스 네트워크 VPC 연결 사용.

  서비스 네트워크 연결을 사용하는 경우 각 리소스에는 AWS 소유 및 라우팅할 수 없는 129.224.0.0/17 블록의 서브넷당 IP가 할당됩니다. 이는 VPC Lattice가 트래픽을 VPC Lattice 네트워크를 통해 서비스로 라우팅할 때 사용하는 관리형 접두사 목록과 별도로 적용됩니다. 이 두 IP 모두 VPC 라우팅 테이블에 업데이트됩니다.

서비스 네트워크 VPC 엔드포인트와 서비스 네트워크 VPC 연결을 사용하는 경우, 리소스 구성은 Account-B의 서비스 네트워크에 포함되어야 합니다. 서비스 네트워크는 계정 간 공유가 가능합니다. 따라서 Account-B는 (리소스 구성을 포함한) 자신의 서비스 네트워크를 Account-C와 공유하여 Account-C에서도 리소스에 액세스할 수 있습니다. 이러한 전이적 공유를 방지하려면, 리소스 구성이 계정 간 공유 가능한 서비스 네트워크에 추가되지 않도록 지정할 수 있습니다. 이 설정을 하면 Account-B는 해당 리소스를 공유되거나 공유 가능한 서비스 네트워크에 추가할 수 없습니다.

를 통해 리소스 구성 공유 AWS RAM

리소스 구성은와 통합됩니다 AWS Resource Access Manager. AWS RAM을 통해 리소스 구성을 다른 계정과 공유할 수 있습니다. 리소스 구성을 AWS 계정과 공유하면 해당 계정의 클라이언트가 리소스에 비공개로 액세스할 수 있습니다. 리소스 구성은 AWS RAM의 리소스 공유를 사용하여 공유할 수 있습니다.

AWS RAM 콘솔을 사용하여 추가된 리소스 공유, 액세스할 수 있는 공유 리소스, 리소스를 공유한 AWS 계정을 볼 수 있습니다. 자세한 내용은 AWS RAM 사용 설명서의 공유받은 리소스를 참조하세요.

리소스 구성과 동일한 계정의 다른 VPC에서 리소스에 액세스하려면 리소스 구성을 공유할 필요가 없습니다 AWS RAM.

모니터링

리소스 구성에서 모니터링 로그를 활성화할 수 있습니다. 로그를 전송할 대상을 선택할 수 있습니다.

VPC Lattice에서 리소스 구성 생성

리소스 구성을 생성합니다.

AWS Management Console

콘솔을 사용하여 리소스 구성 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 PrivateLink 및 Lattice에서 리소스 구성을 선택합니다.
3. 리소스 구성 생성을 선택합니다.
4. AWS 계정 내에서 고유한 이름을 입력합니다. 리소스 구성이 생성된 후에는 이 이름을 변경할 수 없습니다.
5. 구성 유형에서 단일 또는 하위 리소스용 리소스 또는 하위 리소스 그룹용 리소스 그룹을 선택합니다.
6. 이전에 생성한 리소스 게이트웨이를 선택하거나 새로 생성합니다.
7. (선택 사항) 사용자 지정 도메인 이름을 입력하려면 다음 중 하나를 수행합니다.
   - 단일 유형의 리소스 구성이 있는 경우 사용자 지정 도메인 이름을 입력할 수 있습니다. 리소스 소비자는이 도메인 이름을 사용하여 리소스 구성에 액세스할 수 있습니다.
   - 유형 그룹 및 하위의 리소스 구성이 있는 경우 먼저 그룹 리소스 구성에서 그룹 도메인을 지정해야 합니다. 다음으로 하위 리소스 구성에는 그룹 도메인의 하위 도메인인 사용자 지정 도메인이 있을 수 있습니다.
8. (선택 사항) 확인 ID를 입력합니다.

   도메인 이름을 확인하려는 경우 확인 ID를 제공합니다. 이를 통해 리소스 소비자는 사용자가 도메인 이름을 소유하고 있음을 알 수 있습니다.
9. 이 리소스 구성으로 나타낼 리소스의 식별자를 선택합니다.
10. 리소스를 공유할 포트 범위를 선택합니다.
11. 연결 설정에서 이 리소스 구성을 공유 가능한 서비스 네트워크와 연결할 수 있는지 여부를 지정합니다.

12. 리소스 구성 공유에서 이 리소스에 액세스할 수 있는 보안 주체를 식별하는 리소스 공유를 선택합니다.
13. (선택 사항) 모니터링에서 리소스 액세스 로그와 전송 대상을 활성화하여 리소스 구성을 오가는 요청과 응답을 모니터링할 수 있습니다.
14. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
15. 리소스 구성 생성을 선택합니다.

AWS CLI

다음 create-resource-configuration 명령은 단일 리소스 구성을 생성하고 이를 사용자 지정 도메인 이름과 연결합니다`example.com`.

```
aws vpc-lattice create-resource-configuration \
    --name my-resource-config \
    --type SINGLE \
    --resource-gateway-identifier rgw-0bba03f3d56060135 \
    --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
    --custom-domain-name example.com \
    --verification-id dv-aaaa0000000111111
```

다음 create-resource-configuration 명령은 그룹 리소스 구성을 생성하고 이를 사용자 지정 도메인 이름과 연결합니다`example.com`.

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa0000000111111
```

다음 create-resource-configuration 명령은 하위 리소스 구성을 생성하고 이를 사용자 지정 도메인 이름과 연결합니다`child.example.com`.

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
  --type CHILD \
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-
west-2.elb.amazonaws.com,ipAddressType=IPV4}' \
  --resource-configuration-group-identifier rcfg-07129f3acded87626 \
```

```
--custom-domain-name child.example.com
```

VPC Lattice 리소스 구성을 위한 연결 관리

리소스 구성을 공유한 소비자 계정과 본인 계정의 클라이언트는 해당 리소스 구성에 직접 리소스 VPC 엔드포인트를 통해 액세스하거나 서비스 네트워크 엔드포인트를 통해 액세스할 수 있습니다. 이로 인해 리소스 구성에는 엔드포인트 연결과 서비스 네트워크 연결이 생성됩니다.

서비스 네트워크 리소스 연결 관리

서비스 네트워크 연결을 생성하거나 삭제할 수 있습니다.

> **Note**
>
> 서비스 네트워크와 리소스 구성 간의 연결을 생성하는 동안 액세스 거부 메시지가 표시되면 AWS RAM 정책 버전을 확인하고 버전 2인지 확인합니다. 자세한 내용은 AWS RAM 사용 설명서를 참조하세요.

콘솔을 사용하여 서비스-네트워크 연결 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 PrivateLink 및 Lattice에서 리소스 구성을 선택합니다.
3. 리소스 구성의 이름을 선택하여 세부 정보 페이지를 엽니다.
4. 서비스 네트워크 연결 탭을 선택합니다.
5. 연결 생성을 선택합니다.
6. VPC Lattice 서비스 네트워크에서 서비스 네트워크를 선택합니다. 서비스 네트워크를 생성하려면 VPC Lattice 네트워크 생성을 선택합니다.
7. (선택 사항) 태그를 추가하려면 서비스 연결 태그를 확장하고 새 태그 추가를 선택하여 태그 키와 태그 값을 입력합니다.
8. (선택 사항)이 서비스 네트워크 리소스 연결에 프라이빗 DNS 이름을 활성화하려면 프라이빗 DNS 이름 활성화를 선택합니다. 자세한 내용은 the section called “서비스 네트워크 소유자의 사용자 지정 도메인 이름” 단원을 참조하십시오.
9. 변경 사항 저장을 선택합니다.
10. 연결을 삭제하려면 연결의 확인란을 선택한 다음 작업, 삭제를 선택합니다. 확인 메시지가 나타나면 **confirm**을 입력한 다음 삭제를 선택합니다.

를 사용하여 서비스 네트워크 연결을 생성하려면 AWS CLI

create-service-network-resource-association 명령을 사용합니다.

를 사용하여 서비스 네트워크 연결을 삭제하려면 AWS CLI

delete-service-network-resource-association 명령을 사용합니다.

리소스 VPC 엔드포인트 연결 관리

리소스 구성에 액세스할 수 있는 소비자 계정 또는 계정의 클라이언트는 리소스 VPC 엔드포인트를 사용하여 리소스 구성에 액세스할 수 있습니다. 리소스 구성에 사용자 지정 도메인 이름이 있는 경우 프라이빗 DNS 활성화를 사용하여 VPC Lattice가 리소스 엔드포인트 또는 서비스 네트워크 엔드포인트에 프라이빗 호스팅 영역을 프로비저닝하도록 허용할 수 있습니다. 이를 통해 클라이언트는 도메인 이름을 직접 컬링하여 리소스 구성에 액세스할 수 있습니다. 자세한 내용은 the section called “리소스 소비자의 사용자 지정 도메인 이름” 단원을 참조하십시오.

AWS Management Console

1. 새 엔드포인트 연결을 생성하려면 왼쪽 탐색 창에서 PrivateLink 및 Lattice로 이동하여 엔드포인트를 선택합니다.
2. 엔드포인트 생성을 선택합니다.
3. VPC에 연결할 리소스 구성을 선택합니다.
4. VPC, 서브넷 및 보안 그룹을 선택합니다.
5. (선택 사항) 프라이빗 DNS를 켜고 DNS 옵션을 구성하려면 DNS 이름 활성화를 선택합니다.
6. (선택 사항) VPC 엔드포인트에 태그를 지정하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
7. 엔드포인트 생성을 선택합니다.

AWS CLI

다음 create-vpc-endpoint 명령은 프라이빗 DNS를 사용하는 VPC 엔드포인트를 생성합니다. 프라이빗 DNS 기본 설정은 로 설정VERIFIED_AND_SELECTED되고 선택한 도메인은 example.com 및 입니다example.org. VPC Lattice는 확인된 도메인 또는 example.com에 대해서만 프라이빗 호스팅 영역을 프로비저닝합니다example.org.

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
```

```
  --vpc-id vpc-111122223333aabbc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

를 사용하여 VPC 엔드포인트 연결을 생성하려면 AWS CLI

create-vpc-endpoint 명령을 사용합니다.

를 사용하여 VPC 엔드포인트 연결을 삭제하려면 AWS CLI

delete-vpc-endpoint 명령을 사용합니다.

VPC Lattice의 리소스 게이트웨이

리소스 게이트웨이는 리소스가 존재하는 VPC로 들어오는 트래픽의 진입 지점입니다. 여러 가용 영역에 걸쳐 구성됩니다.

다른 VPC나 계정에서 VPC 내 리소스에 액세스할 계획이라면, 해당 VPC에는 반드시 리소스 게이트웨이가 있어야 합니다. 공유하는 모든 리소스는 리소스 게이트웨이와 연결됩니다. 다른 VPC 또는 계정의 클라이언트가 사용자 VPC에 있는 리소스에 액세스하면 해당 리소스는 트래픽이 그 VPC 내의 리소스 게이트웨이에서 로컬로 들어오는 것처럼 인식합니다. 트래픽의 소스 IP는 리소스 게이트웨이의 IP 주소입니다. 리소스 게이트웨이에 여러 개의 IP 주소를 할당하여 리소스와의 네트워크 연결을 확장할 수 있습니다. 하나의 VPC 내 여러 리소스가 동일한 리소스 게이트웨이와 연결될 수 있습니다.

리소스 게이트웨이는 로드 밸런싱 기능을 제공하지 않습니다.

내용

- 고려 사항
- 보안 그룹
- IP 주소 유형
- ENI당 IPv4 주소
- VPC Lattice에서 리소스 게이트웨이 생성
- VPC Lattice에서 리소스 게이트웨이 삭제

고려 사항

리소스 게이트웨이에는 다음과 같은 고려 사항이 적용됩니다.

- 리소스가 모든 가용 영역에서 액세스 가능하도록 하려면, 리소스 게이트웨이를 가능한 많은 가용 영역에 걸쳐 생성하는 것이 좋습니다.
- VPC 엔드포인트와 리소스 게이트웨이는 최소 1개 이상 가용 영역이 겹쳐야 합니다.
- 하나의 VPC에는 최대 100개의 리소스 게이트웨이를 생성할 수 있습니다. 자세한 내용은 VPC Lattice 할당량을 참조하세요.
- 공유 서브넷에서는 리소스 게이트웨이를 생성할 수 없습니다.

보안 그룹

리소스 게이트웨이에 보안 그룹을 연결할 수 있습니다. 리소스 게이트웨이에 대한 보안 그룹 규칙은 리소스 게이트웨이에서 리소스로 향하는 아웃바운드 트래픽을 제어합니다.

데이터베이스 리소스로 향하는 리소스 게이트웨이 트래픽에 권장되는 아웃바운드 규칙

리소스 게이트웨이에서 리소스로 트래픽이 흐르도록 하려면, 리소스에서 허용하는 리스너 프로토콜과 포트 범위에 대한 아웃바운드 규칙을 생성해야 합니다.

Destination	프로토콜	포트 범위	설명
#### CIDR ##	TCP	3306	리소스 게이트웨이에서 데이터베이스로 향하는 트래픽을 허용합니다.

IP 주소 유형

리소스 게이트웨이에는 IPv4, IPv6 또는 듀얼 스택 주소가 있을 수 있습니다. 리소스 게이트웨이의 IP 주소 유형은 여기에 설명된 대로 리소스 게이트웨이의 서브넷과 리소스의 IP 주소 유형과 호환되어야 합니다.

- IPv4 - 게이트웨이 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있고, 리소스에도 IPv4 주소가 있는 경우에만 지원됩니다.

- IPv6 - 게이트웨이 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷이고, 리소스에도 IPv6 주소가 있는 경우에만 지원됩니다.
- 듀얼 스택 - 게이트웨이 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4와 IPv6 주소 범위가 모두 있고, 리소스에 IPv4 또는 IPv6 주소가 있는 경우에만 지원됩니다.

리소스 게이트웨이의 IP 주소 유형은 클라이언트의 IP 주소 유형 또는 리소스에 액세스하는 VPC 엔드포인트와 독립적입니다.

ENI당 IPv4 주소

리소스 게이트웨이가 IPv4 또는 듀얼 스택 IP 주소 유형을 사용하는 경우, 리소스 게이트웨이의 각 ENI에 할당할 IPv4 주소 수를 구성할 수 있습니다. 리소스 게이트웨이를 생성할 때 1에서 62까지의 IPv4 주소 중에서 선택합니다. 한 번 설정한 IPv4 주소 수는 변경할 수 없습니다.

IPv4 주소는 네트워크 주소 변환에 사용되며, 리소스에 대한 동시 IPv4 연결의 최대 수를 결정합니다. 기본적으로 모든 리소스 게이트웨이에는 ENI당 16개의 IPv4 주소가 할당됩니다. 이는 백엔드 리소스와 연결을 형성하기에 적절한 IP 수입니다.

리소스 게이트웨이가 IPv6 주소 유형을 사용하는 경우, 리소스 게이트웨이는 자동으로 ENI당 /80 CIDR을 수신합니다. 이 값은 변경할 수 없습니다.

VPC Lattice에서 리소스 게이트웨이 생성

콘솔을 사용하여 리소스 게이트웨이를 생성합니다.

콘솔을 사용하여 리소스 게이트웨이 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 PrivateLink 및 Lattice에서 리소스 게이트웨이를 선택합니다.
3. 리소스 게이트웨이 생성을 선택합니다.
4. AWS 계정 내에서 고유한 이름을 입력합니다.
5. 리소스 게이트웨이의 IP 주소 유형을 선택합니다.
6. IP 주소 유형에서 리소스 게이트웨이트의 IP 주소 유형을 선택합니다.
    - IPv4 또는 듀얼 스택을 IP 주소 유형으로 선택한 경우, 리소스 게이트웨이의 각 ENI에 할당할 IPv4 주소 수를 입력할 수 있습니다.

기본값은 ENI당 16개의 IPv4 주소입니다. 이는 백엔드 리소스와 연결을 형성하기에 적절한 IP 수입니다.

7. 리소스가 속한 VPC를 선택합니다.
8. VPC에서 서비스 네트워크로 들어오는 트래픽을 제어할 최대 5개의 보안 그룹을 선택합니다.
9. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
10. 리소스 게이트웨이 생성을 선택합니다.

를 사용하여 리소스 게이트웨이를 생성하려면 AWS CLI

create-resource-gateway 명령을 사용합니다.

VPC Lattice에서 리소스 게이트웨이 삭제

리소스 게이트웨이를 사용하여 리소스를 삭제합니다.

콘솔을 사용하여 리소스 게이트웨이 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 PrivateLink 및 Lattice에서 리소스 게이트웨이를 선택합니다.
3. 삭제하려는 리소스 게이트웨이의 확인란을 선택한 후 작업, 삭제를 차례로 선택합니다. 확인 메시지가 나타나면 **`confirm`**을 입력한 다음 삭제를 선택합니다.

를 사용하여 리소스 게이트웨이를 삭제하려면 AWS CLI

delete-resource-gateway 명령을 사용합니다.

를 통해 서비스 네트워크에 액세스 AWS PrivateLink

서비스 네트워크 VPC 엔드포인트(서비스-네트워크 엔드포인트)를 사용하면 VPC에서 서비스 네트워크에 비공개로 연결할 수 있습니다. 서비스-네트워크 엔드포인트를 통해 해당 서비스 네트워크와 연결된 리소스와 서비스에 비공개로 안전하게 액세스할 수 있습니다. 이렇게 하면 단일 VPC 엔드포인트를 통해 여러 리소스와 서비스에 비공개로 액세스할 수 있습니다.

서비스 네트워크는 리소스 구성과 VPC Lattice 서비스의 논리적 모음입니다. 서비스-네트워크 엔드포인트를 사용하면 서비스 네트워크를 VPC에 연결하고 VPC 또는 온프레미스에서 해당 리소스와 서비스에 비공개로 액세스할 수 있습니다. 서비스-네트워크 엔드포인트가 하나면 하나의 서비스 네트워크에 연결할 수 있습니다. VPC에서 여러 서비스 네트워크에 연결하려면 각각 다른 서비스 네트워크를 가리키는 서비스-네트워크 엔드포인트를 여러 개 생성하면 됩니다.

서비스 네트워크는 AWS Resource Access Manager ()와 통합됩니다AWS RAM. AWS RAM을 통해 다른 계정과 서비스 네트워크를 공유할 수 있습니다. 서비스 네트워크를 다른 AWS 계정과 공유하는 경우 해당 계정은 서비스 네트워크에 연결할 서비스 네트워크 엔드포인트를 생성할 수 있습니다. 서비스 네트워크는 AWS RAM의 리소스 공유를 통해 공유할 수 있습니다.

AWS RAM 콘솔을 사용하여 추가된 리소스 공유, 액세스할 수 있는 공유 서비스 네트워크, 리소스를 공유한 AWS 계정을 볼 수 있습니다. 자세한 내용은 AWS RAM 사용 설명서의 공유받은 리소스를 참조하세요.

가격 책정

서비스 네트워크와 연결된 리소스 구성에 대해서는 시간 단위로 요금이 청구됩니다. 또한 서비스-네트워크 VPC 엔드포인트를 통해 리소스에 액세스할 때 처리된 데이터량(GB 단위)에 따라 요금이 청구됩니다. 서비스-네트워크 VPC 엔드포인트 자체에는 시간 단위 요금이 부과되지 않습니다. 자세한 내용은 Amazon VPC Lattice 요금을 참조하십시오.

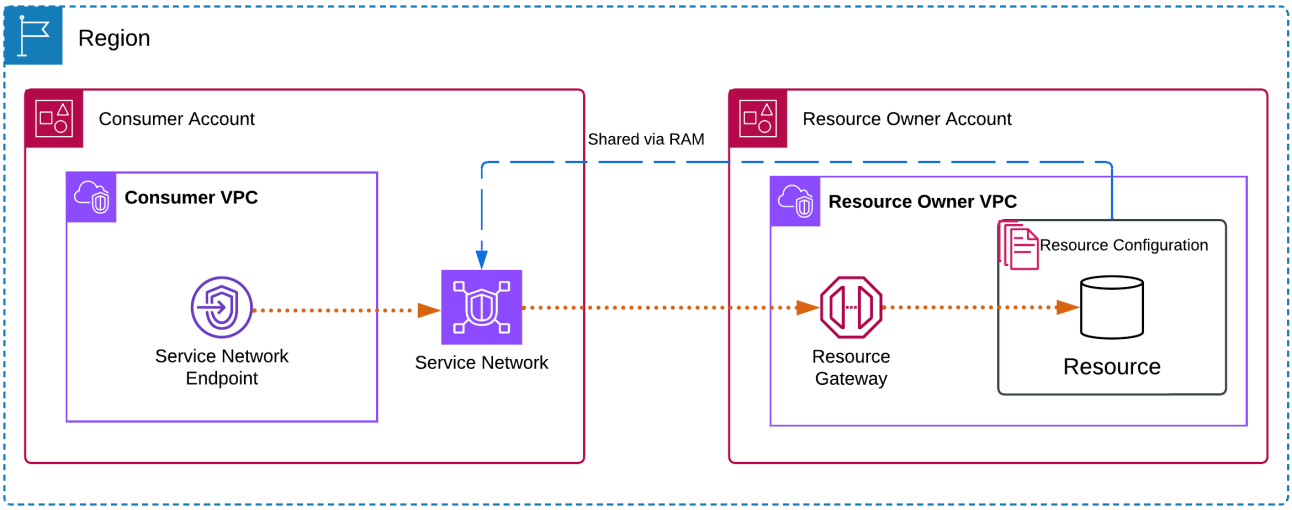
내용

- 서비스-네트워크 엔드포인트 관리

개요

자체 서비스 네트워크를 생성하거나 다른 계정과 서비스 네트워크를 공유할 수 있습니다. 어느 경우든 VPC에서 연결하기 위해 서비스-네트워크 엔드포인트를 생성할 수 있습니다. 서비스 네트워크를 생성하고 리소스 구성을 연결하는 방법에 대한 자세한 내용은 Amazon VPC Lattice 사용 설명서를 참조하세요.

다음 다이어그램은 VPC 내의 서비스-네트워크 엔드포인트가 서비스 네트워크에 액세스하는 방식을 보여줍니다.



네트워크 연결은 서비스-네트워크 엔드포인트가 있는 VPC에서만 서비스 네트워크 내의 리소스와 서비스로 시작할 수 있습니다. 리소스와 서비스가 있는 VPC에서는 엔드포인트 VPC로 네트워크 연결을 시작할 수 없습니다.

DNS 호스트 이름

를 사용하면 프라이빗 엔드포인트를 사용하여 서비스 네트워크로 트래픽을 AWS PrivateLink전송합니다. 서비스-네트워크 VPC 엔드포인트를 생성하면, VPC 또는 온프레미스에서 해당 리소스 및 서비스와 통신할 때 사용할 수 있는 리전별 DNS 이름(기본 DNS 이름이라고 함)이 각 리소스와 서비스에 대해 생성됩니다. 엔드포인트에 연결된 IP 주소는 변경될 수 있습니다. 따라서 서비스 네트워크에 연결할 때는 엔드포인트 IP 대신 DNS를 사용하는 것이 좋습니다.

서비스 네트워크 내 리소스의 기본 DNS 이름 구문은 다음과 같습니다.

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

서비스 네트워크 내 Lattice 서비스의 기본 DNS 이름 구문은 다음과 같습니다.

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

를 사용하는 경우 연결 탭에서 DNS 이름을 찾을 AWS Management Console수 있습니다. 를 사용하는 경우 describe-vpc-endpoint-associations 명령을 AWS CLI사용합니다.

프라이빗 DNS는 서비스 네트워크가 Amazon RDS 데이터베이스 서비스에 대한 ARN 유형 리소스 구성을 가지고 있을 때만 활성화할 수 있습니다. 프라이빗 DNS를 사용하면 AWS 서비스에서 리소스에 프로비저닝된 DNS 이름을 사용하여 리소스에 계속 요청할 수 있으며 서비스 네트워크 VPC 엔드포인트를 통한 프라이빗 연결을 활용할 수 있습니다. 자세한 내용은 the section called “DNS 확인” 단원을 참조하십시오.

DNS 확인

서비스 네트워크 엔드포인트를 생성하면, 해당 서비스 네트워크와 연결된 각 리소스 구성과 Lattice 서비스에 대해 DNS 이름이 생성됩니다. 이 DNS 레코드는 공개 상태입니다. 따라서 해당 DNS 이름은 공개적으로 확인할 수 있습니다. 그러나 VPC 외부에서의 DNS 요청은 여전히 서비스-네트워크 엔드포인트의 네트워크 인터페이스가 가진 프라이빗 IP 주소를 반환합니다. 따라서 VPN 또는 Direct Connect를 통해 서비스-네트워크 엔드포인트가 속한 VPC에 액세스할 수 있다면, 온프레미스에서도 이 DNS 이름을 사용하여 리소스와 서비스에 액세스할 수 있습니다.

프라이빗 DNS

서비스 네트워크 VPC 엔드포인트에 대해 프라이빗 DNS를 활성화하고 VPC에 DNS 호스트 이름과 DNS 확인이 모두 활성화된 경우 사용자 지정 DNS 이름이 있는 리소스 구성에 대해 숨겨진 AWS관리형 프라이빗 호스팅 영역이 생성됩니다. 이 호스팅 영역에는 VPC 내 서비스-네트워크 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소로 확인되는 리소스에 대한 기본 DNS 이름의 레코드 세트가 포함됩니다.

Amazon은 Route 53 Resolver라고 하는 VPC용 DNS 서버를 제공합니다. Route 53 Resolver는 프라이빗 호스팅 영역의 로컬 VPC 도메인 이름 및 레코드를 자동으로 확인합니다. 하지만 VPC 외부에서는 Route 53 Resolver를 사용할 수 없습니다. 온프레미스 네트워크에서 VPC 엔드포인트에 액세스하려는 경우 기본 DNS 이름을 사용하거나 Route 53 Resolver 엔드포인트 및 Resolver 규칙을 사용할 수 있습니다. 자세한 내용은 AWS PrivateLink 및 AWS Transit Gateway 와 통합을 참조하세요 Amazon Route 53 Resolver.

서브넷 및 가용 영역

가용 영역당 1개의 서브넷으로 VPC 엔드포인트를 구성할 수 있습니다. 선택한 서브넷에 대해 VPC 엔드포인트용 탄력적 네트워크 인터페이스가 생성됩니다. VPC 엔드포인트의 IP 주소 유형이 IPv4인 경우, 각 탄력적 네트워크 인터페이스에는 /28 단위로 IP 주소가 서브넷에서 할당됩니다. 각 서브넷에 할당되는 IP 주소 수는 리소스 구성 수에 따라 달라지며, 필요 시 /28 블록 단위로 추가 IP를 할당합니다. 프로덕션 환경에서는 고가용성과 복원력을 위해 각 VPC 엔드포인트에 대해 최소 2개의 가용 영역을 구성하고 연속 IP 주소가 사용 가능하도록 설정하는 것이 좋습니다.

IP 주소 유형

서비스-네트워크 엔드포인트는 IPv4, IPv6 또는 듀얼 스택 주소를 지원할 수 있습니다. IPv6를 지원하는 엔드포인트는 AAAA 레코드를 사용하여 DNS 쿼리에 응답할 수 있습니다. 서비스-네트워크 엔드포인트의 IP 주소 유형은 여기에 설명된 대로 리소스 엔드포인트의 서브넷과 호환되어야 합니다.

- IPv4 - 엔드포인트 네트워크 인터페이스에 IPv4 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 주소 범위가 있는 경우에만 지원됩니다.
- IPv6 - 엔드포인트 네트워크 인터페이스에 IPv6 주소를 할당합니다. 이 옵션은 선택한 모든 서브넷이 IPv6 전용 서브넷인 경우에만 지원됩니다.
- 듀얼 스택 - 엔드포인트 네트워크 인터페이스에 IPv4 및 IPv6 주소를 모두 할당합니다. 이 옵션은 선택한 모든 서브넷에 IPv4 및 IPv6 주소 범위가 모두 있는 경우에만 지원됩니다.

서비스-네트워크 VPC 엔드포인트가 IPv4를 지원하면 엔드포인트 네트워크 인터페이스에는 IPv4 주소가 할당됩니다. 서비스-네트워크 VPC 엔드포인트가 IPv6를 지원하면 엔드포인트 네트워크 인터페이스에는 IPv6 주소가 할당됩니다. 엔드포인트 네트워크 인터페이스의 IPv6 주소는 인터넷을 통해 연결할 수 없습니다. 엔드포인트 네트워크 인터페이스를 IPv6 주소를 사용하여 설명하는 경우 `denyAllIgwTraffic`이 활성화됩니다.

서비스-네트워크 엔드포인트를 통해 서비스 네트워크 액세스

서비스-네트워크 엔드포인트를 사용하면 서비스 네트워크에 액세스할 수 있습니다. 서비스-네트워크 엔드포인트는 서비스 네트워크 내의 리소스 구성과 서비스에 대한 프라이빗 액세스를 제공합니다.

사전 조건

서비스-네트워크 엔드포인트를 생성하려면 다음 사전 조건을 충족해야 합니다.

- 자신이 생성했거나 다른 계정에서 AWS RAM을 통해 공유받은 서비스 네트워크가 있어야 합니다.
- 다른 계정에서 서비스 네트워크를 공유받은 경우, 해당 서비스 네트워크를 포함하는 리소스 공유를 검토하고 수락해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 초대 수락 및 거부를 참조하세요.
- 서비스-네트워크 엔드포인트는 처음 생성 시, 가용 영역 내에서 연속된 /28 IPv4 블록이 필요합니다. 엔드포인트와 연결된 리소스 구성을 서비스 네트워크에 추가하면, 각 리소스가 가용 영역별로 고유 IP를 사용하므로 동일 서브넷에서 추가 /28 블록이 필요합니다.

  서비스 네트워크에 16개 이상의 리소스 구성을 추가할 계획이라면, 새로운 리소스를 수용하기 위해 서비스-네트워크 엔드포인트에서 추가 /28 블록이 사용됩니다. VPC CIDR IP를 사용하지 않으려면 서비스 네트워크 VPC 연결을 사용하는 것이 좋습니다. 자세한 내용은 Amazon VPC Lattice 사용 설명서의 VPC 엔드포인트 연결 관리를 참조하세요.

서비스 네트워크 엔드포인트 생성

공유받은 서비스 네트워크에 액세스하기 위해 서비스-네트워크 엔드포인트를 생성합니다. 서비스-네트워크 엔드포인트를 생성한 후에는 해당 보안 그룹 또는 태그만 수정할 수 있습니다.

서비스-네트워크 엔드포인트 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 PrivateLink and Lattice에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 엔드포인트를 쉽게 찾고 관리할 수 있도록 이름을 지정할 수 있습니다.
5. 유형에서 서비스 네트워크를 선택합니다.
6. 서비스 네트워크에서 서비스 네트워크를 선택합니다.
7. 네트워크 설정에서 서비스 네트워크에 액세스할 VPC를 선택합니다.
8. 프라이빗 DNS 지원을 구성하려면 추가 설정, 프라이빗 DNS 이름 활성화를 선택합니다. 이 기능을 사용하려면 VPC에서 DNS 호스트 이름 활성화와 DNS 지원 활성화 속성이 활성화되어 있어야 합니다.
9. 서브넷에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷을 선택합니다.

   프로덕션 환경에서는 고가용성과 복원력을 위해 각 VPC 엔드포인트에 대해 최소 2개의 가용 영역을 구성하는 것이 좋습니다.
10. 보안 그룹에서 보안 그룹을 선택합니다.

보안 그룹을 지정하지 않은 경우 VPC에 대한 기본 보안 그룹이 연결됩니다.

11. 엔드포인트 생성을 선택합니다.

명령줄을 사용하여 서비스-네트워크 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(Windows PowerShell용 도구)

서비스-네트워크 엔드포인트 관리

서비스-네트워크 엔드포인트를 생성한 후 해당 보안 그룹 또는 태그를 업데이트할 수 있습니다.

작업

- 엔드포인트 삭제
- 서비스-네트워크 엔드포인트 업데이트

엔드포인트 삭제

VPC 엔드포인트 사용을 마치면 엔드포인트를 삭제할 수 있습니다.

콘솔을 사용하여 엔드포인트 삭제하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 서비스-네트워크 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 표시되면 **delete**를 입력합니다.
6. 삭제를 선택합니다.

명령줄을 사용하여 엔드포인트 삭제하기

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(Windows PowerShell용 도구)

서비스-네트워크 엔드포인트 업데이트

VPC 엔드포인트를 업데이트할 수 있습니다.

콘솔을 사용하여 엔드포인트 업데이트하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 엔드포인트를 선택합니다.
4. 작업과 적절한 옵션을 선택합니다.
5. 콘솔 단계에 따라 업데이트를 제출합니다.

명령줄을 사용하여 엔드포인트 업데이트하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

에 대한 자격 증명 및 액세스 관리 AWS PrivateLink

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 AWS PrivateLink 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

내용

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 수행하는 작업에 따라 다릅니다 AWS PrivateLink.

서비스 사용자 - AWS PrivateLink 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 AWS PrivateLink 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다.

서비스 관리자 - 회사에서 AWS PrivateLink 리소스를 책임지고 있는 경우에 대한 전체 액세스 권한을 가지고 있을 것입니다 AWS PrivateLink. 서비스 관리자는 서비스 사용자가 액세스해야 하는 AWS PrivateLink 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요.

IAM 관리자 - IAM 관리자라면 AWS PrivateLink에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한

정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS PrivateLink 에서 IAM을 사용하는 방법

IAM을 사용하여 액세스를 관리하기 전에 사용할 수 있는 IAM 기능에 대해 AWS PrivateLink알아봅니다 AWS PrivateLink.

IAM 특성	AWS PrivateLink 지원
자격 증명 기반 정책	예
리소스 기반 정책	예

IAM 특성	AWS PrivateLink 지원
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

AWS PrivateLink 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

에 대한 자격 증명 기반 정책 AWS PrivateLink

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

에 대한 자격 증명 기반 정책 예제 AWS PrivateLink

자격 AWS PrivateLink 증명 기반 정책의 예를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS PrivateLink.

내의 리소스 기반 정책 AWS PrivateLink

리소스 기반 정책 지원: 예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

AWS PrivateLink 서비스는 엔드포인트 정책이라고 하는 한 가지 유형의 리소스 기반 정책을 지원합니다. 엔드포인트 정책을 통해 엔드포인트를 사용하여 엔드포인트 서비스에 액세스할 수 있는 AWS 보안 주체가 제어됩니다. 자세한 내용은 the section called “엔드포인트 정책” 단원을 참조하십시오.

에 대한 정책 작업 AWS PrivateLink

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

ec2 네임스페이스의 작업

에 대한 일부 작업은 Amazon EC2 API의 일부 AWS PrivateLink 입니다. 이러한 정책 작업은 `ec2` 접두사를 사용합니다. 자세한 내용은 Amazon EC2 API 참조의 AWS PrivateLink 작업을 참조하세요.

vpce 네임스페이스의 작업

AWS PrivateLink 는 `AllowMultiRegion` 권한 전용 작업도 제공합니다. 이 정책 작업은 `vpce` 접두사를 사용합니다.

에 대한 정책 리소스 AWS PrivateLink

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

에 대한 정책 조건 키 AWS PrivateLink

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

다음 조건 키는에 고유합니다 AWS PrivateLink.

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

자세한 내용은 Amazon EC2의 조건 키를 참조하세요.

ACLs AWS PrivateLink

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

를 사용한 ABAC AWS PrivateLink

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

에서 임시 자격 증명 사용 AWS PrivateLink

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는AWS 서비스 섹션을 참조하세요.

에 대한 교차 서비스 보안 주체 권한 AWS PrivateLink

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

에 대한 서비스 역할 AWS PrivateLink

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

에 대한 서비스 연결 역할 AWS PrivateLink

서비스 연결 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

에 대한 자격 증명 기반 정책 예제 AWS PrivateLink

기본적으로 사용자 및 역할에는 AWS PrivateLink 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS PrivateLink에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Amazon EC2에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

예제

- VPC 엔드포인트 사용 제어
- 서비스 소유자를 기반으로 VPC 엔드포인트 생성 제어
- VPC 엔드포인트 서비스에 대해 지정할 수 있는 프라이빗 DNS 이름 제어
- VPC 엔드포인트 서비스에 대해 지정할 수 있는 서비스 이름 제어

VPC 엔드포인트 사용 제어

기본적으로 사용자에게는 엔드포인트 사용 권한이 없습니다. ID 기반 정책을 생성하여 사용자에게 엔드포인트를 생성, 수정, 설명, 삭제할 수 있는 권한을 부여할 수 있습니다. 다음은 예입니다.

JSON

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

```
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

VPC 엔드포인트를 사용하는 서비스에 대한 액세스 제어에 대한 자세한 내용은 the section called “엔드포인트 정책” 섹션을 참조하세요.

서비스 소유자를 기반으로 VPC 엔드포인트 생성 제어

`ec2:VpceServiceOwner` 조건 키를 사용하여 서비스를 소유한 사람(`amazon`, `aws-marketplace` 또는 계정 ID) 기준으로 생성 가능한 VPC 엔드포인트를 제어할 수 있습니다. 다음 예제에서는 지정된 서비스 소유자에게 VPC 엔드포인트를 생성할 수 있는 권한을 부여합니다. 이 예제를 사용하려면 리전, 계정 ID 및 서비스 소유자를 대체해야 합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

VPC 엔드포인트 서비스에 대해 지정할 수 있는 프라이빗 DNS 이름 제어

VPC 엔드포인트 서비스와 연결된 프라이빗 DNS 이름을 기준으로 수정 또는 생성 가능한 VPC 엔드포인트 서비스를 `ec2:VpceServicePrivateDnsName` 조건 키를 사용하여 제어할 수 있습니다. 다음 예제에서는 지정된 프라이빗 DNS 이름에 VPC 엔드포인트 서비스를 생성할 수 있는 권한을 부여합니다. 이 예제를 사용하려면 리전, 계정 ID 및 프라이빗 DNS 이름을 대체해야 합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

VPC 엔드포인트 서비스에 대해 지정할 수 있는 서비스 이름 제어

VPC 엔드포인트 서비스 이름을 기준으로 생성 가능한 VPC 엔드포인트를 `ec2:VpceServiceName` 조건 키를 사용하여 제어할 수 있습니다. 다음 예제에서는 지정된 서비스 이름에 VPC 엔드포인트를 생성할 수 있는 권한을 부여합니다. 이 예제를 사용하려면 리전, 계정 ID 및 서비스 이름을 대체해야 합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
    ]
}
```

엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어

엔드포인트 정책은 엔드포인트를 사용하여에 액세스할 수 있는 AWS 보안 주체를 제어하기 위해 VPC 엔드포인트에 연결하는 리소스 기반 정책입니다 AWS 서비스.

엔드포인트 정책은 ID 기반 정책이나 리소스 기반 정책을 재정의하거나 대체하지 않습니다. 예를 들어 인터페이스 엔드포인트를 사용하여 Amazon S3에 연결하는 경우, Amazon S3 버킷 정책을 사용하여 특정 엔드포인트나 특정 VPC의 버킷에 대한 액세스를 제어할 수도 있습니다.

내용

고려 사항

- 엔드포인트 정책은 IAM 정책 언어를 사용하는 JSON 정책 문서입니다. 위탁자 요소가 포함되어 있어야 합니다. 엔드포인트 정책의 크기는 공백을 포함하여 20,480자를 초과할 수 없습니다.
- 에 대한 인터페이스 또는 게이트웨이 엔드포인트를 생성할 때 엔드포인트에 단일 엔드포인트 정책을 연결할 AWS 서비스수 있습니다. 언제든지 엔드포인트 정책을 업데이트할 수 있습니다. 엔드포인트 정책을 연결하지 않으면 기본 엔드포인트 정책이 연결됩니다.
- 모든가 엔드포인트 정책을 AWS 서비스 지원하는 것은 아닙니다. 가 엔드포인트 정책을 지원하지 AWS 서비스 않는 경우 서비스의 모든 엔드포인트에 대한 전체 액세스를 허용합니다. 자세한 내용은 the section called “엔드포인트 정책 지원 보기” 단원을 참조하십시오.
- AWS 서비스 이외의 엔드포인트 서비스를 위한 VPC 엔드포인트를 생성하면 엔드포인트에 대한 전체 액세스 권한이 허용됩니다.
- 와일드카드 문자(* 또는 ?) 또는 숫자 조건 연산자는 시스템 생성 식별자(예: `aws:PrincipalAccount` 또는 `aws:SourceVpc`)를 참조하는 전역 컨텍스트 키와 함께 사용할 수 없습니다.
- 문자열 조건 연산자를 사용할 때는 각 와일드카드 문자 앞뒤에 최소 6개의 연속 문자를 사용해야 합니다.
- 리소스 또는 조건 요소에 ARN을 지정할 때는 ARN의 계정 부분에 계정 ID 또는 와일드카드 문자를 포함할 수 있지만 둘 다 포함할 수는 없습니다.

- 엔드포인트 정책을 업데이트할 경우 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다.

기본 엔드포인트 정책

기본 엔드포인트 정책을 통해 엔드포인트에 대한 전체 액세스 권한이 부여됩니다.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

인터페이스 엔드포인트 정책

에 대한 엔드포인트 정책의 예는 섹션을 AWS 서비스참조하세요the section called “통합되는 서비스”. 표의 첫 번째 열에는 각에 대한 AWS PrivateLink 설명서 링크가 포함되어 있습니다 AWS 서비스. 가 엔드포인트 정책을 AWS 서비스 지원하는 경우 해당 설명서에는 예제 엔드포인트 정책이 포함되어 있습니다.

게이트웨이 엔드포인트의 보안 주체

게이트웨이 엔드포인트에서 `Principal` 요소는 `*`로 설정해야 합니다. 보안 주체를 지정하려면 `aws:PrincipalArn` 조건 키를 사용합니다.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

다음 형식으로 위탁자를 지정하면 계정의 모든 사용자 및 역할이 아닌 AWS 계정 루트 사용자 에게만 액세스 권한이 부여됩니다.

```
"AWS": "account_id"
```

게이트웨이 엔드포인트에 대한 엔드포인트 정책의 예는 다음을 참조하세요.

- Amazon S3에 대한 엔드포인트
- DynamoDB에 대한 엔드포인트

VPC 엔드포인트 정책 업데이트

다음 절차에 따라 AWS 서비스에 대한 엔드포인트 정책을 업데이트합니다. 엔드포인트 정책을 업데이트할 경우 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다.

콘솔을 사용하여 엔드포인트 정책 업데이트하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. VPC 엔드포인트를 선택합니다.
4. 작업(Actions), 정책 관리(Manage policy)를 선택합니다.
5. 모든 액세스(Full Access)를 선택하여 서비스에 대한 전체 액세스를 허용하거나 사용자 지정(Custom)을 선택하고 사용자 지정 정책을 연결합니다.
6. 저장을 선택합니다.

명령줄 사용하여 엔드포인트 정책 업데이트하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(Windows PowerShell용 도구)

AWS 에 대한 관리형 정책 AWS PrivateLink

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향

을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AWS PrivateLink AWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS PrivateLink 이후부터의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS PrivateLink 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AWS PrivateLink 에서 변경 내용 추적 시작	AWS PrivateLink 가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2021년 3월 1일

에 대한 CloudWatch 지표 AWS PrivateLink

AWS PrivateLink 는 인터페이스 엔드포인트, Gateway Load Balancer 엔드포인트 및 엔드포인트 서비스에 대한 데이터 포인트를 Amazon CloudWatch에 게시합니다. CloudWatch를 사용하면 이러한 데이터 요소에 대한 통계를 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 통계를 지표라고 합니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 각 데이터 포인트에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

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

지표는 모든 인터페이스 엔드포인트, Gateway Load Balancer 엔드포인트 및 엔드포인트 서비스에 대해 게시됩니다. 그러나 게이트웨이 엔드포인트나 교차 리전 액세스를 사용하는 엔드포인트 서비스 소비자에게는 게시되지 않습니다. 기본적으로는 추가 비용 없이 1분 간격으로 CloudWatch에 지표를 AWS PrivateLink 전송합니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

내용

엔드포인트 지표 및 차원

`AWS/PrivateLinkEndpoints` 네임스페이스에는 인터페이스 엔드포인트와 Gateway Load Balancer 엔드포인트에 대한 다음과 같은 지표가 포함됩니다.

지표	설명
`ActiveConnections`	동시 활성 연결 수입니다. 여기에는 SYN_SENT 및 ESTABLISHED 상태의 연결이 포함됩니다. 보고 기준: 엔드포인트가 1분 기간 동안 트래픽을 수신했습니다.

지표	설명
	통계: 가장 유용한 통계는 Average, Maximum 및 Minimum입니다. 측정 기준 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
BytesProcessed	엔드포인트와 엔드포인트 서비스 간에 교환된 바이트 수로, 양방향으로 집계됩니다. 이것은 엔드포인트 소유자에게 청구되는 바이트 수입니다. 청구서에는 GB 단위로 이 값이 표시됩니다. 보고 기준: 엔드포인트가 1분 기간 동안 트래픽을 수신했습니다. 통계: 가장 유용한 통계는 Average, Sum, Maximum 및 Minimum입니다. 측정 기준 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
NewConnections	엔드포인트를 통해 설정된 새 연결의 수입니다. 보고 기준: 엔드포인트가 1분 기간 동안 트래픽을 수신했습니다. 통계: 가장 유용한 통계는 Average, Sum, Maximum 및 Minimum입니다. 측정 기준 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

지표	설명
PacketsDropped	엔드포인트에서 삭제한 패킷의 수입니다. 이 지표는 모든 패킷 드롭을 캡처하지 못할 수 있습니다. 증가한 값은 엔드포인트 또는 엔드포인트 서비스가 비정상임을 나타낼 수 있습니다. 보고 기준: 엔드포인트가 1분 기간 동안 트래픽을 수신했습니다. 통계: 가장 유용한 통계는 Average, Sum 및 Maximum입니다. 측정 기준 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
RstPacketsReceived	엔드포인트에서 수신된 RST 패킷의 수입니다. 증가한 값은 엔드포인트 서비스가 비정상임을 나타낼 수 있습니다. 보고 기준: 엔드포인트가 1분 기간 동안 트래픽을 수신했습니다. 통계: 가장 유용한 통계는 Average, Sum 및 Maximum입니다. 측정 기준 • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

이러한 지표를 필터링하려면 다음 차원을 사용하세요.

차원	설명
Endpoint Type	엔드포인트 유형(Interface | GatewayLoadBalancer)을 기준으로 지표 데이터를 필터링합니다.
Service Name	서비스 이름을 기준으로 지표 데이터를 필터링합니다.
Subnet Id	서브넷을 기준으로 지표 데이터를 필터링합니다.

차원	설명
VPC Endpoint Id	VPC 엔드포인트를 기준으로 지표 데이터를 필터링합니다.
VPC Id	VPC를 기준으로 지표 데이터를 필터링합니다.

엔드포인트 서비스 지표 및 차원

AWS/PrivateLinkServices 네임스페이스에는 엔드포인트 서비스의 다음 지표가 포함됩니다.

지표	설명
ActiveConnections	클라이언트에서 엔드포인트를 통과하여 대상에 이르는 활성 연결의 최대 수입니다. 증가한 값은 로드 밸런서에 대상을 추가해야 함을 나타낼 수 있습니다. 보고 기준: 엔드포인트 서비스에 연결된 엔드포인트가 1분 기간 동안 트래픽을 전송했습니다. 통계: 가장 유용한 통계는 Average 및 Maximum입니다. 측정 기준 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
BytesProcessed	엔드포인트 서비스와 엔드포인트 간에 양방향으로 교환된 바이트의 수입니다. 보고 기준: 엔드포인트 서비스에 연결된 엔드포인트가 1분 기간 동안 트래픽을 전송했습니다. 통계: 가장 유용한 통계는 Average, Sum 및 Maximum입니다.

지표	설명
	측정 기준 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
EndpointsCount	엔드포인트 서비스에 연결된 엔드포인트의 수입니다. 보고 기준: 5분 기간 동안 0이 아닌 값이 있습니다. 통계: 가장 유용한 통계는 Average 및 Maximum입니다. 측정 기준 • Service Id
NewConnections	클라이언트에서 엔드포인트를 통과하여 대상에 이르는 새 연결의 수입니다. 증가한 값은 로드 밸런서에 대상을 추가해야 함을 나타낼 수 있습니다. 보고 기준: 엔드포인트 서비스에 연결된 엔드포인트가 1분 기간 동안 트래픽을 전송했습니다. 통계: 가장 유용한 통계는 Average, Sum 및 Maximum입니다. 측정 기준 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

지표	설명
RstPacketsSent	엔드포인트 서비스가 엔드포인트로 전송한 RST 패킷의 수입니다. 증가한 값은 비정상적인 대상이 있음을 나타낼 수 있습니다. 보고 기준: 엔드포인트 서비스에 연결된 엔드포인트가 1분 기간 동안 트래픽을 전송했습니다. 통계: 가장 유용한 통계는 Average, Sum 및 Maximum입니다. 측정 기준 • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

이러한 지표를 필터링하려면 다음 차원을 사용하세요.

차원	설명
Az	가용 영역을 기준으로 지표 데이터를 필터링합니다.
Load Balancer Arn	로드 밸런서를 기준으로 지표 데이터를 필터링합니다.
Service Id	엔드포인트 서비스를 기준으로 지표 데이터를 필터링합니다.
VPC Endpoint Id	VPC 엔드포인트를 기준으로 지표 데이터를 필터링합니다.

CloudWatch 지표 보기

다음과 AWS CLI 같이 Amazon VPC 콘솔, CloudWatch 콘솔 또는를 사용하여 이러한 CloudWatch 지표를 볼 수 있습니다.

Amazon VPC 콘솔을 사용하여 지표 보기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다. 엔드포인트를 선택한 다음 모니터링(Monitoring) 탭을 선택합니다.
3. 탐색 창에서 엔드포인트 서비스를 선택합니다. 엔드포인트 서비스를 선택한 다음 모니터링(Monitoring) 탭을 선택합니다.

CloudWatch 콘솔을 사용하여 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표를 선택합니다.
3. AWS/PrivateLinkEndpoints 네임스페이스를 선택합니다.
4. AWS/PrivateLinkServices 네임스페이스를 선택합니다.

를 사용하여 지표를 보려면 AWS CLI

다음 list-metrics 명령을 사용하여 인터페이스 엔드포인트 및 Gateway Load Balancer 엔드포인트에 대해 사용 가능한 지표를 나열합니다.

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

다음 list-metrics 명령을 사용하여 엔드포인트 서비스에 대해 사용 가능한 지표를 나열합니다.

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

기본 제공되는 Contributor Insights 규칙 사용

AWS PrivateLink 는 지원되는 각 지표에 가장 큰 기여자인 엔드포인트를 찾는 데 도움이 되는 엔드포인트 서비스에 대한 기본 제공 Contributor Insights 규칙을 제공합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Contributor Insights 섹션을 참조하세요.

AWS PrivateLink 는 다음 규칙을 제공합니다.

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` - 활성 연결 수를 기준으로 엔드포인트의 순위를 매깁니다.

- `VpcEndpointService-BytesByEndpointId-v1` - 처리된 바이트의 수를 기준으로 엔드포인트의 순위를 매깁니다.
- `VpcEndpointService-NewConnectionsByEndpointId-v1` - 새 연결 수를 기준으로 엔드포인트의 순위를 매깁니다.
- `VpcEndpointService-RstPacketsByEndpointId-v1` - 엔드포인트로 전송된 RST 패킷의 수를 기준으로 엔드포인트의 순위를 매깁니다.

기본 제공 규칙을 사용하려면 먼저 규칙을 활성화해야 합니다. 규칙을 활성화하면 기여자 데이터 수집이 시작됩니다. Contributor Insights 요금에 대한 자세한 내용은 Amazon CloudWatch 요금 섹션을 참조하세요.

Contributor Insights를 사용하려면 다음의 권한이 있어야 합니다.

- `cloudwatch:DeleteInsightRules` – Contributor Insights 규칙을 삭제합니다.
- `cloudwatch:DisableInsightRules` – Contributor Insights 규칙을 비활성화합니다.
- `cloudwatch:GetInsightRuleReport` – 데이터를 가져옵니다.
- `cloudwatch:ListManagedInsightRules` – 사용 가능한 Contributor Insights 규칙을 나열합니다.
- `cloudwatch:PutManagedInsightRules` – Contributor Insights 규칙을 활성화합니다.

작업

- Contributor Insights 규칙 활성화
- Contributor Insights 규칙 비활성화
- Contributor Insights 규칙 삭제

Contributor Insights 규칙 활성화

다음 절차에 따라 AWS Management Console 또는를 AWS PrivateLink 사용하기 위한 기본 제공 규칙을 활성화합니다 AWS CLI.

콘솔을 AWS PrivateLink 사용하여에 대한 Contributor Insights 규칙을 활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.

4. Contributor Insights 탭에서 활성화(Enable)를 선택합니다.
5. (선택 사항) 기본적으로 모든 규칙이 활성화됩니다. 특정 규칙만 활성화하려면 활성화하지 않을 규칙을 선택한 다음 작업(Actions), 규칙 비활성화(Disable rule)를 선택합니다. 확인 메시지가 나타나면 비활성화를 선택합니다.

를 AWS PrivateLink 사용하여에 대한 Contributor Insights 규칙을 활성화하려면 AWS CLI

1. 다음과 같이 list-managed-insight-rules 명령을 사용하여 사용 가능한 규칙을 열거합니다. `--resource-arn` 옵션에서 엔드포인트 서비스의 ARN을 지정합니다.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. `list-managed-insight-rules` 명령 출력에서 `TemplateName` 필드의 템플릿 이름을 복사합니다. 다음은 이 필드의 예입니다.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. 다음과 같이 put-managed-insight-rules 명령을 사용하여 규칙을 활성화합니다. 엔드포인트 서비스의 템플릿 이름과 ARN을 지정해야 합니다.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Contributor Insights 규칙 비활성화

AWS PrivateLink 언제든지에 대한 기본 제공 규칙을 비활성화할 수 있습니다. 규칙을 비활성화하면 기여자 데이터 수집이 중지되지만 기존 기여자 데이터는 15일이 경과할 때까지 보관됩니다. 규칙을 비활성화한 후, 다시 활성화하여 기여자 데이터 수집을 다시 시작할 수 있습니다.

AWS PrivateLink 콘솔 사용에 대한 Contributor Insights 규칙을 비활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.

4. Contributor Insights 탭에서 모두 비활성화(Disable all)를 선택해 모든 규칙을 비활성화합니다. 또는 규칙(Rules) 패널을 확장해 비활성화하려는 규칙을 선택한 후 작업(Actions), 규칙 비활성화(Disable rule)를 선택합니다
5. 확인 메시지가 나타나면 비활성화를 선택합니다.

를 AWS PrivateLink 사용하여에 대한 Contributor Insights 규칙을 비활성화하려면 AWS CLI

disable-insight-rules 명령을 사용해 규칙을 비활성화합니다.

Contributor Insights 규칙 삭제

다음 절차에 따라 AWS Management Console 또는 AWS PrivateLink 사용에 대한 기본 제공 규칙을 삭제합니다 AWS CLI. 규칙을 삭제하면 기여자 데이터 수집이 중단되고 기존 기여자 데이터가 삭제됩니다.

콘솔을 AWS PrivateLink 사용하여에 대한 Contributor Insights 규칙을 삭제하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 인사이트(Insights)를 선택한 다음, Contributor Insights를 선택합니다.
3. 규칙(Rules) 패널을 확장하고 규칙을 선택합니다.
4. 작업(Actions), 규칙 삭제(Delete rule)를 선택합니다.
5. 확인 메시지가 나타나면 삭제를 선택합니다.

를 AWS PrivateLink 사용하여에 대한 Contributor Insights 규칙을 삭제하려면 AWS CLI

delete-insight-rules 명령을 사용하여 규칙을 삭제합니다.

AWS PrivateLink 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다. 리소스별로 적용되는 할당량 증가를 요청하는 경우 리전에 있는 모든 리소스의 할당량이 증가합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

요청 스로틀링

AWS PrivateLink에 대한 API 작업은 Amazon EC2 API의 일부입니다. Amazon EC2는 AWS 계정 수준에서 API 요청을 제한합니다. 자세한 내용은 Amazon EC2 개발자 가이드의 요청 스로틀링을 참조하세요. 또한 API 요청은 AWS PrivateLink의 성능을 돕기 위해 조직 수준에서도 제한됩니다. AWS Organizations를 사용 중인데 계정 수준 API 한도 내에 있음에도 `RequestLimitExceeded` 오류 코드가 표시되는 경우, 많은 수의 API 호출을 수행하는 조직의 AWS 계정을 식별하는 방법 문서를 참조하세요. 도움이 필요하면 계정 팀에 문의하거나 VPC 서비스와 VPC 엔드포인트 범주로 기술 지원 사례를 개설하세요. `RequestLimitExceeded` 오류 코드의 이미지를 첨부해야 합니다.

VPC 엔드포인트 할당량

AWS 계정에는 엔드포인트와 관련된 다음과 같은 할당량이 있습니다.

명칭	기본값	조정 가능	설명
VPC당 인터페이스 및 Gateway Load Balancer 엔드포인트	50	예	인터페이스 엔드포인트 및 Gateway Load Balancer 엔드포인트에 대한 결합된 할당량입니다.
리전당 게이트웨이 VPC 엔드포인트	20	예	VPC당 게이트웨이 엔드포인트를 255개까지 생성할 수 있습니다.
VPC당 리소스 VPC 엔드포인트	200	예	
VPC당 서비스 네트워크 VPC 엔드포인트	50	예	

명칭	기본값	조정 가능	설명
VPC 엔드포인트 정책당 문자 수	20,480	아니요	VPC 엔드포인트 정책의 최대 크기는 공백을 포함합니다

다음 고려 사항은 VPC 엔드포인트를 통과하는 트래픽에 적용됩니다.

- 기본적으로 각 VPC 엔드포인트는 가용 영역당 최대 10Gbps의 대역폭을 지원하고 최대 100Gbps까지 자동으로 조정됩니다. 모든 가용 영역에 부하를 분산할 때 VPC 엔드포인트의 최대 대역폭은 가용 영역 수에 100Gbps를 곱한 값입니다. 애플리케이션에 더 높은 처리량이 필요한 경우 AWS Support에 문의하세요.
- 네트워크 연결의 최대 전송 단위(MTU)는 VPC 엔드포인트를 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. MTU가 클수록 하나의 패킷으로 전달할 수 있는 데이터의 양이 늘어납니다. VPC 엔드포인트는 8500바이트의 MTU를 지원합니다. VPC 엔드포인트에 도착하는 크기가 8500바이트보다 큰 패킷은 삭제됩니다.
- 경로 MTU 검색(PMTUD)은 지원되지 않습니다. VPC 엔드포인트는 `Destination Unreachable: Fragmentation needed and Don't Fragment was Set`(유형 3, 코드 4)과 같은 ICMP 메시지를 생성하지 않습니다.
- VPC 엔드포인트는 모든 패킷에 대해 최대 세그먼트 크기(MSS) 클램핑을 적용합니다. 자세한 내용은 RFC879를 참조하세요.

AWS PrivateLink에 대한 문서 기록

다음 표에서는 AWS PrivateLink의 릴리스를 설명합니다.

변경 사항	설명	날짜
리소스 및 서비스 네트워크 액세스	AWS PrivateLink는 VPC 및 계정 경계를 넘어 리소스와 서비스 네트워크에 액세스하는 기능을 지원합니다.	2024년 12월 1일
교차 리전 액세스	서비스 공급자는 하나의 리전에서 서비스를 호스팅하고, 여러 AWS 리전에서 해당 서비스를 제공할 수 있습니다. 서비스 소비자는 엔드포인트를 생성할 때 서비스 리전을 선택합니다.	2024년 11월 26일
지정된 IP 주소	VPC 엔드포인트를 생성하거나 수정할 때 엔드포인트 네트워크 인터페이스에 대한 IP 주소를 지정할 수 있습니다.	2023년 8월 17일
IPv6 지원	IPv4 및 IPv6 주소를 모두 지원하거나 IPv6 주소만 지원하도록 Gateway Load Balancer 엔드포인트 서비스와 Gateway Load Balancer 엔드포인트를 구성할 수 있습니다.	2022년 12월 12일
Contributor Insights	기본 제공 Contributor Insights 규칙을 사용하여 AWS PrivateLink의 CloudWatch 지표에 가장 많이 기여하는 특정 엔드포인트를 식별할 수 있습니다.	2022년 8월 18일

IPv6 지원	서비스 공급자는 백엔드 서비스에서 IPv4만 지원하는 경우에도 엔드포인트 서비스에서 IPv6 요청을 수락하도록 설정할 수 있습니다. 엔드포인트 서비스에서 IPv6 요청을 수락하면 서비스 소비자는 IPv6를 통해 엔드포인트 서비스에 액세스할 수 있도록 인터페이스 엔드포인트의 IPv6 지원을 활성화할 수 있습니다.	2022년 5월 11일
CloudWatch 지표	AWS PrivateLink는 인터페이스 엔드포인트, Gateway Load Balancer 엔드포인트 및 엔드포인트 서비스에 대한 CloudWatch 지표를 게시합니다.	2022년 1월 27일
Gateway Load Balancer 엔드포인트	VPC에 Gateway Load Balancer 엔드포인트를 생성하여 Gateway Load Balancer를 사용하여 구성한 VPC 엔드포인트 서비스로 트래픽을 라우팅할 수 있습니다.	2020년 11월 10일
VPC 엔드포인트 정책	AWS 서비스를 위한 VPC 엔드포인트에 IAM 정책을 연결하여 해당 서비스에 대한 액세스를 제어할 수 있습니다.	2020년 3월 23일
VPC 엔드포인트 및 엔드포인트 서비스에 대한 조건 키	EC2 조건 키를 사용하여 VPC 엔드포인트 및 엔드포인트 서비스에 대한 액세스를 제어할 수 있습니다.	2020년 3월 6일

VPC 엔드포인트 및 엔드포인트 서비스 생성 시 태깅	VPC 엔드포인트 또는 엔드포인트 서비스를 생성할 때 태그를 추가할 수 있습니다.	2020년 2월 5일
프라이빗 DNS 이름	프라이빗 DNS 이름을 사용하여 VPC 내에서 AWS PrivateLink 기반 서비스에 액세스할 수 있습니다.	2020년 1월 6일
VPC 엔드포인트 서비스	자체 엔드포인트 서비스를 생성하고 다른 AWS 계정 및 사용자가 인터페이스 VPC 엔드포인트를 통해 서비스에 연결하도록 할 수 있습니다. AWS Marketplace에서 엔드포인트 서비스에 대한 구독을 제공할 수 있습니다.	2017년 11월 28일
에 대한 인터페이스 VPC 엔드포인트AWS 서비스	인터페이스 엔드포인트를 생성하면 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고도 AWS PrivateLink와 통합된 AWS 서비스 서비스에 연결할 수 있습니다.	2017년 11월 8일
DynamoDB용 VPC 엔드포인트	게이트웨이 VPC 엔드포인트를 생성하여 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고 VPC에서 Amazon DynamoDB에 액세스할 수 있습니다.	2017년 8월 16일
Amazon S3에 대한 VPC 엔드포인트	게이트웨이 VPC 엔드포인트를 생성하여 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고 VPC에서 Amazon S3에 액세스할 수 있습니다.	2015년 5월 11일

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