AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

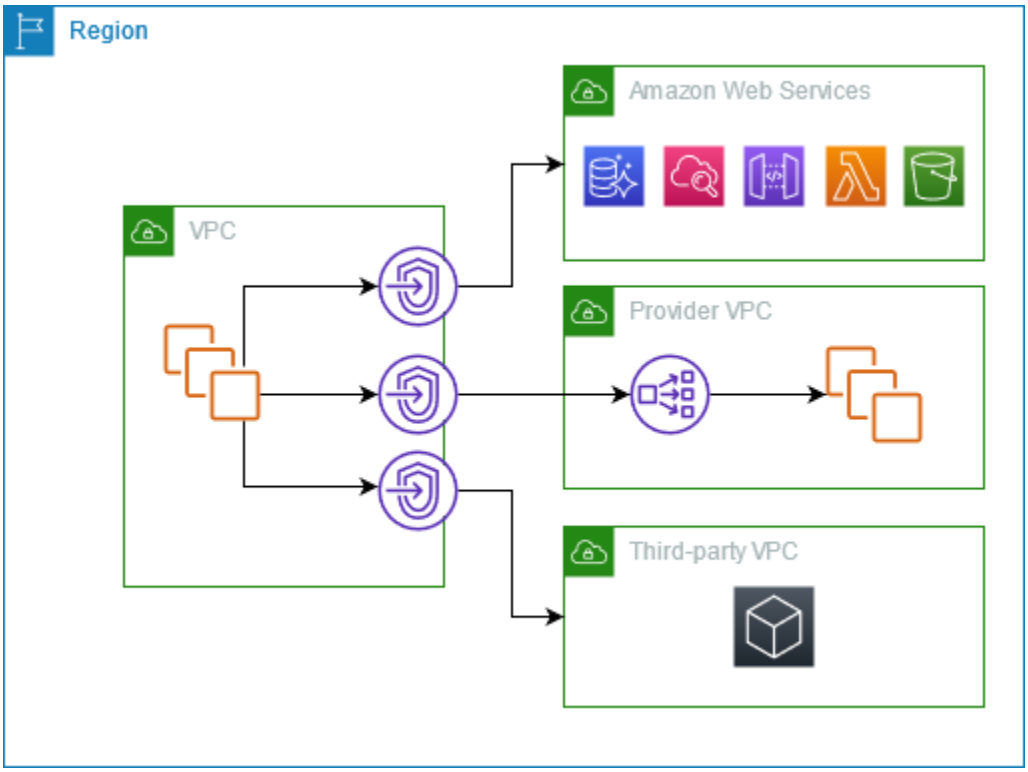
무엇입니까 AWS PrivateLink?

AWS PrivateLink VPC를 마치 VPC에 있는 것처럼 서비스에 비공개로 연결하는 데 사용할 수 있는 가용성과 확장성이 뛰어난 기술입니다. 인터넷 게이트웨이, NAT 디바이스, 퍼블릭 IP 주소, AWS Direct Connect 연결 또는 AWS Site-to-Site VPN 연결을 사용하지 않아도 프라이빗 서브넷에서 서비스와 통신할 수 있습니다. 따라서 VPC에서 연결할 수 있는 특정 API 엔드포인트, 사이트 및 서비스를 제어할 수 있습니다.

사용 사례

VPC 엔드포인트를 생성하여 VPC의 리소스를 통합되는 서비스에 연결할 수 있습니다. AWS PrivateLink자체 VPC 엔드포인트 서비스를 만들어 다른 AWS 고객이 사용할 수 있도록 할 수 있습니다. 자세한 정보는 the section called “개념”을 참조하세요.

다음 다이어그램에서 왼쪽의 VPC에는 프라이빗 서브넷에 여러 EC2 인스턴스와 3개의 인터페이스 VPC 엔드포인트가 있습니다. 최상위 VPC 엔드포인트는 에 연결됩니다. AWS 서비스중간 VPC 엔드포인트는 다른 VPC 엔드포인트에서 호스팅하는 서비스 AWS 계정 (VPC 엔드포인트 서비스) 에 연결됩니다. 하단 VPC 엔드포인트는 AWS Marketplace 파트너 서비스에 연결됩니다.



자세히 알아보기

- the section called “개념”
- 액세스 AWS 서비스
- 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 포함한 광범위한 세트에 대한 AWS 서비스명령을 제공합니다. AWS PrivateLink의 명령에 대한 AWS PrivateLink자세한 내용은 AWS CLI 명령 참조의 ec2를 참조하십시오.
- AWS CloudFormation - AWS 리소스를 설명하는 템플릿을 생성합니다. 템플릿을 사용하여 이러한 리소스를 하나의 단위로 프로비저닝하고 관리할 수 있습니다. 자세한 내용은 다음 AWS PrivateLink 리소스를 참조하십시오.
  - AWS::EC2::VPCEndpoint
  - AWS: :EC2: :VPC 알림 EndpointConnection
  - AWS::EC2::VPCEndpointService
  - AWS: :EC2: :VPC 권한 EndpointService
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDK — 언어별 API를 제공합니다. SDK는 서명 계산, 요청 재시도 처리 및 오류 처리와 같은 많은 연결 세부 정보를 관리합니다. 자세한 내용은 빌드할 도구를 참조하십시오. AWS
- 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.

요금

VPC 엔드포인트 요금에 대한 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

AWS PrivateLink 개념

Amazon VPC를 사용하면 논리적으로 분리된 가상 네트워크인 Virtual Private Cloud(VPC)를 정의할 수 있습니다. VPC에서 AWS 리소스를 시작할 수 있습니다. 그리고 VPC의 리소스에서 해당 VPC 외부의 리소스에 연결하도록 허용할 수 있습니다. 예를 들어 VPC에 인터넷 게이트웨이를 추가하여 인터넷 액세스를 허용하거나 VPN 연결을 추가하여 온프레미스 네트워크 액세스를 허용할 수 있습니다. 또는 VPC의 리소스가 VPC에서 직접 호스팅되는 것처럼 프라이빗 IP 주소를 사용하여 다른 VPC의 서비스에 연결할 수 있도록 하는 데 사용합니다 AWS PrivateLink .

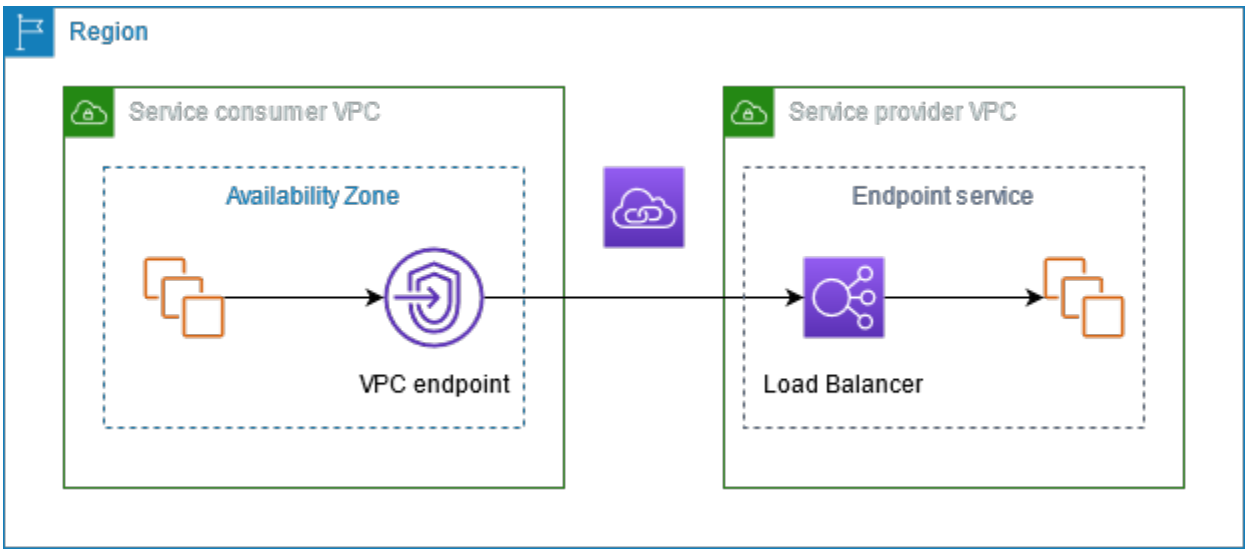
다음은 AWS PrivateLink사용을 시작하려면 알아야 하는 중요한 개념입니다.

내용

- 아키텍처 다이어그램
- 서비스 공급자
- 서비스 소비자
- AWS PrivateLink 연결
- 프라이빗 호스팅 영역

아키텍처 다이어그램

다음 다이어그램은 작동 방식에 대한 개괄적인 개요를 제공합니다. AWS PrivateLink 서비스 소비자는 인터페이스 VPC 엔드포인트를 생성하여 서비스 공급자가 호스팅하는 엔드포인트 서비스에 연결합니다.



서비스 공급자

서비스 소유자가 서비스 공급자입니다. 서비스 공급자에는 AWS, AWS 파트너 및 AWS 계정기타가 포함됩니다. 서비스 공급자는 EC2 인스턴스와 같은 AWS 리소스를 사용하거나 온프레미스 서버를 사용하여 서비스를 호스팅할 수 있습니다.

개념

- 엔드포인트 서비스
- 서비스 이름
- 서비스 상태

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 소비자가 서비스 이름을 쿼리할 수 있습니다. AWS 서비스서비스 공급자는 제공하는 서비스의 이름을 서비스 소비자와 공유해야 합니다.

서비스 상태

엔드포인트 서비스의 가능한 상태는 다음과 같습니다.

- `Pending` - 엔드포인트 서비스를 생성하는 중입니다.
- `Available` - 엔드포인트 서비스를 사용할 수 있습니다.
- `Failed` - 엔드포인트 서비스를 생성할 수 없습니다.
- `Deleting` - 서비스 공급자가 엔드포인트 서비스를 삭제했으며 삭제가 진행 중입니다.
- `Deleted` - 엔드포인트 서비스가 삭제되었습니다.

서비스 소비자

서비스 사용자를 서비스 소비자라고 합니다. 서비스 소비자는 EC2 인스턴스와 같은 AWS 리소스 또는 온프레미스 서버에서 엔드포인트 서비스에 액세스할 수 있습니다.

개념

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

VPC 엔드포인트

서비스 소비자는 VPC 엔드포인트를 생성하여 VPC를 엔드포인트 서비스에 연결합니다. 서비스 소비자는 VPC 엔드포인트를 생성할 때 엔드포인트 서비스의 서비스 이름을 지정해야 합니다. VPC 엔드포인트는 여러 유형이 있습니다. 엔드포인트 서비스에서 요구하는 유형의 VPC 엔드포인트를 생성합니다.

- `Interface` - TCP 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.

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

엔드포인트 네트워크 인터페이스

엔드포인트 네트워크 인터페이스는 엔드포인트 서비스로 전달되는 트래픽의 진입점 역할을 하는 요청자가 관리하는 네트워크 인터페이스입니다. 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 네트워크 인터페이스의 IP 주소는 VPC 엔드포인트의 수명 기간 동안 변경되지 않습니다.

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

VPC 엔드포인트를 생성할 때 엔드포인트 서비스는 연결 요청을 수신합니다. 서비스 공급자는 이 요청을 수락하거나 거부할 수 있습니다. 서비스 공급자가 요청을 수락하면 서비스 소비자는 VPC 엔드포인트를 `Available` 상태가 된 후 사용할 수 있습니다.

VPC 엔드포인트의 가능한 상태는 다음과 같습니다.

- `PendingAcceptance` - 연결 요청이 보류 중입니다. 요청을 수동으로 수락하는 경우의 초기 상태입니다.
- `Pending` - 서비스 공급자가 연결 요청을 수락했습니다. 요청이 자동으로 수락되는 경우의 초기 상태입니다. 서비스 소비자가 VPC 엔드포인트를 수정하면 VPC 엔드포인트가 이 상태로 돌아갑니다.
- `Available` - VPC 엔드포인트를 사용할 수 있습니다.

- `Rejected` - 서비스 공급자가 연결 요청을 거부했습니다. 서비스 공급자는 서비스를 사용할 수 있게 된 후 연결을 거부할 수도 있습니다.
- `Expired` - 연결 요청이 만료되었습니다.
- `Failed` - VPC 엔드포인트를 사용하도록 설정할 수 없습니다.
- `Deleting` - 서비스 소비자가 VPC 엔드포인트를 삭제했으며 삭제가 진행 중입니다.
- `Deleted` - VPC 엔드포인트가 삭제되었습니다.

AWS PrivateLink 연결

VPC의 트래픽은 VPC 엔드포인트와 엔드포인트 서비스 간 연결을 사용하여 엔드포인트 서비스로 전송됩니다. VPC 엔드포인트와 엔드포인트 서비스 간의 트래픽은 퍼블릭 인터넷을 통과하지 않고 AWS 네트워크 내에서 유지됩니다.

서비스 공급자는 서비스 소비자가 엔드포인트 서비스에 액세스할 수 있도록 권한을 추가합니다. 서비스 소비자가 연결을 시작하고 서비스 공급자는 연결 요청을 수락하거나 거부합니다.

인터페이스 VPC 엔드포인트를 통해 서비스 소비자는 엔드포인트 정책을 사용하여 엔드포인트 서비스에 액세스하기 위해 VPC 엔드포인트를 사용할 수 있는 IAM 보안 주체를 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.

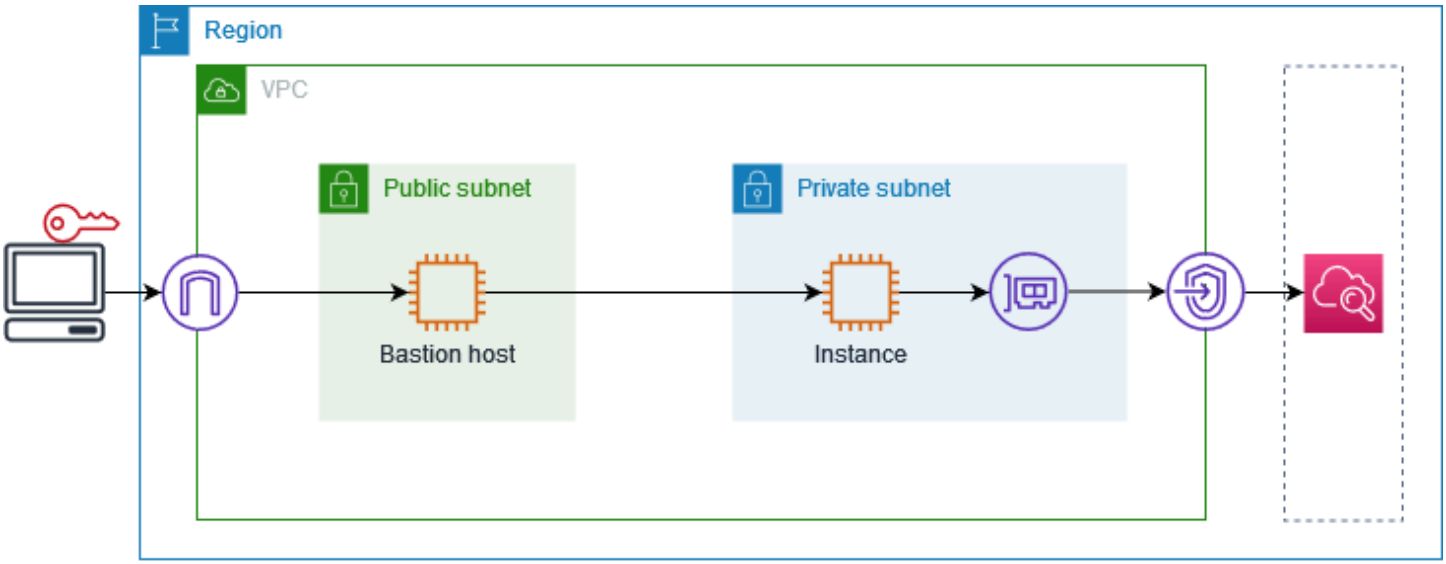
도메인 트래픽을 VPC 엔드포인트로 라우팅하도록 Amazon Route 53을 구성할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 VPC 엔드포인트로 트래픽 라우팅을 참조하세요.

Route 53을 사용하여 스플릿 호라이즌 DNS를 구성할 수 있습니다. 스플릿 호라이즌 DNS는 퍼블릭 웹 사이트와 기반 엔드포인트 서비스 모두에 동일한 도메인 이름을 사용합니다. AWS PrivateLink소비자 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.

다음으로 시작하세요 AWS PrivateLink

이 자습서에서는 를 사용하여 프라이빗 서브넷의 EC2 인스턴스에서 Amazon으로 요청을 보내는 방법을 보여줍니다. CloudWatch AWS PrivateLink

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. 에 대한 CloudWatch VPC 엔드포인트를 설정하면 대상 인스턴스의 트래픽이 엔드포인트 네트워크 인터페이스로 전송된 다음 VPC 엔드포인트를 사용하여 CloudWatch 전송됩니다. CloudWatch



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: 액세스 테스트 CloudWatch
- 4단계: 액세스할 VPC 엔드포인트 생성 CloudWatch
- 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 여세요.
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.

필수 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 프로필을 생성하고 액세스 정책을 연결합니다. CloudWatch ReadOnly

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: 액세스 테스트 CloudWatch

다음 절차를 사용하여 인스턴스가 액세스할 수 없는지 확인합니다 CloudWatch. 에 대한 CloudWatch 읽기 전용 AWS CLI 명령을 사용하여 그렇게 할 것입니다.

액세스를 CloudWatch 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 CloudWatch 인스턴스에서 액세스할 수 없음을 보여줍니다.

   ```
   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: 액세스할 VPC 엔드포인트 생성 CloudWatch

다음 절차를 사용하여 에 연결되는 VPC 엔드포인트를 생성합니다. CloudWatch

전제 조건

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

VPC 엔드포인트를 만들려면 CloudWatch

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 로 요청을 보내고 있는지 확인합니다. CloudWatch

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
```

응답이 오면 (결과가 비어 있더라도) 를 CloudWatch 사용하는 AWS PrivateLink것으로 연결됩니다.

`UnauthorizedOperation`오류가 발생하는 경우 인스턴스에 액세스를 CloudWatch 허용하는 IAM 역할이 있는지 확인하십시오.

요청 시간이 초과되면 다음을 확인합니다.

- 엔드포인트의 보안 그룹은 트래픽을 CloudWatch 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.

AWS 서비스 를 통한 액세스 AWS PrivateLink

엔드포인트를 AWS 서비스 사용하여 액세스합니다. 기본 서비스 엔드포인트는 퍼블릭 인터페이스 이므로 트래픽이 VPC에서 AWS 서비스로 이동할 수 있도록 VPC에 인터넷 게이트웨이를 추가해야 합니다. 이 구성이 네트워크 보안 요구 사항에 맞지 않는 경우 인터넷 게이트웨이를 사용하지 AWS PrivateLink 않고 VPC에 있는 AWS 서비스 것처럼 VPC를 연결할 수 있습니다.

VPC 엔드포인트를 AWS PrivateLink 사용하여 AWS 서비스 통합되는 서버에 비공개로 액세스할 수 있습니다. 이 경우 인터넷 게이트웨이를 사용하지 않고도 애플리케이션 스택의 모든 계층을 구축하고 관리할 수 있습니다.

요금

각 가용 영역에 인터페이스 VPC 엔드포인트가 프로비저닝된 시간당 요금이 청구됩니다. 또한 처리된 데이터의 GB당도 청구됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

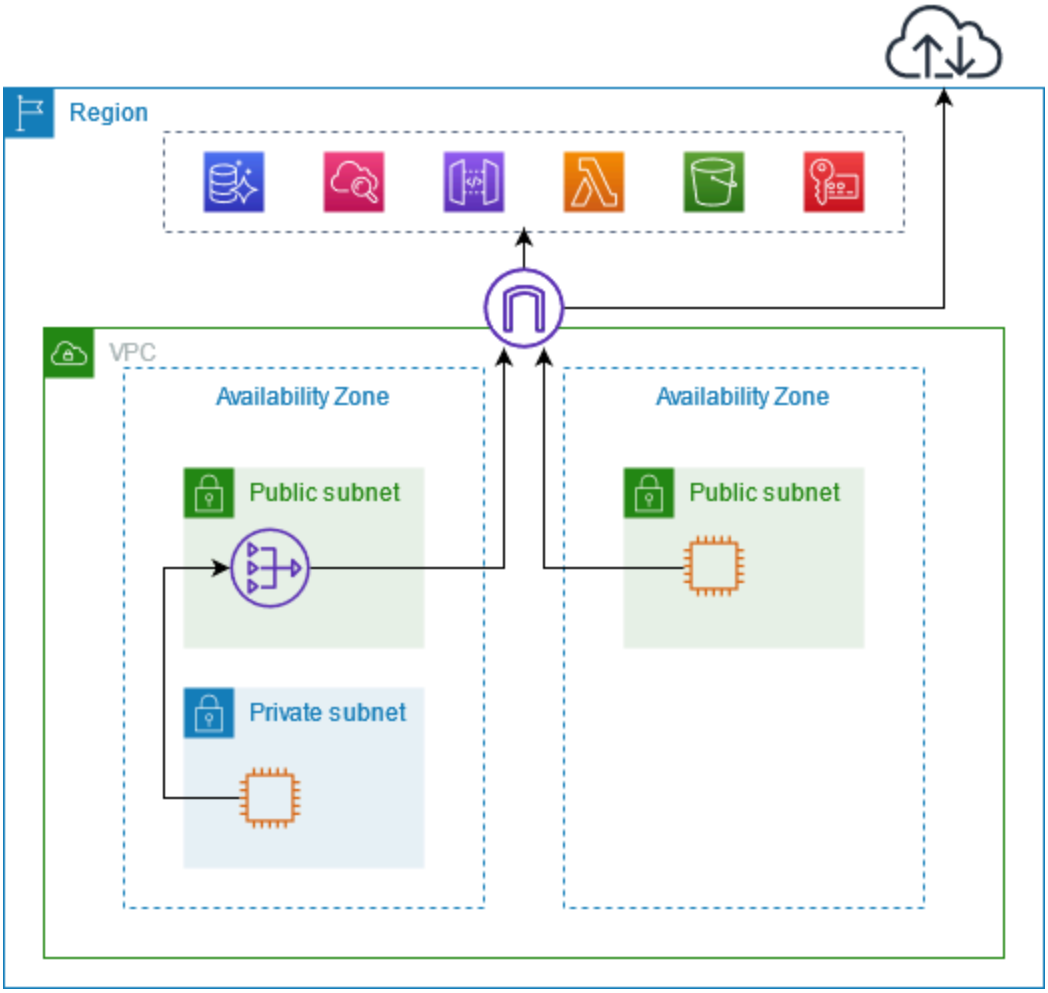
내용

개요

공용 서비스 엔드포인트를 AWS 서비스 통해 액세스하거나 지원되는 AWS 서비스 엔드포인트를 사용하여 연결할 수 있습니다. AWS PrivateLink이 개요에서는 두 방법을 비교합니다.

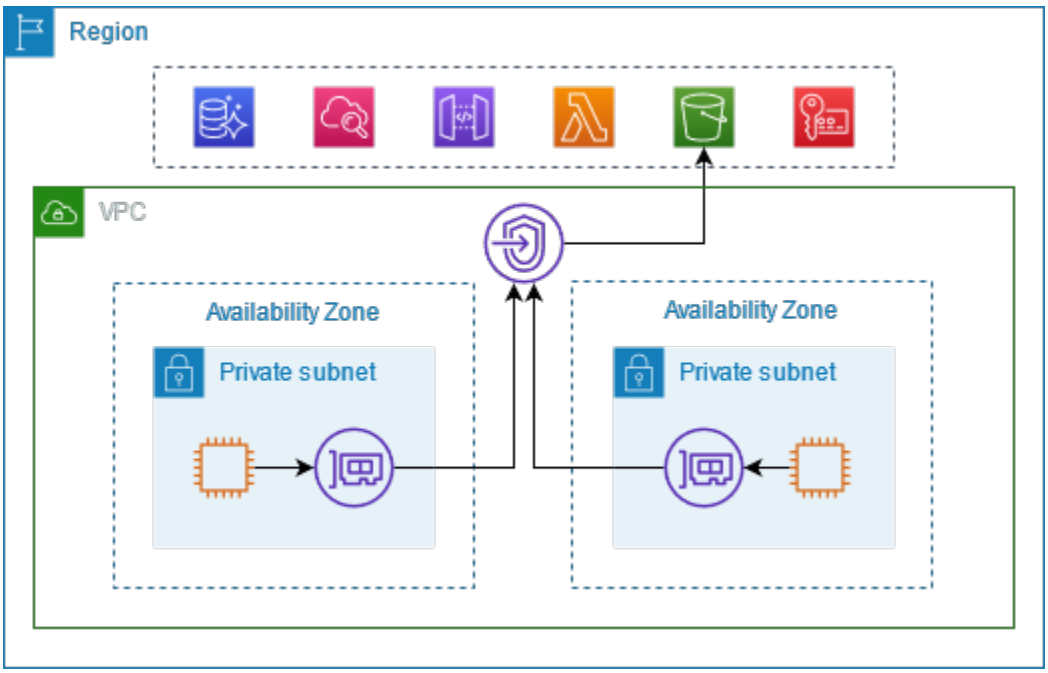
퍼플릭 서비스 엔드포인트를 통한 액세스

다음 다이어그램은 퍼블릭 서비스 엔드포인트를 AWS 서비스 통해 인스턴스에 액세스하는 방법을 보여줍니다. 퍼블릭 서브넷의 AWS 서비스 인스턴스에서 들어오는 트래픽은 VPC의 인터넷 게이트웨이로 라우팅된 다음 VPC의 인터넷 게이트웨이로 라우팅됩니다. AWS 서비스프라이빗 서브넷의 인스턴스에서 AWS 서비스 로의 트래픽은 차례로 NAT 게이트웨이, VPC의 인터넷 게이트웨이, AWS 서비스로 라우팅됩니다. 이 트래픽은 인터넷 게이트웨이를 통과하지만 네트워크를 벗어나지는 않습니다. AWS



연결: AWS PrivateLink

다음 다이어그램은 인스턴스가 어떻게 AWS 서비스 접속하는지를 보여줍니다 AWS PrivateLink. 먼저 인터페이스 VPC 엔드포인트를 생성합니다. 이 엔드포인트는 VPC의 서브넷과 네트워크 인터페이스를 사용하는 서브넷 간에 연결을 설정합니다. AWS 서비스 로 향하는 AWS 서비스 트래픽은 DNS를 사용하여 엔드포인트 네트워크 인터페이스의 사설 IP 주소로 확인된 다음 VPC 엔드포인트와 VPC 엔드포인트 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 다음과 같은 구문을 가진 퍼블릭 리전 엔드포인트를 AWS 서비스 제공합니다.

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

예를 들어 CloudWatch us-east-2에 있는 Amazon의 퍼블릭 엔드포인트는 다음과 같습니다.

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

AWS PrivateLink에서는 프라이빗 엔드포인트를 사용하여 서비스에 트래픽을 전송합니다. 인터페이스 VPC 엔드포인트를 생성하면 VPC에서 통신하는 데 사용할 수 있는 지역 및 영역 DNS 이름이 생성됩니다. AWS 서비스

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 AWS 서비스활성화할 수 있습니다. 프라이빗 DNS를 사용하면 인터페이스 VPC 엔드포인트를 통한 프라이빗 연결을 활용하면서 퍼블릭 엔드포인트의 DNS 이름을 사용하여 서비스에 계속 요청할 수 있습니다. 자세한 정보는 the section called “DNS 확인”을 참조하세요.

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 CloudWatch 활성화된 Amazon의 인터페이스 엔드포인트에 대한 예제 출력입니다. 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 프라이빗 DNS를 활성화하고 VPC에 DNS 호스트 이름과 DNS 확인이 모두 활성화되어 있는 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 지역 엔드포인트를 AWS 서비스 사용하여 요청을 보내는 기존 애플리케이션이 있는 경우 이제 해당 애플리케이션을 변경할 필요 없이 해당 요청이 엔드포인트 네트워크 인터페이스를 통해 전달됩니다.

VPC 엔드포인트의 프라이빗 DNS 이름을 활성화하는 것이 좋습니다. AWS 서비스이렇게 하면 퍼블릭 서비스 엔드포인트를 사용하는 요청 (예: AWS SDK를 통한 요청) 이 VPC 엔드포인트로 해결됩니다.

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 및 통합을 AWS Transit Gateway 참조하십시오. AWS PrivateLink Amazon Route 53 Resolver

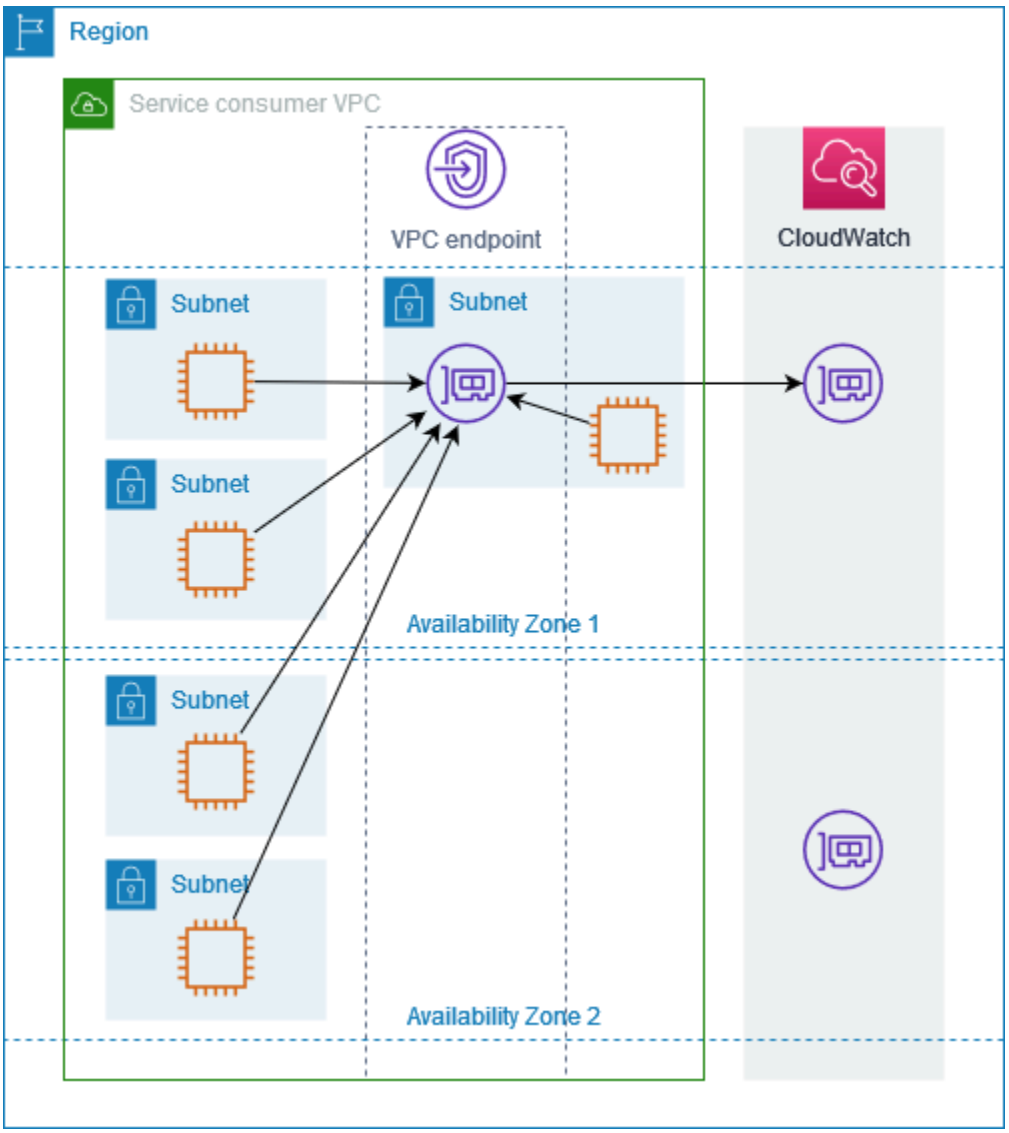
서브넷 및 가용 영역

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.

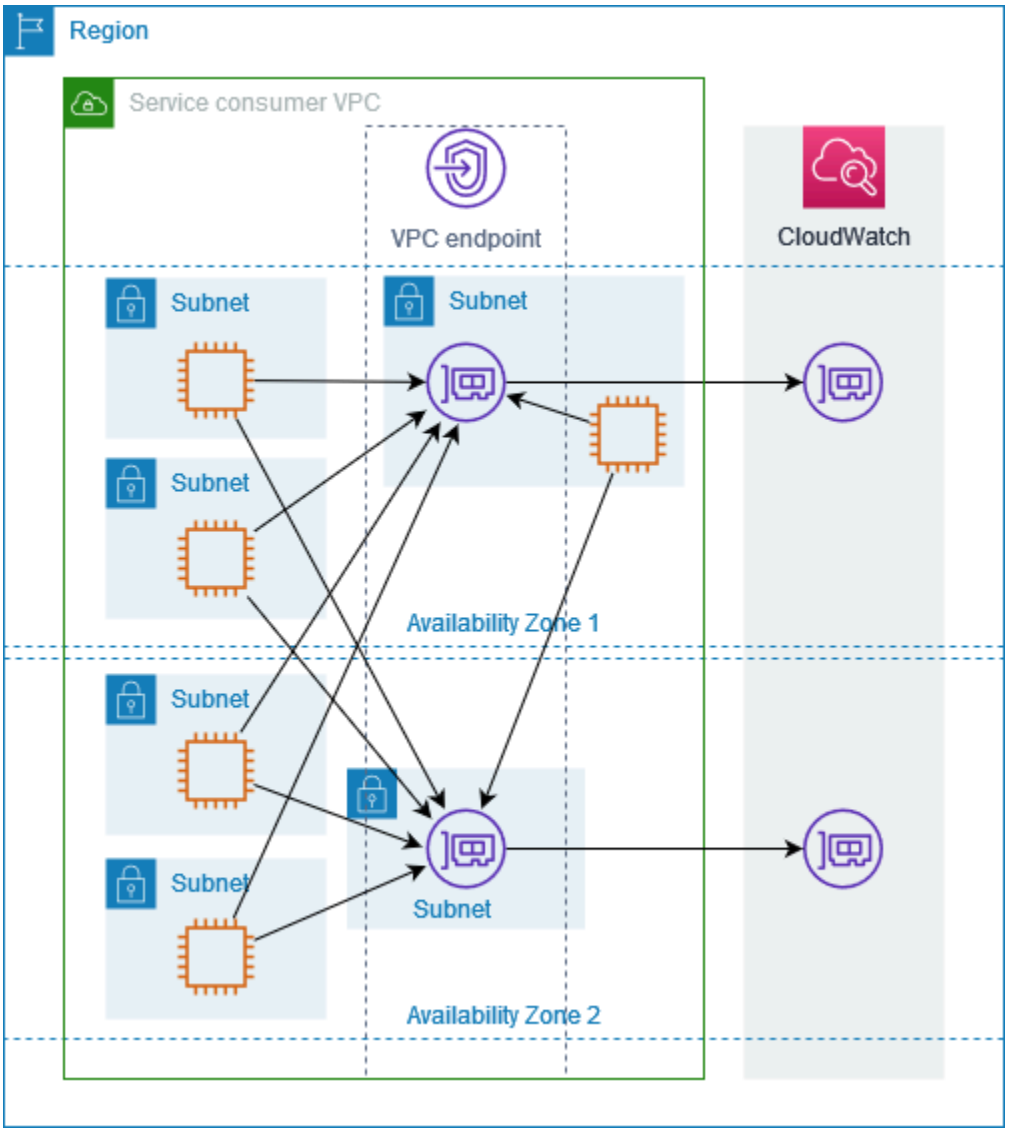
프로덕션 환경에서는 고가용성 및 복원력을 위해 다음과 같이 진행하는 것이 좋습니다.

- VPC 엔드포인트당 최소 두 개의 가용 영역을 구성하고 이러한 가용 영역에 액세스해야 하는 AWS 리소스를 배포하십시오. AWS 서비스
- VPC 엔드포인트의 프라이빗 DNS 이름을 구성합니다.
- 퍼블릭 엔드포인트라고도 AWS 서비스 하는 지역 DNS 이름을 사용하여 액세스합니다.

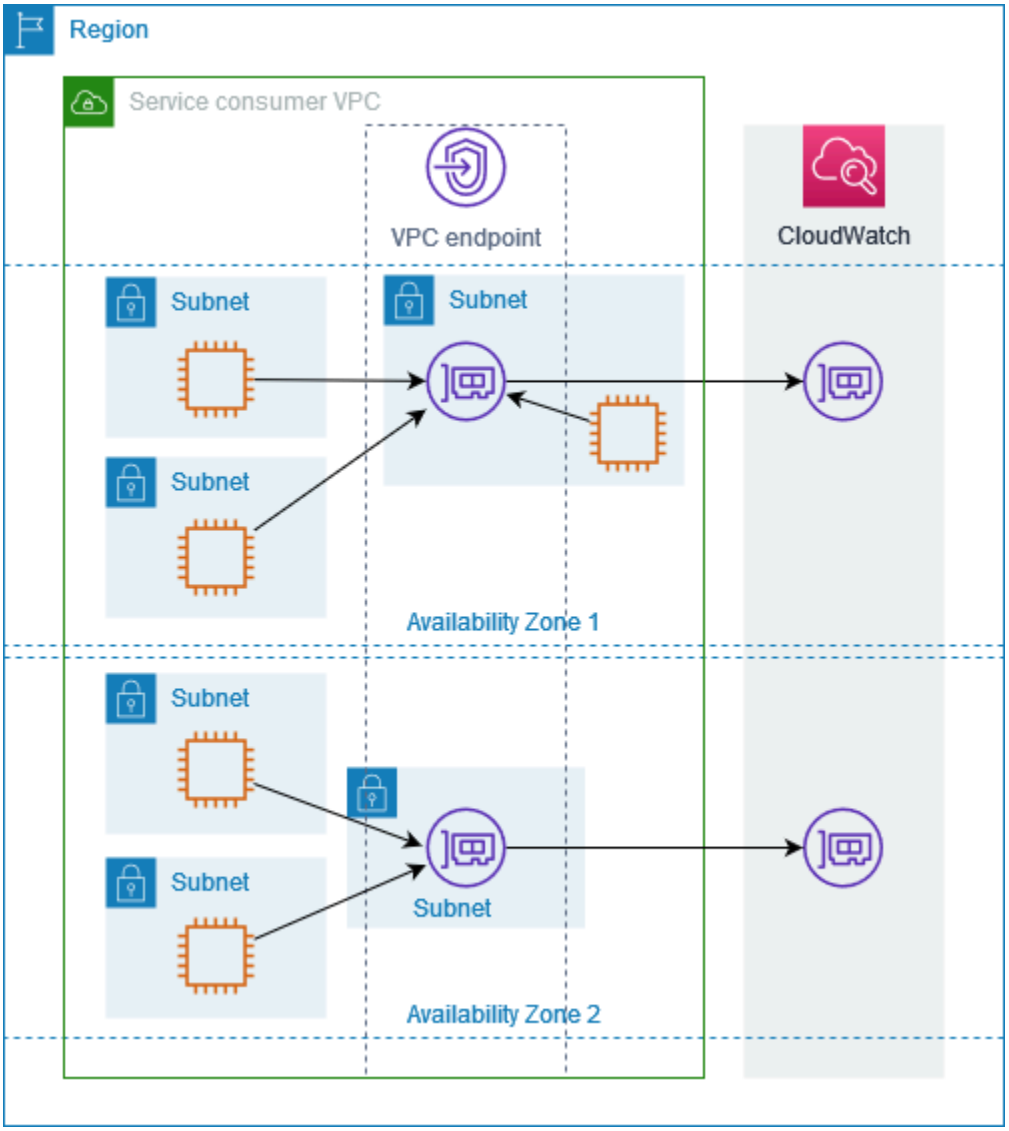
다음 다이어그램은 단일 가용 영역에 엔드포인트 네트워크 인터페이스가 CloudWatch 있는 Amazon 용 VPC 엔드포인트를 보여줍니다. VPC의 서브넷에 있는 리소스가 퍼블릭 엔드포인트를 사용하여 CloudWatch Amazon에 액세스하면 엔드포인트 네트워크 인터페이스의 IP 주소로 전달되는 트래픽을 해결합니다. 여기에는 다른 가용 영역에 있는 서브넷의 트래픽도 포함됩니다. 하지만 가용 영역 1이 손상되면 가용 영역 2의 리소스는 Amazon에 대한 액세스 권한을 잃게 CloudWatch 됩니다.



다음 다이어그램은 두 가용 영역에 엔드포인트 네트워크 인터페이스가 CloudWatch 있는 Amazon 용 VPC 엔드포인트를 보여줍니다. VPC의 서브넷에 있는 리소스가 퍼블릭 엔드포인트를 사용하여 CloudWatch Amazon에 액세스하는 경우 라운드 로빈 알고리즘을 사용하여 두 인터페이스를 번갈아 가며 사용하는 정상적인 엔드포인트 네트워크 인터페이스를 선택합니다. 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 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

- IPv6를 통해 AWS 서비스 서비스 엔드포인트를 사용할 수 있도록 해야 합니다. 자세한 정보는 the section called “IPv6 지원 보기”을 참조하세요.
- 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.

AWS 서비스 다음과 통합되는 AWS PrivateLink

다음은 와 AWS 서비스 AWS PrivateLink통합됩니다. VPC 엔드포인트를 생성하면 이러한 서비스에 비공개로 연결하여 자체 VPC에서 실행 중인 것처럼 서비스를 이용할 수 있습니다.

AWS 서비스열의 링크를 선택하면 통합되는 서비스에 대한 설명서를 볼 수 있습니다 AWS PrivateLink. 서비스 이름 열에는 인터페이스 VPC 엔드포인트를 만들 때 지정하는 서비스 이름이 포함되거나 서비스가 엔드포인트를 관리함을 나타냅니다.

AWS 서비스	서비스 이름
Access Analyzer	com.amazonaws.*region*.access-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata
AWS App Mesh	com.amazonaws.*region*.appmesh
	com.amazonaws.*region*.appmesh-envoy-management

AWS 서비스	서비스 이름
AWS 앱 러너	com.amazonaws.*region*.apprunner
AWS App Runner 서비스	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS 애플리케이션 마이그레이션 서비스	com.amazonaws.*region*.mgn
아마존 AppStream 2.0	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
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS B2B Data Interchange	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*region*.bedrock
	com.amazonaws. *##. ###-####*
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-runtime
AWS Billing Conductor	com.amazonaws.*region*.billingconductor

AWS 서비스	서비스 이름
Amazon Braket	com.amazonaws.*region*.braket
AWS 클린 룸	com.amazonaws.*region*.cleanrooms
AWS 클린 룸 ML	com.amazonaws. *##. ###-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
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
아마존 CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics
아마존 CloudWatch 로그	com.amazonaws.*region*.logs

AWS 서비스	서비스 이름
아마존 CloudWatch 네트워크 모니터	com.amazonaws. *## #### ###*
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. *## #####.api*
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	amazonaws*region*.codedeploy-commands-secure
아마존 CodeGuru 프로파일러	com.amazonaws.*region*.codeguru-profiler
아마존 CodeGuru 리뷰어	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
아마존 CodeWhisperer	com.amazonaws.*region*.codewhisperer
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Config	com.amazonaws.*region*.config

AWS 서비스	서비스 이름
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. *## ## ####*
AWS Data Exchange	com.amazonaws.*region*.dataexchange
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws.*region*.dms
	com.amazonaws.*region*.dms-fips
AWS DataSync	com.amazonaws.*region*.datasync
아마존 DataZone	com.amazonaws.*region*.datazone
AWS Deadline Cloud	com.amazonaws. *##, ###, ##*
	com.amazonaws. *##. ###. ####*
아마존 DevOps 전문가	com.amazonaws.*region*.devops-guru
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws. *##. dynamodb*
Amazon EBS 다이렉트 API	com.amazonaws.*region*.ebs

AWS 서비스	서비스 이름
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
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
	com.amazonaws.*region*.eks-auth
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
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
아마존 ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect

AWS 서비스	서비스 이름
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR on EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless
아마존 EMR 월	com.amazonaws. *.emrwal.prod ##*
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
아마존 EventBridge	com.amazonaws.*region*.events
	com.amazonaws. *##. ###-###*
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
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
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Amazon Managed Grafana	com.amazonaws.*region*.grafana

AWS 서비스	서비스 이름
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
아마존 GuardDuty	com.amazonaws.*region*.guardduty-data
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws. *##.dicom-###-###*
	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*.control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.workflows-omics
IAM Identity Center	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials
	com.amazonaws.*region*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws.*region*.deviceadvisor.iot

AWS 서비스	서비스 이름
AWS IoT Core for LoRaWAN	com.amazonaws.*region*.iotwireless.api
	com.amazonaws.*region*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns
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
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex

AWS 서비스	서비스 이름
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console

AWS 서비스	서비스 이름
	com.amazonaws.*region*.signin
Amazon MemoryDB for Redis	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 Neptune Analytics	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
아마존 OpenSearch 서비스	이러한 엔드포인트는 서비스 관리형입니다.
AWS Organizations	com.amazonaws. *##. ##*
	com.amazonaws. *##. ##-fips*
AWS Outposts	com.amazonaws. *##. ## ##*
AWS Panorama	com.amazonaws.*region*.panorama
AWS 결제 및 암호화	com.amazonaws.*region*.payment-cryptography.controlplane
	com.amazonaws.*region*.payment-cryptography.dataplane
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime

AWS 서비스	서비스 이름
AWS Supply Chain	com.amazonaws. *.scn ##*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS 프라이빗 5G	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q 비즈니스용	aws.api. *##. q ####*
Amazon QLDB	com.amazonaws.*region*.qldb.session
아마존 QuickSight	com.amazonaws. *##. #### ####*
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS Data API	com.amazonaws.*region*.rds-data
AWS re:포스트 비공개	com.amazonaws. *##. ########*
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
Amazon Redshift 데이터 API	com.amazonaws.*region*.redshift-data
	com.amazonaws. 지역*. #####-###-fips*
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips

AWS 서비스	서비스 이름
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Amazon S3 다중 리전 액세스 포인트	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws.*region*.s3-outposts
아마존 SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts
서비스 카탈로그	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry
Amazon SES	com.amazonaws.*region*.email-smtp
AWS SimSpace Weaver	com.amazonaws.*region*.simspaceweaver

AWS 서비스	서비스 이름
AWS Snow Device Management	com.amazonaws.*region*.snow-device-management
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
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 Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS 텔코 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*
InfluxDB용 Amazon Timestream	com.amazonaws. 지역 *.timestream-influxdb*
Amazon Transcribe	com.amazonaws.*region*.transcribe

AWS 서비스	서비스 이름
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
아마존 WorkSpaces	com.amazonaws.*region*.workspaces
아마존 WorkSpaces 씬 클라이언트	com.amazonaws. *## .thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

사용 가능한 AWS 서비스 이름 보기

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

다음 예제는 지정된 지역에서 인터페이스 AWS 서비스 엔드포인트를 지원하는 방법을 보여줍니다. 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 예 출력입니다.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

서비스에 대한 정보 보기

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

다음 예제는 지정된 지역의 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. VpcEndpointPolicySupported는 엔드포인트 정책이 지원되는지 여부를 나타냅니다. SupportedIpAddressTypes는 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"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "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
```

출력의 예제는 다음과 같습니다.

```
True
```

다음 예제는 지정된 지역에서 엔드포인트 정책을 AWS 서비스 지원하는 목록을 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'
```

출력의 예제는 다음과 같습니다.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

다음 예제는 지정된 지역에서 엔드포인트 정책을 지원하지 AWS 서비스 않는 항목을 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'
```

출력의 예제는 다음과 같습니다.

```
[
    "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.cleanrooms",
    "com.amazonaws.us-east-1.cleanrooms-ml",
```

```
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

IPv6 지원 보기

다음 describe-vpc-endpoint-services 명령을 사용하여 지정된 지역에서 IPv6를 통해 액세스할 수 AWS 서비스 있는 항목을 볼 수 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 예 출력입니다.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

인터페이스 AWS 서비스 VPC 엔드포인트 액세스 및 사용

인터페이스 VPC 엔드포인트를 생성하여 이를 통해 AWS PrivateLink구동되는 서비스 (여러 서비스 포함) 에 연결할 수 있습니다. AWS 서비스개요는 the section called “개념” and 액세스 AWS 서비스을(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

- 필수 조건
- VPC 엔드포인트 생성
- 공유 서브넷

필수 조건

- VPC에서 액세스할 리소스를 배포합니다 AWS 서비스 .
- 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 엔드포인트에서 IPv6를 활성화하려면 IPv6를 통한 액세스를 AWS 서비스 지원해야 합니다. 자세한 정보는 the section called “IP 주소 유형”을 참조하세요.
- VPC의 리소스에서 들어오는 예상 트래픽을 허용하는 엔드포인트 네트워크 인터페이스용 보안 그룹을 생성합니다. 예를 들어 에서 HTTPS 요청을 에 보낼 AWS CLI 수 있게 하려면 보안 그룹이 인바운드 HTTPS 트래픽을 허용해야 합니다. AWS 서비스
- 리소스가 네트워크 ACL이 있는 서브넷에 있는 경우, 네트워크 ACL이 VPC의 리소스와 엔드포인트 네트워크 인터페이스 간의 트래픽을 허용하는지 확인하십시오.
- 리소스에는 할당량이 있습니다. AWS PrivateLink 자세한 정보는 AWS PrivateLink 할당량을 참조하세요.

VPC 엔드포인트 생성

다음 절차에 따라 AWS 서비스에 연결하는 인터페이스 VPC 엔드포인트를 생성합니다.

에 대한 인터페이스 엔드포인트를 만들려면 AWS 서비스

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. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
5. 서비스 이름(Service name)에서 서비스를 선택합니다. 자세한 정보는 the section called “통합되는 서비스”을 참조하세요.
6. VPC에서 AWS 서비스에 액세스하는 데 사용할 VPC를 선택합니다.
7. 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 퍼블릭 서비스 엔드포인트를 사용하는 요청 (예: AWS SDK를 통한 요청) 이 VPC 엔드포인트로 해결됩니다.

8. 서브넷(Subnets)에서 AWS 서비스액세스를 시작할 서브넷을 가용 영역당 하나만 선택합니다. 동일한 가용 영역에서 여러 서브넷을 선택할 수 없습니다. 자세한 정보는 the section called “서브넷 및 가용 영역”을 참조하세요.

   선택한 각 서브넷에서 엔드포인트 네트워크 인터페이스가 생성됩니다. 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. 서브넷 CIDR 블록의 처음 4개 IP 주소와 마지막 IP 주소는 내부용으로 예약되어 있으므로 엔드포인트 네트워크 인터페이스에 지정할 수 없습니다.

9. IP 주소 유형(IP address type)에서 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.

10. 보안 그룹의 경우 VPC 엔드포인트의 엔드포인트 네트워크 인터페이스에 연결할 보안 그룹을 선택합니다. 기본적으로 VPC에 대한 기본 보안 그룹이 연결됩니다.

11. 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. 이 옵션은 서비스에서 VPC 엔드포인트 정책을 지원하는 경우에만 사용할 수 있습니다. 자세한 정보는 엔드포인트 정책을 참조하세요.

12. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.

13. Create endpoint(엔드포인트 생성)을 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(윈도우용 도구) PowerShell

공유 서브넷

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

인터페이스 엔드포인트 구성

엔인터페이스 VPC 엔드포인트를 생성한 후 해당 구성을 업데이트할 수 있습니다.

Tasks

- 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 정보는 the section called “서브넷 및 가용 영역”을 참조하세요.

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(윈도우용 도구 PowerShell)

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(윈도우용 도구 PowerShell)

VPC 엔드포인트 정책 편집

에서 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 정보는 엔드포인트 정책을 참조하세요.

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. 저장(Save)을 선택합니다.

명령줄을 사용하여 엔드포인트 정책 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(윈도우용 도구 PowerShell)

프라이빗 DNS 이름 활성화

VPC 엔드포인트의 프라이빗 DNS 이름을 활성화하는 것이 좋습니다. AWS 서비스이렇게 하면 퍼블릭 서비스 엔드포인트를 사용하는 요청 (예: AWS SDK를 통한 요청) 이 VPC 엔드포인트로 해결됩니다.

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 해제하십시오. 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” 섹션을 참조하세요.
7. 변경 사항 저장(Save changes)을 선택합니다.

명령줄을 사용하여 프라이빗 DNS 이름 옵션 변경하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(윈도우용 도구) PowerShell

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(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. 저장(Save)을 선택합니다.

명령줄을 사용하여 태그 관리하기

- create-tags 및 delete-tags(AWS CLI)

- New-EC2Tag및 Remove-EC2Tag(윈도우용 도구 PowerShell)

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.

Tasks

- 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. 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 인터페이스 엔드포인트에 대한 알림 생성하기

- create-vpc-endpoint-connection-notification(AWS CLI)

- New-EC2VpcEndpointConnectionNotification(윈도우용 도구 PowerShell)

액세스 정책 추가

Amazon SNS 주제에 다음과 같이 사용자 대신 알림을 AWS PrivateLink 게시할 수 있는 액세스 정책을 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.

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

키 정책 추가

암호화된 SNS 주제를 사용하는 경우 KMS 키의 리소스 정책이 AWS KMS API 작업을 AWS PrivateLink 호출할 수 있도록 신뢰해야 합니다. 다음은 예제 키 정책입니다.

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

```
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

인터페이스 엔드포인트 삭제

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

콘솔을 사용하여 인터페이스 엔드포인트를 삭제하려면

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(윈도우용 도구 PowerShell)

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 PrivateLink달리 사용하지 않습니다.

Amazon S3와 DynamoDB는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다. 옵션을 비교하려면 다음을 참조하십시오.

- Amazon S3의 VPC 엔드포인트 유형
- Amazon DynamoDB의 VPC 엔드포인트 유형

요금

게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다.

내용

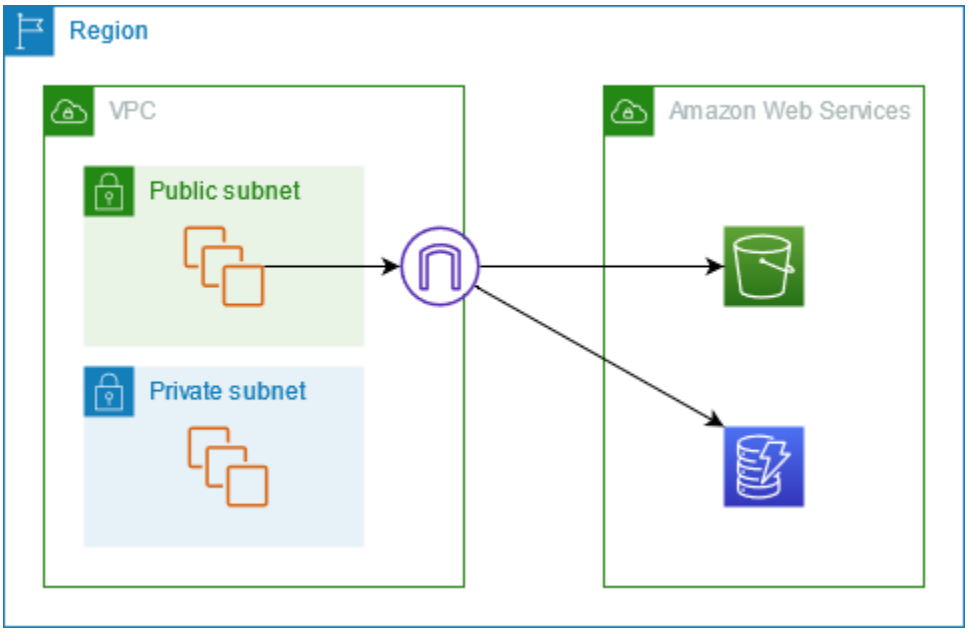
개요

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

인터넷 게이트웨이를 통한 액세스

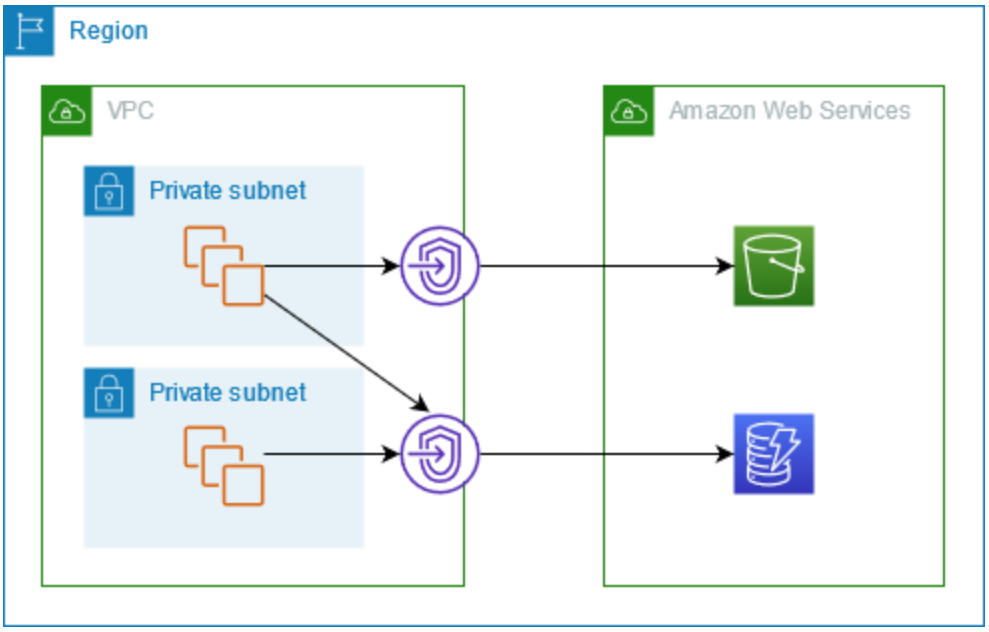
다음 다이어그램은 인스턴스에서 퍼블릭 서비스 엔드포인트를 통해 Amazon S3 및 DynamoDB에 액세스하는 방법을 보여줍니다. 퍼블릭 서브넷의 인스턴스에서 Amazon S3 또는 DynamoDB로의 트래픽은 VPC의 인터넷 게이트웨이를 거쳐 서비스로 라우팅됩니다. 프라이빗 서브넷의 인스턴스는 Amazon S3 또는 DynamoDB로 트래픽을 전송할 수 없습니다. 기본적으로 프라이빗 서브넷에는 인터넷 게이트웨이에 대한 라우팅이 없기 때문입니다. 프라이빗 서브넷의 인스턴스에서 Amazon S3 또는 DynamoDB로 트래픽을 보내려면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

픽을 NAT 디바이스로 라우팅합니다. Amazon S3 또는 DynamoDB로 향하는 트래픽은 인터넷 게이트웨이를 통과하지만 네트워크를 벗어나지 않습니다. AWS



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. 대상은 소유한 서비스의 접두사 AWS 목록이고 대상은 게이트웨이 엔드포인트입니다.

대상 주소	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 라우팅을 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 곳으로 향하는 트래픽은 인터넷 AWS 서비스 게이트웨이를 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.

대상	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.

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

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. 하지만 게이트웨이 엔드포인트는 온프레미스 네트워크, 다른 AWS 지역의 피어링된 VPC 또는 트랜짓 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 대한 AWS 서비스 액세스가 필요한 서버를 사용하고 있는지 확인하십시오. 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 액세스할 수 있도록 허용하는지 확인하십시오.
- 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.
- 게이트웨이 엔드포인트는 IPv4 트래픽만 지원합니다.
- Amazon S3가 수신한 해당 서브넷에 있는 인스턴스의 원본 IPv4 주소는 퍼블릭 IPv4 주소에서 VPC의 프라이빗 IPv4 주소로 변경됩니다. 엔드포인트는 네트워크 라우팅을 스위칭하고 열린 TCP 연결

을 끊습니다. 퍼블릭 IPv4 주소를 사용한 이전 연결이 다시 시작되지 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, 트랜짓 게이트웨이 또는 AWS Direct Connect VPC 연결의 반대편에 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.

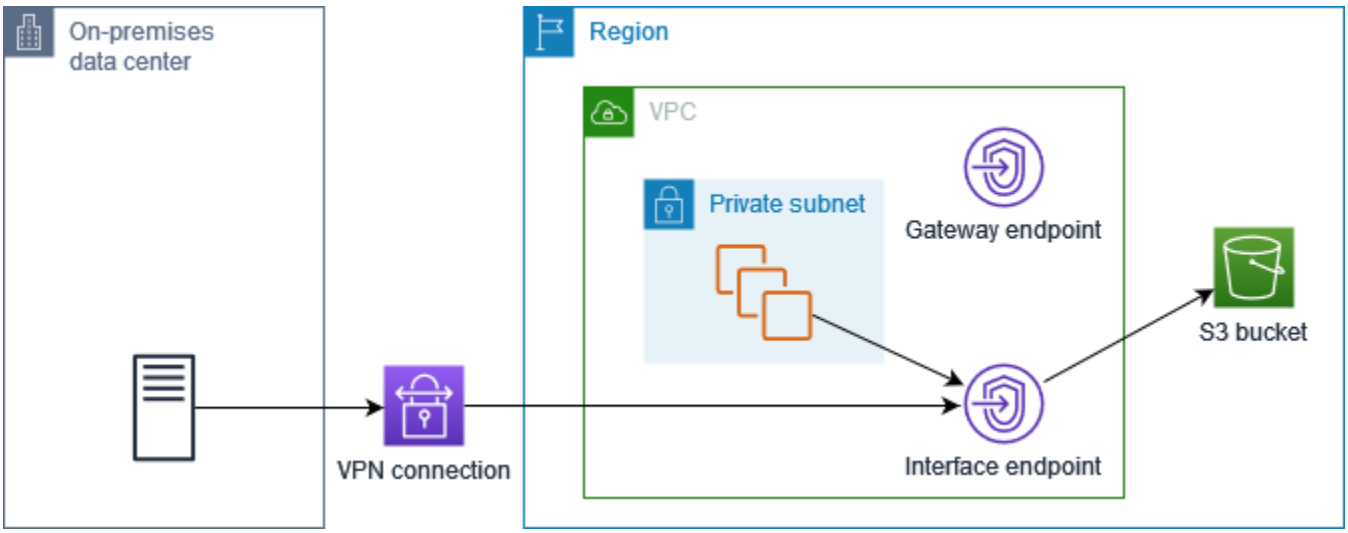
Route 53 Resolver

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 엔드포인트는 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.

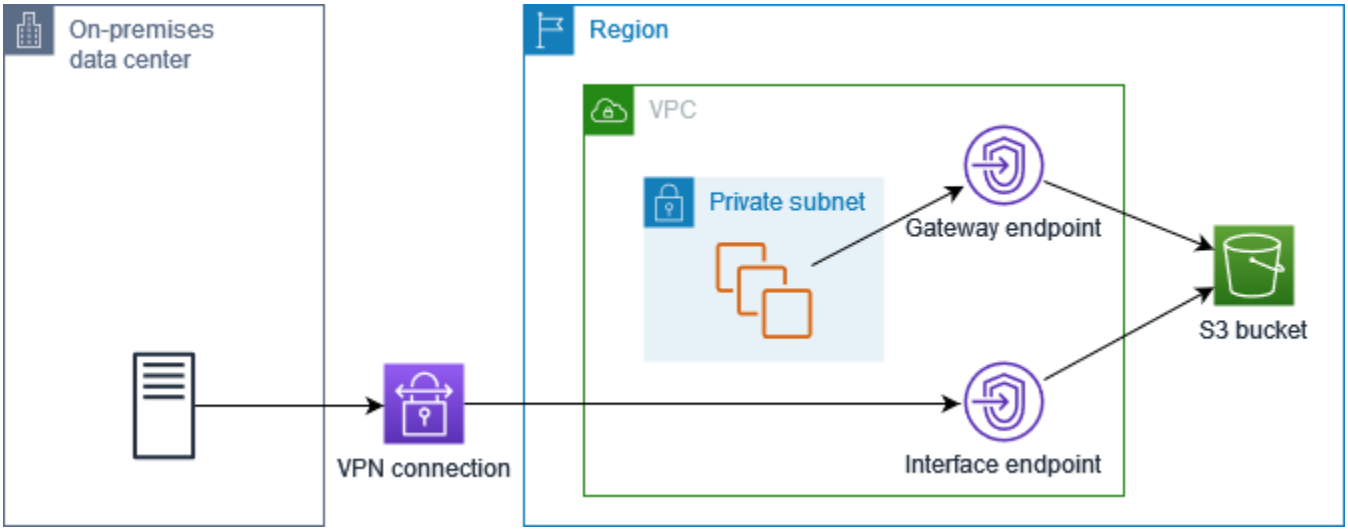
프라이빗 DNS

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.



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. Create endpoint(엔드포인트 생성)을 선택합니다.
4. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
5. 서비스의 경우 유형 = 게이트웨이 필터를 추가하고 com.amazonaws를 선택합니다. **`.s3 ##.`**
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. Create endpoint(엔드포인트 생성)을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(PowerShell윈도우용 도구)

버킷 정책을 사용한 액세스 제어

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

Example 예: 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.

```
{
  "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"
        }
      }
    }
  ]
}
```

Example 예: 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.

```
{
  "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"
        }
      }
    }
  ]
}
```

Example 예: 특정 IP 주소 범위에 대한 액세스 제한

aws: VpcSource Ip 조건 키를 사용하여 특정 IP 주소 범위에 대한 액세스를 제한하는 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.

```
{
  "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"
        }
      }
    }
  ]
}
```

Example 예: 특정 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.

```
{
  "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(PowerShell윈도우용 도구)

VPC 엔드포인트 정책 편집

게이트웨이 엔드포인트에 대한 엔드포인트 정책을 편집하여 VPC에서 엔드포인트를 통해 Amazon S3에 대한 액세스를 제어할 수 있습니다. 기본 정책에서는 모든 액세스를 허용합니다. 자세한 정보는 엔드포인트 정책을 참조하세요.

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. 저장(Save)을 선택합니다.

다음은 Amazon S3에 액세스하기 위한 엔드포인트 정책의 예입니다.

Example 예: 특정 버킷에 대한 액세스 제한

특정 S3 버킷에 대해서만 액세스를 제한하는 정책을 생성할 수 있습니다. VPC에 S3 버킷을 사용하는 다른 AWS 서비스 버킷이 있는 경우 유용합니다.

```
{
  "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/*"
      ]
    }
```

```
  ]
}
```

Example 예: 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.

```
{
  "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"
        }
      }
    }
  ]
}
```

Example 예: 특정 계정의 사용자에 대한 액세스 제한

특정 계정에 대한 액세스를 제한하는 정책을 생성할 수 있습니다.

```
{
  "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(윈도우용 도구) PowerShell

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 VPC용 인터넷 게이트웨이 또는 NAT 디바이스 없이도 추가 비용 없이 VPC에서 DynamoDB에 액세스할 수 있습니다. 하지만 게이트웨이 엔드포인트는 온프레미스 네트워크, 다른 지

역의 피어링된 VPC 또는 트랜짓 게이트웨이를 통한 액세스를 허용하지 않습니다. AWS 이러한 시나리오에서는 추가 비용을 지불한 후 사용할 수 있는 인터페이스 엔드포인트를 사용해야 합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 DynamoDB용 VPC 엔드포인트 유형을 참조하십시오.

내용

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.
- 를 사용하여 DynamoDB 작업을 AWS CloudTrail 기록하는 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, 트랜짓 게이트웨이 또는 AWS Direct Connect VPC 연결의 반대편에 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. Create endpoint(엔드포인트 생성)을 선택합니다.
4. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.
5. 서비스의 경우 유형 = 게이트웨이라는 필터를 추가하고 com.amazonaws를 선택합니다. ***#*** ***#: .dynamodb.***
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. Create endpoint(엔드포인트 생성)을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(윈도우용 도구) PowerShell

IAM 정책을 사용하여 액세스 제어

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

Example 예: 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.

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

Example 예: 특정 IAM 역할의 액세스 허용

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

```
{
   "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"
               }
            }
         }
      ]
}
```

Example 예: 특정 계정의 액세스 허용

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

```
{
   "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(윈도우용 도구 PowerShell)

VPC 엔드포인트 정책 편집

게이트웨이 엔드포인트에 대한 엔드포인트 정책을 편집하여 VPC에서 엔드포인트를 통해 DynamoDB에 대한 액세스를 제어할 수 있습니다. 기본 정책에서는 모든 액세스를 허용합니다. 자세한 정보는 엔드포인트 정책을 참조하세요.

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. 저장(Save)을 선택합니다.

명령줄을 사용하여 게이트웨이 엔드포인트 수정하기

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(윈도우용 도구 PowerShell)

다음은 DynamoDB에 액세스하기 위한 엔드포인트 정책의 예입니다.

Example 예제: 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": "*"
    }
  ]
}
```

Example 예: 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(윈도우용 도구 PowerShell)

다음을 통해 SaaS 제품에 액세스할 수 있습니다. AWS PrivateLink

를 사용하면 AWS PrivateLink마치 자체 VPC에서 실행되는 것처럼 SaaS 제품에 비공개로 액세스할 수 있습니다.

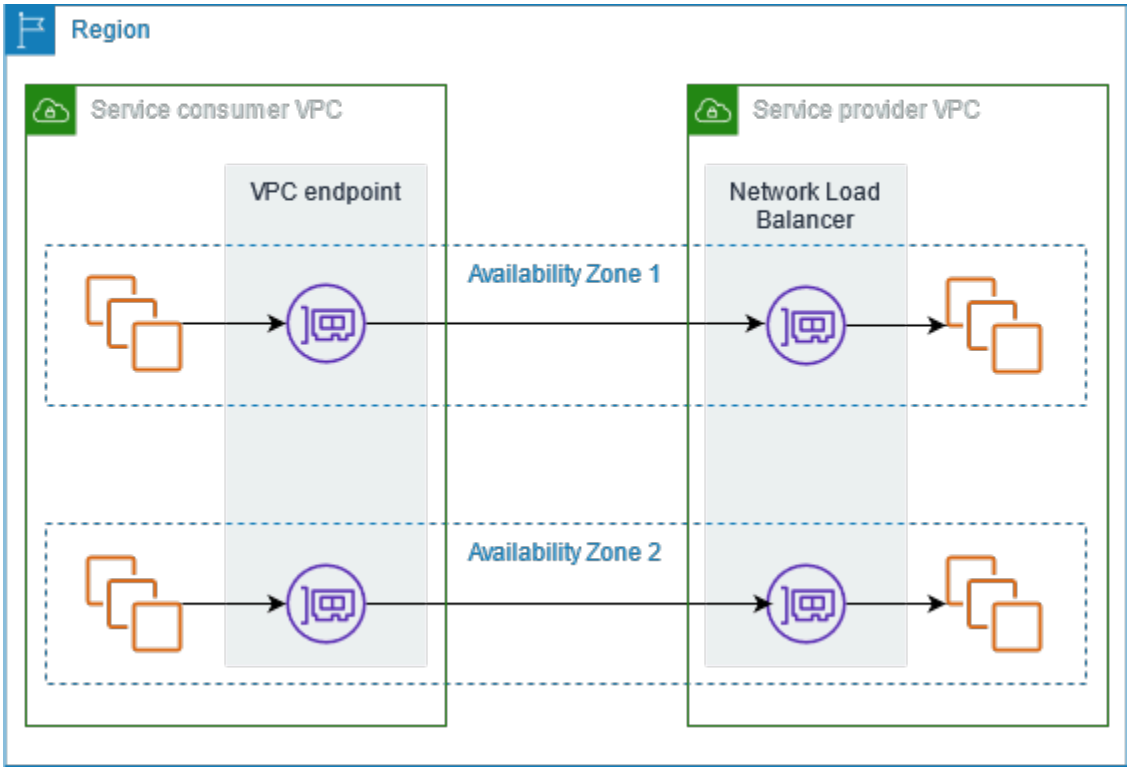
내용

개요

를 통해 AWS PrivateLink 구동되는 SaaS 제품을 검색, 구매 및 프로비저닝할 수 있습니다. AWS Marketplace자세한 내용은 AWS Marketplace다음을 참조하십시오. - PrivateLink.

파트너가 제공하는 SaaS 제품도 찾을 수 AWS PrivateLink 있습니다 AWS . 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 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. 에서 AWS Marketplace서비스를 구입한 경우 다음을 수행하십시오.
   a. 서비스 범주(Service category)에서 AWS Marketplace 서비스를 선택합니다.
   b. 서비스 이름을 입력합니다.
5. AWS Service Ready로 지정된 서비스에 가입한 경우 다음을 수행하십시오.
   a. 서비스 범주에서 PrivateLink Ready 파트너 서비스를 선택합니다.

b. 서비스 이름을 입력하고 서비스 확인(Verify service)을 선택합니다.

6. VPC에서 제품에 액세스하는 데 사용할 VPC를 선택합니다.
7. 서브넷(Subnets)에서 제품 액세스를 시작할 서브넷을 가용 영역당 하나만 선택합니다.
8. 보안 그룹(Security group)에서 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. Create endpoint(엔드포인트 생성)을 선택합니다.

인터페이스 엔드포인트를 구성하려면

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

를 통해 가상 어플라이언스에 액세스 AWS PrivateLink

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

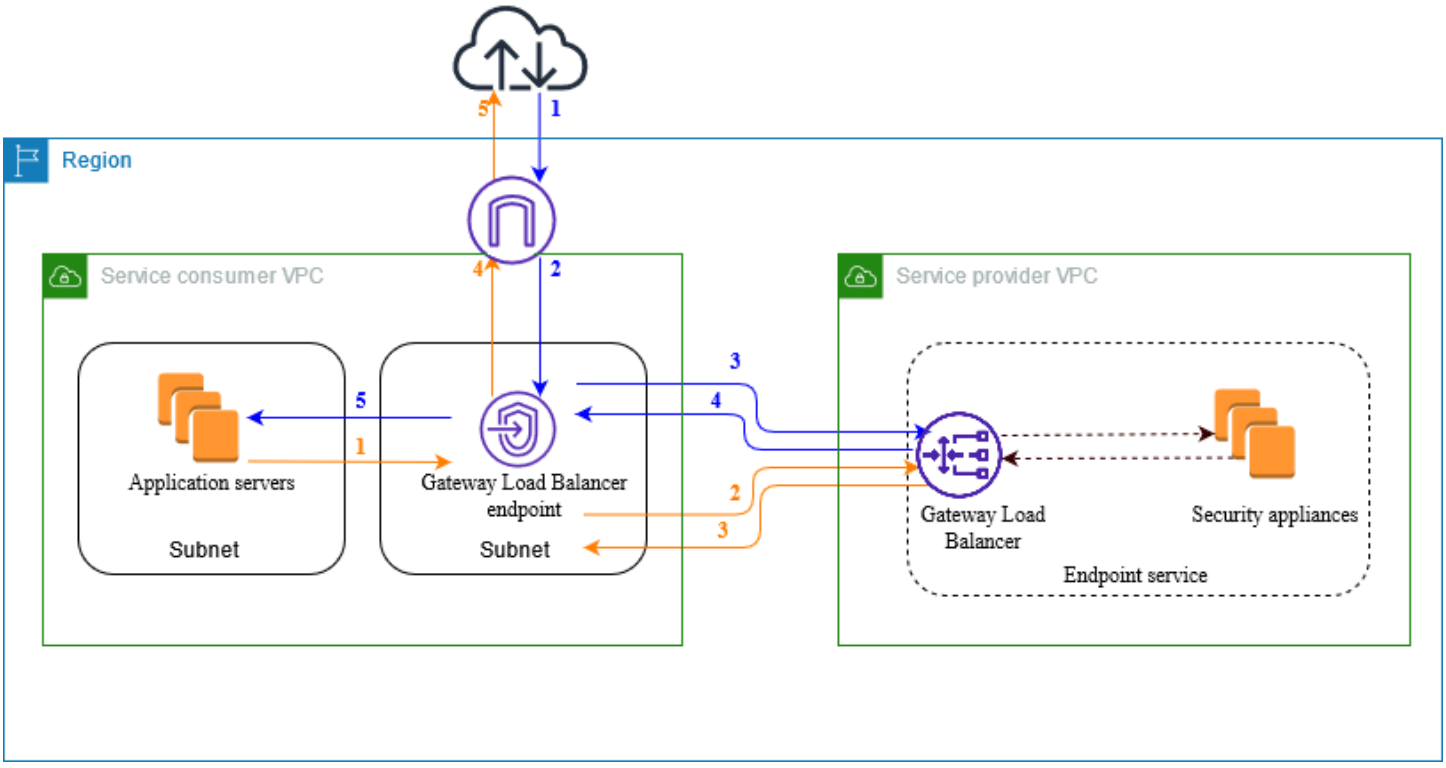
각 가용 영역에 Gateway Load Balancer 엔드포인트가 프로비저닝된 시간당 요금이 청구됩니다. 또한 처리된 데이터의 GB당도 청구됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

내용

자세한 내용은 Gateway Load Balancers를 참조하세요.

개요

다음 다이어그램은 애플리케이션 서버가 보안 어플라이언스에 액세스하는 방법을 보여줍니다. AWS PrivateLink애플리케이션 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 이중 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. 이중 스택 구성에는 IPv6 경로가 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

에 의해 구동되는 자체 서비스를 생성할 수 AWS PrivateLink있으며, 이를 엔드포인트 서비스라고 합니다. 귀하는 서비스 공급자이며, 서비스에 대한 AWS 연결을 생성하는 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

- 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 참조하십시오.

- 리소스에는 할당량이 있습니다. AWS PrivateLink 자세한 정보는 AWS PrivateLink 할당량을 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 이중 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 서비스(Endpoint services)를 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 새로운 태그 추가(Add new tag)를 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(윈도우용 도구) PowerShell

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 정보는 the section called “권한 관리”을 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 정보는 the section called “연결 요청 수락 또는 거부” 섹션을 참조하세요.

AWS 보안 주체는 Gateway Load Balancer 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 정보는 Gateway Load Balancer 엔드포인트 생성을 참조하세요.

Gateway Load Balancer 엔드포인트를 사용하여 검사 시스템 액세스

Gateway Load Balancer 엔드포인트를 생성하여 AWS PrivateLink기반 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 요청자 관리 네트워크 인터페이스입니다. 에서 확인할 수 있지만 직접 AWS 계정관리할 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 참조하십시오.
- 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 게이트웨이 로드 밸런서 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 게이트웨이 로드 밸런서 엔드포인트를 통해 라우팅되면 네트워크 로드 밸런서 클라이언트 IP 보존이 지원되지 않습니다.
- 리소스에는 할당량이 있습니다. AWS PrivateLink 자세한 정보는 AWS PrivateLink 할당량을 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. Create endpoint(엔드포인트 생성)을 선택합니다.
4. 서비스 범주(Service category)에서 기타 엔드포인트 서비스(Other endpoint services)를 선택합니다.
5. Service name(서비스 이름)에 서비스의 이름을 입력한 다음 Verify service(서비스 확인)를 선택합니다.
6. VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
7. Subnet(서브넷)에서 엔드포인트를 생성할 서브넷을 선택합니다.
8. IP 주소 유형(IP address type)에서 다음 옵션 중에서 선택합니다.
   - 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.
9. (선택 사항) 태그를 추가하려면 새 태그 추가를 선택하고 태그 키와 태그 값을 입력합니다.
10. Create endpoint(엔드포인트 생성)을 선택합니다. 초기 상태는 `pending acceptance`입니다.

명령줄을 사용하여 Gateway Load Balancer 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(윈도우용 도구) PowerShell

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 정보는 the section called “라우팅”을 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), Edit routes(라우팅 편집)를 선택합니다.
   b. IPv4를 지원하는 경우 Add route(라우팅 추가)를 선택합니다. Destination(대상)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 저장를 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 저장를 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 저장를 선택합니다.

명령줄을 사용하여 라우팅 구성하기

- create-route(AWS CLI)
- New-EC2Route(윈도우용 도구 PowerShell)

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. 저장(Save)을 선택합니다.

명령줄을 사용하여 태그 관리하기

- create-tags 및 delete-tags(AWS CLI)
- New-EC2Tag및 Remove-EC2Tag(윈도우용 도구 PowerShell)

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 여세요.
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)

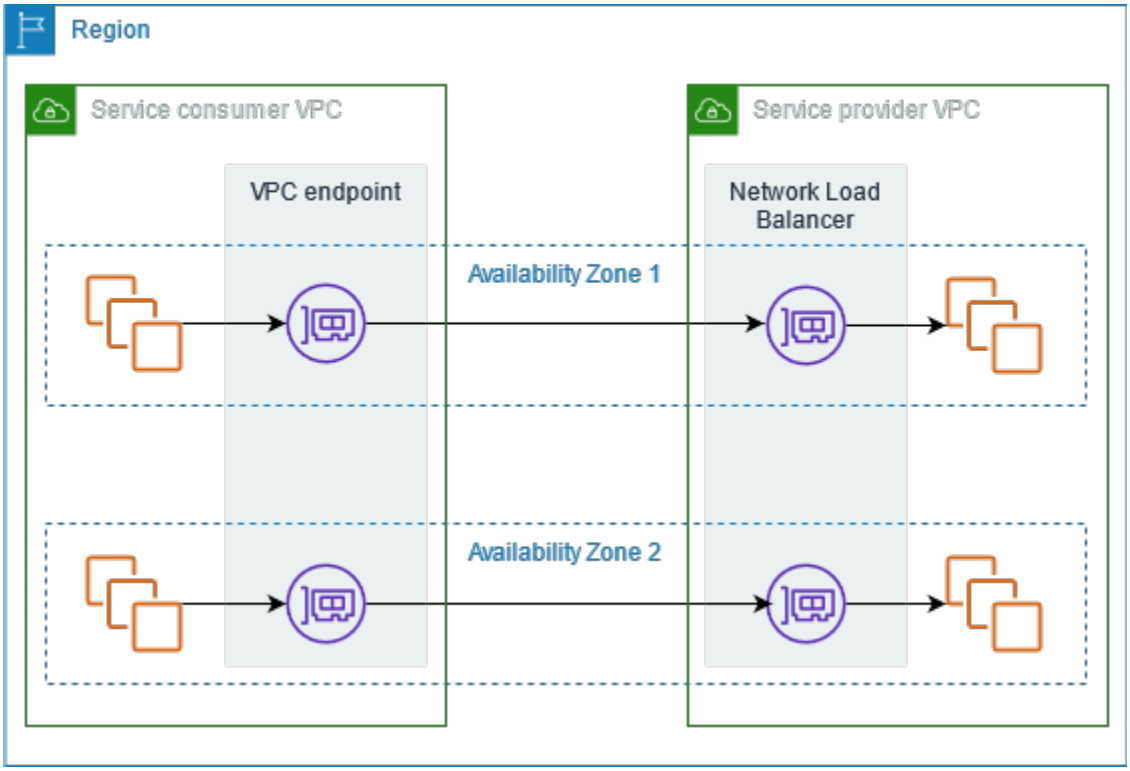
를 통해 서비스를 공유하세요 AWS PrivateLink

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

내용

개요

다음 다이어그램은 호스팅된 서비스를 다른 AWS 고객과 공유하는 방법과 해당 AWS 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 생성할 때 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.region.vpce.amazonaws.com
```

영역 이름의 구문은 다음과 같습니다.

```
endpoint_id-zone.endpoint_service_id.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 정보는 DNS 이름 관리을 참조하세요.

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.

에 의해 구동되는 서비스를 생성하십시오. AWS PrivateLink

에 의해 구동되는 자체 서비스를 생성할 수 AWS PrivateLink있으며, 이를 엔드포인트 서비스라고 합니다. 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. VPC 피어링을 사용하면 다른 리전에서 엔드포인트 서비스에 액세스할 수 있습니다.
- 엔드포인트 서비스는 TCP를 통한 트래픽만 지원합니다.
- 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 참조하십시오.
- 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.
- 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.
- 리소스에는 할당량이 있습니다. AWS PrivateLink 자세한 정보는 AWS PrivateLink 할당량을 참조하세요.

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 주소로부터 들어오는 인바운드 트래픽을 허용해야 합니다. 또는 통과하는 트래픽에 대한 인바운드 보안 그룹 규칙 평가를 해제할 수도 있습니다. AWS PrivateLink자세한 내용은 네트워크 부하 분산기 사용 설명서의 보안 그룹을 참조하십시오.
- 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.

  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 네트워크 부하 분산기 사용 설명서의 영역 간 부하 분산을 참조하십시오.

엔드포인트 서비스 생성

Network Load Balancer를 사용하여 엔드포인트 서비스를 생성하려면 다음 절차를 따르세요.

콘솔을 사용하여 엔드포codedeploy-commands-인트 서비스 생성하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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. 포함된 가용 영역에는 선택한 네트워크 로드 밸런서에 사용할 수 있는 가용 영역이 나열되어 있습니다. 엔드포인트 서비스는 이러한 가용 영역에서 사용할 수 있습니다.
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 요청이 자동으로 수락됩니다.
7. 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 액세스하

는 데 사용할 수 있는 프라이빗 DNS 이름을 연결한 다음 프라이빗 DNS 이름을 입력합니다. 그렇지 않으면 서비스 소비자가 에서 제공한 엔드포인트별 DNS 이름을 사용할 수 있습니다. AWS서비스 소비자가 프라이빗 DNS 이름을 사용할 수 있으려면 서비스 공급자가 소비자의 도메인 소유 사실을 증명해야 합니다. 자세한 정보는 DNS 이름 관리을 참조하세요.

8. 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.
9. (선택 사항) 태그를 추가하려면 새로운 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
10. 생성(Create)을 선택합니다.

명령줄을 사용하여 엔드포인트 서비스 생성하기

- create-vpc-endpoint-service-configuration(AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(윈도우용 도구) PowerShell

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

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. Create endpoint(엔드포인트 생성)을 선택합니다.
4. 서비스 범주(Service category)에서 기타 엔드포인트 서비스(Other endpoint services)를 선택합니다.
5. 서비스 이름(Service name)에 서비스의 이름(예: `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`)을 입력하고 서비스 확인(Verify service)을 선택합니다.
6. VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
7. Subnets(서브넷)에서 엔드포인트 서비스에 액세스할 서브넷(가용 영역)을 선택합니다.
8. IP 주소 유형(IP address type)에서 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.
9. 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.
10. 보안 그룹(Security group)에서 엔드포인트 네트워크 인터페이스에 연결할 보안 그룹을 선택합니다.
11. Create endpoint(엔드포인트 생성)을 선택합니다.

명령줄을 사용하여 인터페이스 엔드포인트 생성하기

- create-vpc-endpoint(AWS CLI)
- New-EC2VpcEndpoint(윈도우용 도구) PowerShell

엔드포인트 서비스 구성

엔드포인트 서비스를 생성한 후 해당 구성을 업데이트할 수 있습니다.

Tasks

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

권한 관리

권한과 수락 설정의 조합을 통해 엔드포인트 서비스에 액세스할 수 있는 서비스 소비자 (AWS 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 보안 주체의 Amazon 리소스 이름 (ARN) 이 필요합니다. 다음 목록에는 지원되는 AWS 보안 주체의 ARN 예시가 포함되어 있습니다.

보안 주체를 위한 ARN AWS

AWS 계정 (계정 내 모든 보안 주체 포함)

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

역할

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

User

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

모든 주도자 모두 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 이전에 수락된 엔드포인트와 서비스 간의 기존 연결에는 영향을 주지 않습니다.

콘솔을 사용해 엔드포인트 서비스에 대한 권한 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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 보안 주체를 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(Windows용 도구 PowerShell)

연결 요청 수락 또는 거부

권한과 수락 설정의 조합을 통해 엔드포인트 서비스에 액세스할 수 있는 서비스 소비자 (AWS 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.

연결 요청이 수락되거나 거부될 때 알림을 받을 수 있습니다. 자세한 정보는 the section called “엔드포인트 서비스 이벤트에 대한 알림 받기”을 참조하세요.

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.
- 이미 수락된 요청을 거부해도 엔드포인트와 서비스 간의 연결에는 영향을 미치지 않습니다.

콘솔을 사용하여 수락 설정 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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 저장(Save changes)을 선택합니다

명령줄을 사용하여 수락 설정 수정하기

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

콘솔을 사용하여 연결 요청 수락 또는 거부하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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-EC2EndpointConnection또는 Deny-EC2EndpointConnection(윈도우용 도구 PowerShell)

로드 밸런서 관리

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

Network Load Balancer에 대해 다른 가용 영역을 활성화하는 경우 엔드포인트 서비스의 가용 영역도 활성화할 수 있습니다. 엔드포인트 서비스에 대한 가용 영역을 활성화하면 서비스 소비자가 해당 가용 영역의 서브넷을 인터페이스 VPC 엔드포인트에 추가할 수 있습니다.

콘솔을 사용하여 엔드포인트 서비스의 로드 밸런서를 관리하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 작업(Actions), 로드 밸런서 연결 또는 연결 해제(Associate or disassociate load balancers)를 선택합니다.
5. 필요에 따라 엔드포인트 서비스 구성을 변경합니다. 예:
   - 로드 밸런서를 엔드포인트 서비스에 연결할 로드 밸런서의 확인란을 선택합니다.
   - 로드 밸런서의 확인란을 선택 취소하여 엔드포인트 서비스와의 연결을 끊습니다. 하나 이상의 로드 밸런서를 선택한 상태로 유지해야 합니다.
   - 최근에 로드 밸런서에 다른 가용 영역을 활성화한 경우 포함된 가용 영역 아래에 해당 가용 영역이 나타납니다. 다음 단계에서 변경 내용을 저장하면 새 가용 영역에 대한 엔드포인트 서비스가 활성화됩니다.

6. 변경 사항 저장(Save changes)을 선택합니다

명령줄을 사용하여 엔드포인트 서비스의 로드 밸런서를 관리하려면

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

로드 밸런서에 대해 최근에 활성화된 가용 영역에서 엔드포인트 서비스를 활성화하려면 엔드포인트 서비스의 ID를 사용하여 명령을 호출하기만 하면 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 정보는 DNS 이름 관리을 참조하세요.

콘솔을 사용하여 엔드포인트 서비스 프라이빗 DNS 이름 수정하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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 serivce)을 선택하고 프라이빗 DNS 이름을 입력합니다.
   - 도메인 이름에는 소문자를 사용해야 합니다.
   - 도메인 이름에 와일드카드를 사용할 수 있습니다(예: **`*.myexampleservice.com`**).
6. 변경 사항 저장를 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(PowerShellWindows용 도구)

콘솔을 사용하여 도메인 확인 시작하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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(윈도우용 도구 PowerShell)

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 서비스(Endpoint services)를 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 저장를 선택합니다.

명령줄을 사용하여 지원되는 IP 주소 유형 수정하기

- modify-vpc-endpoint-service-configuration(AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(윈도우용 도구 PowerShell)

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 서비스(Endpoint services)를 선택합니다.
3. VPC 엔드포인트 서비스를 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 태그 값을 입력합니다.
6. 태그를 제거하려면 태그 키 및 값 오른쪽에 있는 제거(Remove)를 선택합니다.
7. 저장(Save)을 선택합니다.

콘솔을 사용해 엔드포인트 연결에 대한 태그 관리하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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. 저장(Save)을 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 서비스(Endpoint services)를 선택합니다.
3. VPC 엔드포인트 서비스를 선택한 다음 보안 주체 허용(Allow principals) 탭을 선택합니다.
4. 보안 주체를 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. 저장(Save)을 선택합니다.

명령줄을 사용하여 태그 추가 또는 제거하기

- create-tags 및 delete-tags(AWS CLI)
- New-EC2Tag및 Remove-EC2Tag(윈도우용 도구 PowerShell)

VPC 엔드포인트 서비스의 DNS 이름 관리

서비스 공급자는 엔드포인트 서비스의 프라이빗 DNS 이름을 구성할 수 있습니다. 서비스 공급자가 기존 퍼블릭 DNS 이름을 엔드포인트 서비스의 프라이빗 DNS 이름으로 사용하는 경우에는 서비스 소비자가 기존 퍼블릭 DNS 이름을 사용하는 애플리케이션을 변경할 필요가 없습니다. 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.
- 프라이빗 DNS 이름에 대해 A 레코드를 생성하지 않아야 합니다. 그래야만 서비스 소비자 VPC의 서버만 프라이빗 DNS 이름을 확인할 수 있습니다.
- Gateway Load Balancer 엔드포인트에는 프라이빗 DNS 이름이 지원되지 않습니다.
- 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 63자까지 사용할 수 있으며 전체 도메인 이름은 총 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.

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 구성되어 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 서비스(Endpoint services)를 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. 또한 다음 describe-vpc-endpoint-service-configuration AWS CLI 명령을 사용하여 지정된 엔드포인트 서비스의 프라이빗 DNS 이름 구성에 대한 정보를 검색할 수 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.

명칭	유형	값
_6e86v84tqgqubxbwi i1m.example.com	TXT	RxlTtvPCE:L6P0E 45JevFWoCP

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 대한 레코드를 생성합니다. 다음 값을 사용합니다.

- 레코드 유형(Record type)에 대해 TXT를 선택합니다.
- TTL(초)(TTL (seconds))에 **1800**을 입력합니다.
- 라우팅 정책(Routing policy)에 대해 단순 라우팅(Simple routing)을 선택합니다.
- Record name(레코드 이름)에 도메인 또는 하위 도메인을 입력합니다.
- 값/트래픽 라우팅 대상(Value/Route traffic to)에 도메인 확인 값을 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	/eNom을 사용하여 DNS 레코드를 관리합니다. HostGator
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. Windows 및 Linux에서 사용할 수 있는 nslookup 명령을 실행합니다.

도메인에 서비스를 제공하는 DNS 서버에는 도메인에 대한 up-to-date 정보가 가장 많이 포함되어 있으므로 해당 서버를 쿼리해야 합니다. 도메인 정보가 다른 DNS 서버로 전파되는 데에는 시간이 걸립니다.

TXT 레코드가 DNS 서버에 게시되었는지 확인하려면

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.

Tasks

- 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 서비스(Endpoint services)를 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(윈도우용 도구 PowerShell)

액세스 정책 추가

사용자를 대신하여 알림을 AWS PrivateLink 게시할 수 있는 액세스 정책을 SNS 주제에 추가합니다. 예를 들면 다음과 같습니다. 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.

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

키 정책 추가

암호화된 SNS 주제를 사용하는 경우 KMS 키의 리소스 정책이 AWS KMS API 작업을 AWS PrivateLink 호출할 수 있도록 신뢰해야 합니다. 다음은 예제 키 정책입니다.

```
{
```

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

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 서비스(Endpoint services)를 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(윈도우용 도구 PowerShell)

에 대한 ID 및 액세스 관리 AWS PrivateLink

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS PrivateLink IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

내용

고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. AWS PrivateLink

서비스 사용자 - AWS PrivateLink 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS PrivateLink 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다.

서비스 관리자 — 회사에서 AWS PrivateLink 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS PrivateLink있습니다. 서비스 사용자가 액세스해야 하는 AWS PrivateLink 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오.

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

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 연동 자격 증명으로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

연동 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS

Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참

조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

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.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

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

액세스 제어 목록(ACLs)

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

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습

니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS PrivateLink 작동 방식

IAM을 사용하여 액세스를 AWS PrivateLink관리하기 전에 어떤 IAM 기능과 함께 사용할 수 있는지 알아보세요. AWS PrivateLink

함께 사용할 수 있는 IAM 기능 AWS PrivateLink

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

대부분의 IAM 기능과 함께 AWS 서비스 작동하는 방식 AWS PrivateLink 및 기타 기능을 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

아이덴티티 기반 정책은 다음과 같습니다. AWS PrivateLink

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

다음에 대한 ID 기반 정책 예제 AWS PrivateLink

AWS PrivateLink ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS PrivateLink

내 리소스 기반 정책 AWS PrivateLink

리소스 기반 정책 지원	예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신

뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 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 정보는 the section called “엔드포인트 정책”을 참조하세요.

에 대한 정책 조치 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 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

AWS PrivateLink API 네임스페이스를 Amazon EC2와 공유합니다. 정책 조치는 조치 앞에 다음 접두사를 AWS PrivateLink 사용합니다.

```
ec2
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "ec2:Describe*"
```

작업 목록을 보려면 Amazon EC2 API 참조의 AWS PrivateLink AWS PrivateLink 작업을 참조하십시오. 자세한 정보는 서비스 승인 참조의 Amazon EC2에서 정의한 작업을 참조하세요.

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 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 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 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리

적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

다음 조건 키는 다음과 같은 경우에만 해당됩니다. AWS PrivateLink

- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon EC2에서 정의한 작업을 참조하십시오.

내 ACL AWS PrivateLink

ACL 지원	아니요

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

ABAC 포함 AWS PrivateLink

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 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 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

임시 자격 증명 사용: AWS PrivateLink

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

서비스 간 사용자 권한: AWS PrivateLink

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

서비스 역할: AWS PrivateLink

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

서비스 연결 역할 AWS PrivateLink

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

다음과 같은 ID 기반 정책 예제 AWS PrivateLink

기본적으로 사용자 및 역할에는 AWS PrivateLink 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형의 ARN 형식을 비롯하여 에서 정의한 AWS PrivateLink작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon EC2용 작업, 리소스 및 조건 키를 참조하십시오.

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.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

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

엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어

엔드포인트 정책은 VPC 엔드포인트에 연결하여 엔드포인트를 사용하여 액세스할 수 있는 보안 AWS 주체를 제어하는 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. 보안 주체 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 수 있습니다. AWS 서비스언제든지 엔드포인트 정책을 업데이트할 수 있습니다. 엔드포인트 정책을 연결하지 않으면 기본 엔드포인트 정책이 연결됩니다.
- 모든 사람이 엔드포인트 정책을 AWS 서비스 지원하는 것은 아닙니다. 에서 엔드포인트 정책을 AWS 서비스 지원하지 않는 경우 서비스의 모든 엔드포인트에 대한 전체 액세스를 허용합니다. 자세한 정보는 the section called “엔드포인트 정책 지원 보기”을 참조하세요.
- AWS 서비스 이외의 엔드포인트 서비스를 위한 VPC 엔드포인트를 생성하면 엔드포인트에 대한 전체 액세스 권한이 허용됩니다.

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 AWS 서비스을 참조하십시오the section called “통합되는 서비스”. 표의 첫 번째 열에는 각 AWS PrivateLink 설명서에 대한 링크가 AWS 서비스있습니다. 에서 엔드포인트 정책을 AWS 서비스 지원하는 경우 해당 설명서에는 엔드포인트 정책 예제가 포함됩니다.

게이트웨이 엔드포인트의 보안 주체

게이트웨이 엔드포인트의 경우 `Principal` 요소를 로 설정해야 `*` 합니다. 보안 주체를 지정하려면 `aws:PrincipalArn` 조건 키를 사용합니다.

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

다음 형식으로 보안 주체를 지정하면 해당 계정의 모든 사용자와 역할이 아니라 해당 AWS 계정 루트 사용자 계정에만 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 정책을 업데이트하는 방법

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. 저장(Save)을 선택합니다.

명령줄 사용하여 엔드포인트 정책을 업데이트하는 방법

- modify-vpc-endpoint(AWS CLI)
- Edit-EC2VpcEndpoint(윈도우용 도구 PowerShell)

AWS PrivateLink의 CloudWatch 지표

AWS PrivateLink는 인터페이스 엔드포인트, 게이트웨이 로드 밸런서 엔드포인트 및 엔드포인트 서비스를 위해 Amazon CloudWatch에 데이터 포인트를 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, 게이트웨이 로드 밸런서 엔드포인트 및 엔드포인트 서비스에 대해 게시됩니다. 게이트웨이 엔드포인트에 대해서는 게시되지 않습니다. 기본적으로 AWS PrivateLink는 추가 비용 없이 1분 간격으로 CloudWatch에 지표를 전송합니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

목차

엔드포인트 지표 및 차원

`AWS/PrivateLinkEndpoints` 네임스페이스에는 인터페이스 엔드포인트와 게이트웨이 로드 밸런서 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. 통계: 가장 유용한 통계는 `Average`, `Maximum` 및 `Minimum`입니다.

지표	설명
	측정기준 • 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. 측정기준 • 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. 측정기준 • 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. 측정기준 • 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. 측정기준 • 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. 측정기준 • 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
	측정기준 • 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. 측정기준 • 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. 측정기준 • 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. 측정기준 • 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 같이 Amazon VPC 콘솔, CloudWatch 콘솔 또는 AWS CLI를 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 서비스(Endpoint services)를 선택합니다. 엔드포인트 서비스를 선택한 다음 모니터링(Monitoring) 탭을 선택합니다.

CloudWatch 콘솔을 사용하여 지표 보기

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

AWS CLI를 사용하여 지표 보기

다음 list-metrics 명령을 사용하여 인터페이스 엔드포인트 및 게이트웨이 로드 밸런서 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 PrivateLink는 지원되는 각 지표에 가장 크게 기여하는 엔드포인트를 찾을 수 있도록 엔드포인트 서비스에 대한 기본 제공 Contributor Insights 규칙을 제공합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Contributor Insights 단원을 참조하세요.

AWS PrivateLink에서는 다음 결과를 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 단원을 참조하십시오.

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

AWS Management Console 또는 AWS CLI 중 하나를 사용해 다음 절차에 따라 AWS PrivateLink에 대한 기본 제공 규칙을 활성화합니다.

콘솔을 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 활성화하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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.

AWS CLI를 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 활성화하기

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

언제든지 AWS PrivateLink에 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.

콘솔을 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 비활성화하기

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint services)를 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.

AWS CLI를 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 비활성화하기

disable-insight-rules 명령을 사용해 규칙을 비활성화합니다.

Contributor Insights 규칙 삭제

AWS Management Console 또는 AWS CLI 중 하나를 사용해 다음 절차에 따라 AWS PrivateLink에 대한 기본 제공 규칙을 삭제합니다. 규칙을 삭제하면 기여자 데이터 수집이 중단되고 기존 기여자 데이터가 삭제됩니다.

콘솔을 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 삭제하기

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 Delete(삭제)를 선택합니다.

AWS CLI를 사용해 AWS PrivateLink에 대한 Contributor Insights 규칙 삭제하기

delete-insight-rules 명령을 사용하여 규칙을 삭제합니다.

AWS PrivateLink 할당량

다음 표에는 사용자 계정 관련 각 리전의 AWS PrivateLink 리소스 할당량(이전에는 제한이라고 했던) 값이 나열되어 있습니다. 달리 명시되지 않는 한 이러한 할당량의 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

리소스별로 적용되는 할당량 증가를 요청하는 경우 리전에 있는 모든 리소스의 할당량이 증가합니다.

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.
VPC 엔드포인트 정책당 문자 수	20,480개	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 참조하십시오.

에 대한 문서 기록 AWS PrivateLink

다음 표에서는 의 릴리스에 대해 AWS PrivateLink설명합니다.

변경 사항	설명	날짜
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	내장된 Contributor Insights 규칙을 사용하여 지표에 가장 많이 기여하는 특정 엔드포인트를 식별할 수 있습니다. CloudWatch AWS PrivateLink	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 PrivateLink 인터페이스 엔드포인트, Gateway Load Balancer 엔드포인트 및 엔드포인트 서비스에 대한 CloudWatch 메트릭을 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 서비스의 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	VPC 내에서 프라이빗 DNS 이름을 사용하여 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
인터페이스 VPC 엔드포인트에 대한 AWS 서비스	인터넷 게이트웨이 또는 NAT 디바이스를 AWS PrivateLink 사용하지 않고 AWS 서비스 해당 통합에 연결할 인터페이스 엔드포인트를 생성할 수 있습니다.	2017년 11월 8일
DynamoDB에 대한 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.