Amazon Virtual Private Cloud

AWS PrivateLink

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

AWS PrivateLink 및 VPC 엔드포인트

AWS PrivateLink는 지원되는 AWS 서비스, 기타 AWS 계정에서 호스팅된 서비스(VPC 엔드포인트 서비스) 및 지원되는 AWS Marketplace 파트너 서비스에 VPC를 비공개로 연결할 수 있도록 하는 가용성과 확장성이 높은 기술입니다. 서비스와 통신하는 데 인터넷 게이트웨이, NAT 디바이스, 퍼블릭 IP 주소, AWS Direct Connect 연결 또는 AWS Site-to-Site VPN 연결을 사용하지 않아도 됩니다. 따라서 VPC가 퍼블릭 인터넷에 노출되지 않습니다.

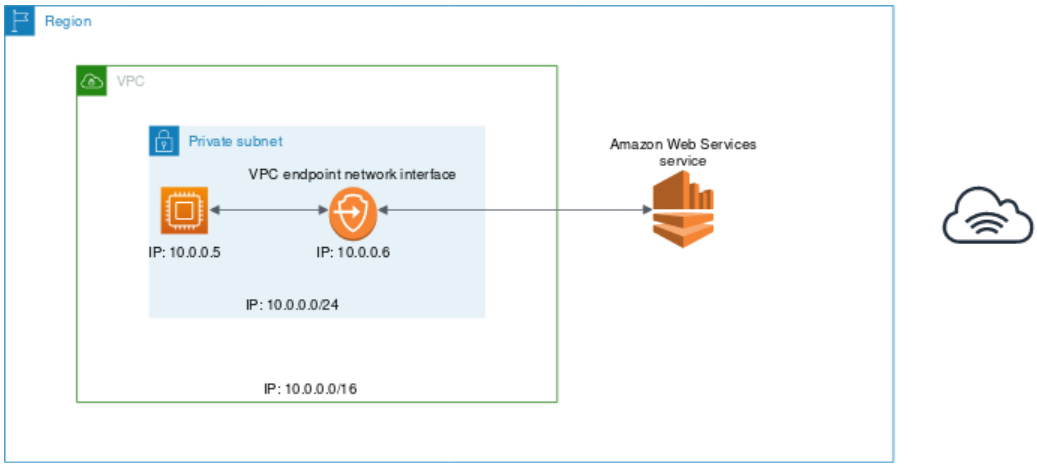
AWS PrivateLink로 구동되는 자체 VPC 엔드포인트 서비스를 생성하고 다른 AWS 고객이 해당 서비스에 액세스할 수 있도록 합니다.

VPC 엔드포인트 개념

다음은 VPC 엔드포인트의 핵심 개념입니다.

- VPC 엔드포인트 — 서비스에 프라이빗하게 연결할 수 있는 VPC의 진입점입니다. 다음은 다양한 유형의 VPC 엔드포인트입니다. 지원되는 서비스에서 요구하는 유형의 VPC 엔드포인트를 생성합니다.
  - 게이트웨이 엔드포인트 (p. 19)
  - 인터페이스 엔드포인트 (p. 3)
  - Gateway Load Balancer 엔드포인트 (p. 16)
- 엔드포인트 서비스 — VPC에 있는 자체 애플리케이션 또는 서비스입니다. 다른 AWS 보안 주체는 VPC에서 사용자의 엔드포인트 서비스로 이어지는 엔드포인트를 생성할 수 있습니다.

AWS PrivateLink를 사용하려면 VPC에 서비스에 대한 VPC 엔드포인트를 생성해야 합니다. 지원되는 서비스에서 요구하는 유형의 VPC 엔드포인트를 생성합니다. 서비스로 전달되는 트래픽에 대한 진입점 역할을 하는 프라이빗 IP 주소를 포함하여 서브넷에 탄력적 네트워크 인터페이스를 생성합니다. 다음 다이어그램에서는 VPC를 AWS PrivateLink를 지원하는 AWS 서비스에 안전하게 연결하는 기본 아키텍처를 보여 줍니다.



VPC 엔드포인트 작업

다음 중 하나를 사용하여 VPC 엔드포인트를 생성, 액세스하고 관리할 수 있습니다.

- AWS Management Console — VPC 엔드포인트에 액세스할 때 사용할 수 있는 웹 인터페이스를 제공합니다.
- AWS Command Line Interface(AWS CLI) - Amazon VPC를 포함하여 다양한 AWS 서비스에 대한 명령을 제공합니다. AWS CLI는 Windows, macOS, Linux에서 지원됩니다. 자세한 내용은 AWS Command Line Interface 섹션을 참조하세요.
- AWS SDK - 언어별 API를 제공합니다. SDK는 서명 계산, 요청 재시도 처리 및 오류 처리와 같은 많은 연결 세부 정보를 관리합니다. 자세한 정보는 AWS SDK를 참조하세요.
- 쿼리 API — HTTPS 요청을 사용하여 호출하는 하위 수준의 API 작업을 제공합니다. 쿼리 API 사용은 Amazon VPC에 액세스하는 가장 직접적인 방법입니다. 하지만 이를 사용하려면 애플리케이션에서 요청에 서명할 해시 생성 및 오류 처리와 같은 하위 수준의 세부 정보를 처리해야 합니다. 자세한 내용은 Amazon EC2 API 참조를 확인하세요.

엔드포인트 구성 예제

AWS PrivateLink 및 VPC 피어링 예제에 대한 자세한 내용은 Amazon VPC 사용 설명서에서 예제: AWS PrivateLink 및 VPC 피어링을 사용하는 서비스를 참조하세요.

엔드포인트의 요금

엔드포인트 요금에 대한 자세한 내용은 AWS PrivateLink 요금을 참조하세요.

VPC 엔드포인트

VPC 엔드포인트를 통해 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결이 필요 없이 Virtual Private Cloud(VPC)와 지원 서비스 간에 연결을 설정할 수 있습니다. 따라서 VPC가 퍼블릭 인터넷에 노출되지 않습니다.

VPC 엔드포인트는 가상 디바이스입니다. 수평으로 확장된 고가용성 중복 VPC 구성 요소입니다. 다음은 다양한 유형의 VPC 엔드포인트입니다. 지원되는 서비스에서 요구하는 유형의 VPC 엔드포인트를 생성합니다.

인터페이스 엔드포인트

인터페이스 엔드포인트 (p. 3)는 서브넷의 IP 주소 범위에서 프라이빗 IP 주소를 사용하는 탄력적 네트워크 인터페이스이며, AWS가 소유하거나 AWS 고객 또는 파트너가 소유한 서비스로 전달되는 트래픽에 대한 진입점 역할을 합니다. AWS PrivateLink와 통합하는 AWS 서비스의 목록은 AWS PrivateLink를 지원하는 서비스 (p. 67) 섹션을 참조하세요.

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

Gateway Load Balancer 엔드포인트

Gateway Load Balancer 엔드포인트 (p. 16)는 서브넷의 IP 주소 범위에서 프라이빗 IP 주소를 사용하는 탄력적 네트워크 인터페이스입니다. 트래픽을 가로채고 Gateway Load Balancer를 사용하여 구성한 네트워크 또는 보안 서비스로 라우팅하는 진입점 역할을 합니다. Gateway Load Balancer 엔드포인트를 라우팅 테이블의 경로에 대한 대상으로 지정합니다. Gateway Load Balancer 엔드포인트는 Gateway Load Balancer를 사용해 구성된 엔드포인트 서비스에서만 지원됩니다.

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

게이트웨이 엔드포인트

게이트웨이 엔드포인트 (p. 19)는 라우팅 테이블의 경로에 대한 대상인 게이트웨이로, Amazon S3 또는 DynamoDB로 전달되는 트래픽에 사용됩니다.

게이트웨이 엔드포인트 사용에 따르는 요금은 없습니다.

Amazon S3는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다. 두 선택 사항을 비교하려면 Amazon S3 사용 설명서의 Amazon S3용 VPC 엔드포인트 유형을 참조하세요.

인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트(인터페이스 엔드포인트)를 통해 AWS PrivateLink로 지원하는 서비스에 연결할 수 있습니다. 이러한 서비스에는 일부 AWS 서비스, 다른 AWS 고객 및 파트너가 자체 VPC로 호스팅한 서비스(엔드포인트 서비스라고 함) 및 지원되는 AWS Marketplace 파트너 서비스가 포함됩니다. 서비스의 소유자는 서비스 공급자이고, 인터페이스 엔드포인트를 생성하는 주체는 서비스 소비자입니다.

다음은 인터페이스 엔드포인트 설정의 일반적인 단계입니다.

1. 인터페이스 엔드포인트를 생성할 VPC를 선택하고, 연결하는 AWS 서비스, 엔드포인트 서비스 또는 AWS Marketplace 서비스의 이름을 입력합니다.
2. 인터페이스 엔드포인트를 사용할 VPC의 서브넷을 선택합니다. 서브넷에서 엔드포인트 네트워크 인터페이스가 생성됩니다. 엔드포인트 네트워크 인터페이스에는 서브넷의 IP 주소 범위에서 프라이빗 IP 주소가

할당되고 인터페이스 엔드포인트가 삭제될 때까지 이 IP 주소가 유지됩니다. 각기 다른 가용 영역(서비스에 의해 지원)에서 하나 이상의 서브넷을 지정하여 인터페이스 엔드포인트가 가용 영역 장애 발생 시 복원을 지원합니다. 이러한 경우 사용자가 지정한 각 서브넷에서 엔드포인트 네트워크 인터페이스가 생성됩니다.

Note

엔드포인트 네트워크 인터페이스는 요청자 관리형 네트워크 인터페이스입니다. 계정에서 볼 수는 있지만 직접 관리할 수는 없습니다. 자세한 내용은 요청자 관리 네트워크 인터페이스를 참조하세요.

3. 보안 그룹을 지정하여 엔드포인트 네트워크 인터페이스와 연결합니다. 보안 그룹 규칙은 VPC의 리소스로부터 엔드포인트 네트워크 인터페이스로의 트래픽을 제어합니다. 보안 그룹을 지정하지 않은 경우 VPC에 대한 기본 보안 그룹이 연결됩니다.
4. (선택 사항, AWS 서비스 및 AWS Marketplace 파트너 서비스만 해당) 엔드포인트에 대한 프라이빗 DNS (p. 4)를 활성화하면 기본 DNS 호스트 이름을 사용하여 서비스에 요청을 생성할 수 있습니다.

   Important

   프라이빗 DNS는 AWS 서비스 및 AWS Marketplace 파트너 서비스용으로 생성한 엔드포인트에 대해 기본적으로 활성화됩니다.
   프라이빗 DNS는 동일한 VPC와 가용 영역 또는 로컬 영역에 있는 다른 서브넷에서 활성화됩니다.
5. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 the section called “인터페이스 엔드포인트 가용 영역 관련 고려 사항” (p. 7)에서 인터페이스 엔드포인트 가용 영역을 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하세요.
6. 인터페이스 엔드포인트를 생성한 이후 서비스 공급자가 이를 수락하면 사용할 수 있습니다. 서비스 공급자는 서비스가 요청을 자동 또는 수동으로 수락하도록 구성해야 합니다. AWS 서비스 및 AWS Marketplace서비스는 일반적으로 모든 엔드포인트 요청을 자동적으로 수락합니다. 엔드포인트의 수명 주기에 대한 자세한 내용은 인터페이스 엔드포인트 수명 주기 (p. 7) 단원을 참조하세요.

서비스가 엔드포인트를 통한 VPC의 리소스 요청을 시작할 수 없습니다. 엔드포인트는 VPC의 리소스로부터 시작한 트래픽에 대한 응답만 반환합니다. 서비스와 엔드포인트를 통합하기 전에 서비스별 VPC 엔드포인트 설명서에서 서비스별 구성 및 제한 사항을 검토하세요.

목차

인터페이스 엔드포인트에 대한 프라이빗 DNS

Important

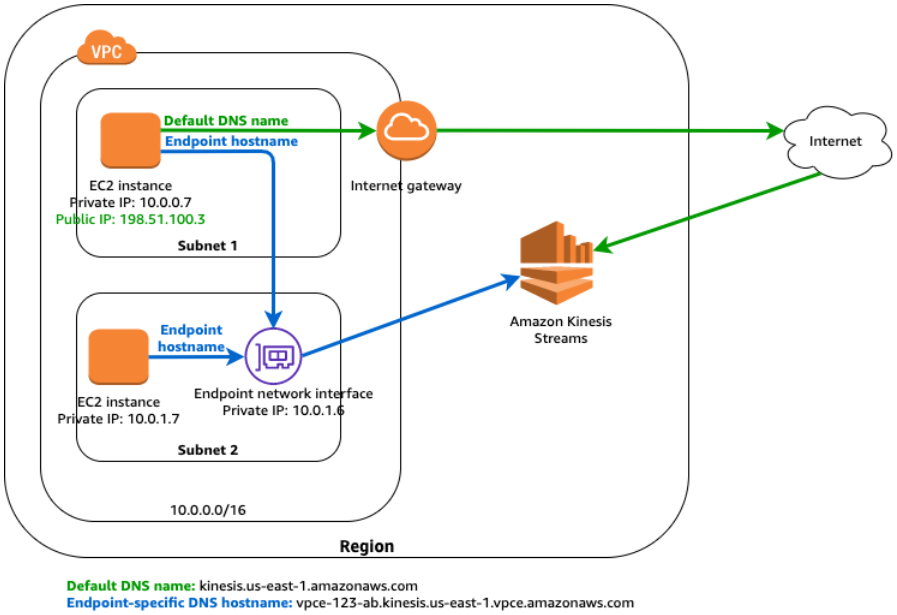
Amazon S3 인터페이스 엔드포인트에는 프라이빗 DNS가 지원되지 않습니다.

인터페이스 엔드포인트를 생성하면 서비스와의 통신에 사용할 수 있는 엔드포인트별 DNS 호스트 이름이 생성됩니다. AWS 서비스 및 AWS Marketplace 파트너 서비스의 경우, 프라이빗 DNS 옵션(기본적으로 활성화됨)은 프라이빗 호스팅 영역을 VPC와 연결합니다. 호스팅 영역에는 VPC에 있는 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소를 확인하는 서비스(예: `ec2.us-east-1.amazonaws.com`)에 대한 기본 DNS 이름의 레코드 세트가 포함됩니다. 이를 통해 엔드포인트별 DNS 호스트 이름 대신 기본 DNS 호스트 이름을 사용하여 서비스에 요청을 생성할 수 있습니다. 예를 들어 기존 애플리케이션이 AWS 서비스에 대한 요청을 생성하는 경우 구성을 변경할 필요 없이 인터페이스 엔드포인트를 통해 계속해서 요청을 생성할 수 있습니다.

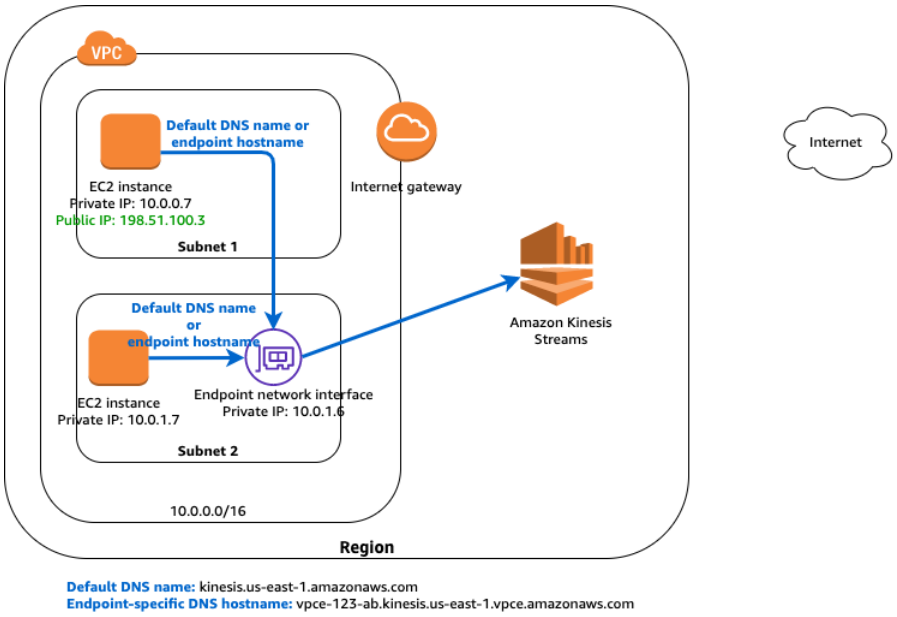
다음 다이어그램에 표시된 예에서는 Amazon Kinesis Data Streams에 대한 인터페이스 엔드포인트와 서브넷 2의 엔드포인트 네트워크 인터페이스가 있습니다. 인터페이스 엔드포인트에 대한 프라이빗 DNS가 비활성화되어 있습니다. 서브넷의 라우팅 테이블에는 다음과 같은 경로가 있습니다.

서브넷 1	
대상	대상
10.0.0.0/16	로컬
0.0.0.0/0	internet-gateway-id
서브넷 2	
대상	대상
10.0.0.0/16	로컬

두 서브넷의 인스턴스는 엔드포인트별 DNS 호스트 이름을 사용하여 인터페이스 엔드포인트를 통해 Amazon Kinesis Data Streams에 요청을 보낼 수 있습니다. 서브넷 1의 인스턴스는 기본 DNS 이름을 사용하여 AWS 리전의 퍼블릭 IP 주소 공간을 통해 Amazon Kinesis Data Streams와 통신할 수 있습니다.



다음 다이어그램에는 엔드포인트의 프라이빗 DNS가 활성화되어 있습니다. 두 서브넷의 인스턴스는 기본 DNS 호스트 이름 또는 엔드포인트별 DNS 호스트 이름을 사용하여 인터페이스 엔드포인트를 통해 Amazon Kinesis Data Streams에 요청을 보낼 수 있습니다.



Important

프라이빗 DNS를 사용하려면 다음 VPC 속성을 `true`로 설정해야 합니다. `enableDnsHostnames` 및 `enableDnsSupport`. 자세한 내용은 VPC에 대한 DNS 지원 보기 및 업데이트를 참조하세요. IAM 사용자는 호스팅 영역으로 작업할 권한이 있어야 합니다. 자세한 내용은 Route 53에 대한 인증 및 액세스 제어를 참조하세요.

인터페이스 엔드포인트 속성 및 제한

인터페이스 엔드포인트를 사용하려면 속성 및 현재 제한 사항을 알고 있어야 합니다.

- 각 인터페이스 엔드포인트에서 가용 영역당 1개의 서브넷만 선택할 수 있습니다.
- 인터페이스 엔드포인트를 통해 모든 가용 영역에서 서비스를 사용할 수 없을 수 있습니다. 지원되는 가용 영역을 확인하려면 describe-vpc-endpoint-services 명령을 사용하거나 Amazon VPC 콘솔을 사용하세요. 자세한 내용은 인터페이스 엔드포인트 생성 (p. 8) 단원을 참조하세요.
- 인터페이스 엔드포인트를 생성할 때 계정에 매핑된 가용 영역에 엔드포인트가 생성됩니다. 이 가용 영역은 다른 계정과는 별도입니다. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 the section called “인터페이스 엔드포인트 가용 영역 관련 고려 사항” (p. 7)에서 인터페이스 엔드포인트 가용 영역을 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하세요.
- 서비스 공급자와 소비자의 계정이 서로 다르며 여러 가용 영역을 사용하고 소비자가 VPC 엔드포인트 서비스 정보를 보는 경우 응답에는 공통 가용 영역만 포함됩니다. 예를 들어 서비스 공급자 계정에서 `us-east-1a` 및 `us-east-1c`를 사용하고 소비자가 `us-east-1a` 및 `us-east-1b`를 사용하는 경우 응답에는 공통 가용 영역 `us-east-1a`의 VPC 엔드포인트 서비스가 포함됩니다.
- 기본적으로 각 인터페이스 엔드포인트는 가용 영역당 최대 10Gbps의 대역폭과 최대 40Gbp의 버스트를 지원할 수 있습니다. 애플리케이션에 더 높은 버스트 또는 지속적인 처리량이 필요한 경우 AWS Support에 문의하세요.
- 서브넷에 대한 네트워크 ACL이 트래픽을 제한하는 경우 엔드포인트 네트워크 인터페이스를 통해 트래픽을 보내지 못할 수 있습니다. 서브넷의 CIDR 블록에서 주고 받는 트래픽을 허용하는 적절한 규칙을 추가해야 합니다.
- 엔드포인트 네트워크 인터페이스와 연결된 보안 그룹이 서비스와 통신하는 VPC의 리소스와 엔드포인트 네트워크 인터페이스 간의 통신을 허용하는지 확인합니다. AWS CLI 같은 명령줄 도구가 HTTPS를 통해 VPC의 리소스에서 AWS 서비스로 요청하려면 보안 그룹에서 인바운드 HTTPS(포트 443) 트래픽을 허용해야 합니다.

- 인터페이스 엔드포인트는 TCP 트래픽만을 지원합니다.
- 엔드포인트를 만들 경우, 연결하려는 서비스에 대한 액세스를 제어하는 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 자세한 내용은 정책 모범 사례 및 the section called “서비스에 대한 액세스 제어” (p. 35)를 참조하세요.
- 엔드포인트 서비스에 대한 서비스별 제한을 검토합니다.
- 참가자는 자신이 소유하지 않은 VPC에서 Amazon Route53 Resolver 엔드포인트를 생성할 수 없습니다. VPC 소유자만 인바운드 엔드포인트와 같은 VPC 수준 리소스를 생성할 수 있습니다.
- 엔드포인트는 동일한 리전에서만 지원됩니다. VPC와 다른 리전의 서비스 간에 엔드포인트를 생성할 수 없습니다.
- 엔드포인트는 IPv4 트래픽만 지원합니다.
- VPC 간에 또는 서비스 간에 엔드포인트를 전송할 수 없습니다.
- VPC당 생성할 수 있는 엔드포인트 수에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 (p. 75) 단원을 참조하세요.

온프레미스 데이터 센터 연결

인터페이스 엔드포인트와 온프레미스 데이터 센터 간 연결에 다음 유형의 연결을 사용할 수 있습니다.

- AWS Direct Connect
- AWS Site-to-Site VPN

인터페이스 엔드포인트 수명 주기

인터페이스 엔드포인트는 생성 시(엔드포인트 연결 요청)부터 다양한 단계를 거칩니다. 각 단계에서 서비스 소비자와 서비스 공급자가 수행할 수 있는 작업이 있을 수 있습니다.

다음 규칙이 적용됩니다.

- 서비스 공급자는 서비스가 인터페이스 엔드포인트 요청을 자동 또는 수동으로 수락하도록 구성할 수 있습니다. AWS 서비스 및 AWS Marketplace서비스는 일반적으로 모든 엔드포인트 요청을 자동적으로 수락합니다.
- 서비스 공급자는 서비스에 대한 인터페이스 엔드포인트를 삭제할 수 없습니다. 인터페이스 엔드포인트 연결을 요청한 서비스 소비자만이 인터페이스 엔드포인트를 삭제할 수 있습니다.
- 서비스 공급자는 인터페이스 엔드포인트를 수락(수동 또는 자동으로)한 이후에도 이를 거부할 수 있으며, `available` 상태가 됩니다.

인터페이스 엔드포인트 가용 영역 관련 고려 사항

인터페이스 엔드포인트를 생성할 때 계정에 매핑된 가용 영역에 엔드포인트가 생성됩니다. 이 가용 영역은 다른 계정과는 별도입니다. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 인터페이스 엔드포인트 가용 영역을 고유하고 지속적으로 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하세요. 예를 들어 `use1-az1`은 `us-east-1` 리전의 가용 영역 ID이고 모든 AWS 계정에서 동일한 위치에 매핑됩니다. 가용 영역 ID에 대한 자세한 정보는 AWS RAM 사용 설명서의 리소스에 대한 AZ ID를 참조하거나 describe-availability-zones를 사용하세요.

인터페이스 엔드포인트를 통해 모든 가용 영역에서 서비스를 사용할 수 없을 수 있습니다. 다음 작업 중 하나를 사용하여 서비스에 지원되는 가용 영역을 확인할 수 있습니다.

- describe-vpc-endpoint-services(AWS CLI)
- DescribeVpcEndpointServices(API)

- 인터페이스 엔드포인트를 생성할 때의 Amazon VPC 콘솔. 자세한 내용은 the section called “인터페이스 엔드포인트 생성” (p. 8) 단원을 참조하세요.

사용 가능한 AWS 서비스 이름 보기

Amazon VPC 콘솔을 사용하여 엔드포인트를 생성할 때, 사용 가능한 AWS 서비스 이름 목록을 가져올 수 있습니다.

AWS CLI를 사용하여 엔드포인트를 생성할 때 describe-vpc-endpoint-services 명령을 사용하여 서비스 이름을 확인한 다음 create-vpc-endpoint 명령을 사용하여 엔드포인트를 생성할 수 있습니다.

Console

콘솔을 사용하여 사용 가능한 AWS 서비스를 보려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]와 [Create Endpoint]를 선택합니다.
3. [Service Name] 섹션에 사용 가능한 서비스가 나열됩니다.

Command line

AWS CLI를 사용하여 사용 가능한 AWS 서비스를 보려면

- describe-vpc-endpoint-services 명령을 사용하여 연결할 수 있는 사용 가능 서비스 목록을 가져옵니다. `ServiceType` 필드는 인터페이스 또는 게이트웨이 엔드포인트를 통해 서비스에 연결할지 여부를 나타냅니다. `ServiceName` 필드는 서비스의 이름을 제공합니다. 다음 예제에서는 모든 인터페이스 엔드포인트의 이름과 소유자를 나열합니다.

```
aws ec2 describe-vpc-endpoint-services --filter "Name=service-
type,Values=Interface" --query "ServiceDetails[*].[ServiceName, Owner]" --output
 table
```

```
------------------------------------------------------------------
|                   DescribeVpcEndpointServices                  |
+--------------------------------------------------------+---------+
|  aws.sagemaker.us-west-2.notebook                      |  amazon |
|  aws.sagemaker.us-west-2.studio                        |  amazon |
|  com.amazonaws.us-west-2.access-analyzer               |  amazon |
|  com.amazonaws.us-west-2.acm-pca                       |  amazon |
...
```

AWS Tools for Windows PowerShell를 사용하여 사용 가능한 AWS 서비스를 보려면

- Get-EC2VpcEndpointService

API를 사용하여 사용 가능한 AWS 서비스를 보려면

- DescribeVpcEndpointServices

인터페이스 엔드포인트 생성

인터페이스 엔드포인트를 생성하려면 인터페이스 엔드포인트를 생성하려는 VPC 및 연결을 설정할 서비스를 지정해야 합니다.

AWS 서비스 또는 AWS Marketplace 파트너 서비스의 경우 엔드포인트에 대한 프라이빗 DNS (p. 4)를 활성화하면 기본 DNS 호스트 이름을 사용하여 서비스에 요청을 생성할 수 있습니다.

> **Important**
>
> 프라이빗 DNS는 AWS 서비스 및 AWS Marketplace 파트너 서비스용으로 생성한 엔드포인트에 대해 기본적으로 활성화됩니다.

Console

콘솔을 사용하여 AWS 서비스에 대한 인터페이스 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]와 [Create Endpoint]를 선택합니다.
3. 서비스 범주에서 AWS 서비스를 선택해야 합니다.
4. [Service Name]에서 연결할 서비스를 선택합니다. [Type]에서 [Interface]를 나타내는지 확인합니다.
5. 다음 정보를 입력한 다음 [Create endpoint]를 선택합니다.

   - VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
   - [Subnets]에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷(가용 영역)을 선택합니다.

     일부 AWS 서비스에서 지원되지 않는 가용 영역도 있습니다.
   - 인터페이스 엔드포인트에 대한 프라이빗 DNS를 활성화하려면 DNS 이름 활성화(Enable DNS Name)에서 해당 확인란을 선택합니다.

     > **Important**
     >
     > Amazon S3 인터페이스 엔드포인트에는 프라이빗 DNS가 지원되지 않습니다.

     이 옵션은 기본적으로 활성화되어 있습니다. 프라이빗 DNS 옵션을 사용하려면 VPC 속성 `true` 및 `enableDnsHostnames`를 `enableDnsSupport`로 설정해야 합니다. 자세한 내용은 VPC에 대한 DNS 지원 보기 및 업데이트를 참조하세요.
   - [Security group]에서 보안 그룹을 선택하여 엔드포인트 네트워크 인터페이스와 연결합니다.
   - (선택) 태그를 추가하거나 제거할 수 있습니다.

     태그 추가 태그 추가를 선택하고 다음을 수행합니다.
     - 키에 키 이름을 입력합니다.
     - 값에 키 값을 입력합니다.

     [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

엔드포인트 서비스에 대한 인터페이스 엔드포인트를 생성하려면 연결할 서비스의 이름을 보유해야 합니다. 서비스 공급자가 이름을 제공할 수 있습니다.

엔드포인트 서비스에 대한 인터페이스 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Endpoints, Create Endpoint를 선택합니다.
3. [Service category]에서 [Find service by name]을 선택합니다.
4. [Service Account Name]에서 서비스의 이름(예: `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`)을 입력한 다음 [Verify]를 선택합니다.
5. 다음 정보를 입력한 다음 [Create endpoint]를 선택합니다.

   - VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
   - Subnets에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷(가용 영역)을 선택합니다.

모든 가용 영역이 서비스를 지원할 수 있는 것은 아닙니다.

- Security group에서 보안 그룹을 선택하여 엔드포인트 네트워크 인터페이스와 연결합니다.
- (선택) 태그를 추가하거나 제거할 수 있습니다.

  태그 추가 태그 추가를 선택하고 다음을 수행합니다.
  - 키에 키 이름을 입력합니다.
  - 값에 키 값을 입력합니다.

  [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

AWS Marketplace 파트너 서비스에 대한 인터페이스 엔드포인트를 생성하려면

1. AWS Marketplace의 PrivateLink 페이지로 이동한 다음 서비스형 소프트웨어(SaaS) 공급자로부터 서비스를 구독합니다. 인터페이스 엔드포인트를 지원하는 서비스는 엔드포인트를 통한 연결 옵션을 포함합니다.
2. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
3. 탐색 창에서 [Endpoints]와 [Create Endpoint]를 선택합니다.
4. 서비스 범주(Service category)에서 사용자의 AWS Marketplace 서비스(Marketplace services)를 선택합니다.
5. 구독한 AWS Marketplace 서비스를 선택합니다.
6. 다음 정보를 입력한 다음 [Create endpoint]를 선택합니다.

   - VPC에서 엔드포인트를 생성할 VPC를 선택합니다.
   - Subnets에서 엔드포인트 네트워크 인터페이스를 생성할 서브넷(가용 영역)을 선택합니다.

     모든 가용 영역이 서비스를 지원할 수 있는 것은 아닙니다.
   - Security group에서 보안 그룹을 선택하여 엔드포인트 네트워크 인터페이스와 연결합니다.
   - (선택) 태그를 추가하거나 제거할 수 있습니다.

     태그 추가 태그 추가를 선택하고 다음을 수행합니다.
     - 키에 키 이름을 입력합니다.
     - 값에 키 값을 입력합니다.

     [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

Command line

AWS CLI를 사용하여 인터페이스 엔드포인트를 생성하려면

1. describe-vpc-endpoint-services 명령을 사용하여 사용 가능한 목록을 가져옵니다. 반환된 출력에 표시된 연결할 서비스의 이름을 메모해 둡니다. `ServiceType` 필드는 인터페이스 또는 게이트웨이 엔드포인트를 통해 서비스에 연결할지 여부를 나타냅니다. `ServiceName` 필드는 서비스의 이름을 제공합니다.
2. 인터페이스 엔드포인트를 생성하려면 create-vpc-endpoint 명령을 사용하고 VPC ID, VPC 엔드포인트의 유형(인터페이스), 서비스 이름, 엔드포인트를 사용할 서브넷 및 엔드포인트 네트워크 인터페이스와 연결할 보안 그룹을 지정합니다.

   다음 예제에서는 Elastic Load Balancing 서비스에 대한 인터페이스 엔드포인트를 생성합니다.

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-
abababab --security-group-id sg-1a2b3c4d
```

```
{
    "VpcEndpoint": {
        "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\",
 \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\":
 \"*\"\n    }\n  ]\n}",
        "VpcId": "vpc-ec43eb89",
        "NetworkInterfaceIds": [
            "eni-bf8aa46b"
        ],
        "SubnetIds": [
            "subnet-abababab"
        ],
        "PrivateDnsEnabled": true,
        "State": "pending",
        "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
        "RouteTableIds": [],
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "VpcEndpointId": "vpce-088d25a4bbf4a7abc",
        "VpcEndpointType": "Interface",
        "CreationTimestamp": "2017-09-05T20:14:41.240Z",
        "DnsEntries": [
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-
ks83awe7.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z1K56Z6FNPJRR",
                "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
            }
        ]
    }
}
```

또는 다음 예제에서는 다른 계정의 엔드포인트 서비스(서비스 공급자가 제공한 엔드포인트 서비스의 이름)에 대한 인터페이스 엔드포인트를 생성합니다.

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-
id subnet-abababab --security-group-id sg-1a2b3c4d
```

반환된 출력에 표시된 `privateDnsNames` 필드를 메모해 둡니다. 이 DNS 이름을 사용하여 AWS 서비스에 액세스할 수 있습니다.

AWS Tools for Windows PowerShell을 사용하여 사용 가능한 서비스를 설명하고 VPC 엔드포인트를 생성하려면

- Get-EC2VpcEndpointService
- New-EC2VpcEndpoint

API를 사용하여 사용 가능한 서비스를 설명하고 VPC 엔드포인트를 생성하려면

- DescribeVpcEndpointServices
- CreateVpcEndpoint

인터페이스 엔드포인트 보기

인터페이스 엔드포인트를 생성한 후 그에 관한 정보를 볼 수 있습니다.

Console

콘솔을 사용하여 인터페이스 엔드포인트에 대한 정보를 확인하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 인터페이스 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트에 대한 정보를 보려면 [Details]를 선택합니다. [DNS Names] 필드는 서비스 액세스에 사용할 DNS 이름을 표시합니다.
4. 인터페이스 엔드포인트가 생성된 서브넷과 각 서브넷의 엔드포인트 네트워크 인터페이스 ID를 보려면 [Subnets]를 선택합니다.
5. 엔드포인트 네트워크 인터페이스와 연결된 보안 그룹을 보려면 [Security Groups]를 선택합니다.

Command line

AWS CLI를 사용하여 인터페이스 엔드포인트를 설명하려면

- describe-vpc-endpoints 명령을 사용하여 엔드포인트를 설명할 수 있습니다.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

AWS Tools for PowerShell 또는 API를 사용하여 VPC 엔드포인트를 설명하려면

- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints(Amazon EC2 쿼리 API)

인터페이스 엔드포인트에 대한 알림 생성 및 관리

인터페이스 엔드포인트에서 발생하는 특정 이벤트에 대한 알림을 받도록 알림을 생성할 수 있습니다. 예를 들어 서비스 공급자가 인터페이스 엔드포인트를 수락할 때 이메일을 받을 수 있습니다. 알림을 생성하려면 Amazon SNS 주제를 알림에 연결해야 합니다. SNS 주제를 구독하여 엔드포인트 이벤트가 발생할 때 이메일 알림을 받을 수 있습니다.

알림에 대해 사용할 Amazon SNS 주제는 Amazon의 VPC 엔드포인트 서비스가 사용자를 대신해 알림을 게시하도록 허용하는 주제 정책을 보유해야 합니다. 주제 정책에 다음 문이 포함되어야 합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS의 Identity and Access Management를 참조하세요.

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

```
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Command line

AWS CLI를 사용하여 알림을 생성 및 관리하려면

1. 인터페이스 엔드포인트에 대한 알림을 만들려면 create-vpc-endpoint-connection-notification 명령을 사용합니다. 다음 예와 같이 SNS 주제의 ARN, 알림을 받을 이벤트 및 엔드포인트의 ID를 지정합니다.

   ```
   aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
   arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events
    Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
   ```

2. 알림을 보려면 describe-vpc-endpoint-connection-notifications 명령을 사용합니다.

   ```
   aws ec2 describe-vpc-endpoint-connection-notifications
   ```

3. 알림에 대한 SNS 주제 및 엔드포인트 이벤트를 변경하려면 modify-vpc-endpoint-connection-notification 명령을 사용합니다.

   ```
   aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-
   id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-
   arn arn:aws:sns:us-east-2:123456789012:mytopic
   ```

4. 알림을 삭제하려면 delete-vpc-endpoint-connection-notifications 명령을 사용합니다.

   ```
   aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
   ids vpce-nfn-008776de7e03f5abc
   ```

인터페이스 엔드포인트를 통해 서비스에 액세스

인터페이스 엔드포인트를 생성한 후 엔드포인트 URL을 통해 지원 서비스에 대한 요청을 제출할 수 있습니다. 다음을 사용할 수 있습니다.

- 엔드포인트(프라이빗 호스팅 영역, AWS 서비스 및 AWS Marketplace 파트너 서비스만 해당)에 대한 프라이빗 DNS를 활성화한 경우 리전에 대한 AWS 서비스의 기본 DNS 호스트 이름입니다. 예: `ec2.us-east-1.amazonaws.com`.

  Important

  Amazon S3 인터페이스 엔드포인트에는 프라이빗 DNS가 지원되지 않습니다.
- 인터페이스 엔드포인트에 대해 생성한 엔드포인트별 리전 DNS 호스트 이름. 호스트 이름은 고유한 엔드포인트 식별자, 서비스 식별자, 리전 및 `vpce.amazonaws.com`을 이름에 포함합니다. 예: `vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com`.
- 엔드포인트를 사용할 수 있는 각 가용 영역에 대해 생성한 엔드포인트별 영역 DNS 호스트 이름. 호스트 이름에는 이름의 가용 영역을 포함합니다. 예: `vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com`. 아키텍처가 가용 영역을 격리하는 경우(예를 들어 결함 제한이나 리전 데이터 전송 비용 절감 등을 위해) 이 옵션을 사용할 수 있습니다.

영역 단위 DNS 호스트 이름에 대한 요청이 서비스 공급자 계정의 해당 가용 영역 위치로 전달되는데, 사용자 계정과 가용 영역의 이름이 다를 수도 있습니다. 자세한 정보는 리전 및 가용 영역 개념을 참조하세요.

- VPC에 있는 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소.

리전 및 영역별 DNS 이름을 가져오려면 인터페이스 엔드포인트 보기 (p. 12)를 참조하세요.

예를 들어 Elastic Load Balancing에 대한 인터페이스 엔드포인트를 보유하고 프라이빗 DNS 옵션을 활성화하지 않은 서브넷에서 인스턴스로부터 다음 AWS CLI 명령을 사용하여 로드 밸런서를 설명합니다. 이 명령은 엔드포인트별 리전 DNS 호스트 이름을 사용하여 인터페이스 엔드포인트를 통해 요청을 생성합니다.

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

프라이빗 DNS 옵션을 활성화한 경우 요청에 엔드포인트 URL을 지정할 필요가 없습니다. AWS CLI는 리전의 AWS 서비스에 대해 기본 엔드포인트를 사용합니다(`elasticloadbalancing.us-east-1.amazonaws.com`).

인터페이스 엔드포인트 수정

인터페이스 엔드포인트의 다음 속성을 수정할 수 있습니다.

- 인터페이스 엔드포인트가 위치한 서브넷
- 엔드포인트 네트워크 인터페이스와 연결된 보안 그룹
- 태그
- 프라이빗 DNS 옵션

  Note

  프라이빗 DNS를 활성화하면 프라이빗 IP 주소를 사용할 수 있게 되기까지 몇 분 정도 걸릴 수 있습니다.
- 엔드포인트 정책(서비스에서 지원하는 경우)

인터페이스 엔드포인트에 대한 서브넷을 제거하면 서브넷의 해당 엔드포인트 네트워크 인터페이스가 삭제됩니다.

Console

인터페이스 엔드포인트에 대한 서브넷을 변경하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 인터페이스 엔드포인트를 선택합니다.
3. [Actions], [Manage Subnets]를 선택합니다.
4. 필요에 따라 서브넷을 선택하거나 선택 취소한 후 [Modify Subnets]를 선택합니다.

인터페이스 엔드포인트와 연결된 보안 그룹을 추가 또는 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 인터페이스 엔드포인트를 선택합니다.
3. [Actions], [Manage security groups]를 선택합니다.
4. 필요에 따라 보안 그룹을 선택하거나 선택 취소한 후 저장을 선택합니다.

인터페이스 엔드포인트 태그를 추가하거나 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 인터페이스 엔드포인트를 선택하고 작업, 태그 추가/편집을 선택합니다.
4. 태그를 추가하거나 제거합니다.

   태그 추가 태그 생성을 선택하고 다음을 수행합니다.
   - 키에 키 이름을 입력합니다.
   - 값에 키 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

프라이빗 DNS 옵션을 수정하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 인터페이스 엔드포인트를 선택합니다.
3. 작업, 프라이빗 DNS 이름 수정을 선택합니다.
4. 필요에 따라 이 옵션을 설정하고 프라이빗 DNS 이름 수정을 선택합니다.

엔드포인트 정책을 업데이트하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 인터페이스 엔드포인트를 선택합니다.
3. [Actions], [Edit policy]를 선택합니다.
4. 서비스에 대한 전체 액세스를 허용하려면 모든 액세스를 선택하고, 아니면 사용자 지정을 선택하고 사용자 지정 정책을 지정합니다. 저장(Save)을 선택합니다.

Command line

AWS CLI를 사용하여 VPC 엔드포인트를 수정하려면

1. describe-vpc-endpoints 명령을 사용하여 인터페이스 엔드포인트의 ID를 가져옵니다.

```
aws ec2 describe-vpc-endpoints
```

2. 다음 예제에서는 modify-vpc-endpoint 명령을 사용하여 서브넷 `subnet-aabb1122`를 인터페이스 엔드포인트에 추가합니다.

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-
id subnet-aabb1122
```

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트를 수정하려면

- Edit-EC2VpcEndpoint(AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint(Amazon EC2 쿼리 API)

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트 태그를 추가하거나 제거하려면

- tag-resource(AWS CLI)

- TagResource(AWS Tools for Windows PowerShell)
- untag-resource(AWS CLI)
- TagResource(AWS Tools for Windows PowerShell)

Gateway Load Balancer 엔드포인트(AWS PrivateLink)

Gateway Load Balancer 엔드포인트를 사용하면 트래픽을 가로채고 보안 검사 등을 위해 Gateway Load Balancer를 사용하여 구성한 서비스로 라우팅할 수 있습니다. 서비스의 소유자는 서비스 공급자이고, Gateway Load Balancer 엔드포인트를 생성하는 주체는 서비스 소비자입니다.

다음은 Gateway Load Balancer 엔드포인트 설정의 일반적인 단계입니다.

1. Gateway Load Balancer 엔드포인트 서비스가 구성되어 있는지 확인합니다. 자세한 내용은 Gateway Load Balancer 엔드포인트에 대한 VPC 엔드포인트 서비스 (p. 42) 단원을 참조하십시오.
2. Gateway Load Balancer 엔드포인트를 생성할 VPC를 선택하고 서비스 이름을 제공합니다.
3. VPC에서 Gateway Load Balancer 엔드포인트를 사용할 서브넷을 선택합니다. 서브넷에서 엔드포인트 네트워크 인터페이스가 생성됩니다. 엔드포인트 네트워크 인터페이스에는 서브넷의 IP 주소 범위에서 프라이빗 IP 주소가 할당되고 Gateway Load Balancer 엔드포인트가 삭제될 때까지 이 IP 주소가 유지됩니다.

   Note

   엔드포인트 네트워크 인터페이스는 요청자 관리형 네트워크 인터페이스입니다. 계정에서 볼 수는 있지만 직접 관리할 수는 없습니다. 자세한 내용은 요청자 관리 네트워크 인터페이스를 참조하십시오.
4. Gateway Load Balancer 엔드포인트를 생성한 이후 서비스 공급자가 이를 수락하면 사용할 수 있습니다. 서비스 공급자는 서비스가 인터페이스 요청을 자동 또는 수동으로 수락하도록 구성할 수 있습니다.
5. 트래픽이 Gateway Load Balancer 엔드포인트로 전달되도록 서브넷 라우팅 테이블과 게이트웨이 라우팅 테이블을 구성합니다. 자세한 내용은 Amazon VPC 사용 설명서에서 Gateway Load Balancer 엔드포인트로의 라우팅을 참조하세요.

목차

Gateway Load Balancer 엔드포인트 속성 및 제한

Gateway Load Balancer 엔드포인트를 사용하려면 다음 사항에 유의하십시오.

- 각 Gateway Load Balancer 엔드포인트에 대해 VPC에서 가용 영역(서브넷)을 하나만 선택할 수 있습니다. 나중에 서브넷을 변경할 수 없습니다. 다른 서브넷에서 Gateway Load Balancer 엔드포인트를 사용하려면 해당 서브넷에 새 Gateway Load Balancer 엔드포인트를 생성합니다. 서비스의 가용 영역당 하나의 Gateway Load Balancer 엔드포인트를 생성할 수 있지만 Gateway Load Balancer가 지원하는 가용 영역에 대해서만 생성합니다.
- 각 Gateway Load Balancer 엔드포인트는 최대 40Gbps의 최대 대역폭을 지원합니다.

- 서브넷에 대한 네트워크 ACL이 트래픽을 제한하는 경우 Gateway Load Balancer 엔드포인트를 통해 트래픽을 보내지 못할 수 있습니다. 서브넷의 CIDR 블록에서 주고 받는 트래픽을 허용하는 적절한 규칙을 추가해야 합니다.
- 보안 그룹은 지원되지 않습니다.
- 엔드포인트 정책이 지원되지 않습니다.
- Gateway Load Balancer 엔드포인트를 통해 모든 가용 영역에서 서비스를 사용할 수 없을 수 있습니다. 지원되는 가용 영역을 확인하려면 describe-vpc-endpoint-services 명령을 사용하거나 Amazon VPC 콘솔을 사용하십시오. 자세한 내용은 Gateway Load Balancer 엔드포인트 생성 (p. 17) 단원을 참조하십시오.
- Gateway Load Balancer 엔드포인트를 생성할 때 계정에 매핑된 가용 영역에 엔드포인트가 생성됩니다. 이 가용 영역은 다른 계정과는 별도입니다. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 엔드포인트 가용 영역을 고유하고 지속적으로 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하십시오. 예를 들어 `use1-az1`은 `us-east-1` 리전의 가용 영역 ID이고 모든 AWS 계정에서 동일한 위치에 매핑됩니다. 가용 영역 ID에 대한 자세한 정보는 AWS RAM 사용 설명서의 리소스에 대한 AZ ID를 참조하거나 describe-availability-zones를 사용하세요.
- 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.
- 엔드포인트는 동일한 리전에서만 지원됩니다. VPC와 다른 리전의 서비스 간에 엔드포인트를 생성할 수 없습니다.
- 엔드포인트는 IPv4 트래픽만 지원합니다.
- VPC 간에 또는 서비스 간에 엔드포인트를 전송할 수 없습니다.
- VPC당 생성할 수 있는 엔드포인트 수에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 (p. 75) 단원을 참조하십시오.

Gateway Load Balancer 엔드포인트 수명 주기

Gateway Load Balancer 엔드포인트는 생성 시(엔드포인트 연결 요청)부터 다양한 단계를 거칩니다. 각 단계에서 서비스 소비자와 서비스 공급자가 수행할 수 있는 작업이 있을 수 있습니다.

다음 규칙이 적용됩니다.

- 서비스 공급자는 서비스가 Gateway Load Balancer 엔드포인트 요청을 자동 또는 수동으로 수락하도록 구성할 수 있습니다.
- 서비스 공급자는 서비스에 대한 Gateway Load Balancer 엔드포인트를 삭제할 수 없습니다. 연결을 요청한 서비스 소비자만 Gateway Load Balancer 엔드포인트를 삭제할 수 있습니다.
- 서비스 공급자는 Gateway Load Balancer 엔드포인트를 수락한 이후에도 이를 거부할 수 있으며, `available` 상태가 됩니다.

Gateway Load Balancer 엔드포인트의 요금

서비스에 대한 Gateway Load Balancer 엔드포인트 생성 및 사용에 대한 요금이 청구됩니다. 시간당 사용 요금 및 데이터 처리 요금이 적용됩니다. 자세한 내용은 AWS PrivateLink 요금을 참조하세요. Amazon VPC 콘솔 또는 AWS CLI를 사용하여 Gateway Load Balancer 엔드포인트의 총 수를 볼 수 있습니다.

Gateway Load Balancer 엔드포인트 생성

Gateway Load Balancer 엔드포인트를 생성하려면 엔드포인트를 생성하려는 VPC 및 연결을 설정할 서비스를 지정해야 합니다.

Console

Gateway Load Balancer 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Endpoints와 Create Endpoint를 선택합니다.
3. [Service category]에서 [Find service by name]을 선택합니다.
4. 서비스 이름(Service Name)에 서비스 이름을 입력한 다음 확인(Verify)을 선택합니다.
5. 다음 정보를 입력한 다음 [Create endpoint]를 선택합니다.
   - [VPC]에서 엔드포인트를 생성할 VPC를 선택합니다.
   - 서브넷(Subnets)에서 Gateway Load Balancer 엔드포인트를 생성할 서브넷(가용 영역)을 선택합니다.
   - (선택 사항) 태그를 추가하려면 태그 추가(Add tag)를 선택한 다음 해당 태그에 대한 키와 값을 지정합니다.

Command line

AWS CLI를 사용하여 Gateway Load Balancer 엔드포인트를 생성하려면

create-vpc-endpoint 명령을 사용하여 VPC ID, VPC 엔드포인트 유형(Gateway Load Balancer), 서비스 이름 및 Gateway Load Balancer 엔드포인트를 생성할 서브넷을 지정합니다.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --vpc-id vpc-id --
subnet-ids subnet-id --service-name gateway-load-balancer-service-name
```

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트 서비스를 생성하려면

- New-EC2VpcEndpoint()
- CreateVpcEndpoint

Gateway Load Balancer 엔드포인트 보기

Gateway Load Balancer 엔드포인트를 생성한 후 그에 관한 정보를 볼 수 있습니다.

Console

콘솔을 사용하여 Gateway Load Balancer 엔드포인트에 대한 정보를 확인하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트(Endpoints)를 선택한 후 Gateway Load Balancer 엔드포인트를 선택합니다.
3. 세부 정보를 선택합니다.
4. Gateway Load Balancer 엔드포인트가 생성된 서브넷과 엔드포인트 네트워크 인터페이스 ID를 보려면 서브넷(Subnets)을 선택합니다.

Command line

명령줄 도구 또는 API를 사용하여 Gateway Load Balancer 엔드포인트를 설명하려면

- describe-vpc-endpoints(AWS CLI)

- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints(Amazon EC2 쿼리 API)

Gateway Load Balancer 엔드포인트에 대한 태그 추가 또는 제거

Gateway Load Balancer 엔드포인트에 대한 태그를 추가하거나 제거할 수 있습니다.

Console

태그를 추가하거나 제거하려면.

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Gateway Load Balancer 엔드포인트를 선택하고 작업(Actions), 태그 추가/편집(Add/Edit Tags)을 선택합니다.
4. 태그를 추가하거나 제거합니다.

   태그 추가 태그 생성을 선택하고 다음을 수행합니다.
   - 키에 키 이름을 입력합니다.
   - 값에 키 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

Command line

명령줄 도구 또는 API를 사용하여 태그를 추가하거나 제거하려면

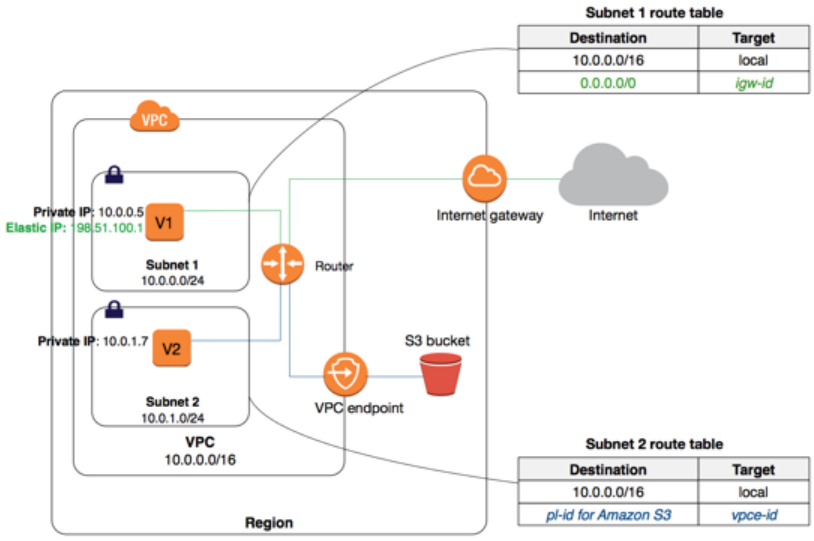
- create-tags 및 delete-tags를 사용합니다.(AWS CLI)
- New-EC2Tag 및 Remove-EC2Tag를 사용합니다.(AWS Tools for Windows PowerShell)
- CreateTags 및 DeleteTags를 사용합니다. (Amazon EC2 쿼리 API)

게이트웨이 VPC 엔드포인트

게이트웨이 엔드포인트를 생성 및 설정하려면 다음의 일반 단계를 따릅니다.

1. 엔드포인트를 만들 VPC와 여기에 연결하려는 서비스를 지정합니다. 서비스는 AWS 관리형 접두사 목록 - 즉 리전의 서비스 이름 및 ID로 식별됩니다. AWS 접두사 목록 ID는 `pl-xxxxxxx` 형식을 사용하고 AWS 접두사 목록 이름은 'com.amazonaws.*region*.*service*' 형식을 사용합니다. AWS 접두사 목록 이름(서비스 이름)을 사용하여 엔드포인트를 만듭니다.
2. 연결하려는 모든 서비스 또는 일부 서비스에 액세스를 허용하는 엔드포인트 정책을 엔드포인트에 추가합니다. 자세한 내용은 VPC 종단점 정책 사용 (p. 35) 단원을 참조하세요.
3. 서비스에 대한 경로를 생성할 하나 이상의 라우팅 테이블을 지정합니다. 라우팅 테이블은 VPC와 다른 서비스 간의 트래픽 라우팅을 제어합니다. 이러한 라우팅 테이블 중 하나와 연결된 각 서브넷은 엔드포인트에 액세스할 수 있으며, 해당 서브넷의 인스턴스에서 서비스로 전송되는 트래픽은 엔드포인트를 통해 라우팅됩니다.

다음 다이어그램에서 서브넷 2의 인스턴스는 게이트웨이 엔드포인트를 통해 Amazon S3에 액세스할 수 있습니다.



하나의 VPC에 여러 엔드포인트를 만들 수 있습니다. 예를 들어 여러 서비스에 대한 엔드포인트를 만들 수 있습니다. 또한 하나의 서비스에 대해 여러 엔드포인트를 만들 수 있고, 서로 다른 라우팅 테이블을 사용하여 동일한 서비스에 대해 서브넷별로 서로 다른 정책을 적용할 수 있습니다.

엔드포인트를 만든 후 엔드포인트에 추가한 엔드포인트 정책을 수정할 수 있고, 엔드포인트에서 사용하는 라우팅 테이블을 추가하거나 제거할 수 있습니다.

목차

게이트웨이 엔드포인트의 요금

게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다. 데이터 전송 및 리소스 사용량에 대한 표준 요금이 그대로 적용됩니다. 요금에 대한 자세한 정보는 Amazon EC2 요금을 참조하세요.

게이트웨이 엔드포인트의 라우팅

엔드포인트를 만들거나 수정할 경우 엔드포인트를 통해 서비스에 액세스할 때 사용되는 VPC 라우팅 테이블을 지정합니다. 경로는 각각의 라우팅 테이블에 자동으로 추가되며 이때 서비스의 AWS 접두사 목록 ID(`pl-xxxxxxxx`)를 지정하는 대상 주소 및 엔드포인트 ID(`vpce-xxxxxxxx`)를 포함한 대상도 함께 추가됩니다. 예를 들면 다음과 같습니다.

대상 주소	대상
10.0.0.0/16	로컬

대상 주소	대상
pl-1a2b3c4d	vpce-11bb22cc

접두사 목록 ID는 논리적으로 서비스가 사용하는 퍼블릭 IP 주소의 범위를 나타냅니다. 지정된 라우팅 테이블과 연결된 서브넷의 인스턴스는 모두 자동으로 해당 엔드포인트를 사용하여 서비스에 액세스합니다. 지정된 라우팅 테이블과 연결되지 않은 서브넷은 엔드포인트를 사용하지 않습니다. 따라서 다른 서브넷의 리소스를 엔드포인트와 분리할 수 있습니다.

서비스의 현재 퍼블릭 IP 주소 범위를 보려면 describe-prefix-lists 명령 에서 제공한 현재 IP 주소 범위 목록을 확인하세요. .

> **Note**
>
> 서비스의 퍼블릭 IP 주소의 범위는 때때로 변경될 수 있습니다. 서비스의 현재 IP 주소 범위를 기반으로 라우팅을 작성하거나 기타 결정을 내리기 전에 먼저 그 영향을 고려하세요.

다음 규칙이 적용됩니다.

- 하나의 라우팅 테이블에 서로 다른 서비스에 대한 여러 엔드포인트 라우팅을 작성할 수 있으며, 동일한 서비스에 대한 여러 엔드포인트 라우팅을 서로 다른 라우팅 테이블에 작성할 수 있습니다. 하지만 하나의 라우팅 테이블에 동일한 서비스에 대해 여러 엔드포인트 라우팅이 있을 수는 없습니다. 예를 들어 VPC에서 Amazon S3에 대한 두 개의 엔드포인트를 생성하면 동일한 라우팅 테이블에서 두 엔드포인트에 대한 엔드포인트 라우팅을 생성할 수 없습니다.
- 라우팅 테이블 API 또는 Amazon VPC 콘솔의 라우팅 테이블 페이지를 사용하여 라우팅 테이블에서 엔드포인트 라우팅을 명시적으로 추가, 수정 또는 삭제할 수 없습니다. 라우팅 테이블을 엔드포인트와 연결하는 방법으로만 엔드포인트 라우팅을 추가할 수 있습니다. 엔드포인트와 연결된 라우팅 테이블을 변경하려면 엔드포인트를 수정 (p. 34)하면 됩니다.
- 엔드포인트를 수정하여 엔드포인트에서 라우팅 테이블 연결을 제거하거나 엔드포인트를 삭제할 경우 엔드포인트 라우팅이 자동으로 삭제됩니다.

Amazon은 LPM(Longest Prefix Match)을 통해 트래픽과 일치하는 고도로 구체적인 라우팅을 사용하여 트래픽의 라우팅 방법을 결정합니다. 인터넷 게이트웨이를 가리키는 모든 인터넷 트래픽(`0.0.0.0/0`)에 대해 라우팅 테이블에 기존 라우팅이 있을 경우, 해당 서비스로 향하는 모든 트래픽에 대해 엔드포인트 라우팅이 우선합니다. 이는 서비스의 IP 주소 범위가 `0.0.0.0/0`보다 구체적이기 때문입니다. 다른 리전에 있는 서비스로 향하는 트래픽을 비롯하여 다른 모든 인터넷 트래픽은 인터넷 게이트웨이로 전송됩니다.

하지만 인터넷 게이트웨이 또는 NAT 디바이스를 가리키는 구체적인 IP 주소 범위로의 라우팅이 있을 경우 그러한 라우팅이 우선합니다. 서비스가 사용하는 IP 주소와 동일한 IP 주소 범위를 향하는 기존 라우팅이 있을 경우에는 이 라우팅이 우선합니다.

예: 라우팅 테이블의 엔드포인트 라우팅

이 시나리오에서는 라우팅 테이블에 모든 인터넷 트래픽(`0.0.0.0/0`)에 대해 인터넷 게이트웨이를 가리키는 기존의 라우팅이 있습니다. 서브넷에서 또 다른 AWS 서비스를 향하는 모든 트래픽은 인터넷 게이트웨이를 사용합니다.

대상 주소	대상
10.0.0.0/16	로컬
0.0.0.0/0	igw-1a2b3c4d

지원되는 AWS에 대한 엔드포인트를 만든 후 라우팅 테이블을 엔드포인트와 연결할 수 있습니다. 엔드포인트 라우팅은 대상 주소 `pl-1a2b3c4d`(엔드포인트를 만든 서비스를 나타내는 것으로 가정)와 함께 라우팅 테이블에 자동으로 추가됩니다. 이제 같은 리전에서 해당 AWS 서비스를 향하는 서브넷의 모든 트래픽은 인터

넷 게이트웨이가 아닌 엔드포인트로 전송됩니다. 다른 서비스로 향하는 트래픽 및 다른 리전에서 AWS 서비스로 향하는 트래픽을 포함하여 다른 모든 인터넷 트래픽은 인터넷 게이트웨이로 전송됩니다.

대상 주소	대상
10.0.0.0/16	로컬
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

예: 엔드포인트에 대한 라우팅 테이블 조정

이 시나리오에서 `54.123.165.0/24`는 Amazon S3 IP 주소 범위에 있으며 서브넷의 인스턴스가 인터넷 게이트웨이를 통해 Amazon S3 버킷과 통신할 수 있도록 라우팅 테이블을 구성했습니다. `54.123.165.0/24`를 대상으로, 인터넷 게이트웨이를 대상으로 하는 라우팅을 추가했습니다. 이제 엔드포인트를 만든 후 이 라우팅 테이블을 엔드포인트와 연결합니다. 엔드포인트 라우팅은 자동으로 라우팅 테이블에 추가됩니다. 그런 다음 describe-prefix-lists 명령을 사용하여 Amazon S3의 IP 주소 범위를 확인합니다. 범위는 `54.123.160.0/19`이며, 이는 인터넷 게이트웨이를 가리키는 범위보다 구체적이지 않습니다. 따라서 `54.123.165.0/24` IP 주소 범위를 향하는 모든 트래픽은 Amazon S3의 퍼블릭 IP 주소 범위를 유지하는 동안은 인터넷 게이트웨이를 계속 사용하고 엔드포인트를 사용하지 않습니다.

대상 주소	대상
10.0.0.0/16	로컬
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

같은 리전에서 Amazon S3를 향하는 모든 트래픽이 엔드포인트를 통해 라우팅되게 하려면 라우팅 테이블의 라우팅을 조정해야 합니다. 이렇게 하려면 인터넷 게이트웨이에 대한 라우팅을 삭제하면 됩니다. 그러면 같은 리전에서 Amazon S3를 향하는 모든 트래픽은 엔드포인트를 사용하고, 라우팅 테이블과 연결된 서브넷은 프라이빗 서브넷이 됩니다.

대상 주소	대상
10.0.0.0/16	로컬
pl-1a2b3c4d	vpce-11bb22cc

게이트웨이 엔드포인트 제한

게이트웨이 엔드포인트를 사용하려면 현재 제한 사항을 알고 있어야 합니다.

- 엔드포인트에 지정된 서비스에 대한 아웃바운드 트래픽을 허용하거나 거부하기 위해 네트워크 ACL의 아웃바운드 규칙에 AWS 접두사 목록 ID를 사용할 수 없습니다. 네트워크 ACL 규칙이 트래픽을 제한하는 경우 서비스에 대한 CIDR 블록(IP 주소 범위)을 대신 지정해야 합니다. 하지만 아웃바운드 보안 그룹 규칙에는 AWS 접두사 목록 ID를 사용할 수 있습니다. 자세한 내용은 보안 그룹 (p. 36) 단원을 참조하세요.
- 엔드포인트는 동일한 리전에서만 지원됩니다. VPC와 다른 리전의 서비스 간에 엔드포인트를 생성할 수 없습니다.
- 엔드포인트는 IPv4 트래픽만 지원합니다.
- VPC 간에 또는 서비스 간에 엔드포인트를 전송할 수 없습니다.

- VPC당 생성할 수 있는 엔드포인트 수에는 할당량이 있습니다. 자세한 내용은 AWS PrivateLink 할당량 (p. 75) 단원을 참조하세요.
- 엔드포인트 연결은 VPC 외부로 확장할 수 없습니다. VPN 연결, VPC 피어링 연결, 전송 게이트웨이, AWS Direct Connect 연결 또는 VPC의 ClassicLink 연결의 반대쪽에 있는 리소스는 엔드포인트를 사용하여 엔드포인트 서비스의 리소스와 통신할 수 없습니다.
- VPC에서 DNS 확인을 활성화해야 합니다. 또는 자체 DNS 서버를 사용 중인 경우, 필요한 서비스(예: Amazon S3)에 대한 DNS 요청이 AWS에서 유지 관리하는 IP 주소로 제대로 확인되어야 합니다. 자세한 내용은 Amazon VPC 사용 설명서에서 VPC와 함께 DNS 사용 및 Amazon Web Services 일반 참조에서 AWS IP 주소 범위를 참조하세요.
- 엔드포인트 서비스에 대한 서비스별 제한을 검토합니다.

Amazon S3와 관련된 규칙 및 제한에 대한 자세한 내용은 Amazon S3용 엔드포인트 (p. 23)를 참조하세요.

DynamoDB와 관련된 규칙 및 제한에 대한 자세한 내용은 Amazon DynamoDB용 엔드포인트 (p. 29)를 참조하세요.

Amazon S3용 엔드포인트

VPC에서 Amazon S3 리소스로의 액세스를 이미 설정한 경우, 엔드포인트를 설정한 후에도 Amazon S3 DNS 이름을 사용하여 이러한 리소스에 액세스할 수 있습니다. 하지만 다음에 유의하세요.

- 엔드포인트에는 Amazon S3 리소스에 액세스하기 위한 엔드포인트 사용을 제어하는 정책이 있습니다. 기본 정책은 VPC 내의 모든 사용자 또는 서비스가 자격 증명을 사용하여 아무 AWS 계정에서 아무 Amazon S3 리소스에 액세스할 수 있도록 허용합니다. VPC가 연결된 계정이 아닌 다른 AWS 계정에 대한 Amazon S3 리소스도 마찬가지입니다. 자세한 내용은 VPC 종단점으로 서비스에 대한 액세스 제어 (p. 35) 단원을 참조하세요.
- Amazon S3가 수신한 해당 서브넷에 있는 인스턴스의 원본 IPv4 주소는 VPC의 퍼블릭 IPv4 주소에서 프라이빗 IPv4 주소로 변경됩니다. 엔드포인트는 네트워크 라우팅을 스위칭하고 열린 TCP 연결을 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.
- IAM 정책 또는 버킷 정책을 사용하여 VPC IPv4 CIDR 범위(프라이빗 IPv4 주소 범위)로부터의 액세스를 허용할 수 없습니다. VPC CIDR 블록이 중첩되거나 동일할 수 있고 이로 인해 예기치 않은 결과가 발생할 수 있습니다. 따라서 VPC 엔드포인트를 통해 Amazon S3에 요청할 때는 IAM 정책에 `aws:SourceIp` 조건을 사용할 수 없습니다. 사용자 및 역할의 IAM 정책과 모든 버킷 정책에도 같은 사항이 적용됩니다. 문에 `aws:SourceIp` 조건이 포함되어 있는 경우, 값이 제공된 IP 주소 또는 범위와 일치하지 않습니다. 대신에 다음 작업을 할 수 있습니다.
  - 라우팅 테이블을 사용하여 엔드포인트를 통해 Amazon S3의 리소스에 액세스할 수 있는 인스턴스를 제어할 수 있습니다.
  - 버킷 정책의 경우 특정 엔드포인트 또는 특정 VPC에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 Amazon S3 버킷 정책 (p. 27) 단원을 참조하세요.
- 현재 엔드포인트는 교차 리전 요청을 지원하지 않습니다. 버킷과 같은 리전에 엔드포인트를 생성하는지 확인하세요. Amazon S3 콘솔 또는 get-bucket-location 명령을 사용하여 버킷의 위치를 확인할 수 있습니다. 리전별 Amazon S3 엔드포인트를 사용하여 버킷에 액세스하세요(예: `mybucket.s3.us-west-2.amazonaws.com`). Amazon S3의 리전별 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon Simple Storage Service(S3)를 참조하세요. AWS CLI를 사용하여 Amazon S3에 요청할 경우, 기본 리전을 버킷과 동일한 리전으로 설정하거나 요청에 `--region` 파라미터를 사용하세요.

  Note

  Amazon S3의 미국 표준 리전이 `us-east-1` 리전에 매핑된 것으로 간주합니다.
- 엔드포인트는 현재 IPv4 트래픽에 대해서만 지원됩니다.

Amazon S3에서 엔드포인트를 사용하기 전에 게이트웨이 엔드포인트 제한 (p. 22)에 있는 일반 제한 사항을 읽으세요. S3 버킷 생성 및 확인에 관한 자세한 내용은 Amazon Simple Storage Service Console 사용 설명서의 S3 버킷을 생성하려면 어떻게 해야 하나요 및 S3 버킷의 속성을 보려면 어떻게 해야 하나요를 참조하세요.

VPC에서 다른 AWS 서비스를 사용할 경우, 이 서비스에서 특정 태스크에 S3 버킷을 사용할 수도 있습니다. 엔드포인트 정책이 Amazon S3에 대한 모든 액세스를 허용하도록 하거나(기본 정책), 이 서비스에서 사용하는 특정 버킷에 대한 액세스를 허용해야 합니다. 또는 이러한 서비스 중 어느 서비스도 사용하지 않는 서브넷에 엔드포인트를 만들어서 서비스가 퍼블릭 IP 주소를 사용하여 S3 버킷에 계속 액세스하도록 허용합니다.

다음 표에는 엔드포인트의 영향을 받을 수 있는 AWS 서비스와 각 서비스에 대한 특정 정보가 나와 있습니다.

AWS 서비스	참고
Amazon AppStream 2.0	엔드포인트 정책이 사용자 콘텐츠를 저장할 수 있도록 AppStream 2.0이 사용하는 특정 버킷에 대한 액세스를 허용해야 합니다. 자세한 내용은 Amazon AppStream 2.0 관리 안내서의 홈 폴더 및 애플리케이션 설정 지속성을 위한 Amazon S3 VPC 엔드포인트 사용을 참조하세요.
AWS CloudFormation	VPC에 대기 조건 또는 사용자 지정 리소스에 응답해야 하는 리소스가 있을 경우, 엔드포인트 정책은 최소한 이러한 리소스가 사용하는 특정 버킷에 대해 액세스를 허용해야 합니다. 자세한 내용은 AWS CloudFormation에 대한 VPC 엔드포인트 설정을 참조하세요.
CodeDeploy	엔드포인트 정책이 Amazon S3에 대한 모든 액세스를 허용하거나, CodeDeploy 배포를 위해 만든 S3 버킷에 대한 액세스를 허용해야 합니다.
Elastic Beanstalk	엔드포인트 정책이 최소한 Elastic Beanstalk 애플리케이션에 사용하는 S3 버킷에 대한 액세스는 허용해야 합니다. 자세한 내용은 AWS Elastic Beanstalk 개발자 안내서의 Amazon S3와 함께 Elastic Beanstalk 사용을 참조하세요.
Amazon EMR	엔드포인트 정책은 Amazon EMR에서 사용하는 Amazon Linux 리포지토리 및 기타 버킷에 대한 액세스를 허용해야 합니다. 자세한 내용은 Amazon EMR 관리 안내서의 프라이빗 서브넷에 대한 최소 Amazon S3 정책을 참조하세요.
AWS OpsWorks	엔드포인트 정책이 최소한 가 사용하는 특정 버킷에 대해 액세스를 허용해야 합니다AWS OpsWorks 자세한 내용은 AWS OpsWorks 사용 설명서의 VPC에서 스택 실행을 참조하세요.
AWS Systems Manager	AWS 리전의 패치 기준선 작업을 위해, 엔드포인트 정책이 패치 관리자가 사용하는 Amazon S3 버킷에 대한 액세스를 허용해야 합니다. 이 버킷에는 패치 기준선 서비스가 가져와 인스턴스에서 실행하는 코드가 포함되어 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 Virtual Private Cloud 엔드포인트 생성을 참조하세요.

AWS 서비스	참고
	이 작업의 SSM Agent에 필요한 S3 버킷 권한 목록은 AWS Systems Manager 사용 설명서의 SSM 에이전트를 위한 최소 S3 버킷 권한 섹션을 참조하세요.
Amazon Elastic 컨테이너 레지스트리	엔드포인트 정책이 Amazon ECR이 Docker 이미지 레이어를 저장하는 데 사용하는 Amazon S3 버킷에 대한 액세스를 허용해야 합니다. 자세한 내용은 Amazon Elastic Container Registry 사용 설명서의 Amazon ECR을 위한 최소 Amazon S3 버킷 권한을 참조하세요.
Amazon WorkDocs	Workspaces의 Amazon WorkDocs 클라이언트나 EC2 인스턴스를 사용하는 경우, 엔드포인트 정책은 Amazon S3에 대한 모든 액세스를 허용해야 합니다.
WorkSpaces	WorkSpaces는 Amazon S3에 직접적으로 구애받지 않습니다. 하지만 WorkSpaces 사용자에게 인터넷 액세스를 제공한 경우 다른 회사의 웹 사이트, HTML 이메일 및 인터넷 서비스가 Amazon S3를 의존할 수는 있습니다. 이러한 서비스가 올바르게 작동하려면 엔드포인트 정책이 Amazon S3에 대한 모든 액세스를 허용해야 합니다.

VPC 및 S3 버킷 간 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

Amazon S3에 대한 엔드포인트 정책

다음은 Amazon S3에 액세스하기 위한 엔드포인트 정책의 예입니다. 자세한 내용은 VPC 종단점 정책 사용 (p. 35) 단원을 참조하세요. 비즈니스 요구를 충족하는 정책 제한은 사용자가 결정합니다.

> **Important**
>
> IAM 사용자 정책, 엔드포인트 정책, S3 버킷 정책 및 Amazon S3 ACL 정책(있는 경우)을 비롯한 모든 유형의 정책은 Amazon S3에 액세스하기 위해 필요한 권한을 부여해야 합니다.
> AWS는 엔드포인트의 특정 호출자의 사용을 제한하는 경우 VPC 엔드포인트 정책에서 IAM `Principal` 요소 대신, IAM 조건을 사용하도록 권장합니다. 이러한 조건의 예로는 `aws:PrincipalArn`, `aws:PrincipalAccount`, `aws:PrincipalOrgId`, `aws:PrincipalOrgPaths`가 있습니다. 글로벌 조건 컨텍스트 키에 대한 자세한 내용은 AWS Identity and Access Management IAM 사용 설명서의 AWS 글로벌 조건 컨텍스트 키를 참조하세요.

Example 예: 특정 버킷에 대한 액세스 제한

특정 S3 버킷에 대해서만 액세스를 제한하는 정책을 만들 수 있습니다. 이는 VPC에 S3 버킷을 사용하는 다른 AWS 서비스가 있을 경우 유용합니다. 다음은 지정된 버킷에 대해서만 액세스를 제한하는 정책의 예입니다.

```
{
  "Effect": "Allow",
  "Action": [
     "s3:ListBucket",
     "s3:GetObject",
     "s3:PutObject"
  ],
  "Resource": [
     "arn:aws:s3:::example-bucket",
     "arn:aws:s3:::example-bucket/*"
```

```
  ]
}
```

Example 예: 이 VPC 종단점을 계정의 특정 IAM 역할만 사용하도록 제한

VPC 종단점을 특정 IAM 역할만 사용하도록 제한하는 정책을 생성할 수 있습니다. 다음은 지정된 계정의 지정된 역할로 액세스를 제한하는 예입니다.

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 예: 이 VPC 종단점을 특정 계정의 사용자만 사용하도록 제한

VPC 종단점을 특정 계정만 사용하도록 제한하는 정책을 생성할 수 있습니다. 다음은 지정된 계정의 사용자로 액세스를 제한하는 예입니다.

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

Example 예: Amazon Linux AMI 리포지토리 액세스 활성화

Amazon Linux AMI 리포지토리는 각 리전의 Amazon S3 버킷입니다. VPC의 인스턴스가 엔드포인트를 통해 리포지토리에 액세스하도록 하려면 이러한 버킷에 액세스하게 하는 엔드포인트 정책을 만들 수 있습니다.

다음 정책은 사용자가 Amazon Linux 리포지토리에 읽기 전용 액세스를 할 수 있도록 허용합니다.

`region`을 해당 AWS 리전 us-east-1로 대체해야 합니다.

```
{
  "Statement": [
    {
      "Sid": "AmazonLinuxAMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*"
      ]
```

```
    }
  ]
}
```

다음 정책은 사용자가 Amazon Linux 2 리포지토리에 읽기 전용 액세스를 할 수 있도록 허용합니다.

`region`을 해당 AWS 리전 us-east-1로 대체해야 합니다.

```
{
  "Statement": [
    {
      "Sid": "AmazonLinux2AMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*"
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
}
```

Amazon S3 버킷 정책

버킷 정책을 사용하여 특정 엔드포인트, VPC, IP 주소 범위 또는 AWS 계정의 버킷에 대한 액세스를 제어할 수 있습니다.

VPC 엔드포인트를 통해서 Amazon S3에 요청할 때는 버킷 정책에 `aws:SourceIp` 조건을 사용할 수 없습니다. 조건이 지정된 IP 주소 또는 IP 주소 범위와 일치하지 않으므로 Amazon S3 버킷에 요청 시 원하지 않는 결과가 나타날 수 있습니다. 다음 예를 참조하세요.

- 버킷 정책에 `Deny` 결과와 하나 또는 제한된 범위의 IP 주소에서의 액세스만 허용하는 `NotIpAddress` 조건이 있습니다. 엔드포인트를 통해 버킷에 요청하는 경우, `NotIpAddress` 조건이 항상 일치되므로 문의 결과가 적용됩니다(정책의 다른 제약이 일치한다고 가정). 버킷에 대한 액세스는 거부됩니다.
- 버킷 정책에 `Deny` 결과와 하나 또는 제한된 범위의 IP 주소에 대해서만 액세스를 거부하는 `IpAddress` 조건이 포함되어 있습니다. 엔드포인트를 통해 버킷에 요청하는 경우, 조건이 일치되지 않으므로 문이 적용되지 않습니다. `IpAddress` 조건 없이 액세스를 허용하는 다른 문이 있다고 가정하면 버킷에 대한 액세스가 허용됩니다.

대신 `aws:VpcSourceIp`를 사용하여 특정 IP 주소 범위의 액세스를 제어합니다.

IAM 사용자가 버킷 정책을 사용할 수 있도록 하려면 `s3:GetBucketPolicy` 및 `s3:PutBucketPolicy` 작업을 사용할 권한을 그 사용자에게 부여해야 합니다.

Amazon S3의 버킷 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 정책 및 사용자 정책 사용을 참조하세요.

Example 예: 특정 엔드포인트에 대한 액세스 제한

`aws:sourceVpce` 조건을 사용하여 특정 엔드포인트에 대한 액세스를 제한하는 버킷 정책을 만들 수 있습니다. 다음은 엔드포인트 `vpce-1a2b3c4d`의 버킷인 `example_bucket`에 대해서 액세스를 허용하는 S3 버킷 정책의 예입니다. 이 정책은 지정된 엔드포인트가 사용되지 않으면 버킷에 대한 모든 액세스를 거부합니다. `aws:sourceVpce` 조건은 VPC 엔드포인트 리소스에 대한 ARN을 요구하지 않고 엔드포인트 ID만 요구합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example 예: 특정 VPC에 대한 액세스 제한

`aws:sourceVpc` 조건을 사용하여 특정 VPC에 대한 액세스를 제한하는 버킷 정책을 만들 수 있습니다. 이는 같은 VPC에 여러 엔드포인트가 구성되어 있으며, 모든 엔드포인트의 S3 버킷에 대한 액세스를 관리하려는 경우에 유용합니다. 다음은 VPC `vpc-111bbb22`가 `example_bucket`과 해당 객체에 액세스할 수 있도록 허용하는 정책의 예입니다. 이 정책은 지정된 VPC가 사용되지 않으면 버킷에 대한 모든 액세스를 거부합니다. `aws:sourceVpc` 조건은 VPC 리소스의 ARN을 요구하지 않고 VPC ID만 요구합니다.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "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:VpcSourceIp` 조건을 사용하여 특정 IP 주소 범위에 대한 액세스를 제한하는 버킷 정책을 만들 수 있습니다. 다음은 `172.31.0.0/16`에서 `example_bucket` 및 해당 객체에 액세스할 수 있도록 허용하는 정책의 예입니다. 이 정책은 다른 IP 주소 범위로부터 버킷에 대한 액세스를 거부합니다.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-CIDR-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
```

```
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example 예: 특정 AWS 계정의 버킷에 대한 액세스 제한

`s3:ResourceAccount` 조건을 사용하여 특정 AWS 계정의 S3 버킷에 대한 액세스를 제한하는 만들 수 있습니다. 이 정책은 VPC 내의 클라이언트가 자신이 소유하지 않은 버킷에 액세스하지 못하도록 제한하려는 경우에 유용합니다. 다음은 계정 ID가 `111122223333`인 단일 AWS 계정이 소유한 리소스에 대한 액세스를 제한하는 정책의 예입니다.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Amazon DynamoDB용 엔드포인트

VPC에서 DynamoDB 테이블로의 액세스를 이미 설정한 경우, 게이트웨이 엔드포인트를 설정한 후에도 보통 때처럼 테이블에 계속 액세스할 수 있습니다. 하지만 다음에 유의하세요.

- 엔드포인트에는 엔드포인트를 이용한 DynamoDB 리소스 액세스를 제어하는 정책이 있습니다. 기본 정책은 VPC 내 모든 사용자 또는 서비스가 자격 증명을 사용하여 아무 AWS 계정에서 아무 DynamoDB 리소스에 액세스할 수 있게 합니다. 자세한 내용은 VPC 종단점으로 서비스에 대한 액세스 제어 (p. 35) 단원을 참조하세요.
- DynamoDB는 (테이블 등에 대한) 리소스 기반 정책을 지원하지 않습니다. DynamoDB 액세스는 개별 IAM 사용자 및 역할에 대한 엔드포인트 정책 및 IAM 정책을 통해 제어됩니다.
- 현재 엔드포인트는 교차 리전 요청을 지원하지 않습니다. DynamoDB 테이블과 같은 리전에 엔드포인트를 생성하는지 확인하세요.
- AWS CloudTrail을 사용하여 DynamoDB 작업을 기록할 경우 로그 파일에는 VPC에 있는 EC2 인스턴스의 프라이빗 IP 주소와 엔드포인트를 통해 수행된 모든 작업에 대한 엔드포인트 ID가 포함되어 있습니다.
- 해당 서브넷에 있는 인스턴스의 원본 IPv4 주소는 VPC의 퍼블릭 IPv4 주소에서 프라이빗 IPv4 주소로 변경됩니다. 엔드포인트는 네트워크 라우팅을 스위칭하고 열린 TCP 연결을 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 DynamoDB에 다시 연결할 수 있는지 테스트해야 합니다.

DynamoDB에서 엔드포인트를 사용하기 전에 게이트웨이 엔드포인트 제한 (p. 22)에 있는 일반 제한 사항을 읽으세요.

게이트웨이 VPC 엔드포인트 생성에 대한 자세한 내용은 게이트웨이 VPC 엔드포인트 (p. 19)를 참조하세요.

DynamoDB에 대한 엔드포인트 정책

엔드포인트 정책은 연결 중인 일부 또는 모든 서비스에 액세스할 수 있도록 엔드포인트에 연결하는 IAM 정책입니다. 다음은 DynamoDB에 액세스하기 위한 엔드포인트 정책의 예입니다.

> **Important**
>
> IAM 사용자 정책, 엔드포인트 정책 같은 모든 유형의 정책은 DynamoDB에 액세스하기 위해 필요한 권한을 부여해야 합니다.

Example 예: 읽기 전용 액세스

VPC 엔드포인트를 통한 DynamoDB 테이블 나열 및 설명으로만 작업을 제한하는 정책을 만들 수 있습니다.

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

Example 예: 특정 테이블에 대한 액세스 제한

특정 DynamoDB 테이블에 대한 액세스를 제한하는 정책을 만들 수 있습니다. 이 예의 엔드포인트 정책은 `StockTable`에 대해서만 액세스를 허용합니다.

```
{
  "Statement": [
    {
      "Sid": "AccessToSpecificTable",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"
    }
  ]
}
```

IAM 정책을 사용하여 DynamoDB에 대한 액세스 제어

IAM 사용자, 그룹 또는 역할이 특정 VPC 엔드포인트에서만 DynamoDB 테이블에 액세스하도록 제한하는 IAM 정책을 만들 수 있습니다. 이렇게 하려면 IAM 정책에서 테이블 리소스에 대한 `aws:sourceVpce` 조건 키를 사용해야 합니다.

DynamoDB에 대한 액세스를 관리하는 방법에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 Amazon DynamoDB에 대한 인증 및 액세스 제어를 참조하세요.

Example 예: 특정 엔드포인트에서의 액세스 제한

이 예에서는 엔드포인트 `vpce-11aa22bb`를 통해 액세스하는 경우를 제외하고 사용자의 DynamoDB 테이블 사용 권한이 거부됩니다.

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

Example 예: 이 VPC 종단점을 계정의 특정 IAM 역할만 사용하도록 제한

VPC 종단점을 특정 IAM 역할만 사용하도록 제한하는 정책을 생성할 수 있습니다. 다음은 `SomeRole` 계정의 `111122223333`로 액세스를 제한하는 예입니다.

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 예: 이 VPC 종단점을 특정 계정의 사용자만 사용하도록 제한

VPC 종단점을 특정 계정만 사용하도록 제한하는 정책을 생성할 수 있습니다. 다음은 `111122223333` 계정의 사용자로 액세스를 제한하는 예입니다.

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
```

```
    }
}
```

게이트웨이 엔드포인트 생성

엔드포인트를 만들려면 엔드포인트를 만들려는 VPC 및 연결을 설정할 서비스를 지정해야 합니다.

콘솔을 사용하여 게이트웨이 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]와 [Create Endpoint]를 선택합니다.
3. [Service Name]에서 연결할 서비스를 선택합니다. DynamoDB 또는 Amazon S3에 대한 게이트웨이 엔드포인트를 생성하려면 유형 열이 게이트웨이여야 합니다.
4. 다음 정보를 입력한 다음 [Create endpoint]를 선택합니다.
   - [VPC]에서 엔드포인트를 생성할 VPC를 선택합니다.
   - [Configure route tables]에서 엔드포인트에서 사용할 라우팅 테이블을 선택합니다. 엔드포인트, 선택한 라우팅 테이블에 대한 서비스를 향하는 트래픽을 가리키는 경로가 자동으로 추가됩니다.
   - [Policy]에서 정책의 유형을 선택합니다. 기본 옵션인 [Full Access]를 그대로 사용하여 서비스에 대한 모든 액세스를 허용합니다. 또는 사용자 지정을 선택한 후 AWS 정책 생성기를 사용하여 사용자 지정 정책을 만들거나, 정책 창에서 직접 정책을 입력할 수도 있습니다.
   - (선택) 태그를 추가하거나 제거할 수 있습니다.

     태그 추가 태그 추가를 선택하고 다음을 수행합니다.
     - 키에 키 이름을 입력합니다.
     - 값에 키 값을 입력합니다.

     [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

엔드포인트를 생성한 후 그에 관한 정보를 볼 수 있습니다.

콘솔을 사용하여 게이트웨이 엔드포인트에 대한 정보를 확인하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 엔드포인트를 선택합니다.
3. 엔드포인트에 대한 정보를 보려면 [Summary]를 선택합니다. [서비스(Service)] 상자에서 서비스에 대한 AWS 접두사 목록 이름을 가져올 수 있습니다.
4. 엔드포인트가 사용하는 라우팅 테이블에 대한 정보를 보려면 [Route Tables]를 선택합니다.
5. 엔드포인트에 연결된 IAM 정책을 보려면 정책을 선택합니다.

   Note

   [Policy] 탭에는 엔드포인트 정책만 표시됩니다. 엔드포인트 작업 권한이 있는 IAM 사용자의 IAM 정책 관련 정보는 표시되지 않습니다. 또한 S3 버킷 정책과 같은 서비스별 정책도 표시되지 않습니다.

AWS CLI를 사용하여 엔드포인트를 생성하고 보려면

1. describe-vpc-endpoint-services 명령을 사용하여 사용 가능한 목록을 가져옵니다. 반환된 출력에 표시된 연결하고자 하는 서비스의 이름을 메모해 둡니다. `serviceType` 필드는 인터페이스 엔드포인트 또는 게이트웨이 엔드포인트를 통해 서비스에 연결할지 여부를 나타냅니다.

```
aws ec2 describe-vpc-endpoint-services
```

```
{
    "serviceDetailSet": [
        {
            "serviceType": [
                {
                    "serviceType": "Gateway"
                }
            ...
```

2. 게이트웨이 엔드포인트(예: Amazon S3에 대한 엔드포인트)를 생성하려면 create-vpc-endpoint 명령을 사용하고 VPC ID, 서비스 이름, 엔드포인트를 사용할 라우팅 테이블을 지정합니다. 선택적으로 `--policy-document` 파라미터를 사용하여 서비스 액세스를 제어할 사용자 지정 정책을 지정할 수 있습니다. 파라미터를 사용하지 않는 경우 서비스에 대한 전체 액세스를 허용하는 기본 정책이 연결됩니다.

   Amazon S3의 경우 `--vpc-endpoint-type` 파라미터를 `Gateway`로 설정해야 합니다.

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-east-1.s3 --route-table-ids rtb-11aa22bb --vpc-endpoint-type Gateway
```

3. describe-vpc-endpoints 명령을 사용하여 엔드포인트를 설명합니다.

```
aws ec2 describe-vpc-endpoints
```

AWS Tools for Windows PowerShell 또는 API를 사용하여 사용 가능한 서비스를 설명하려면

- Get-EC2VpcEndpointService(AWS Tools for Windows PowerShell)
- DescribeVpcEndpointServices(Amazon EC2 쿼리 API)

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트 서비스를 생성하려면

- New-EC2VpcEndpoint(AWS Tools for Windows PowerShell)
- CreateVpcEndpoint(Amazon EC2 쿼리 API)

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트를 설명하려면

- Get-EC2VpcEndpoint(AWS Tools for Windows PowerShell)
- DescribeVpcEndpoints(Amazon EC2 쿼리 API)

보안 그룹 수정

인스턴스에 연결된 VPC 보안 그룹이 아웃바운드 트래픽을 제한할 경우, AWS 서비스를 향하는 트래픽을 허용하는 규칙을 추가하여 인스턴스를 유지해야 합니다.

게이트웨이 엔드포인트에 대한 아웃바운드 규칙을 추가하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Security Groups]를 선택합니다.
3. VPC 보안 그룹을 선택하고 아웃바운드 규칙(Outbound Rules) 탭을 선택한 후 아웃바운드 규칙 편집(Edit outbound rules)을 선택합니다.
4. [Type] 목록에서 트래픽 유형을 선택한 후 필요한 경우, 포트 범위를 입력합니다. 예를 들어 인스턴스를 사용하여 Amazon S3에서 객체를 검색할 경우 유형 목록에서 HTTPS를 선택합니다.

5. 대상에서 `pl-` 입력을 시작하여 사용 가능한 AWS 서비스에 대한 접두사 목록 ID와 이름의 목록을 표시합니다. AWS 서비스의 접두사 목록 ID를 선택하거나 입력합니다.
6. 저장(Save)을 선택합니다.

명령줄 또는 API를 사용하여 접두사 목록 이름, ID 및 AWS 서비스에 대한 IP 주소 범위를 가져오려면

- describe-prefix-lists(AWS CLI)
- Get-EC2PrefixList(AWS Tools for Windows PowerShell)
- DescribePrefixLists(Amazon EC2 쿼리 API)

게이트웨이 엔드포인트 수정

정책을 변경하거나 삭제하고, 엔드포인트에서 사용하는 라우팅 테이블을 추가하거나 삭제하여 게이트웨이 엔드포인트를 수정할 수 있습니다.

기존 Amazon S3 게이트웨이 엔드포인트를 인터페이스 엔드포인트로 마이그레이션하려면 Amazon S3 인터페이스 엔드포인트를 생성한 후 Amazon S3 게이트웨이 엔드포인트를 삭제합니다. 자세한 내용은 the section called “인터페이스 엔드포인트 생성” (p. 8) 및 the section called “VPC 종단점 삭제” (p. 36) 단원을 참조하세요.

게이트웨이 엔드포인트와 연결된 정책을 변경하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 엔드포인트를 선택합니다.
3. [Actions], [Edit policy]를 선택합니다.
4. [Full Access]를 선택하여 모든 액세스를 허용할 수 있습니다. 또는 사용자 지정을 선택한 후 AWS 정책 생성기를 사용하여 사용자 지정 정책을 만들거나, 정책 창에서 직접 정책을 입력할 수도 있습니다. 완료되면 [Save]를 선택합니다.

   Note

   정책 변경 사항이 적용되려면 몇 분 정도 걸릴 수 있습니다.

게이트웨이 엔드포인트가 사용하는 라우팅 테이블을 추가 또는 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoints]를 선택한 후 엔드포인트를 선택합니다.
3. 작업(Actions), 라우팅 테이블 관리(Manage route tables)를 선택합니다.
4. 필요한 라우팅 테이블을 선택하거나 선택 취소한 후 라우팅 테이블 수정을 선택합니다.

AWS CLI를 사용하여 게이트웨이 엔드포인트를 수정하려면

1. describe-vpc-endpoints 명령을 사용하여 게이트웨이 엔드포인트의 ID를 가져옵니다.

```
aws ec2 describe-vpc-endpoints
```

2. 다음 예제는 modify-vpc-endpoint 명령을 사용하여 라우팅 테이블 `rtb-aaa222bb`를 게이트웨이 엔드포인트에 연결하고 정책 문서를 재설정합니다.

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

AWS Tools for Windows PowerShell 또는 API를 사용하여 VPC 엔드포인트를 수정하려면

- Edit-EC2VpcEndpoint(AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint(Amazon EC2 쿼리 API)

게이트웨이 엔드포인트 태그 추가 또는 제거

태그는 게이트웨이 엔드포인트를 식별하는 방법을 제공합니다. 태그를 추가하거나 제거할 수 있습니다.

게이트웨이 엔드포인트 태그를 추가 또는 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 게이트웨이 엔드포인트를 선택하고 작업, 태그 추가/편집을 선택합니다.
4. 태그를 추가하거나 제거합니다.

   태그 추가 태그 생성을 선택하고 다음을 수행합니다.
   - 키에 키 이름을 입력합니다.
   - 값에 키 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 삭제 버튼("x")을 선택합니다.

AWS Tools for Windows PowerShell 또는 API를 사용하여 태그를 추가하거나 제거하려면

- create-tags(AWS CLI)
- CreateTags(AWS Tools for Windows PowerShell)
- delete-tags(AWS CLI)
- DeleteTags(AWS Tools for Windows PowerShell)

VPC 종단점으로 서비스에 대한 액세스 제어

인터페이스 또는 게이트웨이 엔드포인트를 생성할 경우, 연결하려는 서비스에 대한 액세스를 제어하는 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 엔드포인트 정책은 JSON 형식으로 작성해야 합니다. 모든 서비스가 엔드포인트 정책을 지원하는 것은 아닙니다.

Amazon S3에 대한 엔드포인트를 사용할 경우, Amazon S3 버킷 정책을 사용하여 특정 엔드포인트 또는 특정 VPC의 버킷에 대한 액세스를 제어할 수도 있습니다. 자세한 내용은 Amazon S3 버킷 정책 (p. 27) 단원을 참조하세요.

목차

VPC 종단점 정책 사용

VPC 엔드포인트 정책은 엔드포인트를 만들거나 수정 시 엔드포인트에 연결하는 IAM 리소스 정책입니다. 엔드포인트를 만들 때 정책을 추가하지 않으면 서비스에 대한 모든 액세스를 허용하는 기본 정책이 추가됩니다. 서비스가 엔드포인트 정책을 지원하지 않는 경우, 엔드포인트는 그 서비스에 대한 모든 액세스를 허용합니다. 엔드포인트 정책은 IAM 사용자 정책 또는 서비스별 정책(예: S3 버킷 정책)을 무시하거나 교체하지 않습니다. 이는 엔드포인트에서 지정된 서비스로의 액세스를 제어하기 위한 별도의 정책입니다.

하나의 엔드포인트에 둘 이상의 정책을 연결할 수 없습니다. 그러나 언제든 정책을 수정할 수 있습니다. 정책을 수정할 경우, 변경 사항이 적용되기까지 몇 분 정도 걸릴 수 있습니다. 정책 작성에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 개요를 참조하세요.

엔드포인트 정책은 IAM 정책과 비슷하지만 다음에 유의해야 합니다.

- 정책에는 주체 요소가 있어야 합니다. 게이트웨이 엔드포인트에 관한 자세한 내용은 게이트웨이 엔드포인트에 대한 엔드포인트 정책 (p. 36)를 참조하세요.
- 엔드포인트 정책의 크기는 20,480자를 초과할 수 없습니다(공백 포함).

엔드포인트 정책을 지원하는 서비스에 대한 자세한 내용은 AWS PrivateLink를 지원하는 서비스 (p. 67) 섹션을 참조하세요.

게이트웨이 엔드포인트에 대한 엔드포인트 정책

게이트웨이 엔드포인트에 적용된 엔드포인트 정책의 경우 `Principal` 또는 `"AWS":"account-ID"` 형식으로 `"AWS":"arn:aws:iam::account-ID:root"`을 지정하면 계정 루트 사용자에게만 액세스 권한이 부여되며 계정의 모든 IAM 사용자 및 역할에게 액세스 권한이 부여되는 것은 아닙니다.

`Principal` 요소에 Amazon 리소스 이름(ARN)을 지정하면 정책을 저장할 때 해당 ARN이 고유 보안 주체 ID로 변환됩니다.

Amazon S3 및 DynamoDB용 엔드포인트 정책 예는 다음 주제를 참조하세요.

- Amazon S3에 대한 엔드포인트 정책 (p. 25)
- DynamoDB에 대한 엔드포인트 정책 (p. 30)

보안 그룹

인터페이스 엔드포인트를 생성할 때 서비스와의 통신에 사용할 수 있는 엔드포인트별 VPC 호스트 이름이 생성됩니다. 보안 그룹을 지정하지 않을 경우 VPC에 대한 기본 보안 그룹이 엔드포인트 네트워크 인터페이스에 자동적으로 연결됩니다. 보안 그룹에 대한 규칙이 엔드포인트 네트워크 인터페이스 및 서비스와 통신하는 VPC의 리소스 사이의 통신을 허용하도록 해야 합니다.

게이트웨이 엔드포인트에서 보안 그룹의 아웃바운드 규칙이 제한된 경우, VPC에서 엔드포인트에 지정된 서비스로의 아웃바운드 트래픽을 허용하는 규칙을 추가해야 합니다. 이렇게 하려면 아웃바운드 규칙에서 서비스의 AWS 접두사 목록 ID를 대상으로 사용합니다. 자세한 내용은 보안 그룹 수정 (p. 33) 단원을 참조하세요.

보안 그룹은 Gateway Load Balancer 엔드포인트에는 적용되지 않습니다.

VPC 종단점 삭제

엔드포인트가 더 이상 필요하지 않으면 이를 삭제할 수 있습니다. 게이트웨이 엔드포인트를 삭제하면 엔드포인트가 사용하는 라우팅 테이블의 엔드포인트 라우팅도 삭제됩니다. 하지만 엔드포인트가 상주하는 VPC와 연결된 보안 그룹에는 아무런 영향이 없습니다. 인터페이스 엔드포인트 또는 Gateway Load Balancer 엔드포인트를 삭제하면 엔드포인트 네트워크 인터페이스도 삭제됩니다.

라우팅 테이블에 엔드포인트를 가리키는 경로가 있으면 Gateway Load Balancer 엔드포인트를 삭제할 수 없습니다.

엔드포인트를 삭제하려면

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

2. 탐색 창에서 [Endpoints]를 선택한 후 엔드포인트를 선택합니다.
3. [Actions], [Delete Endpoint]를 차례로 선택합니다.
4. 확인 화면에서 [Yes, Delete]를 선택합니다.

VPC 엔드포인트를 삭제하려면

- delete-vpc-endpoints(AWS CLI)
- Remove-EC2VpcEndpoint(AWS Tools for Windows PowerShell)
- DeleteVpcEndpoints(Amazon EC2 쿼리 API)

VPC 엔드포인트 서비스(AWS PrivateLink)

VPC에서 자체 애플리케이션을 생성하고 AWS PrivateLink 구동 서비스(엔드포인트 서비스라고도 함)로서 구성할 수 있습니다. 기타 AWS 보안 주체는 서비스 유형에 따라 인터페이스 VPC 엔드포인트 (p. 3) 또는 Gateway Load Balancer 엔드포인트 (p. 16)를 사용하여 VPC에서 엔드포인트 서비스로 이어지는 연결을 생성할 수 있습니다. 서비스 공급자인 경우 서비스에 연결을 생성하는 AWS 보안 주체는 서비스 소비자가 됩니다.

목차

인터페이스 엔드포인트를 위한 VPC 엔드포인트 서비스

다음은 인터페이스 엔드포인트를 위한 엔드포인트 서비스 생성의 일반적인 단계입니다.

1. VPC에서 애플리케이션에 대한 Network Load Balancer를 생성하고 서비스를 사용할 수 있어야 하는 각 서브넷(가용 영역)에 대해 이를 구성합니다. 로드 밸런서는 서비스 소비자로부터 요청을 받아 서비스로 전달합니다. 또는 Application Load Balancer를 네트워크 로드 밸런서의 대상으로 구성하면 Application Load Balancer가 요청을 서비스로 라우팅할 수 있습니다. 자세한 내용은 Network Load Balancer 사용 설명서를 참조하세요.

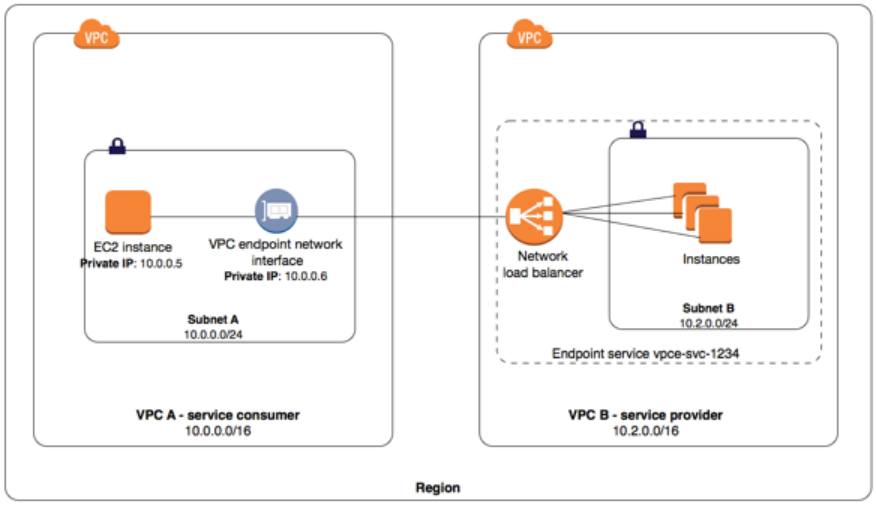
   리전 내 모든 가용 영역에 서비스를 구성하는 것이 좋습니다.
2. VPC 엔드포인트 서비스 구성을 생성하고 Network Load Balancer를 지정합니다.

다음은 서비스 소비자를 서비스에 연결해주는 일반적인 단계입니다.

1. 특정 서비스 소비자(AWS 계정, IAM 사용자 및 IAM 역할)에게 엔드포인트 서비스에 연결을 생성할 수 있는 권한을 부여합니다.
2. 권한이 부여된 서비스 소비자는 서비스를 구성한 각 가용 영역에 선택적으로 서비스에 대한 인터페이스 엔드포인트를 생성합니다.
3. 연결을 활성화하려면 인터페이스 엔드포인트 연결 요청을 수락합니다. 기본적으로 연결 요청은 수동으로 수락되어야 합니다. 그러나 연결 요청을 자동으로 수락하도록 엔드포인트 서비스에 대한 수락 설정을 구성할 수도 있습니다.

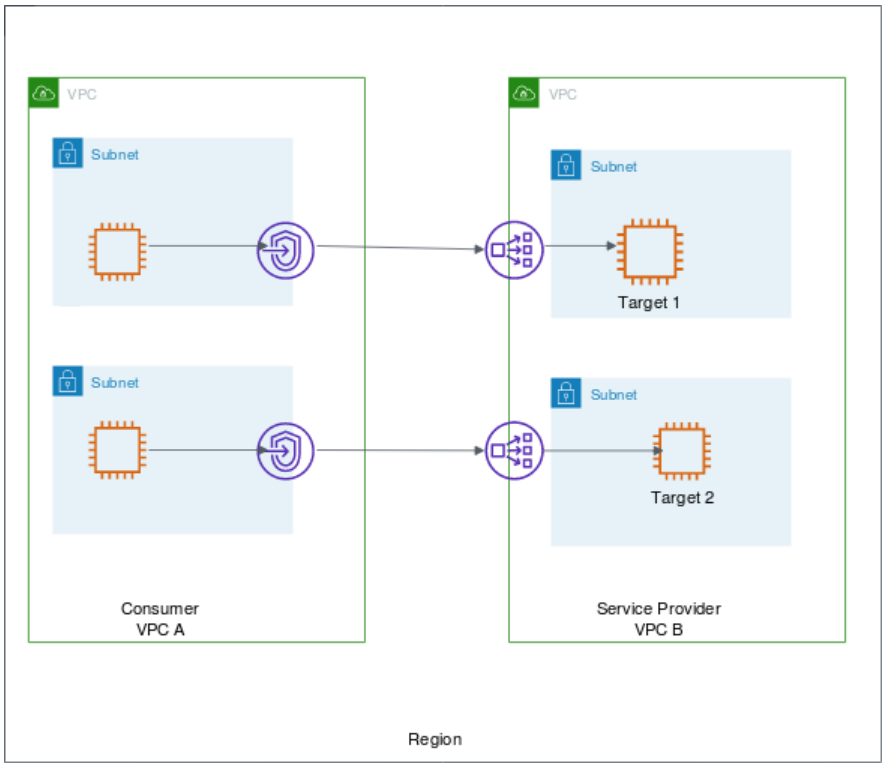
권한 및 수락 설정을 조합하면 서비스에 액세스할 수 있는 서비스 소비자(AWS 보안 주체)를 제어하는 데 도움이 될 수 있습니다. 예를 들어 신뢰할 수 있고 자동으로 모든 연결 요청을 수락하는 선택된 보안 주체에 권한을 부여하거나, 더 넓은 범위의 보안 주체 그룹에 권한을 부여하고 신뢰할 수 있는 특정 연결 요청을 수동으로 수락할 수 있습니다.

다음 다이어그램에서 VPC B의 계정 소유자가 서비스 공급자이고, 서브넷 B의 인스턴스에서 실행 중인 서비스가 있습니다. VPC B의 소유자는 서브넷 B의 인스턴스를 대상으로 가리키는 연결된 Network Load Balancer를 포함한 서비스 엔드포인트(vpce-svc-1234)을 보유합니다. VPC A의 서브넷 A에 있는 인스턴스는 인터페이스 엔드포인트를 사용하여 서브넷 B의 서비스에 액세스합니다.



낮은 대기 시간과 내결함성을 위해 AWS 리전의 모든 가용 영역에 대상을 포함한 Network Load Balancer를 사용할 것을 권장합니다. 서비스 액세스에 영역 단위 DNS 호스트 이름 (p. 13)을 사용하는 서비스 소비자에 고가용성을 보장하는 데 도움을 받기 위해 교차 영역 로드 밸런싱을 활성화시킬 수 있습니다. 교차 영역 로드 밸런싱은 로드 밸런서를 활성화해 모든 활성 가용 영역의 등록된 대상들로 트래픽을 분산시킵니다. 자세한 내용은 Network Load Balancer 사용 설명서의 교차 영역 로드 밸런싱을 참조하십시오. 교차 영역 로드 밸런싱이 활성화된 경우 리전별 데이터 전송 요금이 계정에 적용될 수 있습니다.

다음 다이어그램에서 VPC B의 소유자는 서비스 공급자이며, 가용 영역 두 개에 대상이 포함된 Network Load Balancer를 구성했습니다. 서비스 소비자(VPC A)는 자신의 VPC에 동일한 두 개 가용 영역의 인터페이스 엔드포인트를 생성했습니다. VPC A 인스턴스에서 서비스를 요청하는데 두 인터페이스 엔드포인트 중 하나를 사용할 수 있습니다.



서비스를 구성하고 서비스 소비자가 VPC 피어링 연결을 통해 해당 서비스에 액세스할 수 있도록 하는 예제는 Amazon VPC 사용 설명서에서 예제: AWS PrivateLink 및 VPC 피어링을 사용하는 서비스를 참조하세요.

엔드포인트 서비스 가용 영역 관련 고려 사항

엔드포인트 서비스를 생성할 때 계정에 매핑된 가용 영역에 서비스가 생성됩니다. 이 가용 영역은 다른 계정과는 별도입니다. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 엔드포인트 서비스 가용 영역을 고유하고 지속적으로 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하십시오. 예를 들어, `use1-az1`은 `us-east-1` 리전의 AZ ID이고, 모든 AWS 계정에서 위치가 동일합니다. 가용 영역 ID에 대한 자세한 정보는 AWS RAM 사용 설명서의 리소스에 대한 AZ ID를 참조하거나 describe-availability-zones를 사용하세요.

서비스 공급자와 소비자의 계정이 서로 다르며 여러 가용 영역을 사용하고 소비자가 VPC 엔드포인트 서비스 정보를 보는 경우 응답에는 공통 가용 영역만 포함됩니다. 예를 들어 서비스 공급자 계정에서 `us-east-1a` 및 `us-east-1c`를 사용하고 소비자가 `us-east-1a` 및 `us-east-1b`를 사용하는 경우 응답에는 공통 가용 영역 `us-east-1a`의 VPC 엔드포인트 서비스가 포함됩니다.

엔드포인트 서비스 DNS 이름

VPC 엔드포인트 서비스를 생성하면 AWS에서 서비스와의 통신에 사용할 수 있는 엔드포인트별 DNS 호스트 이름을 생성합니다. 이러한 이름에는 VPC 엔드포인트 ID, 가용 영역 이름 및 리전 이름이 포함됩니다. 예를 들어, vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com입니다. 기본적으로 소비자는 해당 DNS 이름으로 서비스에 액세스하며 일반적으로 애플리케이션 구성을 수정해야 합니다.

엔드포인트 서비스가 AWS 서비스용이거나 AWS Marketplace에 제공된 서비스인 경우, 기본 DNS 이름이 있습니다. 다른 서비스의 경우, 서비스 공급자는 프라이빗 DNS 이름을 구성하여, 소비자가 애플리케이션을 변경하지 않고 기존 DNS 이름을 사용해 서비스에 액세스하도록 할 수 있습니다. 자세한 내용은 프라이빗 DNS 이름 (p. 58) 단원을 참조하십시오.

서비스 공급자는 IAM 정책 설명에 ec2:VpceServicePrivateDnsName 조건 컨텍스트 키를 사용하여, 생성할 수 있는 프라이빗 DNS 이름을 제어할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Amazon EC2에서 정의한 작업을 참조하십시오.

프라이빗 DNS 이름 요구 사항

서비스 공급자는 새 엔드포인트 서비스 또는 기존 엔드포인트 서비스에 대한 프라이빗 DNS 이름을 지정할 수 있습니다. 프라이빗 DNS 이름을 사용하려면 이 기능을 활성화한 다음 프라이빗 DNS 이름을 지정합니다. 소비자가 프라이빗 DNS 이름을 사용할 수 있으려면, 여러분이 도메인/하위 도메인을 제어할 수 있는지 확인해야 합니다. Amazon VPC 콘솔 또는 API를 사용하여 도메인 소유권 확인을 시작할 수 있습니다. 도메인 소유권 확인이 완료되면 소비자는 프라이빗 DNS 이름을 사용하여 엔드포인트에 액세스합니다.

온프레미스 데이터 센터에 대한 연결

인터페이스 엔드포인트와 온프레미스 데이터 센터 간 연결에 다음 유형의 연결을 사용할 수 있습니다.

- AWS Direct Connect
- AWS Site-to-Site VPN

VPC 피어링 연결을 통해 서비스에 액세스

VPC 엔드포인트와 함께 VPC 피어링 연결을 사용하여 VPC 피어링 연결에서 소비자에게 프라이빗 액세스를 허용할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서에서 예제: AWS PrivateLink 및 VPC 피어링을 사용하는 서비스를 참조하세요.

연결 정보에 대한 프록시 프로토콜 사용

Network Load Balancer는 애플리케이션(서비스)에 대한 원본 IP 주소를 제공합니다. 서비스 소비자가 인터페이스 엔드포인트를 통해 서비스로 트래픽을 전송할 때 애플리케이션에 제공된 원본 IP 주소는 Network Load Balancer 노드의 프라이빗 IP 주소이며, 서비스 소비자의 IP 주소가 아닙니다.

서비스 소비자의 IP 주소와 해당 인터페이스 엔드포인트 ID가 필요한 경우 로드 밸런서의 프록시 프로토콜을 활성화하고 프록시 프로토콜 헤더에서 클라이언트 IP 주소를 가져옵니다. 자세한 내용은 Network Load Balancer 사용 설명서의 프록시 프로토콜을 참조하십시오.

규칙 및 제한 사항

엔드포인트 서비스를 사용하려면 현재 규칙과 제한 사항을 알고 있어야 합니다.

- 엔드포인트 서비스는 TCP를 통한 IPv4 트래픽만 지원합니다.
- 서비스 소비자는 엔드포인트별 DNS 호스트 이름을 사용하여 엔드포인트 서비스 또는 프라이빗 DNS 이름에 액세스할 수 있습니다.
- 엔드포인트 서비스가 여러 Network Load Balancer에 연결되어 있는 경우 특정 가용 영역에 대해 인터페이스 엔드포인트는 한 개의 로드 밸런서에만 연결을 설정합니다.
- 엔드포인트 서비스의 경우 연결된 Network Load Balancer는 각각의 고유 대상(IP 주소 및 포트)에 대해 55,000건의 동시 연결 또는 분당 약 55,000건의 연결을 지원할 수 있습니다. 연결 건수가 이보다 더 많을 경우, 포트 할당 오류가 발생할 가능성이 증가합니다. 포트 할당 오류를 해결하려면 대상 그룹에 더 많은 대상들을 추가하십시오. 네트워크 로드 밸런서 대상 그룹에 대한 자세한 내용은 네트워크 로드 밸런서 사용 설명서의 네트워크 로드 밸런서 대상 그룹 및 대상 그룹에 대상 등록을 참조하세요.
- 한 계정의 가용 영역이 다른 계정의 가용 영역과 동일한 위치로 매핑되지 않을 수 있습니다. 예를 들어 한 계정의 `us-east-1a` 가용 영역이 다른 계정의 `us-east-1a` 가용 영역과 동일한 위치에 존재하지 않을 수 있습니다. 자세한 내용은 리전 및 영역을 참조하십시오. 엔드포인트를 구성하는 경우 사용자 계정으로 매핑된 가용 영역으로 구성됩니다.
- 엔드포인트 서비스는 해당 서비스를 생성한 리전에서만 사용할 수 있습니다.
- 엔드포인트 서비스에 대한 서비스별 제한을 검토합니다.

- 엔드포인트 서비스에 대한 보안 모범 사례 및 예제를 검토합니다. 자세한 내용은 정책 모범 사례 및 the section called “서비스에 대한 액세스 제어” (p. 35)를 참조하세요.

Gateway Load Balancer 엔드포인트에 대한 VPC 엔드포인트 서비스

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. Gateway Load Balancer를 VPC 엔드포인트 서비스로 구성하면 다른 AWS 보안 주체가 Gateway Load Balancer 엔드포인트를 통해 서비스에 액세스하게 할 수 있습니다.

다음은 Gateway Load Balancer 엔드포인트를 위한 엔드포인트 서비스 생성의 일반적인 단계입니다.

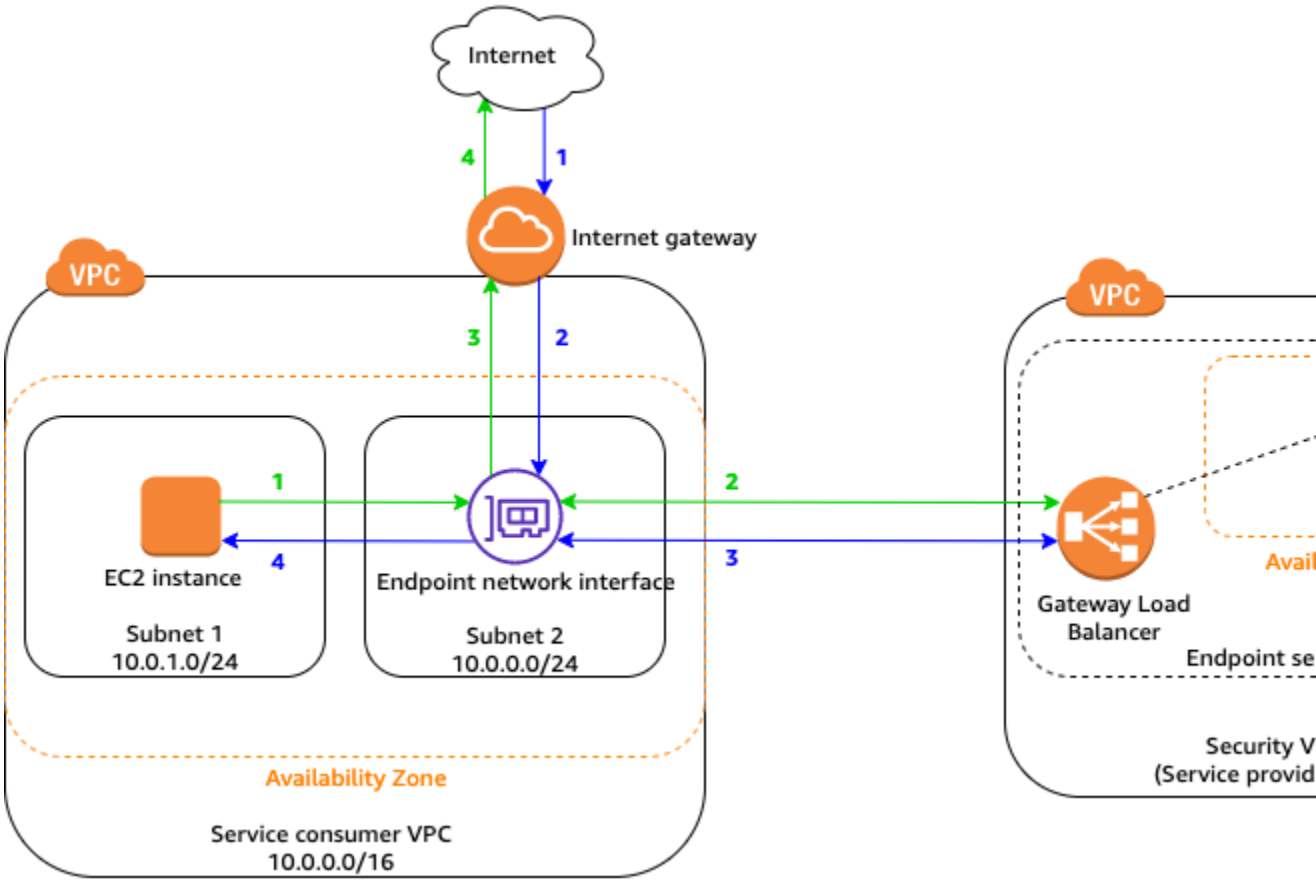
1. 가상 어플라이언스에 대한 Gateway Load Balancer를 생성합니다. 자세한 내용은 Getting started with Gateway Load Balancers를 참조하십시오.

   리전 내 모든 가용 영역에 서비스를 구성하는 것이 좋습니다.
2. VPC 엔드포인트 서비스 구성을 생성하고 Gateway Load Balancer를 지정합니다.

다음은 서비스 소비자를 서비스에 연결해주는 일반적인 단계입니다.

1. 특정 서비스 소비자(AWS 계정, IAM 사용자 및 IAM 역할)에게 엔드포인트 서비스에 연결을 생성할 수 있는 권한을 부여합니다.
2. 권한이 부여된 서비스 소비자는 서비스에 대한 Gateway Load Balancer 엔드포인트 (p. 16)를 생성합니다.
3. 연결을 활성화하려면 엔드포인트 연결 요청을 수락합니다. 기본적으로 연결 요청은 수동으로 수락되어야 합니다. 그러나 연결 요청을 자동으로 수락하도록 엔드포인트 서비스에 대한 수락 설정을 구성할 수도 있습니다.

다음 예에서는 보안 VPC의 Gateway Load Balancer 뒤에 보안 어플라이언스 플릿이 구성됩니다. 엔드포인트 서비스는 Gateway Load Balancer에 대해 구성됩니다. 서비스 소비자 VPC의 소유자는 VPC의 서브넷 2에 Gateway Load Balancer 엔드포인트를 생성합니다(엔드포인트 네트워크 인터페이스로 표시됨). 인터넷 게이트웨이를 통해 VPC로 들어오는 모든 트래픽은 먼저 보안 VPC가 검사할 수 있도록 Gateway Load Balancer 엔드포인트로 라우팅된 후 대상 서브넷으로 라우팅됩니다. 마찬가지로 서브넷 1에서 EC2 인스턴스를 나가는 모든 트래픽은 보안 VPC가 검사할 수 있도록 먼저 Gateway Load Balancer 엔드포인트로 라우팅된 후 인터넷으로 라우팅됩니다.



이 시나리오의 라우팅 구성에 대한 자세한 내용은 Amazon VPC 사용 설명서에서 Gateway Load Balancer 엔드포인트로의 라우팅을 참조하세요.

가용 영역 고려 사항

엔드포인트 서비스를 생성할 때 계정에 매핑된 가용 영역에 서비스가 생성됩니다. 이 가용 영역은 다른 계정과는 별도입니다. 서비스 공급자와 소비자가 다른 계정에 있는 경우에는 엔드포인트 서비스 가용 영역을 고유하고 지속적으로 식별하기 위한 가용 영역 ID를 사용하는 방법을 확인하십시오. 예를 들어, `use1-az1`은 `us-east-1` 리전의 AZ ID이고, 모든 AWS 계정에서 위치가 동일합니다. 가용 영역 ID에 대한 자세한 정보는 AWS RAM 사용 설명서의 리소스에 대한 AZ ID를 참조하거나 describe-availability-zones를 사용하세요.

서비스 공급자와 소비자의 계정이 서로 다르며 여러 가용 영역을 사용하고 소비자가 VPC 엔드포인트 서비스 정보를 보는 경우 응답에는 공통 가용 영역만 포함됩니다. 예를 들어 서비스 공급자 계정에서 `us-east-1a` 및 `us-east-1c`를 사용하고 소비자가 `us-east-1a` 및 `us-east-1b`를 사용하는 경우 응답에는 공통 가용 영역 `us-east-1a`의 VPC 엔드포인트 서비스가 포함됩니다.

규칙 및 제한 사항

Gateway Load Balancer 엔드포인트에 대한 엔드포인트 서비스를 사용하려면 현재 규칙과 제한 사항을 알고 있어야 합니다.

- 엔드포인트 서비스가 여러 Gateway Load Balancer에 연결되어 있는 경우 특정 가용 영역에 대해 Gateway Load Balancer 엔드포인트는 한 개의 로드 밸런서에만 연결을 설정합니다.
- 프라이빗 DNS 이름은 지원되지 않습니다.

- 한 계정의 가용 영역이 다른 계정의 가용 영역과 동일한 위치로 매핑되지 않을 수 있습니다. 예를 들어 한 계정의 `us-east-1a` 가용 영역이 다른 계정의 `us-east-1a` 가용 영역과 동일한 위치에 존재하지 않을 수 있습니다. 자세한 내용은 리전 및 영역을 참조하십시오. 엔드포인트를 구성하는 경우 사용자 계정으로 매핑된 가용 영역으로 구성됩니다.

인터페이스 엔드포인트에 대한 VPC 종단점 서비스 구성 생성

Amazon VPC 콘솔 또는 명령줄을 사용하여 엔드포인트 서비스 구성을 생성할 수 있습니다. VPC 엔드포인트 제한에 대한 자세한 내용은 Amazon VPC 사용 설명서의 제한을 참조하세요.

시작하기 전에 서비스에 대한 VPC에 Network Load Balancer가 하나 이상 있는지 확인합니다. 자세한 내용은 Network Load Balancer 사용 설명서의 Network Load Balancer 시작하기를 참조하십시오.

구성에서, 사용자가 서비스에 대한 인터페이스 엔드포인트 연결 요청을 수동으로 수락해야 하도록 선택적으로 지정할 수 있습니다. 알림을 생성 (p. 50)하여 연결 요청이 있을 때 알림을 받을 수 있습니다. 연결을 수락하지 않으면 서비스 소비자가 서비스에 액세스할 수 없습니다.

Note

수락 설정에 관계없이 서비스 소비자는 서비스에 대해 연결을 생성할 수 있는 권한 (p. 46)이 있어야 합니다.

엔드포인트 서비스 구성을 생성한 후에는 서비스 소비자가 서비스에 대한 인터페이스 엔드포인트를 생성하도록 해주는 권한을 추가해야 합니다.

Console

엔드포인트 서비스를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint Services)를 선택한 후 엔드포인트 서비스 생성(Create Endpoint Service)을 선택합니다.
3. 로드 밸런서 유형(Load balancer type)에서 네트워크(Network)를 선택합니다.
4. 사용 가능한 로드 밸런서(Available load balancers)에서 엔드포인트 서비스에 연결된 Network Load Balancer를 선택합니다.
5. [Require acceptance for endpoint]에서 서비스에 대한 연결 요청을 수동으로 수락한다는 확인란을 선택합니다. 그렇지 않은 경우 엔드포인트 연결은 자동으로 수락됩니다.
6. 프라이빗 DNS 이름 활성화(Enable private DNS name)를 선택한 다음, 서비스와 연결할 프라이빗 DNS 이름 옆의 확인란을 선택하고 프라이빗 DNS의 이름을 입력합니다.
7. (선택 사항) 태그를 추가하려면 새로운 태그 추가(Add new tag)를 선택하고 해당 태그에 대한 키와 값을 입력합니다.
8. Create를 선택합니다.

AWS CLI

엔드포인트 서비스를 생성하려면

create-vpc-endpoint-service-configuration 명령을 사용하고 Network Load Balancer에 대한 ARN을 하나 이상 지정합니다. 서비스 연결을 위해 수락을 요구할 것인지, 서비스에 프라이빗 DNS 이름이 있는지 등을 선택적으로 지정할 수 있습니다.

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532 --acceptance-required --privateDnsName exampleservice.com
```

다음은 예제 출력입니다.

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "NetworkLoadBalancerArns": [
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532"
        ],
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
        "ServiceState": "Available",
        "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
        "PrivateDnsName": "exampleService.com",
        "AcceptanceRequired": true,
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "BaseEndpointDnsNames": [
            "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
        ]
    }
}
```

Tools for Windows PowerShell

엔드포인트 서비스를 생성하려면

New-EC2VpcEndpointServiceConfiguration을 사용합니다.

API

엔드포인트 서비스를 생성하려면

CreateVpcEndpointServiceConfiguration을 사용합니다.

Gateway Load Balancer 엔드포인트에 대한 VPC 종단점 서비스 구성 생성

Amazon VPC 콘솔 또는 명령줄을 사용하여 엔드포인트 서비스 구성을 생성할 수 있습니다. 시작하기 전에 서비스에 대한 VPC에서 서비스에 대한 하나 이상의 Gateway Load Balancer를 생성했는지 확인합니다. 자세한 내용은 Getting started with Gateway Load Balancers를 참조하십시오.

구성에서, 사용자가 서비스에 대한 Gateway Load Balancer 엔드포인트 연결 요청을 수동으로 수락해야 하도록 선택적으로 지정할 수 있습니다. 알림을 생성 (p. 50)하여 연결 요청이 있을 때 알림을 받을 수 있습니다. 연결을 수락하지 않으면 서비스 소비자가 서비스에 액세스할 수 없습니다.

엔드포인트 서비스 구성을 생성한 후에는 서비스 소비자가 서비스에 대한 Gateway Load Balancer 엔드포인트를 생성하도록 해주는 권한 (p. 46)을 추가해야 합니다.

Console

엔드포인트 서비스를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스(Endpoint Services)를 선택한 후 엔드포인트 서비스 생성(Create Endpoint Service)을 선택합니다.
3. 로드 밸런서 유형(Load balancer type)에서 게이트웨이(Gateway)를 선택합니다.
4. 사용 가능한 로드 밸런서(Available load balancers)에서 엔드포인트 서비스에 연결된 Gateway Load Balancer를 선택합니다.
5. [Require acceptance for endpoint]에서 서비스에 대한 연결 요청을 수동으로 수락한다는 확인란을 선택합니다. 그렇지 않은 경우 엔드포인트 연결은 자동으로 수락됩니다.
6. (선택 사항) 태그를 추가하려면 새로운 태그 추가(Add new tag)를 선택하고 해당 태그에 대한 키와 값을 입력합니다.
7. Create를 선택합니다.

AWS CLI

엔드포인트 서비스를 생성하려면

create-vpc-endpoint-service-configuration 명령을 사용하고 Gateway Load Balancer에 대한 ARN을 하나 이상 지정합니다. 선택적으로 서비스 연결 수락이 필요한지 여부를 지정할 수 있습니다.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-arns gateway-load-balancer-arn --no-acceptance-required
```

Tools for Windows PowerShell

엔드포인트 서비스를 생성하려면

New-EC2VpcEndpointServiceConfiguration을 사용합니다.

API

엔드포인트 서비스를 생성하려면

CreateVpcEndpointServiceConfiguration을 사용합니다.

엔드포인트 서비스에 대한 권한 추가 및 제거

엔드포인트 서비스 구성을 생성한 후에는 어떤 서비스 소비자가 서비스에 연결할 인터페이스 엔드포인트 또는 Gateway Load Balancer 엔드포인트를 생성할 수 있는지를 제어할 수 있습니다. 서비스 소비자는 IAM 보안 주체 - 즉 IAM 사용자, IAM 역할 및 AWS 계정입니다. 보안 주체에 대한 권한을 추가하거나 제거하려면, ARN(Amazon 리소스 이름)이 필요합니다.

- AWS 계정(및 계정에 있는 모든 보안 주체)의 경우, ARN이 `arn:aws:iam::aws-account-id:root` 양식으로 되어 있습니다.
- 특정 IAM 사용자는 ARN이 `arn:aws:iam::aws-account-id:user/user-name` 형식입니다.
- 특정 IAM 역할은 ARN이 `arn:aws:iam::aws-account-id:role/role-name` 형식입니다.

Note

권한을 "누구나 액세스 가능(anyone can access)"으로 설정하고 수락 모델을 "모든 요청 수락(accept all requests)"으로 설정하면 로드 밸런서를 퍼블릭으로 구성한 것입니다. AWS 계정을 쉽게

얻을 수 있으므로 퍼블릭 IP 주소가 없어도 사실상 모든 사용자가 로드 밸런서에 액세스할 수 있습니다.

Console

엔드포인트 서비스에 대한 권한을 추가하거나 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택하고 작업(Actions), 보안 주체 허용(Allow principals)을 선택합니다.
4. 권한을 추가할 주체에 대한 ARN을 지정합니다. 보안 주체를 더 추가하려면 보안 주체 추가(Add principal)를 선택합니다. 보안 주체를 제거하려면 항목 옆에 있는 제거(Remove)를 선택합니다.

   *를 지정하면 모든 주체에 권한을 추가합니다. 이렇게 하면 모든 AWS 계정에 있는 모든 보안 주체가 엔드포인트 서비스에 대해 엔드포인트를 생성할 수 있습니다.
5. 보안 주체 허용(Allow principals)을 선택합니다.

AWS CLI

엔드포인트 서비스에 대한 권한을 추가하려면

modify-vpc-endpoint-service-permissions 명령을 사용합니다. 보안 주체에 대해 하나 이상의 ARN을 추가하도록 `--add-allowed-principals` 파라미터를 지정합니다.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

엔드포인트 서비스에 대해 추가한 권한을 보려면

describe-vpc-endpoint-service-permissions 명령을 사용합니다.

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3
```

다음은 예제 출력입니다.

```
{
    "AllowedPrincipals": [
        {
            "PrincipalType": "Account",
            "Principal": "arn:aws:iam::123456789012:root"
        }
    ]
}
```

엔드포인트 서비스에 대한 권한을 제거하려면

modify-vpc-endpoint-service-permissions 명령을 사용합니다. 보안 주체에 대해 하나 이상의 ARN을 제거하도록 `--remove-allowed-principals` 파라미터를 지정합니다.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --remove-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Tools for Windows PowerShell

엔드포인트 서비스에 대한 권한을 추가하거나 제거하려면

Edit-EC2EndpointServicePermission을 사용합니다.

API

엔드포인트 서비스에 대한 권한을 추가하거나 제거하려면

ModifyVpcEndpointServicePermissions를 사용합니다.

엔드포인트 서비스 구성 변경

엔드포인트 서비스에 연결된 로드 밸런서를 변경하고 엔드포인트 서비스 연결 요청 시 수락이 필요한지 여부를 변경함으로써 엔드포인트 서비스 구성을 수정할 수 있습니다.

엔드포인트 서비스에 연결된 엔드포인트가 있는 경우 로드 밸런서를 연결 해제할 수 없습니다.

Console

엔드포인트 서비스에 대한 로드 밸런서를 변경하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 작업(Actions), 로드 밸런서 연결 또는 연결 해제(Associate or disassociate load balancers)를 선택합니다.
4. 필요에 따라 로드 밸런서를 선택하거나 선택 취소한 후 변경 사항 저장(Save changes)를 선택합니다.

수락 설정을 수정하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 작업(Actions), 엔드포인트 수락 설정 수정(Modify endpoint acceptance setting)을 차례로 선택합니다.
4. 수락 필요(Acceptance required)를 선택 또는 선택 해제한 다음 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI

엔드포인트 서비스에 대한 로드 밸런서를 변경하려면

modify-vpc-endpoint-service-configuration 명령을 사용합니다. 다음 예에서는 `--remove-network-load-balancer-arn` 매개 변수를 사용하여 Network Load Balancer를 제거합니다.

```
aws ec2 modify-vpc-endpoint-service-configuration --service-
id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532
```

수락 필요 여부를 변경하려면

modify-vpc-endpoint-service-configuration 명령을 사용하고 `--acceptance-required` 또는 `--no-acceptance-required`를 지정합니다.

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-
svc-09222513e6e77dc86 --no-acceptance-required
```

Tools for Windows PowerShell

엔드포인트 서비스 구성을 변경하려면

Edit-EC2VpcEndpointServiceConfiguration을 사용합니다.

API

엔드포인트 서비스 구성을 변경하려면

ModifyVpcEndpointServiceConfiguration을 사용합니다.

엔드포인트 연결 요청 수락 및 거부

엔드포인트 서비스를 생성한 후에는 권한이 추가된 서비스 소비자가 서비스에 연결할 인터페이스 엔드포인트 또는 Gateway Load Balancer 엔드포인트를 생성할 수 있습니다. 자세한 내용은 인터페이스 VPC 엔드포인트(AWS PrivateLink) (p. 3) 및 Gateway Load Balancer 엔드포인트(AWS PrivateLink) (p. 16) 단원을 참조하십시오.

연결 요청에 대한 수락이 필요하다고 지정한 경우 엔드포인트 서비스에 대한 엔드포인트 연결 요청을 수동으로 수락 또는 거부해야 합니다. 엔드포인트가 수락되면 `available` 상태가 됩니다. 검증 상태 변경이 완료되고 `available` 상태가 때까지 시간이 걸릴 수 있습니다.

`available` 상태가 된 이후 엔드포인트 연결을 거부할 수 있습니다.

Console

연결 요청을 수락 또는 거부하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 엔드포인트 연결(Endpoint connections) 탭에서 엔드포인트를 선택합니다. 연결 요청을 수락하려면 작업(Actions), 엔드포인트 연결 요청 수락(Accept endpoint connection request)을 차례로 선택합니다. 연결 요청을 거부하려면 작업(Actions), 엔드포인트 연결 요청 거부(Reject endpoint connection request)를 차례로 선택합니다.

AWS CLI

수락 보류 중인 엔드포인트 연결을 보려면

describe-vpc-endpoint-connections 명령을 사용하고 `pendingAcceptance` 상태를 기준으로 필터링합니다.

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-
state,Values=pendingAcceptance
```

다음은 예제 출력입니다.

```
{
    "VpcEndpointConnections": [
        {
            "VpcEndpointId": "vpce-0c1308d7312217abc",
            "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
            "CreationTimestamp": "2017-11-30T10:00:24.350Z",
            "VpcEndpointState": "pendingAcceptance",
```

```
            "VpcEndpointOwner": "123456789012"
        }
    ]
}
```

엔드포인트 연결 요청을 수락하려면

accept-vpc-endpoint-connections 명령을 사용하고 엔드포인트 ID와 엔드포인트 서비스 ID를 지정합니다.

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

엔드포인트 연결 요청을 거부하려면

reject-vpc-endpoint-connections 명령을 사용합니다.

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

Tools for Windows PowerShell

연결 요청을 수락 또는 거부하려면

Confirm-EC2EndpointConnection 및 Deny-EC2EndpointConnection을 사용합니다.

API

연결 요청을 수락 또는 거부하려면

AcceptVpcEndpointConnections 및 RejectVpcEndpointConnections를 사용합니다.

엔드포인트 서비스에 대한 알림 생성 및 관리

엔드포인트 서비스에 연결된 엔드포인트에서 발생하는 특정 이벤트에 대한 알림을 받도록 알림을 생성할 수 있습니다. 예를 들어 엔드포인트 서비스에 대한 엔드포인트 요청이 수락 또는 거부될 때 이메일을 받을 수 있습니다. 알림을 생성하려면 Amazon SNS 주제를 알림에 연결해야 합니다. SNS 주제를 구독하여 엔드포인트 이벤트가 발생할 때 이메일 알림을 받을 수 있습니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서를 참조하십시오.

알림에 대해 사용할 Amazon SNS 주제는 Amazon VPC 엔드포인트 서비스가 사용자를 대신해 알림을 게시하도록 허용하는 주제 정책을 보유해야 합니다. 주제 정책에 다음 문이 포함되어야 합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 주제에 대한 액세스 관리를 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
```

```
}
```

Console

엔드포인트 서비스에 대한 알림을 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 알림(Notifications) 탭을 선택합니다.
4. 알림 생성(Create Notification)을 선택합니다.
5. 알림 ARN(Notificatioin ARN)에서 알림과 연결할 SNS 주제에 대한 ARN을 선택합니다.
6. 이벤트(Events)에서 알림을 수신할 대상이 되는 엔드포인트 이벤트를 선택합니다.
7. 알림 생성(Create Notification)을 선택합니다.

알림을 생성한 후 해당 설정을 수정할 수 있습니다.

엔드포인트 서비스에 대한 알림을 수정하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 알림(Notifications) 탭을 선택합니다.
4. 알림을 선택하고 작업(Actions), 알림 수정(Modify Notification)을 선택합니다.
5. 필요에 따라 SNS 주제나 엔드포인트 이벤트를 변경합니다.
6. [Save changes]를 선택합니다.

알림이 더 이상 필요하지 않으면 삭제할 수 있습니다.

알림을 삭제하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 알림(Notifications) 탭을 선택합니다.
4. 알림을 선택하고 작업(Actions), 알림 삭제(Delete Notification)를 선택합니다.
5. 확인 메시지가 나타나면 **delete**를 입력한 다음 삭제를 선택합니다.

AWS CLI

엔드포인트 서비스에 대한 알림을 생성하려면

create-vpc-endpoint-connection-notification 명령을 선택합니다. SNS 주제의 ARN, 알림을 받을 이벤트 및 엔드포인트 서비스의 ID를 지정합니다.

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect
 Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

다음은 예제 출력입니다.

```
{
    "ConnectionNotification": {
        "ConnectionNotificationState": "Enabled",
```

```
        "ConnectionNotificationType": "Topic",
        "ServiceId": "vpce-svc-1237881c0d25a3abc",
        "ConnectionEvents": [
            "Reject",
            "Accept",
            "Delete",
            "Connect"
        ],
        "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
        "ConnectionNotificationArn": "arn:aws:sns:us-
east-2:123456789012:VpceNotification"
    }
}
```

알림을 보려면

describe-vpc-endpoint-connection-notifications 명령을 선택합니다.

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

알림에 대한 SNS 주제 또는 엔드포인트 이벤트를 변경하려면

modify-vpc-endpoint-connection-notification 명령을 선택합니다.

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-
nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

알림을 삭제하려면

delete-vpc-endpoint-connection-notifications 명령을 선택합니다.

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

Tools for Windows PowerShell

알림을 생성 및 관리하려면

다음을 사용합니다.

- New-EC2VpcEndpointConnectionNotification
- Get-EC2EndpointConnectionNotification
- Edit-EC2VpcEndpointConnectionNotification
- Remove-EC2EndpointConnectionNotification

API

알림을 생성 및 관리하려면

다음을 사용합니다.

- CreateVpcEndpointConnectionNotification
- DescribeVpcEndpointConnectionNotifications
- ModifyVpcEndpointConnectionNotification
- DeleteVpcEndpointConnectionNotifications

VPC 종단점 서비스 태그 추가 또는 제거

태그는 VPC 엔드포인트 서비스를 식별하는 방법을 제공합니다. 태그를 추가하거나 제거할 수 있습니다.

Console

VPC 엔드포인트 서비스 태그를 추가 또는 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. VPC 엔드포인트 서비스를 선택하고 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
4. 태그를 추가하거나 제거합니다.

   [태그 추가] 새 태그 추가(Add new tag)를 선택한 다음 태그 키와 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 제거(Remove)를 선택합니다.

AWS CLI

create-tags 및 delete-tags를 사용합니다.

API

CreateTags 및 DeleteTags를 사용합니다.

엔드포인트 서비스 구성 삭제

엔드포인트 서비스 구성을 삭제할 수 있습니다. 구성을 삭제해도 VPC 또는 연결된 로드 밸런서에 호스팅된 애플리케이션이 삭제되지 않습니다.

엔드포인트 서비스 구성을 삭제하기 전에 서비스에 연결된 `available` 또는 `pending-acceptance` 상태의 모든 VPC 엔드포인트를 거부해야 합니다. 자세한 내용은 섹션을 참조하세요엔드포인트 연결 요청 수락 및 거부 (p. 49)

Console

엔드포인트 서비스 구성을 삭제하려면

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

AWS CLI

엔드포인트 서비스 구성을 삭제하려면

delete-vpc-endpoint-service-configurations 명령을 사용합니다. 서비스의 ID를 지정합니다.

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-
svc-03d5ebb7d9579a2b3
```

Tools for Windows PowerShell

엔드포인트 서비스 구성을 삭제하려면

Remove-EC2EndpointServiceConfiguration을 사용합니다.

API

엔드포인트 서비스 구성을 삭제하려면

DeleteVpcEndpointServiceConfigurations를 사용합니다.

VPC 엔드포인트 및 VPC 엔드포인트 서비스에 대한 ID 및 액세스 관리

IAM을 사용하여 VPC 엔드포인트 및 VPC 엔드포인트 서비스에 대한 액세스를 관리합니다.

VPC 종단점 사용 제어

기본적으로 IAM 사용자에게는 엔드포인트 사용 권한이 없습니다. IAM 사용자 정책을 만들어 사용자에게 엔드포인트를 생성, 수정, 설명, 삭제할 수 있는 권한을 부여할 수 있습니다. 다음은 예제입니다.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

VPC 엔드포인트를 사용하는 서비스에 대한 액세스 제어에 대한 자세한 내용은 the section called “서비스에 대한 액세스 제어” (p. 35) 단원을 참조하세요.

서비스 소유자를 기반으로 VPC 종단점 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 서비스의 프라이빗 DNS 이름

VPC 종단점 서비스를 생성하면 서비스와의 통신에 사용할 수 있는 엔드포인트별 DNS 호스트 이름을 생성합니다. 이러한 이름에는 VPC 엔드포인트 ID, 가용 영역 이름 및 리전 이름(예: vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com)이 포함됩니다. 기본적으로 소비자는 해당 DNS 이름으로 서비스에 액세스하며 일반적으로 애플리케이션 구성을 수정해야 합니다.

엔드포인트 서비스가 AWS 서비스용이거나 AWS Marketplace에 제공된 서비스인 경우, 기본 DNS 이름이 있습니다. 다른 서비스의 경우, 서비스 공급자는 프라이빗 DNS 이름을 구성하여, 소비자가 애플리케이션을 변경하지 않고 기존 DNS 이름을 사용해 서비스에 액세스하도록 할 수 있습니다. 자세한 내용은 섹션을 참조하세요VPC 엔드포인트 서비스 (p. 38)

서비스 공급자는 새 엔드포인트 서비스 또는 기존 엔드포인트 서비스에 대한 프라이빗 DNS 이름을 지정할 수 있습니다. 프라이빗 DNS 이름을 사용하려면 이 기능을 활성화한 다음 프라이빗 DNS 이름을 지정합니다. 소비자가 프라이빗 DNS 이름을 사용할 수 있으려면, 여러분이 도메인/하위 도메인을 제어할 수 있는지 확인해야 합니다. Amazon VPC 콘솔 또는 API를 사용하여 도메인 소유권 확인을 시작할 수 있습니다. 도메인 소유권 확인이 완료되면 소비자는 프라이빗 DNS 이름을 사용하여 엔드포인트에 액세스합니다.

도메인을 확인하려면 퍼블릭 호스팅 이름 또는 퍼블릭 DNS 공급자가 있어야 합니다.

Gateway Load Balancer 엔드포인트에 대해 생성하는 엔드포인트 서비스에는 프라이빗 DNS 이름이 지원되지 않습니다.

상위 수준의 절차는 다음과 같습니다.

1. 프라이빗 DNS 이름을 추가합니다. 자세한 내용은 the section called “인터페이스 엔드포인트에 대한 VPC 종단점 서비스 구성 생성” (p. 44) 또는 the section called “기존 엔드포인트 서비스 프라이빗 DNS 이름 수정” (p. 60) 섹션을 참조하세요.
2. DNS 서버 레코드에 필요한 도메인 확인 값과 도메인 확인 이름을 기록합니다. 자세한 내용은 섹션을 참조하세요the section called “엔드포인트 서비스 프라이빗 DNS 이름 구성 보기” (p. 61)
3. DNS 서버에 레코드를 추가합니다. 자세한 내용은 섹션을 참조하세요the section called “VPC 엔드포인트 서비스 프라이빗 DNS 이름 확인” (p. 59)
4. 프라이빗 DNS 이름을 확인합니다. 자세한 내용은 섹션을 참조하세요the section called “수동으로 엔드포인트 서비스 프라이빗 DNS 이름 도메인 확인 시작” (p. 61)

Amazon VPC 콘솔 또는 Amazon VPC API를 사용하여 확인 프로세스를 관리할 수 있습니다.

- the section called “VPC 엔드포인트 서비스 프라이빗 DNS 이름 확인” (p. 59)
- the section called “기존 엔드포인트 서비스 프라이빗 DNS 이름 수정” (p. 60)
- the section called “엔드포인트 서비스 프라이빗 DNS 이름 제거” (p. 62)
- the section called “엔드포인트 서비스 프라이빗 DNS 이름 구성 보기” (p. 61)
- Amazon VPC 프라이빗 DNS 이름 도메인 확인 TXT 레코드 (p. 63)

도메인 이름 확인 고려 사항

도메인 소유권 확인과 관련된 다음과 같은 중요한 사항을 기록해 둡니다.

- 확인 상태가 확인됨인 경우, 소비자는 프라이빗 DNS 이름만 사용하여 엔드포인트 서비스에 액세스할 수 있습니다.

- 확인 상태가 확인됨에서 pendingVerification 또는 실패로 변경되면 기존 소비자 연결은 유지되지만 새 연결 요청은 거부됩니다.

  Important

  검증된 상태가 아닌 엔드포인트 서비스 연결이 우려되는 서비스 공급자의 경우, DescribeVpcEndpoints를 사용하여 확인 상태를 주기적으로 확인하는 것이 좋습니다. 하루에 한 번 이상 이 검사를 수행하는 것이 좋습니다.
- 엔드포인트 서비스당 프라이빗 DNS 이름은 하나만 있을 수 있습니다.
- 새 엔드포인트 서비스 또는 기존 엔드포인트 서비스에 대해 프라이빗 DNS 이름을 지정할 수 있습니다.
- 퍼블릭 도메인 이름 서버만 사용할 수 있습니다.
- 도메인 이름에 와일드카드(예: "*.myexampleservice.com")를 사용할 수 있습니다.
- 각 엔드포인트 서비스마다 별도의 도메인 소유권 확인 검사를 수행해야 합니다.
- 하위 도메인의 도메인을 확인할 수 있습니다. 예를 들어, a.example.com 대신 example.com을 확인할 수 있습니다. RFC 1034에 지정된 바에 따라 각 DNS 레이블은 최대 63자를 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 추가합니다. 소비자가 이름을 사용할 수 있으려면, 여러분이 example.com 또는 b.example.com 을 확인해야 합니다.
- 도메인 이름은 소문자여야 합니다.

VPC 엔드포인트 서비스 프라이빗 DNS 이름 확인

도메인은 DNS 공급자를 통해 관리하는 DNS(도메인 이름 시스템) 집합과 연결되어 있습니다. TXT 레코드는 도메인에 대한 추가 정보를 제공하는 DNS 레코드 유형입니다. 각 TXT 레코드는 이름과 값으로 구성됩니다.

도메인 소유권 확인을 시작하면 TXT 레코드에 사용할 이름과 값을 제공해 드립니다. 예를 들어 도메인이 myexampleservice.com이면, 생성되는 TXT 레코드 설정은 다음 예와 같습니다.

엔드포인트 프라이빗 DNS 이름 TXT 레코드

도메인 확인 이름	Type	도메인 확인 값
_vpce:aksldja21i1	TXT	vpce:asjdakjshd78126eu21

지정된 도메인 확인 이름과 도메인 확인 값을 사용하여 도메인의 DNS 서버에 TXT 레코드를 추가합니다. 도메인의 DNS 설정에 TXT 레코드가 있다는 것이 확인되면 도메인 소유권 확인이 완료됩니다.

DNS 공급자가 DNS 레코드 이름에 밑줄 사용을 허용하지 않는 경우, 도메인 확인 이름에서 _aksldja21i1을 생략할 수 있습니다. 이 경우 앞의 예에서 TXT 레코드 이름은 _aksldja21i1.myexampleservice.com이 아닌 myexampleservice.com이 됩니다.

도메인의 DNS 서버에 TXT 레코드 추가

도메인의 DNS 서버에 TXT 레코드를 추가하는 절차는 DNS 서비스를 제공하는 대상에 따라 다릅니다. DNS 공급자가 Amazon Route 53 또는 다른 도메인 이름 등록자일 수 있습니다. 이 단원에서는 Route 53에 TXT 레코드를 추가하는 절차와, 다른 DNS 공급자에게 적용되는 일반 절차를 제공합니다.

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

4. 세부 정보 탭에서 도메인 확인 값 및 도메인 확인 이름 옆에 표시된 값을 확인합니다.
5. 확인하려는 도메인에 대해 Route 53에서 DNS 서비스를 제공할 경우 Route 53에 사용하는 것과 같은 계정으로 AWS Management Console에 로그인하면 Amazon VPC 콘솔에서 즉시 DNS 서버를 업데이트하는 옵션을 사용할 수 있습니다.

   다른 DNS 공급자를 사용하는 경우 DNS 레코드를 업데이트하는 절차는 사용하는 DNS 또는 웹 호스팅 공급자에 따라 달라집니다. 다음 표에 몇몇 일반적인 공급자의 설명서 링크가 나와 있습니다. 이 목록에 모든 공급자가 빠짐없이 포함된 것은 아니며, 이 목록에 포함되어 있다고 해서 어떤 회사의 제품 또는 서비스를 승인 또는 추천하는 것은 아닙니다. 공급자가 표에 없으면 엔드포인트를 통해 도메인을 사용할 수도 있습니다.

DNS/호스팅 공급자	설명서 링크
GoDaddy	Add a TXT record(외부 링크)
Dreamhost	사용자 지정 DNS 레코드를 추가하는 방법(외부 링크)
Cloudflare	Managing DNS records in CloudFlare(외부 링크)
HostGator	HostGator/eNom을 통한 DNS 레코드 관리(외부 링크)
Namecheap	도메인에서 TXT/SPF/DKIM/DMARC 레코드를 추가하는 방법(외부 링크)
Names.co.uk	도메인 DNS 설정 변경(외부 링크)
Wix	Adding or Updating TXT Records in Your Wix Account(외부 링크)

   확인이 완료되면 Amazon VPC 콘솔의 도메인 상태가 Pending(대기 중)에서 Verified(확인됨)으로 변경됩니다.
6. 이제 VPC 엔드포인트 서비스에 프라이빗 도메인 이름을 사용할 수 있습니다.

DNS 설정이 올바르게 업데이트되지 않으면, 도메인 상태가 세부 정보 탭에 실패로 표시됩니다. 이러한 상황이 발생할 경우, the section called “일반적인 도메인 확인 문제 해결” (p. 64)에서 문제 해결 페이지의 단계를 완료하십시오. TXT 레코드가 올바르게 만들어졌는지 확인한 후 작업을 다시 시도하십시오.

기존 엔드포인트 서비스 프라이빗 DNS 이름 수정

신규 또는 기존 엔드포인트 서비스에 대한 엔드포인트 서비스 프라이빗 DNS 이름을 수정할 수 있습니다.

이름을 업데이트한 후 DNS 서버의 도메인 항목을 업데이트합니다. DNS 서버가 자동으로 폴링되어 서버에 레코드가 있는지 확인합니다. DNS 레코드 업데이트가 적용되려면 최대 48시간이 걸릴 수 있지만, 대개는 이보다 훨씬 더 빨리 적용됩니다. 자세한 내용은 the section called “프라이빗 DNS 이름 도메인 확인 TXT 레코드” (p. 63) 및 the section called “VPC 엔드포인트 서비스 프라이빗 DNS 이름 확인” (p. 59) 단원을 참조하십시오.

Console

엔드포인트 서비스 프라이빗 DNS 이름을 수정하려면

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

2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 작업, 프라이빗 DNS 이름 수정을 선택합니다.
4. 프라이빗 DNS 이름을 서비스와 연결(Associate a private DNS name with the serivce)을 선택하고 프라이빗 DNS 이름을 입력합니다.
5. [Save changes]를 선택합니다.

AWS CLI

엔드포인트 서비스 프라이빗 DNS 이름을 수정하려면

modify-vpc-endpoint-service-configuration을 사용합니다.

API

엔드포인트 서비스 프라이빗 DNS 이름을 수정하려면

ModifyVpcEndpointServiceConfiguration을 사용합니다.

엔드포인트 서비스 프라이빗 DNS 이름 구성 보기

엔드포인트 서비스에 대한 엔드포인트 서비스 프라이빗 DNS 이름을 볼 수 있습니다.

Console

엔드포인트 서비스 프라이빗 DNS 이름 구성을 보려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Endpoint Services]를 선택한 후 엔드포인트 서비스를 선택합니다.
3. 세부 정보 탭에는 프라이빗 DNS 도메인 소유권 검사에 대한 다음 정보가 표시됩니다.
   - 도메인 확인 상태: 확인 상태.
   - 도메인 확인 유형: 확인 유형.
   - 도메인 확인 값: DNS 값.
   - 도메인 확인 이름: 레코드 하위 도메인의 이름.

AWS CLI

엔드포인트 서비스 프라이빗 DNS 이름 구성을 보려면

describe-vpc-endpoint-service-configurations를 사용합니다.

API

엔드포인트 서비스 프라이빗 DNS 이름 구성을 보려면

DescribeVpcEndpointServiceConfigurations를 사용합니다.

수동으로 엔드포인트 서비스 프라이빗 DNS 이름 도메인 확인 시작

소비자가 프라이빗 DNS 이름을 사용할 수 있으려면, 서비스 공급자가 프라이빗 DNS 이름 도메인 소유 사실을 증명해야 합니다.

Console

프라이빗 DNS 이름 도메인의 확인 프로세스를 시작하려면

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

   DNS 설정이 올바르게 업데이트되지 않으면 도메인 확인 상태가 실패(failed)가 됩니다. 이러한 상황이 발생할 경우, the section called “일반적인 도메인 확인 문제 해결” (p. 64)에서 문제 해결 페이지의 단계를 완료하세요.

AWS CLI

프라이빗 DNS 이름 도메인의 확인 프로세스를 시작하려면

start-vpc-endpoint-service-private-dns-verification을 사용합니다.

API

프라이빗 DNS 이름 도메인의 확인 프로세스를 시작하려면

StartVpcEndpointServicePrivateDnsVerification을 사용합니다.

엔드포인트 서비스 프라이빗 DNS 이름 제거

서비스에 대한 연결이 없어야 엔드포인트 서비스 프라이빗 DNS 이름을 제거할 수 있습니다.

Console

엔드포인트 서비스 프라이빗 DNS 이름을 제거하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택한 다음 작업, 프라이빗 DNS 이름 수정을 선택합니다.
4. 프라이빗 DNS 이름을 서비스에 연결(Associate a private DNS name with the service)을 취소합니다.
5. [Save changes]를 선택합니다.

AWS CLI

엔드포인트 서비스 프라이빗 DNS 이름을 제거하려면

modify-vpc-endpoint-service-configuration을 사용합니다.

API

엔드포인트 서비스 프라이빗 DNS 이름을 제거하려면

ModifyVpcEndpointServiceConfiguration을 사용합니다.

Amazon VPC 프라이빗 DNS 이름 도메인 확인 TXT 레코드

도메인은 DNS 공급자를 통해 관리하는 DNS(도메인 이름 시스템) 집합과 연결되어 있습니다. TXT 레코드는 도메인에 대한 추가 정보를 제공하는 DNS 레코드 유형입니다. 각 TXT 레코드는 이름과 값으로 구성됩니다.

Amazon VPC 콘솔 또는 API를 사용하여 도메인 소유권 확인을 시작하면 AWS에서 TXT 레코드에 사용할 이름과 값을 제공합니다. 예를 들어 도메인이 myexampleservice.com이면 Amazon VPC에서 생성하는 TXT 레코드 설정은 다음과 비슷한 형식이 됩니다.

엔드포인트 프라이빗 DNS 이름 TXT 레코드

도메인 확인 이름	Type	도메인 확인 값
_vpce:aksldja21i1.myexampleservice.com	TXT	vpce:asjdakjshd78126eu21

지정된 도메인 확인 이름과 도메인 확인 값을 사용하여 도메인의 DNS 서버에 TXT 레코드를 추가합니다. Amazon VPC에서 도메인의 DNS 설정에 TXT 레코드가 있음을 감지하면 Amazon VPC 도메인 소유권 확인이 완료됩니다.

DNS 공급자가 DNS 레코드 이름에 밑줄 사용을 허용하지 않는 경우, 도메인 이름을 도메인 확인 이름으로 사용할 수 있습니다. 이 경우 앞의 예제에서 TXT 레코드 이름은 myexampleservice.com이 됩니다.

도메인 소유권 확인 설정을 확인하는 방법에 대한 문제 해결 정보와 지침은 일반적인 프라이빗 DNS 도메인 확인 문제 해결 (p. 64)에서 찾아볼 수 있습니다.

Amazon Route 53

도메인의 DNS 서버에 TXT 레코드를 추가하는 절차는 DNS 서비스를 제공하는 대상에 따라 다릅니다. DNS 공급자가 Amazon Route 53 또는 다른 도메인 이름 등록자일 수 있습니다. 이 단원에서는 Route 53에 TXT 레코드를 추가하는 절차와, 다른 DNS 공급자에게 적용되는 일반 절차를 제공합니다.

Route 53 관리형 도메인의 DNS 레코드에 TXT 레코드를 추가하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 엔드포인트 서비스를 선택합니다.
3. 엔드포인트 서비스를 선택합니다.
4. 세부 정보 탭에서 도메인 확인 값 및 도메인 확인 이름 옆에 표시된 값을 확인합니다.
5. Amazon Route 53 콘솔에서 호스팅 영역에 대한 레코드를 생성합니다. 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서에서 Amazon Route 53 콘솔을 사용하여 레코드 생성을 참조하세요. 다음 값을 사용합니다.
   - [레코드 유형(Record type)]에 대해 [TXT]를 선택합니다.
   - TTL(초)에 **1800**을 입력합니다.
   - [라우팅 정책(Routing policy)]에 대해 [단순 라우팅(Simple routing)]을 선택합니다.
   - [값/트래픽 라우팅 대상(Value/Route traffic to)]에 Amazon VPC의 [도메인 확인 값(Domain verification value)]을 입력합니다.
6. Amazon VPC 콘솔에 있는 엔드포인트 서비스 페이지의 세부 정보 탭에서 엔드포인트 옆에 있는 도메인 확인 상태(Domain verification status) 열의 값을 확인합니다. 상태가 "확인 보류 중"인 경우 몇 분 더 기다렸다가 새로 고침을 선택합니다. 상태 열의 값이 "verified(확인됨)"가 될 때까지 이 과정을 반복합니다. 확인 프로세스를 수동으로 시작할 수 있습니다. 자세한 내용은 섹션을 참조하세요the section called “수동으로 엔드포인트 서비스 프라이빗 DNS 이름 도메인 확인 시작” (p. 61)

Generic procedures for other DNS providers

DNS 구성에 TXT 레코드를 추가하는 절차는 공급자마다 다릅니다. 구체적인 단계는 DNS 공급자의 설명서를 확인하세요. 이 섹션의 절차는 도메인의 DNS 구성에 TXT 레코드를 추가할 때 따라야 할 단계의 기본 개요를 제공합니다.

도메인의 DNS 서버에 TXT 레코드를 추가하려면(일반 절차)

1. DNS 공급자의 웹 사이트로 이동합니다. 도메인을 제공하는 DNS 공급자를 잘 모를 경우, 무료 Whois service를 사용하여 찾아볼 수 있습니다.
2. 공급자의 웹 사이트에서 계정에 로그인합니다.
3. 도메인의 DNS 레코드를 업데이트하는 페이지를 찾습니다. 이 페이지의 이름은 보통 DNS Records, DNS Zone File 또는 Advanced DNS 같은 이름입니다. 확실하지 않다면 공급자의 설명서를 확인하십시오.
4. 에서 제공한 이름과 값이 포함된 TXT 레코드를 추가합니다AWS

   Important

   일부 DNS 공급자는 DNS 레코드의 끝에 도메인 이름을 자동으로 추가합니다. 도메인 이름(예: _pmBGN/7Mjnf.example.com)을 이미 포함하고 있는 레코드를 추가하면 도메인 이름이 중복될 수 있습니다(예: _pmBGN/7Mjnfexample.com.example.com). 도메인 이름 중복을 방지하려면 DNS 레코드의 도메인 이름 끝에 마침표를 추가하십시오. 이를 통해 DNS 공급자에게 레코드 이름이 정규화되었다는 것을 알리고(즉 도메인 이름과 더 이상 관련이 없음), DNS 공급자가 도메인 이름을 추가하는 것을 방지할 수 있습니다.
5. 변경 내용을 저장합니다. DNS 레코드 업데이트가 적용되려면 최대 48시간이 걸릴 수 있지만, 대개는 이보다 훨씬 더 빨리 적용됩니다.

일반적인 프라이빗 DNS 도메인 확인 문제 해결

Amazon VPC로 엔드포인트 서비스 프라이빗 DNS 도메인 이름을 확인하려면 Amazon VPC 콘솔이나 API를 사용하여 프로세스를 시작합니다. 이 단원에는 확인 절차 관련 문제를 해결하는 데 도움이 될 수 있는 정보가 포함되어 있습니다.

일반적인 도메인 확인 문제

도메인을 확인하려고 할 때 문제가 발생하면 아래의 가능한 원인과 해결 방법을 검토하십시오.

- 소유하지 않은 도메인을 확인하려고 합니다. 도메인을 소유하지 않으면 도메인을 확인할 수 없습니다.
- DNS 공급자는 TXT 레코드 이름에 밑줄을 허용하지 않습니다. 일부 DNS 공급자는 도메인의 DNS 레코드 이름에 밑줄 문자를 포함하도록 허용하지 않습니다. 공급자에게 해당되는 경우 TXT 레코드 이름에서 _amazovpc를 생략할 수 있습니다.
- DNS 공급자가 TXT 레코드 끝에 도메인 이름을 추가했습니다. 일부 DNS 공급자는 도메인 이름을 TXT 레코드의 속성 이름에 자동으로 추가합니다. 예를 들어 속성 이름이 _amazonvpc.example.com인 레코드를 생성하는 경우 공급자는 도메인 이름을 추가하여 _amazonvpc.example.com.example.com을 생성할 수 있습니다. 도메인 이름의 중복을 방지하려면 TXT 레코드를 생성할 때 도메인 이름의 끝에 마침표를 추가합니다. 이 단계에서는 TXT 레코드에 도메인 이름을 추가할 필요가 없음을 DNS 공급자에게 알려줍니다.
- DNS 공급자가 DNS 레코드 값을 수정했습니다. 일부 공급자는 소문자만 사용하도록 DNS 레코드 값을 자동으로 수정합니다. AWS는 도메인 확인 절차를 시작할 때 AWS가 제공한 값과 속성 값이 정확히 일치하는 확인 레코드를 감지한 경우에만 도메인을 확인합니다. 도메인에 대한 DNS 공급자가 소문자만 사용하도록 TXT 레코드 값을 변경하는 경우 DNS 공급자에게 연락하여 추가 지원을 요청하십시오.
- 동일한 도메인을 여러 번 확인하려고 합니다. 여러 리전에서 전송하거나 동일한 도메인을 사용하여 여러 AWS 계정에서 전송하기 때문에 도메인을 여러 번 확인해야 할 수 있습니다. DNS 공급자가 속성 이름이 동일한 TXT 레코드를 두 개 이상 허용하지 않는 경우 두 개의 도메인을 확인할 수 있습니다. DNS 공급자가 이를 허용하는 경우 동일한 TXT 레코드에 여러 속성 값을 할당할 수 있습니다. 예를 들어 Amazon

Route 53에서 사용자의 DNS를 관리하는 경우 사용자는 다음 단계를 완료하여 동일한 TXT 레코드에 여러 값을 설정할 수 있습니다.

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

DNS 공급자가 동일한 TXT 레코드에 여러 값을 할당하도록 허용하지 않는 경우 TXT 레코드의 속성 이름에서 도메인을 값으로 한 번 확인한 후 다음 번 확인할 때는 속성 이름에서 값을 제거합니다. 예를 들어, "_asnbcdasd"로 확인한 다음 "asnbcdasd"로 확인합니다. 이 솔루션의 단점은 동일한 도메인을 두 번만 확인할 수 있다는 것입니다.

도메인 확인 설정을 확인하는 방법

다음 절차를 사용하여 프라이빗 DNS 이름 도메인 소유권 확인 TXT 레코드가 DNS 서버에 올바르게 게시되었는지 확인할 수 있습니다. 이 절차는 Windows 및 Linux에서 사용 가능한 nslookup 도구를 사용합니다. Linux의 경우, dig도 사용할 수 있습니다.

이 지침에서 명령은 Windows 7에서 실행되며 사용된 예제 도메인은 example.com입니다.

이 절차에서, 먼저 사용자의 도메인에 서비스하는 DNS 서버를 찾은 후 해당 서버에 TXT 레코드를 보기 위한 쿼리를 전송합니다. 사용자의 도메인에 서비스하는 DNS 서버로 쿼리하는 이유는 이들 서버가 도메인에 대한 가장 최신 정보를 포함하고 있으며, 이 정보가 다른 DNS 서버로 전파되려면 시간이 걸릴 수 있기 때문입니다.

도메인 소유권 확인 TXT 레코드가 올바로 DNS 서버에 게시되었는지 확인하려면

1. 다음 단계에 따라 도메인의 이름 서버를 찾습니다.
   a. 명령줄로 이동합니다. Windows 7에서 명령줄로 이동하려면 시작을 선택하고 cmd를 입력하십시오. Linux 기반 운영 체제에서, 터미널 창을 엽니다.
   b. 명령 프롬프트에서 다음을 입력합니다. 여기서 <domain>은 사용자의 도메인입니다.

      ```
      nslookup -type=NS <domain>
      ```

      예를 들어 도메인이 example.com인 경우 명령은 다음과 같습니다.

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

      이 명령의 출력은 사용자의 도메인에 서비스하는 모든 이름 서버를 나열합니다. 다음 단계에서 이들 서버 중 하나에 쿼리합니다.
2. 다음 단계에 따라 TXT 레코드가 올바로 게시되었는지 확인합니다.
   a. 명령 프롬프트에서 다음을 입력합니다. 여기서 <domain>은 사용자의 도메인이고 <name server>는 1단계에서 검색한 이름 서버 중 하나입니다.

      ```
      nslookup -type=TXT  _aksldja21i1.<domain> <name server>
      ```

      _aksldja21i1.example.com 예에서, 1단계에서 검색된 이름 서버가 ns1.name-server.net이라면 다음을 입력합니다.

      ```
      nslookup -type=TXT  _aksldja21i1.example.com ns1.name-server.net
      ```

   b. 명령의 출력에서 `text =` 이하의 문자열이 Amazon VPC 콘솔의 자격 증명 목록에서 도메인을 선택하면 표시되는 TXT 값과 일치하는지 확인합니다.

예에서는 _aksldja21i1.example.com 값이 `asjdakjshd78126eu21`인 TXT 레코드를 찾습니다. 이 레코드가 올바로 게시되었다면 명령이 다음을 출력할 것으로 기대할 수 있습니다.

```
_aksldja21i1.example.com text = "asjdakjshd78126eu21"
```

AWS PrivateLink와 통합되는 AWS 서비스

다음 서비스가 AWS PrivateLink와 통합됩니다. 인터페이스 엔드포인트 (p. 3)를 생성하여 이러한 서비스에 연결할 수 있습니다.

서비스가 AWS PrivateLink와 통합되지만 VPC 엔드포인트 정책을 지원하지 않는 경우 [VPC 엔드포인트 정책(VPC endpoint policies)] 열에 '⊗ 아니요(No)'가 표시됩니다. VPC 종단점 정책을 지원하는 서비스에 대한 설명서를 보려면 "예" 링크를 선택합니다.

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
Amazon API Gateway	✓ 예	com.amazonaws.region.execute-api
Amazon AppIntegrations	✓ 예	com.amazonaws.region.app-integrations
AWS App Mesh	⊗ 아니요	com.amazonaws.region.appmesh-envoy-management
AWS App Runner	✓ 예	com.amazonaws.region.apprunner
Application Auto Scaling	✓ 예	com.amazonaws.region.application-autoscaling
AWS Application Discovery Service	⊗ 아니요	com.amazonaws.region.awsconnector
AWS 애플리케이션 마이그레이션 서비스	✓ 예	com.amazonaws.region.mgn
Amazon AppStream 2.0	⊗ 아니요	com.amazonaws.region.appstream.api
		com.amazonaws.region.appstream.streaming
Amazon Athena	✓ 예	com.amazonaws.region.athena
AWS Audit Manager	✓ 예	com.amazonaws.region.auditmanager
Amazon Aurora	✓ 예	com.amazonaws.region.rds
AWS Auto Scaling	✓ 예	com.amazonaws.region.autoscaling-plans
Amazon Braket	✓ 예	com.amazonaws.region.braket
AWS Certificate Manager Private Certificate Authority	✓ 예	com.amazonaws.region.acm-pca
Amazon Cloud Directory	✓ 예	com.amazonaws.region.clouddirectory
AWS CloudFormation	⊗ 아니요	com.amazonaws.region.cloudformation
AWS CloudHSM	✓ 예	com.amazonaws.region.cloudhsmv2

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
AWS CloudTrail	⊗아니요	com.amazonaws.region.cloudtrail
Amazon CloudWatch	✓ 예	com.amazonaws.region.monitoring
		com.amazonaws.region.synthetics
Amazon CloudWatch Events	✓ 예	com.amazonaws.region.events
Amazon CloudWatch Logs	✓ 예	com.amazonaws.region.logs
AWS CodeArtifact	✓ 예	com.amazonaws.region.codeartifact.api
		com.amazonaws.region.codeartifact.repositories
AWS CodeBuild	✓ 예	com.amazonaws.region.codebuild
		com.amazonaws.region.codebuild-fips
AWS CodeCommit	✓ 예	com.amazonaws.region.codecommit
		com.amazonaws.region.codecommit-fips
		com.amazonaws.region.git-codecommit
		com.amazonaws.region.git-codecommit-fips
AWS CodeDeploy	✓ 예	com.amazonaws.region.codedeploy
		com.amazonaws.region.codedeploy-commands-secure
Amazon CodeGuru Profiler	⊗아니요	com.amazonaws.region.codeguru-profiler
Amazon CodeGuru Reviewer	⊗아니요	com.amazonaws.region.codeguru-reviewer
AWS CodePipeline	⊗아니요	com.amazonaws.region.codepipeline
AWS CodeStar 연결	✓ 예	com.amazonaws.region.codestar-connections.api
Amazon Comprehend	✓ 예	com.amazonaws.region.comprehend
Amazon Comprehend Medical	✓ 예	com.amazonaws.region.comprehendmedical
AWS Config	✓ 예	com.amazonaws.region.config
Amazon Connect Customer Profiles	✓ 예	com.amazonaws.region.profile
Amazon Connect 음성 ID	✓ 예	com.amazonaws.region.voiceid
AWS Database Migration Service	✓ 예	com.amazonaws.region.dms
		com.amazonaws.region.dms-fips

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
AWS Data Exchange	✓ 예	com.amazonaws.region.dataexchange
AWS DataSync	✗ 아니요	com.amazonaws.region.datasync
AWS Device Farm	✗ 아니요	
Amazon DevOps Guru	✓ 예	com.amazonaws.region.devops-guru
Amazon EBS 다이렉트 API	✗ 아니요	com.amazonaws.region.ebs
Amazon EC2	✓ 예	com.amazonaws.region.ec2
EC2 Image Builder	✓ 예	com.amazonaws.region.imagebuilder
Amazon EC2 Auto Scaling	✓ 예	com.amazonaws.region.autoscaling
AWS Elastic Beanstalk	✓ 예	com.amazonaws.region.elasticbeanstalk
		com.amazonaws.region.elasticbeanstalk-health
Amazon Elastic File System	✓ 예	com.amazonaws.region.elasticfilesystem
		com.amazonaws.region.elasticfilesystem-fips
Elastic Load Balancing	✓ 예	com.amazonaws.region.elasticloadbalancing
Amazon Elastic 컨테이너 레지스트리	✓ 예	com.amazonaws.region.ecr.api
		com.amazonaws.region.ecr.dkr
Amazon Elastic Container Service	✓ 예	com.amazonaws.region.ecs
		com.amazonaws.region.ecs-agent
		com.amazonaws.region.ecs-telemetry
AWS Elastic Disaster Recovery	✓ 예	com.amazonaws.region.drs
AWS Elastic Inference	✗ 아니요	com.amazonaws.region.elastic-inference.runtime
Amazon EMR	✓ 예	com.amazonaws.region.elasticmapreduce
Amazon EMR on EKS	✓ 예	com.amazonaws.region.emr-containers
Amazon EventBridge	✓ 예	com.amazonaws.region.events
AWS Fault Injection Simulator	✓ 예	com.amazonaws.region.fis
Amazon FinSpace	✓ 예	com.amazonaws.region.finspace
		com.amazonaws.region.finspace-api

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
Amazon Fraud Detector	✓ 예	com.amazonaws.region.frauddetector
AWS Glue	✓ 예	com.amazonaws.region.glue
AWS Glue DataBrew	✓ 예	com.amazonaws.region.databrew
AWS Ground Station	✓ 예	com.amazonaws.region.groundstation
IAM Access Analyzer	✓ 예	com.amazonaws.region.access-analyzer
Amazon HealthLake	✓ 예	com.amazonaws.region.healthlake
AWS IoT Core	✗ 아니요	com.amazonaws.region.iot.data
AWS IoT Core for LoRaWAN	✗ 아니요	com.amazonaws.region.iotwireless.api
		com.amazonaws.region.lorawan.cups
		com.amazonaws.region.lorawan.lns
AWS IoT Greengrass	✓ 예	com.amazonaws.region.greengrass
AWS IoT SiteWise	✗ 아니요	com.amazonaws.region.iotsitewise.api
		com.amazonaws.region.iotsitewise.data
Amazon Kendra	✓ 예	com.amazonaws.region.kendra
AWS Key Management Service	✓ 예	com.amazonaws.region.kms
Amazon Keyspaces(Apache Cassandra 용)	✓ 예	com.amazonaws.region.cassandra
		com.amazonaws.region.cassandra-fips
Amazon Kinesis Data Firehose	✓ 예	com.amazonaws.region.kinesis-firehose
Amazon Kinesis Data Streams	✓ 예	com.amazonaws.region.kinesis-streams
AWS Lake Formation	✓ 예	com.amazonaws.region.lakeformation
AWS Lambda	✓ 예	com.amazonaws.region.lambda
AWS License Manager	✓ 예	com.amazonaws.region.license-manager
		com.amazonaws.region.license-manager-fips
Amazon Lookout for Equipment	✓ 예	com.amazonaws.region.lookoutequipment
Amazon Lookout for Metrics	✓ 예	com.amazonaws.region.lookoutmetrics
Amazon Lookout for Vision	✓ 예	com.amazonaws.region.lookoutvision

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
Amazon Macie	✓ 예	com.amazonaws.region.macie2
Amazon Managed Blockchain	✗ 아니요	
Amazon Managed Service for Prometheus	✗ 아니요	com.amazonaws.region.aps
		com.amazonaws.region.aps-workspaces
Amazon Managed Workflows for Apache Airflow	✓ 예	com.amazonaws.region.airflow.api
		com.amazonaws.region.airflow.env
		com.amazonaws.region.airflow.ops
Amazon Nimble Studio	✓ 예	com.amazonaws.region.nimble
AWS Proton	✓ 예	com.amazonaws.region.proton
Amazon QLDB	✓ 예	com.amazonaws.region.qldb.session
Amazon RDS	✓ 예	com.amazonaws.region.rds
Amazon RDS Data API	✓ 예	com.amazonaws.region.rds-data
Amazon Redshift	✓ 예	com.amazonaws.region.redshift
		com.amazonaws.region.redshift-data
		com.amazonaws.region.redshift-fips
Amazon Rekognition	✓ 예	com.amazonaws.region.rekognition
		com.amazonaws.region.rekognition-fips
Amazon S3	✓ 예	com.amazonaws.region.s3
Amazon S3의 다중 리전 액세스 포인트	✓ 예	com.amazonaws.s3-global.accesspoint
Amazon SageMaker	✓ 예	aws.sagemaker.region.notebook
		aws.sagemaker.region.studio
		com.amazonaws.region.sagemaker.api
		com.amazonaws.region.sagemaker.featurestore-runtime
		com.amazonaws.region.sagemaker.runtime
		com.amazonaws.region.sagemaker.runtime-fips
AWS Secrets Manager	✓ 예	com.amazonaws.region.secretsmanager
AWS Security Hub	✓ 예	com.amazonaws.region.securityhub

AWS 서비스	VPC 엔드포인트 정책	서비스 이름
AWS Security Token Service	✓ 예	com.amazonaws.region.sts
AWS Server Migration Service	✗ 아니요	com.amazonaws.region.sms
		com.amazonaws.region.sms-fips
AWS Service Catalog	✗ 아니요	com.amazonaws.region.servicecatalog
		com.amazonaws.region.servicecatalog-appregistry
Amazon SES	✗ 아니요	com.amazonaws.region.email-smtp
Amazon SNS	✓ 예	com.amazonaws.region.sns
Amazon SQS	✓ 예	com.amazonaws.region.sqs
AWS Snow Device Management	✓ 예	com.amazonaws.region.snow-device-management
AWS Step Functions	✓ 예	com.amazonaws.region.states
		com.amazonaws.region.sync-states
AWS Systems Manager	✓ 예	com.amazonaws.region.ec2messages
		com.amazonaws.region.ssm
		com.amazonaws.region.ssmmessages
AWS Storage Gateway	✗ 아니요	com.amazonaws.region.storagegateway
Amazon Textract	✓ 예	com.amazonaws.region.textract
		com.amazonaws.region.textract-fips
Amazon Transcribe	✓ 예	com.amazonaws.region.transcribe
		com.amazonaws.region.transcribestreaming
Amazon Transcribe Medical	✓ 예	com.amazonaws.region.transcribe
		com.amazonaws.region.transcribestreaming
AWS Transfer for SFTP	✗ 아니요	com.amazonaws.region.transfer
		com.amazonaws.region.transfer.server
Amazon WorkSpaces	✓ 예	com.amazonaws.region.workspaces
AWS X-Ray	✓ 예	com.amazonaws.region.xray

사용 가능한 AWS 서비스 이름 보기

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

다음 명령을 실행하여 게이트웨이 또는 인터페이스 엔드포인트에 대한 서비스 이름 목록을 가져올 수 있습니다. `service-type` 필터에 사용할 수 있는 값은 `Interface` 및 `Gateway`입니다. 이 `--query` 옵션은 출력을 서비스 이름으로 제한합니다.

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=service-type --
query ServiceNames
```

다음 예제에서는 인터페이스 엔드포인트를 지원하는 서비스를 표시합니다.

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=Interface --query
 ServiceNames
```

다음은 예제 출력입니다.

```
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.acm-pca",
    "com.amazonaws.us-east-1.airflow.api",
    "com.amazonaws.us-east-1.airflow.env",
    "com.amazonaws.us-east-1.airflow.ops",
    "com.amazonaws.us-east-1.application-autoscaling",
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.athena",
...
```

서비스 이름이 표시된 후에 다음 명령을 사용하여 자세한 정보를 볼 수 있습니다.

```
aws ec2 describe-vpc-endpoint-services --service-name service-name
```

다음 예에서는 `us-east-1` 리전의 Amazon S3 인터페이스 엔드포인트에 대한 정보를 표시합니다. `service-type` 필터는 출력에서 Amazon S3 게이트웨이 엔드포인트를 제외합니다.

```
aws ec2 describe-vpc-endpoint-services --service-name "com.amazonaws.us-east-1.s3" --filter
 Name=service-type,Values=Interface --region us-east-1
```

다음은 예제 출력입니다.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.s3",
            "ServiceId": "vpce-svc-081d84efcdc7bac15",
            "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": [
                "s3.us-east-1.vpce.amazonaws.com"
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": []
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.s3"
    ]
}
```

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, AWS는 리전에 있는 모든 리소스의 할당량을 증가시킵니다.

이름(Name)	기본값	조정 가능	설명
리전당 게이트웨이 VPC 엔드포인트	20	예	VPC당 게이트웨이 엔드포인트는 255개로 제한됩니다.
VPC당 인터페이스 및 Gateway Load Balancer 엔드포인트	50	예	VPC의 인터페이스 엔드포인트 및 Gateway Load Balancer 엔드포인트에 대한 결합된 할당량입니다.
VPC 엔드포인트 정책 크기	20,480자	아니요	VPC 엔드포인트 정책의 크기는 공백을 포함합니다.

다음 사항은 VPC 엔드포인트를 통과하는 트래픽에 적용됩니다.

- 기본적으로 각 인터페이스 엔드포인트는 가용 영역당 최대 10Gbps의 대역폭과 최대 40Gbp의 버스트를 지원할 수 있습니다. 애플리케이션에 더 높은 버스트 또는 지속적인 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.
- VPC 엔드포인트에서 FRAG_NEEDEDICMP 패킷을 생성하지 않으므로 경로 MTU 검색(PMTUD)이 지원되지 않습니다.
- VPC 엔드포인트는 모든 패킷에 대해 최대 세그먼트 크기(MSS) 클램핑을 적용합니다. 자세한 내용은 RFC879를 참조하세요.