사용자 가이드

AWS Direct Connect

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Direct Connect: 사용자 가이드

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

의 상표 및 브랜드 디자인은 외 제품 또는 서비스와 함께, 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. 이 소유하지 않은 기타 모든 상표는 과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

이게 뭐야 AWS Direct Connect? 1
- AWS Direct Connect 구성 요소 2
- 네트워크 요구 사항 2
- AWS Direct Connect요금 3
- AWS Direct Connect 유지 관리 4
- 다이렉트 커넥트 유지 관리 5
- 원격 AWS 리전 액세스 6
  - 원격 리전의 퍼블릭 서비스 액세스 6
  - 원격 리전의 VPC 액세스 6
  - 네트워크와 Amazon VPC 간 연결 옵션 7
- 라우팅 정책 및 BGP 커뮤니티 7
  - 퍼블릭 가상 인터페이스 라우팅 정책 7
  - 퍼블릭 가상 인터페이스 BGP 커뮤니티 8
  - 프라이빗 가상 인터페이스 및 전송 가상 인터페이스 라우팅 정책 10
  - 프라이빗 가상 인터페이스 라우팅 예제 12

AWS Direct Connect 복원력 툴킷을 사용하여 시작하기 14
- 사전 조건 15
- 최대 복원성 17
  - 1단계: AWS 가입 19
  - 2단계: 복원 모델 구성 20
  - 3단계: 가상 인터페이스 생성 21
  - 4단계: 가상 인터페이스 복원력 구성 확인 28
  - 5단계: 가상 인터페이스 연결 확인 28
- 높은 복원성 29
  - 1단계: AWS 가입 31
  - 2단계: 복원 모델 구성 32
  - 3단계: 가상 인터페이스 생성 33
  - 4단계: 가상 인터페이스 복원력 구성 확인 40
  - 5단계: 가상 인터페이스 연결 확인 40
- 개발 및 테스트 41
  - 1단계: AWS 가입 42
  - 2단계: 복원 모델 구성 44
  - 3단계: 가상 인터페이스 생성 45
  - 4단계: 가상 인터페이스 복원력 구성 확인 53

5단계: 가상 인터페이스 확인 53
클래식 54
사전 조건 54
1단계: AWS 가입 55
2단계: AWS Direct Connect 전용 연결 요청 56
(전용 연결) 3단계: LOA-CFA 다운로드 58
4단계: 가상 인터페이스 생성 59
5단계: 라우터 구성 다운로드 67
6단계: 가상 인터페이스 확인 68
(권장 사항) 7단계: 중복 연결 구성 68
AWS Direct Connect 장애 조치 테스트 70
테스트 기록 71
검증 권한 71
가상 인터페이스 장애 조치 테스트 시작 71
가상 인터페이스 장애 조치 테스트 기록 보기 72
가상 인터페이스 장애 조치 테스트 중지 73
MAC 보안 74
MACsec 개념 74
지원되는 연결 75
전용 연결에서 MACsec으로 시작하기 75
MACsec 전제 조건 76
서비스 연결 역할 76
MACsec에서 사전 공유한 CKN/CAK 주요 고려 사항 76
1단계: 연결 생성 77
(선택 사항) 2단계: 링크 집계 그룹 (LAG) 생성 77
3단계: CKN/CAK를 연결 또는 LAG에 연결 77
4단계: 온프레미스 라우터 구성 77
5단계: (선택 사항) CKN/CAK와 연결 또는 LAG 간의 연결 제거 77
연결 79
전용 연결 79
연결 마법사를 사용하여 연결 생성 80
Classic 연결 생성 82
LOA-CFA를 다운로드 83
연결 업데이트 85
MACsec CKN/CAK를 연결에 연결 86
MACsec 암호 키와 연결 사이의 연결을 제거합니다 87

호스팅 연결 ... 88
호스팅 연결 수락 ... 89
연결 세부 정보 보기 ... 89
연결 삭제 ... 90
교차 연결 ... 92
미국 동부(오하이오) ... 93
미국 동부(버지니아 북부) ... 94
미국 서부(캘리포니아 북부) ... 95
미국 서부(오레곤) ... 96
아프리카(케이프타운) ... 96
아시아 태평양(자카르타) ... 97
아시아 태평양(뭄바이) ... 97
아시아 태평양(서울) ... 97
아시아 태평양(싱가포르) ... 98
아시아 태평양(시드니) ... 99
아시아 태평양(도쿄) ... 99
캐나다(중부) ... 100
중국(베이징) ... 100
중국(닝샤) ... 100
유럽(프랑크푸르트) ... 101
유럽(아일랜드) ... 102
유럽(밀라노) ... 102
유럽(런던) ... 102
유럽(파리) ... 103
유럽(스톡홀름) ... 103
유럽(취리히) ... 103
이스라엘(텔아비브) ... 104
중동(바레인) ... 104
중동(UAE) ... 104
남아메리카(상파울루) ... 105
AWS GovCloud (미국 동부) ... 105
AWS GovCloud (미국 서부) ... 105
가상 인터페이스 ... 106
퍼블릭 가상 인터페이스 접두사 광고 규칙 ... 106
호스팅 가상 인터페이스 ... 107
SiteLink ... 112

가상 인터페이스 필수 조건 113
가상 인터페이스 생성 118
가상 퍼블릭 인터페이스 생성 118
가상 프라이빗 인터페이스 생성 120
Direct Connect 게이트웨이에 대한 전송 가상 인터페이스 생성 122
라우터 구성 파일 다운로드 124
가상 인터페이스 세부 정보 보기 126
BGP 피어 추가 또는 삭제 127
BGP 피어 추가 127
BGP 피어 삭제 128
프라이빗 가상 인터페이스 또는 전송 가상 인터페이스에 대한 네트워크 MTU 설정 129
가상 인터페이스 태그를 추가 또는 제거 130
가상 인터페이스 삭제 131
호스팅되는 가상 인터페이스 생성 132
호스팅되는 가상 프라이빗 인터페이스 생성 132
호스팅되는 가상 퍼블릭 인터페이스 생성 133
호스팅되는 전송 가상 인터페이스 생성 135
호스팅된 가상 인터페이스 수학 137
가상 인터페이스를 마이그레이션 138
LAG 140
MACsec 고려 사항 141
LAG 생성 141
LAG 세부 정보 보기 144
LAG 업데이트 145
연결을 LAG에 연결 146
연결을 LAG에서 연결을 해제합니다 147
MACsec CKN/CAK를 LAG와 연결 148
MACsec 암호 키와 LAG 간의 연결을 제거합니다 149
LAG 삭제 150
Direct Connect 게이트웨이 사용 151
Direct Connect 게이트웨이 151
가상 프라이빗 게이트웨이 연결 153
계정 간 가상 프라이빗 게이트웨이 연결 153
트랜짓 게이트웨이 연결 154
계정 간 전송 게이트웨이 연결 155
Direct Connect 게이트웨이 생성 156

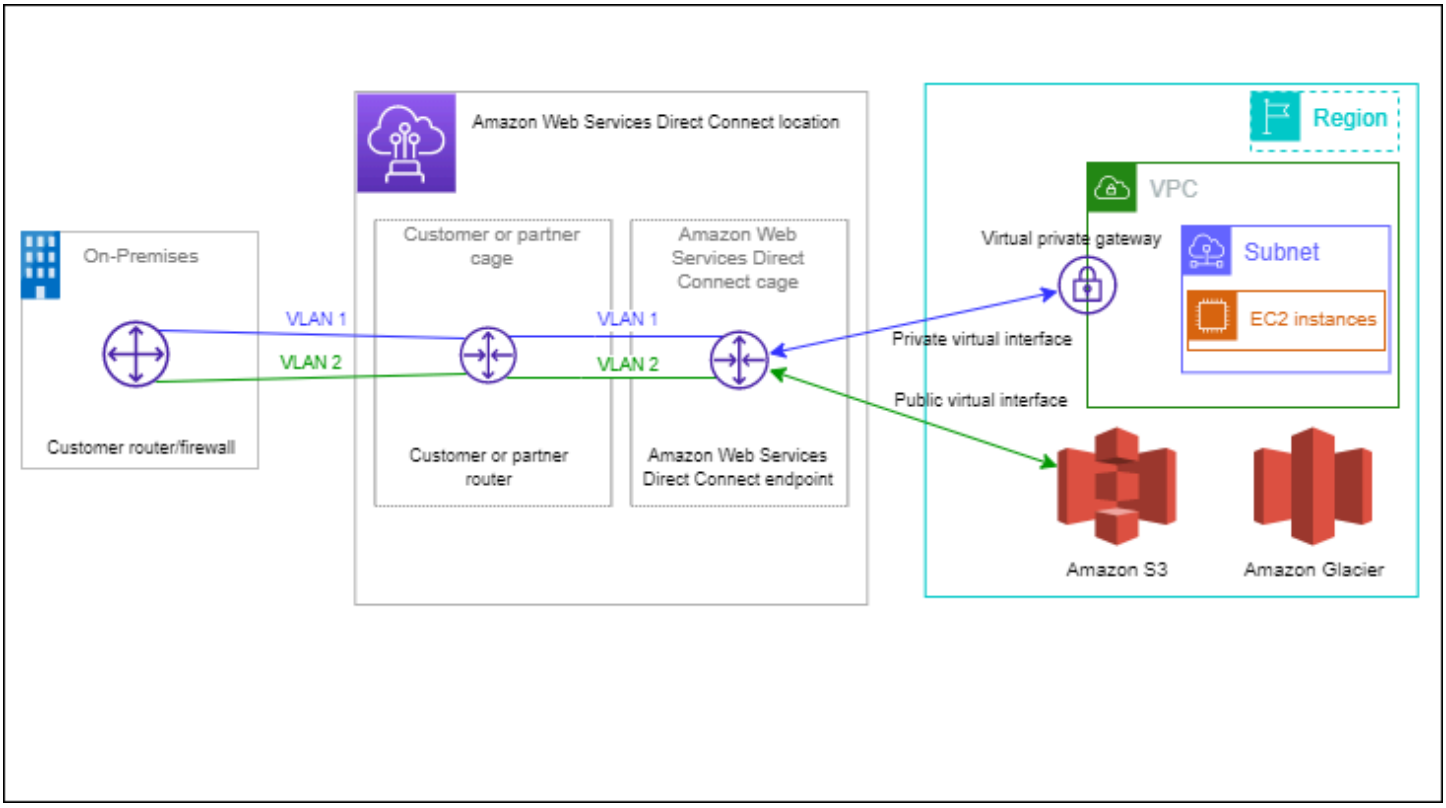
Direct Connect 게이트웨이 삭제 ... 157
가상 프라이빗 게이트웨이에서 Direct Connect 게이트웨이로 마이그레이션 ... 157
가상 프라이빗 게이트웨이 연결 ... 158
가상 프라이빗 게이트웨이 생성 ... 159
가상 프라이빗 게이트웨이 연결 및 연결 해제 ... 161
Direct Connect 게이트웨이에 대한 프라이빗 가상 인터페이스 생성 ... 162
계정 간 가상 프라이빗 게이트웨이 연결 ... 164
트랜짓 게이트웨이 연결 ... 168
전송 게이트웨이 연결 및 연결 해제 ... 169
Direct Connect 게이트웨이에 대한 전송 가상 인터페이스 생성 ... 171
계정 간 전송 게이트웨이 연결 ... 173
허용되는 접두사 상호 작용 ... 177
가상 프라이빗 게이트웨이 연결 ... 177
트랜짓 게이트웨이 연결 ... 178
예: 전송 게이트웨이 구성에서 접두사 허용 ... 179
리소스에 태그 지정 ... 181
태그 제한 ... 182
CLI 또는 API를 사용한 태그 작업 ... 183
예시 ... 183
보안 ... 184
데이터 보호 ... 184
인터네트워크 트래픽 개인 정보 보호 ... 186
암호화 ... 186
ID 및 액세스 관리 ... 187
고객 ... 187
ID를 통한 인증 ... 188
정책을 사용한 액세스 관리 ... 191
Direct Connect 에서 IAM을 사용하는 방식 ... 193
자격 증명 기반 정책 예시 ... 199
서비스 연결 역할 ... 209
AWS 관리형 정책 ... 212
문제 해결 ... 214
로깅 및 모니터링 ... 215
규정 준수 확인 ... 216
복원성 ... 217
장애 조치 ... 217

인프라 보안 218
Border Gateway Protocol 218
AWS CLI 사용 219
1단계: 연결 생성 219
2단계: LOA-CFA 다운로드 220
3단계: 가상 인터페이스 생성 및 라우터 구성 가져오기 221
API 호출 로깅 226
CloudTrail의 AWS Direct Connect 정보 226
AWS Direct Connect 로그 파일 항목 이해 227
모니터링 232
모니터링 도구 232
자동 모니터링 도구 232
수동 모니터링 도구 233
아마존을 통한 모니터링 CloudWatch 234
AWS Direct Connect 지표 및 측정기준 234
AWS Direct Connect CloudWatch 메트릭 보기 240
연결을 AWS Direct Connect 모니터링하기 위한 CloudWatch 경보 생성 241
할당량 243
BGP 쿼터 245
로드 밸런싱 고려 사항 246
문제 해결 247
레이어 1(물리적) 문제 247
레이어 2(데이터 링크) 문제 249
계층 3/4(네트워크/전송) 문제 250
라우팅 문제 253
문서 기록 255
..... cclxi

이게 뭐야 AWS Direct Connect?

AWS Direct Connect 표준 이더넷 광섬유 케이블을 통해 내부 네트워크를 특정 AWS Direct Connect 위치에 연결합니다. 케이블의 한쪽 끝을 사용자의 라우터에 연결하고 다른 쪽 끝을 AWS Direct Connect 라우터에 연결합니다. 이 연결을 통해 네트워크 경로의 인터넷 서비스 공급자를 우회하여 공용 AWS 서비스 (예: Amazon S3) 또는 Amazon VPC에 직접 연결되는 가상 인터페이스를 생성할 수 있습니다. AWS Direct Connect 위치는 해당 위치가 연결된 지역에 대한 액세스를 AWS 제공합니다. 공용 지역에서 단일 연결을 사용하거나 다른 모든 공용 지역의 공용 AWS 서비스에 액세스할 수 있습니다. AWS GovCloud (US)

다음 다이어그램은 네트워크와의 AWS Direct Connect 인터페이스 방식에 대한 개괄적인 개요를 보여줍니다.



내용

- AWS Direct Connect 구성 요소
- 네트워크 요구 사항
- AWS Direct Connect요금
- AWS Direct Connect 유지 관리

- 다이렉트 커넥트 유지 관리
- 원격 AWS 리전 액세스
- 라우팅 정책 및 BGP 커뮤니티

AWS Direct Connect 구성 요소

사용하는 주요 구성 요소는 다음과 AWS Direct Connect같습니다.

연결

특정 AWS Direct Connect 위치에 연결을 생성하여 온프레미스에서 특정 AWS 지역으로 네트워크 연결을 설정하십시오. 자세한 정보는 AWS Direct Connect 연결을 참조하세요.

가상 인터페이스

AWS 서비스에 액세스할 수 있는 가상 인터페이스를 만드세요. 퍼블릭 가상 인터페이스는 Amazon S3와 같은 퍼블릭 서비스에 대한 액세스를 제공합니다. 프라이빗 가상 인터페이스는 사용자의 VPC에 대한 액세스를 제공합니다. 자세한 내용은 AWS Direct Connect 가상 인터페이스 및 가상 인터페이스 필수 조건 섹션을 참조하세요.

네트워크 요구 사항

특정 AWS Direct Connect AWS Direct Connect 위치에서 사용하려면 네트워크가 다음 조건 중 하나를 충족해야 합니다.

- 네트워크가 기존 AWS Direct Connect 위치와 같은 위치에 있습니다. 사용 가능한 AWS Direct Connect 위치에 대한 자세한 내용은 AWS Direct Connect 제품 세부 정보를 참조하십시오.
- AWS Direct Connect 파트너 네트워크 (APN) 의 회원인 AWS 파트너와 협력하고 있습니다. 자세한 내용은 AWS Direct Connect를 지원하는 APN 파트너를 참조하세요.
- 독립 서비스 공급자와 협력하여 AWS Direct Connect에 연결합니다.

네트워크가 다음 조건도 충족해야 합니다.

- 사용자의 네트워크는 1기가비트 이더넷의 경우 1000BASE-LX(1310nm) 송수신장치, 10기가비트 이더넷의 경우 10GBASE-LR(1310nm) 송수신장치, 100기가비트 이더넷의 경우 100GBASE-LR4가 있는 단일 모드 광섬유를 사용해야 합니다.

- 포트 속도가 1Gbps를 초과하는 연결의 경우 포트 자동 협상을 비활성화해야 합니다. 하지만 연결을 제공하는 AWS Direct Connect 엔드포인트에 따라 1Gbps 연결에 대해 자동 협상을 활성화하거나 비활성화해야 할 수 있습니다. 가상 인터페이스가 계속 다운되는 경우 계층 2(데이터 링크) 문제 해결를 참조하세요.
- 중간 디바이스를 비롯하여 네트워크 전체적으로 802.1Q VLAN 캡슐화를 지원해야 합니다.
- 디바이스에서 BGP(Border Gateway Protocol)와 BGP MD5 인증을 지원해야 합니다.
- (선택 사항) 네트워크에 BFD(Bidirectional Forwarding Detection)를 구성할 수 있습니다. 비동기 BFD는 각 가상 인터페이스에서 자동으로 활성화됩니다. AWS Direct Connect Direct Connect 가상 인터페이스에 대해서는 자동으로 활성화되지만, 라우터에서 이를 구성해야만 작동이 시작됩니다. 자세한 내용은 Direct Connect 연결을 위한 BFD 활성화를 참조하세요.

AWS Direct Connect IPv4 및 IPv6 통신 프로토콜을 모두 지원합니다. 공용 AWS 서비스에서 제공하는 IPv6 주소는 공용 가상 인터페이스를 통해 액세스할 수 있습니다. AWS Direct Connect

AWS Direct Connect 는 링크 계층에 이더넷 프레임 크기 1522 또는 9023바이트(14바이트 이더넷 헤더 + 4바이트 VLAN 태그 + IP 데이터그램 바이트 + 4바이트 FCS)를 지원합니다. 프라이빗 가상 인터페이스의 MTU를 설정할 수 있습니다. 자세한 정보는 프라이빗 가상 인터페이스 또는 전송 가상 인터페이스에 대한 네트워크 MTU 설정을 참조하세요.

AWS Direct Connect요금

AWS Direct Connect 결제 요소에는 포트 시간과 아웃바운드 데이터 전송이라는 두 가지 요소가 있습니다. 포트 시간 요금은 용량 및 연결 유형(전용 연결 또는 호스팅 연결)에 따라 결정됩니다.

프라이빗 인터페이스 및 트랜짓 가상 인터페이스에 대한 데이터 전송 요금은 데이터 전송을 담당하는 AWS 계정에 할당됩니다. 다중 계정 AWS Direct Connect 게이트웨이를 사용하는 데 추가 요금이 부과되지 않습니다.

공개적으로 주소를 지정할 수 있는 AWS 리소스 (예: Amazon S3 버킷, Classic EC2 인스턴스 또는 인터넷 게이트웨이를 통과하는 EC2 트래픽) 의 경우 아웃바운드 트래픽이 동일한 AWS 지불자 계정이 소유한 퍼블릭 접두사로 향하고 퍼블릭 가상 인터페이스를 AWS 통해 적극적으로 광고되는 경우 데이터 전송 속도 기준으로 DTO (Data Transfer Out) 사용량이 리소스 소유자를 기준으로 측정됩니다. AWS Direct Connect AWS Direct Connect

자세한 내용은 AWS Direct Connect 요금을 참조하세요.

AWS Direct Connect 유지 관리

AWS Direct Connect Direct Connect가 서비스를 지원하는 하드웨어 플릿에 대해 정기적으로 유지 관리 작업을 수행하는 완전 관리형 서비스입니다. Direct Connect 연결은 독립형 하드웨어 장치에 제공되므로 온-프레미스 인프라 간에 Amazon Virtual Private Cloud 복원력이 뛰어난 네트워크 연결을 만들 수 있습니다. 이 기능을 사용하면 안정적이고 확장 가능하며 비용 효율적인 방식으로 AWS 리소스에 액세스할 수 있습니다. 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하세요.

Direct Connect 유지 관리 유형은 계획 유지 관리와 긴급 유지 관리, 두 가지입니다.

- 계획 유지 관리. 가용성을 높이고 새 기능을 제공하기 위해 계획된 유지 관리가 미리 예정되어 있습니다. 이러한 유형의 유지 관리는 3가지 알림 (달력일 14일, 7일, 달력 1일) 이 제공되는 유지 관리 기간 중에 예약됩니다.

  > **Note**
  > 달력일에는 비영업일 및 현지 공휴일이 포함됩니다.

- 긴급 유지 관리. 서비스에 영향을 미치는 서비스 장애로 인해 긴급 유지 관리가 시작되어 AWS 로부터 서비스를 복원하기 위해 즉각적인 조치를 취해야 합니다. 이러한 유형의 유지 관리는 사전에 계획된 것이 아닙니다. 영향을 받는 고객에게는 유지 보수 시작 60분 전까지 긴급 유지 관리 알림이 제공됩니다.

유지 관리 중에 트래픽을 이중화된 Direct Connect 연결로 원활하고 능동적으로 전환할 수 있도록 AWS Direct Connect 복원력 권장 사항을 따르는 것이 좋습니다. 또한 정기적으로 중복 연결의 복원력을 사전 예방적으로 테스트하여 장애 조치가 의도한 대로 작동하는지 확인하는 것이 좋습니다. 이 the section called “AWS Direct Connect 장애 조치 테스트” 기능을 사용하면 트래픽이 중복 가상 인터페이스 중 하나를 통해 라우팅되는지 확인할 수 있습니다.

계획 유지 관리 취소 요청을 시작하는 자격 기준에 대한 지침은 Direct Connect 유지 관리 이벤트를 취소하려면 어떻게 해야 합니까?를 참조하세요.

> **Note**
> 긴급 유지 관리 요청은 취소할 수 없으므로 서비스를 복원하려면 즉시 조치를 AWS 취해야 합니다.

유지 관리 이벤트에 대한 자세한 내용은 AWS Direct Connect FAQ의 유지 관리 이벤트를 참조하십시오.

다이렉트 커넥트 유지 관리

AWS Direct Connect Direct Connect가 서비스를 지원하는 하드웨어 플릿에 대해 정기적으로 유지 관리 작업을 수행하는 완전 관리형 서비스입니다. Direct Connect 연결은 독립형 하드웨어 장치에 제공되므로 온-프레미스 인프라 간에 Amazon Virtual Private Cloud 복원력이 뛰어난 네트워크 연결을 만들 수 있습니다. 이 기능을 사용하면 안정적이고 확장 가능하며 비용 효율적인 방식으로 AWS 리소스에 액세스할 수 있습니다. 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하세요.

Direct Connect 유지 관리 유형은 계획 유지 관리와 긴급 유지 관리, 두 가지입니다.

- 계획 유지 관리. 가용성을 높이고 새 기능을 제공하기 위해 계획된 유지 관리가 미리 예정되어 있습니다. 이러한 유형의 유지 관리는 10일, 5일, 달력 1일 등 세 가지 알림을 제공하는 유지 관리 기간 중에 예약됩니다.

  > **Note**
  >
  > 달력일에는 비영업일 및 현지 공휴일이 포함됩니다.

- 긴급 유지 관리. 서비스에 영향을 미치는 서비스 장애로 인해 긴급 유지 관리가 시작되어 AWS 로부터 서비스를 복원하기 위해 즉각적인 조치를 취해야 합니다. 이러한 유형의 유지 관리는 사전에 계획된 것이 아닙니다. 영향을 받는 고객에게는 유지 보수 시작 60분 전까지 긴급 유지 관리 알림이 제공됩니다.

유지 보수 이벤트 중에는 광고 또는 경로 수락을 AWS 중단합니다. 디바이스를 다시 시작해야 하는 경우를 제외하고 BGP 세션은 일반적으로 이벤트 중에 계속 작동하므로 링크 상태 추적과 함께 고정 경로를 사용하는 대신 BGP를 사용하여 장애 조치를 수행하는 것이 좋습니다.

유지 관리 중에 이중화된 Direct Connect 연결로 트래픽이 원활하고 AWS Direct Connect 능동적으로 전송될 수 있도록 복구 권장 사항을 따르는 것이 좋습니다. 또한 정기적으로 중복 연결의 복원력을 사전 예방적으로 테스트하여 장애 조치가 의도한 대로 작동하는지 확인하는 것이 좋습니다. 이 the section called “AWS Direct Connect 장애 조치 테스트” 기능을 사용하면 트래픽이 중복 가상 인터페이스 중 하나를 통해 라우팅되는지 확인할 수 있습니다.

계획 유지 관리 취소 요청을 시작하는 자격 기준에 대한 지침은 Direct Connect 유지 관리 이벤트를 취소하려면 어떻게 해야 합니까?를 참조하세요.

> **Note**
> 긴급 유지 관리 요청은 취소할 수 없으므로 서비스를 복원하려면 즉시 조치를 AWS 취해야 합니다.

유지 관리 이벤트에 대한 자세한 내용은 AWS Direct Connect FAQ의 유지 관리 이벤트를 참조하십시오.

원격 AWS 리전 액세스

퍼블릭 리전 또는 AWS GovCloud (US)의 AWS Direct Connect 위치는 다른 모든 퍼블릭 리전(중국(베이징과 닝샤) 제외)의 퍼블릭 서비스에 액세스할 수 있습니다. 또한 퍼블릭 리전 또는 AWS GovCloud (US)의 AWS Direct Connect 연결은 다른 모든 퍼블릭 리전(중국(베이징과 닝샤) 제외)에서 사용자 계정으로 VPC에 액세스하도록 구성할 수 있습니다. 따라서 단일 AWS Direct Connect 연결을 사용하여 다중 리전 서비스를 구현할 수 있습니다. 사용자가 퍼블릭 AWS 서비스에 액세스하든 다른 리전의 VPC에 액세스하든 관계없이 모든 네트워킹 트래픽은 AWS 글로벌 네트워크 백본에 남아 있습니다.

원격 리전으로부터의 모든 데이터 전송은 원격 리전 데이터 전송 요금으로 청구됩니다. 데이터 전송 요금에 대한 자세한 정보는 AWS Direct Connect 세부 정보 페이지의 요금 단원을 참조하십시오.

AWS Direct Connect 연결을 위한 라우팅 정책 및 지원되는 BGP 커뮤니티에 대한 자세한 내용은 라우팅 정책 및 BGP 커뮤니티 단원을 참조하십시오.

원격 리전의 퍼블릭 서비스 액세스

원격 리전의 퍼블릭 리소스에 액세스하려면 퍼블릭 가상 인터페이스를 설정하고 BGP(Border Gateway Protocol) 세션을 설정해야 합니다. 자세한 내용은 AWS Direct Connect 가상 인터페이스 섹션을 참조하세요.

퍼블릭 가상 인터페이스를 만들고 그에 대한 BGP 세션을 설정하면 라우터가 다른 퍼블릭 AWS 리전의 경로를 학습합니다. AWS이(가) 현재 광고하는 접두사에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS IP 주소 범위를 참조하십시오.

원격 리전의 VPC 액세스

모든 퍼블릭 리전에서 Direct Connect 게이트웨이를 만들 수 있습니다. 이를 사용하여 프라이빗 가상 인터페이스를 통해 AWS Direct Connect 연결을 다른 리전 또는 전송 게이트웨이에 있는 계정의 VPC에 연결합니다. 자세한 내용은 Direct Connect 게이트웨이 사용 섹션을 참조하세요.

또는 AWS Direct Connect 연결을 위한 퍼블릭 가상 인터페이스를 만든 다음 원격 리전의 VPC에 VPN 연결을 설정할 수 있습니다. VPC에 대한 VPN 연결을 구성하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 Amazon Virtual 프라이빗 클라우드 사용 시나리오를 참조하십시오.

네트워크와 Amazon VPC 간 연결 옵션

다음 구성을 사용하여 원격 네트워크를 Amazon VPC 환경에 연결할 수 있습니다. 이러한 옵션은 AWS 리소스를 기존 온사이트 서비스와 통합하는 데 유용합니다.

- Amazon Virtual Private Cloud(VPC) 연결 오류

라우팅 정책 및 BGP 커뮤니티

AWS Direct Connect 공용 연결에 대한 인바운드 (온프레미스 데이터 센터) 및 아웃바운드 (AWS 지역) 라우팅 정책을 적용합니다. AWS Direct Connect Amazon에서 공급하는 라우팅에서 Border Gateway Protocol(BGP) 커뮤니티 태그를 사용하고, 사용자가 Amazon에 공급하는 해당 라우팅에 BGP 커뮤니티 태그를 적용할 수도 있습니다.

퍼블릭 가상 인터페이스 라우팅 정책

를 사용하여 AWS Direct Connect 공용 AWS 서비스에 액세스하는 경우 BGP를 통해 광고할 퍼블릭 IPv4 접두사 또는 IPv6 접두사를 지정해야 합니다.

다음과 같은 인바운드 라우팅 정책이 적용됩니다.

- 사용자는 퍼블릭 접두사를 소유하고 있어야 하며, 이러한 접두사는 해당 지역 인터넷 등록 기관에 반드시 등록해야 합니다.
- 트래픽의 목적지는 Amazon 퍼블릭 접두사여야 합니다. 연결간 전이적 라우팅은 지원되지 않습니다.
- AWS Direct Connect 인바운드 패킷 필터링을 수행하여 트래픽의 소스가 광고된 접두사에서 비롯되었는지 확인합니다.

다음과 같은 아웃바운드 라우팅 정책이 적용됩니다.

- AS_PATH 및 Longest Prefix Match는 라우팅 경로를 결정하는 데 사용됩니다. AWS 인터넷과 공용 가상 인터페이스 모두에 동일한 접두사를 알리는 AWS Direct Connect 경우를 사용하여 보다 구체적인 경로를 광고하는 것이 좋습니다.
- AWS Direct Connect 가능한 경우 모든 로컬 및 원격 AWS 지역 접두사를 알리고 가능한 경우 다른 AWS 비지역 접속 지점 (PoP) 의 온넷 접두사를 포함합니다 (예: Route 53). CloudFront

> **Note**
>
> - AWS IP 주소 범위 JSON 파일 ip-ranges.json에 나열된 중국 지역의 접두사는 중국 지역에서만 광고됩니다. AWS AWS
> - 상업 지역의 AWS IP 주소 범위 JSON 파일인 ip-ranges.json에 나열된 접두사는 상업 지역에서만 광고됩니다. AWS AWS
>
> ip-ranges.json 파일에 대한 자세한 내용은AWS 일반 참조의 AWS IP 주소 범위를 참조하세요.

- AWS Direct Connect 최소 경로 길이가 3인 접두사를 광고합니다.
- AWS Direct Connect 모든 공개 접두사를 잘 알려진 BGP 커뮤니티에 광고합니다. NO_EXPORT
- 서로 다른 두 개의 공용 가상 인터페이스를 사용하여 서로 다른 두 지역의 동일한 접두사를 광고하고 둘 다 BGP 속성이 같고 접두사 길이가 가장 긴 경우 아웃바운드 트래픽은 홈 지역의 우선 순위를 지정합니다. AWS
- AWS Direct Connect 연결이 여러 개인 경우 경로 속성이 동일한 접두사를 광고하여 인바운드 트래픽의 부하 분담을 조정할 수 있습니다.
- 에서 광고하는 접두사를 연결의 네트워크 경계를 넘어서 AWS Direct Connect 광고해서는 안 됩니다. 예를 들어, 이 접두사는 퍼블릭 인터넷 라우팅 테이블에 포함되면 안됩니다.
- AWS Direct Connect Amazon 네트워크 내에서 고객이 광고하는 접두사를 보관합니다. 퍼블릭 VIF에서 학습한 고객 접두사를 다음과 같이 다시 광고하지 않습니다.
  - 기타 고객 AWS Direct Connect
  - AWS 글로벌 네트워크와 피어링하는 네트워크
  - Amazon의 전송 서비스 제공업체

퍼블릭 가상 인터페이스 BGP 커뮤니티

AWS Direct Connect 스코프 BGP 커뮤니티 태그를 지원하여 퍼블릭 가상 인터페이스에서 트래픽의 범위 (지역 또는 글로벌) 및 경로 선호도를 제어하는 데 도움이 됩니다. AWS 퍼블릭 VIF에서 수신한 모든 경로를 NO_EXPORT BGP 커뮤니티 태그가 지정된 것처럼 취급합니다. 즉, 네트워크에서만 해당 라우팅 정보를 사용하게 됩니다. AWS

BGP 커뮤니티 범위

사용자가 Amazon에 공급하는 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용하면 Amazon 네트워크(로컬 AWS 리전 전용, 대륙 내 모든 리전 또는 모든 퍼블릭 리전을 대상)에서 접두사를 전파할 범위를 나타낼 수 있습니다.

AWS 리전 커뮤니티

인바운드 라우팅 정책에 대해서는 다음과 같은 BGP 커뮤니티를 사용할 수 있습니다.

- `7224:9100`—로컬 AWS 리전
- `7224:9200`—한 AWS 리전 대륙에 대한 모든 것:
  - 북미 전역
  - 아시아 태평양
  - 유럽, 중동 및 아프리카
- `7224:9300`—글로벌 (모든 공개 지역) AWS

> **Note**
>
> 커뮤니티 태그를 적용하지 않으면 기본적으로 접두사가 모든 공개 AWS 지역 (글로벌) 에 광고됩니다.
> 같은 커뮤니티가 표시되고 동일한 AS_PATH 속성을 가진 접두사가 다중 경로의 후보입니다.

커뮤니티 `7224:1` – `7224:65535`는 AWS Direct Connect에 의해 예약됩니다.

아웃바운드 라우팅 정책의 경우 다음 BGP 커뮤니티를 광고된 경로에 AWS Direct Connect 적용합니다.

- `7224:8100`—접속 지점이 연결된 동일한 AWS 지역에서 출발하는 AWS Direct Connect 경로.
- `7224:8200`—거주 AWS Direct Connect 지점이 연결된 동일한 대륙에서 출발하는 노선.
- 태그 없음 - 다른 대륙에서 출발하는 노선입니다.

> **Note**
>
> 모든 AWS 공개 접두사를 수신하려면 필터를 적용하지 마십시오.

AWS Direct Connect 공용 연결이 지원되지 않는 커뮤니티는 제거됩니다.

NO_EXPORT BGP 커뮤니티

아웃바운드 라우팅 정책의 경우 NO_EXPORT BGP 커뮤니티 태그는 퍼블릭 가상 인터페이스에 지원됩니다.

AWS Direct Connect 또한 광고된 Amazon 경로에 BGP 커뮤니티 태그를 제공합니다. 를 AWS Direct Connect 사용하여 공용 AWS 서비스에 액세스하는 경우 이러한 커뮤니티 태그를 기반으로 필터를 만들 수 있습니다.

공용 가상 인터페이스의 경우 고객에게 AWS Direct Connect 광고하는 모든 경로에 NO_EXPORT 커뮤니티 태그가 지정됩니다.

프라이빗 가상 인터페이스 및 전송 가상 인터페이스 라우팅 정책

를 사용하여 프라이빗 AWS Direct Connect AWS 리소스에 액세스하는 경우 BGP를 통해 광고할 IPv4 또는 IPv6 접두사를 지정해야 합니다. 이러한 접두사는 공개 또는 비공개일 수 있습니다.

광고된 접두사에 따라 다음과 같은 아웃바운드 라우팅 규칙이 적용됩니다.

- AWS 가장 긴 접두사 길이를 먼저 평가합니다. AWS 원하는 라우팅 경로가 액티브/패시브 연결용인 경우 여러 Direct Connect 가상 인터페이스를 사용하여 보다 구체적인 경로를 알릴 것을 권장합니다. 자세한 내용은 Longest Prefix Match를 사용하여 하이브리드 네트워크를 통한 트래픽에 영향을 미치기를 참조하십시오.
- 로컬 기본 설정은 원하는 라우팅 경로가 액티브/패시브 연결용이고 광고되는 접두사 길이가 동일할 때 사용하는 것이 권장되는 BGP 속성입니다. 이 값은 —Medium 로컬 기본 설정 커뮤니티 값을 사용하여 동일한 AWS Direct Connect 연결이 있는 위치를 선호하도록 지역별로 설정됩니다. AWS 리전 7224:7200 로컬 지역이 Direct Connect 위치와 연결되지 않은 경우 더 낮은 값으로 설정됩니다. 이는 로컬 기본 설정 커뮤니티 태그가 할당되지 않은 경우에만 적용됩니다.
- 접두사 길이와 로컬 기본 설정이 동일한 경우 AS_PATH 길이를 사용하여 라우팅 경로를 결정할 수 있습니다.
- 접두사 길이, 로컬 기본 설정 및 AS_PATH가 동일한 경우 다중 종료 식별자 (MED) 를 사용하여 라우팅 경로를 결정할 수 있습니다. AWS MED 값은 평가 우선 순위가 낮으므로 사용하지 않는 것이 좋습니다.
- AWS 접두사의 길이와 BGP 속성이 동일한 경우 여러 트랜짓 또는 프라이빗 가상 인터페이스에서 부하를 공유합니다.

프라이빗 가상 인터페이스 및 전송 가상 인터페이스 BGP 커뮤니티

Direct Connect 사설 또는 트랜짓 가상 인터페이스를 통해 온-프레미스 위치로 트래픽을 라우팅하는 경우 Direct Connect 위치와 관련된 AWS 리전 위치가 동일 비용 다중 경로 라우팅 (ECMP) 을 사용하는 능력에 영향을 줍니다. AWS 리전 AWS 리전 AWS 리전 기본적으로 동일한 연결 위치의 Direct Connect 위치를 선호합니다. 모든 Direct Connect 위치와 관련된 AWS 리전 위치를 식별하려면 위치를 참조하십시오AWS Direct Connect .

로컬 기본 설정 커뮤니티 태그가 적용되지 않은 경우 Direct Connect는 다음 시나리오에서 둘 이상의 경로에서 동일한 길이, AS_PATH 길이 및 MED 값을 가진 접두사에 대해 프라이빗 또는 트랜짓 가상 인터페이스를 통해 ECMP를 지원합니다.

- AWS 리전 전송 트래픽에는 동일한 코로케이션 시설이든 다른 코로케이션 시설에 있든 관계없이 동일한 관련 AWS 리전위치에서 오는 두 개 이상의 가상 인터페이스 경로가 있습니다.
- AWS 리전 전송 트래픽에는 같은 지역에 있지 않은 위치에서 오는 두 개 이상의 가상 인터페이스 경로가 있습니다.

자세한 내용은 사설 또는 트랜짓 가상 인터페이스에서 액티브/액티브 또는 액티브/패시브 Direct Connect 연결을 AWS 설정하려면 어떻게 해야 합니까? 를 참조하십시오.

> **Note**
>
> 이는 ECMP와 온프레미스 위치 간의 ECMP 간에는 영향을 미치지 않습니다. AWS 리전

경로 기본 설정을 제어하기 위해 Direct Connect는 프라이빗 가상 인터페이스 및 트랜짓 가상 인터페이스에 대한 로컬 기본 설정 BGP 커뮤니티 태그를 지원합니다.

로컬 기본 설정 BGP 커뮤니티

로컬 기본 설정 BGP 커뮤니티 태그를 사용하여 수신 트래픽에 대한 로드 밸런싱 및 경로 기본 설정을 네트워크에 적용할 수 있습니다. BGP 세션을 통해 공급하는 각 접두사에 대해 커뮤니티 태그를 적용하여 트래픽 반환을 위해 연결된 경로의 우선 순위를 나타낼 수 있습니다.

다음 로컬 기본 설정 BGP 커뮤니티 태그가 지원됩니다.

- `7224:7100`—낮은 선호도
- `7224:7200`—중간 선호도

- `7224:7300`—높은 선호도

로컬 기본 설정 BGP 커뮤니티 태그는 상호 배타적입니다. 동일하거나 다른 AWS 지역에 홈으로 AWS Direct Connect 연결된 여러 연결 (액티브/액티브) 간에 트래픽의 부하를 분산하려면 동일한 커뮤니티 태그 `7224:7200` (예: medium preference) 를 연결 접두사 전체에 적용하십시오. 연결 중 하나에 장애가 발생하면 홈 지역 연결에 관계없이 ECMP를 사용하여 나머지 활성 연결 간에 트래픽의 부하를 분산합니다. 여러 AWS Direct Connect 연결(액티브/패시브)에 대한 장애 조치를 지원하려면 기본 또는 활성 가상 인터페이스의 접두사에 선호도가 높은 커뮤니티 태그를 적용하고 백업 또는 패시브 가상 인터페이스의 접두사에는 선호도가 낮은 태그를 적용합니다. 예를 들면 `7224:7300` (선호도 높음)와(과)의 기본 또는 활성 가상 인터페이스에는 BGP 커뮤니티 태그를, 패시브 가상 인터페이스에는 `7224:7100` (낮은 선호도)를 설정합니다.

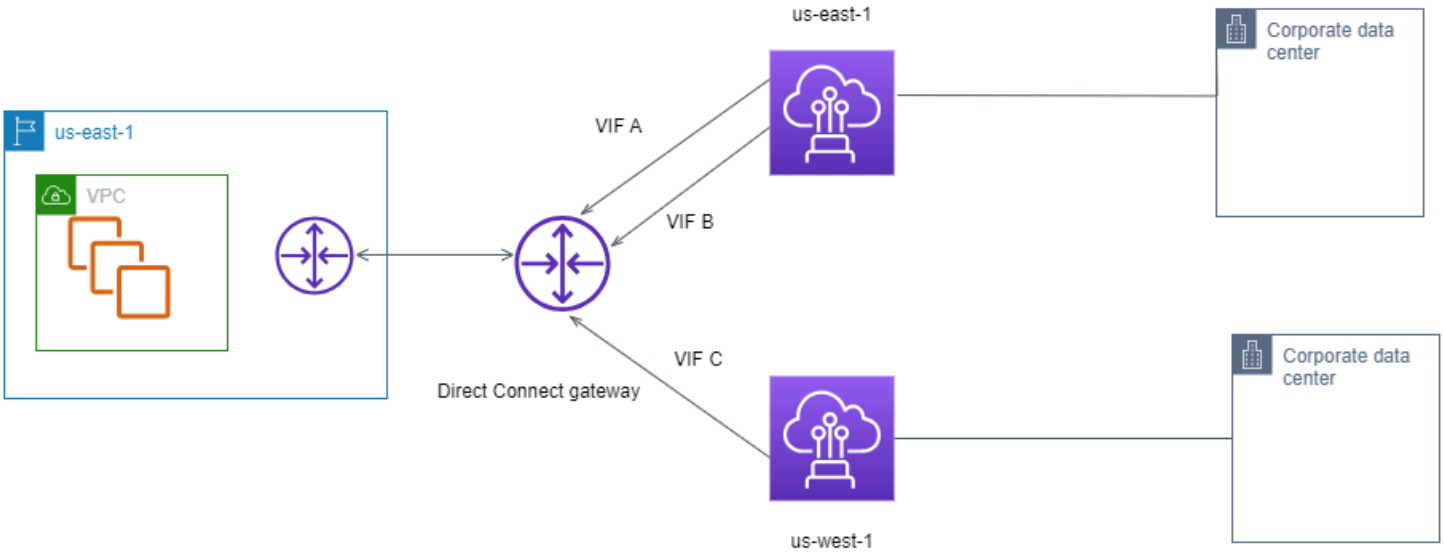
로컬 기본 설정 BGP 커뮤니티 태그는 AS_PATH 속성 전에 평가되며, 가장 낮은 기본 설정부터 가장 높은 기본 설정 순서로 평가됩니다(가장 높은 기본 설정이 선호됨).

프라이빗 가상 인터페이스 라우팅 예제

AWS Direct Connect 위치 1 홈 지역이 VPC 홈 지역과 동일한 구성을 고려해 보십시오. 다른 지역에 중복 AWS Direct Connect 위치가 있습니다. 위치 1 (AWS Direct Connect us-east-1) 에서 직접 연결 게이트웨이까지 두 개의 프라이빗 VIF (VIF A 및 VIF B) 가 있습니다. AWS Direct Connect 위치 (us-west-1) 에서 다이렉트 커넥트 게이트웨이까지 하나의 프라이빗 VIF (VIF C) 가 있습니다. VIF A보다 먼저 VIF B를 통해 트래픽을 AWS 라우팅하려면 VIF B의 AS_PATH 속성을 VIF A AS_PATH 속성보다 짧게 설정하십시오.

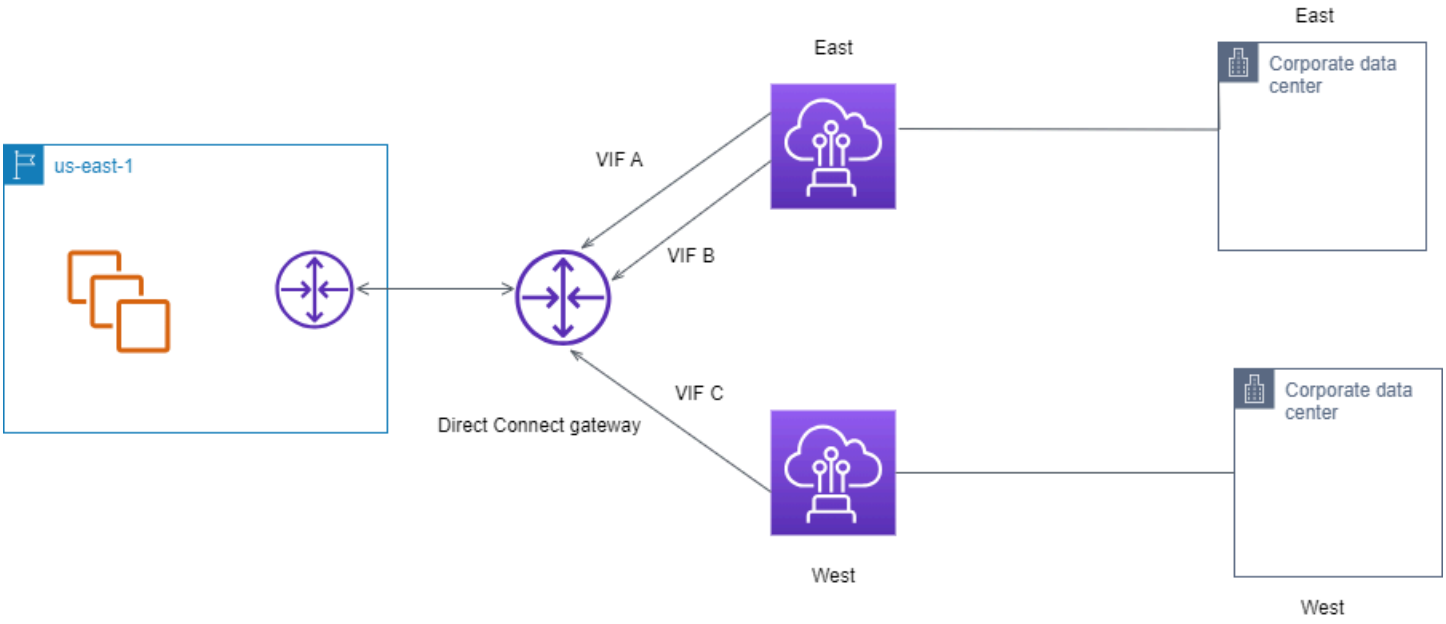
VIF에는 다음과 같은 구성이 있습니다.

- VIF A(us-east-1에 속함)는 172.16.0.0/16을 광고하며 AS_PATH 속성은 65001, 65001, 65001입니다
- VIF B(us-east-1에 속함)는 172.16.0.0/16을 광고하며 AS_PATH 속성은 65001, 65001입니다
- VIF C(us-west-1에 속함)는 172.16.0.0/16을 광고하며 AS_PATH 속성은 65001입니다



VIF C의 CIDR 범위 구성을 변경하는 경우 VIF C CIDR 범위에 속하는 경로는 접두사 길이가 가장 길기 때문에 VIF C를 사용합니다.

- VIF C(us-west-1에 속함)는 172.16.0.0/24을 광고하며 AS_PATH 속성은 65001입니다



AWS Direct Connect 복원력 툴킷을 사용하여 시작하기

AWS는 고객에게 Amazon Virtual Private Cloud(VPC)와 온프레미스 인프라 간에 복원력이 높은 네트워크 연결을 확보할 수 있는 기능을 제공합니다. AWS Direct Connect 복원력 툴킷은 여러 복원 모델이 포함된 Connection Wizard를 제공합니다. 이러한 모델은 SLA 목표를 달성하기 위해 전용 연결 수를 결정한 다음 주문하는 데 도움이 됩니다. 복원 모델을 선택하면 AWS Direct Connect 복원력 툴킷이 전용 연결 주문 과정을 안내합니다. 복원 모델은 여러 위치에 적절한 수의 전용 연결을 갖도록 설계되었습니다.

AWS Direct Connect 복원력 툴킷에는 다음과 같은 이점이 있습니다.

- 적절한 중복 AWS Direct Connect 전용 연결을 선택하고 주문하는 방법에 대한 지침을 제공합니다.
- 중복 전용 연결 간에 동일한 속도를 보장합니다.
- 전용 연결 이름을 자동으로 구성합니다.
- 기존 AWS 계정을 가지고 있는 경우 알려진 AWS Direct Connect 파트너를 선택하면 자동으로 전용 연결을 승인합니다. LOA(Letter of Authority)를 즉시 다운로드할 수 있습니다.
- 사용자가 새 AWS 고객이거나 알 수 없는(기타) 파트너를 선택할 경우 전용 연결 승인을 위한 지원 티켓을 자동으로 생성합니다.
- 달성할 수 있는 SLA 및 주문한 전용 연결의 포트-시간 요금이 명시되어 있는 전용 연결(들)에 대한 주문 요약을 제공합니다.
- 링크 집계 그룹(LAG)을 생성하고 1Gbps, 10Gbps 또는 100Gbps 이외의 속도를 선택할 때 LAG에 적절한 수의 전용 연결을 추가합니다.
- 달성할 수 있는 SLA 및 LAG의 일부로 주문한 각 전용 연결의 총 포트-시간 요금이 명시되어 있는 전용 연결(들)에 대한 LAG 요약을 제공합니다.
- 동일한 AWS Direct Connect 디바이스에서 전용 연결이 종료되지 않도록 방지합니다.
- 복원력에 대해 구성을 테스트할 수 있는 방법을 제공합니다. 트래픽이 중복 가상 인터페이스 중 하나로 라우팅되는지 확인하기 위해 AWS를 사용하여 BGP 피어링 세션을 중단합니다. 자세한 설명은 the section called “AWS Direct Connect 장애 조치 테스트” 섹션을 참조하세요.
- 연결 및 가상 인터페이스에 대한 Amazon CloudWatch 메트릭을 제공합니다. 자세한 설명은 모니터링 섹션을 참조하세요.

AWS Direct Connect 복원력 툴킷에서 사용 가능한 복원 모델은 다음과 같습니다.

- 최대 복원성: 이 모델은 99.99%의 SLA를 달성하기 위한 전용 연결을 주문하는 방법을 제공합니다. 이 경우 AWS Direct Connect 서비스 수준 계약에 명시되어 있는 SLA 달성을 위한 모든 요구 사항을 충족해야 합니다.
- 높은 복원성: 이 모델은 99.9%의 SLA를 달성하기 위한 전용 연결을 주문하는 방법을 제공합니다. 이 경우 AWS Direct Connect 서비스 수준 계약에 명시되어 있는 SLA 달성을 위한 모든 요구 사항을 충족해야 합니다.
- 개발 및 테스트: 이 모델은 한 위치의 개별 디바이스에서 종료하는 별도의 연결을 사용하여 중요하지 않은 워크로드에 대한 개발 및 테스트 복원성을 확보할 수 있는 방법을 제공합니다.
- 클래식: 이 모델은 기존 연결을 가지고 있고 추가 연결을 원하는 사용자를 위해 설계되었습니다. 이 모델은 SLA를 제공하지 않습니다.

가장 좋은 방법은 AWS Direct Connect Resiliency Toolkit의 연결 마법사를 이용하여 SLA 목표를 달성하기 위한 전용 연결을 주문하는 것입니다.

복원 모델을 선택하면 AWS Direct Connect 복원력 툴킷이 다음 절차를 단계별로 안내합니다.

- 전용 연결 수 선택
- 연결 용량 및 전용 연결 위치 선택
- 전용 연결 주문
- 전용 연결을 사용할 준비가 되었는지 확인
- 각 전용 연결에 대한 LOA-CFA 다운로드
- 구성이 복원력 요구 사항을 충족하는지 확인

사전 조건

AWS Direct Connect는 단일 모드 파이버를 통해 1기가비트 이더넷에는 1000BASE-LX (1310nm) 트랜시버, 10기가비트에는 10GBASE-LR (1310nm) 트랜시버, 100기가비트 이더넷에는 100GBASE-LR4 트랜시버 포트 속도를 지원합니다.

다음 방법 중 하나를 사용하여 AWS Direct Connect 연결을 설정할 수 있습니다.

모델	대역폭	메서드
전용 연결	1Gbps, 10Gbps, 100Gbps	AWS Direct Connect 파트너 또는 네트워크 공급자와 협력하여 데이터 센터, 사무

모델	대역폭	메서드
		실 또는 코로케이션 환경에서 AWS Direct Connect 위치까지 라우터를 연결할 수 있습니다. 네트워크 공급자는 AWS Direct Connect 파트너가 아니어도 사용자를 전용 연결에 연결해 줄 수 있습니다. AWS Direct Connect 전용 연결은 단일 모드 광섬유를 통해 1Gbps: 1000BASE-LX(1310nm), 10Gbps: 10GBASE-LR(1310nm), 100Gbps: 100GBASE-LR4의 포트 속도를 지원합니다.
호스팅 연결	50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, 500Mbps, 1Gbps, 2Gbps, 5Gbps 및 10Gbps	AWS Direct Connect 파트너 프로그램에서 파트너와 협력하여 데이터 센터, 사무실 또는 콜로케이션 환경에서 AWS Direct Connect 위치까지 라우터를 연결할 수 있습니다. 특정 파트너만 더 많은 용량의 연결을 제공합니다.

대역폭이 1Gbps 이상인 AWS Direct Connect 연결의 경우, 네트워크가 다음 요구 사항을 충족해야 합니다.

- 사용자의 네트워크는 1기가비트 이더넷의 경우 1000BASE-LX(1310nm) 송수신장치, 10기가비트 이더넷의 경우 10GBASE-LR(1310nm) 송수신장치, 100기가비트 이더넷의 경우 100GBASE-LR4가 있는 단일 모드 광섬유를 사용해야 합니다.
- 포트 속도가 1Gbps를 초과하는 연결의 경우 포트 자동 협상을 비활성화해야 합니다. 하지만 연결을 담당하는 AWS Direct Connect 엔드포인트에 따라 1Gbps 연결에 대해 자동 협상을 활성화하거나 비활성화해야 할 수도 있습니다. 가상 인터페이스가 계속 다운되는 경우 계층 2(데이터 링크) 문제 해결를 참조하세요.

- 중간 디바이스를 비롯하여 네트워크 전체적으로 802.1Q VLAN 캡슐화를 지원해야 합니다.
- 디바이스에서 BGP(Border Gateway Protocol)와 BGP MD5 인증을 지원해야 합니다.
- (선택 사항) 네트워크에 BFD(Bidirectional Forwarding Detection)를 구성할 수 있습니다. 각 AWS Direct Connect 가상 인터페이스에 대해 비동기 BFD가 자동으로 활성화됩니다. Direct Connect 가상 인터페이스에 대해서는 자동으로 활성화되지만, 라우터에서 이를 구성해야만 작동이 시작됩니다. 자세한 내용은 Direct Connect 연결을 위한 BFD 활성화를 참조하세요.

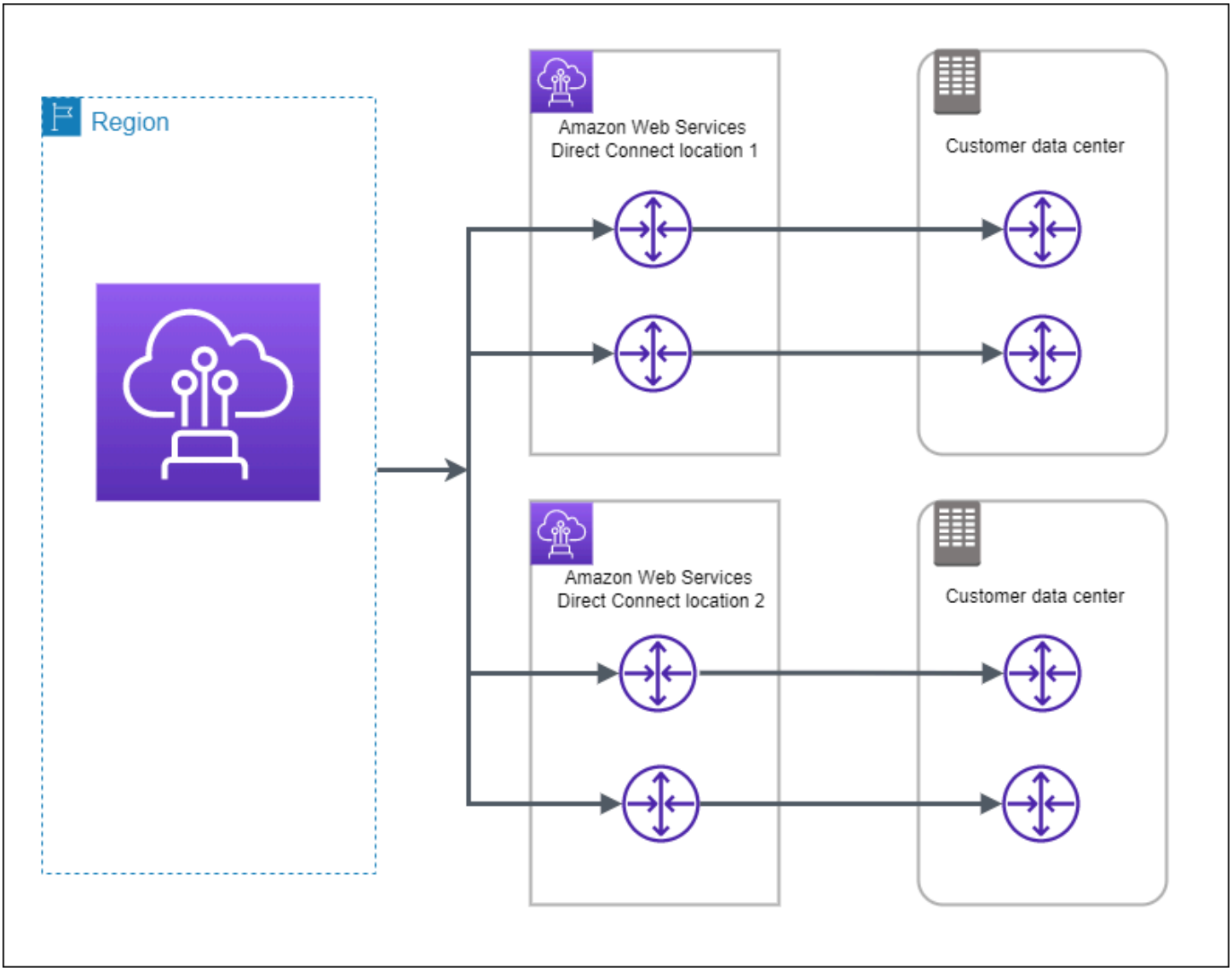
구성을 시작하기 전에 다음 정보가 있는지 확인합니다.

- 사용할 복원 모델
- 모든 연결에 대한 속도, 위치 및 파트너

  하나의 연결을 위한 속도만 필요합니다.

최대 복원성

둘 이상 위치의 개별 디바이스에서 종료하는 별도의 연결을 사용하여 중요 워크로드에 대해 최대 복원성을 확보할 수 있습니다 이 모델은 디바이스, 연결, 전체 위치 오류에 대한 복원성을 제공합니다. 다음 그림은 각 고객 데이터 센터에서 동일한 AWS Direct Connect 위치로 연결되는 두 연결을 보여줍니다. 필요에 따라 고객 데이터 센터의 각 연결을 서로 다른 위치로 연결할 수 있습니다.



다음 절차는 AWS Direct Connect 복원력 툴킷을 사용하여 최대 복원력 모델을 구성하는 방법을 보여줍니다.

주제

- 1단계: AWS 가입
- 2단계: 복원 모델 구성
- 3단계: 가상 인터페이스 생성
- 4단계: 가상 인터페이스 복원력 구성 확인
- 5단계: 가상 인터페이스 연결 확인

1단계: AWS 가입

AWS Direct Connect를 사용하려면 AWS 계정이 있어야 합니다(아직 없는 경우).

AWS 계정에 등록

AWS 계정 항목이 없으면 다음 절차에 따라 생성하십시오.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자 항목이 생성됩니다. 루트 사용자에게 계정의 모든 AWS 서비스 및 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS가 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자를 보안하며 AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자 보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) 섹션을 참조하십시오.

관리 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서에서 Enabling AWS IAM Identity Center를 참조하세요.

2. IAM Identity Center에서 관리 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 Configure user access with the default IAM Identity Center 디렉터리를 참조하세요.

관리 사용자로 로그인

- IAM 자격 증명 센터 사용자로 로그인하려면 IAM 자격 증명 센터 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.

2단계: 복원 모델 구성

최대 복원성 모델을 구성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택한 다음 연결 생성을 선택합니다.
3. 연결 순서 유형에서 Connection Wizard를 선택합니다.
4. 복원성 수준에서 최대 복원성을 선택한 후 다음을 선택합니다.
5. 연결 구성 창의 연결 설정에서 다음을 수행합니다.

   a. 대역폭에서 전용 연결 대역폭을 선택합니다.

      이 대역폭은 생성된 모든 연결에 적용됩니다.

   b. 첫 번째 위치 서비스 공급자에서 전용 연결을 위한 적절한 AWS Direct Connect 위치를 선택합니다.

c. 해당되는 경우, 첫 번째 하위 위치에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

d. 최초 위치 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

e. 두 번째 위치 서비스 공급자에서 적절한 AWS Direct Connect 위치를 선택합니다.

f. 해당되는 경우, 두 번째 하위 위치에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

g. 두 번째 위치 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

h. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

6. 다음을 선택합니다.
7. 연결을 검토한 다음 계속을 선택합니다.

   LOA가 준비되면 LOA 다운로드를 선택한 다음 계속을 클릭합니다.

   AWS가 요청을 검토하고 연결용 포트를 프로비저닝하려면 최대 72시간이 걸릴 수 있습니다. 이 시간 동안 사용 사례 또는 지정된 위치에 대한 추가 정보를 요청하는 이메일을 받을 수 있습니다. 이 이메일은 AWS에 가입할 때 사용한 이메일 주소로 발송됩니다. 7일 이내에 응답해야 하며, 그렇지 않으면 연결이 삭제됩니다.

3단계: 가상 인터페이스 생성

가상 프라이빗 인터페이스를 생성하여 VPC에 연결할 수 있습니다. 또는 퍼블릭 가상 인터페이스를 생성하여 VPC에 없는 퍼블릭 AWS 서비스에 연결할 수 있습니다. VPC에 대한 프라이빗 가상 인터페이스를 만드는 경우, 연결할 VPC마다 하나의 프라이빗 가상 인터페이스가 필요합니다. 예를 들어 3개의 VPC에 연결하려면 프라이빗 가상 인터페이스도 3개가 필요합니다.

시작하기 전에 다음 정보가 있는지 확인하십시오.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다. 호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.
피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러 BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다. • IPv4:

Resource	필수 정보

	• (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	• (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다.
	• IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.

Resource	필수 정보
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

Resource	필수 정보
(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

퍼블릭 접두사 또는 ASN이 ISP 또는 네트워크 사업자에 속하는 경우, 추가 정보를 요청합니다. 이것은 공식 회사 편지지를 사용하는 문서가 될 수도 있고 네트워크 접두사/ASN을 사용자가 사용할 수 있음을 확인하는, 회사 도메인 이름에서 전송된 이메일이 될 수도 있습니다.

퍼블릭 가상 인터페이스를 만드는 경우, AWS가 요청을 검토하고 승인하는 데 최대 72시간이 걸릴 수 있습니다.

비 VPC 서비스에 연결되는 가상 퍼블릭 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 여십시오. AWS Direct Connect
2. 탐색 창에서 가상 인터페이스를 선택합니다.

3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public virtual interface settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   d. BGP ASN에 게이트웨이의 BGP(Border Gateway Protocol) ASN(자율 시스템 번호)을 입력합니다.

      유효한 값은 1-2147483647입니다.
6. 추가 설정 아래에서 다음을 수행합니다.

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. 직접 BGP 키를 제공하려면 BGP MD5 키를 입력합니다.

      값을 입력하지 않으면 BGP 키가 생성됩니다.

   c. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.

   d. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
7. 가상 인터페이스 생성을 선택합니다.

VPC에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. 게이트웨이 유형에 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이를 선택합니다.

   d. 가상 인터페이스 소유자는 다른 AWS 계정을 선택한 다음 AWS 계정을 입력합니다.

   e. 가상 프라이빗 게이트웨이에 이 인터페이스에 사용할 가상 프라이빗 게이트웨이를 선택합니다.

   f. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   g. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1~2147483647입니다.
6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다.

- RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
- RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

4단계: 가상 인터페이스 복원력 구성 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 설정한 후 가상 인터페이스 장애 조치 테스트를 수행하여 구성이 복원력 요구 사항을 충족하는지 확인합니다. 자세한 설명은 the section called "AWS Direct Connect 장애 조치 테스트" 섹션을 참조하세요.

5단계: 가상 인터페이스 연결 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 구성한 후에는 다음 절차에 따라 AWS Direct Connect 연결을 확인할 수 있습니다.

AWS 클라우드에 대한 가상 인터페이스 연결을 확인하는 방법

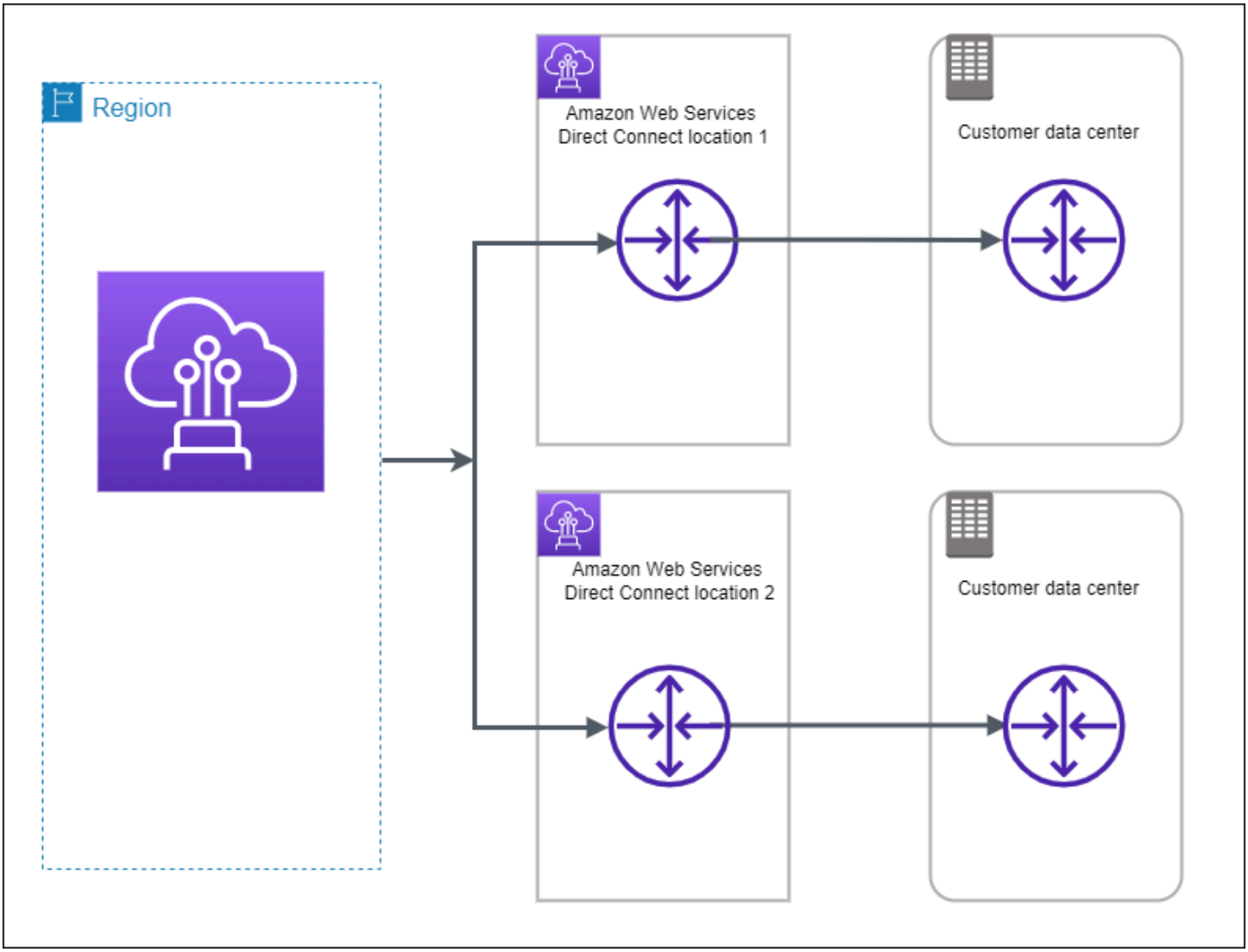
- `traceroute`를 실행하고 AWS Direct Connect 식별자가 네트워크 추적에 있는지 확인합니다.

Amazon VPC에 대한 가상 인터페이스 연결을 확인하는 방법

1. Amazon Linux AMI 같이 ping할 수 있는 AMI를 사용하여 가상 프라이빗 게이트웨이에 연결되는 VPC로 EC2 인스턴스를 시작합니다. Amazon EC2 콘솔의 인스턴스 시작 마법사를 사용하면 빠른 시작 탭에서 Amazon Linux AMI를 사용할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하세요. 인스턴스와 연결되는 보안 그룹이 인바운드 ICMP 트래픽을 허용하는 규칙을 포함해야 합니다(핑 요청을 위해).
2. 인스턴스가 실행되고 나면 프라이빗 IPv4 주소(예: 10.0.0.4)를 얻게 됩니다. Amazon EC2 콘솔에 주소가 인스턴스 세부 정보의 일부로 표시됩니다.
3. 프라이빗 IPv4 주소를 ping하고 응답을 받습니다.

높은 복원성

여러 위치에 두 개의 단일 연결을 사용하여 중요 워크로드에 대한 높은 복원성을 확보할 수 있습니다(아래 그림 참조). 이 모델은 광섬유 절단 또는 디바이스 오류로 인해 발생하는 연결 오류에 대한 복원성을 제공합니다. 또한 전체 위치 오류를 방지하는 데에도 도움이 됩니다.



다음 절차는 AWS Direct Connect 복원력 툴킷을 사용하여 높은 복원력 모델을 구성하는 방법을 보여줍니다.

주제

- 1단계: AWS 가입
- 2단계: 복원 모델 구성
- 3단계: 가상 인터페이스 생성
- 4단계: 가상 인터페이스 복원력 구성 확인
- 5단계: 가상 인터페이스 연결 확인

1단계: AWS 가입

AWS Direct Connect를 사용하려면 AWS 계정이 있어야 합니다(아직 없는 경우).

AWS 계정에 등록

AWS 계정 항목이 없으면 다음 절차에 따라 생성하십시오.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자 항목이 생성됩니다. 루트 사용자에게 계정의 모든 AWS 서비스 및 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS가 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자를 보안하며 AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자 보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) 섹션을 참조하십시오.

관리 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서에서 Enabling AWS IAM Identity Center를 참조하세요.

2. IAM Identity Center에서 관리 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 Configure user access with the default IAM Identity Center 디렉터리를 참조하세요.

관리 사용자로 로그인

- IAM 자격 증명 센터 사용자로 로그인하려면 IAM 자격 증명 센터 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.

2단계: 복원 모델 구성

높은 복원성 모델을 구성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택한 다음 연결 생성을 선택합니다.
3. 연결 순서 유형에서 Connection Wizard를 선택합니다.
4. 복원성 수준에서 높은 복원성을 선택한 후 다음을 선택합니다.
5. 연결 구성 창의 연결 설정에서 다음을 수행합니다.

   a. 대역폭에서 연결 대역폭을 선택합니다.

      이 대역폭은 생성된 모든 연결에 적용됩니다.

   b. 첫 번째 위치 서비스 공급자에서 적절한 AWS Direct Connect 위치를 선택합니다.

c. 해당되는 경우, 첫 번째 하위 위치에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

d. 최초 위치 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

e. 두 번째 위치 서비스 공급자에서 적절한 AWS Direct Connect 위치를 선택합니다.

f. 해당되는 경우, 두 번째 하위 위치에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

g. 두 번째 위치 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

h. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

6. 다음을 선택합니다.
7. 연결을 검토한 다음 계속을 선택합니다.

   LOA가 준비되면 LOA 다운로드를 선택한 다음 계속을 클릭합니다.

   AWS가 요청을 검토하고 연결용 포트를 프로비저닝하려면 최대 72시간이 걸릴 수 있습니다. 이 시간 동안 사용 사례 또는 지정된 위치에 대한 추가 정보를 요청하는 이메일을 받을 수 있습니다. 이 이메일은 AWS에 가입할 때 사용한 이메일 주소로 발송됩니다. 7일 이내에 응답해야 하며, 그렇지 않으면 연결이 삭제됩니다.

3단계: 가상 인터페이스 생성

가상 프라이빗 인터페이스를 생성하여 VPC에 연결할 수 있습니다. 또는 퍼블릭 가상 인터페이스를 생성하여 VPC에 없는 퍼블릭 AWS 서비스에 연결할 수 있습니다. VPC에 대한 프라이빗 가상 인터페이스를 만드는 경우, 연결할 VPC마다 하나의 프라이빗 가상 인터페이스가 필요합니다. 예를 들어 3개의 VPC에 연결하려면 프라이빗 가상 인터페이스도 3개가 필요합니다.

시작하기 전에 다음 정보가 있는지 확인하십시오.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다. 호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.
피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러 BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다. • IPv4:

Resource	필수 정보

	• (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	• (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다.
	• IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.

Resource	필수 정보
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

Resource	필수 정보
(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

퍼블릭 접두사 또는 ASN이 ISP 또는 네트워크 사업자에 속하는 경우, AWS가 추가 정보를 요청합니다. 이것은 공식 회사 편지지를 사용하는 문서가 될 수도 있고 네트워크 접두사/ASN을 사용자가 사용할 수 있음을 확인하는, 회사 도메인 이름에서 전송된 이메일이 될 수도 있습니다.

퍼블릭 가상 인터페이스를 만드는 경우, AWS가 요청을 검토하고 승인하는 데 최대 72시간이 걸릴 수 있습니다.

비 VPC 서비스에 연결되는 가상 퍼블릭 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 여십시오. AWS Direct Connect
2. 탐색 창에서 가상 인터페이스를 선택합니다.

3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public virtual interface settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   d. BGP ASN에 게이트웨이의 BGP(Border Gateway Protocol) ASN(자율 시스템 번호)을 입력합니다.

      유효한 값은 1-2147483647입니다.
6. 추가 설정 아래에서 다음을 수행합니다.

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. 직접 BGP 키를 제공하려면 BGP MD5 키를 입력합니다.

      값을 입력하지 않으면 BGP 키가 생성됩니다.

   c. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.

   d. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
7. 가상 인터페이스 생성을 선택합니다.

VPC에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. 게이트웨이 유형에 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이를 선택합니다.

   d. 가상 인터페이스 소유자는 다른 AWS 계정을 선택한 다음 AWS 계정을 입력합니다.

   e. 가상 프라이빗 게이트웨이에 이 인터페이스에 사용할 가상 프라이빗 게이트웨이를 선택합니다.

   f. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   g. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1~2147483647입니다.
6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다.

- RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
- RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

4단계: 가상 인터페이스 복원력 구성 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 설정한 후 가상 인터페이스 장애 조치 테스트를 수행하여 구성이 복원력 요구 사항을 충족하는지 확인합니다. 자세한 설명은 the section called “AWS Direct Connect 장애 조치 테스트” 섹션을 참조하세요.

5단계: 가상 인터페이스 연결 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 구성한 후에는 다음 절차에 따라 AWS Direct Connect 연결을 확인할 수 있습니다.

AWS 클라우드에 대한 가상 인터페이스 연결을 확인하는 방법

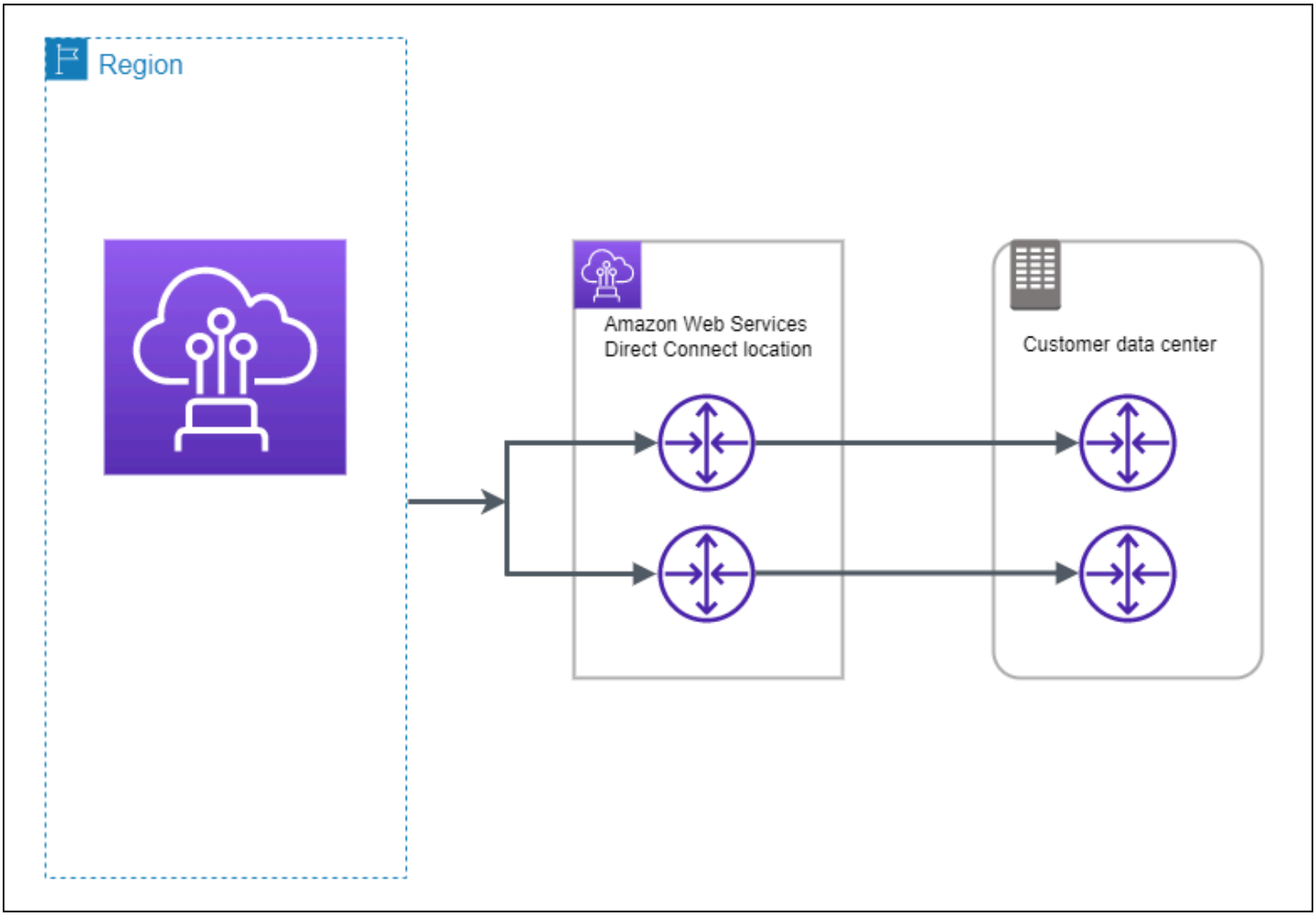
- `traceroute`를 실행하고 AWS Direct Connect 식별자가 네트워크 추적에 있는지 확인합니다.

Amazon VPC에 대한 가상 인터페이스 연결을 확인하는 방법

1. Amazon Linux AMI 같이 ping할 수 있는 AMI를 사용하여 가상 프라이빗 게이트웨이에 연결되는 VPC로 EC2 인스턴스를 시작합니다. Amazon EC2 콘솔의 인스턴스 시작 마법사를 사용하면 빠른 시작 탭에서 Amazon Linux AMI를 사용할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하세요. 인스턴스와 연결되는 보안 그룹이 인바운드 ICMP 트래픽을 허용하는 규칙을 포함해야 합니다(핑 요청을 위해).
2. 인스턴스가 실행되고 나면 프라이빗 IPv4 주소(예: 10.0.0.4)를 얻게 됩니다. Amazon EC2 콘솔에 주소가 인스턴스 세부 정보의 일부로 표시됩니다.
3. 프라이빗 IPv4 주소를 ping하고 응답을 받습니다.

개발 및 테스트

한 위치의 개별 디바이스에서 종료하는 별도의 연결을 사용하여 중요하지 않은 워크로드에 대한 개발 및 테스트 복원성을 확보할 수 있습니다(아래 그림 참조). 이 모델은 디바이스 오류에 대한 복원성은 제공하지만 위치 오류에 대한 복원성은 제공하지 않습니다.



다음 절차는 AWS Direct Connect 복원력 툴킷을 사용하여 개발 및 테스트 복원 모델을 구성하는 방법을 보여줍니다.

주제

- 1단계: AWS 가입
- 2단계: 복원 모델 구성
- 3단계: 가상 인터페이스 생성
- 4단계: 가상 인터페이스 복원력 구성 확인
- 5단계: 가상 인터페이스 확인

1단계: AWS 가입

AWS Direct Connect를 사용하려면 AWS 계정이 있어야 합니다(아직 없는 경우).

AWS 계정에 등록

AWS 계정 항목이 없으면 다음 절차에 따라 생성하십시오.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자 항목이 생성됩니다. 루트 사용자에게 계정의 모든 AWS 서비스 및 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS가 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자를 보안하며 AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자 보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) 섹션을 참조하십시오.

관리 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서에서 Enabling AWS IAM Identity Center를 참조하세요.

2. IAM Identity Center에서 관리 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 Configure user access with the default IAM Identity Center 디렉터리를 참조하세요.

관리 사용자로 로그인

- IAM 자격 증명 센터 사용자로 로그인하려면 IAM 자격 증명 센터 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.

2단계: 복원 모델 구성

복원 모델을 구성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택한 다음 연결 생성을 선택합니다.
3. 연결 순서 유형에서 Connection Wizard를 선택합니다.
4. 복원성 수준에서 개발 및 테스트를 선택한 후 다음을 선택합니다.
5. 연결 구성 창의 연결 설정에서 다음을 수행합니다.

   a. 대역폭에서 연결 대역폭을 선택합니다.

      이 대역폭은 생성된 모든 연결에 적용됩니다.

   b. 첫 번째 위치 서비스 공급자에서 적절한 AWS Direct Connect 위치를 선택합니다.

   c. 해당되는 경우, 첫 번째 하위 위치에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

   d. 최초 위치 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

e. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

6. 다음을 선택합니다.
7. 연결을 검토한 다음 계속을 선택합니다.

   LOA가 준비되면 LOA 다운로드를 선택한 다음 계속을 클릭합니다.

   AWS가 요청을 검토하고 연결용 포트를 프로비저닝하려면 최대 72시간이 걸릴 수 있습니다. 이 시간 동안 사용 사례 또는 지정된 위치에 대한 추가 정보를 요청하는 이메일을 받을 수 있습니다. 이 이메일은 AWS에 가입할 때 사용한 이메일 주소로 발송됩니다. 7일 이내에 응답해야 하며, 그렇지 않으면 연결이 삭제됩니다.

3단계: 가상 인터페이스 생성

AWS Direct Connect 연결 사용을 시작하려면 가상 인터페이스를 만들어야 합니다. 가상 프라이빗 인터페이스를 생성하여 VPC에 연결할 수 있습니다. 또는 퍼블릭 가상 인터페이스를 생성하여 VPC에 없는 퍼블릭 AWS 서비스에 연결할 수 있습니다. VPC에 대한 프라이빗 가상 인터페이스를 만드는 경우, 연결할 VPC마다 하나의 프라이빗 가상 인터페이스가 필요합니다. 예를 들어 3개의 VPC에 연결하려면 프라이빗 가상 인터페이스도 3개가 필요합니다.

시작하기 전에 다음 정보가 있는지 확인하십시오.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.

Resource	필수 정보
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다. 호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.

Resource	필수 정보

피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러 BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다.
	
	• IPv4:
	  • (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	  • (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0`

Resource	필수 정보
	`.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다. • IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

Resource	필수 정보

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

Resource	필수 정보
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

퍼블릭 접두사 또는 ASN이 ISP 또는 네트워크 사업자에 속하는 경우, 추가 정보를 요청합니다. 이것은 공식 회사 편지지를 사용하는 문서가 될 수도 있고 네트워크 접두사/ASN을 사용자가 사용할 수 있음을 확인하는, 회사 도메인 이름에서 전송된 이메일이 될 수도 있습니다.

퍼블릭 가상 인터페이스를 만드는 경우, AWS가 요청을 검토하고 승인하는 데 최대 72시간이 걸릴 수 있습니다.

비 VPC 서비스에 연결되는 가상 퍼블릭 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 여십시오. AWS Direct Connect
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public virtual interface settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.
   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.
   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.
   c. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.
   d. BGP ASN에 게이트웨이의 BGP(Border Gateway Protocol) ASN(자율 시스템 번호)을 입력합니다.

유효한 값은 1-2147483647입니다.

6. 추가 설정 아래에서 다음을 수행합니다.

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. 직접 BGP 키를 제공하려면 BGP MD5 키를 입력합니다.

      값을 입력하지 않으면 BGP 키가 생성됩니다.

   c. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.

   d. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

VPC에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

c. 게이트웨이 유형에 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이를 선택합니다.

d. 가상 인터페이스 소유자는 다른 AWS 계정을 선택한 다음 AWS 계정을 입력합니다.

e. 가상 프라이빗 게이트웨이에 이 인터페이스에 사용할 가상 프라이빗 게이트웨이를 선택합니다.

f. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

g. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

   유효한 값은 1~2147483647입니다.

6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다.
      >
      > - RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
      > - RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

4단계: 가상 인터페이스 복원력 구성 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 설정한 후 가상 인터페이스 장애 조치 테스트를 수행하여 구성이 복원력 요구 사항을 충족하는지 확인합니다. 자세한 설명은 the section called "AWS Direct Connect 장애 조치 테스트" 섹션을 참조하세요.

5단계: 가상 인터페이스 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 구성한 후에는 다음 절차에 따라 AWS Direct Connect 연결을 확인할 수 있습니다.

AWS 클라우드에 대한 가상 인터페이스 연결을 확인하는 방법

- `traceroute`를 실행하고 AWS Direct Connect 식별자가 네트워크 추적에 있는지 확인합니다.

Amazon VPC에 대한 가상 인터페이스 연결을 확인하는 방법

1. Amazon Linux AMI 같이 ping할 수 있는 AMI를 사용하여 가상 프라이빗 게이트웨이에 연결되는 VPC로 EC2 인스턴스를 시작합니다. Amazon EC2 콘솔의 인스턴스 시작 마법사를 사용하면 빠른 시작 탭에서 Amazon Linux AMI를 사용할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하세요. 인스턴스와 연결되는 보안 그룹이 인바운드 ICMP 트래픽을 허용하는 규칙을 포함해야 합니다(핑 요청을 위해).
2. 인스턴스가 실행되고 나면 프라이빗 IPv4 주소(예: 10.0.0.4)를 얻게 됩니다. Amazon EC2 콘솔에 주소가 인스턴스 세부 정보의 일부로 표시됩니다.
3. 프라이빗 IPv4 주소를 ping하고 응답을 받습니다.

클래식

기존 연결이 있는 경우 클래식을 선택합니다.

다음 절차는 AWS Direct Connect 연결을 설정하는 일반적 시나리오를 보여 줍니다.

내용

- 사전 조건
- 1단계: AWS 가입
- 2단계: AWS Direct Connect 전용 연결 요청
- (전용 연결) 3단계: LOA-CFA 다운로드
- 4단계: 가상 인터페이스 생성
- 5단계: 라우터 구성 다운로드
- 6단계: 가상 인터페이스 확인
- (권장 사항) 7단계: 중복 연결 구성

사전 조건

포트 속도가 1Gbps 이상인 AWS Direct Connect 연결의 경우, 네트워크가 다음 요구 사항을 충족해야 합니다.

- 사용자의 네트워크는 1기가비트 이더넷의 경우 1000BASE-LX(1310nm) 송수신장치, 10기가비트 이더넷의 경우 10GBASE-LR(1310nm) 송수신장치, 100기가비트 이더넷의 경우 100GBASE-LR4가 있는 단일 모드 광섬유를 사용해야 합니다.
- 포트 속도가 1Gbps를 초과하는 연결의 경우 포트 자동 협상을 비활성화해야 합니다. 하지만 연결을 담당하는 AWS Direct Connect 엔드포인트에 따라 1Gbps 연결에 대해 자동 협상을 활성화하거나 비활성화해야 할 수도 있습니다. 가상 인터페이스가 계속 다운되는 경우 계층 2(데이터 링크) 문제 해결를 참조하세요.
- 중간 디바이스를 비롯하여 네트워크 전체적으로 802.1Q VLAN 캡슐화를 지원해야 합니다.
- 디바이스에서 BGP(Border Gateway Protocol)와 BGP MD5 인증을 지원해야 합니다.
- (선택 사항) 네트워크에 BFD(Bidirectional Forwarding Detection)를 구성할 수 있습니다. 각 AWS Direct Connect 가상 인터페이스에 대해 비동기 BFD가 자동으로 활성화됩니다. Direct Connect 가상 인터페이스에 대해서는 자동으로 활성화되지만, 라우터에서 이를 구성해야만 작동이 시작됩니다. 자세한 내용은 Direct Connect 연결을 위한 BFD 활성화를 참조하세요.

1단계: AWS 가입

AWS Direct Connect를 사용하려면 계정이 있어야 합니다(아직 없는 경우).

AWS 계정에 등록

AWS 계정 항목이 없으면 다음 절차에 따라 생성하십시오.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자 항목이 생성됩니다. 루트 사용자에게 계정의 모든 AWS 서비스 및 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS가 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자를 보안하며 AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자 보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) 섹션을 참조하십시오.

관리 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서에서 Enabling AWS IAM Identity Center를 참조하세요.

2. IAM Identity Center에서 관리 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 Configure user access with the default IAM Identity Center 디렉터리를 참조하세요.

관리 사용자로 로그인

- IAM 자격 증명 센터 사용자로 로그인하려면 IAM 자격 증명 센터 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.

2단계: AWS Direct Connect 전용 연결 요청

전용 연결의 경우 AWS Direct Connect 콘솔을 사용하여 연결 요청을 제출할 수 있습니다. 호스팅 연결의 경우 AWS Direct Connect 파트너와 협력하여 호스팅 연결을 요청합니다. 다음 정보가 있는지 확인합니다.

- 필요한 포트 속도입니다. 연결 요청을 생성한 후에는 포트 속도를 변경할 수 없습니다.
- 연결이 종료될 AWS Direct Connect 위치입니다.

> **Note**
>
> AWS Direct Connect 콘솔을 사용하여 호스팅 연결을 요청할 수 없습니다. 대신 AWS Direct Connect 파트너에 연락하여 해당 파트너가 사용자를 대신하여 호스팅 연결을 생성하면 그 다음 이를 수락하면 됩니다. 다음 절차를 건너뛰고 호스팅 연결 수락 단원으로 이동합니다.

새로운 AWS Direct Connect 연결을 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택한 다음 연결 생성을 선택합니다.
3. 클래식을 선택합니다.
4. 연결 생성 창의 연결 설정 아래에서 다음을 수행합니다.

   a. 이름에 연결의 이름을 입력합니다.

   b. 위치에서 적절한 AWS Direct Connect 위치를 선택합니다.

   c. 해당되는 경우, [Sub Location]에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.

   d. 포트 속도에서 연결 대역폭을 선택합니다.

   e. 온프레미스는 이 연결을 사용하여 데이터 센터에 연결할 때 파트너를 통해 연결AWS Direct Connect을 선택합니다.

   f. 서비스 공급자에 대해 AWS Direct Connect 파트너를 선택합니다. 목록에 없는 공급자를 이용하는 경우 기타를 선택합니다.

   g. 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.

   h. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

5. 연결 생성을 선택합니다.

AWS가 요청을 검토하고 연결용 포트를 프로비저닝하려면 최대 72시간이 걸릴 수 있습니다. 이 시간 동안 사용 사례 또는 지정된 위치에 대한 추가 정보를 요청하는 이메일을 받을 수 있습니다. 이 이메일은 AWS에 가입할 때 사용한 이메일 주소로 발송됩니다. 7일 이내에 응답해야 하며, 그렇지 않으면 연결이 삭제됩니다.

자세한 설명은 AWS Direct Connect 연결 섹션을 참조하세요.

호스팅 연결 수락

먼저 AWS Direct Connect 콘솔에서 호스팅 연결을 수락해야 가상 인터페이스를 생성할 수 있습니다. 이 단계는 호스팅된 연결에만 적용됩니다.

호스팅 가상 인터페이스를 수락하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 호스팅된 연결을 선택한 다음 수락을 선택합니다.

   수락을 선택합니다.

(전용 연결) 3단계: LOA-CFA 다운로드

연결을 요청한 후에는 다운로드할 수 있는 LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 제공하거나 추가 정보를 요청하는 이메일을 보냅니다. LOA-CFA는 AWS 연결에 대한 승인이며, 콜로케이션 공급자 또는 네트워크 공급자가 교차 네트워크 연결(교차 연결)을 설정하기 위해 필요합니다.

LOA-CFA를 다운로드하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 연결을 선택하고 세부 정보 보기를 선택합니다.
4. LOA-CFA 다운로드를 선택합니다.

   LOA-CFA는 PDF 파일로 컴퓨터에 다운로드됩니다.

   > **Note**
   >
   > 이 링크가 활성화되지 않았다면 아직 LOA-CFA를 다운로드할 수 없는 것입니다. 추가 정보 요청 이메일이 있는지 확인하십시오. 여전히 링크를 사용할 수 없을 경우, 또는 72시간 후에도 이메일을 수신하지 못한 경우 AWS Support에 문의하세요.

5. LOA-CFA를 다운로드한 후 다음 중 하나를 수행합니다.

- AWS Direct Connect 파트너 또는 네트워크 공급자와 협력 중인 경우 AWS Direct Connect 위치에서 사용자 대신 교차 연결을 주문할 수 있도록 이들에게 LOA-CFA를 보냅니다. APN 멤버나 네트워크 공급자가 교차 연결을 대신 주문할 수 없는 경우, 코로케이션 공급자에게 직접 연락할 수 있습니다.
- AWS Direct Connect 위치에 장비가 있는 경우 코로케이션 공급자에게 연락하여 교차 네트워크 연결을 요청합니다. 코로케이션 공급자의 고객이어야 합니다. 또한 콜로케이션 공급자에게 AWS 라우터 연결을 승인하는 LOA-CFA와 네트워크 연결에 필요한 정보를 제공해야 합니다.

여러 사이트로 등재된 AWS Direct Connect 위치(예: Equinix DC1-DC6 & DC10-DC11)는 캠퍼스로 설정됩니다. 사용자 또는 네트워크 공급자의 장비가 이러한 사이트에 있는 경우 다른 캠퍼스 건물에 있더라도 할당된 포트에 대한 교차 연결을 요청할 수 있습니다.

> **Important**
>
> 캠퍼스는 하나의 AWS Direct Connect 위치로 간주됩니다. 높은 가용성을 얻으려면 여러 AWS Direct Connect 위치로 연결을 구성하십시오.

사용자 또는 네트워크 공급자가 물리적 연결 설정에 문제를 겪는 경우 계층 1(물리적) 문제 해결 단원을 참조하십시오.

4단계: 가상 인터페이스 생성

AWS Direct Connect 연결 사용을 시작하려면 가상 인터페이스를 만들어야 합니다. 가상 프라이빗 인터페이스를 생성하여 VPC에 연결할 수 있습니다. 또는 퍼블릭 가상 인터페이스를 생성하여 VPC에 없는 퍼블릭 AWS 서비스에 연결할 수 있습니다. VPC에 대한 프라이빗 가상 인터페이스를 만드는 경우, 연결할 VPC마다 하나의 프라이빗 가상 인터페이스가 필요합니다. 예를 들어 3개의 VPC에 연결하려면 프라이빗 가상 인터페이스도 3개가 필요합니다.

시작하기 전에 다음 정보가 있는지 확인하십시오.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.

Resource	필수 정보
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다. 호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.

Resource	필수 정보

피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러 BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다.
	
	• IPv4:
	  • (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	  • (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0`

Resource	필수 정보
	`.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다. • IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

Resource	필수 정보

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

Resource	필수 정보
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

퍼블릭 접두사 또는 ASN이 ISP 또는 네트워크 사업자에 속하는 경우, 추가 정보를 요청합니다. 이것은 공식 회사 편지지를 사용하는 문서가 될 수도 있고 네트워크 접두사/ASN을 사용자가 사용할 수 있음을 확인하는, 회사 도메인 이름에서 전송된 이메일이 될 수도 있습니다.

프라이빗 가상 인터페이스 및 퍼블릭 가상 인터페이스의 경우 네트워크 연결의 최대 전송 단위(MTU)는 연결을 통해 전달될 수 있는 최대 허용 가능 패킷의 크기(바이트)입니다. 가상 프라이빗 인터페이스의 MTU는 1500 또는 9001(점보 프레임)일 수 있습니다. 전송 가상 인터페이스의 MTU는 1500 또는 8500(점보 프레임)일 수 있습니다. 인터페이스를 만들 때 또는 만든 후 업데이트할 때 MTU를 지정할 수 있습니다. 가상 인터페이스의 MTU를 8500(점보 프레임) 또는 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 요약 탭에서 점보 프레임 가능을 찾습니다.

퍼블릭 가상 인터페이스를 만드는 경우, AWS가 요청을 검토하고 승인하는 데 최대 72시간이 걸릴 수 있습니다.

비 VPC 서비스에 연결되는 가상 퍼블릭 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 여십시오. AWS Direct Connect
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.

4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public virtual interface settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   d. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 BGP(Border Gateway Protocol) 자율 시스템 번호를 입력합니다.

      유효한 값은 1-2147483647입니다.
6. 추가 설정 아래에서 다음을 수행합니다.

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. 직접 BGP 키를 제공하려면 BGP MD5 키를 입력합니다.

      값을 입력하지 않으면 BGP 키가 생성됩니다.

   c. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.

   d. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
7. 가상 인터페이스 생성을 선택합니다.

VPC에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. 게이트웨이 유형에 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이를 선택합니다.

   d. 가상 인터페이스 소유자는 다른 AWS 계정을 선택한 다음 AWS 계정을 입력합니다.

   e. 가상 프라이빗 게이트웨이에 이 인터페이스에 사용할 가상 프라이빗 게이트웨이를 선택합니다.

   f. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   g. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1~2147483647입니다.
6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다.

- RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
- RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.
8. BGP 장치를 사용하여 퍼블릭 VIF 연결에 사용하는 네트워크를 알려야 합니다.

5단계: 라우터 구성 다운로드

AWS Direct Connect 연결을 위한 가상 인터페이스를 생성한 후에는 라우터 구성 파일을 다운로드할 수 있습니다. 이 파일에는 프라이빗 또는 퍼블릭 가상 인터페이스에 사용할 라우터를 구성하는 데 필요한 명령이 포함되어 있습니다.

라우터 구성을 다운로드하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 연결을 선택하고 세부 정보 보기를 선택합니다.
4. 라우터 구성 다운로드를 선택합니다.
5. 라우터 구성 다운로드에서 다음을 수행합니다.

   a. 공급업체에서 라우터의 제조업체를 선택합니다.

   b. 플랫폼에서 라우터의 모델을 선택합니다.
   c. 소프트웨어에서 라우터의 소프트웨어 버전을 선택합니다.
6. Download(다운로드)를 선택한 다음 라우터에 적합한 구성을 사용하여 AWS Direct Connect에 연결할 수 있는지 확인합니다.

구성 파일의 예는 라우터 구성 파일 예를 참조하십시오.

라우터를 구성한 후 가상 인터페이스의 상태가 UP으로 바뀝니다. 가상 인터페이스가 여전히 down 상태이고 AWS Direct Connect 디바이스의 피어 IP 주소를 ping할 수 없다면 계층 2(데이터 링크) 문제 해결 단원을 참조하십시오. 피어 IP 주소를 ping할 수 있다면 계층 3/4(네트워크/전송) 문제 해결 단원을 참조하십시오. BGP 피어링 세션이 설정되었지만 트래픽을 라우팅할 수 없다면 라우팅 문제 해결 단원을 참조하십시오.

6단계: 가상 인터페이스 확인

AWS 클라우드 또는 Amazon VPC에 대한 가상 인터페이스를 구성한 후에는 다음 절차에 따라 AWS Direct Connect 연결을 확인할 수 있습니다.

AWS 클라우드에 대한 가상 인터페이스 연결을 확인하는 방법

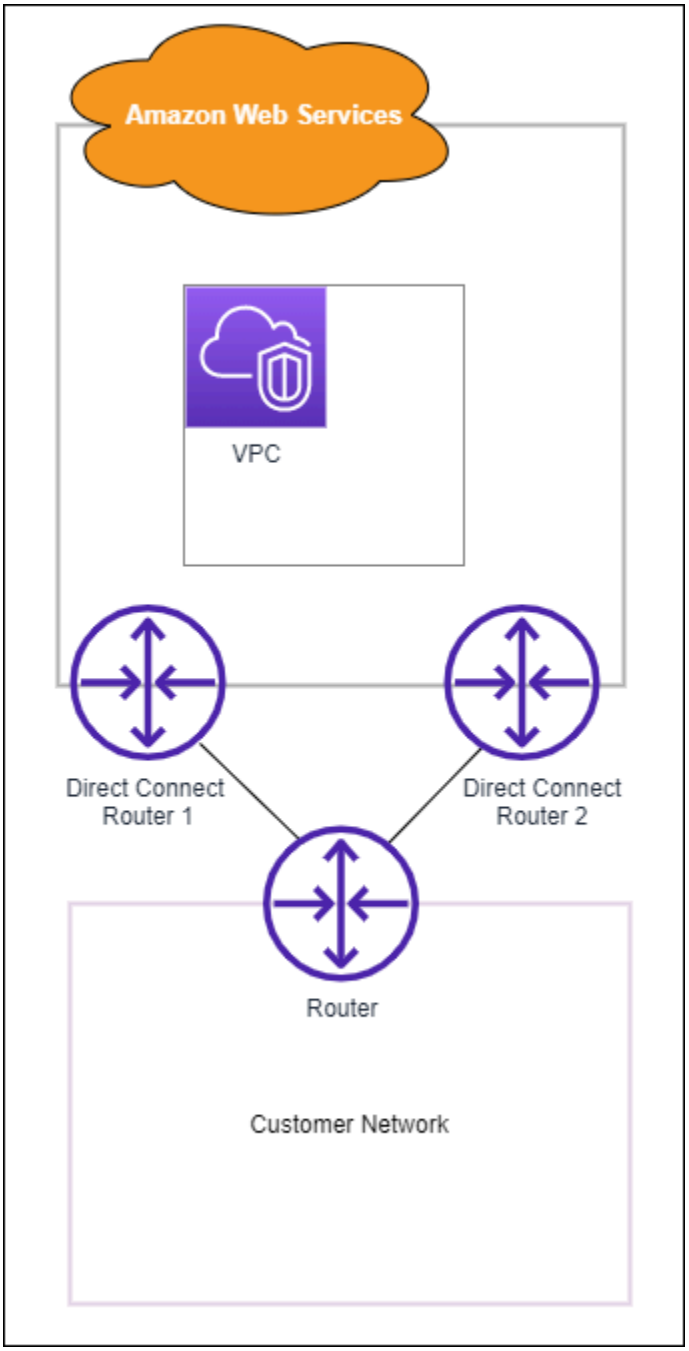
- `traceroute`를 실행하고 AWS Direct Connect 식별자가 네트워크 추적에 있는지 확인합니다.

Amazon VPC에 대한 가상 인터페이스 연결을 확인하는 방법

1. Amazon Linux AMI 같이 ping할 수 있는 AMI를 사용하여 가상 프라이빗 게이트웨이에 연결되는 VPC로 EC2 인스턴스를 시작합니다. Amazon EC2 콘솔의 인스턴스 시작 마법사를 사용하면 빠른 시작 탭에서 Amazon Linux AMI를 사용할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하세요. 인스턴스와 연결되는 보안 그룹이 인바운드 ICMP 트래픽을 허용하는 규칙을 포함해야 합니다(핑 요청을 위해).
2. 인스턴스가 실행되고 나면 프라이빗 IPv4 주소(예: 10.0.0.4)를 얻게 됩니다. Amazon EC2 콘솔에 주소가 인스턴스 세부 정보의 일부로 표시됩니다.
3. 프라이빗 IPv4 주소를 ping하고 응답을 받습니다.

(권장 사항) 7단계: 중복 연결 구성

장애 조치로, 그림에 표시된 것처럼 AWS에 2개의 전용 연결을 요청하고 구성하는 것이 좋습니다. 이러한 연결은 네트워크에 있는 한 두개의 라우터에서 종료될 수 있습니다.



2개의 전용 연결을 프로비저닝할 경우 서로 다른 구성을 선택할 수 있습니다.

- 액티브/액티브(BGP 다중 경로). 기본 구성으로, 두 연결이 모두 활성화됩니다. AWS Direct Connect는 동일한 위치 내의 여러 가상 인터페이스로의 다중 경로 지정을 지원하며, 트래픽은 흐름을 기반으로 인터페이스 간에 로드 공유됩니다. 한 연결을 사용할 수 없게 될 경우 모든 트래픽이 다른 연결을 통해 라우팅됩니다.

- 액티브/패시브(failover). 한 연결이 트래픽을 처리하는 동안 다른 연결은 대기 상태에 있습니다. 액티브 연결을 사용할 수 없게 될 경우 모든 트래픽이 패시브 연결을 통해 라우팅됩니다. 수동적 링크가 되도록 링크 중 하나에 대한 라우팅 앞에 AS 경로를 추가해야 합니다.

연결을 구성하는 방법은 중복성에 영향을 미치지 않지만 두 연결을 통해 데이터가 라우팅되는 방식을 결정하는 정책에는 영향을 미칩니다. 두 연결을 모두 액티브로 구성하는 것이 좋습니다.

중복성을 위해 VPN 연결을 사용하는 경우 상태 확인 및 장애 조치 메커니즘을 구현해야 합니다. 다음 구성 중 하나를 사용하는 경우 새 네트워크 인터페이스로 라우팅하려면 라우팅 테이블의 라우팅을 확인해야 합니다.

- 라우팅에 사용자 자신의 고유한 인스턴스를 사용합니다. 예를 들어 해당 인스턴스는 방화벽입니다.
- VPN 연결을 종료하는 사용자 자신의 고유한 인스턴스를 사용합니다.

높은 가용성을 얻으려면 여러 AWS Direct Connect 위치로 연결을 구성할 것을 적극 권장합니다.

AWS Direct Connect 복원력에 대한 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하세요.

AWS Direct Connect 장애 조치 테스트

AWS Direct Connect 복원력 툴킷 복원 모델은 여러 위치에 적절한 수의 가상 인터페이스 연결을 갖도록 설계되었습니다. 마법사를 완료한 후 AWS Direct Connect 복원력 툴킷 장애 조치 테스트를 사용하여 트래픽이 중복 가상 인터페이스 중 하나로 라우팅되고 복원력 요구 사항을 충족하는지 확인하기 위해 BGP 피어링 세션을 중단하세요.

테스트를 사용하여 가상 인터페이스가 서비스 불가능하게 되었을 때 중복 가상 인터페이스를 통해 트래픽이 라우팅되는지 확인합니다. 가상 인터페이스, BGP 피어링 세션 및 테스트 실행 기간을 선택하여 테스트를 시작합니다. AWS는 선택한 가상 인터페이스 BGP 피어링 세션을 중단 상태로 전환합니다. 인터페이스가 이 상태이면 트래픽이 중복 가상 인터페이스를 통해 이동해야 합니다. 구성에 적절한 중복 연결이 포함되어 있지 않으면 BGP 피어링 세션이 실패하고 트래픽이 라우팅되지 않습니다. 테스트가 완료되거나 수동으로 테스트를 중지하면 AWS에서 BGP 세션이 복원됩니다. 테스트가 완료되면 AWS Direct Connect 복원력 툴킷을 사용하여 구성을 조정할 수 있습니다.

> **Note**
>
> Direct Connect 유지 관리 기간에는 이 기능을 사용하지 마십시오. BGP 세션은 유지 관리 도중이나 유지 관리 후에 조기에 복원될 수 있습니다.

테스트 기록

AWS는 365일 후에 테스트 기록을 삭제합니다. 테스트 기록에는 모든 BGP 피어에서 실행된 테스트의 상태가 포함됩니다. 기록에는 테스트된 BGP 피어링 세션, 시작 및 종료 시간 및 다음 값 중 하나인 테스트 상태가 포함됩니다.

- 진행 중 - 테스트가 현재 실행 중입니다.
- 완료됨 - 지정한 시간 동안 테스트가 실행되었습니다.
- 취소됨 - 지정된 시간 이전에 테스트가 취소되었습니다.
- 실패 - 지정한 시간 동안 테스트가 실행되지 않았습니다. 이는 라우터에 문제가 있을 때 발생할 수 있습니다.

자세한 설명은 the section called “가상 인터페이스 장애 조치 테스트 기록 보기” 섹션을 참조하세요.

검증 권한

장애 조치 테스트를 실행할 수 있는 권한이 있는 유일한 계정은 가상 인터페이스를 소유한 계정입니다. 계정 소유자는 AWS CloudTrail을 통해 가상 인터페이스에서 테스트가 실행되었다는 표시를 받습니다.

가상 인터페이스 장애 조치 테스트 시작

AWS Direct Connect 콘솔 또는 AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트를 시작할 수 있습니다.

AWS Direct Connect 콘솔에서 가상 인터페이스 장애 조치 테스트를 시작하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 엽니다. AWS Direct Connect
2. 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택한 다음 작업, BGP 중단을 선택합니다.

   퍼블릭, 프라이빗 또는 전송 가상 인터페이스에서 테스트를 실행할 수 있습니다.

4. 장애 테스트 시작 대화 상자에서 다음을 수행합니다.

   a. Peerings to bring down to test(테스트하기 위해 중단할 피어링)에서 테스트할 피어링 세션(예: IPv4)을 선택합니다.
   b. 테스트 최대 시간에 테스트가 지속될 시간(분)을 입력합니다.

      최대값은 4,320분(72시간)입니다.

      기본값은 180분(3시간)입니다.
   c. To confirm test(테스트를 확인하려면)에 확인을 입력합니다.
   d. 확인을 선택합니다.

   BGP 피어링 세션이 중단 상태로 전환됩니다. 트래픽을 전송하여 중단이 없는지 확인할 수 있습니다. 필요한 경우 즉시 테스트를 중지할 수 있습니다.

AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트를 시작하려면

사용하세요 StartBgpFailoverTest.

가상 인터페이스 장애 조치 테스트 기록 보기

AWS Direct Connect 콘솔 또는 AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트 기록을 볼 수 있습니다.

AWS Direct Connect 콘솔에서 가상 인터페이스 장애 조치 테스트 기록을 보려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.
4. 테스트 기록을 선택합니다.

   콘솔에는 가상 인터페이스에 대해 수행한 가상 인터페이스 테스트가 표시됩니다.
5. 특정 테스트에 대한 세부 정보를 보려면 테스트 ID를 선택합니다.

AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트 기록을 보려면

사용하세요 ListVirtualInterfaceTestHistory.

가상 인터페이스 장애 조치 테스트 중지

AWS Direct Connect 콘솔 또는 AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트를 중지할 수 있습니다.

AWS Direct Connect 콘솔에서 가상 인터페이스 장애 조치 테스트를 중지하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택한 다음 작업, 테스트 취소를 선택합니다.
4. 확인을 선택합니다.

AWS는 BGP 피어링 세션을 복원합니다. 테스트 기록에 테스트에 대해 “취소됨”이 표시됩니다.

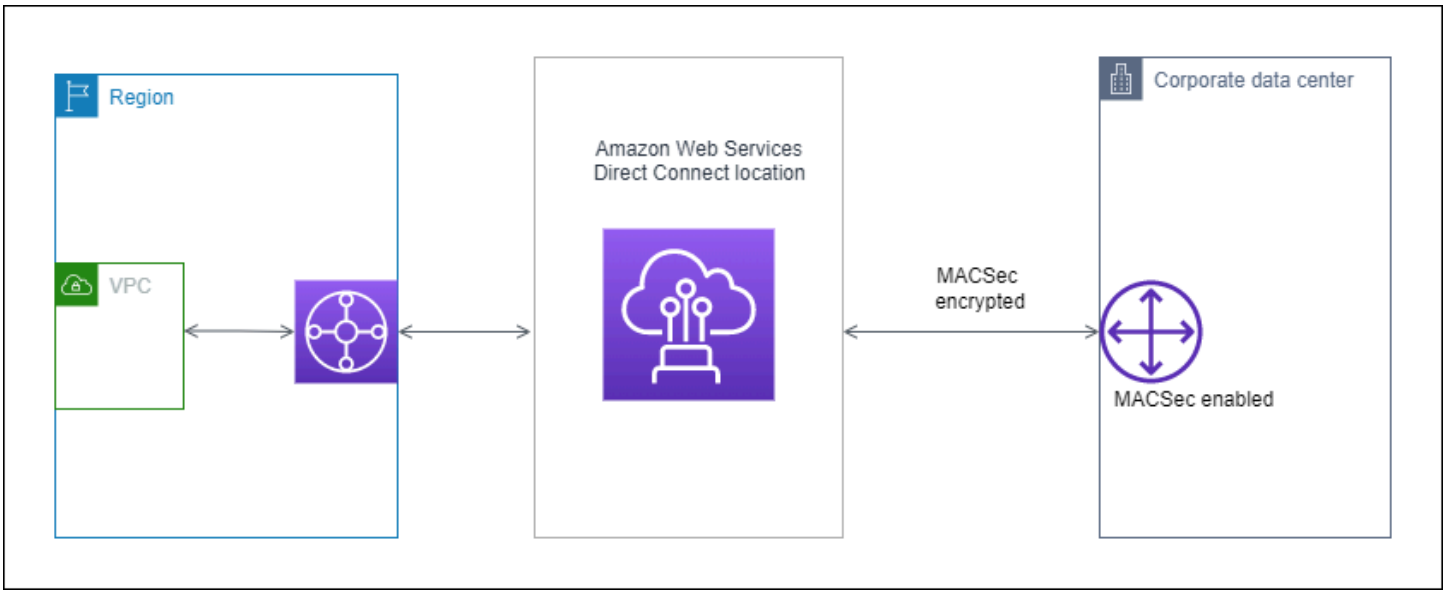
AWS CLI를 사용하여 가상 인터페이스 장애 조치 테스트를 중지하려면

사용하세요 StopBgpFailoverTest.

MAC 보안

MAC 보안(MACsec)은 데이터 기밀성, 데이터 무결성 및 데이터 원본 인증을 제공하는 IEEE 표준입니다. MACsec을 지원하는 AWS Direct Connect 연결을 사용하여 회사 데이터 센터의 데이터를 AWS Direct Connect 위치로 암호화할 수 있습니다. 데이터 센터 및 리전과 상호 연결되는 AWS 글로벌 네트워크를 통해 흐르는 모든 데이터는 데이터 센터를 떠나기 전에 물리적 계층에서 자동으로 암호화됩니다.

다음 다이어그램에서는 전용 연결과 온프레미스 리소스 모두 MACsec을 지원해야 합니다. 전용 연결을 통해 데이터 센터를 오가는 레이어 2 트래픽은 암호화됩니다.



MACsec 개념

다음은 MACsec의 핵심 개념입니다.

- MAC 보안(MACsec) — 데이터 기밀성, 데이터 무결성 및 데이터 원본 신뢰성을 제공하는 IEEE 802.1 Layer 2 표준입니다. 프로토콜에 대한 자세한 내용은 802.1AE: MAC 보안(MACsec)을 참조하십시오.
- MACsec 암호 키 - 고객 온프레미스 라우터와 AWS Direct Connect 위치의 연결 포트 간에 MACsec 연결을 설정하는 사전 공유 키입니다. 키는 사용자가 AWS 에 제공하고 디바이스에도 프로비저닝한 CKN/CAK 쌍을 사용하여 연결 끝에 있는 디바이스에서 생성됩니다.
- 연결 키 이름(CKN)과 연결 키(CAK) - 이 쌍의 값은 MACsec 암호 키를 생성하는 데 사용됩니다. 쌍 값을 생성하여 AWS Direct Connect 연결에 연결하고 AWS Direct Connect 연결 종료 시 엣지 디바이스에 제공합니다.

지원되는 연결

MACsec은 전용 연결에서 사용할 수 있습니다. MACsec을 지원하는 연결 순서 지정 방법에 대한 자세한 내용은 AWS Direct Connect을(를) 참조하십시오.

전용 연결에서 MACsec으로 시작하기

다음 작업은 AWS Direct Connect 전용 연결에서 MacSec에 익숙해지는 데 도움이 됩니다. MACsec 사용에 따른 추가 요금은 없습니다.

전용 연결에서 MACsec을 구성하기 전에 다음 사항을 참고하십시오.

- MACsec은 선택된 접속 지점의 10Gbps 및 100Gbps 전용 Direct Connect 연결에서 지원됩니다. 이러한 연결의 경우 다음과 같은 MACsec 암호 제품군이 지원됩니다.
  - 10Gbps 연결의 경우 GCM-AES-256 및 GCM-AES-XPN-256.
  - 100Gbps 연결의 경우 GCM-AES-XPN-256.
- 256비트 MACsec 키만 지원됩니다.
- 100Gbps 연결에는 확장 패킷 번호 지정 (XPN) 이 필요합니다. 10Gbps 연결의 경우 다이렉트 커넥트는 GCM-AES-256 및 GCM-AES-XPN-256 모두를 지원합니다. 100Gbps 전용 연결과 같은 고속 연결은 MACsec의 원래 32비트 패킷 번호 지정 공간을 빠르게 소진시킬 수 있으며, 이 경우 몇 분마다 암호화 키를 교체하여 새로운 연결 연결을 설정해야 합니다. 이러한 상황을 방지하기 위해 IEEE Std 802.1AEBW-2013 수정안은 확장된 패킷 번호 지정을 도입하여 번호 지정 공간을 64비트로 늘리고 키 교체에 대한 적시성 요구 사항을 완화했습니다.
- 보안 채널 식별자 (SCI) 가 필요하며 반드시 켜야 합니다. 이 설정은 조정할 수 없습니다.
- IEEE 802.1Q (dot1q/VLAN) 태그 오프셋/도트1은 VLAN 태그를 암호화된 페이로드 외부로 이동하는 데 지원되지 q-in-clear 않습니다.

직접 연결 및 MACsec에 대한 자세한 내용은 FAQ의AWS Direct Connect MACsec 섹션을 참조하십시오.

주제

- MACsec 전제 조건
- 서비스 연결 역할
- MACsec에서 사전 공유한 CKN/CAK 주요 고려 사항

- 1단계: 연결 생성
- (선택 사항) 2단계: 링크 집계 그룹 (LAG) 생성
- 3단계: CKN/CAK를 연결 또는 LAG에 연결
- 4단계: 온프레미스 라우터 구성
- 5단계: (선택 사항) CKN/CAK와 연결 또는 LAG 간의 연결 제거

MACsec 전제 조건

MACsec를 전용 연결로 구성하기 전에 다음 작업을 완료합니다.

- MACsec 암호 키에 사용할 CKN/CAK 쌍을 생성하세요.

  개방형 표준 도구를 사용하여 쌍을 만들 수 있습니다. 쌍은 the section called “4단계: 온프레미스 라우터 구성”의 요구 사항을 충족해야 합니다.
- 연결 끝에 MACsec를 지원하는 장치가 있어야 합니다.
- 보안 채널 식별자 (SCI) 를 켜야 합니다.
- 256비트 MACsec 키만 지원되므로 최신 고급 데이터 보호 기능을 제공합니다.

서비스 연결 역할

AWS Direct Connect AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Direct Connect서비스 연결 역할은 미리 정의되며 서비스에서 사용자를 AWS Direct Connect 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS 서비스에 연결된 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS Direct Connect 더 쉬워집니다. AWS Direct Connect 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS Direct Connect 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다. 자세한 설명은 the section called “서비스 연결 역할” 섹션을 참조하세요.

MACsec에서 사전 공유한 CKN/CAK 주요 고려 사항

AWS Direct Connect 연결 또는 LAG에 연결하는 사전 공유 키에 AWS 관리형 CMK를 사용합니다. Secrets Manager는 사전 공유한 CKN 및 CAK 쌍을 시크릿 관리자의 루트 키가 암호화하는 시크릿으로 저장합니다. 자세한 사항은AWS Key Management Service 개발자 안내서의 AWS 관리형 CMK를 참조하세요.

저장된 키는 기본적으로 읽기 전용이지만 AWS Secrets Manager 콘솔 또는 API를 사용하여 7~30일 삭제를 예약할 수 있습니다. 삭제를 예약하면 CKN을 읽을 수 없으며, 이로 인해 네트워크 연결에 영향을 미칠 수 있습니다. 이 경우 다음과 같은 규칙이 적용됩니다.

- 연결이 보류 상태인 경우 연결에서 CKN의 연결을 끊습니다.
- 연결이 사용 가능한 상태인 경우 연결 소유자에게 이메일로 알립니다. 30일 이내에 아무 조치도 취하지 않으면 연결에서 CKN의 연결이 끊어집니다.

연결에서 마지막 CKN의 연결을 끊고 연결 암호화 모드를 "반드시 암호화"로 설정하면 갑작스러운 패킷 손실을 방지하기 위해 모드를 "should_encrypt"로 설정합니다.

1단계: 연결 생성

MACsec 사용을 시작하려면 전용 연결을 만들 때 이 기능을 켜야 합니다. 자세한 설명은 the section called “연결 마법사를 사용하여 연결 생성” 섹션을 참조하세요.

(선택 사항) 2단계: 링크 집계 그룹 (LAG) 생성

이중화를 위해 여러 연결을 사용하는 경우 MACsec을 지원하는 LAG를 만들 수 있습니다. 자세한 내용은 the section called “MACsec 고려 사항” 및 the section called “LAG 생성” 섹션을 참조하세요.

3단계: CKN/CAK를 연결 또는 LAG에 연결

MACsec을 지원하는 연결 또는 LAG를 생성한 후에는 CKN/CAK를 연결에 연결해야 합니다. 자세한 내용은 다음 중 하나를 참조하십시오.

- the section called “MACsec CKN/CAK를 연결에 연결”
- the section called “MACsec CKN/CAK를 LAG와 연결”

4단계: 온프레미스 라우터 구성

MACsec 암호 키로 온프레미스 라우터를 업데이트하세요. 온프레미스 라우터와 해당 위치의 MACsec 비밀 키는 일치해야 합니다. AWS Direct Connect 자세한 설명은 the section called “라우터 구성 파일 다운로드” 섹션을 참조하세요.

5단계: (선택 사항) CKN/CAK와 연결 또는 LAG 간의 연결 제거

MACsec 키와 연결 또는 LAG 간의 연결을 제거해야 할 경우, 다음 방법 중 하나를 사용하면 됩니다.

- the section called “MACsec 암호 키와 연결 사이의 연결을 제거합니다”
- the section called “MACsec 암호 키와 LAG 간의 연결을 제거합니다”

AWS Direct Connect 연결

AWS Direct Connect 네트워크와 AWS Direct Connect 위치 중 하나 사이에 전용 네트워크 연결을 설정할 수 있습니다.

다음과 같은 두 가지 유형의 연결이 있습니다.

- 전용 연결: 단일 고객과 연결된 물리적 이더넷 연결입니다. 고객은 AWS Direct Connect 콘솔, CLI 또는 API를 통해 전용 연결을 요청할 수 있습니다. 자세한 설명은 the section called “전용 연결” 섹션을 참조하세요.
- 호스팅된 연결: AWS Direct Connect 파트너가 고객을 대신하여 프로비저닝하는 물리적 이더넷 연결입니다. 고객은 연결을 프로비저닝하는 AWS Direct Connect 파트너 프로그램에 연락하여 호스팅 연결을 요청합니다. 자세한 설명은 the section called “호스팅 연결” 섹션을 참조하세요.

전용 연결

AWS Direct Connect 전용 연결을 생성하려면 다음 정보가 필요합니다.

AWS Direct Connect location

AWS Direct Connect 파트너 프로그램에서 파트너와 협력하여 특정 AWS Direct Connect 위치와 데이터 센터, 사무실 또는 코로케이션 환경 간에 네트워크 회로를 설정할 수 있도록 도와주세요. 이들 파트너는 해당 위치와 같은 시설 내에 코로케이션 공간을 제공할 수도 있습니다. 자세한 내용은 AWS Direct Connect를 지원하는 APN 파트너를 참조하세요.

포트 속도

가능한 값은 1Gbps, 10Gbps 및 100Gbps입니다.

연결 요청을 생성한 후에는 포트 속도를 변경할 수 없습니다. 포트 속도를 변경하려면 새 연결을 생성하고 구성해야 합니다.

연결 마법사를 사용하거나 클래식 연결을 생성하여 연결을 생성할 수 있습니다. 연결 마법사를 사용하면 복원력 권장 사항을 사용하여 연결을 설정할 수 있습니다. 연결을 처음 설정하는 경우 이 마법사를 사용하는 것이 좋습니다. 원하는 경우 Classic을 사용하여 연결을 one-at-a-time 만들 수 있습니다. 연결을 추가하려는 기존 설정이 이미 있는 경우 클래식을 사용하는 것이 좋습니다. 독립 실행형 연결을 생성할 수도 있고 계정에서 LAG와 연결할 연결을 생성할 수도 있습니다. 연결을 LAG와 연결하는 경우 LAG에 지정된 것과 동일한 포트 속도 및 위치를 사용하여 연결이 생성됩니다.

연결을 요청한 후 다운로드할 수 있는 LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 제공하거나 추가 정보를 요청하는 이메일을 보내 드립니다. 추가 정보 요청을 받은 경우 7일 이내에 회신해야 합니다. 그렇지 않으면 연결이 삭제됩니다. LOA-CFA는 연결 권한이며 AWS, 네트워크 공급자가 대신 교차 연결을 주문하기 위해 필요합니다. 해당 AWS Direct Connect 지역에 장비가 없는 경우, 해당 지역에서 직접 크로스 커넥트를 주문할 수 없습니다.

다음은 전용 연결에서 사용할 수 있는 작업입니다.

- the section called “연결 마법사를 사용하여 연결 생성”
- the section called “Classic 연결 생성”
- the section called “연결 세부 정보 보기”
- the section called “연결 업데이트”
- the section called “MACsec CKN/CAK를 연결에 연결”
- the section called “MACsec 암호 키와 연결 사이의 연결을 제거합니다”
- the section called “연결 삭제”

다중 연결을 단일 연결로 처리할 수 있는 링크 집계 그룹(LAG)에 대한 전용 연결을 추가할 수 있습니다. 자세한 내용은 연결을 LAG에 연결 섹션을 참조하세요.

연결을 생성한 후에는 퍼블릭 및 프라이빗 AWS 리소스에 연결할 가상 인터페이스를 생성합니다. 자세한 설명은 AWS Direct Connect 가상 인터페이스 섹션을 참조하세요.

현장에 장비가 없는 경우 먼저 AWS Direct Connect AWS Direct Connect 파트너 프로그램의 파트너에게 문의하십시오. AWS Direct Connect 자세한 내용은 AWS Direct Connect를 지원하는 APN 파트너를 참조하세요.

MAC 보안(MACsec)을 사용하는 연결을 만들려면 연결을 만들기 전에 사전 요구 사항을 검토하세요. 자세한 설명은 the section called “MACsec 전제 조건 ” 섹션을 참조하세요.

연결 마법사를 사용하여 연결 생성

이 섹션에서는 연결 마법사를 사용하여 연결을 만드는 방법에 대해 설명합니다. Classic Connection 연결을 생성하려면 the section called “2단계: AWS Direct Connect 전용 연결 요청”의 단계를 참조하세요.

연결 마법사에 연결을 생성하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택한 다음 연결 생성을 선택합니다.
3. 연결 만들기 페이지의 연결 순서 유형에서 연결 마법사를 선택합니다.
4. 네트워크 연결의 복원력 수준을 선택합니다. 복원력 수준은 다음 중 하나가 될 수 있습니다.
   - 최대 복원력
   - 높은 복원력
   - 개발과 시험

   이 복원력 수준에 대한 설명과 자세한 내용은 AWS Direct Connect 복원력 툴킷을 사용하여 시작하기을(를) 참조하세요.
5. 다음을 선택합니다.
6. 연결 구성 페이지에서 다음 세부 정보를 제공하세요.
   a. 대역폭 드롭다운 목록에서 연결에 필요한 대역폭을 선택합니다. 이 속도는 1Gbps에서 100Gbps 사이이면 됩니다.
   b. 위치에서 적절한 AWS Direct Connect 위치를 선택한 다음 첫 번째 위치 서비스 공급자를 선택하고 이 위치에서 연결을 위한 연결을 제공하는 서비스 공급자를 선택합니다.
   c. 두 번째 위치의 경우 두 번째 AWS Direct Connect 위치에서 적절한 위치를 선택한 다음 두 번째 위치 서비스 공급자를 선택하고 이 두 번째 위치에서 연결에 대한 연결을 제공하는 서비스 공급자를 선택합니다.
   d. (선택 사항) 연결을 위한 MAC 보안(MACsec)을 구성합니다. 추가 설정에서 MACsec 지원 포트 요청을 선택합니다.

      MACsec은 전용 연결에서만 사용 가능합니다.
   e. (선택 사항) 이 연결을 식별하는 데 도움이 되도록 키/값 쌍을 추가하려면 태그 추가를 선택합니다.
      - 키에서 키 이름을 입력합니다.
      - 값에서 키 값을 입력합니다.

      기존 태그를 제거하려면 태그를 선택한 다음 태그 제거를 선택합니다. 태그는 비어 있을 수 없습니다.

7. 다음을 선택합니다.
8. 검토 및 생성 페이지에서 연결을 확인합니다. 이 페이지에는 포트 사용에 대한 예상 비용과 추가 데이터 전송 요금도 표시됩니다.
9. 생성을 선택하세요.
10. 승인서와 연결 시설 배정(LOA-CFA)을 다운로드하십시오. 자세한 내용은 the section called "LOA-CFA를 다운로드"을(를) 참조하세요.

다음 명령 중 하나를 사용합니다.

- create-connection (AWS CLI)
- CreateConnection(AWS Direct Connect API)

Classic 연결 생성

전용 연결의 경우 AWS Direct Connect 콘솔을 사용하여 연결 요청을 제출할 수 있습니다. 호스팅된 연결의 경우 AWS Direct Connect 파트너와 협력하여 호스팅된 연결을 요청하세요. 다음 정보가 있는지 확인합니다.

- 필요한 포트 속도입니다. 전용 연결은 연결 요청을 생성한 후에는 포트 속도를 변경할 수 없습니다. 호스팅된 연결의 경우 AWS Direct Connect 파트너가 속도를 변경할 수 있습니다.
- 연결이 종료될 AWS Direct Connect 위치.

> **Note**
>
> AWS Direct Connect 콘솔을 사용하여 호스팅된 연결을 요청할 수는 없습니다. 대신 호스팅된 연결을 생성해 줄 수 있는 AWS Direct Connect 파트너에게 문의하면 수락하십시오. 다음 절차를 건너뛰고 호스팅 연결 수락 단원으로 이동합니다.

새 AWS Direct Connect 연결을 만들려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. AWS Direct Connect 화면의 시작하기 아래에서 연결 생성을 선택합니다.
3. 클래식을 선택합니다.

4. 이름에 연결의 이름을 입력합니다.
5. 위치에서 적절한 AWS Direct Connect 위치를 선택합니다.
6. 해당되는 경우, [Sub Location]에서 사용자 또는 사용자의 네트워크 공급자와 가장 가까운 층을 선택합니다. 이 옵션은 해당 위치가 건물의 여러 층에 MMR(meet-me room)을 갖고 있는 경우에만 사용할 수 있습니다.
7. 포트 속도에서 연결 대역폭을 선택합니다.
8. 온프레미스는 이 연결을 사용하여 데이터 센터에 연결할 때 파트너를 통해 연결 AWS Direct Connect 을 선택합니다.
9. 서비스 제공업체의 경우 AWS Direct Connect 파트너를 선택합니다. 목록에 없는 공급자를 이용하는 경우 기타를 선택합니다.
10. 서비스 제공업체로 기타를 선택한 경우, 다른 제공업체의 이름에는 사용하는 파트너의 이름을 입력합니다.
11. (선택 사항) 이 연결을 식별하는 데 도움이 되도록 키/값 쌍을 추가하려면 태그 추가를 선택합니다.

    - 키에서 키 이름을 입력합니다.
    - 값에서 키 값을 입력합니다.

    기존 태그를 제거하려면 태그를 선택한 다음 태그 제거를 선택합니다. 태그는 비어 있을 수 없습니다.
12. 연결 생성을 선택합니다.

요청을 검토하고 연결용 AWS 포트를 제공하는 데 최대 72시간이 걸릴 수 있습니다. 이 시간 동안 사용 사례 또는 지정된 위치에 대한 추가 정보를 요청하는 이메일을 받을 수 있습니다. 이메일은 가입할 때 사용한 이메일 주소로 전송됩니다 AWS. 7일 이내에 응답해야 하며, 그렇지 않으면 연결이 삭제됩니다.

자세한 설명은 AWS Direct Connect 연결 섹션을 참조하세요.

LOA-CFA를 다운로드

연결 요청을 처리하고 나면 LOA-CFA를 다운로드할 수 있습니다. 이 링크가 활성화되지 않았다면 아직 LOA-CFA를 다운로드할 수 없는 것입니다. 자세한 내용은 이메일을 확인하십시오.

포트가 활성화된 시점 또는 LOA가 발급된 지 90일 후(둘 중 먼저 도래하는 날에)에 결제가 자동으로 시작됩니다. 활성화하기 전이나 LOA가 발급된 후 90일 이내에 포트를 삭제하면 청구 요금을 피할 수 있습니다.

90일이 지나도 연결이 되지 않고 LOA-CFA가 발급되지 않은 경우, 10일 후에 포트가 삭제된다는 알림 이메일을 보내드립니다. 추가로 10일 이내에 포트를 활성화하지 못하면 포트가 자동으로 삭제되므로 포트 생성 프로세스를 다시 시작해야 합니다.

> **Note**
>
> 요금에 대한 자세한 내용은 AWS Direct Connect 요금 부분을 참조하세요. LOA-CFA를 재발급한 후 더 이상 연결을 원치 않을 경우 사용자가 직접 연결을 삭제해야 합니다. 자세한 설명은 연결 삭제 섹션을 참조하세요.

Console

LOA-CFA를 다운로드하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 연결을 선택하고 세부 정보 보기를 선택합니다.
4. LOA-CFA 다운로드를 선택합니다.

   > **Note**
   >
   > 이 링크가 활성화되지 않았다면 아직 LOA-CFA를 다운로드할 수 없는 것입니다. 추가 정보를 요청하는 Support 케이스가 생성됩니다. 요청에 응답하고 요청이 처리되면 LOA-CFA를 다운로드할 수 있습니다. 여전히 사용할 수 없는 경우 AWS Support에 문의하세요.

5. 네트워크 공급자나 코로케이션 공급자가 연결을 대신 주문할 수 있도록 LOA-CFA를 이들 공급자에게 보냅니다. 연락 프로세스는 코로케이션 공급자에 따라 다를 수 있습니다. 자세한 설명은 AWS Direct Connect 위치에서 크로스 커넥트 요청 섹션을 참조하세요.

Command line

명령줄 또는 API를 사용하여 LOA-CFA를 다운로드하는 방법

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

연결 업데이트

다음 속성을 업데이트할 수 있습니다.

- 연결의 이름입니다.
- 연결의 MACsec 암호화 모드입니다.

> **Note**
> MACsec은 전용 연결에서만 사용 가능합니다.

유효한 값은 다음과 같습니다.

- `should_encrypt`
- `must_encrypt`

  암호화 모드를 이 값으로 설정하면 암호화가 중단되면 연결이 끊어집니다.
- `no_encrypt`

Console

연결 업데이트

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 연결을 선택하고 편집을 선택합니다.
4. 연결을 수정합니다.

   [이름 변경] 이름에 새 연결 이름을 입력합니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.
   - 키(Key)에 키 이름을 입력합니다.
   - 값에서 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
5. 연결 편집을 선택합니다.

Command line

명령줄을 사용하여 태그를 추가 또는 제거하는 방법

- tag-resource(AWS CLI)
- untag-resource(AWS CLI)

명령줄 또는 API를 사용하여 연결을 업데이트하는 방법

- update-connection(AWS CLI)
- UpdateConnection(AWS Direct Connect API)

MACsec CKN/CAK를 연결에 연결

MACsec을 지원하는 연결을 생성한 후 CKN/CAK를 연결에 연결할 수 있습니다.

> **Note**
>
> MACsec 암호 키를 연결에 연결한 후에는 수정할 수 없습니다. 키를 수정해야 하는 경우 연결에서 키를 분리한 다음 새 키를 연결에 연결하세요. 연결 제거에 대한 자세한 내용은 the section called “MACsec 암호 키와 연결 사이의 연결을 제거합니다”을(를) 참조하세요.

Console

연결을 MACsec 연결하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 왼쪽 창에서 연결을 선택합니다.
3. 연결을 선택하고 세부 정보 보기를 선택합니다.
4. 키 연결을 선택합니다.
5. MACsec 키를 입력합니다.

   [CAK/CKN 쌍 사용] 키 쌍을 선택하고 다음을 수행하세요.

   - 연결성 연결 키(CAK)에 CAK를 입력합니다.

- 연결성 연결 키 이름(CKN)에 CKN을 입력합니다.

[암호 사용] 기존 암호 관리자 암호를 선택한 다음 암호에 대해 MACsec 암호 키를 선택합니다.

6. 키 연결을 선택합니다.

Command line

연결을 MACsec 연결하는 방법

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

MACsec 암호 키와 연결 사이의 연결을 제거합니다

연결과 MACsec 키 간의 연결을 제거할 수 있습니다.

Console

연결 및 MACsec 키 간의 연결을 제거하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2.
3. 왼쪽 창에서 연결을 선택합니다.
4. 연결을 선택하고 세부 정보 보기를 선택합니다.
5. 제거할 MACsec 암호를 선택한 다음 키 연결 해제를 선택합니다.
6. 확인 대화 상자에 연결 해제를 입력한 다음 연결 해제를 선택합니다.

Command line

연결 및 MACsec 키 간의 연결을 제거하는 방법

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

호스팅 연결

AWS Direct Connect 호스팅된 연결을 생성하려면 다음 정보가 필요합니다.

AWS Direct Connect location

AWS Direct Connect AWS Direct Connect 파트너 프로그램에서 파트너와 협력하여 특정 AWS Direct Connect 위치와 데이터 센터, 사무실 또는 코로케이션 환경 간에 네트워크 회로를 구축할 수 있도록 도와주세요. 이들 파트너는 해당 위치와 같은 시설 내에 코로케이션 공간을 제공할 수도 있습니다. 자세한 내용은 AWS Direct Connect 배송 파트너를 참조하세요.

> **Note**
>
> AWS Direct Connect 콘솔을 통해 호스팅된 연결을 요청할 수 없습니다. 하지만 AWS Direct Connect 파트너가 대신 호스팅된 연결을 생성하고 구성할 수 있습니다. 구성이 완료되면 콘솔의 연결 패널에 연결이 표시됩니다.
> 호스팅 연결을 사용하려면 먼저 수락해야 합니다. 자세한 설명은 the section called “호스팅 연결 수락” 섹션을 참조하세요.

포트 속도

호스팅된 연결의 경우 가능한 값은 50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, 500Mbps, 1Gbps, 2Gbps, 5Gbps 및 10Gbps입니다. 특정 요구 사항을 충족한 AWS Direct Connect 파트너만 1Gbps, 2Gbps, 5Gbps 또는 10Gbps 호스팅 연결을 생성할 수 있다는 점에 유의하십시오.

유념할 사항:

- 연결 포트 속도는 파트너만 변경할 수 있습니다. AWS Direct Connect 포트 속도를 변경하려면 호스팅된 연결을 관리하는 AWS Direct Connect 파트너에게 문의하세요.
- AWS 호스팅된 연결에 트래픽 정책을 사용합니다. 즉, 트래픽 속도가 구성된 최대 속도에 도달하면 초과 트래픽이 삭제됩니다. 이로 인해 급증하는 트래픽의 처리량이 급증하지 않는 트래픽보다 낮을 수 있습니다.
- AWS Direct Connect 호스팅된 상위 연결에서 원래 활성화된 경우에만 연결에서 점보 프레임을 활성화할 수 있습니다. 상위 연결에서 점보 프레임을 활성화하지 않으면 어떤 연결에서도 점보 프레임을 활성화할 수 없습니다.

호스팅된 연결을 요청하고 수락한 후에는 다음과 같은 콘솔 작업을 수행할 수 있습니다.

- the section called “연결 세부 정보 보기”
- the section called “연결 업데이트”
- the section called “연결 삭제”

연결을 수락한 후에는 퍼블릭 및 프라이빗 AWS 리소스에 연결할 가상 인터페이스를 생성합니다. 자세한 설명은 AWS Direct Connect 가상 인터페이스 섹션을 참조하세요.

호스팅 연결 수락

호스팅된 연결을 구매하려면 AWS Direct Connect 파트너 프로그램의 파트너에게 문의해야 합니다. AWS Direct Connect 이 파트너가 대신하여 연결을 프로비저닝합니다. 연결이 구성되면 AWS Direct Connect 콘솔의 연결 패널에 해당 연결이 나타납니다.

호스팅 연결 사용을 시작하기 전에 연결을 수락해야 합니다.

Console

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 호스팅 연결을 선택하고 세부 정보 보기를 선택합니다.
4. 확인란을 선택하고 수락을 선택합니다.

Command line

명령줄 또는 API를 사용하여 호스팅 연결을 허용하려면

- confirm-connection (AWS CLI)
- ConfirmConnection(AWS Direct Connect API)

연결 세부 정보 보기

연결의 현재 상태를 볼 수 있습니다. 또한 연결 ID(예: `dxcon-12nikabc`)를 보고 받았거나 다운로드한 LOA-CFA에 기재된 연결 ID와 일치하는지 확인할 수 있습니다.

연결 모니터링에 대한 자세한 내용은 모니터링 단원을 참조하십시오.

Console

연결에 대한 세부 정보를 보는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 왼쪽 창에서 연결을 선택합니다.
3. 연결을 선택하고 세부 정보 보기를 선택합니다.

Command line

명령줄 또는 API를 사용하여 연결을 설명하는 방법

- describe-connections (AWS CLI)
- DescribeConnections(AWS Direct Connect API)

연결 삭제

가상 인터페이스가 연결되어 있지 않은 경우 연결을 삭제할 수 있습니다. 연결을 삭제하면 이 연결에 대한 모든 포트 시간 요금이 중지되지만 교차 연결 또는 네트워크 회로 요금이 계속 발생할 수 있습니다 (아래 참조). AWS Direct Connect데이터 전송 요금은 가상 인터페이스와 관련이 있습니다. 가상 인터페이스 삭제 방법에 대한 자세한 내용은 가상 인터페이스 삭제를 참조하십시오.

연결을 삭제하기 전에 교차 계정 정보가 들어 있는 연결의 LOA를 다운로드하여 연결이 끊기는 회로에 대한 관련 정보를 확인하십시오. 연결 LOA를 다운로드하는 단계는 the section called “LOA-CFA를 다운로드”을(를) 참조하세요.

연결을 삭제하면 코로케이션 공급자에게 해당 패치 패널에서 광섬유 교차 연결 케이블을 제거하여 Direct Connect 라우터에서 네트워크 장치 연결을 끊으라고 지시합니다. AWS AWS 그러나 교차 연결 케이블이 네트워크 장치에 아직 연결되어 있을 수 있기 때문에 코로케이션 또는 회로 공급자가 여전히 교차 연결 또는 네트워크 회로 요금을 청구할 수 있습니다. 교차 연결에 대한 이러한 요금은 Direct Connect와는 별개이며 LOA의 정보를 사용하여 코로케이션 또는 회로 공급자와 함께 취소해야 합니다.

연결이 링크 집계 그룹(LAG)의 일부일 경우, 연결을 삭제했을 때 LAG가 최소 작동 연결 수 설정을 충족하지 못하게 된다면 해당 연결을 삭제할 수 없습니다.

Console

연결 삭제

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 엽니다. AWS Direct Connect
2. 탐색 창에서 연결을 선택합니다.
3. 연결을 선택하고 삭제를 선택합니다.
4. 삭제 확인 대화 상자에서 삭제를 선택합니다.

Command line

명령줄 또는 API를 사용하여 연결을 삭제하는 방법

- delete-connection (AWS CLI)
- DeleteConnection(AWS Direct Connect API)

AWS Direct Connect 위치에서 크로스 커넥트 요청

LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 다운로드한 후 교차 네트워크 연결, 즉 교차 연결을 완료해야 합니다. 특정 AWS Direct Connect 위치에 장비가 이미 있는 경우 해당 공급자에게 문의하여 교차 연결을 완료하십시오. 공급자별 지침은 아래의 표를 참조하십시오. 교차 연결 요금은 공급자에게 문의하십시오. 교차 연결이 구성되면 AWS Direct Connect 콘솔을 사용하여 가상 인터페이스를 만들 수 있습니다.

일부 위치는 캠퍼스로 설정됩니다. 각 위치에서 사용할 수 있는 속도를 비롯한 자세한 내용은 AWS Direct Connect 위치를 참조하세요.

특정 AWS Direct Connect 위치에 장비가 아직 없는 경우 파트너 네트워크 (APN) 의 파트너 중 한 명과 협력할 수 있습니다. AWS 이들 파트너는 AWS Direct Connect 위치에 연결할 수 있도록 도와줍니다. 자세한 내용은 APN 파트너 지원을 참조하십시오. AWS Direct Connect 원활한 교차 연결 요청을 위해서는 선택한 파트너와 LOA-CFA를 공유해야 합니다.

AWS Direct Connect 연결을 통해 다른 지역의 리소스에 액세스할 수 있습니다. 자세한 설명은 원격 AWS 리전 액세스 섹션을 참조하세요.

> **Note**
>
> 90일 내에 교차 연결이 완료되지 않으면 LOA-CFA를 통해 부여된 권한이 만료됩니다. 만료된 LOA-CFA를 갱신하려면 AWS Direct Connect 콘솔에서 다시 다운로드할 수 있습니다. 자세한 설명은 LOA-CFA를 다운로드 섹션을 참조하세요.

콜로케이션

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오레곤)
- 아프리카(케이프타운)
- 아시아 태평양(자카르타)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)

- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 중국(베이징)
- 중국(닝샤)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(밀라노)
- 유럽(런던)
- 유럽(파리)
- 유럽(스톡홀름)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- AWS GovCloud (미국 동부)
- AWS GovCloud (미국 서부)

미국 동부(오하이오)

위치	연결을 요청하는 방법
Cologix COL2, Columbus	콜로직스에게 sales@cologix.com 으로 문의하세요.
Cologix MIN3, 미니애폴리스	콜로직스에게 sales@cologix.com 번으로 문의하세요.
CyrusOne 웨스트 III, 휴스턴	고객 포털을 사용하여 요청을 제출합니다.
Equinix CH2, 시카고	Equinix에 문의(awsdealreg@equinix.com)하십시오.
QTS, 시카고	QTS에 문의(AConnect@qtsdatacenters.com)하십시오.

위치	연결을 요청하는 방법
Netrality Data Centers, 1102 Grand, Kansas City	Netrality Properties(support@netrality.com)에 문의 하세요.

미국 동부(버지니아 북부)

위치	연결을 요청하는 방법
165 Halsey Street, Newark	operations@165halsey.com에 문의합니다.
CoreSite 32k, 뉴욕	CoreSite 고객 포털을 사용하여 주문하십시오. 양식을 작성하고 주문 내역이 정확한지 검토한 다음 웹사이트에서 승인합니다.
CoreSite VA1-VA2, 레스턴	CoreSite 고객 포털에서 주문하세요. 양식을 작성하고 주문 내역이 정확한지 검토한 다음 웹사이트에서 승인합니다.
디지털 부동산 ATL1 & ATL2, 애틀랜타	Digital Realty(amazon.orders@digitalrealty.com)에 문의하십시오.
디지털 부동산 IAD38, 애슈번	Digital Realty(amazon.orders@digitalrealty.com)에 문의하십시오.
에퀴닉스 DC1-DC6 및 DC10-D12, 애슈번	Equinix에 문의(awsdealreg@equinix.com)하십시오.
에퀴닉스 DAA1-DC3 및 DC6, 댈러스	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix MI1, 마이애미	Equinix에 문의(awsdealreg@equinix.com)하십시오.
에퀴닉스 NY5, 시코커스	Equinix에 문의(awsdealreg@equinix.com)하십시오.
KIO 네트웍스 QRO1, 케레타로, MX	KIO 네트웍스에 문의하기".
Markley, 1 섬머 스트리트, 보스턴	현재 고객의 경우 고객 포털을 사용하여 요청을 생성하십시오. 기타 문의는 sales@markleygroup.com으로 하시기 바랍니다.

위치	연결을 요청하는 방법
뉴트럴리티 데이터 센터, MMR 2층, 필라델피아	Netrality Properties(support@netrality.com)에 문의 하세요.
QTS ATL1, 애틀랜타	QTS에 문의(AConnect@qtsdatacenters.com)하십시오.

미국 서부(캘리포니아 북부)

위치	연결을 요청하는 방법
CoreSite, LA1, 로스앤젤레스	CoreSite 고객 포털을 사용하여 주문하십시오. 양식을 작성하고 주문 내역이 정확한지 검토한 다음 웹사이트에서 승인합니다.
CoreSite SV2, 밀피타스	고객 포털을 CoreSite 사용하여 주문하세요. 양식을 작성하고 주문 내역이 정확한지 검토한 다음 웹사이트에서 승인합니다.
CoreSite SV4, 산타클라라	CoreSite 고객 포털을 사용하여 주문하세요. 양식을 작성한 후 주문이 정확한지 검토한 다음 MyCoreSite 웹 사이트를 사용하여 주문을 승인하십시오.
EdgeConneX, 피닉스	EdgeOS 고객 포털을 사용하여 주문합니다. 양식을 제출하면 EdgeConne X가 승인을 위한 서비스 주문 양식을 제공합니다. 문의 사항은 cloudaccess@edgeconnex.com으로 보낼 수 있습니다.
Equinix LA3, 엘 세군도	Equinix에 문의(awsdealreg@equinix.com)하십시오.
에퀴닉스 SV1 및 SV5, 산호세	Equinix에 문의(awsdealreg@equinix.com)하십시오.
PhoenixNAP, 피닉스	phoenixNAP Provisioning에 문의(provisioning@phoenixnap.com)하십시오.

미국 서부(오레곤)

위치	연결을 요청하는 방법
CoreSite DE1, 덴버	CoreSite 고객 포털을 사용하여 주문하세요. 양식을 작성하고 주문 내역이 정확한지 검토한 다음 웹사이트에서 승인합니다.
디지털 부동산 SEA10, 웨스틴 빌딩, 시애틀	Digital Realty(amazon.orders@digitalrealty.com)에 문의하십시오.
EdgeConneX, 포틀랜드	EdgeOS 고객 포털을 사용하여 주문합니다. 양식을 제출하면 EdgeConne X가 승인을 위한 서비스 주문 양식을 제공합니다. 문의 사항은 cloudaccess@edgeconnex.com으로 보낼 수 있습니다.
Equinix SE2, 시애틀	Equinix에 문의(support@equinix.com)하십시오.
Pittock Block, 포틀랜드	이메일(crossconnect@pittock.com) 또는 전화(+1 503 226 6777)로 요청을 보내십시오.
Switch SUPERNAP 8, Las Vegas	Switch SUPERNAP에 문의(orders@supernap.com)하십시오.
TierPoint 시애틀	TierPoint sales@tierpoint.com 으로 문의하세요.

아프리카(케이프타운)

위치	연결을 요청하는 방법
케이프타운 인터넷 교환/ Teraco 데이터 센터	Teraco에 문의(support@teraco.co.za(기존 Teraco 고객), connect@teraco.co.za(신규 고객))하십시오.
Teraco JB1, Johannesburg, South Africa	Teraco에 문의(support@teraco.co.za(기존 Teraco 고객), connect@teraco.co.za(신규 고객))하십시오.

아시아 태평양(자카르타)

위치	연결을 요청하는 방법
DCI JK3, Jakarta	DCI 인도네시아(jessie.w@dci-indonesia.com.com)에 문의하세요.
NTT 2 Data Center, Jakarta	NTT(tps.cms.presales@global.ntt)에 문의하세요.

아시아 태평양(뭄바이)

위치	연결을 요청하는 방법
Equinix, Mumbai	Equinix에 문의(awsdealreg@equinix.com)하십시오.
NetMagic DC2, 방갈로르	18001033130 또는 marketing@netmagicsolutions.com 으로 무료 NetMagic 영업 및 마케팅 팀에 문의하십시오.
Sify Rabale, 뭄바이	Sify에 문의(aws.directconnect@sifycorp.com)하십시오.
STT Delhi DC2, 델리	자세한 내용은 STT에 문의하십시오. AWSDX@sttelemediag dc .in.
STT GDC Pvt. Ltd. VSB, 첸나이	문의는 STT에 문의하세요. AWSDX@sttelemediagdc .in.
STT Hyderabad DC1, 하이데라바드	문의는 STT에 문의하세요. AWSDX@sttelemediagdc .in.

아시아 태평양(서울)

위치	연결을 요청하는 방법
디지털 부동산 ICN1, 서울	Digital Realty(amazon.orders@digitalrealty.com)에 문의하십시오.

위치	연결을 요청하는 방법
서울 KINX 가산 데이터 센터	KINX에 문의(sales@kinx.net)하십시오.
LG U+ Pyeong-Chon Mega Center, Seoul	kidcadmin@lguplus.co.kr 및 center8@kidc.net에 LOA 문서를 제출하십시오.

아시아 태평양(싱가포르)

위치	연결을 요청하는 방법
Equinix HK1, Tsuen Wan N.T., Hong Kong SAR	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix SG2, Singapore	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Global Switch, Singapore	Global Switch에 문의(salessingapore@globalswitch.com)하십시오.
GPX, Mumbai	GPX(Equinix)(awsdealreg@equinix.com)에 문의하세요.
iAdvantage Mega-i, Hong Kong	iAdvantage에 이메일(cs@iadvantage.net)을 보내거나 iAdvantage Cabling Order e-Form을 이용해 주문을 하십시오.
Menara AIMS, Kuala Lumpur	기존 AIMS 고객은 고객 서비스 포털에서 엔지니어링 작업 주문 요청서 양식을 작성하여 X-Connect 주문을 요청할 수 있습니다. 요청을 제출하는 데 문제가 있을 경우 service.delivery@aims.com.my로 문의하십시오.
TCC Data Center, Bangkok	TCC Technology Co., Ltd(gateway.ne@tcc-technology.com)에 문의하세요.

아시아 태평양(시드니)

위치	연결을 요청하는 방법
CDC 홈 2, 캔버라	CDC 고객 포털의 고객 포털에 로그인하세요.
데이터콤 DH6, 오클랜드	데이터콤 오빗 — 오클랜드의 데이터콤에 문의하세요.
에퀴닉스 ME2, 멜버른	Equinix에 문의(awsdealreg@equinix.com)하십시오.
시드니 Equinix SY3	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Global Switch, 시드니	Global Switch에 문의(salessydney@globalswitch.com)하십시오.
NEXTDC C1, 캔버라	NEXTDC에 문의(nxtops@nextdc.com)하십시오.
NEXTDC M1, 멜버른	NEXTDC에 문의(nxtops@nextdc.com)하십시오.
NEXTDC P1, 퍼스	NEXTDC에 문의(nxtops@nextdc.com)하십시오.
NEXTDC S2, Sydney	NEXTDC에 문의(nxtops@nextdc.com)하십시오.

아시아 태평양(도쿄)

위치	연결을 요청하는 방법
AT 도쿄 추오 데이터 센터, 도쿄	AT TOKYO(at-sales@attokyo.co.jp)에 문의하십시오.
Chief Telecom LY, 타이페이	Chief Telecom에 문의(vicky_chan@chief.com.tw)하십시오.
Chunghwa Telecom, 타이페이	CHT Taipei IDC NOC에 문의(taipei_idc@cht.com.tw)하십시오.
Equinix OS1, 오사카	Equinix에 문의(awsdealreg@equinix.com)하십시오.
도쿄 Equinix TY2	Equinix에 문의(awsdealreg@equinix.com)하십시오.
NEC Inzai, Inzai	NEC Inzai(connection_support@ices.jp.nec.com)에 문의하세요.

캐나다(중부)

위치	연결을 요청하는 방법
Allied 250 Front St W, Toronto	driches@alliedreit.com에 문의하십시오.
Cologix MTL3, 몬트리올	콜로직스에게 sales@cologix.com 으로 문의하세요.
Cologix VAN2, 밴쿠버	콜로직스에게 sales@cologix.com 번으로 문의하세요.
eStruxture, 몬트리올	eStruxture에 문의(directconnect@estruxture.com)하십시오.

중국(베이징)

위치	연결을 요청하는 방법
CIDS Jiachuang IDC, 베이징	dx-order@sinnet.com.cn에 문의하십시오.
Sinnet Jiuxianqiao IDC, 베이징	dx-order@sinnet.com.cn에 문의하십시오.
GDS No. 3 Data Center, 상하이	dx@nwcdcloud.cn에 문의하십시오.
GDS No. 3 Data Center, 선전	dx@nwcdcloud.cn에 문의하십시오.

중국(닝샤)

위치	연결을 요청하는 방법
Industrial Park IDC, 닝샤	dx@nwcdcloud.cn에 문의하십시오.
Shapotou IDC, 닝샤	dx@nwcdcloud.cn에 문의하십시오.

유럽(프랑크푸르트)

위치	연결을 요청하는 방법
CE Colo, Prague, Czech Republic	CE Colo에 문의(info@cecolo.com)하십시오.
DigiPlex 울벤, 오슬로, 노르웨이	helpme@digiplex.com 으로 문의하세요 DigiPlex .
Equinix AM3, Amsterdam, Netherlands	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix FR5, 프랑크프루트	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix HE6, 헬싱키	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix MU1, 뮌헨	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix WA1, 바르샤바	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Interxion AMS7, 암스테르담	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion CPH2, Copenhagen	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion FRA6, 프랑크푸르트	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion MAD2, 마드리드	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion VIE2, 비엔나	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion ZUR1, 취리히	Interxion에 문의(customer.services@interxion.com)하십시오.
IPB, Berlin	IPB에 문의(kontakt@ipb.de)하십시오.
Equinix ITConic MD2, 마드리드	Equinix에 문의(awsdealreg@equinix.com)하십시오.

유럽(아일랜드)

위치	연결을 요청하는 방법
Digital Realty(UK), 도클랜즈	Digital Realty(UK)(amazon.orders@digitalrealty.com)에 문의하십시오.
Eircom Clonshaugh	Eircom에 문의(awsorders@eircom.ie)하십시오.
Equinix DX1, Dublin	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix LD5, 런던(슬라우)	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Interxion DUB2, 더블린	Interxion에 문의(customer.services@interxion.com)하십시오.
Interxion MRS1, 마르세유	Interxion에 문의(customer.services@interxion.com)하십시오.

유럽(밀라노)

위치	연결을 요청하는 방법
CDLAN srl Via Caldera 21, 밀라노	CDLAN(sales@cdlan.it)에 문의하십시오.
Equinix, ML2, Milano, Italy	Equinix에 문의(awsdealreg@equinix.com)하십시오.

유럽(런던)

위치	연결을 요청하는 방법
Digital Realty(UK), 도클랜즈	Digital Realty(UK)(amazon.orders@digitalrealty.com)에 문의하십시오.
Equinix LD5, 런던(슬라우)	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix MA3, 맨체스터	Equinix에 문의(awsdealreg@equinix.com)하십시오.

위치	연결을 요청하는 방법
Telehouse West, 런던	Telehouse UK에 문의(sales.support@uk.telehouse.net)하십시오.

유럽(파리)

위치	연결을 요청하는 방법
Equinix PA3, 파리	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Interxion PAR7, Paris	Interxion에 문의(customer.services@interxion.com)하십시오.
Telehouse Voltaire, Paris	연락처 페이지를 사용하여 텔레하우스 파리 볼테르에 문의하세요.

유럽(스톡홀름)

위치	연결을 요청하는 방법
Interxion STO1, 스톡홀름	Interxion에 문의(customer.services@interxion.com)하십시오.

유럽(취리히)

위치	연결을 요청하는 방법
Equinix ZRH51, Oberengstringen, Switzerland	Equinix에 문의(awsdealreg@equinix.com)하십시오.

이스라엘(텔아비브)

위치	연결을 요청하는 방법
MedOne, 하이파	support@Medone.co.il 으로 문의하기 MedOne
EdgeConnex, 헤르즐리야	info@edgeconnecx.com 으로 문의하기 EdgeConnect

중동(바레인)

위치	연결을 요청하는 방법
AWS 바레인 DC53, 마나마	연결을 완료하려면 해당 지역의 네트워크 공급자 파트너 중 하나와 협력하여 연결을 설정합니다. 그런 다음 네트워크 공급자로부터 AWS 지원 센터를 AWS 통해 위임장 (LOA) 을 제출합니다. AWS 이 위치에서 교차 연결을 완료합니다.
AWS 바레인 DC52, 마나마	연결을 완료하려면 해당 지역의 네트워크 공급자 파트너 중 하나와 협력하여 연결을 설정합니다. 그런 다음 네트워크 공급자로부터 AWS 지원 센터를 AWS 통해 위임장 (LOA) 을 제출합니다. AWS 이 위치에서 교차 연결을 완료합니다.

중동(UAE)

위치	연결을 요청하는 방법
Equinix DX1, Dubai	Equinix에 문의(awsdealreg@equinix.com)하십시오.
에티살랏 SmartHub 데이터센터, 푸자이라, UAE	-C& WS@etisalat.ae 으로 에티살랏 데이터센터에 문의하세요. SmartHub IntlSales

남아메리카(상파울루)

위치	연결을 요청하는 방법
Equinix RJ2, 리우데자네이루	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Equinix SP4, São Paulo	Equinix에 문의(awsdealreg@equinix.com)하십시오.
Tivit	Tivit에 문의(aws@tivit.com.br)하십시오.

AWS GovCloud (미국 동부)

이 리전에서 연결을 주문할 수 없습니다.

AWS GovCloud (미국 서부)

위치	연결을 요청하는 방법
Equinix SV5, 새너제이	Equinix에 문의(awsdealreg@equinix.com)하십시오.

AWS Direct Connect 가상 인터페이스

AWS Direct Connect연결 사용을 시작하려면 다음 VIF (가상 인터페이스) 중 하나를 만들어야 합니다.

- 프라이빗 가상 인터페이스: 프라이빗 IP 주소를 사용하여 Amazon VPC에 액세스하려면 프라이빗 가상 인터페이스를 사용해야 합니다.
- 퍼블릭 가상 인터페이스: 퍼블릭 가상 인터페이스는 퍼블릭 IP 주소를 사용하여 모든 AWS 퍼블릭 서비스에 액세스할 수 있습니다.
- 전송 가상 인터페이스: Direct Connect 게이트웨이와 연결된 하나 이상의 Amazon VPC Transit Gateways에 액세스하려면 전송 가상 인터페이스를 사용해야 합니다. 모든 속도의 AWS Direct Connect 전용 또는 호스팅 연결과 함께 전송 가상 인터페이스를 사용할 수 있습니다. Direct Connect 게이트웨이 구성에 대한 자세한 내용은 the section called “Direct Connect 게이트웨이” 단원을 참조하십시오.

IPv6 주소를 사용하는 다른 AWS 서비스에 연결하려면 서비스 설명서에서 IPv6 주소 지정이 지원되는지 확인해야 합니다.

퍼블릭 가상 인터페이스 접두사 광고 규칙

Amazon에서는 VPC 또는 다른 AWS 서비스에 액세스할 수 있도록 적절한 Amazon 접두사를 공급합니다. 이 연결을 통해 모든 AWS 접두사에 액세스할 수 있습니다(예: Amazon EC2, Amazon S3, Amazon.com). 비 Amazon 접두사에 액세스할 수 없습니다. AWS에서 알리는 현재 접두사 목록은 Amazon Web Services 일반 참조의 AWS IP 주소 범위를 참조하십시오. AWS는 AWS Direct Connect 퍼블릭 가상 인터페이스를 통해 수신한 고객 접두사를 다른 고객에게 다시 알리지 않습니다. 퍼블릭 가상 인터페이스 및 라우팅 정책에 대한 자세한 내용은 the section called “퍼블릭 가상 인터페이스 라우팅 정책”을(를) 참조하세요.

> **Note**
>
> 일부 접두사에서 송수신하는 트래픽을 제어하려면 (패킷의 원본/대상 주소를 기반으로 한) 방화벽 필터를 사용하는 것이 좋습니다. 접두사 필터(라우팅 맵)를 사용하는 경우, 필터가 정확하게 일치하거나 더 긴 접두사를 허용하는지 확인합니다. AWS Direct Connect의 접두사는 집계될 수 있으며 접두사 필터에 정의된 접두사와는 다를 수 있습니다.

호스팅 가상 인터페이스

다른 계정에서 AWS Direct Connect 연결을 사용하려면 그 계정에 대한 호스팅 가상 인터페이스를 만들어야 합니다. 다른 계정 소유자가 호스팅 가상 인터페이스를 사용하려면 먼저 호스팅 가상 인터페이스를 수락해야 합니다. 호스팅 가상 인터페이스는 표준 가상 인터페이스와 동일하게 작동하며 퍼블릭 리소스 또는 VPC에 연결할 수 있습니다.

원하는 속도의 Direct Connect 전용 또는 호스팅된 연결과 함께 트랜짓 가상 인터페이스를 사용할 수 있습니다. 호스팅된 연결은 가상 인터페이스 하나만 지원합니다.

가상 인터페이스를 만들려면 다음 정보가 필요합니다.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다.

Resource	필수 정보
	호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.

Resource	필수 정보

피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러 BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다.
	
	• IPv4:
	  • (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	  • (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0`

Resource	필수 정보
	`.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다. • IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

Resource	필수 정보

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

Resource	필수 정보
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

SiteLink

프라이빗 또는 트랜짓 가상 인터페이스를 생성하는 경우 사용할 수 있습니다. SiteLink

SiteLink 가상 전용 인터페이스용 선택적 Direct Connect 기능으로, AWS 네트워크를 통해 사용 가능한 최단 경로를 사용하여 동일한 AWS 파티션에 있는 두 개의 Direct Connect 접속 지점 (PoPs) 간에 연결을 가능하게 합니다. 이렇게 하면 트래픽을 리전을 통해 라우팅할 필요 없이 AWS 글로벌 네트워크를 통해 온프레미스 네트워크를 연결할 수 있습니다. 자세한 내용은 SiteLink AWS Direct Connect SiteLink소개를 참조하십시오.

> **Note**
>
> SiteLink AWS GovCloud (US)및 중국 지역에서는 사용할 수 없습니다.

사용에 대한 별도의 요금이 SiteLink 부과됩니다. 자세한 내용은 AWS Direct Connect 요금을 참조하세요.

SiteLink 모든 가상 인터페이스 유형을 지원하지는 않습니다. 다음 테이블은 인터페이스 유형과 지원 여부를 보여줍니다.

가상 인터페이스 유형	지원됨/지원되지 않음
전송 가상 인터페이스	지원
가상 게이트웨이가 있고 Direct Connect 게이트웨이에 연결된 가상 프라이빗 게이트웨이	지원
가상 게이트웨이 또는 전송 게이트웨이와 관련이 없고 Direct Connect 게이트웨이에 연결된 가상 프라이빗 게이트웨이	지원
가상 게이트웨이에 연결된 프라이빗 가상 인터페이스	지원되지 않음
프라이빗 가상 인터페이스	지원되지 않음

SiteLink 활성화된 가상 인터페이스를 통해 AWS 리전 (가상 또는 트랜짓 게이트웨이) 에서 온프레미스 위치로 들어오는 트래픽의 트래픽 라우팅 동작은 AWS 경로 앞에 경로가 추가된 기본 Direct Connect 가상 인터페이스 동작과 약간 다릅니다. SiteLink가 활성화되면 의 가상 인터페이스는 연결된 지역에 관계없이 Direct Connect 위치의 AS 경로 길이가 더 짧은 BGP 경로를 AWS 리전 선호합니다. 예를 들어, 연결된 리전은 각 Direct Connect 위치에 대해 광고됩니다. 를 사용하지 않도록 설정하면 기본적으로 가상 또는 트랜짓 게이트웨이에서 들어오는 트래픽은 해당 위치와 연결된 Direct Connect 위치를 선호합니다. 이는 다른 지역에 연결된 Direct Connect 위치의 라우터가 AS 경로 길이가 더 짧은 경로를 알려주더라도 마찬가지입니다. SiteLink AWS 리전 가상 또는 전송 게이트웨이는 여전히 로컬 Direct Connect 위치에서 연결된 AWS 리전 위치까지의 경로를 선호합니다.

SiteLink 가상 인터페이스 유형에 따라 최대 점보 프레임 MTU 크기를 8500 또는 9001로 지원합니다. 자세한 설명은 the section called “프라이빗 가상 인터페이스 또는 전송 가상 인터페이스에 대한 네트워크 MTU 설정” 섹션을 참조하세요.

가상 인터페이스 필수 조건

가상 인터페이스를 생성하기 전에 다음을 수행합니다.

- 연결을 생성합니다. 자세한 설명은 the section called “연결 마법사를 사용하여 연결 생성” 섹션을 참조하세요.

- 단일 연결로 처리할 다중 연결이 있으면 링크 집계 그룹(LAG)을 생성합니다. 자세한 내용은 연결을 LAG에 연결 섹션을 참조하세요.

가상 인터페이스를 만들려면 다음 정보가 필요합니다.

Resource	필수 정보
Connection	가상 인터페이스를 생성하려는 AWS Direct Connect 연결 또는 링크 집계 그룹(LAG)입니다.
Virtual interface name(가상 인터페이스 이름)	가상 인터페이스의 이름입니다.
Virtual interface owner(가상 인터페이스 소유자)	다른 계정을 위해 가상 인터페이스를 생성하는 경우 다른 계정의 AWS 계정 ID가 필요합니다.
(프라이빗 가상 인터페이스만 해당) Connection(연결)	동일한 AWS 리전의 VPC에 연결하려면 VPC용 가상 프라이빗 게이트웨이가 필요합니다. BGP 세션의 Amazon 측 ASN은 가상 프라이빗 게이트웨이에서 상속됩니다. 가상 프라이빗 게이트웨이를 생성할 때 고유한 프라이빗 ASN을 지정할 수 있습니다. 그렇지 않으면 Amazon이 기본 ASN을 제공합니다. 자세한 내용은 Amazon VPC 사용 설명서의 가상 프라이빗 게이트웨이 생성을 참조하세요. Direct Connect 게이트웨이를 통해 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하십시오.
VLAN	연결에서 아직 사용 중이 아닌 고유한 VLAN(Virtual Local Area Network) 태그입니다. 값은 1~4094이고 Ethernet 802.1Q 표준을 준수해야 합니다. 이 태그는 AWS Direct Connect 연결을 통과하는 트래픽에 필요합니다. 호스팅 연결이 있는 경우 AWS Direct Connect 파트너가 이 값을 제공합니다. 가상 인터페이스를 생성한 후에는 이 값을 수정할 수 없습니다.
피어 IP 주소	가상 인터페이스는 IPv4, IPv6 또는 하나씩(듀얼 스택)에 대해 BGP 피어링 세션을 지원할 수 있습니다. Amazon 풀에서 엘라스틱 IP (EIP) 또는 자체 IP 주소 가져오기 (BYOIP) 를 사용하여 퍼블릭 가상 인터페이스를 생성하지 마십시오. 동일한 가상 인터페이스에서 동일한 IP 주소를 사용하는 제품군에 대해 여러

Resource	필수 정보

	BGP 세션을 생성할 수 없습니다. BGP 피어링 세션용 가상 인터페이스의 각 엔드에 할당된 IP 주소 범위입니다.
	
	• IPv4:
	  • (퍼블릭 가상 인터페이스만 해당) 사용자가 소유한 고유의 퍼블릭 IPv4 주소를 지정해야 합니다. 값은 다음 중 하나일 수 있습니다.
	  • 고객 소유의 IPv4 CIDR
	
	  이는 아무 퍼블릭 IP(고객 소유 또는 AWS 제공)여도 되지만 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/31` 범위(예: `203.0.113.0/31`)를 할당하는 경우 피어 IP에는 `203.0.113.0` 을(를), AWS 피어 IP에는 `203.0.113.1` 을(를) 사용하면 됩니다. 또는 `/24` 범위(예: `198.51.100.0/24`)를 할당하는 경우 피어 IP에는 `198.51.100.10` 을(를), AWS 피어 IP에는 `198.51.100.20` 을(를) 사용해도 됩니다.
	  • AWS Direct Connect 파트너 또는 ISP가 소유한 IP 범위 및 LOA-CFA 승인
	  • AWS 제공 /31 CIDR. AWS Support에 문의하여 퍼블릭 IPv4 CIDR를 요청하십시오(그리고 어떤 사용 사례로 요청하는지 알려주세요)
	
	  Note
	  AWS 제공 퍼블릭 IPv4 주소에 대한 모든 요청을 충족할 수 있다고 보장할 수 없습니다.
	• (프라이빗 가상 인터페이스만 해당) Amazon이 사용자 대신 프라이빗 IPv4 주소를 생성할 수 있습니다. 직접 지정하는 경우 라우터 인터페이스 및 AWS Direct Connect 인터페이스에만 프라이빗 CIDR을 지정해야 합니다. 예를 들어, 로컬 네트워크에서 다른 IP 주소를 지정하지 마세요. 퍼블릭 가상 인터페이스와 마찬가지로 피어 IP와 AWS 라우터 피어 IP 모두에 동일한 서브넷 마스크를 사용해야 합니다. 예를 들어 `/30` 범위(예: `192.168.0.0/30`)를 할당하는 경우 피어 IP에는 `192.168.0.1` 을(를), AWS 피어 IP에는 `192.168.0.2` 을(를) 사용하면 됩니다.

Resource	필수 정보
	• IPv6: Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다. 사용자 자체 피어 IPv6 주소는 지정할 수 없습니다.
Address family(주소 패밀리)	BGP 피어링 세션이 IPv4를 통하는지 또는 IPv6를 통하는지를 표시합니다.
BGP information(BGP 정보)	• 사용자 측 BGP 세션에 대한 퍼블릭 또는 프라이빗 BGP(Border Gateway Protocol) ASN(자율 시스템 번호). 공인 ASN을 사용 중이면 ASN을 소유하고 있어야 합니다. 프라이빗 ASN을 사용하는 경우 사용자 지정 ASN 값을 설정할 수 있습니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 1~2147483647 범위여야 합니다. 퍼블릭 가상 인터페이스를 위해 프라이빗 ASN을 사용하는 경우 AS(자율 시스템) 접두어가 작동하지 않습니다. • AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다. • MD5 BGP 인증 키. 사용자는 자체로 제공할 수도 있고 Amazon이 사용자 대신 생성하도록 허용할 수도 있습니다.

(퍼블릭 가상 인터페이스만 해당) Prefixes you want to advertise (공급할 접두사)	BGP를 통해 공급할 퍼블릭 IPv4 경로 또는 IPv6 경로입니다. BGP를 사용하는 접두사를 적어도 하나, 최대 1,000개까지 보급해야 합니다.
	• IPv4: IPv4 CIDR은 다음 중 하나에 해당하는 경우 AWS Direct Connect를 사용하여 발표된 다른 퍼블릭 IPv4 CIDR과 겹칠 수 있습니다.
	  • CIDR은 서로 다른 AWS 리전에 속해 있습니다. 퍼블릭 접두사에 BGP 커뮤니티 태그를 적용해야 합니다.
	  • 액티브/패시브 구성에 퍼블릭 ASN이 있는 경우 AS_PATH를 사용합니다.
	  자세한 내용은 라우팅 정책과 BGP 커뮤니티를 참조하세요.
	• IPv6: /64 이하의 접두사 길이를 지정합니다.
	• 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 광고하려는 추가 CIDR 접두사 목록을 제공하세요.
	• Direct Connect 퍼블릭 가상 인터페이스에서 원하는 접두사 길이를 지정할 수 있습니다. IPv4는 /1 - /32 범위를 지원해야 하며 IPv6는 /1 - /64 범위를 모두 지원해야 합니다.

Resource	필수 정보
(프라이빗 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 점보 프레임은 AWS Direct Connect에서 전파된 경로에만 적용됩니다. 가상 프라이빗 게이트웨이를 가리키는 라우팅 테이블에 정적 경로를 추가하면 정적 경로를 통해 라우팅된 트래픽은 1500 MTU를 사용하여 전송됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.
(전송 가상 인터페이스만 해당) Jumbo frames(점보 프레임)	AWS Direct Connect를 통한 패킷의 최대 전송 단위(MTU)입니다. 기본값은 1500입니다. 가상 인터페이스의 MTU를 8500(점보 프레임)으로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. Direct Connect의 경우 점보 프레임은 최대 8500 MTU까지 지원됩니다. Transit Gateway 라우팅 테이블에 구성된 고정 경로 및 전파된 경로는 VPC 고정 라우팅 테이블 항목이 있는 EC2 인스턴스에서 Transit Gateway Attachment에 이르는 것을 포함하여 점보 프레임을 지원합니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 가상 인터페이스 일반 구성 페이지에서 점보 프레임 가능을 찾습니다.

가상 인터페이스를 만들 때 가상 인터페이스를 소유하는 계정을 지정할 수 있습니다. 사용자 계정이 아닌 AWS 계정을 선택하면 다음 규칙이 적용됩니다.

- 프라이빗 VIF 및 전송 VIF의 경우 계정이 가상 인터페이스 및 가상 프라이빗 게이트웨이/Direct Connect 게이트웨이 대상에 적용됩니다.
- 퍼블릭 VIF의 경우 이 계정은 가상 인터페이스 결제에 사용됩니다. 데이터 송신(DTO) 사용량은 AWS Direct Connect 데이터 전송 속도로 리소스 소유자에 대해 측정됩니다.

> **Note**
>
> 31비트 접두사는 모든 Direct Connect 가상 인터페이스 유형에서 지원됩니다. 자세한 내용은 RFC 3021: IPv4 지점 간 링크의 31비트 접두사 사용을 참조하세요.

가상 인터페이스 생성

전송 게이트웨이에 연결하기 위한 전송 가상 인터페이스, 퍼블릭 리소스(비 VPC 서비스)에 연결하기 위한 퍼블릭 가상 인터페이스, VPC에 연결하기 위한 프라이빗 가상 인터페이스를 만들 수 있습니다.

본인의 계정과 다른 AWS Organizations, 또는 AWS Organizations 내의 계정을 위한 가상 인터페이스를 생성하기 위해, 호스팅 가상 인터페이스를 생성하십시오. 자세한 설명은 the section called "호스팅 되는 가상 인터페이스 생성" 섹션을 참조하세요.

사전 조건

시작하기 전에 먼저 가상 인터페이스 필수 조건의 내용을 읽으십시오.

가상 퍼블릭 인터페이스 생성

퍼블릭 가상 인터페이스를 만드는 경우, 요청을 검토하고 승인하는 데 최대 72시간이 걸릴 수 있습니다.

가상 퍼블릭 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 여십시오. AWS Direct Connect
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public virtual interface settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.
   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.
   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.
   c. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.
   d. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

유효한 값은 1-2147483647입니다.

6. 추가 설정 아래에서 다음을 수행합니다.

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. 직접 BGP 키를 제공하려면 BGP MD5 키를 입력합니다.

      값을 입력하지 않으면 BGP 키가 생성됩니다. 사용자가 직접 키를 제공했거나 자동으로 키를 생성한 경우 해당 값은 가상 인터페이스의 가상 인터페이스 세부 정보 페이지에 있는 BGP 인증 키 열에 표시됩니다.

   c. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.

      > **Important**
      >
      > 기존 퍼블릭 VIF에 접두사를 추가하고 AWS 지원팀에 문의하여 이를 알릴 수 있습니다. 지원 사례의 경우 퍼블릭 VIF에 추가하고 알리려는 추가 CIDR 접두사 목록을 제공하세요.

   d. (선택) 태그를 추가하거나 제거할 수 있습니다.

      [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

      - 키(Key)에 키 이름을 입력합니다.
      - Value(값)의 경우, 키 값을 입력합니다.

      [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

8. 디바이스의 라우터 구성을 다운로드합니다. 자세한 설명은 라우터 구성 파일 다운로드 섹션을 참조하세요.

명령줄 또는 API를 사용하여 퍼블릭 가상 인터페이스를 만드는 방법

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface(AWS Direct ConnectAPI)

가상 프라이빗 인터페이스 생성

AWS Direct Connect 연결과 동일한 리전의 가상 프라이빗 게이트웨이에 프라이빗 가상 인터페이스를 프로비저닝할 수 있습니다. AWS Direct Connect 게이트웨이에 프라이빗 가상 인터페이스를 프로비저닝하는 방법에 대한 자세한 내용은 Direct Connect 게이트웨이 사용 단원을 참조하십시오.

VPC 마법사를 사용해 VPC를 생성할 경우 라우팅 전파가 자동으로 활성화됩니다. 경로 전파를 사용하면 VPC의 경로 테이블에 경로가 자동으로 전파됩니다. 원하는 경우 경로 전파를 비활성화할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서에서 라우팅 테이블의 경로 전파 활성화를 참조하세요.

네트워크 연결의 MTU(최대 전송 단위)는 연결을 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. 가상 프라이빗 인터페이스의 MTU는 1500 또는 9001(점보 프레임)일 수 있습니다. 전송 가상 인터페이스의 MTU는 1500 또는 8500(점보 프레임)일 수 있습니다. 인터페이스를 만들 때 또는 만든 후 업데이트할 때 MTU를 지정할 수 있습니다. 가상 인터페이스의 MTU를 8500(점보 프레임) 또는 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 요약 탭에서 점보 프레임 가능을 찾습니다.

VPC에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

c. 가상 인터페이스 소유자일 경우 가상 인터페이스가 AWS 계정을 대상으로 하는 경우 내 AWS 계정을 선택합니다.

d. Direct Connect 게이트웨이에서 Direct Connect 게이트웨이를 선택합니다.

e. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

f. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

   유효한 값은 1~2147483647입니다.

6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정 (비 RFC 1918) 을 사용하고 주소를 직접 지정해야 합니다.
      >
      > - RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
      > - RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

      [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

   b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

   c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.
8. 디바이스의 라우터 구성을 다운로드합니다. 자세한 설명은 라우터 구성 파일 다운로드 섹션을 참조하세요.

명령줄 또는 API를 사용하여 프라이빗 가상 인터페이스를 만드는 방법

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct ConnectAPI)

Direct Connect 게이트웨이에 대한 전송 가상 인터페이스 생성

AWS Direct Connect 연결을 전송 게이트웨이에 연결하려면 연결을 위한 전송 인터페이스를 생성해야 합니다. 연결할 Direct Connect 게이트웨이를 지정합니다.

네트워크 연결의 MTU(최대 전송 단위)는 연결을 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. 가상 프라이빗 인터페이스의 MTU는 1500 또는 9001(점보 프레임)일 수 있습니다. 전송 가상 인터페이스의 MTU는 1500 또는 8500(점보 프레임)일 수 있습니다. 인터페이스를 만들 때 또는 만든 후 업데이트할 때 MTU를 지정할 수 있습니다. 가상 인터페이스의 MTU를 8500(점보 프레임) 또는 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 요약 탭에서 점보 프레임 가능을 찾습니다.

> **Important**
>
> 전송 게이트웨이를 하나 이상의 Direct Connect 게이트웨이와 연결하는 경우 전송 게이트웨이와 Direct Connect 게이트웨이에서 사용하는 ASN(자율 시스템 번호)이 달라야 합니다. 예를 들어 전송 게이트웨이와 Direct Connect 게이트웨이 모두에 대해 기본 ASN 64512를 사용하면 연결 요청이 실패합니다.

Direct Connect 게이트웨이에 전송 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형)에서 유형에 대해 전송을 선택합니다.
5. Transit virtual interface settings(전송 가상 인터페이스 설정)에서 다음을 수행합니다:

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. 가상 인터페이스 소유자일 경우 가상 인터페이스가 AWS 계정을 대상으로 하는 경우 내 AWS 계정을 선택합니다.

   d. Direct Connect 게이트웨이에서 Direct Connect 게이트웨이를 선택합니다.

   e. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   f. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1~2147483647입니다.
6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

      > **Important**
      >
      > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정 (비 RFC 1918) 을 사용하고 주소를 직접 지정해야 합니다.

- RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
- RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. 최대 전송 단위(MTU)를 1500(기본값)에서 8500(점보 프레임)으로 변경하려면 Jumbo MTU(MTU 크기 8500)를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

가상 인터페이스를 만든 후 사용하는 디바이스를 위한 라우터 구성을 다운로드할 수 있습니다. 자세한 설명은 라우터 구성 파일 다운로드 섹션을 참조하세요.

명령줄 또는 API를 사용하여 전송 가상 인터페이스를 생성하려면

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct ConnectAPI)

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이에 연결된 가상 인터페이스를 보려면

- describe-direct-connect-gateway-첨부 파일 () AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct ConnectAPI)

라우터 구성 파일 다운로드

가상 인터페이스를 생성한 후 인터페이스 상태가 UP인 경우 해당 라우터의 라우터 구성 파일을 다운로드할 수 있습니다.

MACsec이 켜진 가상 인터페이스에 다음 라우터 중 하나를 사용하는 경우 라우터의 구성 파일이 자동으로 생성됩니다.

- NX-OS 9.3 이상 소프트웨어를 실행하는 Cisco Nexus 9K+ 시리즈 스위치
- JunOS 9.5 이상의 소프트웨어를 실행하는 M/MX Series

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.
4. 라우터 구성 다운로드를 선택합니다.
5. 라우터 구성 다운로드에서 다음을 수행합니다.
   a. 공급업체에서 라우터의 제조업체를 선택합니다.
   b. 플랫폼에서 라우터의 모델을 선택합니다.
   c. 소프트웨어에서 라우터의 소프트웨어 버전을 선택합니다.
6. Download(다운로드)를 선택한 다음 라우터에 적합한 구성을 사용하여 AWS Direct Connect에 연결할 수 있는지 확인합니다.

MACsec 고려 사항

MACsec용으로 라우터를 수동으로 구성해야 하는 경우 다음 표를 지침으로 사용하세요.

파라미터	설명
CKN 길이	64자의 16진수 문자(0~9, A~E) 문자열입니다. 전체 길이를 사용하여 플랫폼 간 호환성을 극대화하세요.
CAK 길이	64자의 16진수 문자(0~9, A~E) 문자열입니다. 전체 길이를 사용하여 플랫폼 간 호환성을 극대화하세요.
암호화 알고리즘	AES_256_CMAC
SAK 암호 그룹	• 100Gbps 연결의 경우: GCM_AES_XPN_256 •

파라미터	설명
	10Gbps 연결의 경우: GCM_AES_XPN_256 또는 GCM_AES _256
키 암호 그룹	16
기밀 오프셋	0
ICV 인디케이터	아니요
SAK 교체 시간	PN 롤오버>

가상 인터페이스 세부 정보 보기

가상 인터페이스의 현재 상태를 볼 수 있습니다. 세부 정보에 포함되는 내용은 다음과 같습니다.

- 연결 상태
- 명칭
- 위치
- VLAN
- BGP 세부 정보
- 피어 IP 주소

가상 인터페이스 세부 정보를 보려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 왼쪽 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.

명령줄 또는 API를 사용하여 가상 인터페이스를 설명하려면

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces(AWS Direct ConnectAPI)

BGP 피어 추가 또는 삭제

가상 인터페이스에 IPv4 또는 IPv6 BGP 피어링 세션을 추가 또는 삭제합니다.

가상 인터페이스 하나가 단일 IPv4 BGP 피어링 세션 및 단일 IPv6 BGP 피어링 세션을 지원할 수 있습니다.

IPv6 BGP 피어링 세션에는 사용자 고유의 피어 IPv6 주소를 지정할 수 없습니다. Amazon은 /125 IPv6 CIDR을 자동으로 할당합니다.

멀티프로토콜 BGP는 지원되지 않습니다. IPv4 및 IPv6는 가상 인터페이스에 대해 듀얼 스택 모드로 작동합니다.

AWS는 MD5를 기본으로 활성화합니다. 이 옵션은 수정할 수 없습니다.

BGP 피어 추가

다음 절차를 따라 BGP 피어를 추가합니다.

BGP 피어를 추가하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.
4. 피어링 추가를 선택합니다.
5. (프라이빗 가상 인터페이스) IPv4 BGP 피어를 추가하려면 다음을 수행합니다.
   - IPv4를 선택합니다.
   - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다. Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.
6. (퍼블릭 가상 인터페이스) IPv4 BGP 피어를 추가하려면 다음 작업을 수행합니다.
   - 사용자 라우터 피어 IP에 트래픽이 전송되어야 하는 IPv4 CIDR 대상 주소를 입력합니다.
   - Amazon 라우터 피어 IP에 AWS로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

> **Important**
>
> AWS가 IP 주소를 자동 할당하도록 설정하면 /29 CIDR이 169.254.0.0/16에서 할당됩니다. AWS는 고객 라우터 피어 IP 주소를 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 말기를 권장합니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다. RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.

7. (프라이빗 또는 퍼블릭 가상 인터페이스) IPv6 BGP 피어를 추가하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당되므로 사용자 지정 IPv6 주소는 지정할 수 없습니다.
8. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

   퍼블릭 가상 인터페이스의 경우, ASN이 프라이빗이거나 가상 인터페이스에 대해 이미 허용 목록으로 지정되어 있어야 합니다.

   유효한 값은 1-2147483647입니다.

   값을 입력하지 않으면 자동으로 값을 할당합니다.
9. 직접 BGP 키를 제공하려면 BGP 인증 키에 BGP MD5 키를 입력합니다.
10. 피어링 추가를 선택합니다.

명령줄 또는 API를 사용하여 BGP 피어를 만드는 방법

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (AWS Direct Connect API)

BGP 피어 삭제

가상 인터페이스에 IPv4 및 IPv6 BGP 피어링 세션이 둘 다 있는 경우, BGP 피어링 세션 중 하나(둘 다는 안 됨)를 삭제할 수 있습니다.

BGP 피어를 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.

2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.
4. 피어링에서 삭제할 피어링을 선택하고 삭제를 선택합니다.
5. Remove peering from virtual interface(가상 인터페이스에서 피어링 제거) 대화 상자에서 삭제를 선택합니다.

명령줄 또는 API를 사용하여 BGP 피어를 삭제하는 방법

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer(AWS Direct Connect API)

프라이빗 가상 인터페이스 또는 전송 가상 인터페이스에 대한 네트워크 MTU 설정

AWS Direct Connect는 링크 계층에 이더넷 프레임 크기 1522 또는 9023바이트(14바이트 이더넷 헤더 + 4바이트 VLAN 태그 + IP 데이터그램 바이트 + 4바이트 FCS)를 지원합니다.

네트워크 연결의 MTU(최대 전송 단위)는 연결을 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. 가상 프라이빗 인터페이스의 MTU는 1500 또는 9001(점보 프레임)일 수 있습니다. 전송 가상 인터페이스의 MTU는 1500 또는 8500(점보 프레임)일 수 있습니다. 인터페이스를 만들 때 또는 만든 후 업데이트할 때 MTU를 지정할 수 있습니다. 가상 인터페이스의 MTU를 8500(점보 프레임) 또는 9001(점보 프레임)로 설정하면, 점보 프레임을 지원하도록 업데이트되지 않은 경우 기본 물리적 연결로 업데이트될 수 있습니다. 연결을 업데이트하면 연결과 관련된 모든 가상 인터페이스의 네트워크 연결이 최대 30초 동안 중단됩니다. 연결 또는 가상 인터페이스가 점보 프레임을 지원하는지 확인하려면 AWS Direct Connect 콘솔에서 해당 항목을 선택하고 요약 탭에서 점보 프레임 가능을 찾습니다.

프라이빗 가상 또는 전송 가상 인터페이스에 점보 프레임을 활성화한 후, 점보 프레임을 사용할 수 있는 연결 또는 LAG에만 연결할 수 있습니다. 점보 프레임은 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이에 연결된 가상 프라이빗 인터페이스 또는 Direct Connect 게이트웨이에 연결된 가상 전송 인터페이스에서 지원됩니다. 같은 라우팅을 공고하지만 다른 MTU 값을 사용하는 프라이빗 가상 인터페이스가 둘이거나 같은 경로를 알리는 Site-to-Site VPN이 있다면 1500 MTU가 사용됩니다.

> **Important**
>
> 점보 프레임은 AWS Direct Connect를 통해 전파되는 경로와 전송 게이트웨이를 통해 전파되는 고정 경로에만 적용됩니다. 전송 게이트웨이의 점보 프레임은 8500바이트만 지원합니다.

EC2 인스턴스는 점보 프레임을 지원하지 않을 경우 Direct Connect에서 점보 프레임을 삭제합니다. C1, CC1, T1 및 M1을 제외한 모든 EC2 인스턴스 유형은 점보 프레임을 지원합니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 EC2 인스턴스에 대한 네트워크 MTU(최대 전송 단위)를 참조하세요.
호스팅된 연결의 경우 Direct Connect 호스트된 상위 연결에서 원래 활성화된 경우에만 점보 프레임을 활성화할 수 있습니다. 상위 연결에서 점보 프레임을 활성화하지 않으면 어떤 연결에서도 점보 프레임을 활성화할 수 없습니다.

프라이빗 가상 인터페이스의 MTU를 설정하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 편집을 선택합니다.
4. Jumbo MTU(MTU 크기 9001) 또는 Jumbo MTU(MTU 크기 8500)아래에서 활성을 선택합니다.
5. 승인에서 선택한 연결이 잠시 동안 중단된다는 것을 이해합니다를 선택합니다. 업데이트가 완료될 때까지 가상 인터페이스의 상태는 `pending`입니다.

명령줄 또는 API를 사용하여 프라이빗 가상 인터페이스의 MTU를 설정하는 방법

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct ConnectAPI)

가상 인터페이스 태그를 추가 또는 제거

태그는 가상 인터페이스를 식별하는 방법을 제공합니다. 가상 인터페이스의 계정 소유자인 경우 태그를 추가하거나 제거할 수 있습니다.

가상 인터페이스 태그를 추가 또는 제거하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 편집을 선택합니다.

4. 태그를 추가하거나 제거합니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

5. Edit virtual interface(가상 인터페이스 편집)를 선택합니다.

명령줄을 사용하여 태그를 추가 또는 제거하는 방법

- tag-resource(AWS CLI)
- untag-resource(AWS CLI)

가상 인터페이스 삭제

하나 이상의 가상 인터페이스를 삭제합니다. 연결을 삭제하려면 해당 가상 인터페이스를 먼저 삭제해야 합니다. 가상 인터페이스를 삭제하면 가상 인터페이스와 관련된 AWS Direct Connect 데이터 전송 요금이 더 이상 부과되지 않습니다.

가상 인터페이스를 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 왼쪽 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 삭제를 선택합니다.
4. 삭제 확인 대화 상자에서 삭제를 선택합니다.

명령줄 또는 API를 사용하여 가상 인터페이스를 삭제하려면

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface(AWS Direct ConnectAPI)

호스팅되는 가상 인터페이스 생성

퍼블릭, 전송 또는 프라이빗 호스팅 가상 인터페이스를 만들 수 있습니다. 시작하기 전에 먼저 가상 인터페이스 필수 조건의 내용을 읽으십시오.

호스팅되는 가상 프라이빗 인터페이스 생성

호스팅되는 가상 프라이빗 인터페이스를 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

   c. 가상 인터페이스 소유자에서 다른 AWS 계정을 선택한 다음 가상 인터페이스 소유자에 이 가상 인터페이스를 소유할 계정의 ID를 입력합니다.

   d. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

   e. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1-2147483647입니다.
6. 추가 설정에서 다음을 수행합니다:

   a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

      [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

      - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
      - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

> **Important**
>
> AWS가 IP 주소를 자동 할당하도록 설정하면 /29 CIDR이 169.254.0.0/16에서 할당됩니다. AWS는 고객 라우터 피어 IP 주소를 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 말기를 권장합니다. 대신 RFC 1918 또는 기타 주소 지정 (비 RFC 1918) 을 사용하고 주소를 직접 지정해야 합니다. RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 호스팅 가상 인터페이스를 다른 AWS 계정의 소유자가 수락하면 라우터 구성 파일을 다운로드할 수 있습니다.

명령줄 또는 API를 사용하여 호스팅 프라이빗 가상 인터페이스를 만드는 방법

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(API) AWS Direct Connect

호스팅되는 가상 퍼블릭 인터페이스 생성

호스팅되는 가상 퍼블릭 인터페이스를 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.

4. Virtual interface type(가상 인터페이스 유형) 아래에서 유형에 대해 퍼블릭을 선택합니다.
5. Public Virtual Interface Settings(퍼블릭 가상 인터페이스 설정) 아래에서 다음을 수행합니다.

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.
   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.
   c. 가상 인터페이스 소유자에서 다른 AWS 계정을 선택한 다음 가상 인터페이스 소유자에 이 가상 인터페이스를 소유할 계정의 ID를 입력합니다.
   d. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.
   e. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

      유효한 값은 1-2147483647입니다.
6. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

   [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

   - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
   - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

   > **Important**
   >
   > AWS가 IP 주소를 자동 할당하도록 설정하면 /29 CIDR이 169.254.0.0/16에서 할당됩니다. AWS는 고객 라우터 피어 IP 주소를 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 말기를 권장합니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다. RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.

   [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.
7. 접두사를 Amazon에 공급하려면 공급할 접두사에 가상 인터페이스를 통해 트래픽이 라우팅되는 IPv4 CIDR 대상 주소(쉼표로 구분됨)를 입력합니다.
8. 자체 키를 제공하여 BGP 세션을 인증하려면 추가 설정의 BGP 인증 키에 키를 입력합니다.

   값을 입력하지 않으면 BGP 키를 생성합니다.

9. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
10. 가상 인터페이스 생성을 선택합니다.
11. 호스팅 가상 인터페이스를 다른 AWS 계정의 소유자가 수락하면 라우터 구성 파일을 다운로드할 수 있습니다.

명령줄 또는 API를 사용하여 호스팅 퍼블릭 가상 인터페이스를 만드는 방법

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct ConnectAPI)

호스팅되는 전송 가상 인터페이스 생성

호스팅되는 전송 가상 인터페이스를 생성하려면

> **Important**
>
> 전송 게이트웨이를 하나 이상의 Direct Connect 게이트웨이와 연결하는 경우 전송 게이트웨이와 Direct Connect 게이트웨이에서 사용하는 ASN(자율 시스템 번호)이 달라야 합니다. 예를 들어 전송 게이트웨이와 Direct Connect 게이트웨이 모두에 대해 기본 ASN 64512를 사용하면 연결 요청이 실패합니다.

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형)에서 유형에 대해 전송을 선택합니다.
5. Transit virtual interface settings(전송 가상 인터페이스 설정)에서 다음을 수행합니다:

   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.

b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.

c. 가상 인터페이스 소유자에서 다른 AWS 계정을 선택한 다음 가상 인터페이스 소유자에 이 가상 인터페이스를 소유할 계정의 ID를 입력합니다.

d. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

e. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

   유효한 값은 1-2147483647입니다.

6. 추가 설정에서 다음을 수행합니다:

a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

   [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

   - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
   - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

   > **Important**
   >
   > AWS가 IP 주소를 자동 할당하도록 설정하면 /29 CIDR이 169.254.0.0/16에서 할당됩니다. AWS는 고객 라우터 피어 IP 주소를 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 말기를 권장합니다. 대신 RFC 1918 또는 기타 주소 지정을 사용하고 주소를 직접 지정해야 합니다. RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.

   [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. 최대 전송 단위(MTU)를 1500(기본값)에서 8500(점보 프레임)으로 변경하려면 Jumbo MTU(MTU 크기 8500)를 선택합니다.

c. [선택] 태그를 추가할 수 있습니다. 다음을 따릅니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.
8. 호스팅 가상 인터페이스를 다른 AWS 계정의 소유자가 수락하면 라우터 구성 파일을 다운로드할 수 있습니다.

명령줄 또는 API를 사용하여 호스팅 전송 가상 인터페이스를 생성하려면

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct ConnectAPI)

호스팅된 가상 인터페이스 수락

에서 호스팅 가상 인터페이스를 사용하려면 먼저 가상 인터페이스를 수락해야 합니다. 프라이빗 가상 인터페이스의 경우 기존 가상 프라이빗 게이트웨이나 Direct Connect 게이트웨이가 있어야 합니다. 전송 가상 인터페이스의 경우 기존 전송 게이트웨이 또는 Direct Connect 게이트웨이가 있어야 합니다.

호스팅 가상 인터페이스를 수락하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택하고 세부 정보 보기를 선택합니다.
4. 수락을 선택합니다.
5. 이는 프라이빗 가상 인터페이스 및 전송 가상 인터페이스에 적용됩니다.

   (전송 가상 인터페이스) 가상 인터페이스 수락 대화 상자에서 Direct Connect 게이트웨이를 선택한 다음 가상 인터페이스 수락을 선택합니다.

   (프라이빗 가상 인터페이스) 가상 인터페이스 수락 대화 상자에서 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이를 선택한 다음 가상 인터페이스 수락을 선택합니다.
6. 호스팅 가상 인터페이스를 수락하면 AWS Direct Connect 연결의 소유자가 라우터 구성 파일을 다운로드할 수 있습니다. 호스팅 가상 인터페이스를 수락하는 계정에서는 라우터 구성 다운로드 옵션을 사용할 수 없습니다.

명령줄 또는 API를 사용하여 호스팅 프라이빗 가상 인터페이스를 수락하는 방법

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct ConnectAPI)

명령줄 또는 API를 사용하여 호스팅 퍼블릭 가상 인터페이스를 수락하는 방법

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct ConnectAPI)

명령줄 또는 API를 사용하여 호스팅 전송 가상 인터페이스를 수락하려면

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct ConnectAPI)

가상 인터페이스를 마이그레이션

다음과 같은 가상 인터페이스 마이그레이션 작업을 수행하려는 경우 이 절차를 사용합니다.

- 연결과 연결된 기존 가상 인터페이스를 다른 LAG로 마이그레이션합니다.
- 기존 LAG와 연결된 기존 가상 인터페이스를 새 LAG로 마이그레이션합니다.
- 연결과 연결된 기존 가상 인터페이스를 다른 연결로 마이그레이션합니다.

> **Note**
>
> - 가상 인터페이스를 동일한 리전 내의 새 연결로 마이그레이션할 수 있지만 한 리전에서 다른 리전으로 마이그레이션할 수는 없습니다. 기존 가상 인터페이스를 새 연결에 마이그레이션하거나 연결하는 경우 가상 인터페이스와 연결된 구성 파라미터가 동일합니다. 이것을 우회하려면 연결에서 구성을 미리 준비한 다음 BGP 구성을 업데이트해도 됩니다.
> - 한 호스팅된 연결에서 다른 호스팅된 연결로 VIF를 마이그레이션할 수 없습니다. VLAN ID는 고유하므로 이러한 방식으로 VIF를 마이그레이션하면 VLAN이 일치하지 않게 됩니다. 연결 또는 VIF를 삭제한 다음 연결과 VIF 모두에 대해 동일한 VLAN을 사용하여 다시 생성해야 합니다.

> **Important**
>
> 가상 인터페이스는 잠시 동안 중단됩니다. 유지 관리 기간 동안 이 절차를 수행하는 것이 좋습니다.

가상 인터페이스를 마이그레이션하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스를 선택한 다음 편집을 선택합니다.
4. 연결에 대해 LAG 또는 연결을 선택합니다.
5. Edit virtual interface(가상 인터페이스 편집)를 선택합니다.

명령줄 또는 API를 사용하여 가상 인터페이스를 마이그레이션하려면

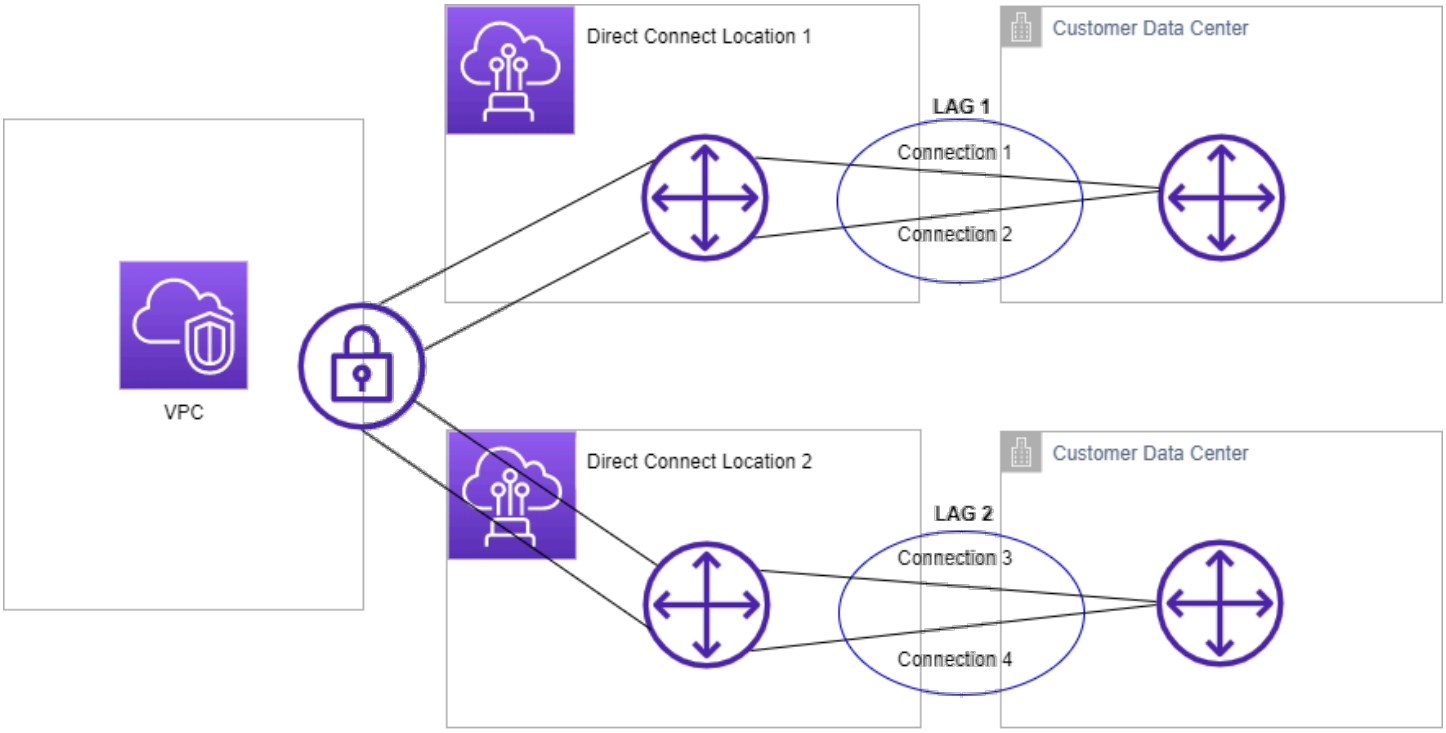
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(AWS Direct ConnectAPI)

링크 집계 그룹

다중 연결을 사용하여 사용 가능한 대역폭을 늘릴 수 있습니다. 링크 집계 그룹(LAG)은 LACP(Link Aggregation Control Protocol)를 사용하여 단일 AWS Direct Connect 엔드포인트에서 복수의 연결을 집계하는 논리적 인터페이스로, 사용자가 이들 연결을 단일의 관리되는 연결로 취급할 수 있습니다. LAG 컨피그레이션이 그룹 내 모든 연결에 적용되므로 LAG는 구성을 간소화합니다.

> **Note**
>
> 다중 섀시 LAG(MLAG)는 AWS에서 지원되지 않습니다.

다음 다이어그램은 각 위치에 2개의 연결로 구성된 4개의 연결을 보여줍니다. 동일한 AWS 디바이스와 동일한 위치에서 종료되는 연결에 대해 LAG를 생성한 다음 구성 및 관리에 4개의 연결 대신 2개의 LAG를 사용할 수 있습니다.



기존 연결로부터 LAG를 생성할 수 있으며, 새 연결을 프로비저닝할 수도 있습니다. LAG를 생성한 후 기존 연결(독립 실행형 또는 다른 LAG의 일부)을 LAG와 연결할 수 있습니다.

다음 규칙이 적용됩니다.

- 모든 연결은 전용 연결이어야 하며 포트 속도가 1Gbps, 10Gbps 또는 100Gbps여야 합니다.

- LAG의 모든 연결은 동일한 대역폭을 사용해야 합니다.
- LAG에서 100G 연결을 최대 두 개 또는 포트 속도가 100G 미만인 연결을 네 개까지 사용할 수 있습니다. LAG의 각 연결은 리전의 전체 연결 제한에 포함됩니다.
- LAG의 모든 연결은 동일한 AWS Direct Connect 엔드포인트에서 종료해야 합니다.
- LAG는 모든 가상 인터페이스 유형(퍼블릭, 프라이빗, 전송)에서 지원됩니다.

LAG를 생성하면 AWS Direct Connect 콘솔에서 개별적으로 새로운 물리적 연결을 LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 다운로드할 수 있습니다. 자세한 설명은 LOA-CFA를 다운로드 섹션을 참조하세요.

모든 LAG에는 LAG 자체가 작동 가능하려면 반드시 작동해야 하는 LAG 내 최소 연결 수를 결정하는 속성이 있습니다. 기본적으로 새 LAG는 이 속성이 0으로 설정되어 있습니다. LAG를 업데이트하여 다른 값을 지정할 수 있습니다. 그러면 작동 가능한 연결의 수가 이 임계값을 하회할 경우 LAG가 작동하지 않게 됩니다. 이 속성을 사용하여 나머지 연결의 과다 사용을 방지할 수 있습니다.

단일 LAG의 모든 연결은 활성/활성 모드로 작동합니다.

> **Note**
>
> LAG를 생성하거나 LAG에 더 많은 연결을 연결할 경우 해당 AWS Direct Connect 엔드포인트에서 사용 가능한 포트가 충분하지 않을 수 있습니다.

MACsec 고려 사항

LAG에서 MACsec을 구성하려면 다음 사항을 고려하세요.

- 기존 연결에서 LAG를 생성하면 모든 MACsec 키가 연결에서 분리됩니다. 그런 다음 LAG에 연결을 추가하고 LAG MACsec 키를 연결에 연결합니다.
- 기존 연결을 LAG에 연결하면 현재 LAG와 연결되어 있는 MACsec 키가 연결과 연결됩니다. 따라서 연결에서 MACsec 키를 분리하고 LAG에 연결을 추가한 다음 LAG MACsec 키를 그 연결에 연결합니다.

LAG 생성

새 연결을 프로비저닝하거나 기존 연결을 집계하여 LAG를 생성할 수 있습니다.

그 결과 리전의 전체 연결 제한을 초과하게 될 경우 새 연결을 사용하여 LAG를 생성할 수 없습니다.

기존 연결로부터 LAG를 생성하려면 각 연결이 동일한 AWS 디바이스에 있어야 합니다(동일한 AWS Direct Connect 엔드포인트에서 종료). 또한 연결은 동일한 대역폭을 사용해야 합니다. 연결을 제거하면 원래 LAG가 최소 작동 연결 수 설정을 충족하지 못하게 될 경우 연결을 기존 LAG로부터 마이그레이션할 수 없습니다.

> **Important**
>
> 기존 연결의 경우, LAG를 생성하는 동안 AWS 접속이 중단됩니다.

Create a LAG with new connections using the console

새 연결을 사용하여 LAG를 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG 생성을 선택합니다.
4. Lag creation type(지연 시간 생성 유형) 아래에서 새 연결 요청을 선택하고 다음 정보를 제공합니다.

   - LAG 이름: LAG의 이름입니다.
   - Location: LAG의 위치입니다.
   - 포트 속도: 연결의 포트 속도입니다.
   - 새 연결 수: 생성할 새 연결 수입니다. 포트 속도가 1G 또는 10G일 때는 최대 네 개, 포트 속도가 100G일 때는 최대 두 개 연결할 수 있습니다.
   - (선택 사항) 연결을 위한 MAC 보안(MACsec)을 구성합니다. 추가 설정에서 MACsec 지원 포트 요청을 선택합니다.

     MACsec은 전용 연결에서만 사용 가능합니다.
   - (선택) 태그를 추가하거나 제거할 수 있습니다.

     [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

     - 키(Key)에 키 이름을 입력합니다.
     - Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

5. LAG 생성을 선택합니다.

Create a LAG with existing connections using the console

기존 연결로부터 LAG를 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG 생성을 선택합니다.
4. Lag creation type(지연 시간 생성 유형) 아래에서 기존 연결 사용을 선택하고 다음 정보를 제공합니다.
   - LAG 이름: LAG의 이름입니다.
   - 기존 연결: LAG에 사용할 Direct Connect 연결입니다.
   - (선택 사항) 새 연결 수: 생성할 새 연결의 수입니다. 포트 속도가 1G 또는 10G일 때는 최대 네 개, 포트 속도가 100G일 때는 최대 두 개 연결할 수 있습니다.
   - 최소 링크: LAG 자체가 작동 가능하려면 반드시 작동해야 하는 최소 연결 수입니다. 값을 지정하지 않으면 기본값 0이 할당됩니다.
5. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.
   - 키(Key)에 키 이름을 입력합니다.
   - Value(값)의 경우, 키 값을 입력합니다.

   [태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.
6. LAG 생성을 선택합니다.

Command line

명령줄 또는 API를 사용하여 LAG를 만드는 방법

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

명령줄 또는 API를 사용하여 LAG를 설명하는 방법

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

명령줄 또는 API를 사용하여 LOA-CFA를 다운로드하는 방법

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

LAG를 생성한 후 여기에서 연결을 연결하거나 해제할 수 있습니다. 자세한 내용은 연결을 LAG에 연결 및 연결을 LAG에서 연결을 해제합니다 섹션을 참조하세요.

LAG 세부 정보 보기

LAG를 생성했으면 세부 정보를 볼 수 있습니다.

Console

LAG에 대한 정보 보기

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 세부 정보 보기를 선택합니다.
4. ID를 포함한 LAG와 연결이 종료되는 AWS Direct Connect 엔드포인트에 관한 정보를 볼 수 있습니다.

Command line

명령줄 또는 API를 사용하여 LAG에 대한 정보를 확인하는 방법

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

LAG 업데이트

다음 링크 집계 그룹(LAG)을 업데이트할 수 있습니다.

- LAG의 이름입니다.
- 최소 링크: LAG 자체가 작동 가능하려면 반드시 작동해야 하는 최소 연결 수의 값입니다.
- LAG의 MACsec 암호화 모드입니다.

  MACsec은 전용 연결에서만 사용 가능합니다.

  AWS는 LAG에 속하는 각 연결에 이 값을 할당합니다.

  유효한 값은 다음과 같습니다.

  - `should_encrypt`
  - `must_encrypt`

    암호화 모드를 이 값으로 설정하면 암호화가 중단되면 연결이 끊어집니다.
  - `no_encrypt`
- 태그입니다.

> **Note**
> 최소 작동 연결 수 임계값을 조정할 경우 새 값 때문에 LAG가 임계값을 충족하지 못해 작동이 불가능해지지 않는지 확인하십시오.

Console

LAG를 업데이트하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 편집을 선택합니다.
4. LAG를 수정합니다.

   [이름 변경] LAG 이름에 새 LAG 이름을 입력합니다.

[최소 연결 수 조정] 최소 링크에 최소 작동 연결 수를 입력합니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- Value(값)의 경우, 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

5. Edit LAG(LAG 편집)를 선택합니다.

Command line

명령줄 또는 API를 사용하여 LAG를 업데이트하려면

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

명령줄을 사용하여 태그를 추가 또는 제거하는 방법

- tag-resource(AWS CLI)
- untag-resource(AWS CLI)

연결을 LAG에 연결

기존 연결을 LAG와 연결할 수 있습니다. 연결은 독립 실행형일 수도 있고 다른 LAG의 일부일 수도 있습니다. 연결은 동일한 AWS 디바이스에 위치해야 하며 LAG와 동일한 대역폭을 사용해야 합니다. 연결이 이미 다른 LAG와 연결되어 있는 경우, 연결을 제거했을 때 LAG가 최소 작동 연결 수 설정을 충족하지 못한다면 해당 연결을 재연결할 수 없습니다.

연결을 LAG에 연결하더라도 자동으로 해당 가상 인터페이스가 LAG에 재연결됩니다.

> **Important**
> 연결 시 해당 연결을 통한 AWS 접속이 중단됩니다.

Console

연결을 LAG에 연결하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 세부 정보 보기를 선택합니다.
4. 연결 아래에서 연결 설정을 선택합니다.
5. 연결에서 LAG에 사용할 Direct Connect 연결을 선택합니다.
6. 연결 설정을 선택합니다.

Command line

명령줄 또는 API를 사용하여 연결을 연결하는 방법

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

연결을 LAG에서 연결을 해제합니다

LAG에서 연결 해제하여 연결을 독립 실행형으로 변환합니다. 연결 해제로 인해 LAG가 최소 작동 연결 수 임계값을 충족하지 못하게 될 경우 연결을 연결 해제할 수 없습니다.

연결을 LAG에서 연결 해제하더라도 자동으로 가상 인터페이스가 연결 해제되지 않습니다.

> **Important**
> 연결 해제 시 AWS 연결이 끊어집니다.

Console

연결을 LAG에서 연결 해제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.

2. 왼쪽 창에서 LAG를 선택합니다.
3. LAG를 선택하고 세부 정보 보기를 선택합니다.
4. 연결 아래의 사용 가능한 연결 목록에서 연결을 선택하고 연결 해제를 선택합니다.
5. 확인 대화 상자에서 연결 해제를 선택합니다.

Command line

명령줄 또는 API를 사용하여 연결을 연결 해제하는 방법

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

MACsec CKN/CAK를 LAG와 연결

MACsec을 지원하는 LAG를 생성한 후 CKN/CAK를 연결에 연결할 수 있습니다.

> **Note**
> LAG에 연결한 후에는 MACsec 암호 키를 수정할 수 없습니다. 키를 수정해야 하는 경우 연결에서 키를 분리한 다음 새 키를 연결에 연결하세요. 연결 제거에 대한 자세한 내용은 the section called “MACsec 암호 키와 LAG 간의 연결을 제거합니다”을(를) 참조하세요.

Console

MACsec 키를 LAG에 연결하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 세부 정보 보기를 선택합니다.
4. 키 연결을 선택합니다.
5. MACsec 키를 입력합니다.

   [CAK/CKN 쌍 사용] 키 쌍을 선택하고 다음을 수행하세요.

- 연결성 연결 키(CAK)에 CAK를 입력합니다.
- 연결성 연결 키 이름(CKN)에 CKN을 입력합니다.

[암호 사용] 기존 암호 관리자 암호를 선택한 다음 암호에 대해 MACsec 암호 키를 선택합니다.

6. 키 연결을 선택합니다.

Command line

MACsec 키를 LAG에 연결하는 방법

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct ConnectAPI)

MACsec 암호 키와 LAG 간의 연결을 제거합니다

LAG와 MACsec 키 간의 연결을 제거할 수 있습니다.

Console

LAG와 MACsec 키 사이의 연결을 제거하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 세부 정보 보기를 선택합니다.
4. 제거할 MACsec 암호를 선택한 다음 키 연결 해제를 선택합니다.
5. 확인 대화 상자에 연결 해제를 입력한 다음 연결 해제를 선택합니다.

Command line

LAG와 MACsec 키 사이의 연결을 제거하는 방법

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

LAG 삭제

더 이상 LAG가 필요 없는 경우 삭제할 수 있습니다. 가상 인터페이스가 연결되어 있는 LAG는 삭제할 수 없습니다. 먼저 가상 인터페이스를 삭제하거나 가상 인터페이스를 다른 LAG 또는 연결과 연결해야 합니다. LAG를 삭제하더라도 LAG 안의 연결은 삭제되지 않습니다. 연결을 직접 삭제해야 합니다. 자세한 설명은 연결 삭제 섹션을 참조하세요.

Console

LAG를 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 LAG] 선택합니다.
3. LAG를 선택하고 삭제를 선택합니다.
4. 확인 대화 상자에서 Delete(삭제)를 선택합니다.

Command line

명령줄 또는 API를 사용하여 LAG를 삭제하려면

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

Direct Connect 게이트웨이 사용

Amazon VPC 콘솔 또는 를 사용하여 AWS Direct Connect 게이트웨이를 사용할 수 있습니다. AWS CLI

내용

- Direct Connect 게이트웨이
- 가상 프라이빗 게이트웨이 연결
- 트랜짓 게이트웨이 연결
- 허용되는 접두사 상호 작용

Direct Connect 게이트웨이

AWS Direct Connect 게이트웨이를 사용하여 VPC를 연결합니다. AWS Direct Connect 게이트웨이를 다음 게이트웨이 중 하나와 연결합니다.

- 동일한 리전에 여러 VPC가 있을 때의 전송 게이트웨이
- 가상 프라이빗 게이트웨이

가상 프라이빗 게이트웨이를 사용하여 로컬 영역을 확장할 수도 있습니다. 이 구성을 사용하면 로컬 영역을 Direct Connect 게이트웨이에 연결할 수 있습니다. Direct Connect 게이트웨이는 리전의 Direct Connect 위치에 연결됩니다. 온프레미스 데이터 센터에는 Direct Connect 위치에 대한 Direct Connect 연결이 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 Direct Connect 게이트웨이를 사용한 로컬 영역 액세스를 참조하세요.

Direct Connect 게이트웨이는 전 세계적으로 사용 가능한 리소스입니다. Direct Connect 게이트웨이를 사용하여 전 세계 모든 리전에 연결할 수 있습니다. 여기에는 AWS 중국 지역이 AWS GovCloud (US) 포함되지만 포함되지는 않습니다.

현재 상위 가용 영역을 우회하는 VPC와 Direct Connect를 사용하는 고객은 Direct Connect 연결 또는 가상 인터페이스를 마이그레이션할 수 없습니다.

다음은 Direct Connect 게이트웨이를 사용할 수 있는 시나리오입니다.

Direct Connect 게이트웨이는 동일한 Direct Connect 게이트웨이에 있는 게이트웨이 연결이 서로 트래픽을 전송하는 것을 허용하지 않습니다(예: 가상 프라이빗 게이트웨이에서 다른 가상 프라이빗 게이

트웨이로). 2021년 11월에 구현된 이 규칙의 예외는 동일한 Direct Connect 게이트웨이 및 동일한 가상 인터페이스에 연결된 가상 프라이빗 게이트웨이(VGW)가 연결된 둘 이상의 VPC에 슈퍼넷이 광고되는 경우입니다. 이 경우 VPC에 Direct Connect 엔드포인트를 통해 서로 통신할 수 있습니다. 예를 들어 Direct Connect 게이트웨이에 연결된 VPC(예: 10.0.0.0/24 및 10.0.1.0/24)와 겹치는 슈퍼넷(예: 10.0.0.0/8 또는 0.0.0.0/0)을 알리고 동일한 가상 인터페이스에서 온프레미스 네트워크에서 VPC가 서로 통신할 수 있습니다.

Direct Connect 게이트웨이 내에서 VPC와 VPC 간 통신을 차단하려면 다음과 같이 하세요.

1. VPC의 인스턴스 및 기타 리소스에 보안 그룹을 설정하여 VPC 간 트래픽을 차단합니다. 이 보안 그룹을 VPC의 기본 보안 그룹의 일부로도 사용합니다.
2. 온프레미스 네트워크에서 VPC에 겹치는 슈퍼넷을 광고하지 마세요. 대신 VPC와 겹치지 않는 온프레미스 네트워크의 경로를 더 구체적으로 광고할 수 있습니다.
3. 여러 VPC에 동일한 Direct Connect 게이트웨이를 사용하는 대신 온프레미스 네트워크에 연결하려는 각 VPC에 대해 단일 Direct Connect 게이트웨이를 프로비저닝하세요. 예를 들어 개발 및 프로덕션 VPC에 단일 Direct Connect 게이트웨이를 사용하는 대신 각 VPC에 별도의 Direct Connect 게이트웨이를 사용하세요.

예를 들어 게이트웨이 연결의 접두사가 포함된 온프레미스 슈퍼넷 라우팅이 있는 경우와 같이 게이트웨이 연결에서 게이트웨이 연결 자체로 트래픽을 전송하는 것은 Direct Connect 게이트웨이에서 금지되지 않습니다. 동일한 Direct Connect 게이트웨이와 연결된 전송 게이트웨이에 연결된 여러 VPC가 있는 구성의 경우 VPC가 통신할 수 있습니다. VPC가 통신하지 못하도록 하려면 라우팅 테이블을 블랙홀 옵션이 설정된 VPC 첨부 파일과 연결하십시오.

다음은 Direct Connect 게이트웨이를 사용할 수 있는 시나리오입니다.

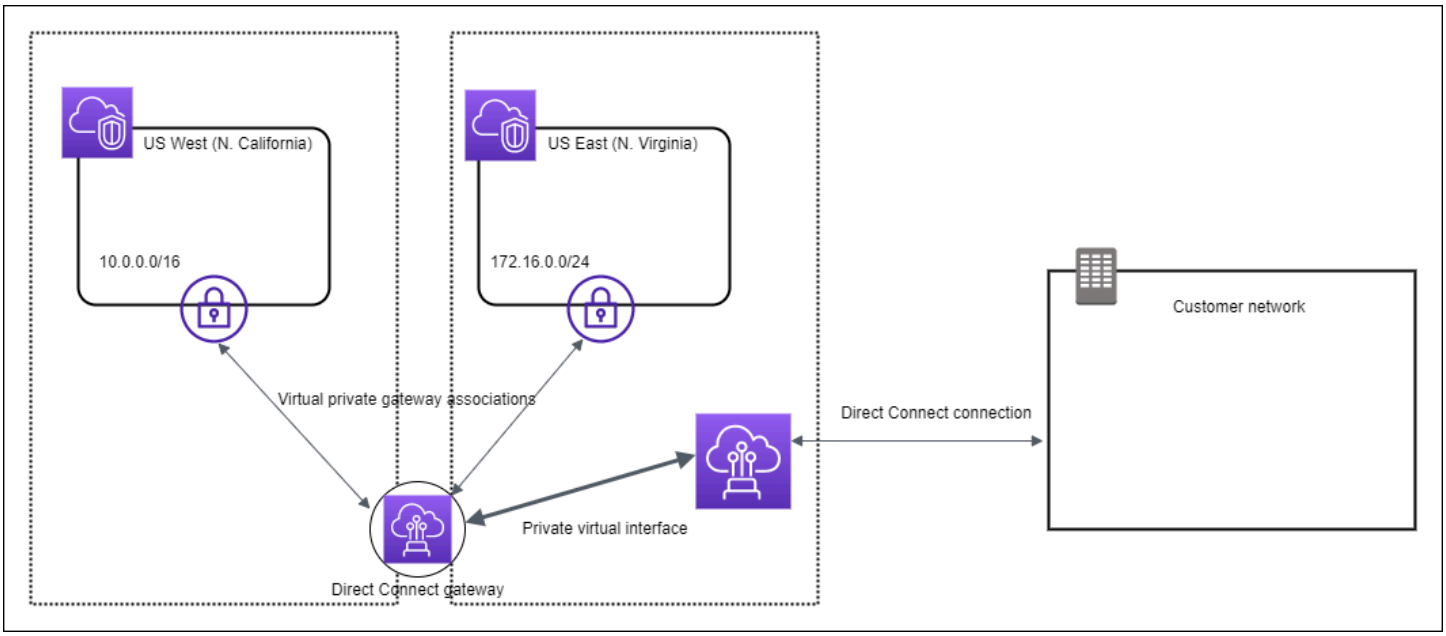
시나리오

- 가상 프라이빗 게이트웨이 연결
- 계정 간 가상 프라이빗 게이트웨이 연결
- 트랜짓 게이트웨이 연결
- 계정 간 전송 게이트웨이 연결
- Direct Connect 게이트웨이 생성
- Direct Connect 게이트웨이 삭제
- 가상 프라이빗 게이트웨이에서 Direct Connect 게이트웨이로 마이그레이션

가상 프라이빗 게이트웨이 연결

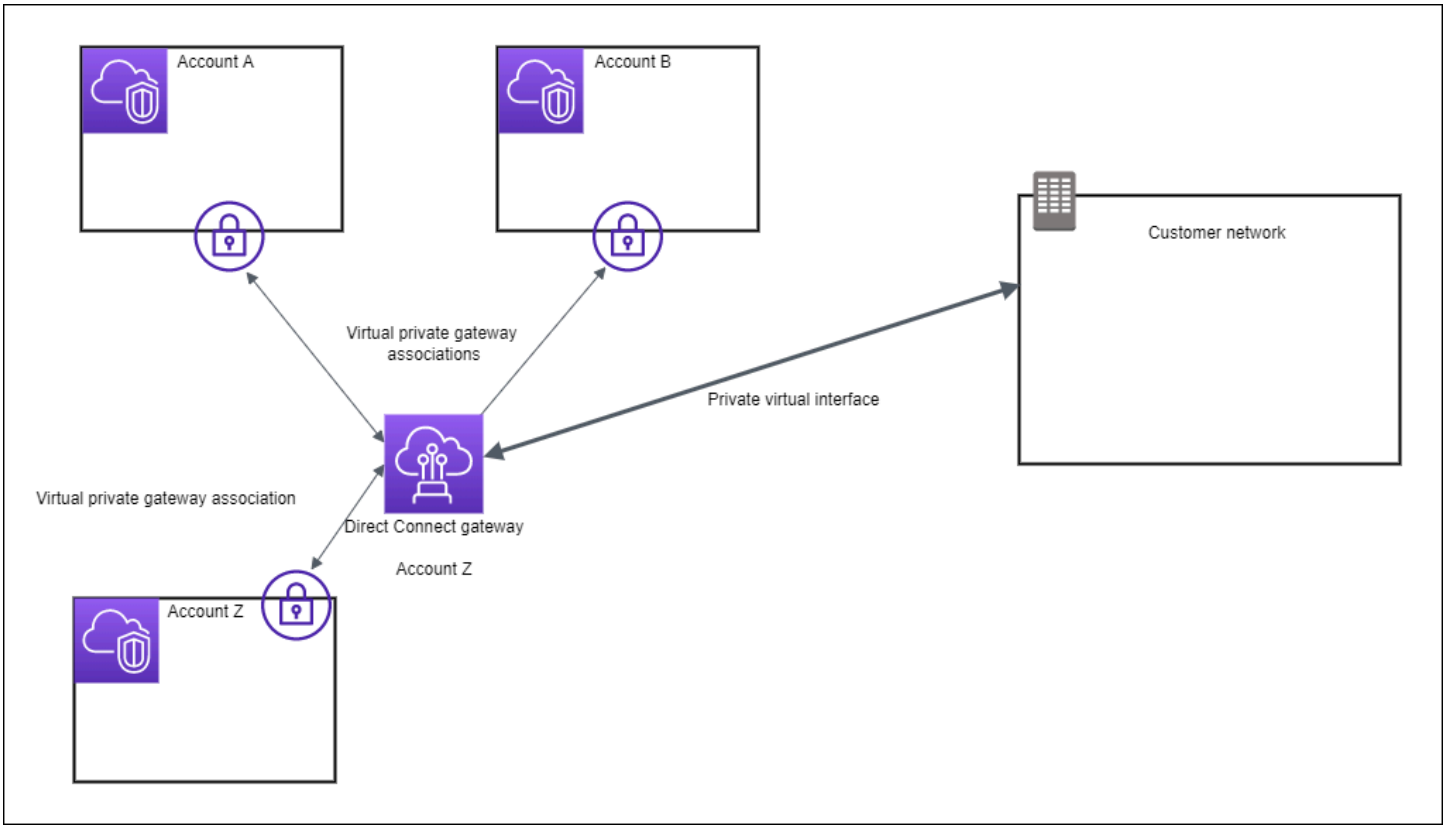
다음 다이어그램에서 Direct Connect 게이트웨이를 사용하면 미국 동부(버지니아 북부) 리전의 AWS Direct Connect 연결을 사용하여 미국 동부(버지니아 북부) 및 미국 서부(캘리포니아 북부) 리전 모두에서 계정의 VPC에 액세스할 수 있습니다.

각 VPC에는 가상 프라이빗 게이트웨이 연결을 사용하여 Direct Connect 게이트웨이에 연결하는 가상 프라이빗 게이트웨이가 있습니다. Direct Connect 게이트웨이는 AWS Direct Connect 위치에 연결할 때 프라이빗 가상 인터페이스를 사용합니다. 위치에서 고객 데이터 센터로의 AWS Direct Connect 연결이 있습니다.



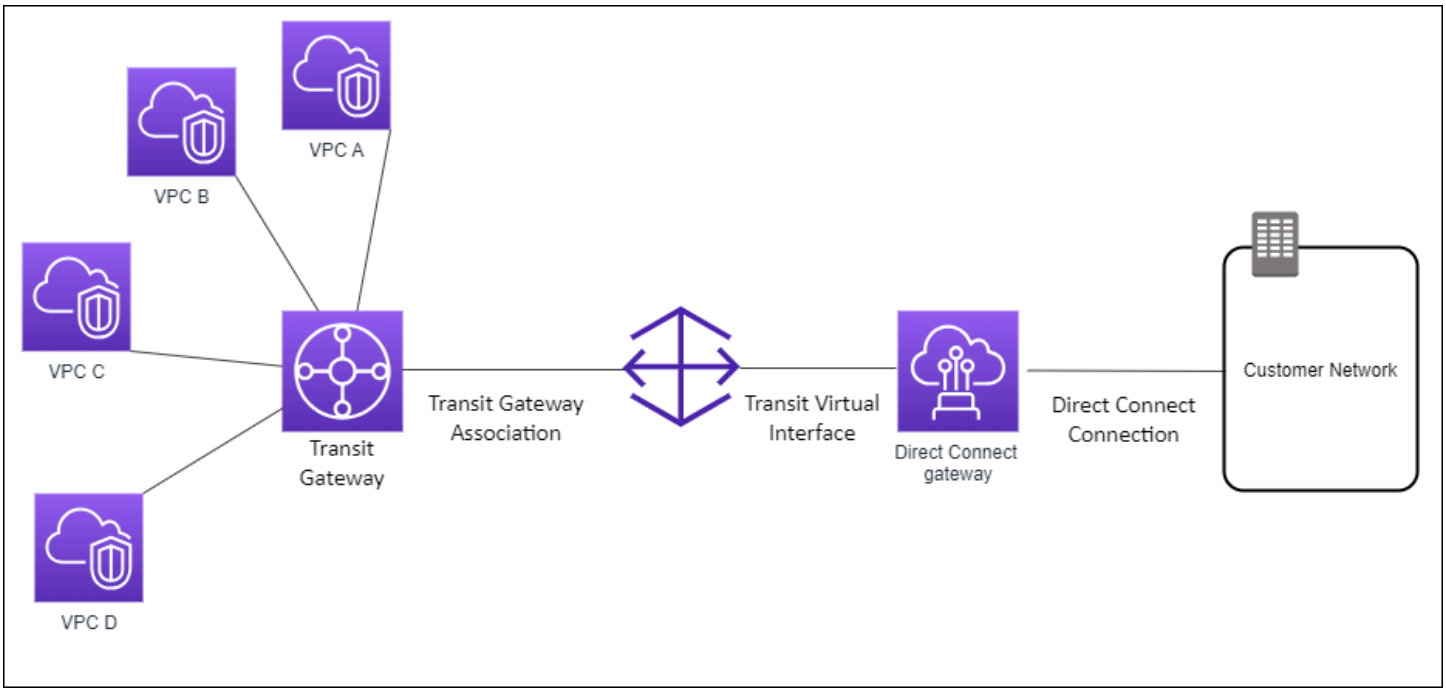
계정 간 가상 프라이빗 게이트웨이 연결

Direct Connect 게이트웨이를 소유하는 Direct Connect 게이트웨이 소유자(계정 Z)에 대한 이 시나리오를 고려해 보십시오. 계정 A와 계정 B가 Direct Connect 게이트웨이를 사용하려고 합니다. 계정 A와 계정 B 각각 계정 Z에 연결 제안을 보냅니다. 계정 Z는 연결 제안을 수락하고 상황에 따라 계정 A의 가상 프라이빗 게이트웨이 또는 계정 B의 가상 프라이빗 게이트웨이에서 허용되는 접두사를 업데이트할 수 있습니다. 계정 Z가 제안을 수락한 후 계정 A 및 계정 B는 자신의 가상 프라이빗 게이트웨이에서 Direct Connect 게이트웨이로의 트래픽을 라우팅할 수 있습니다. 계정 Z는 게이트웨이를 소유하므로 고객으로의 라우팅도 소유합니다.



트랜짓 게이트웨이 연결

다음 다이어그램에서는 Direct Connect 게이트웨이를 사용하여 모든 VPC에서 사용할 수 있는 Direct Connect 연결에 대한 단일 연결을 만드는 방법을 보여줍니다.



이 솔루션에는 다음 구성 요소가 포함됩니다.

- VPC 연결이 있는 전송 게이트웨이.
- Direct Connect 게이트웨이
- Direct Connect 게이트웨이와 Transit Gateway의 연결
- Direct Connect 게이트웨이에 연결되는 전송 가상 인터페이스

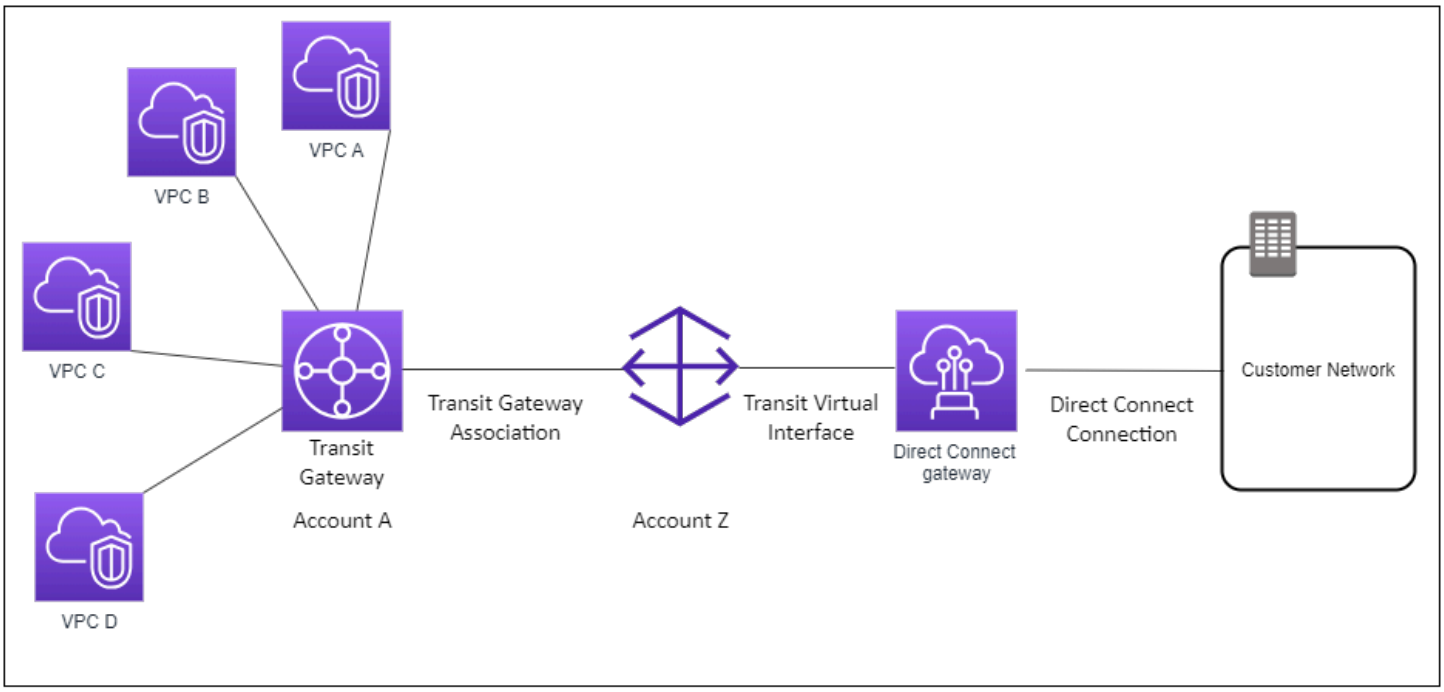
이 구성을 사용하면 다음과 같은 이점이 있습니다. 다음을 할 수 있습니다.

- 동일한 리전에 있는 여러 VPC 또는 VPN에 대한 단일 연결을 관리합니다.
- 온프레미스에서 온프레미스로 또는 온프레미스로 접두사를 AWS 광고하십시오. AWS

전송 게이트웨이 생성과 구성에 대한 자세한 내용은 Amazon VPC Transit 게이트웨이 설명서의 전송 게이트웨이로 작업하기를 참조하세요.

계정 간 전송 게이트웨이 연결

Direct Connect 게이트웨이를 소유하는 Direct Connect 게이트웨이 소유자(계정 Z)에 대한 이 시나리오를 고려해 보십시오. 계정 A가 전송 게이트웨이를 소유하고 있으며 Direct Connect 게이트웨이를 사용하려고 합니다. 계정 Z는 연결 제안을 수락하고 선택적으로 A의 전송 게이트웨이에서 허용되는 접두사를 업데이트할 수 있습니다. 계정 Z가 제안을 수락하면 전송 게이트웨이에 연결된 VPC는 전송 게이트웨이에서 Direct Connect 게이트웨이로 트래픽을 라우팅할 수 있습니다. 계정 Z는 게이트웨이를 소유하므로 고객으로의 라우팅도 소유합니다.



내용

- Direct Connect 게이트웨이 생성
- Direct Connect 게이트웨이 삭제
- 가상 프라이빗 게이트웨이에서 Direct Connect 게이트웨이로 마이그레이션

Direct Connect 게이트웨이 생성

지원되는 리전에서 Direct Connect 게이트웨이를 만들 수 있습니다.

Direct Connect 게이트웨이를 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. Direct Connect 게이트웨이 생성을 선택합니다.
4. 다음 정보를 지정하고 Direct Connect 게이트웨이 생성을 선택합니다.
   - 이름: Direct Connect 게이트웨이를 식별하는 데 도움이 되는 이름을 입력합니다.
   - Amazon 측 ASN: BGP 세션의 Amazon 측 ASN을 지정합니다. ASN은 64,512 ~ 65,534 범위 또는 4,200,000,000 ~ 4,294,967,294 범위여야 합니다.

- 가상 프라이빗 게이트웨이: 가상 프라이빗 게이트웨이를 연결하려면 가상 프라이빗 게이트웨이를 선택합니다.

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이를 생성하려면

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Direct Connect 게이트웨이 삭제

Direct Connect 게이트웨이를 더 이상 필요로 하지 않는 경우 이를 삭제할 수 있습니다. 먼저 연결된 모든 가상 프라이빗 게이트웨이의 연결을 해제하고 연결된 프라이빗 가상 인터페이스를 삭제해야 합니다.

Direct Connect 게이트웨이를 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. 게이트웨이를 선택하고 삭제를 선택합니다.

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이를 삭제하려면

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

가상 프라이빗 게이트웨이에서 Direct Connect 게이트웨이로 마이그레이션

가상 인터페이스에 가상 프라이빗 게이트웨이가 연결되어 있는 경우 Direct Connect 게이트웨이로 마이그레이션하려면 다음 단계를 수행합니다.

Direct Connect 게이트웨이로 마이그레이션하려면

1. Direct Connect 게이트웨이를 생성합니다. 자세한 정보는 the section called “Direct Connect 게이트웨이 생성”을 참조하세요.

2. Direct Connect 게이트웨이에 대한 가상 인터페이스를 생성합니다. 자세한 정보는 the section called "가상 인터페이스 생성"을 참조하세요.
3. 가상 프라이빗 게이트웨이를 Direct Connect 게이트웨이와 연결합니다. 자세한 정보는 the section called "가상 프라이빗 게이트웨이 연결 및 연결 해제"을 참조하세요.
4. 가상 프라이빗 게이트웨이와 연결된 가상 인터페이스를 삭제합니다. 자세한 정보는 the section called "가상 인터페이스 삭제"을 참조하세요.

가상 프라이빗 게이트웨이 연결

AWS Direct Connect 게이트웨이를 사용하면 프라이빗 가상 인터페이스를 통해 AWS Direct Connect 연결을 같은 리전 또는 다른 리전에 있는 계정의 VPC(하나 이상)에 연결할 수 있습니다. Direct Connect 게이트웨이를 VPC의 가상 프라이빗 게이트웨이와 연결합니다. 그런 다음 Direct Connect 게이트웨이 AWS Direct Connect 연결을 위한 프라이빗 가상 인터페이스를 생성합니다. Direct Connect 게이트웨이에 여러 프라이빗 가상 인터페이스를 연결할 수 있습니다.

다음 규칙이 가상 프라이빗 게이트웨이 연결에 적용됩니다.

- 가상 게이트웨이를 Direct Connect 게이트웨이에 연결하기 전까지는 경로 전파를 활성화하지 마십시오. 게이트웨이를 연결하기 전에 경로 전파를 활성화하면 경로가 잘못 전파될 수 있습니다.
- 생성하고 사용할 수 있는 Direct Connect 게이트웨이 수에 제한이 있습니다. 자세한 정보는 할당량을 참조하세요.
- Direct Connect 게이트웨이가 이미 전송 게이트웨이에 연결되어 있는 경우 가상 프라이빗 게이트웨이에 Direct Connect 게이트웨이를 연결할 수 없습니다.
- Direct Connect 게이트웨이를 통해 연결하는 VPC의 CIDR 블록이 중복되어서는 안 됩니다. Direct Connect 게이트웨이와 연결된 VPC에 IPv4 CIDR 블록을 추가하는 경우, 이 CIDR 블록은 그 외에 다른 연결된 VPC에 있는 기존 CIDR 블록과 중첩되어서는 안 됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC에 IPv4 CIDR 블록 추가를 참조하세요.
- Direct Connect 게이트웨이에 대한 퍼블릭 가상 인터페이스를 생성할 수 없습니다.
- Direct Connect 게이트웨이는 연결된 프라이빗 가상 인터페이스와 연결된 가상 프라이빗 게이트웨이 사이의 통신만 지원하며 가상 프라이빗 게이트웨이만 다른 프라이빗 게이트웨이에 활성화할 수 있습니다. 다음 트래픽 흐름은 지원되지 않습니다.
  - 단일 Direct Connect 게이트웨이와 연결되어 있는 VPC 간의 직접 통신. 여기에는 단일 Direct Connect 게이트웨이를 통해 온프레미스 네트워크에서 헤어핀을 사용하여 VPC 간에 전송되는 트래픽이 포함됩니다.
  - 단일 Direct Connect 게이트웨이에 연결되어 있는 가상 인터페이스 간의 직접 통신.

  - 단일 Direct Connect 게이트웨이에 연결되어 있는 가상 인터페이스 및 동일한 Direct Connect 게이트웨이와 연결된 가상 프라이빗 게이트웨이의 VPN 연결 간 직접 통신.
- 가상 프라이빗 게이트웨이를 둘 이상의 Direct Connect 게이트웨이와 연결할 수 없으며 둘 이상의 Direct Connect 게이트웨이에 동일한 프라이빗 가상 인터페이스를 연결할 수 없습니다.
- Direct Connect 게이트웨이와 연결하는 가상 프라이빗 게이트웨이는 VPC에 연결되어야 합니다.
- 가상 프라이빗 게이트웨이 연결 제안은 생성 후 7일 후에 만료됩니다.
- 수락된 가상 프라이빗 게이트웨이 제안 또는 삭제된 가상 프라이빗 게이트웨이 제안은 3 일 동안 계속 표시됩니다.
- 가상 프라이빗 게이트웨이는 Direct Connect 게이트웨이와 연결할 수 있으며 가상 인터페이스에도 연결할 수 있습니다.
- VPC에서 가상 프라이빗 게이트웨이를 분리하면 가상 프라이빗 게이트웨이와 Direct Connect 게이트웨이의 연결도 해제됩니다.

동일한 지역의 VPC에만 AWS Direct Connect 연결을 연결하려면 Direct Connect 게이트웨이를 생성할 수 있습니다. 또는 프라이빗 가상 인터페이스를 생성하여 VPC에 대한 가상 프라이빗 게이트웨이에 연결할 수 있습니다. 자세한 내용은 가상 프라이빗 인터페이스 생성 CloudHubVPN을 참조하십시오.

다른 계정의 VPC와의 AWS Direct Connect 연결을 사용하려면 해당 계정에 대해 호스팅된 프라이빗 가상 인터페이스를 생성하면 됩니다. 다른 계정의 소유자가 호스팅 가상 인터페이스를 수락하는 경우, 해당 소유자는 계정의 가상 프라이빗 게이트웨이 또는 Direct Connect 게이트웨이에 호스팅 가상 인터페이스를 연결할 수 있습니다. 자세한 내용은 AWS Direct Connect 가상 인터페이스 단원을 참조하십시오.

목차

- 가상 프라이빗 게이트웨이 생성
- 가상 프라이빗 게이트웨이 연결 및 연결 해제
- Direct Connect 게이트웨이에 대한 프라이빗 가상 인터페이스 생성
- 계정 간 가상 프라이빗 게이트웨이 연결

가상 프라이빗 게이트웨이 생성

가상 프라이빗 게이트웨이를 연결하고자 하는 VPC에 연결해야 합니다.

> **Note**
>
> Direct Connect 게이트웨이 및 동적 VPN 연결에 가상 프라이빗 게이트웨이를 사용하려는 경우 가상 프라이빗 게이트웨이의 ASN을 VPN 연결에 필요한 값으로 설정합니다. 그렇게 하지 않으면 가상 프라이빗 게이트웨이의 ASN이 허가된 임의의 값으로 설정될 수 있습니다. Direct Connect 게이트웨이는 연결된 모든 VPC를 할당된 ASN을 통해 알립니다.

가상 프라이빗 게이트웨이를 생성한 후 VPC에 연결해야 합니다.

가상 프라이빗 게이트웨이를 생성하여 VPC에 연결하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 프라이빗 게이트웨이를 선택한 후 가상 프라이빗 게이트웨이 생성을 선택합니다.
3. (선택 사항) 가상 프라이빗 게이트웨이에 이름을 입력합니다. `Name` 키와 지정한 값으로 태그가 생성됩니다.
4. ASN에서 기본 선택 항목을 그대로 두고 기본 Amazon ASN을 사용합니다. 그렇지 않으면, 사용자 지정 ASN을 선택하고 값을 입력합니다. 16비트 ASN의 경우, 값은 64512~65534 범위여야 합니다. 32비트 ASN의 경우, 값은 4200000000~4294967294 범위여야 합니다.
5. [Create Virtual Private Gateway]를 선택합니다.
6. 생성된 가상 프라이빗 게이트웨이를 선택한 후 [Actions], [Attach to VPC]를 선택합니다.
7. 목록에서 VPC를 선택하고 [Yes, Attach]를 선택합니다.

명령줄 또는 API를 사용하여 가상 프라이빗 게이트웨이를 만드는 방법

- CreateVpnGateway(아마존 EC2 쿼리 API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

명령줄 또는 API를 사용하여 가상 프라이빗 게이트웨이를 VPC에 연결하는 방법

- AttachVpnGateway(아마존 EC2 쿼리 API)
- attach-vpn-gateway (AWS CLI)

- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

가상 프라이빗 게이트웨이 연결 및 연결 해제

가상 프라이빗 게이트웨이와 Direct Connect 게이트웨이를 연결하거나 연결 해제 할 수 있습니다. 가상 프라이빗 게이트웨이의 계정 소유자가 이 작업을 수행합니다.

가상 프라이빗 게이트웨이를 연결하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택하고 Direct Connect 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. 게이트웨이 연결을 선택하고 게이트웨이 연결을 선택합니다.
5. 게이트웨이에서 연결할 가상 프라이빗 게이트웨이를 선택하고 Associate gateway(게이트웨이 연결)를 선택합니다.

Gateway associations(게이트웨이 연결)를 선택하여 Direct Connect 게이트웨이와 연결된 모든 가상 프라이빗 게이트웨이를 볼 수 있습니다.

가상 프라이빗 게이트웨이 연결을 해제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택하고 Direct Connect 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Gateway associations(게이트웨이 연결)를 선택하고 가상 프라이빗 게이트웨이를 선택합니다.
5. 연결 해제를 선택합니다.

명령줄 또는 API를 사용하여 가상 프라이빗 게이트웨이를 연결하려면

- create-direct-connect-gateway-어소시에이션 ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이와 연결된 가상 프라이빗 게이트웨이를 보려면

- describe-direct-connect-gateway-협회 ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

명령줄 또는 API를 사용하여 가상 프라이빗 게이트웨이 연결을 해제하려면

- delete-direct-connect-gateway-어소시에이션 ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Direct Connect 게이트웨이에 대한 프라이빗 가상 인터페이스 생성

AWS Direct Connect 연결을 원격 VPC에 연결하려면 연결을 위한 프라이빗 가상 인터페이스를 만들어야 합니다. 연결할 Direct Connect 게이트웨이를 지정합니다.

> **Note**
> 호스팅 프라이빗 가상 인터페이스를 수락하는 경우, 본인 계정의 Direct Connect 게이트웨이에 이를 연결할 수 있습니다. 자세한 정보는 호스팅된 가상 인터페이스 수락을 참조하세요.

Direct Connect 게이트웨이에 프라이빗 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형) 아래에서 프라이빗을 선택합니다.
5. Private virtual interface settings(프라이빗 가상 인터페이스 설정) 아래에서 다음을 수행합니다.
   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.
   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.
   c. 가상 인터페이스 소유자의 경우, 가상 인터페이스가 사용자 AWS 계정용인 경우 내 AWS 계정을 선택합니다.
   d. Direct Connect 게이트웨이에서 Direct Connect 게이트웨이를 선택합니다.
   e. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

f. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

유효한 값은 1~2147483647입니다.

6. 추가 설정에서 다음을 수행합니다:

a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

[IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

- 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
- Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

> **Important**
>
> IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS 고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정 (비 RFC 1918) 을 사용하고 주소를 직접 지정해야 합니다.
>
> - RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
> - RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

[IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. MTU(최대 전송 단위)를 1500(기본값)에서 9001(점보 프레임)로 변경하려면 Jumbo MTU (MTU size 9001)(점보 MTU(MTU 크기 9001))를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

[태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- 값에서 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

가상 인터페이스를 만든 후 사용하는 디바이스를 위한 라우터 구성을 다운로드할 수 있습니다. 자세한 정보는 라우터 구성 파일 다운로드을 참조하세요.

명령줄 또는 API를 사용하여 프라이빗 가상 인터페이스를 만드는 방법

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이에 연결된 가상 인터페이스를 보려면

- describe-direct-connect-gateway-첨부 파일 ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

계정 간 가상 프라이빗 게이트웨이 연결

Direct Connect 게이트웨이를 모든 AWS 계정에서 소유한 가상 프라이빗 게이트웨이와 연결할 수 있습니다. Direct Connect 게이트웨이는 기존 게이트웨이가 될 수 있으며, 새 게이트웨이를 생성할 수도 있습니다. 가상 프라이빗 게이트웨이의 소유자는 연결 제안을 생성하고 Direct Connect 게이트웨이의 소유자는 연결 제안을 수락해야 합니다.

연결 제안은 가상 프라이빗 게이트웨이에서 허용되는 접두사를 포함할 수 있습니다. Direct Connect 게이트웨이의 소유자는 상황에 따라 연결 제안의 요청된 접두사를 재정의할 수 있습니다.

허용되는 접두사

가상 프라이빗 게이트웨이를 Direct Connect 게이트웨이와 연결할 때 Direct Connect 게이트웨이에 공급할 Amazon VPC 접두사 목록을 지정합니다. 이 접두사 목록은 동일한 CIDR 또는 보다 작은 CIDR을 Direct Connect 게이트웨이에 공급할 수 있는 필터로 작동합니다. 가상 프라이빗 게이트웨이에서 전체 VPC CIDR을 프로비저닝하므로 Allowed prefixes(허용되는 접두사)를 VPC CIDR보다 넓거나 동일한 범위로 설정해야 합니다.

VPC CIDR이 10.0.0.0/16인 사례를 고려해 보십시오. Allowed prefixes(허용되는 접두사)를 10.0.0.0/16(VPC CIDR 값) 또는 10.0.0.0/15(VPC CIDR보다 넓은 값)로 설정할 수 있습니다.

Direct Connect를 통해 광고되는 네트워크 접두사 내의 모든 가상 인터페이스는 동일한 지역 내에서가 아닌 지역 간 전송 게이트웨이에만 전파됩니다. 허용된 접두사가 가상 프라이빗 게이트웨이 및 전송 게이트웨이와 상호 작용하는 방법에 대한 자세한 내용은 the section called "허용되는 접두사 상호 작용"을(를) 참조하세요.

Tasks

- 연결 제안 생성
- 연결 제안 수락 또는 거부
- 연결에 허용되는 접두사 업데이트
- 연결 제안 삭제

연결 제안 생성

가상 프라이빗 게이트웨이를 소유하는 경우 연결 제안을 생성해야 합니다. 가상 프라이빗 게이트웨이는 계정의 VPC에 연결되어야 합니다. AWS Direct Connect 게이트웨이의 소유자는 Direct Connect 게이트웨이의 ID와 해당 AWS 계정의 ID를 공유해야 합니다. 제안을 생성한 후 Direct Connect 게이트웨이의 소유자가 해당 제안을 수락해야 사용자가 AWS Direct Connect를 통해 온프레미스 네트워크에 액세스할 수 있습니다.

연결 제안을 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 프라이빗 게이트웨이를 선택하고 가상 프라이빗 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Direct Connect gateway associations(Direct Connect 게이트웨이 연결)를 선택하고 Associate Direct Connect gateway(Direct Connect 게이트웨이 연결)를 선택합니다.
5. Association account type(연결 계정 유형)의 계정 소유자에서 다른 계정을 선택합니다.
6. Direct Connect 게이트웨이 소유자에는 Direct Connect 게이트웨이를 소유하는 AWS 계정의 ID를 입력합니다.
7. Association settings(연결 설정)에서 다음을 수행합니다.

   a. Direct Connect gateway ID(Direct Connect 게이트웨이 ID)에 Direct Connect 게이트웨이의 ID를 입력합니다.

   b. Direct Connect 게이트웨이 소유자의 경우 연결에 대한 Direct Connect 게이트웨이를 소유한 AWS 계정의 ID를 입력합니다.

c. (선택 사항) 가상 프라이빗 게이트웨이에서 허용할 접두사 목록을 지정하려면 쉼표를 사용하여 구분하거나 개별 라인에 입력하여 허용되는 접두사에 접두사를 추가합니다.

8. Associate Direct Connect gateway(Direct Connect 게이트웨이 연결)를 선택합니다.

명령줄 또는 API를 사용하여 연결 제안을 생성하려면

- create-direct-connect-gateway-협회 제안 ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

연결 제안 수락 또는 거부

Direct Connect 게이트웨이의 소유자인 경우 연결을 생성하려면 해당 연결 제안을 수락해야 합니다. 생성하지 않으려면 연결 제안을 거부할 수 있습니다.

연결 제안을 수락하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. 대기 중인 제안이 있는 Direct Connect 게이트웨이를 선택하고 세부 정보 보기를 선택합니다.
4. Pending proposals(대기 중인 제안) 탭에서 제안을 선택하고 Accept proposal(제안 수락)을 선택합니다.
5. (선택 사항) 가상 프라이빗 게이트웨이에서 허용할 접두사 목록을 지정하려면 쉼표를 사용하여 구분하거나 개별 라인에 입력하여 허용되는 접두사에 접두사를 추가합니다.
6. Accept proposal(제안 수락)을 선택합니다.

연결 제안을 거부하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. 대기 중인 제안이 있는 Direct Connect 게이트웨이를 선택하고 세부 정보 보기를 선택합니다.
4. Pending proposals(대기 중인 제안) 탭에서 가상 프라이빗 게이트웨이를 선택하고 Reject proposal(제안 거부)을 선택합니다.

5. Reject proposal(제안 거부) 대화 상자에서 삭제를 입력하고 Reject proposal(제안 거부)을 선택합니다.

명령줄 또는 API를 사용하여 연결 제안을 보려면

- describe-direct-connect-gateway-협회 제안 ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

명령줄 또는 API를 사용하여 연결 제안을 수락하려면

- accept-direct-connect-gateway-협회 제안 ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

명령줄 또는 API를 사용하여 연결 제안을 거부하려면

- delete-direct-connect-gateway-협회 제안 ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

연결에 허용되는 접두사 업데이트

Direct Connect 게이트웨이를 통해 가상 프라이빗 게이트웨이에서 허용되는 접두사를 업데이트할 수 있습니다.

가상 프라이빗 게이트웨이의 소유자는 동일한 Direct Connect 게이트웨이 및 가상 프라이빗 게이트웨이에 대해 새 연결 제안을 생성하여 허용할 접두사를 지정합니다.

Direct Connect 게이트웨이의 소유자는 연결 제안을 수락할 때 허용되는 접두사를 업데이트하거나 다음과 같이 기존 연결에 대해 허용되는 접두사를 업데이트합니다.

명령줄 또는 API를 사용하여 기존 연결에 대해 허용되는 접두사를 업데이트하려면

- update-direct-connect-gateway-어소시에이션 ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

연결 제안 삭제

가상 프라이빗 게이트웨이의 소유자는 수락 대기 중 Direct Connect 게이트웨이 연결 제안을 삭제할 수 있습니다. 연결 제안이 수락되면 해당 제안을 삭제할 수 없지만 Direct Connect 게이트웨이에서 가상 프라이빗 게이트웨이의 연결을 해제할 수 있습니다. 자세한 정보는 the section called “가상 프라이빗 게이트웨이 연결 및 연결 해제”을 참조하세요.

연결 제안을 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 프라이빗 게이트웨이를 선택하고 가상 프라이빗 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Pending Direct Connect gateway associations(대기 중인 Direct Connect 게이트웨이 연결)를 선택하고 연결을 선택한 다음 연결 삭제를 선택합니다.
5. Delete association proposal(연결 제안 삭제) 대화 상자에서 삭제를 입력하고 삭제를 선택합니다.

명령줄 또는 API를 사용하여 대기 중인 연결 제안을 삭제하려면

- delete-direct-connect-gateway-협회 제안 ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

트랜짓 게이트웨이 연결

AWS Direct Connect 게이트웨이를 사용하여 전송 가상 인터페이스를 통해 전송 게이트웨이에 연결된 VPC 또는 VPN에 AWS Direct Connect 연결을 할 수 있습니다. Direct Connect 게이트웨이를 전송 게이트웨이와 연결합니다. 그런 다음 Direct Connect 게이트웨이 AWS Direct Connect 연결을 위한 트랜짓 가상 인터페이스를 생성합니다.

다음 규칙이 전송 게이트웨이 연결에 적용됩니다.

- Direct Connect 게이트웨이가 이미 가상 프라이빗 게이트웨이와 연결되어 있거나 프라이빗 가상 인터페이스에 연결되어 있는 경우 전송 게이트웨이에 Direct Connect 게이트웨이를 연결할 수 없습니다.
- 생성하고 사용할 수 있는 Direct Connect 게이트웨이 수에 제한이 있습니다. 자세한 정보는 할당량을 참조하세요.

- Direct Connect 게이트웨이는 연결된 전송 가상 인터페이스와 연결된 전송 게이트웨이 간의 통신을 지원합니다.
- 다른 리전에 있는 여러 전송 게이트웨이에 연결하는 경우, 각 전송 게이트웨이에 고유한 ASN을 사용합니다.
- Direct Connect를 통해 광고되는 네트워크 접두사 내의 모든 가상 인터페이스는 지역 간의 전송 게이트웨이에만 전파되며 동일한 지역 내에서는 전파되지 않습니다.

전송 게이트웨이 연결 및 연결 해제

전송 게이트웨이를 연결하는 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 콘솔을 엽니다. AWS Direct Connect
2. 탐색 창에서 Direct Connect 게이트웨이를 선택하고 Direct Connect 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Gateway associations(게이트웨이 연결)를 선택하고 Associate gateway(게이트웨이 연결)를 선택합니다.
5. 게이트웨이는 연결할 전송 게이트웨이를 선택합니다.
6. 허용된 접두사에는 Direct Connect 게이트웨이가 온프레미스 데이터 센터에 알리는 접두사(쉼표로 구분하거나 새 줄로 표시)를 입력합니다. 허용되는 접두사에 대한 자세한 정보는 the section called “허용되는 접두사 상호 작용” 섹션을 참조하세요.
7. 게이트웨이 연결을 선택합니다

Gateway associations(게이트웨이 연결)를 선택하여 Direct Connect 게이트웨이와 연결된 모든 게이트웨이를 볼 수 있습니다.

전송 게이트웨이 연결 해제 방법

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택하고 Direct Connect 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Gateway associations(게이트웨이 연결)를 선택하고 전송 게이트웨이를 선택합니다.
5. 연결 해제를 선택합니다.

전송 게이트웨이에 허용된 접두사 업데이트하는 방법

전송 게이트웨이에 허용된 접두사를 추가하거나 제거할 수 있습니다.

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택한 다음 허용된 접두사를 추가하거나 제거하려는 Direct Connect 게이트웨이를 선택합니다.
3. 게이트웨이 연결 탭을 선택합니다.
4. 수정하려는 게이트웨이를 선택하고 편집을 선택합니다.
5. 허용된 접두사에는 Direct Connect 게이트웨이가 온프레미스 데이터 센터에 알려주는 접두사를 입력합니다. 접두사가 여러 개인 경우 각 접두사를 쉼표로 구분하거나 각 접두사를 새 줄에 입력하세요. 추가하는 접두사는 모든 가상 프라이빗 게이트웨이의 Amazon VPC CIDR과 일치해야 합니다. 허용되는 접두사에 대한 자세한 정보는 the section called “허용되는 접두사 상호 작용” 섹션을 참조하세요.
6. Edit association(연결 편집)을 선택합니다.

   게이트웨이 연결 섹션에서 상태는 업데이트 내용을 표시합니다. 완료되면 상태가 연결됨 상태로 변경됩니다.
7. 연결 해제를 선택합니다.
8. 연결 해제 다시 선택하면 게이트웨이 연결을 해제할 것인지 확인합니다.

   게이트웨이 연결 섹션에서 상태가 연결 해제로 표시됩니다. 완료되면 확인 메시지가 표시되고 섹션에서 게이트웨이가 제거됩니다. 완료하는 데 몇 분 이상 걸릴 수도 있습니다.

명령줄 또는 API를 사용하여 전송 게이트웨이를 연결하는 방법

- create-direct-connect-gateway-어소시에이션 ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이와 연결된 전송 게이트웨이를 보는 방법

- describe-direct-connect-gateway-협회 ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

명령줄 또는 API를 사용하여 전송 게이트웨이를 연결 해제하는 방법

- delete-direct-connect-gateway-어소시에이션 ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

명령줄 또는 API를 사용하여 전송 게이트웨이에 허용된 접두사를 업데이트하는 방법

- update-direct-connect-gateway-어소시에이션 ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Direct Connect 게이트웨이에 대한 전송 가상 인터페이스 생성

AWS Direct Connect 연결을 트랜짓 게이트웨이에 연결하려면 연결을 위한 트랜짓 인터페이스를 만들어야 합니다. 연결할 Direct Connect 게이트웨이를 지정합니다.

> **Important**
>
> 전송 게이트웨이를 하나 이상의 Direct Connect 게이트웨이와 연결하는 경우 전송 게이트웨이와 Direct Connect 게이트웨이에서 사용하는 ASN(자율 시스템 번호)이 달라야 합니다. 예를 들어 전송 게이트웨이와 Direct Connect 게이트웨이 모두에 대해 기본 ASN 64512를 사용하면 연결 요청이 실패합니다.

Direct Connect 게이트웨이에 전송 가상 인터페이스를 프로비저닝하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 가상 인터페이스를 선택합니다.
3. 가상 인터페이스 생성을 선택합니다.
4. Virtual interface type(가상 인터페이스 유형)에서 유형에 대해 전송을 선택합니다.
5. Transit virtual interface settings(전송 가상 인터페이스 설정)에서 다음을 수행합니다:
   a. 가상 인터페이스 이름에 가상 인터페이스의 이름을 입력합니다.
   b. 연결에서 이 인터페이스에 사용할 Direct Connect 연결을 선택합니다.
   c. 가상 인터페이스 소유자의 경우, 가상 인터페이스가 사용자 AWS 계정용인 경우 내 AWS 계정을 선택합니다.

d. Direct Connect 게이트웨이에서 Direct Connect 게이트웨이를 선택합니다.

e. VLAN에 VLAN(Virtual Local Area Network)의 ID 번호를 입력합니다.

f. BGP ASN의 경우 새 가상 인터페이스에 대한 온프레미스 피어 라우터의 Border Gateway Protocol 자율 시스템 번호를 입력합니다.

   유효한 값은 1~2147483647입니다.

6. 추가 설정에서 다음을 수행합니다:

a. IPv4 BGP 또는 IPv6 피어를 구성하려면 다음을 수행합니다.

   [IPv4] IPv4 BGP 피어를 구성하려면 IPv4를 선택하고 다음을 수행합니다.

   - 이러한 IP 주소를 자체적으로 지정하려면 사용자 라우터 피어 IP에 Amazon이 트래픽을 전송해야 하는 IPv4 CIDR 대상 주소를 입력합니다.
   - Amazon 라우터 피어 IP에 AWS(으)로 트래픽을 전송하는 데 사용할 IPv4 CIDR 주소를 입력합니다.

   > **Important**
   >
   > IPv4 주소를 AWS 자동 할당하도록 설정하면 연결을 위한 RFC 3927에 따라 169.254.0.0/16 IPv4 링크-로컬에서 /29 CIDR이 할당됩니다. point-to-point AWS 고객 라우터 피어 IP 주소를 VPC 트래픽의 원본 및/또는 대상으로 사용하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다. 대신 RFC 1918 또는 기타 주소 지정 (비 RFC 1918) 을 사용하고 주소를 직접 지정해야 합니다.
   >
   > - RFC 1918에 대한 자세한 내용은 프라이빗 인터넷의 주소 할당을 참조하세요.
   > - RFC 3927에 대한 자세한 내용은 IPv4 링크-로컬 주소의 동적 구성을 참조하세요.

   [IPv6] IPv6 BGP 피어를 구성하려면 IPv6을 선택합니다. 피어 IPv6 주소는 Amazon의 IPv6 주소 풀에서 자동으로 할당됩니다. 사용자 지정 IPv6 주소는 지정할 수 없습니다.

b. 최대 전송 단위(MTU)를 1500(기본값)에서 8500(점보 프레임)으로 변경하려면 Jumbo MTU(MTU 크기 8500)를 선택합니다.

c. (선택 사항) Direct Connect 접속 지점 간의 직접 연결을 활성화하려면 활성화에서 활성화를 선택합니다. SiteLink

d. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 태그 추가(Add tag)를 선택하고 다음을 수행합니다.

- 키(Key)에 키 이름을 입력합니다.
- 값에서 키 값을 입력합니다.

[태그 제거] 태그 옆에 있는 태그 제거를 선택합니다.

7. 가상 인터페이스 생성을 선택합니다.

가상 인터페이스를 만든 후 사용하는 디바이스를 위한 라우터 구성을 다운로드할 수 있습니다. 자세한 정보는 라우터 구성 파일 다운로드을 참조하세요.

명령줄 또는 API를 사용하여 전송 가상 인터페이스를 생성하려면

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

명령줄 또는 API를 사용하여 Direct Connect 게이트웨이에 연결된 가상 인터페이스를 보려면

- describe-direct-connect-gateway-첨부 파일 ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

계정 간 전송 게이트웨이 연결

기존 Direct Connect 게이트웨이 또는 새 Direct Connect 게이트웨이를 모든 AWS 계정에서 소유한 전송 게이트웨이와 연결할 수 있습니다. 전송 게이트웨이의 소유자는 연결 제안을 생성하고 Direct Connect 게이트웨이의 소유자는 연결 제안을 수락해야 합니다.

연결 제안은 전송 게이트웨이에서 허용되는 접두사를 포함할 수 있습니다. Direct Connect 게이트웨이의 소유자는 상황에 따라 연결 제안의 요청된 접두사를 재정의할 수 있습니다.

허용되는 접두사

전송 게이트웨이 연결의 경우 Direct Connect 게이트웨이에서 허용된 접두사 목록을 제공합니다. 이 목록은 트랜짓 게이트웨이에 연결된 VPC에 CIDR이 할당되지 않은 경우에도 온프레미스에서 트랜짓 게이트웨이로 트래픽을 라우팅하는 데 사용됩니다. AWS Direct Connect 게이트웨이 허용 접두사 목록의 접두사는 Direct Connect 게이트웨이에서 시작되어 온프레미스 네트워크에 공고됩니다. 허용된 접두사가 전송 게이트웨이 및 가상 프라이빗 게이트웨이와 상호 작용하는 방법에 대한 자세한 내용은 the section called “허용되는 접두사 상호 작용”을(를) 참조하세요.

Tasks

- 전송 게이트웨이 연결 제안 생성
- 전송 게이트웨이 연결 제안 수락 또는 거부
- 전송 게이트웨이 연결에 허용되는 접두사 업데이트
- 전송 게이트웨이 연결 제안 삭제

전송 게이트웨이 연결 제안 생성

전송 게이트웨이를 소유하고 있다면 연결 제안을 생성해야 합니다. 트랜짓 게이트웨이는 계정의 VPC 또는 VPN에 연결되어야 합니다 AWS . Direct Connect 게이트웨이의 소유자는 Direct Connect 게이트웨이의 ID 및 해당 AWS 계정의 ID를 공유해야 합니다. 제안을 생성한 후 Direct Connect 게이트웨이의 소유자가 해당 제안을 수락해야 사용자가 AWS Direct Connect를 통해 온프레미스 네트워크에 액세스할 수 있습니다.

연결 제안을 생성하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 전송 게이트웨이를 선택하고 해당 전송 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Direct Connect gateway associations(Direct Connect 게이트웨이 연결)를 선택하고 Associate Direct Connect gateway(Direct Connect 게이트웨이 연결)를 선택합니다.
5. Association account type(연결 계정 유형)의 계정 소유자에서 다른 계정을 선택합니다.
6. Direct Connect 게이트웨이 소유자에는 Direct Connect 게이트웨이를 소유하는 계정의 ID를 입력합니다.
7. Association settings(연결 설정)에서 다음을 수행합니다.
   a. Direct Connect gateway ID(Direct Connect 게이트웨이 ID)에 Direct Connect 게이트웨이의 ID를 입력합니다.
   b. 가상 인터페이스 소유자에는 해당 연결의 가상 인터페이스를 소유하는 계정의 ID를 입력합니다.
   c. (선택 사항) 전송 게이트웨이에서 허용할 접두사 목록을 지정하려면 쉼표를 사용하여 구분하거나 개별 라인에 입력하여 허용되는 접두사에 접두사를 추가합니다.
8. Associate Direct Connect gateway(Direct Connect 게이트웨이 연결)를 선택합니다.

명령줄 또는 API를 사용하여 연결 제안을 생성하려면

- create-direct-connect-gateway-협회 제안 ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

전송 게이트웨이 연결 제안 수락 또는 거부

Direct Connect 게이트웨이의 소유자인 경우 연결을 생성하려면 해당 연결 제안을 수락해야 합니다. 또한 연결 제안을 거부할 수도 있습니다.

연결 제안을 수락하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. 대기 중인 제안이 있는 Direct Connect 게이트웨이를 선택하고 세부 정보 보기를 선택합니다.
4. Pending proposals(대기 중인 제안) 탭에서 제안을 선택하고 Accept proposal(제안 수락)을 선택합니다.
5. ((선택 사항) 전송 게이트웨이에서 허용할 접두사 목록을 지정하려면 쉼표를 사용하여 구분하거나 개별 라인에 입력하여 허용되는 접두사에 접두사를 추가합니다.
6. Accept proposal(제안 수락)을 선택합니다.

연결 제안을 거부하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 Direct Connect 게이트웨이를 선택합니다.
3. 대기 중인 제안이 있는 Direct Connect 게이트웨이를 선택하고 세부 정보 보기를 선택합니다.
4. Pending proposals(대기 중인 제안) 탭에서 전송 게이트웨이를 선택하고 Reject proposal(제안 거부)을 선택합니다.
5. Reject proposal(제안 거부) 대화 상자에서 삭제를 입력하고 Reject proposal(제안 거부)을 선택합니다.

명령줄 또는 API를 사용하여 연결 제안을 보려면

- describe-direct-connect-gateway-협회 제안 ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

명령줄 또는 API를 사용하여 연결 제안을 수락하려면

- accept-direct-connect-gateway-협회 제안 ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

명령줄 또는 API를 사용하여 연결 제안을 거부하려면

- delete-direct-connect-gateway-협회 제안 ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

전송 게이트웨이 연결에 허용되는 접두사 업데이트

Direct Connect 게이트웨이를 통해 전송 게이트웨이에서 허용되는 접두사를 업데이트할 수 있습니다.

전송 게이트웨이 소유자는 동일한 Direct Connect 게이트웨이 및 가상 프라이빗 게이트웨이에 대해 새 연결 제안을 생성하여 허용할 접두사를 지정합니다.

Direct Connect 게이트웨이의 소유자는 연결 제안을 수락할 때 허용되는 접두사를 업데이트하거나 다음과 같이 기존 연결에 대해 허용되는 접두사를 업데이트합니다.

명령줄 또는 API를 사용하여 기존 연결에 대해 허용되는 접두사를 업데이트하려면

- update-direct-connect-gateway-어소시에이션 ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

전송 게이트웨이 연결 제안 삭제

전송 게이트웨이 소유자는 수락 대기 중 Direct Connect 게이트웨이 연결 제안을 삭제할 수 있습니다. 연결 제안이 수락되면 해당 제안을 삭제할 수 없지만 Direct Connect 게이트웨이에서 전송 게이트웨이의 연결을 해제할 수 있습니다. 자세한 정보는 the section called “전송 게이트웨이 연결 제안 생성”을 참조하세요.

연결 제안을 삭제하려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 전송 게이트웨이를 선택하고 해당 전송 게이트웨이를 선택합니다.
3. 세부 정보 보기를 선택합니다.
4. Pending gateway associations(대기 중인 게이트웨이 연결)를 선택하고 연결을 선택한 다음 연결 삭제를 선택합니다.
5. Delete association proposal(연결 제안 삭제) 대화 상자에서 삭제를 입력하고 삭제를 선택합니다.

명령줄 또는 API를 사용하여 대기 중인 연결 제안을 삭제하려면

- delete-direct-connect-gateway-협회 제안 ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

허용되는 접두사 상호 작용

허용된 접두사가 전송 게이트웨이 및 가상 프라이빗 게이트웨이와 상호 작용하는 방법을 알아봅니다. 자세한 정보는 the section called “라우팅 정책 및 BGP 커뮤니티”을 참조하세요.

가상 프라이빗 게이트웨이 연결

이 접두사 목록(IPv4 and IPv6)은 동일한 CIDR 또는 보다 작은 CIDR 범위를 Direct Connect 게이트웨이에 공급할 수 있는 필터로 작동합니다. 접두사를 VPC CIDR 블록과 같거나 넓은 범위로 설정해야 합니다.

> **Note**
> 허용 목록은 필터 역할만 하며 연결된 VPC CIDR만 고객 게이트웨이에 알립니다.

CIDR 10.0.0.0/16이 포함된 VPC가 가상 프라이빗 게이트웨이에 연결된 시나리오를 고려해 보십시오.

- 허용된 접두사 목록이 22.0.0.0/24로 설정되면 22.0.0.0/24는 10.0.0.0/16과 동일하거나 그보다 넓지 않으므로 라우팅을 수신하지 못합니다.
- 허용된 접두사 목록이 10.0.0.0/24로 설정되면 10.0.0.0/24는 10.0.0.0/16과 동일하지 않으므로 라우팅을 수신하지 못합니다.

- 허용된 접두사 목록이 10.0.0.0/15로 설정되면 이 IP 주소는 10.0.0.0/16보다 넓으므로 10.0.0.0/16을 수신하게 됩니다.

허용된 접두사를 제거하거나 추가할 때 해당 접두사를 사용하지 않는 트래픽은 영향을 받지 않습니다. 업데이트 중에는 상태가 `associated`에서 `updating`(으)로 바뀝니다. 기존 접두사를 수정하면 해당 접두사를 사용하는 트래픽만 지연될 수 있습니다.

트랜짓 게이트웨이 연결

전송 게이트웨이 연결의 경우 Direct Connect 게이트웨이에서 허용된 접두사 목록을 제공합니다. 이 목록은 전송 게이트웨이에 연결된 VPC에 CIDR이 할당되지 않은 경우에도 Direct Connect에 들어오고 나가는 온프레미스을 전송 게이트웨이로 라우팅합니다. 허용되는 접두사는 게이트웨이 유형에 따라 다르게 작동합니다.

- 전송 게이트웨이 연결의 경우 입력된 허용된 접두사만 온프레미스에 광고됩니다. 이는 Direct Connect 게이트웨이 ASN에서 시작된 것으로 표시됩니다.
- 가상 프라이빗 게이트웨이의 경우 입력된 허용된 접두사는 같거나 더 작은 CIDR을 허용하는 필터 역할을 합니다.

CIDR 10.0.0.0/16이 포함된 VPC가 전송 게이트웨이에 연결된 시나리오를 고려해 보세요.

- 허용된 접두사 목록이 22.0.0.0/24로 설정되면 전송 가상 인터페이스의 BGP를 통해 22.0.0.0/24를 수신합니다. 허용된 접두사 목록에 있는 접두사를 직접 제공하기 때문에 10.0.0.0/16은 수신하지 못합니다.
- 허용된 접두사 목록이 10.0.0.0/24로 설정되면 전송 가상 인터페이스의 BGP를 통해 10.0.0.0/24를 수신합니다. 허용된 접두사 목록에 있는 접두사를 직접 제공하기 때문에 10.0.0.0/16은 수신하지 못합니다.
- 허용된 접두사 목록이 10.0.0.0/8로 설정되면 전송 가상 인터페이스의 BGP를 통해 10.0.0.0/8을 수신합니다.

여러 전송 게이트웨이가 Direct Connect 게이트웨이에 연결된 경우 허용된 접두사 중복은 허용되지 않습니다. 예를 들어 10.1.0.0/16을 포함하는 허용된 접두사 목록이 있는 전송 게이트웨이와 10.2.0.0/16 및 0.0.0.0/0을 포함하는 허용된 접두사 목록이 있는 두 번째 전송 게이트웨이가 있는 경우 두 번째 전송 게이트웨이의 연결을 0.0.0.0/0으로 설정할 수 없습니다. 0.0.0.0/0에는 모든 IPv4 네트워크가 포함되므로 Direct Connect 게이트웨이에 연결된 게이트웨이에 연결된 경우 0.0.0.0/0을 구성할 수 없습니

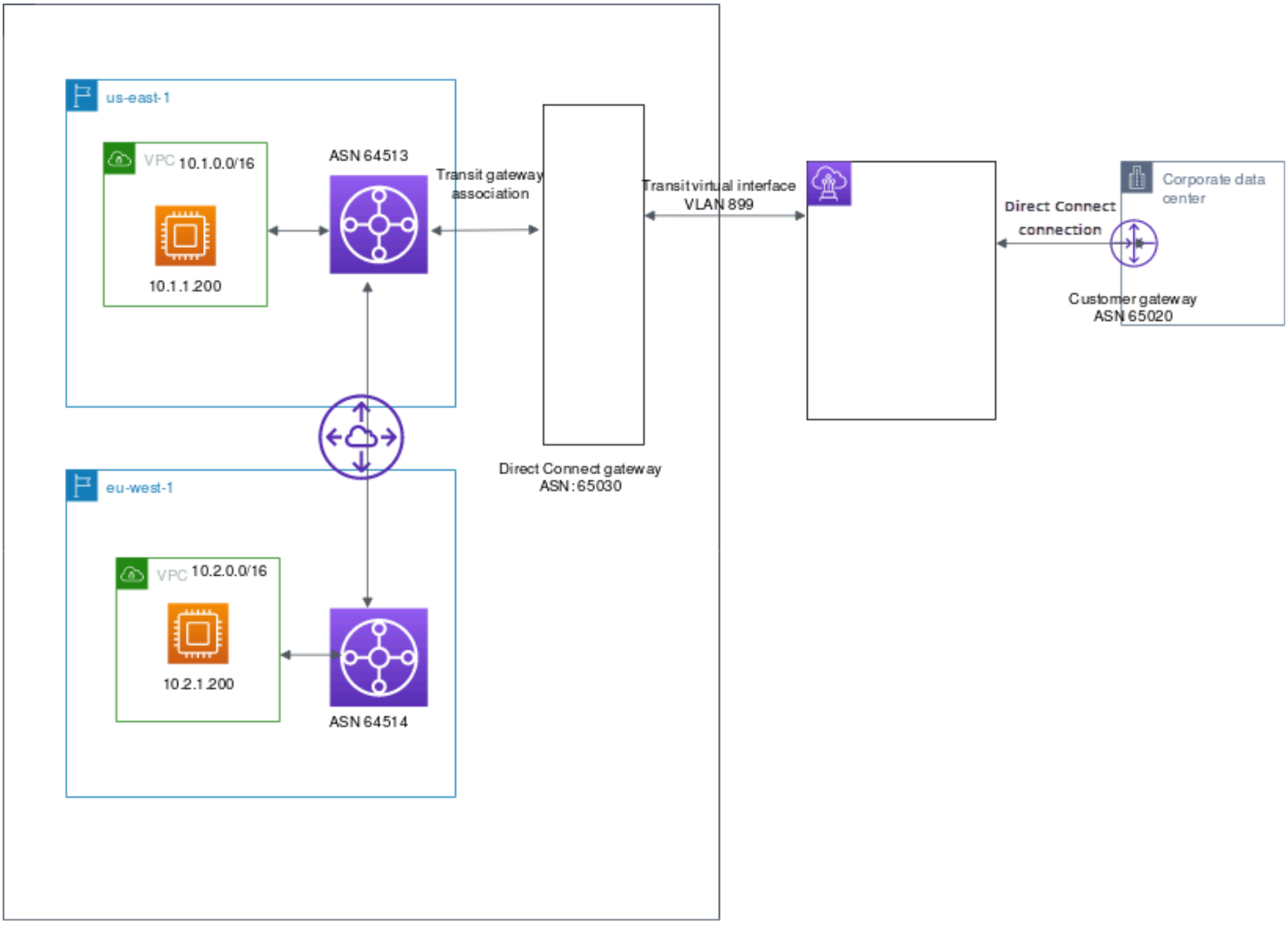
다. 허용된 경로가 Direct Connect 게이트웨이에 있는 하나 이상의 기존 허용 경로와 겹친다는 오류가 반환됩니다.

허용된 접두사를 제거하거나 추가할 때 해당 접두사를 사용하지 않는 트래픽은 영향을 받지 않습니다. 업데이트 중에는 상태가 `associated`에서 `updating`(으)로 바뀝니다. 기존 접두사를 수정하면 해당 접두사를 사용하는 트래픽만 지연될 수 있습니다.

예: 전송 게이트웨이 구성에서 접두사 허용

서로 다른 두 AWS 리전에 기업 데이터 센터에 액세스하는 인스턴스가 있는 구성을 생각해 보세요. 이 구성에 대해 다음 리소스를 구성할 수 있습니다.

- 각 리전의 전송 게이트웨이.
- 전송 게이트웨이 피어링 연결.
- Direct Connect 게이트웨이.
- 전송 게이트웨이 중 하나(us-east-1에 있는 게이트웨이)와 Direct Connect 게이트웨이 간의 전송 게이트웨이 연결입니다.
- 온프레미스 위치와 AWS Direct Connect 위치의 전송 가상 인터페이스.



리소스에 대해 다음과 같은 옵션이 있습니다.

- Direct Connect 게이트웨이: ASN을 65030으로 설정합니다. 자세히 알아보려면 the section called "Direct Connect 게이트웨이 생성"의 내용을 참조하세요.
- 전송 가상 인터페이스: VLAN을 899로 설정하고 ASN을 65020으로 설정합니다. 자세히 알아보려면 the section called "Direct Connect 게이트웨이에 대한 전송 가상 인터페이스 생성"의 내용을 참조하세요.
- 전송 게이트웨이와 Direct Connect 게이트웨이 연결: 허용된 접두사를 10.0.0.0/8로 설정합니다.

  이 CIDR 블록은 두 VPC CIDR 블록을 모두 포함합니다. 자세히 알아보려면 the section called "전송 게이트웨이 연결 및 연결 해제"의 내용을 참조하세요.
- VPC 라우팅: 10.2.0.0 VPC의 트래픽을 라우팅하려면 VPC 라우팅 테이블에 목적지가 0.0.0.0/0이고 전송 게이트웨이 ID가 타겟인 경로를 생성합니다. 전송 게이트웨이 라우팅에 관해 자세한 내용은 Amazon VPC 사용 설명서의 전송 게이트웨이에 대한 라우팅을 참조하세요.

AWS Direct Connect 리소스에 태그 지정

태그는 리소스 소유자가 자신의 AWS Direct Connect 리소스에 지정하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다. 태그를 사용하면 리소스 소유자가 용도 또는 환경을 기준으로 하는 등 AWS Direct Connect 리소스를 다양한 방식으로 분류할 수 있습니다. 이 기능은 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있으므로 동일한 유형의 리소스가 많을 때 유용합니다.

예를 들어, 한 리전에 있는 두 개의 AWS Direct Connect 연결이 각각 다른 위치에 있다고 가정하겠습니다. 연결 `dxcon-11aa22bb`는 프로덕션 트래픽을 처리하는 연결로, 가상 인터페이스 `dxvif-33cc44dd`와 연결되어 있습니다. 연결 `dxcon-abcabcab`는 중복(백업) 연결로, 가상 인터페이스 `dxvif-12312312`와 연결되어 있습니다. 다음과 같이 연결 및 가상 인터페이스를 구별하기 쉽도록 태그를 지정할 수 있습니다.

리소스 ID	태그 키	태그 값
`dxcon-11aa22bb`	용도	프로덕션
	위치	암스테르담
`dxvif-33cc44dd`	용도	프로덕션
`dxcon-abcabcab`	용도	백업
	위치	프랑크푸르트
`dxvif-12312312`	용도	백업

각 리소스 유형에 대한 요건을 충족하는 태그 키 세트를 고안하는 것이 좋습니다. 일관된 태그 키 세트를 사용하면 리소스를 보다 쉽게 관리할 수 있습니다. 태그는 AWS Direct Connect에는 의미가 없으며 엄격하게 문자열로 해석됩니다. 또한 태그는 리소스에 자동으로 배정되지 않습니다. 태그 키와 값을 편집할 수 있으며 언제든지 리소스에서 태그를 제거할 수 있습니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 해당 리소스에 대해 키가 기존 태그와 동일한 태그를 추가하는 경우 새 값이 이전 값을 덮어씁니다. 리소스를 삭제하면 리소스 태그도 삭제됩니다.

AWS Direct Connect 콘솔, AWS Direct Connect API, AWS CLI, AWS Tools for Windows PowerShell 또는 AWS SDK를 사용하여 다음 AWS Direct Connect 리소스에 태그를 지정할 수 있습니다. 이러한

도구를 사용하여 태그를 관리하는 경우 리소스의 Amazon 리소스 이름(ARN)을 지정해야 합니다. ARN에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon 리소스 이름(ARN)을 참조하세요.

리소스	태그 지원	생성 시 태그 지원	액세스 및 리소스 할당을 제어하는 태그 지원	비용 할당 지원
연결	예	예	예	예
가상 인터페이스	예	예	예	아니요
링크 집계 그룹 (LAG)	예	예	예	예
상호 연결	예	예	예	예
Direct Connect 게이트웨이	아니요	아니요	아니요	아니요

태그 제한

태그에 적용되는 규칙 및 제한은 다음과 같습니다.

- 리소스당 최대 태그 수: 50개
- 최대 키 길이: 유니코드 128자
- 최대 값 길이: 유니코드 265자
- 태그 키와 값은 대/소문자를 구분합니다.
- `aws:` 접두사는 AWS용으로 예약되어 있습니다. 태그에 `aws:` 접두사가 있는 태그 키가 있는 경우 태그의 키 또는 값을 편집하거나 삭제할 수 없습니다. `aws:` 접두사가 지정된 태그 키를 가진 태그는 리소스당 태그 수 제한에 포함되지 않습니다.
- 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 공백 및 숫자와 특수 문자 + - = . _ : / @
- 리소스 소유자만 태그를 추가하거나 제거할 수 있습니다. 예를 들어, 호스팅 연결이 있는 경우에는 파트너가 태그를 추가하거나 제거하거나 볼 수 없습니다.
- 비용 할당 태그는 연결, 상호 연결 및 LAG에 대해서만 지원됩니다. 비용 관리로 태그를 이용하는 방법을 알아보려면 AWS Billing and Cost Management 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

CLI 또는 API를 사용한 태그 작업

다음을 사용하여 리소스에 대한 태그를 추가, 업데이트, 나열 및 삭제할 수 있습니다.

태스크	API	CLI
하나 이상의 태그를 추가하거나 덮어씁니다.	TagResource	tag-resource
하나 이상의 태그를 삭제합니다.	UntagResource	untag-resource
하나 이상의 태그에 대해 설명합니다.	DescribeTags	describe-tags

예시

tag-resource 명령을 사용하여 연결 `dxcon-11aa22bb`에 태그를 지정합니다.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

describe-tags 명령을 사용하여 연결 `dxcon-11aa22bb` 태그를 설명합니다.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

untag-resource 명령을 사용하여 연결 `dxcon-11aa22bb`에서 태그를 제거합니다.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

AWS Direct Connect의 보안

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

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

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사원은 정기적으로 AWS 규제 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Direct Connect에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내의 AWS 서비스를 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Direct Connect 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AWS Direct Connect를 구성하는 방법을 보여줍니다. 또한 AWS Direct Connect 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- AWS Direct Connect의 데이터 보호
- Direct Connect의 ID와 액세스 관리
- AWS Direct Connect의 로깅 및 모니터링
- AWS Direct Connect의 규정 준수 확인
- AWS Direct Connect의 복원성
- AWS Direct Connect의 인프라 보안

AWS Direct Connect의 데이터 보호

AWS 공동 책임 모델은 AWS Direct Connect의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS은(는) 모든 AWS 클라우드을(를) 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 Data Privacy FAQ(데

이터 프라이버시 FAQ)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정보안 인증 정보를 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 인증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하세요. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 Name 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS Direct Connect 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 보안 인증를 URL에 포함시켜서는 안 됩니다.

데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

주제

- AWS Direct Connect의 인터네트워크 트래픽 개인 정보 보호
- 전송 중 암호화 AWS Direct Connect

AWS Direct Connect의 인터네트워크 트래픽 개인 정보 보호

서비스와 온프레미스 클라이언트 및 애플리케이션 간의 트래픽

프라이빗 네트워크와 AWS 사이에 두 연결 옵션이 있습니다.

- AWS Site-to-Site VPN에 연결 자세한 내용은 the section called “인프라 보안” 섹션을 참조하세요.
- VPC에 연결. 자세한 정보는 the section called “가상 프라이빗 게이트웨이 연결” 및 the section called “트랜짓 게이트웨이 연결” 섹션을 참조하세요.

같은 리전에 있는 AWS 리소스 사이의 트래픽

다음과 같이 두 가지 연결 옵션이 있습니다.

- AWS Site-to-Site VPN에 연결 자세한 내용은 the section called “인프라 보안” 섹션을 참조하세요.
- VPC에 연결. 자세한 정보는 the section called “가상 프라이빗 게이트웨이 연결” 및 the section called “트랜짓 게이트웨이 연결” 섹션을 참조하세요.

전송 중 암호화 AWS Direct Connect

AWS Direct Connect은(는) 기본 설정상 전송 중인 트래픽은 암호화하지 않습니다. AWS Direct Connect를 통과하는 전송 중인 데이터를 암호화하려면 해당 서비스에 대한 전송 암호화 옵션을 사용해야 합니다. EC2 인스턴스 트래픽 암호화에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 전송 중 암호화를 참조하십시오.

AWS Direct Connect 및 AWS Site-to-Site VPN을(를) 사용하면 하나 이상의 AWS Direct Connect 전용 네트워크 연결을 Amazon VPC VPN과 결합할 수 있습니다. 이 조합은 IPsec으로 암호화된 프라이빗 연결을 제공하여 네트워크 비용을 줄이고, 대역폭 처리량을 늘리고, 인터넷 기반 VPN 연결보다 더 일관된 네트워크 환경을 제공합니다. 자세한 내용은 Amazon VPC-to-Amazon VPC 연결 옵션을 참조하십시오.

MAC 보안(MACsec)은 데이터 기밀성, 데이터 무결성 및 데이터 원본 인증을 제공하는 IEEE 표준입니다. MACsec을 지원하는 AWS Direct Connect 연결을 사용하여 회사 데이터 센터의 데이터를 AWS Direct Connect 위치로 암호화할 수 있습니다. 자세한 내용은 MAC 보안 섹션을 참조하세요.

Direct Connect의 ID와 액세스 관리

AWS Identity and Access Management(IAM)은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 Direct Connect 리소스를 사용할 수 있는 인증(로그인) 및 승인(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- Direct Connect 에서 IAM을 사용하는 방식
- Direct Connect의 ID 중심 정책 예제
- AWS Direct Connect에 대한 서비스 연결 역할
- AWS Direct Connect의 AWS 관리형 정책
- Direct Connect 자격 증명 및 액세스 문제 해결

고객

AWS Identity and Access Management (IAM)를 사용하는 방법은 Direct Connect에서 수행하는 작업에 따라 달라집니다.

서비스 사용자 - Direct Connect 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Direct Connect 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Direct Connect의 기능에 액세스할 수 없는 경우 Direct Connect 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Direct Connect 리소스를 책임지고 있는 경우 Direct Connect에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Direct Connect 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사가 Direct Connect에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Direct Connect 에서 IAM을 사용하는 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Direct Connect에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Direct Connect 자격 증명 기반 정책 예제를 보려면 Direct Connect의 ID 중심 정책 예제 섹션을 참조하세요.

ID를 통한 인증

인증은 ID 보안 인증을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자 또는 IAM 사용자로 또는 IAM 역할을 수임하여 인증(AWS에 로그인)되어야 합니다.

자격 증명 소스를 통해 제공된 보안 인증 정보를 사용하여 페더레이션 ID로 AWS에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증, Google 또는 Facebook 보안 인증이 페더레이션형 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 연동을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임합니다.

사용자 유형에 따라 AWS Management Console 또는AWS 액세스 포털에 로그인할 수 있습니다. AWS에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법을 참조하세요.

AWS에 프로그래밍 방식으로 액세스하는 경우, AWS는 보안 인증 정보를 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK) 및 명령줄 인터페이스(CLI)를 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

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

AWS 계정 루트 사용자

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 태스크에는 루트 사용자를 가급적 사용하지 않는 것이 좋습니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크 섹션을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구합니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리의 사용자 또는 자격 증명 소스를 통해 제공된 보안 인증을 사용하여 AWS 서비스에 액세스하는 모든 사용자입니다. 페더레이션 자격 증명은 AWS 계정에 액세스할 때 역할을 수임하고 역할은 임시 보안 인증을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정및 애플리케이션에서 사용하기 위해 고유한 자격 증명 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정에 속하는 ID입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체 섹션을 참조하세요.

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

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

IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS 계정 내의 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할 전환하여 AWS Management Console에서 IAM 역할을 임시로 수임할 수 있습니다. AWS CLI 또는 AWS API 태스크를 직접적으로 호출하거나 사용자 지정 URL을 사용하여 역

할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 연동 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 집합을 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트 섹션을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스: IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스를 사용하면 정책을 리소스에 직접 연결할 수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하세요.
- 교차 서비스 액세스: 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어 서비스에서 직접적으로 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 액세스 세션 전달(FAS) - IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 태스크를 트리거하는 태스크를 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 보안 주체의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할: 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할: 서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여 섹션을 참조하세요.

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

정책을 사용한 액세스 관리

정책을 생성하고 AWS 자격 증명 또는 리소스에 연결하여 AWS 내 액세스를 제어합니다. 정책은 ID 또는 리소스와 연결될 때 해당 권한을 정의하는 AWS의 개체입니다. AWS는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되는지 또는 거부되는지를 결정합니다. 대부분의 정책은 AWS에 JSON 설명서로서 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

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

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

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

ID 기반 정책

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

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 AWS 계정에 속한 다수의 사용자, 그룹 및 역할에 독립적으로 추가할 수 있는 정책입니다. 관리형 정책에는 AWS관리형 정책과 고객 관리형 정책이 포함되어 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

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

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

액세스 제어 목록(ACLs)

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

Amazon S3, AWS WAF 및 Amazon VPC는 ACL을 지원하는 대표적인 서비스입니다. ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요 섹션을 참조하세요.

기타 정책 유형

AWS은(는) 비교적 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 유형은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계 섹션을 참조하세요.

- 서비스 제어 정책(SCP): SCP는 AWS Organizations에서 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations는 기업이 소유하는 여러 개의 AWS 계정을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자을(를) 비롯하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

Direct Connect 에서 IAM을 사용하는 방식

IAM을 사용하여 Direct Connect에 대한 액세스를 관리하기 전에 Direct Connect에서 사용할 수 있는 IAM 기능을 알아보세요.

Direct Connect에서 사용할 수 있는 IAM 기능

IAM 특성	Direct Connect 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요

IAM 특성	Direct Connect 지원
ABAC(정책 내 태그)	부분
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	아니요

Direct Connect 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서에서 IAM으로 작업하는 AWS 서비스를 참조하세요.

Direct Connect의 ID 중심 정책

ID 기반 정책 지원	예

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

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

Direct Connect의 ID 중심 정책 예제

Direct Connect 자격 증명 기반 정책 예제를 보려면 Direct Connect의 ID 중심 정책 예제 섹션을 참조하세요.

Direct Connect 내의 리소스 기반 정책

리소스 기반 정책 지원	아니요

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

교차 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념합니다. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체(사용자 또는 역할)에도 리소스 액세스 권한을 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 ID 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하세요.

Direct Connect에 대한 정책 조치

정책 작업 지원	예

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

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

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

Direct Connect 작업 목록을 보려면 서비스 권한 부여 참조의 Direct Connect에서 정의한 작업을 참조하십시오.

Direct Connect의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
Direct Connect
```

단일 명령문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
```

```
        "Direct Connect:action1",
        "Direct Connect:action2"
           ]
```

Direct Connect에 대한 정책 리소스

정책 리소스 지원	예

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

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

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Direct Connect 리소스 유형 및 해당 ARN의 목록을 보려면 AWS Direct Connect API 참조의 Direct Connect에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Direct Connect가 정의한 작업을 참조하세요.

Direct Connect 자격 증명 기반 정책 예제를 보려면 Direct Connect의 ID 중심 정책 예제 섹션을 참조하세요.

Direct Connect 리소스 기반 정책의 예제는 Direct Connect 자격 증명 기반 정책 예제(태그 기반 조건 사용) 을 참조하세요.

Direct Connect에 사용되는 조건 키

서비스별 정책 조건 키 지원	예

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

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

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우 AWS는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우 AWS는 논리적 `OR` 작업을 사용하여 조건을 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키 섹션을 참조하세요.

Direct Connect 조건 키 목록을 보려면 AWS Direct ConnectAPI 참의 Direct Connect를 위한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 서비스 권한 부여 참조의 Direct Connect를 위한 작업, 리소스 및 조건 키를 참조하십시오.

Direct Connect 자격 증명 기반 정책 예제를 보려면 Direct Connect의 ID 중심 정책 예제 섹션을 참조하세요.

Direct Connect 방식의 ACL

ACL 지원	아니요

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

Direct Connect 기능을 사용한 ABAC

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수

있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

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

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

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

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

Direct Connect에서 임시 보안 인증 정보 사용

임시 보안안 인증 정보 지원	예

일부 AWS 서비스는 임시 보안 인증을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

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

AWS CLI 또는 AWS API를 사용하여 임시 보안 인증을 수동으로 만들 수 있습니다 그런 다음 이러한 임시 보안 인증을 사용하여 AWS에 액세스할 수 있습니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 보안 인증을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명을 참조하세요.

Direct Connect의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 보안 주체의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Direct Connect의 서비스 역할

서비스 역할 지원	예

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

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 Direct Connect 기능이 중단될 수 있습니다. Direct Connect가 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Direct Connect 에 대한 서비스 연결 역할

서비스 연결 역할 지원	아니요

서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작동하는 AWS 서비스 섹션을 참조하십시오. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Direct Connect의 ID 중심 정책 예제

기본적으로 사용자 및 역할은 Direct Connect 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용해

작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

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

각 리소스 유형에 대한 ARN 형식을 비롯하여 Direct Connect에서 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Direct Connect에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Direct Connect에 사용되는 작업, 리소스 및 조건
- Direct Connect 콘솔 사용
- 사용자가 자신이 권한을 볼 수 있도록 허용
- AWS Direct Connect에 대한 읽기 전용 액세스
- AWS Direct Connect에 대한 전체 액세스
- Direct Connect 자격 증명 기반 정책 예제(태그 기반 조건 사용)

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Direct Connect 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기: 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책) 섹션을 참조하세요.
- 최소 권한 적용: IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한: 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 특정 AWS 서비스(예: AWS CloudFormation)을(를) 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 IAM 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요: AWS 계정 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성) 섹션을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례 섹션을 참조하세요.

Direct Connect에 사용되는 작업, 리소스 및 조건

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스 및 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. Direct Connect은 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알고 싶은 경우 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

관리자는 AWSJSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는 지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

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

Direct Connect의 정책 작업은 작업 앞에 접두사 `directconnect:`을(를) 사용합니다. 예를 들어 누군가에게 Amazon EC2 `DescribeVpnGateways` API 작업을 통해 Amazon EC2 인스턴스를 실행할 권한을 부여하려면 해당 정책에 `ec2:DescribeVpnGateways` 작업을 포함하세요. 정책 문에는

`Action` 또는 `NotAction` 요소가 포함되어야 합니다. Direct Connect은 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

다음과 같은 정책 예시는 AWS Direct Connect에 대한 읽기 액세스를 부여합니다.

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

다음과 같은 정책 예시는 AWS Direct Connect에 대한 모든 액세스를 부여합니다.

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

Direct Connect 작업 목록을 보려면 IAM 사용 설명서의 Direct Connect에서 정의한 작업을 참조하세요.

리소스

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

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

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Direct Connect는 다음 ARN을 사용합니다.

Direct Connect 리소스 ARN

리소스 유형	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARNs) 및 AWS 서비스 네임스페이스를 참조하세요.

예를 들어, 설명문에 `dxcon-11aa22bb` 인터페이스를 지정하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

특정 계정에 속하는 모든 가상 인터페이스를 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

리소스를 생성하기 위한 작업과 같은 일부 Direct Connect 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

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

Direct Connect 리소스 유형 및 해당 ARN의 목록을 보려면 IAM 사용 설명서의 AWS Direct Connect에서 정의된 리소스 유형을 참조하세요. 각 리소스의 ARN을 지정할 수 있는 태스크를 알아보려면 SERVICE-ACTIONS-URL을 참조하세요.

조건 키

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

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

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우 AWS는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우 AWS는 논리적 `OR` 작업을 사용하여 조건을 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키 섹션을 참조하세요.

Direct Connect에서는 자체 조건 키 집합을 정의하고 일부 전역 조건 키 사용도 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

태그 리소스가 있는 조건 키를 사용할 수 있습니다. 자세한 내용은 예제: 특정 리전으로 액세스 제한을 참조하세요.

Direct Connect 조건 키 목록을 보려면 IAM 사용 설명서의 Direct Connect를 위한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 태스크와 리소스를 알아보려면SERVICE-ACTIONS-URL을 참조하세요.

Direct Connect 콘솔 사용

Direct Connect 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한은 AWS 계정에서 Direct Connect 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 개체가 Direct Connect 콘솔을 여전히 사용할 수 있도록 하려면 AWS 관리형 정책도 개체에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

```
directconnect
```

AWS CLI 또는 AWSAPI만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 자신이 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Direct Connect에 대한 읽기 전용 액세스

다음과 같은 정책 예시는 AWS Direct Connect에 대한 읽기 액세스를 부여합니다.

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

AWS Direct Connect에 대한 전체 액세스

다음과 같은 정책 예시는 AWS Direct Connect에 대한 모든 액세스를 부여합니다.

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

```
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Direct Connect 자격 증명 기반 정책 예제(태그 기반 조건 사용)

태그 키 조건을 사용하여 리소스 및 요청에 대한 액세스를 제어할 수 있습니다. 또한 IAM 정책에서 조건을 사용하여 리소스 또는 요청에 특정 태그 키를 사용할 수 있는지 여부를 제어할 수 있습니다.

IAM 정책으로 태그를 이용하는 방법은 IAM 사용 설명서에서 태그를 이용한 액세스 제어를 참조하세요.

태그를 기반으로 하는 Direct Connect 가상 인터페이스 연결

다음 예에서는 태그에 환경 키 및 preprod 또는 프로덕션 값이 포함된 경우에만 가상 인터페이스의 연결을 허용하는 정책을 생성할 수 있는 방법을 보여줍니다

```
       {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": [
            "directconnect:AssociateVirtualInterface"
          ],
          "Resource": "arn:aws:directconnect:*:*:dxvif/*",
          "Condition": {
            "StringEquals": {
              "aws:ResourceTag/environment": [
                "preprod",
                "production"
              ]
            }
          }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "directconnect:DescribeVirtualInterfaces",
            "Resource": "*"
        }
    ]
}
```

태그를 기반으로 하는 요청에 대한 액세스 제어

IAM 정책의 조건을 사용하여 AWS 리소스에 태그를 지정하는 요청에서 어떤 태그 키 값 페어를 전달할 수 있는지를 제어할 수 있습니다. 다음 예제는 태그에 환경 키와 preprod 또는 production 값이 포함된 경우에만 AWS Direct Connect TagResource 작업을 사용하여 가상 인터페이스에 태그를 첨부하도록 허용하는 정책을 만드는 방법을 보여줍니다. 모범 사례로서 `ForAllValues` 변경자를 `aws:TagKeys` 조건 키와 함께 사용하여 요청에서 키 환경만 허용됨을 표시합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

태그 키 제어

IAM 정책에서 조건을 사용하여 리소스 또는 요청에 특정 태그 키를 사용할 수 있는지 여부를 제어할 수 있습니다.

다음 예에서는 태그 키 환경에서만, 리소스에 태그를 지정할 수 있는 정책을 생성할 수 있는 방법을 보여줍니다.

```
    {
     "Version": "2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "directconnect:TagResource",
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringEquals": {
           "aws:TagKeys": [
             "environment"
           ]
         }
       }
     }
   }
```

AWS Direct Connect에 대한 서비스 연결 역할

AWS Direct Connect는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AWS Direct Connect에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Direct Connect에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 AWS Direct Connect 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS Direct Connect에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS Direct Connect에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 AWS Direct Connect 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할(Service-Linked Role) 열에 예(Yes)가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS Direct Connect에 대한 서비스 연결 역할 권한

AWS Direct Connect 은(는) `AWSServiceRoleForDirectConnect` (이)라는 서비스 연결 역할을 사용합니다. 이렇게 하면 AWS Direct Connect 이(가) 사용자 대신 AWS Secrets Manager 에 저장된 MACsec 암호를 검색할 수 있습니다.

`AWSServiceRoleForDirectConnect` 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `directconnect.amazonaws.com`

`AWSServiceRoleForDirectConnect` 서비스 연결 역할은 관리형 정책 `AWSDirectConnectServiceRolePolicy` 을(를) 사용합니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성해야 합니다. `AWSServiceRoleForDirectConnect` 서비스 연결 역할을 성공적으로 생성하기 위해서는 AWS Direct Connect 와(과) 함께 사용하는 IAM ID에 필수 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 IAM ID에 연결하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Direct Connect에 대한 서비스 연결 역할 생성

서비스 연결 역할을 수동으로 생성할 필요는 없습니다. AWS Direct Connect 이(가) 해당 서비스 연결 역할을 생성해 줍니다. `associate-mac-sec-key` 명령을 실행하면 AWS 은(는) AWS Direct

Connect 이(가) 사용자를 대신하여 AWS Management Console, AWS CLI 또는 AWS API의 AWS Secrets Manager 에 저장돼 있는 MACsec 암호를 검색할 수 있는 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 이 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AWS Direct Connect 이(가) 사용자를 위해 서비스 연결 역할을 다시 생성합니다.

IAM 콘솔을 사용해 AWS Direct Connect 사용 사례로 서비스 연결 역할을 생성할 수도 있습니다. AWS CLI 또는 AWS API에서 `directconnect.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성을 참조하세요. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

AWS Direct Connect에 대한 서비스 연결 역할 편집

AWS Direct Connect에서는 `AWSServiceRoleForDirectConnect` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AWS Direct Connect에 대한 서비스 연결 역할 삭제

`AWSServiceRoleForDirectConnect` 역할은 수동으로 삭제할 필요가 없습니다. 서비스 연결 역할을 삭제할 때에는 AWS Secrets Manager 웹 서비스에 저장된 모든 관련 리소스를 삭제해야 합니다. AWS Management Console, AWS CLI, AWS API 또는 AWS Direct Connect 이(가) 사용자 대신 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔을 사용하여 서비스 연결 역할을 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 AWS Direct Connect 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForDirectConnect`에서 사용하는 AWS Direct Connect 리소스를 삭제하려면

1. 모든 MACsec 키와 연결 간의 연결을 제거합니다. 자세한 정보는 the section called "MACsec 암호 키와 연결 사이의 연결을 제거합니다" 섹션을 참조하세요.
2. 모든 MACsec 키와 LAG 간의 연결을 제거합니다. 자세한 정보는 the section called "MACsec 암호 키와 LAG 간의 연결을 제거합니다" 섹션을 참조하세요.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 `AWSServiceRoleForDirectConnect` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

AWS Direct Connect 서비스 연결 역할이 지원되는 리전

AWS Direct Connect 은(는) MAC 보안 서비스를 사용할 수 있는 모든 AWS 리전 에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Direct Connect 위치를 참조하십시오.

AWS Direct Connect의 AWS 관리형 정책

AWS 관리형 정책은 AWS에서 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

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

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS관리형 정책: AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 AWS Direct Connect에 대한 전체 액세스를 허용하는 권한을 부여합니다.

이 정책의 권한을 보려면 AWS Management Console에서 AWSDirectConnectFullAccess를 참조하세요.

AWS관리형 정책: AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 AWS Direct Connect에 대한 읽기 전용 액세스를 허용하는 권한을 부여합니다.

이 정책의 권한을 보려면 AWS Management Console에서 AWSDirectConnectReadOnlyAccess를 참조하세요.

AWS관리형 정책: AWSDirectConnectServiceRolePolicy

이 정책은 사용자 대신 MAC 보안 암호를 검색할 수 AWSServiceRoleForDirectConnectAWS Direct Connect있도록 이름이 지정된 서비스 연결 역할에 연결됩니다. 자세히 알아보려면 the section called "서비스 연결 역할"의 내용을 참조하세요.

이 정책의 권한을 보려면 AWS Management Console에서 AWSDirectConnectServiceRolePolicy를 참조하세요.

AWS 관리형 정책으로 AWS Direct Connect 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 AWS Direct Connect의 AWS 관리형 정책 업데이트에 관한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Direct Connect 문서 기록 페이지에서 RSS 피드를 구독합니다.

변경 사항	설명	날짜
AWSDirectConnectServiceRolePolicy - 새 정책	MAC 보안을 지원하기 위해 AWSServiceRoleForDirectConnect서비스 연결 역할이 추가되었습니다.	2021년 3월 31일
AWS Direct Connect에서 변경 사항 추적 시작	AWS Direct Connect가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2021년 3월 31일

Direct Connect 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Direct Connect와 IAM에서 작업할 때 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Direct Connect에서 작업을 수행할 권한이 없음
- 저는 iam을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사람이 내 Direct Connect 리소스에 액세스할 수 있게 허용하기를 원합니다

Direct Connect에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojacksonIAM` user(IAM 사용자)가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `directconnect:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

이 경우 `directconnect:`*`GetWidget`* 작업을 사용하여 *`my-example-widget`* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하십시오. 관리자는 로그인 보안 인증을 제공한 사람입니다.

저는 iam을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Direct Connect에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 해당 서비스에 기존 역할을 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`(이)라는 IAM 사용자가 콘솔을 사용하여 Direct Connect에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의합니다. 관리자는 로그인 보안 인증을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Direct Connect 리소스에 액세스할 수 있게 허용하기를 원합니다

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Direct Connect에서 이러한 기능을 지원하는지 여부를 알아보려면 Direct Connect 에서 IAM을 사용하는 방식 섹션을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 타사 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 소유한 AWS 계정에 대한 액세스 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

AWS Direct Connect의 로깅 및 모니터링

다음과 같은 자동 모니터링 도구를 사용하여 AWS Direct Connect를 관찰하고 문제 발생 시 보고할 수 있습니다.

- Amazon CloudWatch 경보를 사용하면 지정한 기간에 단일 지표를 감시합니다. 기간 수에 대해 주어진 임계값과 지표 값을 비교하여 하나 이상의 작업을 수행합니다. 이 작업은 Amazon SNS 주제로 전송되는 알림입니다. CloudWatch 경보는 특정 상태에 있다는 이유만으로는 작업을 호출하지 않습니

다. 상태가 변경되고 지정한 기간 동안 유지되어야 합니다. 자세한 내용은 아마존을 통한 모니터링 CloudWatch 섹션을 참조하세요.

- AWS CloudTrail 로그 모니터링 – 계정 간에 로그 파일을 공유하고, CloudTrail 로그 파일을 CloudWatch Log로 전송하여 실시간으로 모니터링합니다. 로그 처리 애플리케이션을 Java로 작성하고, CloudTrail이 로그 파일을 전송한 후 변경되지 않았는지 확인할 수도 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS CloudTrail을 사용하여 AWS Direct Connect API 호출 로깅 및 CloudTrail 로그 파일 작업도 참조하십시오.

자세한 내용은 모니터링 섹션을 참조하세요.

AWS Direct Connect의 규정 준수 확인

AWS 서비스이(가) 특정 규정 준수 프로그램의 범위에 포함되는지 알아보려면 규정 준수 프로그램 제공 범위 내 AWS 서비스을(를) 참조하고 관심 있는 규정 준수 프로그램을 선택하십시오. 일반적인 정보는 AWS규정 준수 프로그램을 참조하세요.

AWS Artifact을(를) 사용하여 제3자 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드 섹션을 참조하세요.

AWS 서비스 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다.AWS에서는 규정 준수를 지원할 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS환경을 배포하기 위한 단계를 제공합니다.
- Architecting for HIPAA Security and Compliance on Amazon Web Services(Amazon Web Services에서 HIPAA 보안 및 규정 준수 기술 백서 설계) - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 만드는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스에 HIPAA 자격이 있는 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조 섹션을 참조하십시오.

- AWS 규정 준수 리소스 - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 컬렉션입니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에서는 AWS 서비스를 보호하기 위한 모범 사례를 요약하고 여러 프레임워크(미국 표준 기술 연구소(NIST),

결제 카드 산업 보안 표준 위원회(PCI), 국제 표준화기구(ISO) 등)에서 보안 제어에 대한 지침을 매핑합니다.

- AWS Config 개발자 가이드의 규칙을 사용하여 리소스 평가 – AWS Config 서비스는 내부 사례, 산업 지침 및 규제에 대한 리소스 구성의 준수 상태를 평가합니다.
- AWS Security Hub – 이 AWS 서비스는 AWS내의 보안 상태에 대한 포괄적인 보기를 제공합니다. Security Hub는 보안 제어를 사용하여 AWS리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조 섹션을 참조하십시오.
- AWS Audit Manager - 이 AWS 서비스는 AWS 사용을 지속적으로 감사하여 리스크를 관리하고 규정 및 업계 표준을 준수하는 방법을 간소화할 수 있도록 지원합니다.

AWS Direct Connect의 복원성

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

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

AWS 글로벌 인프라 뿐만 아니라 AWS Direct Connect도 데이터 복원력과 백업 요구 사항을 지원하는 다양한 기능을 제공합니다.

AWS Direct Connect에서 VPN을 사용하는 방법에 대한 자세한 내용은 AWS Direct Connect Plus VPN을 참조하십시오.

장애 조치

AWS Direct Connect 복원력 툴킷은 SLA 목표를 달성하기 위한 전용 연결을 주문하는 데 도움이 되는 여러 복원 모델이 포함된 Connection Wizard를 제공합니다. 복원 모델을 선택하면 AWS Direct Connect 복원력 툴킷이 전용 연결 주문 과정을 안내합니다. 복원 모델은 여러 위치에 적절한 수의 전용 연결을 갖도록 설계되었습니다.

- 최대 복원력: 둘 이상 위치의 개별 디바이스에서 종료하는 별도의 연결을 사용하여 중요 워크로드에 대해 최대 복원력을 확보할 수 있습니다. 이 모델은 디바이스, 연결, 전체 위치 오류에 대한 복원성을 제공합니다.

- 높은 복원력: 여러 위치에 두 개의 단일 연결을 사용하여 중요 워크로드에 대한 높은 복원력을 확보할 수 있습니다. 이 모델은 광섬유 절단 또는 디바이스 오류로 인해 발생하는 연결 오류에 대한 복원성을 제공합니다. 또한 전체 위치 오류를 방지하는 데에도 도움이 됩니다.
- 개발 및 테스트: 한 위치의 개별 디바이스에서 종료하는 별도의 연결을 사용하여 중요하지 않은 워크로드에 대한 개발 및 테스트 복원력을 확보할 수 있습니다. 이 모델은 디바이스 오류에 대한 복원성은 제공하지만 위치 오류에 대한 복원성은 제공하지 않습니다.

자세한 내용은 AWS Direct Connect 복원력 툴킷을 사용하여 시작하기 섹션을 참조하세요.

AWS Direct Connect의 인프라 보안

관리형 서비스인 AWS Direct Connect은(는) AWS 글로벌 네트워크 보안 절차로 보호됩니다. AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 AWS Direct Connect에 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.2 이상을 지원해야 합니다. TLS 1.3을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

이러한 API 작업은 모든 네트워크 위치에서 호출할 수 있지만, AWS Direct Connect는 원본 IP 주소를 기반으로 하는 제한을 포함할 수 있는 리소스 기반 액세스 정책을 지원합니다. AWS Direct Connect 정책을 사용하여 특정 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트 또는 특정 VPC에서 액세스를 제어할 수도 있습니다. 그러면 AWS 네트워크의 특정 VPC에서만 특정 AWS Direct Connect 리소스에 대한 네트워크 액세스가 효과적으로 격리됩니다. 예제는 the section called “자격 증명 기반 정책 예시”을(를) 참조하십시오.

Border Gateway Protocol(BGP) 보안

인터넷은 네트워크 시스템 간에 정보를 라우팅하기 위해 대부분 BGP에 의존합니다. BGP 라우팅은 때때로 악의적인 공격이나 BGP 하이재킹에 취약할 수도 있습니다. AWS이(가) BGP 하이재킹으로부터 네트워크를 더 안전하게 보호하는 방법을 알아보려면 AWS이(가) 인터넷 라우팅 보안을 지원하는 방법을 참조하십시오.

AWS CLI 사용

AWS CLI를 사용하여 AWS Direct Connect 리소스를 생성하고 사용할 수 있습니다.

다음 예제에서는 AWS CLI 명령을 사용하여 AWS Direct Connect 연결을 생성합니다. LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 다운로드하거나, 프라이빗 또는 퍼블릭 가상 인터페이스를 프로비저닝할 수도 있습니다.

시작하기 전에 AWS CLI를 설치하고 구성해야 합니다. 자세한 정보는 AWS Command Line Interface 사용 설명서를 참조하세요.

목차

- 1단계: 연결 생성
- 2단계: LOA-CFA 다운로드
- 3단계: 가상 인터페이스 생성 및 라우터 구성 가져오기

1단계: 연결 생성

첫 번째 단계는 연결 요청 제출입니다. 필요한 포트 속도와 AWS Direct Connect 위치를 알고 있어야 합니다. 자세한 내용은 AWS Direct Connect 연결 섹션을 참조하세요.

연결 요청을 생성하려면

1. 현재 리전에 대한 AWS Direct Connect 위치를 설명합니다. 반환된 출력에서 연결을 설정하고자 하는 위치에 대한 위치 코드를 적어둡니다.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
```

```
    ]
}
```

2. 연결을 생성하고 이름, 포트 속도 및 위치 코드를 지정합니다. 반환된 출력에서 연결된 ID를 적어 둡니다. 다음 단계에서 LOA-CFA를 얻으려면 이 ID가 필요합니다.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

2단계: LOA-CFA 다운로드

연결을 요청한 후에는 `describe-loa` 명령을 사용하여 LOA-CFA를 가져올 수 있습니다. 출력은 base64 인코딩됩니다. 관련 LOA 내용을 추출하고 디코딩하여 PDF 파일을 생성해야 합니다.

Linux 또는 mac OS를 사용하여 LOA-CFA를 가져오려면

이 예제에서는 명령의 마지막 부분이 base64 유틸리티를 사용하여 내용을 디코딩하고 출력을 PDF 파일로 내보냅니다.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Windows를 사용하여 LOA-CFA를 가져오는 방법

이 예제에서는 출력이 myLoaCfa.base64라고 하는 파일로 추출됩니다. 두 번째 명령은 `certutil` 유틸리티를 사용하여 파일을 디코딩하고 출력을 PDF 파일로 내보냅니다.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

LOA-CFA를 다운로드한 후에는 네트워크 공급자 또는 코로케이션 공급자에게 보냅니다.

3단계: 가상 인터페이스 생성 및 라우터 구성 가져오기

AWS Direct Connect 연결을 주문한 다음 이 연결을 사용하려면 가상 인터페이스를 생성해야 합니다. 가상 프라이빗 인터페이스를 생성하여 VPC에 연결할 수 있습니다. 또는 퍼블릭 가상 인터페이스를 생성하여 VPC에 없는 AWS 서비스에 연결해도 됩니다. IPv4 또는 IPv6 트래픽을 지원하는 가상 인터페이스를 만들 수 있습니다.

시작하기 전에 먼저 필수 가상 인터페이스 필수 조건 단원의 필수 조건을 읽으십시오.

AWS CLI를 사용하여 가상 인터페이스를 만드는 경우 출력에 일반 라우터 구성 정보가 포함됩니다. 디바이스에 대한 전용 라우터 구성을 생성하려면 AWS Direct Connect 콘솔을 사용하십시오. 자세한 내용은 라우터 구성 파일 다운로드 섹션을 참조하세요.

가상 프라이빗 인터페이스를 생성하려면

1. VPC에 연결된 가상 프라이빗 게이트웨이의 ID(vgw-xxxxxxxx)를 얻습니다. 다음 단계에서 가상 인터페이스를 생성하려면 이 ID가 필요합니다.

```
aws ec2 describe-vpn-gateways
```

```
{
    "VpnGateways": [
        {
            "State": "available",
            "Tags": [
                {
                    "Value": "DX_VGW",
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
```

```
                }
            ]
        }
    ]
}
```

2. 가상 프라이빗 인터페이스를 생성합니다. 이름, VLAN ID 및 BGP 자율 시스템 번호(ASN)를 지정해야 합니다.

   IPv4 트래픽의 경우 BGP 피어링 세션의 각 끝에서 프라이빗 IPv4 주소가 필요합니다. 자체 IPv4 주소를 지정하거나 Amazon이 대신 주소를 생성하도록 할 수 있습니다. 다음 예제에서는 IPv4 주소가 생성됩니다.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
```

```
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

IPv6 트래픽을 지원하는 가상 프라이빗 인터페이스를 생성하려면 위와 동일한 명령을 사용해서 `addressFamily` 파라미터에 대한 `ipv6`을 지정합니다. 사용자는 BGP 피어링 세션에 자체 IPv6 주소를 지정할 수 없으며, Amazon이 사용자에게 IPv6 주소를 할당합니다.

3. XML 형식으로 라우터 구성 정보를 보려면 생성한 가상 인터페이스를 설명합니다. `--query` 파라미터를 사용하여 `customerRouterConfig` 정보를 추출하고 `--output` 파라미터를 사용해서 탭으로 구분된 줄로 텍스트를 구성합니다.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

가상 프라이빗 인터페이스를 생성하려면

1. 가상 프라이빗 인터페이스를 생성하려면 이름, VLAN ID 및 BGP 자율 시스템 번호(ASN)를 지정해야 합니다.

또한, IPv4 트래픽의 경우 BGP 피어링 세션의 각 엔드에 대한 퍼블릭 IPv4 주소를 지정하고, BGP를 통해 보급할 퍼블릭 IPv4 경로를 지정해야 합니다. 아래 예제에서는 IPv4 트래픽을 위한 가상 퍼블릭 인터페이스를 생성합니다.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
```

```
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

IPv6 트래픽을 지원하는 가상 퍼블릭 인터페이스를 생성하려면 BGP를 통해 보급할 IPv6 라우터를 지정할 수 있습니다. 사용자는 피어링 세션에 대해 IPv6 주소를 지정할 수 없으며, Amazon이 사용자에게 IPv6 주소를 할당합니다. 아래 예제에서는 IPv6 트래픽을 위한 가상 퍼블릭 인터페이스를 생성합니다.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. XML 형식으로 라우터 구성 정보를 보려면 생성한 가상 인터페이스를 설명합니다. `--query` 파라미터를 사용하여 `customerRouterConfig` 정보를 추출하고 `--output` 파라미터를 사용해서 탭으로 구분된 줄로 텍스트를 구성합니다.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

AWS CloudTrail을 사용하여 AWS Direct Connect API 호출 로깅

AWS Direct Connect는 AWS Direct Connect에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail은 AWS Direct Connect에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Direct Connect 콘솔로부터의 호출과 AWS Direct Connect API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 AWS Direct Connect 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 Event history(이벤트 기록)에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AWS Direct Connect에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

자세한 정보는 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 AWS Direct Connect 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. AWS Direct Connect에서 활동이 발생하면 해당 활동이 [이벤트 기록(Event history)]의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Direct Connect에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

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

모든 AWS Direct Connect 작업은 CloudTrail에서 로깅되고 AWS Direct Connect API 참조에 기록됩니다. 예를 들어 `CreateConnection` 및 `CreatePrivateVirtualInterface` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management (IAM 사용자) 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail `userIdentity` 요소를 참조하십시오.

AWS Direct Connect 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 AWS Direct Connect 에 대한 CloudTrail 로그 레코드의 예입니다.

Example 예: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
```

```
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example 예: CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
```

```
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example 예: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example 예: DescribeVirtualInterfaces

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
```

```
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

모니터링 AWS Direct Connect 리소스

모니터링은 Direct Connect 리소스의 안정성, 가용성 및 성능을 유지 관리하는 데 있어 중요한 부분입니다. 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. 그러나 Direct Connect 모니터링을 시작하기 전에 다음 질문에 대한 답변이 포함된 모니터링 계획을 세워야 합니다.

- 모니터링의 목표
- 어떤 리소스를 모니터링해야 합니까?
- 이러한 리소스를 얼마나 자주 모니터링해야 합니까?
- 사용할 수 있는 모니터링 도구는 무엇입니까?
- 누가 모니터링 작업을 수행합니까?
- 문제 발생 시 알려야 할 대상

다음 단계는 다양한 시간과 다양한 부하 조건에서 성능을 측정하여 사용자 환경의 정상적인 Direct Connect 성능에 대한 기준을 설정하는 것입니다. Direct Connect를 모니터링할 때는 과거 모니터링 데이터를 저장하십시오. 이렇게 하면 현재 성능 데이터와 비교하고, 일반적인 성능 패턴과 성능 이상을 식별하고, 문제를 해결할 방법을 강구할 수 있습니다.

기준을 설정하려면 물리적 Direct Connect 연결의 사용, 상태 및 상태를 모니터링해야 합니다.

내용

- 모니터링 도구
- 아마존을 통한 모니터링 CloudWatch

모니터링 도구

AWS AWS Direct Connect 연결을 모니터링하는 데 사용할 수 있는 다양한 도구를 제공합니다. 이들 도구 중에는 모니터링을 자동으로 수행하도록 구성할 수 있는 도구도 있지만, 수동 작업이 필요한 도구도 있습니다. 모니터링 작업은 최대한 자동화하는 것이 좋습니다.

자동 모니터링 도구

다음과 같은 자동 모니터링 도구를 사용하여 Direct Connect를 관찰하고 문제 발생 시 보고할 수 있습니다.

- Amazon CloudWatch Alarms — 지정한 기간 동안 단일 지표를 관찰합니다. 기간 수에 대해 주어진 임계값과 지표 값을 비교하여 하나 이상의 작업을 수행합니다. 작업은 Amazon SNS 주제에 전송되는 알림입니다. CloudWatch 경보가 특정 상태에 있다는 이유만으로 경보가 작업을 호출하는 것은 아닙니다. 상태가 변경되고 지정된 기간 동안 유지되어야 합니다. 사용 가능 지표 및 차원은 아마존을 통한 모니터링 CloudWatch을(를) 참조하세요.
- AWS CloudTrail 로그 모니터링 - 계정 간에 로그 파일을 공유하고 CloudTrail 로그 파일을 Logs로 전송하여 CloudWatch 실시간으로 모니터링합니다. 로그 처리 애플리케이션을 Java로 작성하고, CloudTrail이 로그 파일을 전송한 후 변경되지 않았는지 확인할 수도 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 로그 파일 작업을 참조하십시오 AWS CloudTrail을 사용하여 AWS Direct Connect API 호출 로깅.

수동 모니터링 도구

AWS Direct Connect 연결 모니터링의 또 다른 중요한 부분은 CloudWatch 경보에서 다루지 않는 항목을 수동으로 모니터링하는 것입니다. Direct Connect 및 CloudWatch 콘솔 대시보드를 통해 AWS 환경 상태를 at-a-glance 볼 수 있습니다.

- AWS Direct Connect 콘솔에는 다음이 표시됩니다.
  - 연결 상태(State 열 참조)
  - 가상 인터페이스 상태(State 열 참조)
- CloudWatch 홈 페이지에는 다음이 표시됩니다.
  - 현재 경보 및 상태
  - 경보 및 리소스 그래프
  - 서비스 상태

  또한 다음을 CloudWatch 사용하여 수행할 수 있습니다.

  - 사용자 지정 대시보드를 만들어 원하는 서비스 모니터링.
  - 지표 데이터를 그래프로 작성하여 문제를 해결하고 추세 파악.
  - 모든 AWS 리소스 메트릭을 검색하고 찾아보십시오.
  - 문제에 대해 알려주는 경보 생성 및 편집

아마존을 통한 모니터링 CloudWatch

를 사용하여 물리적 AWS Direct Connect 연결 및 가상 인터페이스를 모니터링할 수 CloudWatch 있습니다. CloudWatch Direct Connect에서 원시 데이터를 수집하여 읽을 수 있는 지표로 처리합니다. 기본적으로 5분 간격으로 Direct Connect 메트릭 데이터를 CloudWatch 제공합니다.

에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오. CloudWatch 서비스를 모니터링하여 어떤 서비스가 CloudWatch 리소스를 사용하고 있는지 확인할 수도 있습니다. 자세한 내용은 CloudWatch 메트릭을 게시하는 AWS 서비스를 참조하십시오.

내용

- AWS Direct Connect 지표 및 측정기준
- AWS Direct Connect CloudWatch 메트릭 보기
- 연결을 AWS Direct Connect 모니터링하기 위한 CloudWatch 경보 생성

AWS Direct Connect 지표 및 측정기준

지표는 AWS Direct Connect 물리적 연결 및 가상 인터페이스에 사용할 수 있습니다.

AWS Direct Connect 연결 지표

Direct Connect 전용 연결에서 사용할 수 있는 지표는 다음과 같습니다.

지표	설명
`ConnectionState`	connection.1의 상태는 가동을 나타내고 0은 중단을 나타냅니다. 이 지표는 전용 연결과 호스팅 연결에 사용할 수 있습니다. **Note** 이 지표는 연결 소유자 계정 외에 호스팅된 가상 인터페이스 소유자 계정에서도 사용할 수 있습니다.

지표	설명
	단위: 부울
ConnectionBpsEgress	연결 AWS 측의 아웃바운드 데이터에 대한 비트 전송률입니다. 보고되는 숫자는 일정 시간(기본 5분, 최소 1분) 동안 집계된(평균) 수치입니다. 기본 집계를 변경할 수 있습니다. 이 지표는 새 연결에 대해 또는 디바이스가 재부팅될 때 사용하지 못할 수도 있습니다. 연결을 사용하여 트래픽을 보내거나 받을 때 지표가 시작됩니다. 단위: 비트/초
ConnectionBpsIngress	연결 AWS 측으로 전송되는 인바운드 데이터의 비트 전송률입니다. 이 지표는 새 연결에 대해 또는 디바이스가 재부팅될 때 사용하지 못할 수도 있습니다. 연결을 사용하여 트래픽을 보내거나 받을 때 지표가 시작됩니다. 단위: 비트/초
ConnectionPpsEgress	연결 AWS 측의 아웃바운드 데이터에 대한 패킷 속도입니다. 보고되는 숫자는 일정 시간(기본 5분, 최소 1분) 동안 집계된(평균) 수치입니다. 기본 집계를 변경할 수 있습니다. 이 지표는 새 연결에 대해 또는 디바이스가 재부팅될 때 사용하지 못할 수도 있습니다. 연결을 사용하여 트래픽을 보내거나 받을 때 지표가 시작됩니다. 단위: 패킷/초

지표	설명
`ConnectionPpsIngress`	연결 AWS 측으로 전달되는 인바운드 데이터의 패킷 속도입니다. 보고되는 숫자는 일정 시간(기본 5분, 최소 1분) 동안 집계된(평균) 수치입니다. 기본 집계를 변경할 수 있습니다. 이 지표는 새 연결에 대해 또는 디바이스가 재부팅될 때 사용하지 못할 수도 있습니다. 연결을 사용하여 트래픽을 보내거나 받을 때 지표가 시작됩니다. 단위: 패킷/초
`ConnectionCRCErrorCount`	이 개수는 더 이상 사용되지 않습니다. 대신 `ConnectionErrorCount` 을 사용하세요.

지표	설명
`ConnectionErrorCount`	AWS 디바이스의 모든 MAC 레벨 오류 유형에 대한 총 오류 수입니다. 합계에는 순환 중복 검사(CRC) 오류가 포함됩니다. 이 지표는 마지막으로 보고된 데이터포인트 이후 발생한 오류 수입니다. 인터페이스에 오류가 있는 경우 지표는 0이 아닌 값을 보고합니다. 선택한 간격 (예: 5분) 동안 발생한 모든 오류의 총 개수를 구하려면 "합계" 통계를 적용합니다. CloudWatch 합계 통계를 가져오는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 지표에 대한 통계 가져오기를 참조하십시오. 인터페이스의 오류가 중지되면 측정치 값이 0으로 설정됩니다. **Note** 이 지표는 더 이상 사용되지 않는 `ConnectionCRCErrorCount` 를 대체합니다. 단위: 개
`ConnectionLightLevelTx`	연결 AWS 측의 아웃바운드 (이그레스) 트래픽에 대한 파이버 연결 상태를 나타냅니다. 이 지표에 대한 차원은 두 가지입니다. 자세한 설명은 the section called "AWS Direct Connect 사용 가능한 크기" 섹션을 참조하세요. 단위: dBm

지표	설명
`ConnectionLightLevelRx`	연결 AWS 측으로 향하는 인바운드 (인그레스) 트래픽의 광섬유 연결 상태를 나타냅니다. 이 지표에 대한 차원은 두 가지입니다. 자세한 설명은 the section called “AWS Direct Connect 사용 가능한 크기” 섹션을 참조하세요. 단위: dBm
`ConnectionEncryptionState`	연결 암호화 상태를 나타냅니다. 1은 연결 암호화가 up임을 를 나타내고 0은 연결 암호화가 down임을 나타냅니다. 이 메트릭을 LAG에 적용할 경우 1은 LAG의 모든 연결에 암호화 up이(가) 있음을 나타냅니다. 0은 LAG 연결 중 하나 이상이 down임을 나타냅니다.

AWS Direct Connect 가상 인터페이스 메트릭

AWS Direct Connect 가상 인터페이스에서 사용할 수 있는 지표는 다음과 같습니다.

지표	설명
`VirtualInterfaceBpsEgress`	가상 인터페이스 AWS 측면의 아웃바운드 데이터 비트 전송률입니다. 보고되는 숫자는 일정 시간(기본 5분) 동안 집계된(평균) 수치입니다. 단위: 비트/초
`VirtualInterfaceBpsIngress`	가상 인터페이스 AWS 측으로 전송되는 인바운드 데이터의 비트 전송률입니다. 보고되는 숫자는 일정 시간(기본 5분) 동안 집계된(평균) 수치입니다. 단위: 비트/초

지표	설명
`VirtualInterfacePpsEgress`	가상 인터페이스 AWS 측의 아웃바운드 데이터에 대한 패킷 속도입니다. 보고되는 숫자는 일정 시간(기본 5분) 동안 집계된(평균) 수치입니다. 단위: 패킷/초
`VirtualInterfacePpsIngress`	가상 인터페이스 AWS 측으로 전달되는 인바운드 데이터의 패킷 속도입니다. 보고되는 숫자는 일정 시간(기본 5분) 동안 집계된(평균) 수치입니다. 단위: 패킷/초

AWS Direct Connect 사용 가능한 크기

다음 측정기준을 사용하여 AWS Direct Connect 데이터를 필터링할 수 있습니다.

측정기준	설명
`ConnectionId`	이 차원은 Direct Connect 연결 및 가상 인터페이스에 대한 지표에서 사용할 수 있습니다. 이 차원은 연결을 기준으로 데이터를 필터링합니다.
`OpticalLaneNumber`	이 차원은 `ConnectionLightLevelTx` 데이터와 데이터를 필터링하고 Direct Connect 연결의 광학 레인 번호를 기준으로 데이터를 필터링합니다. `ConnectionLightLevelRx`
`VirtualInterfaceId`	이 차원은 Direct Connect 가상 인터페이스의 지표에서 사용할 수 있으며 가상 인터페이스별로 데이터를 필터링합니다.

AWS Direct Connect CloudWatch 메트릭 보기

AWS Direct Connect Direct Connect 연결에 대한 다음 메트릭을 전송합니다. CloudWatch그런 다음 Amazon은 이러한 데이터 포인트를 1분 또는 5분 간격으로 집계합니다. 기본적으로 Direct Connect 지표 데이터는 5분 CloudWatch 간격으로 기록됩니다.

> **Note**
>
> 1분 간격을 설정하면 Direct Connect에서 이 간격을 CloudWatch 사용하여 메트릭을 작성하기 위해 최선을 다하지만 항상 보장할 수는 없습니다.

다음 절차를 사용하여 Direct Connect 연결에 대한 메트릭을 볼 수 있습니다.

CloudWatch 콘솔을 사용하여 지표를 보려면

지표는 먼저 서비스 네임스페이스별로 그룹화된 다음 각 네임스페이스 내에서 다양한 차원 조합별로 그룹화됩니다. 수학 함수 또는 사전 빌드된 쿼리 추가를 포함하여 Direct Connect 지표를 보는 Amazon CloudWatch 데 사용하는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 지표 사용을 참조하십시오.

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표를 선택한 다음 모든 지표를 선택합니다.
3. 지표 섹션에서 DX를 선택합니다.
4. ConnectionId또는 지표 이름을 선택한 후 다음 중 하나를 선택하여 지표를 추가로 정의하십시오.
   - 검색에 추가 - 이 지표를 검색 결과에 추가합니다.
   - 이 지표만 검색 - 이 지표만 검색합니다.
   - 그래프에서 제거 - 그래프에서 이 지표를 제거합니다.
   - 이 지표만 그래프로 작성 — 이 지표만 그래프로 표시합니다.
   - 모든 검색 결과를 그래프로 표시 - 모든 지표를 그래프로 표시합니다.
   - SQL 쿼리를 사용한 그래프 — SQL 쿼리를 생성하여 그래프로 표시할 항목을 선택할 수 있는 Metric Insights -쿼리 빌더를 엽니다. 메트릭 인사이트 사용에 대한 자세한 내용은 Amazon 사용 CloudWatch 설명서의 CloudWatch 메트릭 인사이트를 사용하여 메트릭 쿼리를 참조하십시오.

AWS Direct Connect 콘솔을 사용하여 지표를 보려면

1. https://console.aws.amazon.com/directconnect/v2/home 에서 AWS Direct Connect콘솔을 엽니다.
2. 탐색 창에서 연결을 선택합니다.
3. 연결을 선택합니다.
4. 모니터링 탭을 선택하면 연결에 대한 지표가 표시됩니다.

를 사용하여 지표를 보려면 AWS CLI

명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

연결을 AWS Direct Connect 모니터링하기 위한 CloudWatch 경보 생성

CloudWatch 경보 상태가 변경될 때 Amazon SNS 메시지를 보내는 경보를 생성할 수 있습니다. 경보는 지정한 기간 동안 단일 지표를 감시합니다. 경보는 기간 수에 대한 주어진 임계값과 지표 값을 비교하여 Amazon SNS 주제에 알림을 보냅니다.

예를 들어 AWS Direct Connect 연결 상태를 모니터링하는 경보를 만들 수 있습니다. 이 경보는 연결 상태가 5번 연속 1분간 중단일 경우 알림을 보냅니다. 경보를 생성하기 위해 알아야 할 사항과 경보 생성에 대한 자세한 내용은 Amazon 사용 설명서의 Amazon CloudWatch Alarms 사용을 참조하십시오. CloudWatch

CloudWatch 알람을 만들려면.

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 경보(Alarms)를 선택한 다음 모든 경보(All alarms)를 선택합니다.
3. 경보 생성을 선택합니다.
4. 지표 선택을 선택하고 DX를 선택합니다.
5. 연결 지표 지표를 선택합니다.
6. AWS Direct Connect 연결을 선택한 다음 지표 선택을 선택합니다.
7. 지표 및 조건 지정 페이지에서 경보에 대한 매개 변수를 구성합니다. 지표 및 조건을 지정하는 자세한 내용은 Amazon 사용 설명서의 Amazon CloudWatch Alarms 사용을 참조하십시오. CloudWatch

8. 다음을 선택합니다.
9. 조치 구성 페이지에서 경보 동작을 구성합니다. 경보 작업을 구성하는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 작업을 참조하십시오.
10. 다음을 선택합니다.
11. 이름 및 설명 추가 페이지에서 이름과 선택 사항인 경보 설명을 입력하여 이 경보를 설명하고 다음을 선택합니다.
12. 미리 보기 및 생성 페이지에서 제안된 경보를 확인하세요.
13. 필요한 경우 편집을 선택하여 정보를 변경한 다음 알람 생성을 선택합니다.

    경보 페이지에는 새 경보에 대한 정보가 포함된 새 행이 표시됩니다. 동작 상태는 동작 활성화됨으로 표시되어 경보가 활성 상태임을 나타냅니다.

AWS Direct Connect 할당량

다음 표에는 관련 할당량이 나열되어 있습니다. AWS Direct Connect

구성 요소	할당량	설명
전용 연결별 AWS Direct Connect 프라이빗 또는 퍼블릭 가상 인터페이스	50	이 한도는 늘릴 수 없습니다.
AWS Direct Connect 전용 연결당 전송 가상 인터페이스	4	이 한도는 늘릴 수 없습니다.
전용 연결별 사설 또는 공용 가상 인터페이스 및 AWS Direct Connect 전용 연결별 AWS Direct Connect 전송 가상 인터페이스	51	Amazon VPC Transit Gateways에 대한 AWS Direct Connect 지원이 시작되었을 때 전용 연결당 프라이빗 또는 퍼블릭 가상 인터페이스 50개 할당량에 전송 가상 인터페이스 1개 할당량이 추가되었습니다. 이제 허용되는 전송 가상 인터페이스 수는 4개이며 전용 연결당 최대 51개의 가상 인터페이스를 기준으로 계산됩니다. 이 한도는 늘릴 수 없습니다.
호스팅된 연결당 AWS Direct Connect 프라이빗, 퍼블릭 또는 트랜짓 가상 인터페이스	1	이 한도는 늘릴 수 없습니다.
계정별 지역별 Direct Connect 위치별 활성 AWS Direct Connect 연결	10	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자(TAM)에게 문의하세요.
링크 집계 그룹(LAG)당 가상 인터페이스 수	51	Amazon VPC Transit Gateway에 대한 AWS Direct Connect 지원이 시작되었을 때 LAG당 프라이빗 또는 퍼블릭 가상 인터페이스 50개 할당량에 전송 가상 인터페이스 1개 할당량이 추가되었습니다. 이제 허용되는 전송 가상 인터페이스 수는 4개이며 LAG당 최대 51개의 가상 인터페이스를

구성 요소	할당량	설명
		기준으로 계산됩니다. 이 한도는 늘릴 수 없습니다.
프라이빗 가상 인터페이스 또는 트랜짓 가상 인터페이스에서 온프레미스로의 BGP (Border Gateway Protocol) 세션당 경로. AWS IPv4와 IPv6에 대해 BGP 세션을 통해 100개가 넘는 경로를 광고할 경우 BGP 세션이 BGP 세션 DOWN 표시와 함께 유휴 상태로 전환됩니다.	IPv4 및 IPv6 각각 100개	이 한도는 늘릴 수 없습니다.
가상 퍼블릭 인터페이스의 경계 경로 프로토콜(BGP) 세션당 라우팅	1,000	이 한도는 늘릴 수 없습니다.
링크 집계 그룹(LAG)당 전용 연결	포트 속도가 100G 미만인 경우 4 포트 속도가 100G인 경우 2	
리전당 링크 집계 그룹(LAG)	10	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자(TAM)에게 문의하세요.
AWS Direct Connect 계정당 게이트웨이	200	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자(TAM)에게 문의하세요.
게이트웨이당 가상 프라이빗 게이트웨이 AWS Direct Connect	20	이 한도는 늘릴 수 없습니다.

구성 요소	할당량	설명
게이트웨이당 트랜짓 게이트웨이 AWS Direct Connect	6	이 한도는 늘릴 수 없습니다.
게이트웨이별 AWS Direct Connect 가상 인터페이스 (프라이빗 또는 트랜짓)	30	이 한도는 늘릴 수 없습니다.
트랜짓 가상 AWS Transit Gateway 인터페이스에서 AWS 온프레미스까지의 접두사 수	IPv4 및 IPv6 합산 총 200개	이 한도는 늘릴 수 없습니다.
가상 프라이빗 게이트웨이당 가상 인터페이스 수	제한 없습니다.	
전송 게이트웨이와 연결된 Direct Connect 게이트웨이 수	20	이 한도는 늘릴 수 없습니다.
SiteLink 접두사 제한	100	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자(TAM)에게 문의하세요.

AWS Direct Connect 단일 모드 파이버를 통해 다음과 같은 포트 속도를 지원합니다. 1Gbps: 1000BASE-LX (1310nm), 10Gbps: 10GBASE-LR (1310nm) 및 100Gbps: 100GBASE-LR4.

BGP 쿼터

다음은 BGP 쿼터입니다. BGP 타이머는 라우터 간에 가장 낮은 값까지 협상합니다. BFD 간격은 가장 느린 디바이스를 기준으로 정의됩니다.

- 기본 보류 타이머: 90초
- 최소 보류 타이머: 3초

  보류 값 0은 지원되지 않습니다.
- 기본 킵얼라이브 타이머: 30초
- 최소 킵얼라이브 타이머: 1초

- 정상 재시작 타이머: 120초

  정상 재시작과 BFD는 동시에 구성하지 않는 것이 좋습니다.
- BFD 활성 감지 최소 간격: 300밀리초
- BFD 최소 승수: 3

로드 밸런싱 고려 사항

여러 퍼블릭 VIF에서 로드 밸런싱을 사용하려면 모든 VIF가 동일한 리전에 있어야 합니다.

문제 해결 AWS Direct Connect

다음 문제해결 정보는 AWS Direct Connect 연결 문제 해결에 도움이 됩니다.

목차

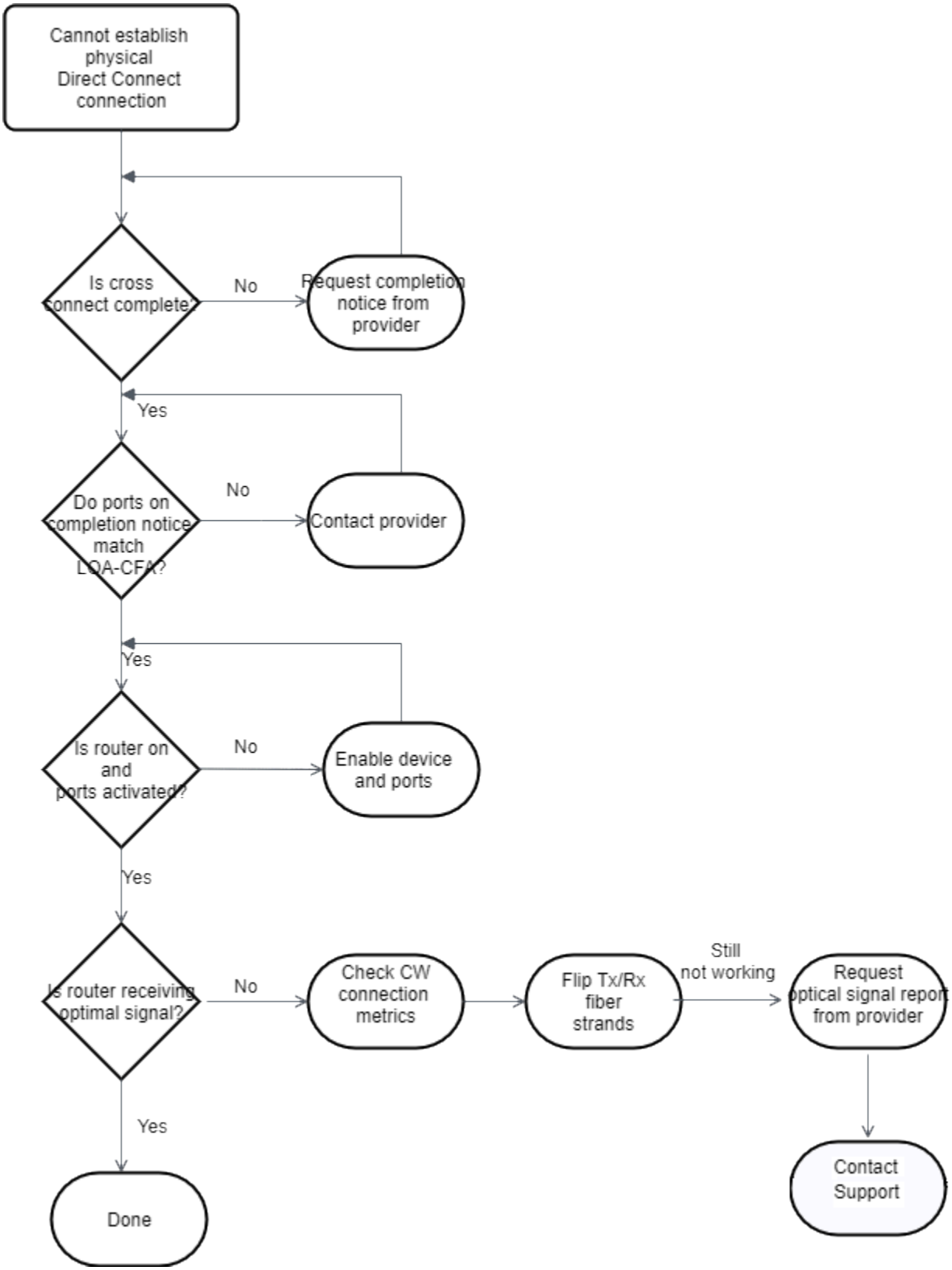
- 계층 1(물리적) 문제 해결
- 계층 2(데이터 링크) 문제 해결
- 계층 3/4(네트워크/전송) 문제 해결
- 라우팅 문제 해결

계층 1(물리적) 문제 해결

사용자 또는 네트워크 공급자가 AWS Direct Connect 장치에 물리적으로 연결하는 데 문제가 있는 경우 다음 단계를 사용하여 문제를 해결하십시오.

1. 코로케이션 공급자에게 교차 연결이 완료되었는지 확인합니다. 코로케이션 공급자 또는 네트워크 공급자에게 교차 연결 완료 알림 제공을 요청하고, 포트를 LOA-CFA에 나열된 것과 비교합니다.
2. 사용자 또는 공급자의 라우터 전원이 켜져 있고 포트가 활성화되어 있는지 확인합니다.
3. 라우터가 올바른 광 트랜시버를 사용하고 있는지 확인하세요. 포트 속도가 1Gbps를 초과하는 연결을 사용하는 경우 포트에 대한 자동 협상을 비활성화해야 합니다. 하지만 연결을 제공하는 AWS Direct Connect 엔드포인트에 따라 1Gbps 연결에 대해 자동 협상을 활성화하거나 비활성화해야 할 수 있습니다. 연결에 대해 자동 협상을 비활성화해야 하는 경우 포트 속도와 전이중 모드를 수동으로 구성해야 합니다. 가상 인터페이스가 계속 다운되는 경우 계층 2(데이터 링크) 문제 해결를 참조하세요.
4. 라우터가 교차 연결을 통해 수신 가능한 광 신호를 수신하고 있는지 확인합니다.
5. Tx/Rx 섬유 스트랜드를 대칭 이동(롤링이라고도 함)해 봅니다.
6. 에 대한 Amazon CloudWatch 지표를 확인하십시오 AWS Direct Connect. AWS Direct Connect 디바이스의 Tx/Rx 광학 판독값 (1Gbps 및 10Gbps 모두), 물리적 오류 수 및 작동 상태를 확인할 수 있습니다. 자세한 내용은 Amazon을 통한 모니터링을 참조하십시오 CloudWatch.
7. 코로케이션 공급자에게 연락하여 교차 연결에서의 Tx/Rx 광 신호에 대한 서면 보고서를 요청합니다.
8. 위의 단계로 물리적 연결 문제가 해결되지 않는 경우, AWS Support에 연락하고 콜로케이션 공급자의 교차 연결 완료 알림 및 광 신호 보고서를 제공합니다.

다음 순서도에는 물리적 연결 문제를 진단하는 단계가 나와 있습니다.

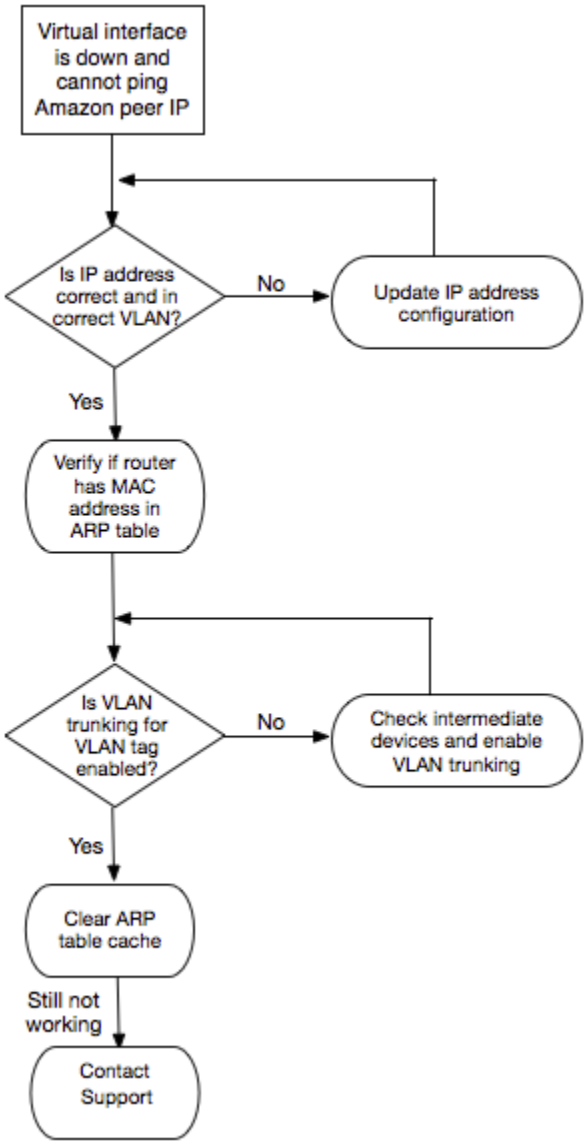


계층 2(데이터 링크) 문제 해결

AWS Direct Connect 물리적 연결은 작동하지만 가상 인터페이스가 다운된 경우 다음 단계를 사용하여 문제를 해결하십시오.

1. Amazon 피어 IP 주소를 ping할 수 없는 경우, 피어 IP 주소가 올바로 구성되어 있고 올바른 VLAN에 있는지 확인합니다. IP 주소가 물리적 인터페이스가 아닌 VLAN 하위 인터페이스에서 구성되었는지 확인합니다 (예: 0/0 대신 GigabitEthernet 0/0.123). GigabitEthernet
2. 라우터에 주소 확인 프로토콜 (ARP) 테이블의 AWS 엔드포인트에서 입력한 MAC 주소가 있는지 확인합니다.
3. 엔드포인트 사이의 모든 중간 디바이스에는 802.1Q VLAN 태그에 대해 활성화된 VLAN 트렁크가 있어야 합니다. 태그가 지정된 트래픽을 AWS 수신하기 전까지는 AWS 측에서 ARP를 설정할 수 없습니다.
4. 사용자 또는 공급자의 ARP 테이블 캐시를 삭제하십시오.
5. 위 단계를 수행해도 ARP가 설정되지 않거나 여전히 Amazon 피어 IP에 ping을 보낼 수 없는 경우 AWS Support에 문의하십시오.

다음 순서도에는 데이터 링크 문제를 진단하는 단계가 나와 있습니다.



이러한 단계를 확인한 후에도 BGP 세션이 설정되지 않으면 계층 3/4(네트워크/전송) 문제 해결 단원을 참조하십시오. BGP 세션이 설정되었지만 라우팅 문제가 있다면 라우팅 문제 해결 단원을 참조하십시오.

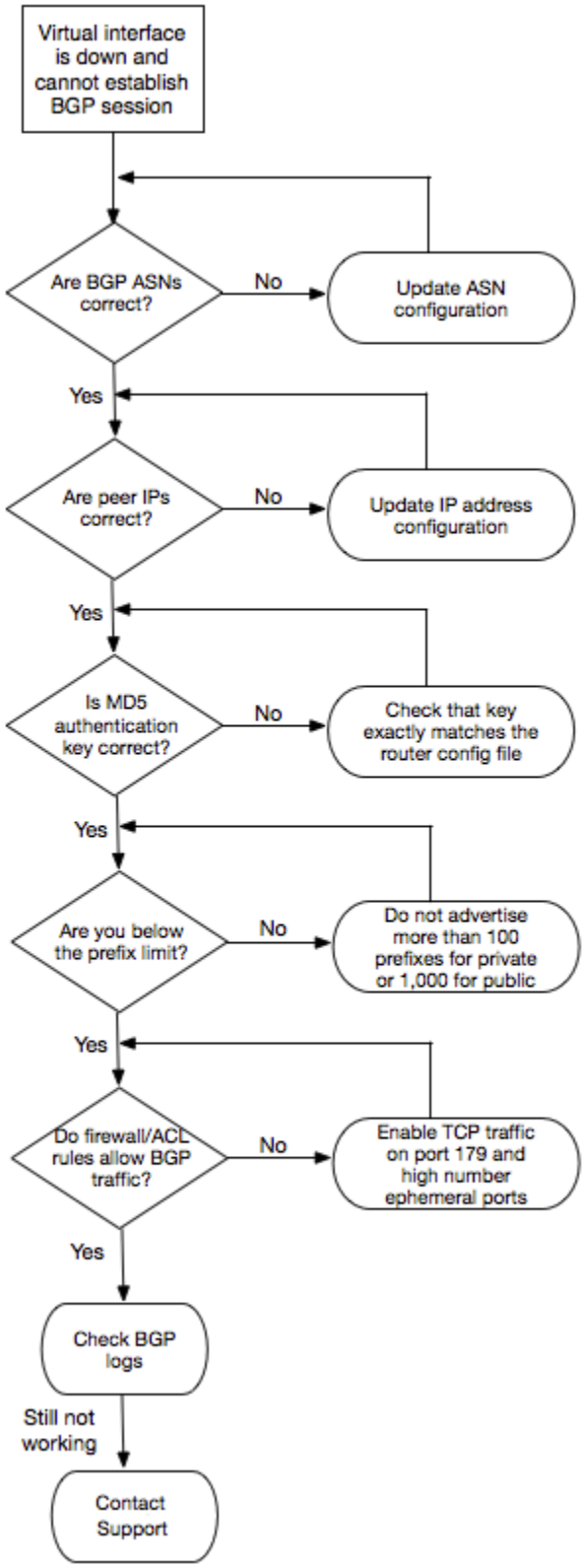
계층 3/4(네트워크/전송) 문제 해결

AWS Direct Connect 물리적 연결이 끊기고 Amazon 피어 IP 주소에 ping을 보낼 수 있는 상황을 생각해 보십시오. 가상 인터페이스가 다운되고 BGP 피어링 세션을 설정할 수 없을 경우 다음 단계를 사용하여 문제를 해결하십시오.

1. BGP 로컬 자율 시스템 번호(ASN)와 Amazon의 ASN이 올바로 구성되어 있는지 확인합니다.
2. BGP 피어링 세션의 양쪽 피어 IP가 올바로 구성되어 있는지 확인합니다.

3. MD5 인증 키가 구성되어 있고 다운로드한 라우터 구성 파일의 키와 정확히 일치하는지 확인합니다. 추가 공백이나 문자가 있는지 확인하십시오.
4. 사용자 또는 공급자가 프라이빗 가상 인터페이스의 경우, 100개 이상, 퍼블릭 가상 인터페이스의 경우, 1,000개 이상의 접두사를 광고하고 있지 않은지 확인합니다. 이 숫자는 하드 제한이며 초과할 수 없습니다.
5. TCP 포트 179 또는 높은 번호의 임시 TCP 포트를 차단하는 방화벽 또는 ACL 규칙이 있는지 확인합니다. 이러한 포트는 BGP가 피어 사이에 TCP 연결을 설정하는 데 필요합니다.
6. BGP 로그에서 오류 또는 경고 메시지가 있는지 확인합니다.
7. 위 단계를 수행해도 BGP 피어링 세션이 설정되지 않으면 Support에 문의하십시오. AWS

다음 순서도에는 BGP 피어링 세션 문제를 진단하는 단계가 나와 있습니다.



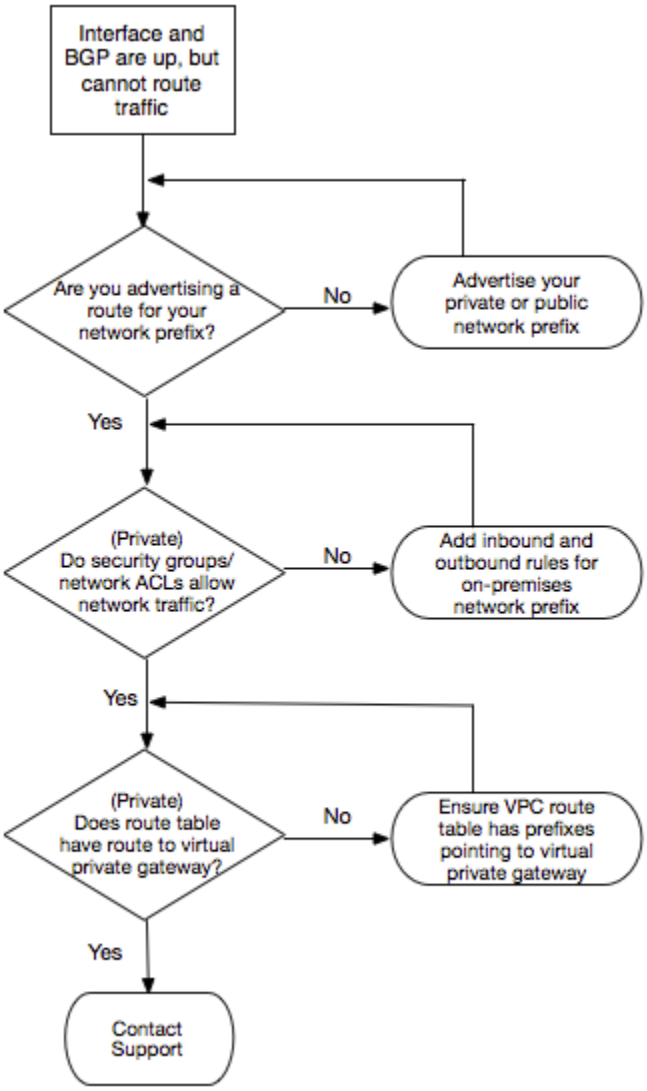
BGP 피어링 세션이 설정되었지만 라우팅 문제가 있다면 라우팅 문제 해결 단원을 참조하십시오.

라우팅 문제 해결

가상 인터페이스가 실행 중이고 BGP 피어링 세션을 설정한 상황을 생각해 보겠습니다. 가상 인터페이스를 통해 트래픽을 라우팅할 수 없을 경우 다음 단계를 통해 문제를 해결하십시오.

1. BGP 세션을 통해 온프레미스 네트워크 접두사의 경로를 광고 중인지 확인합니다. 프라이빗 가상 인터페이스의 경우, 이것은 프라이빗 또는 퍼블릭 네트워크 접두사일 수 있습니다. 퍼블릭 가상 인터페이스의 경우, 이것은 공개적으로 라우팅 가능한 네트워크 접두사여야 합니다.
2. 프라이빗 가상 인터페이스의 경우, VPC 보안 그룹과 네트워크 ACL이 온프레미스 네트워크 접두사에 대한 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹과 네트워크 ACL을 참조합세요.
3. 프라이빗 가상 인터페이스의 경우, VPC 라우팅 테이블에 프라이빗 가상 인터페이스가 연결된 가상 프라이빗 게이트웨이를 가리키는 접두사가 있는지 확인합니다. 예를 들어 기본적으로 모든 트래픽을 온프레미스 네트워크로 라우팅하려는 경우, 가상 프라이빗 게이트웨이와 함께 기본 경로(0.0.0.0/0 또는 ::/0)를 VPC 라우팅 테이블에서 대상으로 추가할 수 있습니다.
   - 또는 경로 전파를 활성화하여 동적 BGP 라우팅 광고에 기반하여 라우팅 테이블에서 자동으로 경로를 업데이트합니다. 라우팅 테이블당 최대 100개의 전파된 경로가 있을 수 있습니다. 이 한도는 늘릴 수 없습니다. 자세한 내용은 Amazon VPC 사용 설명서의 경로 전파 활성화 및 비활성화를 참조하세요.
4. 위 단계를 수행해도 라우팅 문제가 해결되지 않으면 AWS Support에 문의하십시오.

다음 순서도에는 라우팅 문제를 진단하는 단계가 나와 있습니다.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

문서 기록

다음 표에서는 AWS Direct Connect의 릴리스를 설명합니다.

기능	설명	날짜
에 대한 지원 SiteLink	동일한 AWS 지역에 있는 두 Direct Connect 접속 지점 (PoPs) 간에 연결을 가능하게 하는 가상 사설 인터페이스를 만들 수 있습니다. 자세한 내용은 호스팅 가상 인터페이스 섹션을 참조하세요.	2021-12-01
MAC 보안 지원	MACsec을 지원하는 AWS Direct Connect 연결을 사용하여 회사 데이터 센터의 데이터를 AWS Direct Connect 위치로 암호화할 수 있습니다. 자세히 알아보려면 MAC 보안의 내용을 참조하세요.	2021-03-31
100G 지원	100G 전용 연결에 대한 지원 추가를 반영하기 위해 항목이 업데이트되었음.	2021-02-12
이탈리아 내 신규 사무소	이탈리아 신규 위치 추가를 반영하기 위해 주제가 업데이트되었습니다. 자세히 알아보려면 the section called “유럽(밀라노)”의 내용을 참조하세요.	2021-01-22
이스라엘의 새로운 위치	새로운 이스라엘 위치 추가를 반영하기 위해 주제가 업데이트되었습니다. 자세히 알아보려면 the section called “이스라엘(텔아비브)”의 내용을 참조하세요.	2020-07-07
복원력 도구 키트 장애 조치 테스트 지원	복원력 도구 키트 장애 조치 테스트 기능을 사용하여 연결의 복원력을 테스트합니다. 자세히 알아보려면 the section called “AWS Direct Connect 장애 조치 테스트”의 내용을 참조하세요.	2020-06-03
CloudWatch VIF 메트릭 지원	를 사용하여 CloudWatch 물리적 AWS Direct Connect 연결 및 가상 인터페이스를 모니터링할 수 있습니다. 자세히 알아보려면 the section called “아마존을 통한 모니터링 CloudWatch”의 내용을 참조하세요.	2020-05-11

기능	설명	날짜
AWS Direct Connect 복원력 툴킷	AWS Direct Connect 복원력 툴킷은 SLA 목표를 달성하기 위한 전용 연결을 주문하는 데 도움이 되는 여러 복원 모델이 포함된 Connection Wizard를 제공합니다. 자세히 알아보려면 AWS Direct Connect 복원력 툴킷을 사용하여 시작하기의 내용을 참조하세요.	2019-10-07
계정에서 AWS Transit Gateway 지원을 위한 추가 리전 지원	자세한 내용은 the section called “트랜짓 게이트웨이 연결” 섹션을 참조하세요.	2019-09-30
AWS Transit Gateway 에 대한 AWS Direct Connect 지원	AWS Direct Connect 게이트웨이를 사용하여 전송 가상 인터페이스를 통한 AWS Direct Connect 연결을 전송 게이트웨이에 연결된 VPC 또는 VPN에 연결할 수 있습니다. Direct Connect 게이트웨이를 전송 게이트웨이와 연결한 다음 Direct Connect 게이트웨이에 대한 AWS Direct Connect 연결을 위해 전송 가상 인터페이스를 만듭니다. 자세한 내용은 the section called “트랜짓 게이트웨이 연결” 섹션을 참조하세요.	2019년 3월 27일
점보 프레임 지원	AWS Direct Connect를 통해 점보 프레임(9001 MTU)을 전송할 수 있습니다. 자세히 알아보려면 프라이빗 가상 인터페이스 또는 전송 가상 인터페이스에 대한 네트워크 MTU 설정의 내용을 참조하세요.	2018-10-11
로컬 기본 설정 BGP 커뮤니티	로컬 기본 설정 BGP 커뮤니티 태그를 사용하여 수신 트래픽에 대한 로드 밸런싱 및 경로 기본 설정을 네트워크에 적용할 수 있습니다. 자세히 알아보려면 로컬 기본 설정 BGP 커뮤니티의 내용을 참조하세요.	2018-02-06
AWS Direct Connect 게이트웨이	Direct Connect 게이트웨이를 사용하여 AWS Direct Connect 연결을 원격 리전의 VPC에 연결할 수 있습니다. 자세히 알아보려면 Direct Connect 게이트웨이 사용의 내용을 참조하세요.	2017-11-01

기능	설명	날짜
아마존 CloudWatch 메트릭스	AWS Direct Connect연결에 대한 CloudWatch 지표를 볼 수 있습니다. 자세히 알아보려면 아마존을 통한 모니터링 CloudWatch의 내용을 참조하세요.	2017-06-29
링크 집계 그룹	링크 집계 그룹(LAG)을 생성하여 여러 AWS Direct Connect 연결을 집계할 수 있습니다. 자세히 알아보려면 링크 집계 그룹의 내용을 참조하세요.	2017-02-13
IPv6 지원	이제 가상 인터페이스에서 IPv6 BGP 피어링 세션을 지원할 수 있습니다. 자세히 알아보려면 BGP 피어 추가 또는 삭제의 내용을 참조하세요.	2016-12-01
태그 지정 지원	이제 AWS Direct Connect 리소스에 태그를 지정할 수 있습니다. 자세히 알아보려면 AWS Direct Connect 리소스에 태그 지정의 내용을 참조하세요.	2016-11-04
셀프 서비스 LOA-CFA	AWS Direct Connect 콘솔 또는 API를 사용하여 LOA-CFA(Letter of Authorization and Connecting Facility Assignment)를 다운로드할 수 있습니다.	2016-06-22
실리콘밸리의 새로운 위치	미국 서부(노스 캐롤라이나) 리전에서 새로운 실리콘밸리 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2016-06-03
암스테르담의 새로운 위치	유럽(프랑크푸르트) 리전에서 새로운 암스테르담 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2016-05-19
포틀랜드, 오레곤 및 싱가포르의 새로운 위치	미국 서부(오레곤) 및 아시아아 태평양(싱가포르) 리전에서 새로운 오레곤 주 포틀랜드 및 싱가포르 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2016-04-27
브라질 상파울루의 새로운 위치	남미(상파울루) 리전에서 새로운 상파울루 위치 추가를 반영하기 위해 주제가 업데이트되었음.	2015-12-09

기능	설명	날짜
댈러스, 런던, 실리콘밸리 및 뭄바이의 새로운 위치	댈러스 (미국 동부 (버지니아 북부) 지역), 런던 (유럽 (아일랜드) 지역), 실리콘 밸리 ((미국 서부) 지역) 및 뭄바이 (아시아 태평양 AWS GovCloud (싱가포르) 지역) 의 새 위치 추가를 포함하도록 항목이 업데이트되었습니다.	2015-11-27
중국(베이징) 리전의 신규 위치	중국(베이징) 리전에서 새 베이징 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2015-04-14
미국 서부(오레곤) 리전의 새로운 라스베이거스 위치	미국 서부(오레곤) 지역에서 서비스를 제공하는 새로운 AWS Direct Connect 라스베이거스 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2014-11-10
새로운 EU(프랑크푸르트) 리전	EU(프랑크푸르트) 지역에서 서비스를 제공하는 새로운 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2014-10-23
아시아 태평양(시드니) 리전의 새로운 위치	아시아 태평양(시드니) 지역에서 서비스를 제공하는 새로운 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2014-07-14
AWS CloudTrail 지원	활동을 로그인하는 데 사용할 CloudTrail 수 있는 방법을 설명하는 새 항목이 추가되었습니다. AWS Direct Connect 자세히 알아보려면 AWS CloudTrail을 사용하여 AWS Direct Connect API 호출 로깅의 내용을 참조하세요.	2014-04-04
원격 AWS 리전 액세스에 대한 지원	원격 리전에서 퍼블릭 리소스에 액세스하는 방법을 설명하기 위해 새 항목이 추가되었음. 자세히 알아보려면 원격 AWS 리전 액세스의 내용을 참조하세요.	2013-12-19
호스팅 연결에 대한 지원	호스팅 연결에 대한 지원 추가를 반영하기 위해 항목이 업데이트되었음.	2013-10-22

기능	설명	날짜
EU(아일랜드) 리전의 새로운 위치	EU(아일랜드) 지역에서 서비스를 제공하는 새로운 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2013-06-24
미국 서부(오레곤) 리전의 새로운 시애틀 위치	미국 서부(오레곤) 지역에서 서비스를 제공하는 새로운 AWS Direct Connect 시애틀 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2013-05-08
AWS Direct Connect와(과) IAM을 함께 사용하는 것에 대한 지원	AWS Identity and Access Management와 AWS Direct Connect를 함께 사용하는 것에 대한 항목이 추가됨. 자세히 알아보려면 the section called “ID 및 액세스 관리”의 내용을 참조하세요.	2012-12-21
새로운 아시아 태평양(시드니) 리전	아시아 태평양(시드니) 지역에서 서비스를 제공하는 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2012-12-14
새 AWS Direct Connect 콘솔, 미국 동부(버지니아 북부) 및 남아메리카(상파울루) 리전	AWS Direct Connect 시작하기 안내서가 AWS Direct Connect 사용 설명서로 대체되었습니다. 새로운 AWS Direct Connect 콘솔을 포함하는 새 항목, 결제 항목 및 라우터 구성 정보가 추가되었고, 미국 동부(버지니아 북부) 및 남아메리카(상파울루) 리전에서 서비스를 제공하는 두 곳의 새로운 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2012-08-13
EU(아일랜드), 아시아 태평양(싱가포르), 아시아 태평양(도쿄) 지역에 대한 지원	새로운 문제 해결 섹션이 추가되고, 미국 서부(캘리포니아 북부), EU(아일랜드), 아시아 태평양(싱가포르), 아시아 태평양(도쿄) 지역에서 서비스를 제공하는 네 곳의 새로운 AWS Direct Connect 위치 추가를 반영하기 위해 항목이 업데이트되었음.	2012-01-10

기능	설명	날짜
미국 서부(캘리포니아 북부) 지역에 대한 지원	미국 서부(캘리포니아 북부) 지역 추가를 반영하기 위해 주제가 업데이트되었음.	2011-09-08
공개 릴리스	AWS Direct Connect의 첫 번째 릴리스.	2011-08-03

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