aws

랙용 사용 설명서

AWS Outposts

AWS Outposts: 랙용 사용 설명서

Table of Contents

무엇입니까 AWS Outposts? 1
주요 개념 1
AWS Outposts에 관한 자료 2
요금 5
AWS Outposts 작동 원리 6
네트워크 구성 요소 7
VPC 및 서브넷 8
라우팅 8
DNS 9
서비스 링크 9
로컬 게이트웨이 10
로컬 네트워크 인터페이스 10
Outposts 랙 요구 사항 11
시설 11
네트워킹 13
네트워크 준비 체크리스트 13
Power 18
주문 이행 20
Outposts ACE 랙 요구 사항 20
시설 21
네트워킹 21
Power 22
시작 24
Outpost를 생성하고 용량을 주문합니다. 24
1단계: 사이트 생성 24
2단계: Outpost 생성 26
3단계: 주문하기 26
4단계: 인스턴스 용량 수정 27
다음 단계 20
인스턴스 시작 30
1단계: VPC 생성 31
2단계: 서브넷 및 사용자 지정 라우팅 테이블 만들기 32
3단계: 로컬 게이트웨이 연결 구성 33
4단계: 온프레미스 네트워크 구성 39

5단계: Outpost에서 인스턴스 시작 41
6단계: 연결 테스트 42
서비스 링크 47
서비스 링크를 통한 연결 47
요구되는 서비스 링크 최대 전송 단위(MTU) 48
서비스 링크 대역폭 권장 사항 48
방화벽 및 서비스 링크 48
VPC를 사용한 서비스 링크 프라이빗 연결 49
필수 조건 49
중복 인터넷 연결 51
Outpost 및 사이트 52
Outpost 52
사이트 54
로컬 게이트웨이 57
로컬 게이트웨이 기본 사항 57
라우팅 58
로컬 게이트웨이를 통한 연결 58
로컬 게이트웨이 라우팅 테이블 59
직접 VPC 라우팅 60
고객 소유 IP 주소 63
로컬 게이트웨이 라우팅 테이블 사용 67
로컬 네트워크 연결 80
물리적 연결 80
링크 집계 81
가상 LAN. 82
네트워크 계층 연결 83
에이스 랙 커넥티비티 85
서비스 링크 BGP 연결 87
서비스 링크 인프라, 서브넷 광고 및 IP 범위 89
로컬 게이트웨이 BGP 연결 89
로컬 게이트웨이 고객 소유의 IP 서브넷 광고 91
공유 리소스로 작업하기 93
공유 가능한 Outpost 리소스 94
Outpost의 리소스 공유를 위한 사전 조건 95
관련 서비스 95
가용 영역 공유 95

Outpost 리소스 공유 96
공유된 Outpost 리소스 공유 해제 97
공유 Outpost 리소스 식별 97
공유 Outpost 리소스 권한 98
소유자에 대한 권한 98
소비자에 대한 권한 98
결제 및 측정 98
제한 사항 99
보안 100
데이터 보호 100
유휴 시 암호화 101
전송 중 데이터 암호화 101
데이터 삭제 101
자격 증명 및 액세스 관리 101
AWS Outposts와 IAM의 작동 방식 102
정책 예제 108
서비스 링크 역할 사용 110
AWS 관리형 정책 113
인프라 보안 114
변조 모니터링 115
복원력 115
규정 준수 확인 116
인터넷 액세스 117
상위 AWS 지역을 통한 인터넷 액세스 117
로컬 데이터 센터 네트워크를 통한 인터넷 액세스 118
모니터링 120
CloudWatch 메트릭스 121
Outpost 지표 121
Outpost 지표 차원 126
전초 기지의 CloudWatch 지표 보기 127
를 사용하여 API 호출을 기록합니다. CloudTrail 128
AWS Outposts자세한 내용은 CloudTrail 128
AWS Outposts 로그 파일 항목 이해 129
유지 관리 131
하드웨어 유지 관리 131
펌웨어 업데이트 132

네트워크 장비 유지 관리 132
전력 및 네트워크 이벤트 133
전력 이벤트 133
네트워크 연결 이벤트 133
리소스 134
최적화 135
Outpost의 전용 호스트 135
인스턴스 복구 설정 136
Outpost의 배치 그룹 136
랙 네트워크 문제 해결 138
Outpost 네트워크 장치와의 연결 138
AWS Direct Connect 지역에 대한 AWS 공용 가상 인터페이스 연결 139
AWS Direct ConnectAWS 지역에 대한 프라이빗 가상 인터페이스 연결 141
AWS 리전에 대한 ISP 공용 인터넷 연결 141
Outposts는 두 개의 방화벽 장치 뒤에 있습니다. 143
E nd-of-term 옵션 145
구독 갱신 145
구독 종료 146
구독 전환 150
할당량 151
AWS Outposts 그리고 다른 서비스에 대한 할당량 151
문서 기록 152
..... clvi

무엇입니까 AWS Outposts?

AWS Outposts AWS 인프라, 서비스, API 및 도구를 고객 사업장으로 확장하는 완전 관리형 서비스입니다. AWS 관리형 인프라에 대한 로컬 액세스를 제공함으로써 고객은 AWS 지역과 동일한 프로그래밍 인터페이스를 사용하여 온프레미스에서 애플리케이션을 구축하고 실행하는 동시에 로컬 컴퓨팅 및 스토리지 리소스를 사용하여 지연 시간을 줄이고 로컬 데이터 처리 요구 사항을 줄일 수 있습니다. AWS Outposts

Outpost는 고객 사이트에 배포된 AWS 컴퓨팅 및 스토리지 용량 풀입니다. AWS AWS 지역의 일부로서 이 용량을 운영, 모니터링 및 관리합니다. Outpost에서 서브넷을 생성하고 EC2 인스턴스, EBS 볼륨, ECS 클러스터 및 RDS 인스턴스와 같은 AWS 리소스를 생성할 때 서브넷을 지정할 수 있습니다. Outpost 서브넷의 인스턴스는 모두 동일한 VPC 내에서 프라이빗 IP 주소를 사용하여 AWS 해당 지역의 다른 인스턴스와 통신합니다.

> **Note**
>
> Outpost를 동일한 VPC 내에 있는 다른 Outpost 또는 로컬 구역에 연결할 수 없습니다.

자세한 내용은 AWS Outposts 제품 페이지를 참조하세요.

주요 개념

의 주요 개념은 다음과 같습니다. AWS Outposts

- 전초 기지 부지 — Outpost를 설치할 고객이 관리하는 물리적 건물. AWS 사이트는 Outpost에 대한 시설, 네트워킹 및 전원 요구 사항을 충족해야 합니다.
- Outpost 용량 – Outpost에서 사용할 수 있는 컴퓨팅 및 스토리지 리소스. AWS Outposts 콘솔에서 Outpost의 용량을 확인하고 관리할 수 있습니다.
- 전초 기지 장비 — 서비스에 대한 액세스를 제공하는 물리적 하드웨어. AWS Outposts 하드웨어에는 소유하고 관리하는 랙, 서버, 스위치 및 케이블이 포함됩니다. AWS
- Outpost 랙 – 업계 표준 42U 랙인 Outpost 폼 팩터입니다. Outpost 랙에는 랙 장착형 서버, 스위치, 네트워크 패치 패널, 전원 선반 및 블랭크 패널이 포함됩니다.
- Outposts ACE 랙 — 어그리게이션, 코어, 에지 (ACE) 랙은 멀티랙 아웃포스트 배포를 위한 네트워크 어그리게이션 포인트 역할을 합니다. ACE 랙은 논리적 Outposts의 여러 Outpost 컴퓨팅 랙과 온프레미스 네트워크 간의 연결을 제공하여 물리적 네트워킹 포트 수와 논리적 인터페이스 요구 사항을 줄여줍니다.

컴퓨팅 랙이 5개 이상인 경우 ACE 랙을 설치해야 합니다. 컴퓨팅 랙이 5개 미만이지만 향후 랙을 5개 이상으로 확장할 계획이라면 최대한 빨리 ACE 랙을 설치하는 것이 좋습니다.

ACE 랙에 대한 추가 정보는 ACE 랙을 사용한 AWS Outposts 랙 배포 규모 조정을 참조하십시오.

- Outpost 서버 – 업계 표준 1U 또는 2U 서버인Outpost 폼 팩터로, 표준 EIA-310D 19 호환 4포스트 랙에 설치할 수 있습니다. Outpost 서버는 공간이 제한적이거나 용량 요구 사항이 적은 사이트에 로컬 컴퓨팅 및 네트워킹 서비스를 제공합니다.
- 서비스 링크 — Outpost와 관련 지역 간의 통신을 가능하게 하는 네트워크 경로. AWS 각 Outpost는 가용 영역과 관련 리전의 확장본입니다.
- 로컬 게이트웨이 (LGW) — Outpost 랙과 온프레미스 네트워크 간의 통신을 지원하는 논리적 상호 연결 가상 라우터입니다.
- 로컬 네트워크 인터페이스 - Outpost 서버와 온프레미스 네트워크와의 통신을 지원하는 네트워크 인터페이스입니다.

AWS Outposts에 관한 자료

Outpost에서 다음 리소스를 생성하여 온프레미스 데이터 및 애플리케이션과 매우 가까운 거리에서 실행해야 하는 대기 시간이 짧은 워크로드를 지원할 수 있습니다.

컴퓨팅

리소스 유형	랙	서버
Amazon EC2 인스턴스	예	예
Amazon ECS 클러스터	예	예
Amazon EKS 노드	예	아니요

데이터베이스 및 분석

리소스 유형	랙	서버
Amazon ElastiCache 노드 (레디 스 클러스터, 멤캐시 클러스터)	 예	 아니요
Amazon EMR 클러스터	 예	 아니요
Amazon RDS DB 인스턴스	 예	 아니요

네트워킹

리소스 유형	랙	서버
App Mesh Envoy 프록시	 예	 예
Application Load Balancers	 예	 아니요
Amazon VPC 서브넷	 예	 예

리소스 유형	랙	서버
Amazon Route 53	 예	 아니요

스토리지

리소스 유형	랙	서버
Amazon EBS 볼륨	 예	 아니요
Amazon S3 버킷	 예	 아니요

기타 AWS 서비스

Service	랙	서버
AWS IoT Greengrass	 예	 예
아마존 SageMaker 엣지 매니저	 예	 예

요금

다양한 Outpost 구성 중에서 선택할 수 있으며, 각 구성은 EC2 인스턴스 유형과 스토리지 옵션의 조합을 제공합니다. 랙 구성 가격에는 설치, 제거 및 유지 관리가 포함됩니다. 서버의 경우 장비를 설치하고 유지 관리해야 합니다.

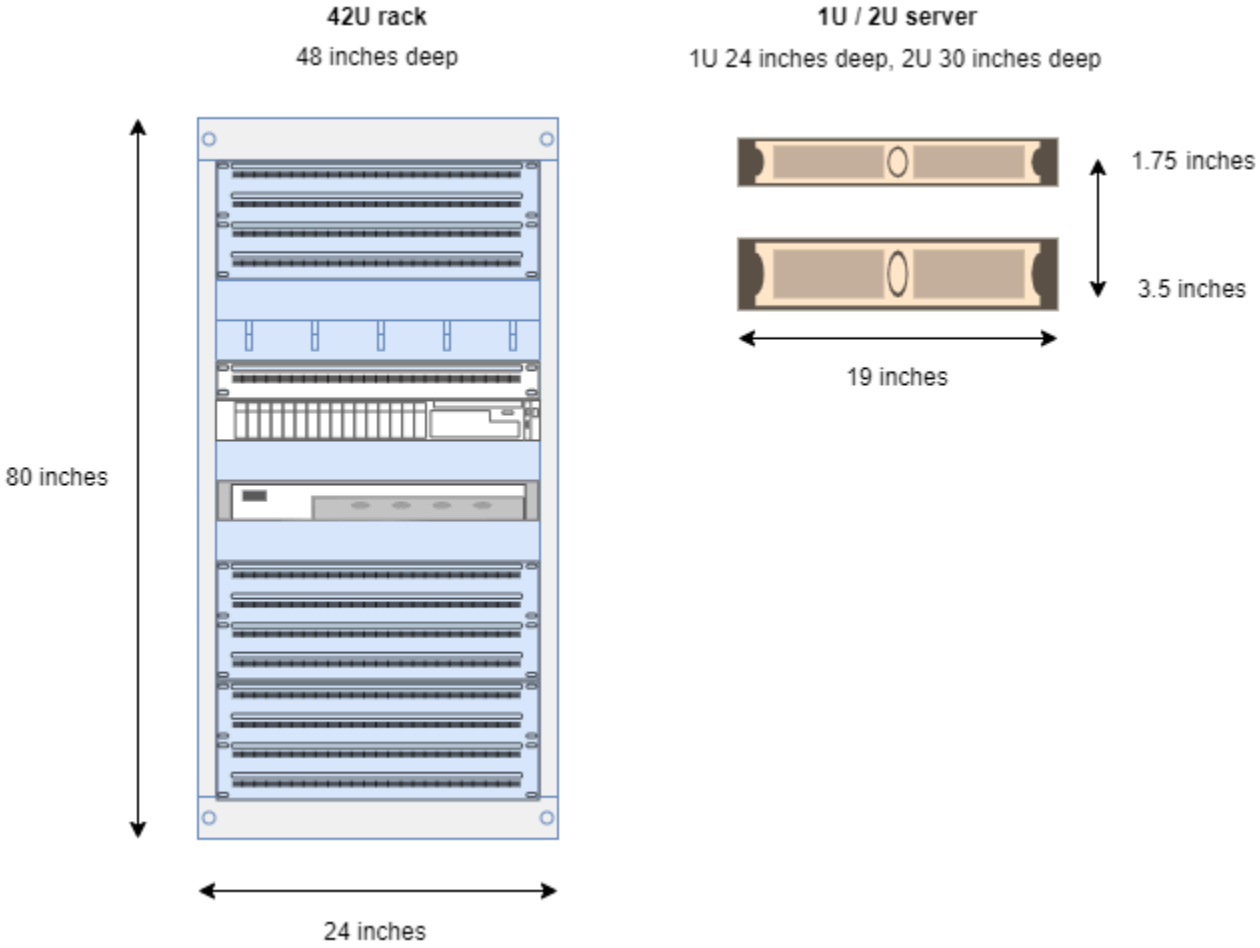
3년 약정 구성을 구매하면 전체 선결제, 부분 선결제, 선결제 없음의 세 가지 결제 옵션 중에서 선택할 수 있습니다. 부분 결제 옵션 또는 선결제 없음 옵션을 선택하면 월별 요금이 적용됩니다. Outpost가 설치되고 컴퓨팅 및 스토리지 용량을 사용할 수 있게 된 후 24시간이 지나면 모든 선결제 요금이 부과됩니다. 자세한 내용은 다음을 참조하세요.

- AWS Outposts 랙 요금
- AWS Outposts 서버 가격

AWS Outposts 작동 원리

AWS Outposts 전초 기지와 AWS 지역 간의 지속적이고 일관된 연결로 작동하도록 설계되었습니다. 리전 및 온프레미스 환경의 로컬 워크로드에 이렇게 연결하려면 Outpost를 온프레미스 네트워크에 연결해야 합니다. 온프레미스 네트워크는 해당 리전과 인터넷에 다시 연결되는 광역 네트워크(WAN) 액세스를 제공해야 합니다. 또한 온프레미스 워크로드 또는 애플리케이션이 있는 로컬 네트워크에 대한 LAN 또는 WAN 액세스를 제공해야 합니다.

다음은 Outpost 폼 팩터를 나타낸 다이어그램입니다.



내용

- 네트워크 구성 요소
- VPC 및 서브넷
- 라우팅
- DNS

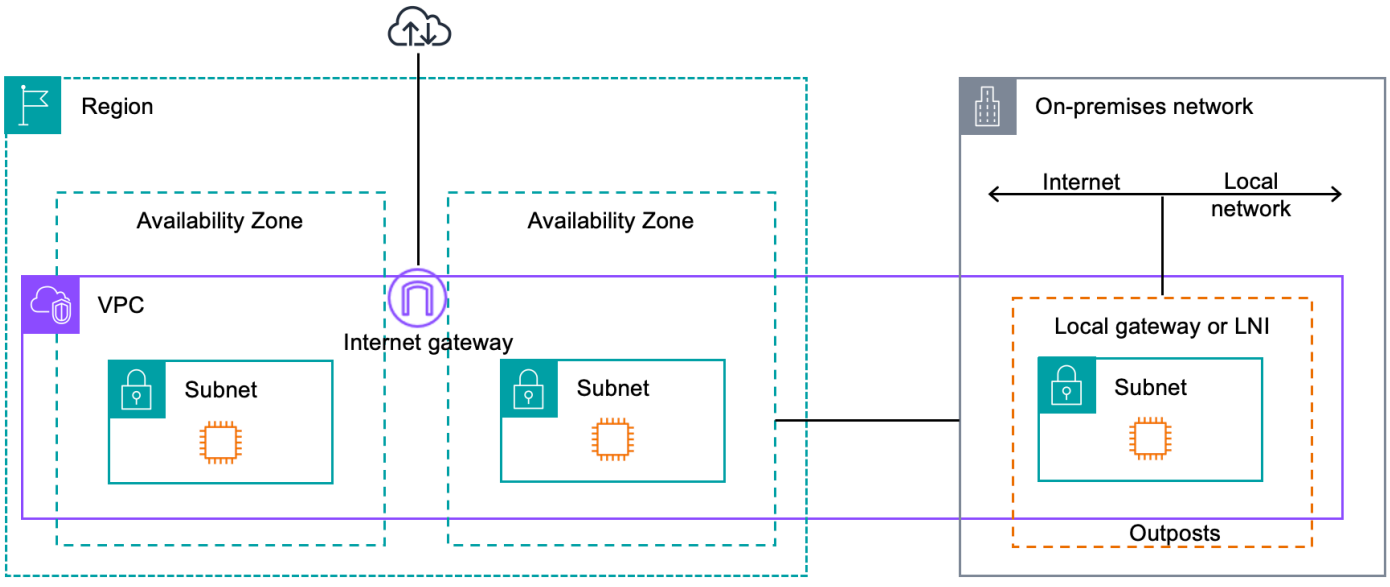
- 서비스 링크
- 로컬 게이트웨이
- 로컬 네트워크 인터페이스

네트워크 구성 요소

AWS Outposts 인터넷 게이트웨이, 가상 사설 게이트웨이, Amazon VPC 전송 게이트웨이, VPC 엔드포인트를 포함하여 지역에서 액세스할 수 있는 VPC 구성 요소를 사용하여 Amazon VPC를 지역에서 Outpost로 확장합니다. AWS Outpost는 리전의 가용 영역에 위치하며 복원력을 위해 사용할 수 있는 해당 가용 영역의 확장본입니다.

다음은 Outpost의 네트워크 구성 요소를 나타낸 다이어그램입니다.

- AWS 리전 A 및 온프레미스 네트워크
- 리전에 여러 서브넷이 있는 VPC
- 온프레미스 네트워크 내의 Outpost
- 로컬 게이트웨이(랙) 또는 로컬 네트워크 인터페이스(서버)를 통해 제공되는 Outpost와 로컬 네트워크 간 연결



VPC 및 서브넷

가상 사설 클라우드 (VPC) 는 해당 지역의 모든 가용 영역을 포괄합니다. AWS Outpost 서브넷을 추가하여 리전의 모든 VPC를 Outpost로 확장할 수 있습니다. VPC에 Outpost 서브넷을 추가하려면 서브넷을 생성할 때 Outpost의 Amazon 리소스 이름(ARN)을 지정합니다.

Outpost는 여러 서브넷을 지원합니다. Outpost에서 EC2 인스턴스를 시작할 때 EC2 인스턴스 서브넷을 지정할 수 있습니다. Outpost는 AWS 컴퓨팅 및 스토리지 용량 풀이기 때문에 인스턴스가 배포되는 기본 하드웨어를 지정할 수 없습니다.

각 Outpost는 Outpost 서브넷이 하나 이상 있을 수 있는 여러 VPC를 지원할 수 있습니다. Amazon VPC 할당량에 대한 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 할당량를 참조하세요.

Outpost를 생성한 VPC의 VPC CIDR 범위에서 Outpost 서브넷을 생성합니다. Outpost 서브넷에 있는 EC2 인스턴스와 같은 리소스에는 Outpost 주소 범위를 사용할 수 있습니다.

라우팅

기본적으로 모든 Outpost 서브넷은 VPC로부터 기본 라우팅 테이블을 상속합니다. 사용자 지정 라우팅 테이블을 생성하여 Outpost 서브넷과 연결할 수 있습니다.

Outpost 서브넷의 라우팅 테이블은 가용 영역 서브넷의 라우팅 테이블과 동일하게 작동합니다. IP 주소, 인터넷 게이트웨이, 로컬 게이트웨이, 가상 프라이빗 게이트웨이 및 피어링 연결을 대상으로 지정할 수 있습니다. 예를 들어, 상속된 기본 라우팅 테이블 또는 사용자 지정 테이블을 통해 각 Outpost 서브넷은 VPC 로컬 경로를 상속합니다. 즉, VPC CIDR에 대상이 있는 Outpost 서브넷을 포함하여 VPC의 모든 트래픽은 VPC에서 라우팅되는 상태를 유지합니다.

Outpost 서브넷 라우팅 테이블에는 다음 대상이 포함될 수 있습니다.

- VPC CIDR 범위 — 설치 시 이를 AWS 정의합니다. 이는 로컬 경로이며, 동일한 VPC에 있는 Outpost 인스턴스 간 트래픽을 포함하여 모든 VPC 라우팅에 적용됩니다.
- AWS 지역 대상 — 여기에는 Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB 게이트웨이 엔드포인트 AWS Transit Gateway, 가상 프라이빗 게이트웨이, 인터넷 게이트웨이 및 VPC 피어링에 대한 접두사 목록이 포함됩니다.

  동일한 Outpost에 있는 여러 VPC와 피어링 연결이 있는 경우 VPC 간 트래픽은 Outpost에 남아 있으며 해당 리전으로 다시 연결되는 서비스 링크를 사용하지 않습니다.

- Outpost에서 로컬 게이트웨이를 통한 VPC 내 통신 – 다이렉트 VPC 라우팅을 사용한 로컬 게이트웨이를 사용하여 여러 Outpost 전반의 동일한 VPC에 있는 서브넷 간 통신을 설정할 수 있습니다. 자세한 내용은 다음을 참조하세요.
  - 직접 VPC 라우팅
  - AWS Outposts 로컬 게이트웨이로 라우팅

DNS

기본적으로, Outpost 서브넷의 EC2 인스턴스는 Amazon Route 53 DNS 서비스를 사용하여 도메인 이름을 IP 주소로 확인할 수 있습니다. Route 53은 Outpost에서 실행 중인 인스턴스의 도메인 등록, DNS 라우팅, 상태 확인을 비롯한 DNS 기능을 지원합니다. 퍼블릭 호스팅 가용 영역과 프라이빗 호스팅 가용 영역 모두 트래픽을 특정 도메인으로 라우팅하는 데 지원됩니다. Route 53 리졸버는 리전에서 호스팅됩니다. AWS 따라서 이러한 DNS 기능이 작동하려면 Outpost에서 AWS 지역으로 다시 연결되는 서비스 링크 연결이 가동되고 실행되고 있어야 합니다.

아웃기지와 지역 간의 경로 지연 시간에 따라 Route 53을 사용하면 DNS 해결 시간이 더 길어질 수 있습니다. AWS 이 경우, 온프레미스 환경에 로컬로 설치된 DNS 서버를 사용할 수 있습니다. 자체 DNS 서버를 사용하려면 온프레미스 DNS 서버용 DHCP 옵션 세트를 생성하고 VPC와 연결해야 합니다. 또한 이러한 DNS 서버에 IP 연결이 있는지 확인해야 합니다. 연결이 용이하도록 로컬 게이트웨이 라우팅 테이블에 경로를 추가해야 할 수도 있지만 이 옵션은 로컬 게이트웨이가 있는 Outpost 랙에만 사용할 수 있습니다. DHCP 옵션 세트는 VPC 범위를 가지므로 VPC의 Outpost 서브넷과 가용 영역 서브넷 모두에 있는 인스턴스는 DNS 이름 확인을 위해 지정된 DNS 서버를 사용하려고 합니다.

Outpost에서 시작된 DNS 쿼리에는 쿼리 로깅이 지원되지 않습니다.

서비스 링크

서비스 링크는 Outpost에서 선택한 AWS 지역 또는 Outposts 홈 지역으로 다시 연결되는 링크입니다. 서비스 링크는 Outpost가 선택한 홈 리전과 통신할 때마다 사용되는 암호화된 VPN 연결 세트입니다. 가상 LAN(VLAN)을 사용하여 서비스 링크의 트래픽을 분류합니다. 서비스 링크 VLAN을 사용하면 전초 기지 관리 및 AWS 지역과 전초 기지 간의 VPC 내 트래픽 관리를 위해 전초 기지와 지역 간의 통신이 가능합니다. AWS

Outpost가 프로비저닝되면 서비스 링크가 생성됩니다. 서버 폼 팩터가 있는 경우 연결을 생성합니다. 랙이 있는 경우, 서비스 링크를 생성합니다. AWS 자세한 내용은 다음을 참조하세요.

- 아웃포스트 연결 AWS 리전

- AWS Outposts 고가용성 설계 및 아키텍처 고려 사항 백서의 애플리케이션/워크로드 라우팅 AWS

로컬 게이트웨이

Outpost 랙에는 온프레미스 네트워크 연결을 제공하는 로컬 게이트웨이가 포함되어 있습니다. Outpost 랙이 있는 경우 온프레미스 네트워크가 대상인 로컬 게이트웨이를 대상으로 포함할 수 있습니다. 로컬 게이트웨이는 Outpost 랙에만 사용할 수 있으며 Outpost 랙과 연결된 VPC 및 서브넷 라우팅 테이블에서만 사용할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 로컬 게이트웨이
- AWS Outposts 고가용성 설계 및 아키텍처 고려 사항 백서의 애플리케이션/워크로드 라우팅 AWS

로컬 네트워크 인터페이스

Outpost 서버에는 온프레미스 네트워크에 대한 연결을 제공하는 로컬 네트워크 인터페이스가 포함되어 있습니다. 로컬 네트워크 인터페이스는 Outpost 서브넷에서 실행되는 Outpost 서버에서만 사용할 수 있습니다. Outpost 랙이나 지역에 있는 EC2 인스턴스의 로컬 네트워크 인터페이스는 사용할 수 없습니다. AWS 로컬 네트워크 인터페이스는 온프레미스 위치에서만 사용할 수 있습니다. 자세한 내용은 Outpost 서버용AWS Outposts 사용 설명서의 로컬 네트워크 인터페이스를 참조하세요.

Outpost 랙의 사이트 요구 사항

Outpost 사이트는 Outpost가 운영되는 물리적 장소입니다. 사이트는 일부 국가 및 지역에서만 사용할 수 있습니다. 자세한 내용은 AWS Outposts 랙 FAQ를 참조하세요. 다음 질문을 참조하십시오: Outpost 랙을 사용할 수 있는 국가 및 리전은 어디입니까?

이 페이지에서는 Outpost 랙의 요구 사항을 다룹니다. 어그리게이션, 코어, 에지 (ACE) 랙을 설치하는 경우 사이트는 에 나열된 요구 사항도 충족해야 합니다. Outposts ACE 랙의 사이트 요구 사항

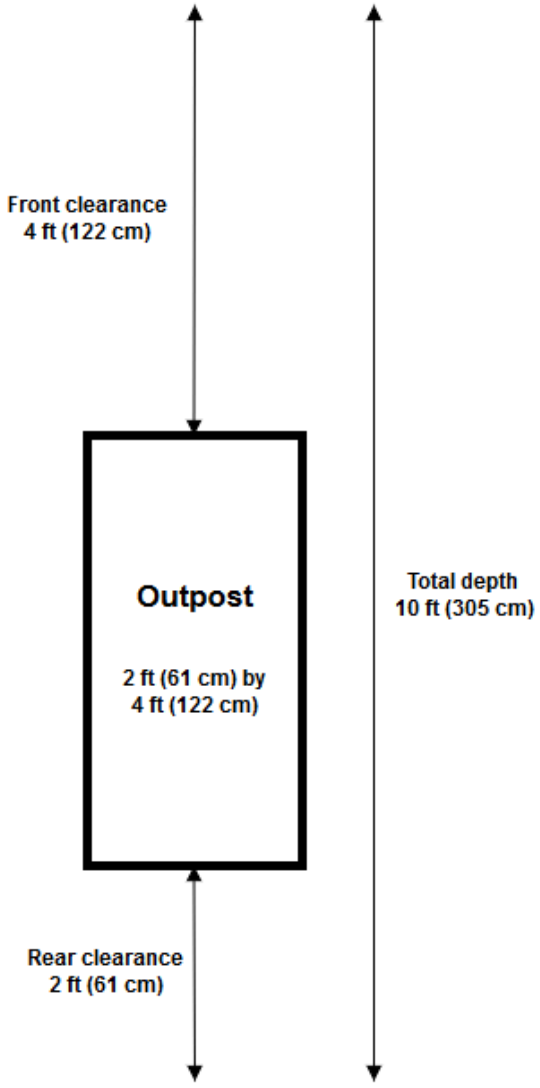
Outpost 서버의 요구 사항은 Outpost 서버용AWS Outposts 사용 설명서의 Outpost 서버의 사이트 요구 사항을 참조하세요.

시설

랙의 시설 요구 사항은 다음과 같습니다.

- 온도 및 습도 – 주변 온도는 41°F(5°C)에서 95°F(35°C) 사이여야 합니다. 상대 습도는 8~ 80% 사이여야 하며 결로 현상이 없어야 합니다.
- 공기 흐름 – 랙은 전면 통로에서 찬 공기를 끌어들이고 후면 통로로 뜨거운 공기를 배출합니다. 랙 위치는 분당 입방 피트(CFM)의 kVA의 145.8배 이상의 공기 흐름을 제공해야 합니다.
- 적재 도크 – 적재 도크에는 높이 94인치(239cm), 너비 54인치(138cm), 깊이 51인치(130cm)의 랙 상자를 수용할 수 있어야 합니다.
- 무게 지원 – 무게는 구성에 따라 다릅니다. 주문 요약에 지정된 구성의 무게는 랙 포인트 로드에서 확인할 수 있습니다. 랙이 설치된 위치와 해당 위치까지의 경로가 지정된 무게를 지탱해야 합니다. 여기에는 경로를 따라 있는 모든 화물 및 일반 엘리베이터가 포함됩니다.
- 여유 공간 – 랙은 높이 80인치(203cm), 너비 24인치(61cm), 깊이 48인치(122cm) 입니다. 모든 출입구, 복도, 회전로, 경사로, 엘리베이터는 충분한 공간을 확보해야 합니다. 최종 휴식 위치에는 Outpost를 놓을 공간이 24인치(61cm), 깊이 48인치(122cm), 추가로 48인치(122cm)의 전면 간격과 24인치(61cm)의 후면 간격이 있어야 합니다. Outpost에 필요한 총 최소 면적은 너비 24인치(61cm), 깊이 10피트(305cm) 입니다.

  다음 다이어그램은 간극을 포함하여 Outpost에 필요한 총 최소 면적을 보여줍니다.



- 내진 브레이싱 — 랙이 시설에 있는 동안 규정 또는 규정에서 요구하는 범위 내에서 랙에 적합한 지진 고정 장치 및 브레이스를 설치하고 유지 관리해야 합니다. AWS 모든 Outposts 랙에서 최대 2.0G의 지진 활동을 보호하는 플로어 브래킷을 제공합니다.
- 본딩 포인트 — AWS공인 기술자가 설치 중에 랙을 접착할 수 있도록 랙 위치에 본딩 와이어/포인트를 제공하는 것이 좋습니다.
- 시설 접근 — 전초 기지 접근, 정비 또는 철거 능력에 부정적인 영향을 미치는 방식으로 시설을 변경해서는 안 됩니다. AWS
- 고도 – 랙이 설치된 공간의 고도는 10,005피트(3,050미터) 미만이어야 합니다.

네트워킹

랙의 네트워킹 요구 사항은 다음과 같습니다.

- 1Gbps, 10Gbps, 40Gbps 또는 100Gbps의 속도로 업링크를 제공합니다.

  서비스 링크 연결에 대한 대역폭 권장 사항은 대역폭 권장 사항을 참조하세요.
- Lucent Connector(LC)가 있는 단일 모드 파이버(SMF), 멀티모드 파이버(MMF) 또는 LC가 있는 MMF OM4를 제공합니다.
- 스위치 또는 라우터일 수 있는 업스트림 장치를 하나 또는 두 개 제공합니다. 고가용성을 제공하려면 두 개의 장치를 사용하는 것이 좋습니다.

네트워크 준비 체크리스트

Outpost 구성을 위한 정보를 수집할 때 이 체크리스트를 사용합니다. 여기에는 LAN, WAN 및 전초 기지와 지역 교통 목적지 사이의 모든 장치, 지역 내 목적지가 포함됩니다. AWS

업링크 속도, 포트 및 광케이블

업링크 속도 및 포트

Outpost에는 로컬 네트워크에 연결되는 Outpost 네트워크 장치 두 개가 있습니다. 각 장치가 지원할 수 있는 업링크 수는 대역폭 요구 사항과 라우터가 지원할 수 있는 항목에 따라 다릅니다. 자세한 내용은 물리적 연결 단원을 참조하세요.

다음 목록은 업링크 속도를 기준으로 각 Outpost 네트워크 장치에 지원되는 업링크 포트 수를 보여줍니다.

1Gbps

  1, 2, 4, 6 또는 8 업링크

10Gbps

  1, 2, 4, 8, 12 또는 16개의 업링크

40Gbps 또는 100Gbps

  1, 2 또는 4개의 업링크

파이버

다음 파이버 유형이 지원됩니다.

- Lucent Connector(LC) 가 있는 싱글모드 파이버(SMF)
- 멀티 모드 파이버(MMF) 또는 MMF OM4(LC 포함)

업링크 속도와 선택한 광케이블 유형에 따라 다음과 같은 광학 표준이 지원됩니다.

업링크 속도	파이버 유형	광학 표준
1Gbps	SMF	— 1000Base-LX
1Gbps	MMF	— 1000베이스-X
10Gbps	SMF	– 10GBASE-IR – 10GBASE-LR
10Gbps	MMF	— 10GBASE-SR
40Gbps	SMF	– 40GBASE-IR4 (LR4L) — 40GBASE-LR4
4 x 10Gbps 브레이크아웃 애플리케이션	MMF	— 40GBASE-ESR4 – 40GBASE-SR4
100Gbps	SMF	— 100G PSM4 MSA — 100GBASE-CWDM4 – 100GBASE-LR4
4 x 25 Gbps 브레이크아웃 애플리케이션	MMF	— 100GBASE-SR4

Outpost 링크 집계 및 VLAN

Outpost와 네트워크 간에는 링크 집계 제어 프로토콜(LACP)이 필요합니다. LACP와 함께 동적 LAG를 사용해야 합니다.

각 Outpost 네트워크 장치에는 다음과 같은 VLAN이 필요합니다. 자세한 내용은 가상 LAN. 단원을 참조하세요.

Outpost 네트워크 장치	서비스 링크 VLAN	로컬 게이트웨이 VLAN
#1	유효한 값: 1-4094	유효한 값: 1-4094
#2	유효한 값: 1-4094	유효한 값: 1-4094

각 Outpost 네트워크 장치에 대해 서비스 링크 및 로컬 게이트웨이에 동일한 VLAN을 사용할지 아니면 다른 VLAN을 사용할지 선택할 수 있습니다. 하지만 각 Outpost 네트워크 장치는 다른 Outpost 네트워크 장치와 다른 VLAN을 사용하는 것이 좋습니다. 자세한 내용은 링크 어그리게이션 및 가상 LAN을 참조하십시오.

또한 이중 레이어 2 연결을 사용하는 것이 좋습니다. LACP는 링크 집계에 사용되며 고가용성에는 사용되지 않습니다. Outpost 네트워크 장치 간 LACP는 지원되지 않습니다.

Outpost 네트워크 장치 IP 연결

Outpost 네트워크 장치 두 개에는 각각 서비스 링크 및 로컬 게이트웨이 VLAN을 위한 CIDR 및 IP 주소가 필요합니다. /30 또는 /31 CIDR을 사용하여 각 네트워크 장치에 전용 서브넷을 할당하는 것이 좋습니다. Outpost 에서 사용할 서브넷과 IP 주소를 지정합니다. 자세한 내용은 네트워크 계층 연결 단원을 참조하세요.

Outpost 네트워크 장치	서비스 링크 요구 사항	로컬 게이트웨이 요구 사항
#1	– 서비스 링크 CIDR(/30 또는 /31) — 서비스 링크 IP 주소	– 로컬 게이트웨이 CIDR(/30 또는 /31) — 로컬 게이트웨이 IP 주소
#2	– 서비스 링크 CIDR(/30 또는 /31) — 서비스 링크 IP 주소	– 로컬 게이트웨이 CIDR(/30 또는 /31) — 로컬 게이트웨이 IP 주소

서비스 링크 최대 전송 단위(MTU)

네트워크는 상위 지역의 Outpost와 서비스 링크 엔드포인트 간의 1500바이트 MTU를 지원해야 합니다. AWS 서비스 링크에 대한 자세한 내용은 AWS OutpostsAWS 지역과의 연결성을(를) 참조하세요.

서비스 링크 테두리 게이트웨이 프로토콜

Outpost는 서비스 링크 VLAN을 통한 서비스 링크 연결을 위해 각 Outpost 네트워크 장치와 로컬 네트워크 장치 간에 외부 BGP (eBGP) 피어링 세션을 설정합니다. 자세한 내용은 서비스 링크 BGP 연결 단원을 참조하세요.

Outpost	서비스 링크 BGP 요구 사항
당신의 Outpost	– Outpost BGP 자율 시스템 번호(ASN). 2바이트(16비트) 또는 4바이트(32비트). 프라이빗 ASN 범위(64512-65534 또는 4200000000-4294967294)에서. – 인프라 CIDR(/26 필수, 두 개의 연속 /27로 광고).

로컬 네트워크 장치	서비스 링크 BGP 요구 사항
#1	— 서비스 링크 BGP 피어 IP 주소. – 서비스 링크 BGP 피어 ASN. 2바이트(16비트) 또는 4바이트(32비트).
#2	— 서비스 링크 BGP 피어 IP 주소. – 서비스 링크 BGP 피어 ASN. 2바이트(16비트) 또는 4바이트(32비트).

서비스 링크 방화벽

UDP 및 TCP 443은 방화벽에 상태 저장 방식으로 나열되어야 합니다.

프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	443	Outpost 서비스 링크 /26	443	Outpost 리전의 공개 경로
TCP	1025-65535	Outpost 서비스 링크 /26	443	Outpost 리전의 공개 경로

AWS Direct Connect 연결 또는 공용 인터넷 연결을 사용하여 Outpost를 해당 지역에 다시 연결할 수 있습니다. AWS Outpost 서비스 링크 연결의 경우, 방화벽 또는 엣지 라우터에서 NAT 또는 PAT를 사용할 수 있습니다. 서비스 링크 설정은 항상 Outpost에서 시작됩니다.

로컬 게이트웨이 Border Gateway Protocol

Outpost는 로컬 네트워크에서 로컬 게이트웨이로 연결하기 위해 각 Outpost 네트워크 장치에서 로컬 네트워크 장치로 eBGP 피어링 세션을 설정합니다. 자세한 내용은 로컬 게이트웨이 BGP 연결 단원을 참조하세요.

Outpost	로컬 게이트웨이 BGP 요구 사항
당신의 Outpost	– Outpost BGP 자율 시스템 번호(ASN). 2바이트(16비트) 또는 4바이트(32비트). 프라이빗 ASN 범위(64512-65534 또는 4200000000-4294967294)에서. – 광고용 CoIP CIDR (퍼블릭 또는 프라이빗, 최소 /26)

로컬 네트워크 장치	로컬 게이트웨이 BGP 요구 사항
#1	— 로컬 게이트웨이 BGP 피어 IP 주소. – 로컬 게이트웨이 BGP 피어 ASN. 2바이트(16비트) 또는 4바이트(32비트).
#2	— 로컬 게이트웨이 BGP 피어 IP 주소.

로컬 네트워크 장치	로컬 게이트웨이 BGP 요구 사항
	– 로컬 게이트웨이 BGP 피어 ASN. 2바이트(16비트) 또는 4바이트(32비트).

Power

Outpost 전원 쉘프는 5kVA, 10kVA 또는 15kVA의 세 가지 전원 구성을 지원합니다. 전원 쉘프의 구성은 Outpost 용량의 총 전력 소비량에 따라 달라집니다. 예를 들어 Outpost 리소스의 최대 전력 소비량이 9.7kVA인 경우 이중 단상 전원을 위해 L6-30P 또는 IEC309 4개, S1에 2드롭, S2에 2드롭 등 10kVA에 대한 전원 구성을 제공해야 합니다. 세 가지 전원 구성은 다음 두 번째 표에 설명되어 있습니다.

다양한 Outpost 자원에 대한 전력 소비량 요구 사항을 보려면 AWS Outposts 콘솔 https://console.aws.amazon.com/outposts/ 에서 카탈로그 찾아보기를 선택하십시오.

요구 사항	사양
AC 라인 전압	단상 208~277VAC, 50Hz 또는 60Hz 3단계: • 208~250VAC (델타), 50~60Hz • 346~480VAC (와이), 50~60Hz
전력 소비	5kVA(4kW), 10kVA(9kW) 또는 15kVA(13kW)
AC 보호(업스트림 파워 브레이커)	1N 입력 (이중화 없음) 및 2N 입력 (예비) 모두의 경우: 30A, 32A 또는 50A (D 커브 또는 K 커브 회로 차단기 포함). 2N 입력(예비)에만 해당: C 커브, D 커브 또는 K 커브 회로 차단기 B-커브 이하는 지원되지 않습니다.
AC 입력 유형(리셉터클)	단상 3xL6-30P, P+P+E, 30A 또는 3XIEC60309 P+N+E, IP67, 32A 플러그 3상, Wye 1XiE C60309, 3P+N+E, IP67, 시계 위치 7, 30A 플러그 또는 1XIEC60309, 3P+N+E, IP67, 시계 위치 6, 32A 플러그

요구 사항	사양
	3상, 델타 1x Non-NEMA 트위스트락 허벨 CS8365C, 3P+E, 센터 그라운드, 50A 플러그 **Note** 가장 좋은 방법은 IP67 플러그를 IP67 콘센트에 연결하는 것입니다. 그렇게 할 수 없는 경우 IP67 플러그는 IP44 리셉터클과 연결됩니다. 플러그와 소켓을 결합한 정격은 더 낮은 등급(IP44)이 됩니다.
휩 길이	3미터(10.25피트)
휩 - 랙 케이블링 입력	랙 위 또는 아래에서

파워 쉘프에는 다음과 같이 구성할 수 있는 두 개의 입력 단자 S1과 S2가 있습니다.

	이중화, 단상	이중화, 3상	단상	3상
5 kVA	L6-30P 또는 IEC309 2개, S1에 한 방울, S2에 한 방울	AH530P7W, AH532P6W 또는 CS8365C 2개, S1에는 한 번, S2에는 한 번 떨어집니다.	L6-30P 또는 IEC309 1개, S1까지 한 번 떨어집니다.	AH530P7W, AH532P6W 또는 CS8365C 1개, S1까지 한 번 떨어집니다.
10kVA	L6-30P 또는 IEC309 4회, S1에는 2회, S2에는 2회 떨어집니다.		L6-30P 또는 IEC309 2개, S1에 2방울	
15kVA	L6-30P 또는 IEC309 6개, S1에는 3회, S2에는 3회 떨어집니다.		L6-30P 또는 IEC309 3개, S1에 3방울	

앞에서 설명한 대로 AWS 제공되는 AC 휩에 대체 전원 플러그를 장착해야 하는 경우 다음 사항을 고려하십시오.

- 고객이 제공한 공인 전기 기술자만이 새 플러그 유형에 맞게 AC 휩을 수정해야 합니다.

- 설치는 해당하는 모든 국가, 주 및 리전 안전 요구 사항을 준수해야 하며 필요에 따라 전기 안전에 대한 검사를 거쳐야 합니다.
- 고객은 AC 휩 플러그의 수정 사항을 AWS 담당자에게 알려야 합니다. 요청 시 수정 사항에 AWS대한 정보를 제공해드립니다. 관할권을 가진 당국에서 발행한 안전 검사 기록도 포함해야 합니다. 이는 AWS 직원이 장비에 대한 작업을 수행하도록 하기 전에 설비의 안전성을 검증하기 위한 요구 사항입니다.

주문 이행

주문을 처리하기 위해 귀하와 함께 날짜와 시간을 정합니다. AWS 설치 전에 확인하거나 제공해야 할 항목의 체크리스트도 받게 됩니다.

AWS 설치 팀이 예정된 날짜와 시간에 현장에 도착합니다. 지정된 위치에 랙을 배치합니다. 랙에 대한 전기 연결 및 설치는 귀하와 귀하의 전기 기술자가 담당합니다.

전기 설비 및 해당 설비의 모든 변경은 모든 관련 법률, 규정 및 모범 사례에 따라 공인 전기 기술자가 수행하도록 해야 합니다. Outpost 하드웨어 또는 전기 설비를 변경하기 전에 서면으로 승인을 AWS 받아야 합니다. 귀하는 규정 준수 및 변경 AWS 사항의 안전성을 확인하는 문서를 제공하는 데 동의합니다. AWS Outpost 전기 설비 또는 시설 전기 배선 또는 변경으로 인해 발생하는 위험에 대해서는 책임을 지지 않습니다. Outpost 하드웨어를 다른 방식으로 변경해서는 안 됩니다.

팀은 고객이 제공하는 업링크를 통해 Outpost 랙에 대한 네트워크 연결을 설정하고 랙 용량을 구성합니다.

Outpost 랙을 위한 Amazon EC2 및 Amazon EBS 용량을 AWS 계정에서 사용할 수 있는지 확인하면 설치가 완료됩니다.

Outposts ACE 랙의 사이트 요구 사항

> **Note**
>
> ACE 랙이 필요하지 않은 경우 이 섹션을 건너뛰십시오.

어그리게이션, 코어, 에지 (ACE) 랙은 멀티랙 아웃포스트 배포를 위한 네트워크 어그리게이션 포인트 역할을 합니다. 컴퓨팅 랙이 5개 이상인 경우 ACE 랙을 설치해야 합니다. 컴퓨팅 랙이 5개 미만이지만 향후 랙을 5개 이상으로 확장할 계획이라면 최대한 빨리 ACE 랙을 설치하는 것이 좋습니다.

ACE 랙을 설치하려면 에 나열된 요구 사항 외에도 이 섹션의 요구 사항을 충족해야 합니다. Outpost 랙의 사이트 요구 사항

시설

ACE 랙의 시설 요구 사항은 다음과 같습니다.

- 전원 — 모든 랙에는 10kVA 단상 (AA+BB, IEC60309 또는 L6-30P Whip 커넥터 유형) 이 함께 제공됩니다.
- 무게 지원 — 랙 무게는 705파운드, 320kg입니다.
- 간격/사이즈 치수 — 랙 높이는 80인치, 203cm입니다.

> **Note**
>
> ACE 랙은 완전히 밀폐되지 않으며 전면 또는 후면 도어를 포함하지 않습니다.

네트워킹

ACE 랙의 네트워킹 요구 사항은 다음과 같습니다. ACE 랙이 Outposts 네트워킹 장치, 온프레미스 네트워킹 장치 및 Outpost 랙을 연결하는 방법을 이해하려면 을 참조하십시오. 에이스 랙 커넥티비티

- 랙 네트워크 요구 사항 - 다음 변경 사항을 제외하고 네트워크 준비 체크리스트 및 랙용 로컬 네트워크 연결 섹션에 나열된 요구 사항을 충족하는지 확인하십시오.
  - ACE 랙에는 업스트림 디바이스에 연결되는 네트워킹 디바이스가 4개 있으며, 단일 Outposts 랙의 경우처럼 두 개가 아닙니다.
  - ACE 랙은 1Gbps 업링크를 지원하지 않습니다.
- 업링크 속도 - 10Gbps, 40Gbps 또는 100Gbps의 속도로 업링크를 제공합니다. 서비스 링크 연결에 대한 대역폭 권장 사항은. 서비스 링크 대역폭 권장 사항

> **Important**
>
> ACE 랙은 1Gbps 업링크를 지원하지 않습니다.

- 파이버 — LC (루슨트 커넥터) 가 있는 SMF (단일 모드 파이버) 또는 LC (루슨트 커넥터) 가 있는 멀티 모드 파이버 (MMF) 를 제공합니다. 지원되는 광케이블 유형 및 광학 표준의 전체 목록은 을 참조하십시오. 업링크 속도, 포트 및 광케이블

- 업스트림 디바이스 - 스위치 또는 라우터일 수 있는 업스트림 디바이스 2개 또는 4개를 제공합니다.
- 서비스 VLAN 및 로컬 게이트웨이 VLAN - 4개의 ACE 네트워킹 디바이스 각각에 대해 서비스 VLAN과 다른 로컬 게이트웨이 VLAN을 제공해야 합니다. 서비스 VLAN과 로컬 게이트웨이 VLAN에 각각 하나씩 두 개의 개별 VLAN만 제공하거나, 서비스 VLAN과 LGW VLAN 모두에 대해 각 ACE 네트워킹 디바이스에서 서로 다른 VLAN을 사용하여 총 8개의 서로 다른 VLAN을 제공하도록 선택할 수 있습니다. LAG (링크 어그리게이션 그룹) 및 VLAN을 사용하는 방법에 대한 자세한 내용은 및 을 참조하십시오. 링크 집계 가상 LAN.
- 서비스 링크 및 로컬 게이트웨이 VLAN의 CIDR 및 IP 주소 - /30 또는 /31 CIDR을 사용하여 각 ACE 네트워킹 장치에 전용 서브넷을 할당하는 것이 좋습니다. 또는 각 서비스 및 로컬 게이트웨이 VLAN에 단일 /29 서브넷을 할당할 수도 있습니다. 두 경우 모두 ACE 네트워킹 디바이스에서 사용할 IP 주소를 지정해야 합니다. 자세한 정보는 네트워크 계층 연결을 참조하세요.
- 서비스 링크 VLAN과 로컬 게이트웨이 VLAN용 고객 및 Outpost BGP ASN (자율 시스템 번호) - Outpost는 서비스 링크 VLAN을 통한 서비스 링크 연결을 위해 각 ACE 랙 장치와 로컬 네트워크 장치 간에 외부 BGP (eBGP) 피어링 세션을 설정합니다. 또한 로컬 네트워크에서 로컬 게이트웨이로 연결하기 위해 각 ACE 네트워킹 장치에서 로컬 네트워크 장치로 eBGP 피어링 세션을 설정합니다. 자세한 내용은 서비스 링크 BGP 연결 및 로컬 게이트웨이 BGP 연결 섹션을 참조하세요.

> **Important**
>
> 서비스 링크 인프라 서브넷 — Outposts 설치에 포함된 각 컴퓨팅 랙에는 서비스 링크 인프라 서브넷 (/26이어야 함) 이 필요합니다.

Power

ACE 랙의 전원 요구 사항은 다음과 같습니다.

요구 사항	사양
AC 라인 전압	단상 200~240VAC, 50Hz 또는 60Hz
전력 소비	10kVA 단상 (AA+BB)
AC 보호(업스트림 파워 브레이커)	2N 입력(예비)에만 해당: C 커브, D 커브 또는 K 커브 회로 차단기 B-커브 이하는 지원되지 않습니다.

요구 사항	사양
AC 입력 유형(리셉터클)	IEC60309 또는 L6-30P 휩 커넥터 유형.

다음으로 시작하세요 AWS Outposts

시작하려면 Outpost를 주문합니다. Outpost 장비를 설치한 후 Amazon EC2 인스턴스를 시작하고 온프레미스 네트워크에 액세스합니다.

Tasks

- Outpost를 생성하고 Outpost 용량을 주문합니다.
- 아웃포스트 랙에서 인스턴스를 시작합니다.

Outpost를 생성하고 Outpost 용량을 주문합니다.

사용을 AWS Outposts시작하려면 전초 기지를 만들고 전초 기지 용량을 주문해야 합니다.

필수 조건

- Outpost 랙에 사용 가능한 구성을 검토합니다.
- Outpost 사이트는 Outpost 장비가 배치되는 물리적 장소입니다. 용량을 주문하기 전에 사이트가 요구 사항을 충족하는지 확인합니다. 자세한 정보는 Outpost 랙의 사이트 요구 사항을 참조하세요.
- AWS 엔터프라이즈 지원 플랜 또는 AWS 엔터프라이즈 온램프 지원 플랜이 있어야 합니다.
- 전초 기지를 AWS 계정 소유할 사람을 결정하십시오. 이 계정을 사용하여 Outpost 사이트를 생성하고 Outpost를 생성하고 주문합니다. 이 계정과 연결된 이메일에서 AWS정보를 확인하세요.

Tasks

- 1단계: 사이트 생성
- 2단계: Outpost 생성
- 3단계: 주문하기
- 4단계: 인스턴스 용량 수정
- 다음 단계

1단계: 사이트 생성

사이트를 만들어 운영 주소를 지정합니다. 운영 주소는 Outpost 랙의 물리적 위치입니다.

필수 조건

- 운영 주소를 결정합니다.

사이트를 생성하려면 다음과 같이 하세요.

1. Outpost를 AWS 계정 소유할 계정을 AWS 사용하여 로그인하세요.
2. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
3. 상위 AWS 리전항목을 선택하려면 페이지 오른쪽 상단의 지역 선택기를 사용합니다.
4. 탐색 창에서 사이트를 선택합니다.
5. 사이트 생성를 선택합니다.
6. 지원되는 하드웨어 유형에서 랙 및 서버를 선택합니다.
7. 사이트에 대한 이름, 설명, 운영 주소를 입력합니다.
8. 사이트 세부에서 사이트에 대해 요청된 정보를 제공합니다.
   - 최대 무게 - 이 사이트에서 지원할 수 있는 최대 랙 무게.
   - 전력 소비량 - 랙의 하드웨어 배치 위치에서 사용할 수 있는 전력 소비량을 kVA 단위로 지정합니다.
   - 전원 옵션 - 하드웨어에 제공할 수 있는 전원 옵션.
   - 전원 커넥터 - AWS 가 하드웨어 연결을 위해 제공해야 할 전원 커넥터.
   - 전원 공급 장치 드롭 - 전원 공급 장치가 랙 위쪽인지 아래인지 보여줍니다.
   - 업링크 속도 - 랙이 Gbps에서 리전 연결에 지원해야 하는 업링크 속도.
   - 업링크 수 - 랙을 네트워크에 연결하는 데 사용하려는 각 Outpost 네트워킹 장치의 업링크 수입니다.
   - 파이버 유형 - Outpost를 네트워크에 연결하는 데 사용할 파이버 유형.
   - 광학 표준 - Outpost를 네트워크에 연결하는 데 사용할 광학 표준 유형.
9. (선택 사항) 사이트 노트의 경우 사이트에 대해 알아두면 유용할 수 있는 기타 정보를 입력합니다. AWS
10. 시설 요구 사항을 읽은 다음 시설 요구 사항을 읽었습니다를 선택합니다.
11. 사이트 생성을 선택합니다.

2단계: Outpost 생성

랙에 대한 Outpost를 생성합니다. 그런 다음 주문할 때 이 Outpost를 지정하세요.

필수 조건

- 사이트와 연결할 AWS 가용 영역을 결정하세요.

Outpost를 생성하려면 다음과 같이 하세요.

1. 탐색 창에서 Outpost를 선택합니다.
2. Outpost 생성을 선택합니다.
3. 랙을 선택합니다.
4. Outpost에 대한 이름과 설명을 입력합니다.
5. Outpost의 가용 영역을 선택합니다.
6. (선택 사항) 프라이빗 연결을 구성하려면 프라이빗 연결 사용을 선택합니다. Outpost와 동일한 가용 영역에서 AWS 계정 VPC와 서브넷을 선택하십시오. 자세한 정보는 the section called “필수 조건”을 참조하세요.
7. 사이트 ID에서 사이트를 선택합니다.
8. Outpost 생성을 선택합니다.

3단계: 주문하기

필요한 Outpost 랙을 주문합니다. 주문을 제출하면 AWS Outposts 담당자가 연락을 드릴 것입니다.

> **Important**
>
> 제출한 후에는 주문을 수정할 수 없으므로 제출하기 전에 모든 세부 정보를 주의 깊게 검토하십시오. 주문을 변경해야 하는 경우 계정 관리자에게 문의하세요. AWS

필수 조건

- 주문 결제 방법을 결정합니다. 선결제 없음, 부분 선결제, 혹은 전체 선결제로 결제할 수 있습니다. 전액 선불로 지불하지 않는 경우 3년 약정 기간 동안 월별 요금을 지불하게 됩니다.

요금에는 제공, 설치, 인프라 서비스 유지 보수, 소프트웨어 매치 및 업그레이드가 포함됩니다.

- 배송 주소가 사이트에 지정한 운영 주소와 다른지 확인합니다.

주문하려면 다음과 같이 하세요.

1. 탐색 창에서 구매 주문를 선택합니다.
2. 주문하기를 선택합니다.
3. 지원되는 하드웨어 유형에서 랙을 선택합니다.
4. 용량을 추가하려면 구성을 선택합니다. 사용 가능한 구성이 요구 사항에 맞지 않는 경우 대신 연락하여 AWS 사용자 지정 용량 구성을 요청할 수 있습니다.
5. 다음을 선택합니다.
6. 기존 Outpost 사용을 선택하고 Outpost를 선택합니다.
7. 다음을 선택합니다.
8. 계약 기간 및 지불 옵션을 선택합니다.
9. 배송 주소를 지정합니다. 새 주소를 지정하거나 사이트 운영 주소를 선택할 수 있습니다. 운영 주소를 선택한 경우 향후 사이트 운영 주소에 대한 변경 사항이 기존 주문에는 적용되지 않는다는 점에 유의하십시오. 기존 주문의 배송 주소를 변경해야 하는 경우 AWS 계정 관리자에게 문의하십시오.
10. 다음을 선택합니다.
11. 검토 및 주문 페이지에서 정보가 정확한지 확인하고 필요에 따라 수정합니다. 주문을 제출한 후에는 주문을 편집할 수 없습니다.
12. 주문하기를 선택합니다.

4단계: 인스턴스 용량 수정

Outpost는 AWS 지역 내 가용 영역의 프라이빗 확장으로서 사이트에 AWS 컴퓨팅 및 스토리지 용량 풀을 제공합니다. Outpost에서 사용할 수 있는 컴퓨팅 및 스토리지 용량은 한정되어 있으며 사이트에 AWS 설치하는 랙의 크기와 수에 따라 결정되므로, 초기 워크로드를 실행하고, 향후 성장에 대응하고, 서버 장애 및 유지 관리 이벤트를 완화할 추가 용량을 제공하는 데 필요한 Amazon AWS Outposts EC2, Amazon EBS 및 Amazon S3의 용량을 결정해야 합니다.

각 새 Outpost 주문의 용량은 기본 용량 구성으로 구성됩니다. 기본 구성을 변환하여 비즈니스 요구 사항에 맞는 다양한 인스턴스를 만들 수 있습니다. 이렇게 하려면 용량 작업을 생성하고, 인스턴스 크기 및 수량을 지정하고, 용량 작업을 실행하여 변경을 구현해야 합니다.

> **Note**
>
> - Outposts를 주문한 후 인스턴스 크기 수량을 변경할 수 있습니다.
> - 인스턴스 크기 및 수량은 Outpost 수준에서 정의됩니다.
> - 인스턴스는 모범 사례에 따라 자동으로 배치됩니다.

인스턴스 용량을 수정하려면

1. AWS Outposts 콘솔의AWS Outposts 왼쪽 탐색 창에서 용량 작업을 선택합니다.
2. 용량 작업 페이지에서 용량 작업 생성을 선택합니다.
3. 시작하기 페이지에서 순서를 선택합니다.
4. 용량을 수정하려면 콘솔의 단계를 사용하거나 JSON 파일을 업로드할 수 있습니다.

Console steps

1. 새 Outpost 용량 구성 수정을 선택합니다.
2. 다음을 선택합니다.
3. 인스턴스 용량 구성 페이지에서 각 인스턴스 유형에는 최대 수량이 미리 선택된 인스턴스 크기가 하나씩 표시됩니다. 인스턴스 크기를 더 추가하려면 [Add instance size] 를 선택합니다.
4. 인스턴스 수량을 지정하고 해당 인스턴스 크기에 표시된 용량을 기록해 둡니다.
5. 각 인스턴스 유형 섹션의 끝에서 용량이 초과되었는지 또는 부족한지 알려주는 메시지를 확인하십시오. 인스턴스 크기 또는 수량 수준을 조정하여 총 가용 용량을 최적화하십시오.
6. 특정 인스턴스 크기에 맞게 인스턴스 수량을 AWS Outposts 최적화하도록 요청할 수도 있습니다. 그렇게 하려면 다음을 수행하세요.

   a. 인스턴스 크기를 선택합니다.

   b. 관련 인스턴스 유형 섹션 끝에서 Auto-Balance를 선택합니다.
7. 각 인스턴스 유형에 대해 최소 하나의 인스턴스 크기에 대해 인스턴스 수량을 지정해야 합니다.
8. 다음을 선택합니다.
9. 검토 및 생성 페이지에서 요청하는 업데이트를 확인합니다.
10. 만들기를 선택합니다. AWS Outposts 용량 작업을 생성합니다.
11. 용량 작업 페이지에서 작업 상태를 모니터링합니다.

> **Note**
>
> - AWS Outposts 용량 작업을 실행할 수 있도록 하나 이상의 인스턴스 실행을 중지하도록 요청할 수 있습니다. 이러한 인스턴스를 중지한 후 에서 작업을 실행합니다. AWS Outposts
> - 주문을 완료한 후 용량을 변경해야 하는 경우 AWS Support 문의하여 변경하십시오.

Upload JSON file

1. 용량 구성 업로드를 선택합니다.
2. 다음을 선택합니다.
3. 용량 구성 계획 업로드 페이지에서 인스턴스 유형, 크기, 수량을 지정하는 JSON 파일을 업로드합니다.

   Example

   JSON 파일 예제

```
{
    "RequestedInstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. 용량 구성 계획 섹션에서 JSON 파일의 내용을 검토하십시오.
5. 다음을 선택합니다.
6. 검토 및 생성 페이지에서 요청하는 업데이트를 확인합니다.
7. 만들기를 선택합니다. AWS Outposts 용량 작업을 생성합니다.
8. 용량 작업 페이지에서 작업 상태를 모니터링합니다.

> **Note**
>
> - AWS Outposts 용량 작업을 실행할 수 있도록 하나 이상의 인스턴스 실행을 중지하도록 요청할 수 있습니다. 이러한 인스턴스를 중지한 후 에서 작업을 실행합니다. AWS Outposts
> - 주문을 완료한 후 용량을 변경해야 하는 경우 AWS Support 문의하여 변경하십시오.

다음 단계

AWS Outposts 콘솔을 사용하여 주문 상태를 볼 수 있습니다. 주문의 초기 상태는 주문 접수입니다. AWS 담당자가 영업일 기준 3일 이내에 연락을 드릴 것입니다. 주문 상태가 주문 처리 중으로 변경되면 확인 이메일을 받게 됩니다. AWS 필요한 추가 정보를 얻기 위해 AWS 담당자가 연락을 드릴 수 있습니다.

주문과 관련하여 질문이 있는 경우 문의해 주십시오 AWS Support.

주문을 처리하기 위해 귀하와 함께 날짜와 시간을 정해 드립니다. AWS

설치 전에 확인하거나 제공해야 할 항목의 체크리스트도 받게 됩니다. AWS 설치 팀이 예정된 날짜와 시간에 현장에 도착합니다. 팀이 랙을 지정된 위치로 굴리면 전기 기술자가 랙에 전원을 공급할 수 있습니다. 팀은 고객이 제공하는 업링크를 통해 랙에 대한 네트워크 연결을 설정하고 랙의 용량을 구성합니다. Outpost의 Amazon EC2 및 Amazon EBS 용량을 계정에서 사용할 수 있는지 확인하면 설치가 완료됩니다. AWS

아웃포스트 랙에서 인스턴스를 시작합니다.

Outpost가 설치되고 컴퓨팅 및 스토리지 용량을 사용할 수 있게 되면 리소스를 생성하여 시작할 수 있습니다. Outpost 서브넷을 사용하여 Amazon EC2 인스턴스를 시작하고 Outpost에서 Amazon EBS 볼륨을 생성합니다. Outpost에서 Amazon EBS 볼륨의 로컬 스냅샷을 생성할 수도 있습니다. Linux에 적용할 수 있는 자세한 내용은 Amazon EC2 사용 설명서의 로컬 Amazon EBS 스냅샷을 참조하십시오. AWS Outposts Windows에 적용할 수 있는 자세한 내용은 Amazon EC2 사용 설명서의 로컬 Amazon EBS 스냅샷을 참조하십시오. AWS Outposts

전제 조건

사이트에 Outpost가 설치되어 있어야 합니다. 자세한 내용은 Outpost를 생성하고 Outpost 용량을 주문합니다. 단원을 참조하세요.

Tasks

- 1단계: VPC 생성
- 2단계: 서브넷 및 사용자 지정 라우팅 테이블 만들기
- 3단계: 로컬 게이트웨이 연결 구성
- 4단계: 온프레미스 네트워크 구성
- 5단계: Outpost에서 인스턴스 시작
- 6단계: 연결 테스트

1단계: VPC 생성

AWS 지역 내 모든 VPC를 아웃포스트까지 확장할 수 있습니다. 사용할 수 있는 VPC가 이미 있다면 이 단계를 건너뛰세요.

아웃포스트용 VPC를 만들려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. Outposts 랙과 동일한 지역을 선택하세요.
3. 탐색 창에서 내 VPC를 선택한 다음 VPC 생성을 선택합니다.
4. VPC만 선택하십시오.
5. (선택 사항) 이름 태그에 VPC의 이름을 입력합니다.
6. IPv4 CIDR 블록의 경우 IPv4 CIDR 수동 입력을 선택하고 IPv4 CIDR 텍스트 상자에 VPC의 IPv4 주소 범위를 입력합니다.

   > **Note**
   >
   > 직접 VPC 라우팅을 사용하려면 온프레미스 네트워크에서 사용하는 IP 범위와 겹치지 않는 CIDR 범위를 지정하십시오.

7. IPv6 CIDR 블록의 경우 IPv6 CIDR 차단 없음을 선택합니다.
8. 테넌시의 경우 기본값을 선택합니다.
9. (선택 사항) VPC에 태그를 추가하려면 [Add tag] 를 선택하고 키와 값을 입력합니다.
10. VPC 생성을 선택합니다.

2단계: 서브넷 및 사용자 지정 라우팅 테이블 만들기

Outpost 서브넷을 생성하여 Outpost가 위치한 AWS 지역의 모든 VPC에 추가할 수 있습니다. 이렇게 하면 VPC에 아웃포스트가 포함됩니다. 자세한 정보는 네트워크 구성 요소을 참조하세요.

> **Note**
>
> 다른 AWS 계정사람이 공유한 Outpost 서브넷에서 인스턴스를 시작하는 경우 으로 건너뛰십시오. 5단계: Outpost에서 인스턴스 시작

2a: 아웃포스트 서브넷 생성

아웃포스트 서브넷을 만들려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 서브넷 생성을 선택합니다. Amazon VPC 콘솔에서 서브넷을 생성하도록 리디렉션됩니다. Outpost와 Outpost가 위치한 가용성 영역을 선택합니다.
4. VPC를 선택합니다.
5. 서브넷 설정에서 선택적으로 서브넷의 이름을 지정하고 서브넷의 IP 주소 범위를 지정합니다.
6. 서브넷 생성(Create subnet)을 선택합니다.
7. (선택 사항) Outpost 서브넷을 더 쉽게 식별하려면 서브넷 페이지에서 Outpost ID 열을 활성화합니다. 열을 활성화하려면 환경설정 아이콘을 선택하고 Outpost ID를 선택한 다음 확인을 선택합니다.

2b: 사용자 지정 라우팅 테이블 만들기

다음 절차를 사용하여 로컬 게이트웨이에 대한 라우팅이 포함된 사용자 지정 라우팅 테이블을 생성합니다. 가용 영역 서브넷과 동일한 라우팅 테이블을 사용할 수 없습니다.

사용자 지정 라우팅 테이블을 생성하려면 다음과 같이 하세요.

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

4. (선택 사항) 이름(Name)에 라우팅 테이블의 이름을 입력합니다.
5. VPC에서 VPC를 선택합니다.
6. (선택 사항) 태그를 추가하려면 새 태그 추가(Add new tag)를 선택하고 태그 키와 태그 값을 입력합니다.
7. 라우팅 테이블 생성을 선택합니다.

2c: Outpost 서브넷과 사용자 지정 라우팅 테이블 연결

특정 서브넷에 라우팅 테이블의 경로를 적용하려면 라우팅 테이블을 서브넷과 연결해야 합니다. 라우팅 테이블은 여러 서브넷과 연결될 수 있습니다. 그러나 서브넷은 한 번에 하나의 라우팅 테이블에만 연결할 수 있습니다. 테이블과 명시적으로 연결되지 않은 서브넷은 기본적으로 기본 라우팅 테이블과 암시적으로 연결됩니다.

Outpost 서브넷과 사용자 지정 라우팅 테이블을 연결하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 라우팅 테이블을 선택합니다.
3. [서브넷 연결(Subnet associations)] 탭에서 [서브넷 연결 편집(Edit subnet associations)]을 선택합니다.
4. 라우팅 테이블과 연결할 서브넷에 대한 확인란을 선택합니다.
5. [연결 저장(Save associations)]을 선택합니다.

3단계: 로컬 게이트웨이 연결 구성

로컬 게이트웨이 (LGW) 를 사용하면 Outpost 서브넷과 온프레미스 네트워크를 연결할 수 있습니다. LGW에 대한 자세한 내용은 로컬 게이트웨이를 참조하십시오.

Outposts 서브넷의 인스턴스와 로컬 네트워크 간에 연결을 제공하려면 다음 작업을 완료해야 합니다.

3a. 사용자 지정 로컬 게이트웨이 라우팅 테이블 생성

콘솔을 사용하여 로컬 게이트웨이 (LGW) 에 대한 사용자 지정 라우팅 테이블을 생성할 수 있습니다. AWS Outposts

콘솔을 사용하여 사용자 지정 LGW 라우팅 테이블을 만들려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.

2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 로컬 게이트웨이 라우팅 테이블 생성을 선택합니다.
5. (선택 사항) 이름에 LGW 라우팅 테이블의 이름을 입력합니다.
6. 로컬 게이트웨이에서 로컬 게이트웨이를 선택합니다.
7. 모드에서 온프레미스 네트워크와 통신하기 위한 모드를 선택합니다.

   - 인스턴스의 프라이빗 IP 주소를 사용하려면 직접 VPC 라우팅을 선택합니다.
   - 고객 소유 IP 주소를 사용하려면 CoIP를 선택합니다.
     - (선택 사항) CoIP 풀 및 추가 CIDR 블록 추가 또는 제거

       [CoIP 풀 추가] 새 풀 추가를 선택하고 다음을 수행합니다.
       - 이름에서 CoIP 풀의 이름을 입력합니다.
       - CIDR의 경우, 고객 소유 IP 주소로 구성된 CIDR 블록을 입력합니다.
     - [CIDR 블록 추가] 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.
     - [CoIP 풀 또는 추가 CIDR 블록 제거] CIDR 블록 오른쪽 또는 CoIP 풀 아래에서 제거를 선택합니다.

       최대 10개의 CoIP 풀과 100개의 CIDR 블록을 지정할 수 있습니다.
8. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 새 태그 추가를 선택하고 다음을 수행합니다.

   - 키에서 키 이름을 입력합니다.
   - 값에 키 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
9. 로컬 게이트웨이 라우팅 테이블 생성을 선택합니다.

3b: VPC를 사용자 지정 LGW 라우팅 테이블에 연결

VPC를 LGW 라우팅 테이블에 연결해야 합니다. 기본적으로 연결되지 않습니다.

다음 절차를 사용하여 VPC를 LGW 라우팅 테이블에 연결합니다.

선택적으로 연결에 태그를 지정하여 조직의 필요에 따라 연결을 식별하거나 분류할 수 있습니다.

AWS Outposts console

VPC를 사용자 지정 LGW 라우팅 테이블에 연결하는 방법

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택한 다음 작), VPC 연결을 선택합니다.
5. VPC ID의 경우 로컬 게이트웨이 라우팅 테이블에 연결할 VPC를 선택합니다.
6. (선택) 태그를 추가하거나 제거할 수 있습니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

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

   태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
7. VPC 연결을 선택합니다.

AWS CLI

VPC를 사용자 지정 LGW 라우팅 테이블에 연결하는 방법

create-local-gateway-route-table-route-table-vpc-association 명령을 사용합니다.

예

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

출력

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
```

```
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

3c: Outpost 서브넷 라우팅 테이블에 경로 항목 추가

Outpost 서브넷 라우팅 테이블에 경로 항목을 추가하여 Outpost 서브넷과 LGW 간의 트래픽을 활성화합니다.

Outpost LGW 라우팅 테이블과 연결된 VPC 내의 Outpost 서브넷에는 라우팅 테이블에 대한 Outpost 로컬 게이트웨이 ID라는 추가 대상 유형이 있을 수 있습니다. 목적지 주소가 172.16.100.0/24인 트래픽을 LGW를 통해 고객 네트워크로 라우팅하려는 경우를 생각해 보십시오. 이렇게 하려면 Outpost 서브넷 라우팅 테이블을 편집하고 대상 네트워크 및 LGW () 의 대상이 포함된 다음 경로를 추가하십시오. `lgw-xxxx`

대상 주소	대상
172.16.100.0/24	`lgw-id`

Outpost 서브넷 라우팅 테이블에 **`lgw-id`** 대상으로 하는 경로 항목을 추가하려면:

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Route tables를 선택하고 에서 생성한 라우팅 테이블을 선택합니다. 2b: 사용자 지정 라우팅 테이블 만들기
3. 작업을 선택한 다음 경로 편집을 선택합니다.
4. 라우팅을 추가하려면 라우팅 추가를 선택합니다.
5. 목적지에 고객 네트워크의 대상 CIDR 블록을 입력합니다.
6. Target에서 Outpost 로컬 게이트웨이 ID를 선택합니다.
7. 변경 사항 저장를 선택합니다.

3d: 사용자 지정 LGW 라우팅 테이블을 LGW VIF 그룹과 연결합니다.

VIF 그룹은 VIF(가상 인터페이스)의 논리적 그룹입니다. 로컬 게이트웨이 라우팅 테이블을 VIF 그룹과 연결합니다.

사용자 지정 LGW 라우팅 테이블을 LGW VIF 그룹과 연결하려면

1. https://console.aws.amazon.com/outposts/ 에서 콘솔을 엽니다. AWS Outposts
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.
5. 세부 정보 창에서 VIF 그룹 연결 탭을 선택한 다음 VIF 그룹 연결 편집을 선택합니다.
6. VIF 그룹 설정의 경우 VIF 그룹 연결을 선택하고 VIF 그룹을 선택합니다.
7. 변경 사항 저장를 선택합니다.

3e: LGW 라우팅 테이블에 경로 항목 추가

로컬 게이트웨이 라우팅 테이블을 편집하여 VIF 그룹을 대상으로 하고 온프레미스 서브넷 CIDR 범위 (또는 0.0.0.0/0) 를 대상으로 하는 고정 경로를 추가합니다.

대상 주소	대상
172.16.100.0/24	`VIF-Group-ID`

LGW 라우팅 테이블에 경로 항목을 추가하려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
3. 로컬 게이트웨이 라우팅 테이블을 선택한 다음 작업, 경로 편집을 선택합니다.
4. 라우팅 추가를 선택합니다.
5. 대상에서 대상 CIDR 블록, 단일 IP 주소 또는 접두사 목록의 ID를 입력합니다.
6. 대상에서 로컬 게이트웨이의 ID를 선택합니다.
7. 라우팅 저장을 선택합니다.

3f: (선택 사항) 고객 소유 IP 주소를 인스턴스에 할당

고객 소유 IP (CoIP) 주소 풀을 사용하도록 Outposts를 구성한 경우 CoIP 주소 풀에서 엘라스틱 IP 주소를 할당하고 엘라스틱 IP 주소를 인스턴스에 연결해야 합니다. 3a. 사용자 지정 로컬 게이트웨이 라우팅 테이블 생성 태그에 대한 자세한 내용은 고객 소유 IP 주소 단원을 참조하세요.

Direct VPC 라우팅 (DVR) 을 사용하도록 Outposts를 구성했다면 이 단계를 건너뛰세요.

Amazon VPC console

인스턴스에 CoIP 주소를 할당하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Elastic IPs]를 선택합니다.
3. 탄력적 IP 주소 할당을 선택합니다.
4. 네트워크 경계 그룹에서 IP 주소를 알리는 그룹을 선택합니다.
5. 퍼블릭 IPv4 주소 풀에서 Amazon의 IPv4 주소 풀를 선택합니다.
6. 고객 소유 IPv4 주소 풀에서 구성한 풀을 선택합니다.
7. 할당을 선택합니다.
8. 연결할 탄력적 IP 주소를 선택하고 작업, 탄력적 IP 주소 연결을 선택합니다.
9. 인스턴스에서 인스턴스를 선택한 후 연결을 선택합니다.

AWS CLI

인스턴스에 CoIP 주소를 할당하려면

1. describe-coip-pools 명령을 사용하여 고객 소유 주소 풀에 대한 정보를 검색할 수 있습니다.

```
aws ec2 describe-coip-pools
```

출력의 예제는 다음과 같습니다.

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. Allocate-Address 명령을 사용하여 탄력적 IP 주소를 할당합니다. 이전 단계에서 반환한 풀 ID를 사용합니다.

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

출력의 예제는 다음과 같습니다.

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. associate-address 명령을 사용하여 다음과 같이 탄력력 IP 주소를 Outpost 인스턴스와 연결합니다. 이전 단계에서 반환되는 할당 ID를 사용합니다.

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

출력의 예제는 다음과 같습니다.

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

공유 고객 소유 IP 주소 풀

공유 고객 소유 IP 주소 풀을 사용하려면 구성을 시작하기 전에 풀을 공유해야 합니다. 고객 소유 IPv4 주소를 공유하는 방법에 대한 자세한 내용은 AWS RAM 사용 설명서의 AWS 리소스 공유를 참조하세요.

4단계: 온프레미스 네트워크 구성

Outpost는 각 Outpost 네트워킹 장치 (OND) 에서 고객 로컬 네트워크 장치 (CND) 로의 외부 BGP 피어링을 설정하여 사내 네트워크에서 Outposts로 트래픽을 보내고 받습니다. 자세한 내용은 로컬 게이트웨이 BGP 연결을 참조하십시오.

온프레미스 네트워크에서 Outpost로 트래픽을 보내고 받으려면 다음을 확인하십시오.

- 고객 네트워크 디바이스에서 로컬 게이트웨이 VLAN의 BGP 세션은 네트워크 디바이스에서 활성 상태입니다.
- 온프레미스에서 Outposts로 이동하는 트래픽의 경우 Outposts로부터 BGP 광고를 CND로 수신하고 있는지 확인하십시오. 이러한 BGP 광고에는 온프레미스 네트워크가 온프레미스에서 Outpost로 트래픽을 라우팅하는 데 사용해야 하는 경로가 포함되어 있습니다. 따라서 Outposts와 온프레미스 리소스 간의 네트워크 라우팅이 올바른지 확인하십시오.
- Outposts에서 온프레미스 네트워크로 이동하는 트래픽의 경우 CND가 온프레미스 네트워크 서브넷의 BGP 경로 광고를 Outposts (또는 0.0.0.0/0) 로 전송하는지 확인하십시오. 대안으로 Outposts에 기본 경로 (예: 0.0.0.0/0) 를 알릴 수 있습니다. CND에서 광고하는 온프레미스 서브넷의 CIDR 범위는 구성한 CIDR 범위와 같거나 이에 포함되어야 합니다. 3e: LGW 라우팅 테이블에 경로 항목 추가

예: 다이렉트 VPC 모드의 BGP 광고

Direct VPC 모드로 구성된 Outpost에서 로컬 게이트웨이 VLAN을 통해 두 개의 고객 로컬 네트워크 디바이스에 연결된 Outposts 랙 네트워크 디바이스가 있는 시나리오를 가정해 보겠습니다. 다음과 같이 구성되어 있습니다.

- CIDR 블록 10.0.0.0/16과의 VPC
- CIDR 블록 10.0.3.0/24가 있는 VPC의 아웃포스트 서브넷입니다.
- CIDR 블록 172.16.100.0/24가 있는 온프레미스 네트워크의 서브넷
- Outposts는 Outpost 서브넷에 있는 인스턴스의 프라이빗 IP 주소 (예: 10.0.3.0/24) 를 사용하여 온프레미스 네트워크와 통신합니다.

이 시나리오에서 광고하는 경로는 다음과 같습니다.

- 고객 디바이스의 로컬 게이트웨이는 10.0.3.0/24입니다.
- 아웃포스트 로컬 게이트웨이로 연결되는 고객 디바이스는 172.16.100.0/24입니다.

따라서 로컬 게이트웨이는 대상 네트워크 172.16.100.0/24를 사용하여 고객 디바이스로 아웃바운드 트래픽을 전송합니다. 네트워크 내의 대상 호스트로 트래픽을 전달할 수 있도록 네트워크에 올바른 라우팅 구성이 있는지 확인하십시오.

BGP 세션의 상태와 해당 세션 내의 광고된 경로를 확인하는 데 필요한 특정 명령 및 구성은 네트워킹 공급업체의 설명서를 참조하십시오. 문제 해결은 AWS Outposts 랙 네트워크 문제 해결 체크리스트를 참조하십시오.

예: CoIP 모드의 BGP 광고

Outpost에서 로컬 게이트웨이 VLAN을 통해 두 개의 고객 로컬 네트워크 장치에 연결된 두 개의 Outposts 랙 네트워크 장치가 있는 시나리오를 생각해 보십시오. 다음과 같이 구성되어 있습니다.

- CIDR 블록 10.0.0.0/16과의 VPC
- CIDR 블록 10.0.3.0/24가 있는 VPC의 서브넷입니다.
- 고객 소유 IP 풀(10.1.0.0/26).
- 10.0.3.112를 10.1.0.2에 연결하는 탄력적 IP 주소 연결입니다.
- CIDR 블록이 있는 온프레미스 네트워크의 서브넷 172.16.100.0/24
- Outpost와 온프레미스 네트워크 간의 통신은 CoIP 탄력적 IP를 사용하여 Outpost의 인스턴스를 처리하며, VPC CIDR 범위는 사용되지 않습니다.

이 시나리오에서 경로는 다음과 같이 광고합니다.

- 고객 디바이스의 로컬 게이트웨이는 10.1.0.0/26입니다.
- 아웃포스트 로컬 게이트웨이로 연결되는 고객 디바이스는 172.16.100.0/24입니다.

따라서 로컬 게이트웨이는 대상 네트워크 172.16.100.0/24를 사용하여 고객 장치로 아웃바운드 트래픽을 전송합니다. 네트워크에 네트워크 내의 대상 호스트로 트래픽을 전달할 수 있는 올바른 라우팅 구성이 있는지 확인하십시오.

BGP 세션의 상태와 해당 세션 내의 광고된 경로를 확인하는 데 필요한 특정 명령 및 구성은 네트워킹 공급업체의 설명서를 참조하십시오. 문제 해결은 AWS Outposts 랙 네트워크 문제 해결 체크리스트를 참조하십시오.

5단계: Outpost에서 인스턴스 시작

생성한 Outpost 서브넷 또는 공유된 Outpost 서브넷에서 EC2 인스턴스를 시작할 수 있습니다. 보안 그룹은 가용 영역 서브넷의 인스턴스와 마찬가지로 Outpost 서브넷의 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어합니다. Outpost 서브넷의 EC2 인스턴스에 연결하려면 가용 영역 서브넷의 인스턴스와 마찬가지로 인스턴스를 시작할 때 키 쌍을 지정할 수 있습니다.

고려 사항

- 배치 그룹을 생성하여 Amazon EC2가 Outpost 하드웨어에 상호 종속적인 인스턴스 그룹을 배치하려고 시도하는 방식에 영향을 줄 수 있습니다. 워크로드 요구 사항에 맞는 배치 그룹 전략을 선택할 수 있습니다.

- Outpost가 고객 소유 IP(CoIP) 주소 풀을 사용하도록 구성된 경우, 시작하는 모든 인스턴스에 고객 소유 IP 주소를 할당해야 합니다.

Outpost 서브넷에서 인스턴스를 시작하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 인스턴트 시작을 선택합니다. Amazon EC2 콘솔에서 인스턴스 시작 마법사로 리디렉션됩니다. Outpost 서브넷을 선택하여 Outposts 랙에서 지원하는 인스턴스 유형만 보여줍니다.
5. Outposts 랙에서 지원하는 인스턴스 유형을 선택합니다. 회색으로 표시된 인스턴스는 Outpost에서 사용할 수 없다는 점에 유의하세요.
6. (선택 사항) 인스턴스를 배치 그룹으로 시작하려면 고급 세부 정보를 확장하고 배치 그룹으로 스크롤합니다. 기존 배치 그룹을 선택하거나 새 배치 그룹을 생성할 수 있습니다.
7. 마법사를 완료하여 Outpost 서브넷에서 인스턴스를 시작합니다. 자세한 내용은 Amazon EC2 사용 설명서의 다음 항목을 참조하세요.
   - Linux — 새 인스턴스 시작 마법사를 사용하여 인스턴스를 시작합니다.
   - Windows - 새 시작 인스턴스 마법사를 사용하여 인스턴스를 시작합니다.

> **Note**
>
> Amazon EBS 볼륨을 생성하는 경우 gp2 볼륨 유형을 사용해야 합니다. 그렇지 않으면 마법사가 실패합니다.

6단계: 연결 테스트

적절한 사용 사례를 사용하여 연결을 테스트할 수 있습니다.

로컬 네트워크에서 Outpost로의 연결을 테스트합니다.

로컬 네트워크의 컴퓨터에서 Outpost 인스턴스의 프라이빗 IP 주소로 `ping` 명령을 실행합니다.

```
ping 10.0.3.128
```

출력의 예제는 다음과 같습니다.

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Outpost 인스턴스와 로컬 네트워크 간의 연결을 테스트합니다.

운영 체제에 따라 ssh 또는 rdp를 사용하여 Outpost 인스턴스의 프라이빗 IP 주소에 연결합니다. Linux 인스턴스 연결에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하십시오. Windows 인스턴스 연결에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

인스턴스가 실행된 후 로컬 네트워크에 있는 컴퓨터의 IP 주소로 ping 명령을 실행합니다. 다음 예제에서 IP 주소는 172.16.0.130입니다.

```
ping 172.16.0.130
```

출력의 예제는 다음과 같습니다.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

AWS 지역과 아웃포스트 간의 연결성 테스트

지역의 서브넷에서 AWS 인스턴스를 시작합니다. 예를 들면 run-instances 명령을 실행합니다.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

인스턴스가 실행된 후 다음 작업을 수행합니다.

1. AWS 지역 내 인스턴스의 프라이빗 IP 주소를 가져옵니다. Amazon EC2 콘솔의 인스턴스 세부 정보 페이지에서 이 정보를 확인할 수 있습니다.
2. 운영 체제에 따라 Outpost 인스턴스의 프라이빗 IP 주소로 연결하는 데 ssh 또는 rdp을(를) 사용합니다.
3. AWS 지역 내 인스턴스의 IP 주소를 지정하여 Outpost 인스턴스에서 ping 명령을 실행합니다.

   ```
   ping 10.0.1.5
   ```

   출력의 예제는 다음과 같습니다.

   ```
   Pinging 10.0.1.5

   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.1.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
   ```

고객 소유 IP 주소 연결 예제

로컬 네트워크에서 Outpost로의 연결을 테스트합니다.

로컬 네트워크의 컴퓨터에서 Outpost 인스턴스의 고객 소유 IP 주소로 ping 명령을 실행합니다.

```
ping 172.16.0.128
```

출력의 예제는 다음과 같습니다.

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Outpost 인스턴스와 로컬 네트워크 간의 연결을 테스트합니다.

운영 체제에 따라 ssh 또는 rdp를 사용하여 Outpost 인스턴스의 프라이빗 IP 주소에 연결합니다. Linux 인스턴스 연결에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하십시오. Windows 인스턴스 연결에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

Outpost 인스턴스가 실행된 후 로컬 네트워크에 있는 컴퓨터의 IP 주소로 ping 명령을 실행합니다.

```
ping 172.16.0.130
```

출력의 예제는 다음과 같습니다.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

AWS 지역과 아웃포스트 간의 연결성 테스트

지역의 서브넷에서 AWS 인스턴스를 시작합니다. 예를 들면 run-instances 명령을 실행합니다.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

인스턴스가 실행된 후 다음 작업을 수행합니다.

1. AWS 지역 인스턴스 사설 IP 주소 (예: 10.0.0.5) 를 가져옵니다. Amazon EC2 콘솔의 인스턴스 세부 정보 페이지에서 이 정보를 확인할 수 있습니다.
2. 운영 체제에 따라 ssh 또는 rdp를 사용하여 Outpost 인스턴스의 프라이빗 IP 주소에 연결합니다.
3. Outpost 인스턴스에서 AWS 지역 인스턴스 IP 주소로 ping 명령을 실행합니다.

   ```
   ping 10.0.0.5
   ```

   출력의 예제는 다음과 같습니다.

   ```
   Pinging 10.0.0.5

   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.0.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
   ```

AWS OutpostsAWS 지역과의 연결성

AWS Outposts 서비스 링크 연결을 통해 광역 네트워크 (WAN) 연결을 지원합니다.

내용

- 서비스 링크를 통한 연결
- VPC를 사용한 서비스 링크 프라이빗 연결
- 중복 인터넷 연결

서비스 링크를 통한 연결

서비스 링크는 Outposts와 선택한 AWS 지역 (또는 홈 지역) 간의 필수 연결이며 Outposts를 관리하고 지역을 오가는 트래픽 교환을 가능하게 합니다. AWS 서비스 링크는 암호화된 VPN 연결 세트를 활용하여 홈 지역과 통신합니다.

서비스 링크 연결을 설정하려면 Outpost 프로비저닝 중에 로컬 네트워크 장치와의 물리적, 가상 LAN (VLAN) 및 네트워크 계층 연결을 구성하거나 AWS 구성해야 합니다. 자세한 내용은 랙의 로컬 네트워크 연결 및 Outposts 랙의 사이트 요구 사항을 참조하십시오.

지역에 대한 광역 네트워크 (WAN) 연결의 경우 AWS 지역의 공용 연결을 통해 서비스 링크 VPN 연결을 설정할 AWS Outposts 수 있습니다. AWS 이를 위해서는 Outposts가 공용 인터넷 또는 AWS Direct Connect 공용 가상 인터페이스를 통해 해당 지역의 공용 IP 범위에 액세스할 수 있어야 합니다. 현재 IP 주소 범위는 Amazon VPC 사용 설명서의 AWS IP 주소 범위를 참조하십시오. 이 연결은 서비스 링크 네트워크 계층 경로에서 특정 또는 기본 (0.0.0.0/0) 경로를 구성하여 활성화할 수 있습니다. 자세한 내용은 서비스 링크 BGP 연결 및 서비스 링크 인프라 서브넷 광고 및 IP 범위를 참조하십시오.

또는 Outpost의 사설 연결 옵션을 선택할 수도 있습니다. 자세한 내용은 VPC를 사용한 서비스 링크 프라이빗 연결을 참조하십시오.

서비스 링크 연결이 설정되면 Outpost가 운영되고 에서 관리합니다. AWS서비스 링크는 다음 트래픽에 사용됩니다.

- 아웃포스트와 모든 관련 VPC 간의 고객 VPC 트래픽.
- 리소스 관리, 리소스 모니터링, 펌웨어 및 소프트웨어 업데이트와 같은 관리 트래픽을 아웃포스트합니다.

요구되는 서비스 링크 최대 전송 단위(MTU)

네트워크 연결의 MTU(최대 전송 단위)는 연결을 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. 네트워크는 Outpost와 상위 지역의 서비스 링크 엔드포인트 간 1500바이트 MTU를 지원해야 합니다. AWS 서비스 링크를 통해 Outpost의 인스턴스와 AWS 지역 내 인스턴스 간에 필요한 MTU에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스의 네트워크 최대 전송 단위 (MTU) 를 참조하십시오.

서비스 링크 대역폭 권장 사항

최적의 환경과 탄력성을 위해 지역에 대한 서비스 링크 연결에 최소 500Mbps (1Gbps가 더 좋음) 의 이중 연결을 사용하는 것이 좋습니다. AWS AWS AWS Direct Connect 또는 인터넷 연결을 서비스 링크에 사용할 수 있습니다. 최소 500Mbps의 서비스 링크 연결을 통해 Amazon EC2 인스턴스를 시작하고, Amazon EBS 볼륨을 연결하고, Amazon EKS, Amazon EMR 및 지표와 같은 서비스에 AWS 액세스할 수 있습니다. CloudWatch

Outpost 서비스 링크 대역폭 요구 사항은 다음 특성에 따라 다릅니다.

- 랙 수 및 용량 구성 AWS Outposts
- AMI 크기, 애플리케이션 탄력성, 버스트 속도 요구, 리전으로의 Amazon VPC 트래픽과 같은 워크로드 특성

요구 사항에 필요한 서비스 링크 대역폭에 대한 맞춤형 권장 사항을 받으려면 AWS 영업 담당자 또는 APN 파트너에게 문의하십시오.

방화벽 및 서비스 링크

이 섹션에서는 방화벽 구성 및 서비스 링크 연결에 대해 설명합니다.

다음 다이어그램에서 구성은 Amazon VPC를 지역에서 아웃포스트까지 AWS 확장합니다. AWS Direct Connect 퍼블릭 가상 인터페이스는 서비스 링크 연결입니다. 다음 트래픽은 서비스 링크와 AWS Direct Connect 연결을 거칩니다.

- 서비스 링크를 통해 Outpost로 유입되는 관리 트래픽
- Outpost와 모든 관련 VPC 간의 트래픽

인터넷 연결과 함께 상태 저장 방화벽을 사용하여 공용 인터넷에서 서비스 링크 VLAN으로의 연결을 제한하는 경우 인터넷에서 시작되는 모든 인바운드 연결을 차단할 수 있습니다. 이는 서비스 링크 VPN이 Outpost에서 해당 리전으로만 시작되고 리전에서 Outpost로는 시작되지 않기 때문입니다.

방화벽을 사용하여 서비스 링크 VLAN으로부터의 연결을 제한하는 경우 모든 인바운드 연결을 차단할 수 있습니다. 다음 표에 따라 AWS 지역에서 Outpost로 다시 아웃바운드 연결을 허용해야 합니다. 방화벽이 상태 저장 상태인 경우 Outpost에서 허용된 아웃바운드 연결, 즉 Outpost에서 시작된 연결은 다시 인바운드로 허용되어야 합니다.

프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	443	AWS Outposts 서비스 링크 /26	443	AWS Outposts 지역 공개 노선
TCP	1025-65535	AWS Outposts 서비스 링크 /26	443	AWS Outposts 지역 공개 노선

> **Note**
>
> Outpost의 인스턴스는 서비스 링크를 사용하여 다른 Outpost의 인스턴스와 통신할 수 없습니다. 로컬 게이트웨이 또는 로컬 네트워크 인터페이스를 통한 라우팅을 활용하여 Outpost 간에 통신할 수 있습니다.
>
> AWS Outposts 또한 랙은 로컬 게이트웨이 구성 요소를 포함한 이중 전원 및 네트워킹 장비로 설계되었습니다. 자세한 내용은 Resilience in을 참조하십시오. AWS Outposts

VPC를 사용한 서비스 링크 프라이빗 연결

Outpost를 생성할 때 콘솔에서 프라이빗 연결 옵션을 선택할 수 있습니다. 이렇게 하면 지정한 VPC와 서브넷을 사용하여 Outpost를 설치한 후에 서비스 링크 VPN 연결이 설정됩니다. 이를 통해 VPC를 통한 프라이빗 연결이 가능하고 공용 인터넷 노출을 최소화합니다.

필수 조건

Outpost의 프라이빗 연결을 구성하려면 다음 사전 요구 사항이 필요합니다.

- 사용자 또는 역할이 서비스 링크 역할을 생성하거나 편집할 수 있도록 IAM 엔터티(사용자 또는 역할)의 권한을 구성해야 합니다. IAM 엔터티에는 다음 작업에 액세스할 수 있는 권한이 필요합니다.
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`의 `iam:CreateServiceLinkedRole`
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`의 `iam:PutRolePolicy`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

  자세한 내용은 ID 및 액세스 관리 (IAM) 에 대한 AWS Outposts 및 AWS Outposts의 서비스 링크 역할 사용 섹션을 참조하세요.
- Outpost와 동일한 AWS 계정 및 가용 영역에서 10.1.0.0/16과 충돌하지 않는 /25 이상의 서브넷을 사용하여 Outpost 프라이빗 연결만을 위한 VPC를 생성하십시오. 예를 들어 10.2.0.0/16을 사용할 수 있습니다.
- 온프레미스 Outpost가 VPC에 액세스할 수 있도록 AWS Direct Connect 연결, 프라이빗 가상 인터페이스, 가상 프라이빗 게이트웨이를 생성합니다. VPC와 다른 AWS 계정에 연결되어 있는 경우 사용 설명서의 AWS Direct Connect 계정 간 가상 프라이빗 게이트웨이 AWS Direct Connect 연결을 참조하십시오.
- 온프레미스 네트워크에 서브넷 CIDR을 알립니다. 이렇게 AWS Direct Connect 하는 데 사용할 수 있습니다. 자세한 내용은 AWS Direct Connect 사용 설명서의 AWS Direct Connect 가상 인터페이스 및 AWS Direct Connect 게이트웨이 사용을 참조하세요.

AWS Outposts 콘솔에서 Outpost를 만들 때 프라이빗 연결 옵션을 선택할 수 있습니다. 지침은 Outpost를 생성하고 Outpost 용량을 주문합니다.을(를) 참조하세요.

> **Note**
>
> Outpost가 PENDING 상태일 때 프라이빗 연결 옵션을 선택하려면 콘솔에서 Outposts를 선택하고 사용자의 Outpost를 선택합니다. 작업, 프라이빗 연결 추가를 선택하고 단계를 따르세요.

Outpost의 개인 연결 옵션을 선택하면 Outpost에서 사용자를 대신하여 다음 작업을 완료할 수 있는 서비스 연결 역할이 계정에 AWS Outposts 자동으로 생성됩니다.

- 지정한 서브넷과 VPC에서 네트워크 인터페이스를 만들고 네트워크 인터페이스에 대한 보안 그룹을 만듭니다.

- 계정에 네트워크 인터페이스를 계정의 AWS Outposts 서비스 링크 엔드포인트 인스턴스에 연결할 수 있는 권한을 서비스에 부여합니다.
- 네트워크 인터페이스를 계정의 서비스 링크 엔드포인트 인스턴스에 연결합니다.

서비스 링크 역할에 대한 자세한 내용은 AWS Outposts의 서비스 링크 역할 사용을(를) 참조하세요.

> **Important**
>
> Outpost를 설치한 후 Outpost에서 서브넷의 프라이빗 IP에 연결되었는지 확인합니다.

중복 인터넷 연결

Outpost에서 AWS 지역으로 연결을 구축할 때는 가용성과 복원력을 높이기 위해 여러 연결을 만드는 것이 좋습니다. 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하세요.

공용 인터넷에 연결해야 하는 경우, 기존 온프레미스 워크로드와 마찬가지로 중복 인터넷 연결과 다양한 인터넷 공급자를 사용할 수 있습니다.

Outpost 및 사이트

에 대한 아웃포스트 및 사이트 관리. AWS Outposts

조직의 요구에 따라 리소스를 식별하거나 분류하는 데 유용하도록 Outpost를 태그할 수 있습니다. 태깅에 대한 자세한 내용은 가이드의 AWS 리소스 태깅을 참조하십시오.AWS 일반 참조

주제

- Outpost 관리
- Outpost 사이트 관리

Outpost 관리

AWS Outposts Outposts라고 하는 하드웨어 및 가상 리소스를 포함합니다. 이 섹션을 사용하여 이름 변경, 세부 정보 또는 태그 추가 또는 보기 등의 Outpost를 생성하고 관리할 수 있습니다.

Outpost를 생성하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 Outposts를 선택합니다.
4. Outpost 생성을 선택합니다.
5. 이 Outpost의 하드웨어 유형을 선택합니다.
6. Outpost에 대한 이름과 설명을 입력합니다.
7. Outpost의 가용 영역을 선택합니다.
8. (선택 사항) 프라이빗 연결 옵션을 선택합니다. VPC 및 서브넷의 경우 Outpost와 동일한 AWS 계정 및 가용 영역에 있는 VPC와 서브넷을 선택합니다.

   > **Note**
   >
   > Outpost의 프라이빗 연결을 취소해야 하는 경우, AWS Enterprise Support에 문의해야 합니다.

9. 사이트 ID에서, 다음 중 하나를 수행합니다.

   - 기존 사이트를 선택하려면 해당 사이트를 선택합니다.

- 새 사이트를 생성하려면 사이트 생성을 선택하고 다음를 클릭한 다음, 새 창에 사이트에 대한 정보를 입력합니다.

  사이트를 만든 후 이 창으로 돌아가서 사이트를 선택합니다. 새 사이트를 보려면 사이트 목록을 새로 고쳐야 할 수 있습니다. 데이터를 새로 고치려면 새로고침 아이콘 () 을 선택합니다.

  자세한 내용은 the section called “사이트”을(를) 참조하세요.

10. Outpost 생성을 선택합니다.

> **Tip**
>
> 새 Outpost에 용량을 추가하려면 주문을 해야 합니다.

다음 단계를 사용하여 Outpost의 이름과 설명을 편집하세요.

Outpost 이름 및 설명을 편집하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 콘솔을 엽니다. AWS Outposts
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 Outposts를 선택합니다.
4. Outpost를 선택하고 작업 및 편집를 선택합니다.
5. 이름과 설명을 수정합니다.

   이름에서 이름을 입력합니다.

   설명의 경우, 설명을 입력합니다.
6. 변경 사항 저장을 선택합니다.

다음 단계에 따라 Outpost에 대한 세부 정보를 봅니다.

Outpost의 세부 정보를 보려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전

3. 탐색 창에서 Outposts를 선택합니다.
4. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.

를 사용하여 Outpost 세부 정보를 볼 수도 있습니다. AWS CLI

다음을 사용하여 전초 기지 세부 정보를 보려면 AWS CLI

- AWS CLI get-outpost 명령을 사용하세요.

다음 단계를 사용하여 Outpost의 태그를 관리합니다.

Outpost 태그를 관리하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 Outposts를 선택합니다.
4. Outpost를 선택한 다음, 작업, 태그 관리를 선택합니다.
5. 태그를 추가하거나 제거합니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

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

   태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
6. 변경 사항 저장을 선택합니다.

Outpost 사이트 관리

Outpost를 설치할 고객 관리 물리적 건물. AWS 사이트는 Outpost에 대한 시설, 네트워킹 및 전원 요구 사항을 충족해야 합니다. 자세한 내용은 Outposts 랙 요구 사항을(를) 참조하세요.

Outpost 사이트를 생성하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전

3. 탐색 창에서 사이트를 선택합니다.
4. 사이트 생성을 선택합니다.
5. 사이트에 대해 지원되는 하드웨어 유형을 선택합니다.
6. 사이트에 대한 이름, 설명, 운영 주소를 입력합니다. 사이트에서 랙을 지원하기로 선택한 경우, 다음 정보를 입력합니다.

   - 최대 무게 - 이 사이트에서 지원할 수 있는 최대 랙 무게를 지정합니다.
   - 전력 소비량 - 랙의 하드웨어 배치 위치에서 사용할 수 있는 전력 소비량을 kVA 단위로 지정합니다.
   - 전원 옵션 - 하드웨어에 제공할 수 있는 전원 옵션을 지정합니다.
   - 전원 커넥터 - 하드웨어 연결에 사용할 전원 커넥터를 지정하십시오. AWS
   - 전력 공급 제공 - 전력 공급 장치가 랙 위쪽인지 아래인지 지정합니다.
   - 업링크 속도 - 랙이 리전 연결에 대해 지원해야 하는 업링크 속도를 지정합니다.
   - 업링크 수 - 랙을 네트워크에 연결하는 데 사용할 각 Outpost 네트워크 장치의 업링크 수를 지정합니다.
   - 파이버 유형 - Outpost를 네트워크에 연결하는 데 사용할 파이버 유형을 지정합니다.
   - 광학 표준 - Outpost를 네트워크에 연결하는 데 사용할 광학 표준 유형을 지정합니다.
   - 참고 – 사이트에 대한 메모를 지정합니다.
7. 시설 요구 사항을 읽고 시설 요구 사항을 읽었습니다를 선택합니다.
8. 사이트 생성을 선택합니다.

Outpost 사이트를 편집하려면 다음 단계를 사용합니다.

사이트를 편집하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 사이트를 선택합니다.
4. 사이트를 선택한 다음 작업, 사이트 편집을 선택합니다.
5. 이름, 설명, 운영 주소 및 사이트 세부 정보를 수정할 수 있습니다.

   운영 주소를 변경하는 경우, 변경 사항이 기존 주문에는 적용되지 않는다는 점에 유의하십시오.
6. 변경 사항 저장을 선택합니다.

Outpost 사이트의 세부 정보를 보려면 다음 단계를 사용합니다.

사이트 세부 정보를 보려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 사이트를 선택합니다.
4. 사이트를 선택한 다음 작업, 세부 정보 보기를 선택합니다.

Outpost 사이트에서 태그를 관리하려면 다음 단계를 사용합니다.

사이트 태그를 관리하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 사이트를 선택합니다.
4. 사이트를 선택한 다음 작업, 태그 관리를 선택합니다.
5. 태그를 추가하거나 제거합니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

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

   태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
6. 변경 사항 저장을 선택합니다.

로컬 게이트웨이

로컬 게이트웨이는 Outpost 아키텍처의 핵심 구성 요소입니다. 로컬 게이트웨이는 Outpost 서브넷과 온프레미스 네트워크를 연결할 수 있게 해줍니다. 온프레미스 인프라에서 인터넷 액세스를 제공하는 경우 Outpost에서 실행되는 워크로드는 로컬 게이트웨이를 활용하여 리전 서비스 또는 리전 워크로드와 통신할 수도 있습니다. 이 연결은 공용 연결(인터넷)을 사용하거나 Direct Connect를 사용하여 수행할 수 있습니다. 자세한 내용은 AWS OutpostsAWS 지역과의 연결성 단원을 참조하세요.

목차

- 로컬 게이트웨이 기본 사항
- 라우팅
- 로컬 게이트웨이를 통한 연결
- 로컬 게이트웨이 라우팅 테이블

로컬 게이트웨이 기본 사항

각 Outpost는 단일 로컬 게이트웨이를 지원합니다. 로컬 게이트웨이의 구성 요소는 다음과 같습니다.

- 라우팅 테이블 – 로컬 게이트웨이 라우팅 테이블을 생성하는 데 사용합니다. 자세한 내용은 the section called “로컬 게이트웨이 라우팅 테이블” 단원을 참조하세요.
- CoIP 풀 - (선택 사항) 소유한 IP 주소 범위를 사용하여 온프레미스 네트워크와 VPC의 인스턴스 간 통신을 원활하게 할 수 있습니다. 자세한 정보는 the section called “고객 소유 IP 주소”을 참조하세요.
- 가상 인터페이스 (VIF) — 각 LAG에 대해 하나의 VIF를 AWS 생성하고 두 VIF를 VIF 그룹에 추가합니다. 로컬 네트워크 연결을 위해 로컬 게이트웨이 라우팅 테이블에는 두 VIFs에 대한 기본 경로가 있어야 합니다. 자세한 정보는 로컬 네트워크 연결을 참조하세요.
- VIF 그룹 연결 — 생성한 VIF를 VIF 그룹에 AWS 추가합니다. VIF 그룹은 VIFs를 논리적으로 그룹화한 것입니다. 자세한 내용은 the section called “VIF 그룹 연결” 단원을 참조하세요.
- VPC 연결 – VPC 및 로컬 게이트웨이 라우팅 테이블과의 VPC 연결을 생성하는 데 사용합니다. Outpost에 있는 서브넷과 연결된 VPC 라우팅 테이블은 로컬 게이트웨이를 라우팅 대상으로 사용할 수 있습니다. 자세한 정보는 the section called “VPC 연결”을 참조하세요.

Outpost 랙을 준비하면 AWS 일부 구성 요소가 만들어지고 나머지 구성 요소는 사용자가 직접 제작합니다.

AWS 책임

- 하드웨어를 제공합니다.
- 로컬 게이트웨이를 생성합니다.
- 가상 인터페이스(VIF)와 VIF 그룹을 생성합니다.

귀하의 책임

- 로컬 게이트웨이 라우팅 테이블을 생성합니다.
- VPC를 게이트웨이 라우팅 테이블과 연결
- VIF 그룹을 로컬 게이트웨이 라우팅 테이블과 연결

라우팅

Outpost 서브넷의 인스턴스는 로컬 게이트웨이를 통해 온프레미스 네트워크와 통신하기 위해 다음 옵션 중 하나를 사용할 수 있습니다.

- 프라이빗 IP 주소 - 로컬 게이트웨이는 Outpost 서브넷에 있는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와의 통신을 용이하게 합니다. 이 값이 기본값입니다.
- 고객 소유 IP 주소 - 로컬 게이트웨이는 Outpost 서브넷의 인스턴스에 할당하는 고객 소유 IP 주소에 대해 네트워크 주소 변환(NAT)을 수행합니다. 이 옵션은 중복되는 CIDR 범위 및 기타 네트워크 토폴로지를 지원합니다.

자세한 내용은 the section called “로컬 게이트웨이 라우팅 테이블” 단원을 참조하세요.

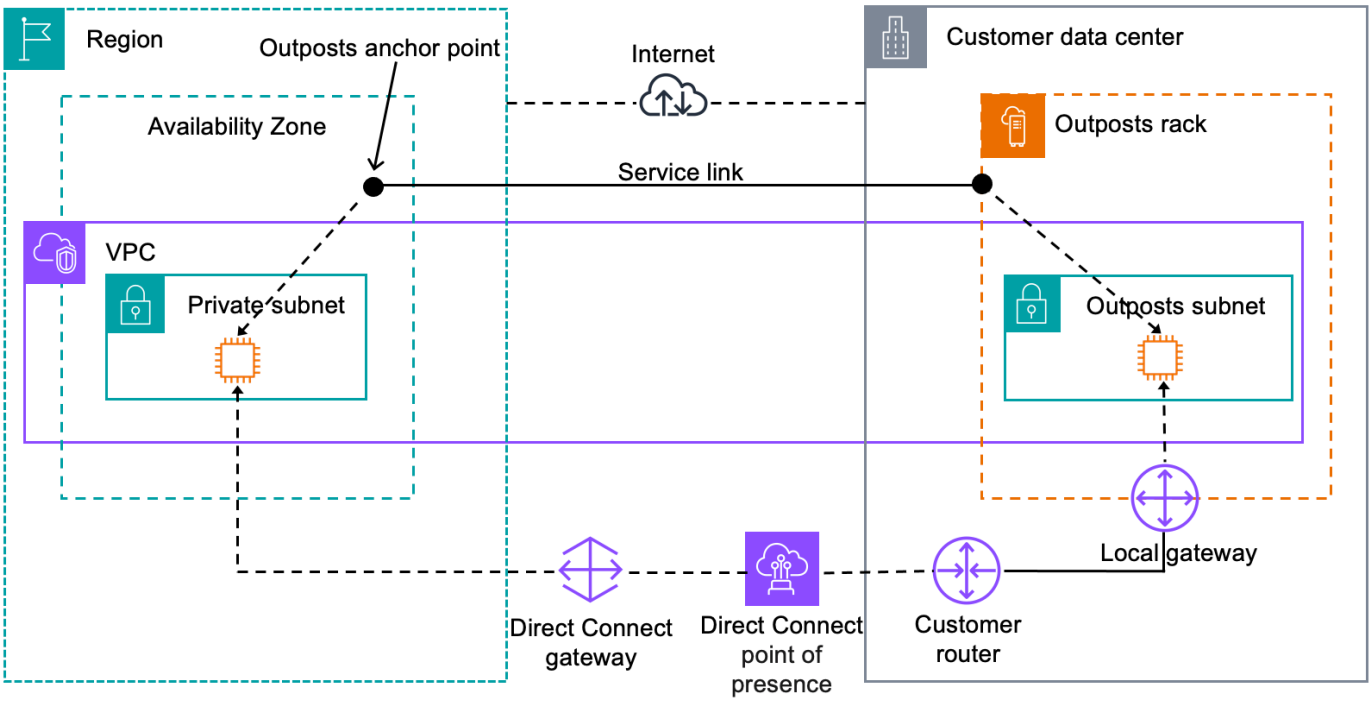
로컬 게이트웨이를 통한 연결

로컬 게이트웨이의 기본 역할은 Outpost에서 로컬 온프레미스 네트워크로의 연결을 제공하는 것입니다. 온프레미스 네트워크를 통해 인터넷에 대한 연결도 제공합니다. 예제는 the section called “직접 VPC 라우팅” 및 the section called “고객 소유 IP 주소” 단원을 참조하세요.

로컬 게이트웨이는 AWS 지역으로 돌아가는 데이터 플레인 경로를 제공할 수도 있습니다. 로컬 게이트웨이의 데이터 플레인 경로는 Outpost에서 로컬 게이트웨이를 거쳐 프라이빗 로컬 게이트웨이 LAN 세그먼트를 통과합니다. 그러면 사설 경로를 따라 해당 리전의 AWS 서비스 엔드포인트로 돌아가게 됩니다. 컨트롤 플레인 경로는 사용하는 데이터 플레인 경로에 관계없이 항상 서비스 링크 연결을 사용한다는 점에 유의하십시오.

온-프레미스 Outposts 인프라를 해당 지역에 AWS 서비스 비공개로 연결할 수 있습니다. AWS Direct Connect프라이빗 콘텐츠에 대한 자세한 내용은 AWS Outposts 프라이빗 연결을 참조하세요.

다음 이미지는 로컬 게이트웨이를 통한 연결을 보여줍니다.



로컬 게이트웨이 라우팅 테이블

랙의 Outpost 서브넷 라우팅 테이블에는 온프레미스 네트워크에 대한 경로가 포함될 수 있습니다. 로컬 게이트웨이는 지연 시간이 짧은 라우팅을 위해 이 트래픽을 온프레미스 네트워크로 라우팅합니다.

기본적으로 Outpost는 Outpost에 있는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와 통신합니다. 이를 AWS Outposts의 직접 VPC 라우팅(또는 직접 VPC 라우팅)이라고 합니다. 하지만 고객 소유 IP 주소 풀(CoIP)이라는 주소 범위를 제공하고 네트워크의 인스턴스가 해당 주소를 사용하여 온프레미스 네트워크와 통신하도록 할 수 있습니다. 직접 VPC 라우팅과 CoIP는 상호 배타적인 옵션이며, 라우팅은 선택에 따라 다르게 작동합니다.

내용

- 직접 VPC 라우팅
- 고객 소유 IP 주소
- 로컬 게이트웨이 라우팅 테이블 사용

직접 VPC 라우팅

다이렉트 VPC 라우팅은 VPC에 있는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와의 통신을 용이하게 합니다. 이 주소는 BGP를 통해 온프레미스 네트워크에 알려집니다. BGP 광고는 Outpost 랙의 서브넷에 속하는 프라이빗 IP 주소에만 해당됩니다. 이 유형의 라우팅은 Outpost의 기본 모드입니다. 이 모드에서는 로컬 게이트웨이가 인스턴스에 대해 NAT를 수행하지 않으므로 EC2 인스턴스에 탄력적 IP 주소를 배정할 필요가 없습니다. 직접 VPC 라우팅 모드 대신 자체 주소 공간을 사용할 수 있습니다. 자세한 내용은 고객 소유 IP 주소 단원을 참조하세요.

직접 VPC 라우팅은 인스턴스 네트워크 인터페이스에만 지원됩니다. 사용자를 대신하여 AWS 생성하는 네트워크 인터페이스 (요청자 관리 네트워크 인터페이스라고 함) 를 사용하면 온프레미스 네트워크에서 해당 사설 IP 주소에 연결할 수 없습니다. 예를 들어 온프레미스 네트워크에서 VPC 엔드포인트로 직접 연결할 수 없습니다.

다음 예는 직접 VPC 라우팅을 설명합니다.

예제

- 예시: VPC를 통한 인터넷 연결
- 예: 온프레미스 네트워크를 통한 인터넷 연결

예시: VPC를 통한 인터넷 연결

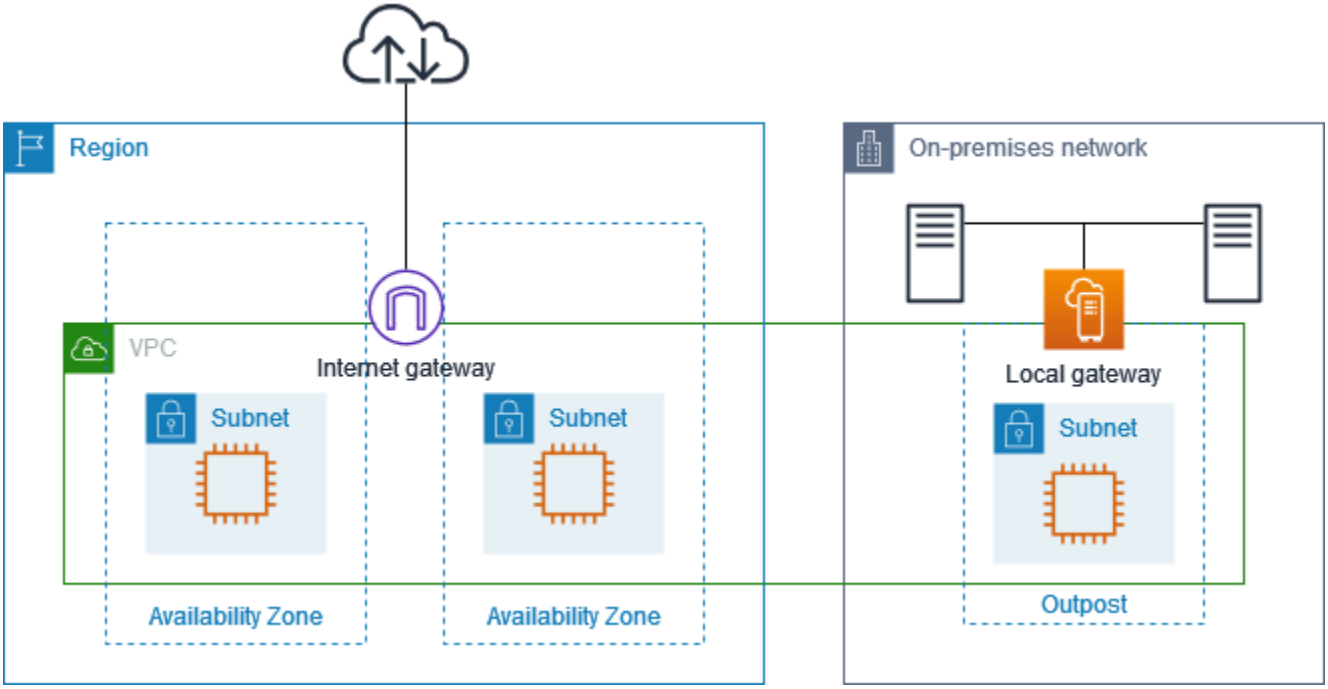
Outpost 서브넷의 인스턴스는 VPC에 연결된 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있습니다.

다음 구성을 고려합니다.

- 상위 VPC는 2개의 가용 영역에 걸쳐 있으며 각 가용 영역에 서브넷이 있습니다.
- Outpost에는 하나의 서브넷이 있습니다.
- 각 서브넷에는 EC2 인스턴스가 있습니다.
- 로컬 게이트웨이는 BGP 광고를 사용하여 Outpost 서브넷의 프라이빗 IP 주소를 온프레미스 네트워크에 알립니다.

> **Note**
>
> BGP 광고는 로컬 게이트웨이를 대상으로 하는 경로가 있는 Outpost의 서브넷에만 지원됩니다. 다른 서브넷은 BGP를 통해 광고되지 않습니다.

다음 다이어그램에서 Outpost 서브넷의 인스턴스에서 나오는 트래픽은 VPC의 인터넷 게이트웨이를 사용하여 인터넷에 액세스할 수 있습니다.



상위 리전을 통해 인터넷에 연결하려면 Outpost 서브넷의 라우팅 테이블에 다음 경로가 있어야 합니다.

대상	대상	설명
VPC CIDR	로컬	VPC의 서브넷 간 연결을 제공합니다.
0.0.0.0	*internet-gateway-id*	인터넷을 대상으로 하는 트래픽을 인터넷 게이트웨이로 전송합니다.
##### #### CIDR	*local-gateway-id*	온프레미스 네트워크로 향하는 트래픽을 로컬 게이트웨이로 보냅니다.

예: 온프레미스 네트워크를 통한 인터넷 연결

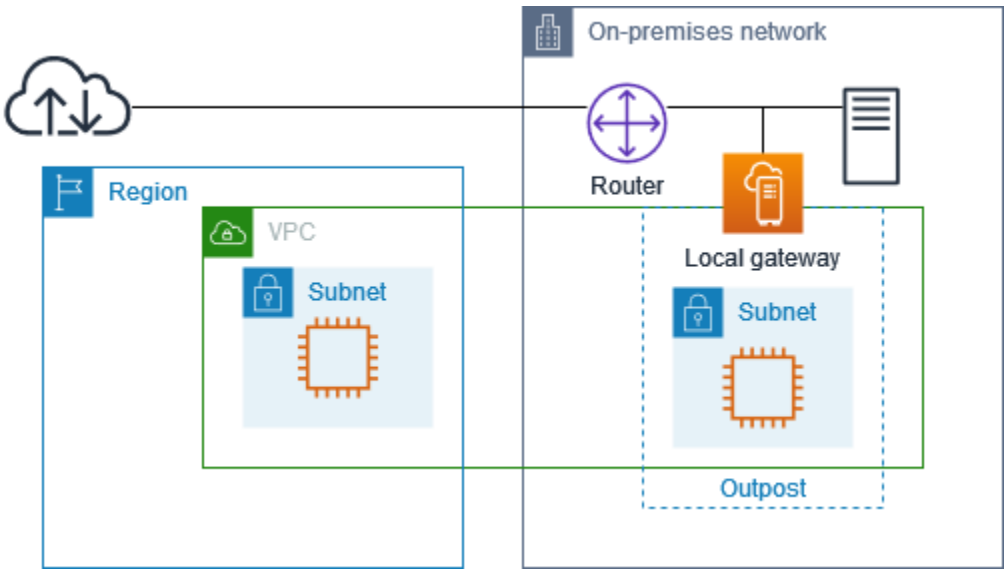
Outpost 서브넷의 인스턴스는 온프레미스 네트워크를 통해 인터넷에 액세스할 수 있습니다. Outpost 서브넷의 인스턴스에는 공용 IP 주소나 탄력적 IP 주소가 필요하지 않습니다.

다음 구성을 고려합니다.

- Outpost 서브넷에는 EC2 인스턴스가 있습니다.
- 온프레미스 네트워크의 라우터는 Network Address Translation(NAT)를 수행합니다.
- 로컬 게이트웨이는 BGP 광고를 사용하여 Outpost 서브넷의 프라이빗 IP 주소를 온프레미스 네트워크에 알립니다.

> **Note**
>
> BGP 광고는 로컬 게이트웨이를 대상으로 하는 경로가 있는 Outpost의 서브넷에만 지원됩니다. 다른 서브넷은 BGP를 통해 광고되지 않습니다.

다음 다이어그램에서 Outpost 서브넷의 인스턴스에서 나오는 트래픽은 로컬 게이트웨이를 사용하여 인터넷 또는 온프레미스 네트워크에 액세스할 수 있습니다. 온프레미스 네트워크의 트래픽은 로컬 게이트웨이를 사용하여 Outpost 서브넷의 인스턴스에 액세스합니다.



온프레미스 네트워크를 통해 인터넷에 연결하려면 Outpost 서브넷의 라우팅 테이블에 다음과 같은 경로가 있어야 합니다.

대상 주소	대상	설명	
VPC CIDR	로컬	VPC의 서브넷 간 연결을 제공합니다.	
0.0.0.0/0	*local-gateway-id*	인터넷으로 향하는 트래픽을 로컬 게이트웨이로 보냅니다.	

인터넷에 대한 아웃바운드 액세스

대상이 인터넷인 Outpost 서브넷의 인스턴스에서 시작된 트래픽은 0.0.0.0/0 경로를 사용하여 트래픽을 로컬 게이트웨이로 라우팅합니다. 로컬 게이트웨이는 라우터로 트래픽을 전송합니다. 라우터는 NAT를 사용하여 프라이빗 IP 주소를 라우터의 공용 IP 주소로 변환한 다음 트래픽을 대상으로 보냅니다.

온프레미스 네트워크에 대한 아웃바운드 액세스

온프레미스 네트워크 대상이 있는 Outpost 서브넷의 인스턴스에서 시작된 트래픽은 0.0.0.0/0의 경로를 사용하여 트래픽을 로컬 게이트웨이로 라우팅합니다. 로컬 게이트웨이는 온프레미스 네트워크의 대상으로 트래픽을 보냅니다.

온프레미스 네트워크를 통한 인바운드 액세스

Outpost 서브넷의 인스턴스 목적지가 있는 온프레미스 네트워크에서 들어오는 트래픽은 인스턴스의 프라이빗 IP 주소를 사용합니다. 트래픽이 로컬 게이트웨이에 도달하면 로컬 게이트웨이는 VPC의 목적지로 트래픽을 보냅니다.

고객 소유 IP 주소

기본적으로 로컬 게이트웨이는 온프레미스 네트워크와의 통신을 용이하게 하기 위해 VPC에 있는 인스턴스의 프라이빗 IP 주소를 사용합니다. 하지만 중복되는 CIDR 범위 및 기타 네트워크 토폴로지를 지원하는 고객 소유 IP 주소 풀(CoIP)이라는 주소 범위를 제공할 수 있습니다.

CoIP를 선택하는 경우 주소 풀을 생성하여 로컬 게이트웨이 라우팅 테이블에 할당하고 BGP를 통해 이러한 주소를 고객 네트워크에 다시 알려야 합니다. 로컬 게이트웨이 라우팅 테이블과 연결된 모든 고객 소유 IP 주소는 라우팅 테이블에 전파된 경로로 표시됩니다.

고객 소유 IP 주소(CoIP)는 온프레미스 네트워크를 통해 Outpost 서브넷의 리소스에 대한 로컬 또는 외부 연결을 제공합니다. 고객 소유 IP 풀에서 새 탄력적 IP 주소를 할당한 다음 리소스에 할당하여 Outpost의 리소스(예: EC2 인스턴스)에 이러한 IP 주소를 할당할 수 있습니다. 자세한 내용은 the section called “3f: (선택 사항) 고객 소유 IP 주소를 인스턴스에 할당”을(를) 참조하세요.

고객 소유 IP 주소 풀에는 다음 요구 사항이 적용됩니다.

- 네트워크에서 주소를 라우팅할 수 있어야 합니다.
- CIDR 블록은 최소 /26이어야 합니다.

고객 소유 IP 주소 풀에서 탄력적 IP 주소를 할당하면 고객 소유 IP 주소 풀의 IP 주소를 계속 소유하게 됩니다. 필요에 따라 내부 네트워크 또는 WAN에 이를 광고할 책임은 귀하에게 있습니다.

를 사용하여 조직 내 여러 사람과 고객 소유 풀을 공유할 수도 있습니다. AWS 계정 AWS Resource Access Manager풀을 공유한 후 참가자는 고객 소유 IP 주소 풀에서 탄력적 IP 주소를 할당한 다음 Outpost의 EC2 인스턴스에 할당할 수 있습니다. 자세한 내용은 AWS RAM 사용 설명서의 AWS 리소스 공유를 참조하세요.

예제

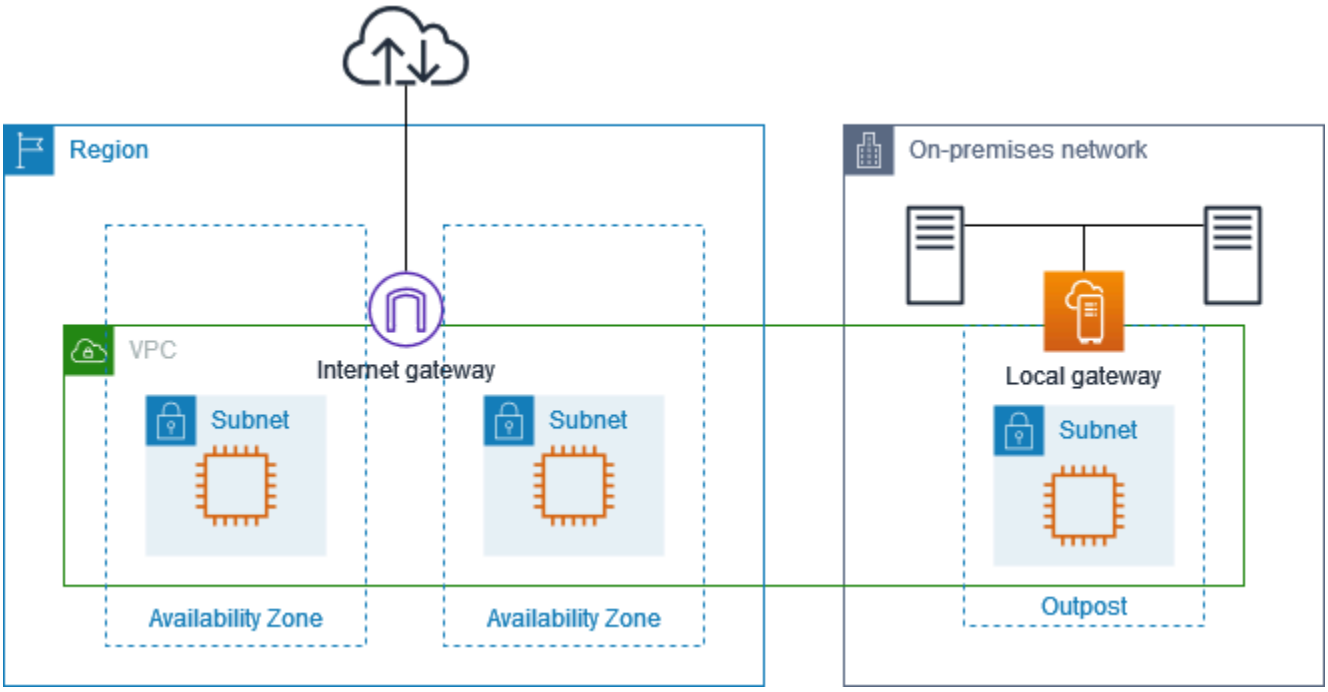
- 예시: VPC를 통한 인터넷 연결
- 예: 온프레미스 네트워크를 통한 인터넷 연결

예시: VPC를 통한 인터넷 연결

Outpost 서브넷의 인스턴스는 VPC에 연결된 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있습니다.

다음 구성을 고려합니다.

- 상위 VPC는 2개의 가용 영역에 걸쳐 있으며 각 가용 영역에 서브넷이 있습니다.
- Outpost에는 하나의 서브넷이 있습니다.
- 각 서브넷에는 EC2 인스턴스가 있습니다.
- 고객 소유의 IP 주소 풀이 있습니다.
- Outpost 서브넷의 인스턴스에는 고객 소유 IP 주소 풀의 탄력적 IP 주소가 있습니다.
- 로컬 게이트웨이는 BGP 광고를 사용하여 고객 소유 IP 주소 풀을 온프레미스 네트워크에 알립니다.



리전을 통해 인터넷에 연결하려면 Outpost 서브넷의 라우팅 테이블에 다음 경로가 있어야 합니다.

대상 주소	대상	설명
VPC CIDR	로컬	VPC의 서브넷 간 연결을 제공합니다.
0.0.0.0	*internet-gateway-id*	공용 인터넷을 대상으로 하는 트래픽을 인터넷 게이트웨이로 보냅니다.
##### #### CIDR	*local-gateway-id*	온프레미스 네트워크로 향하는 트래픽을 로컬 게이트웨이로 보냅니다.

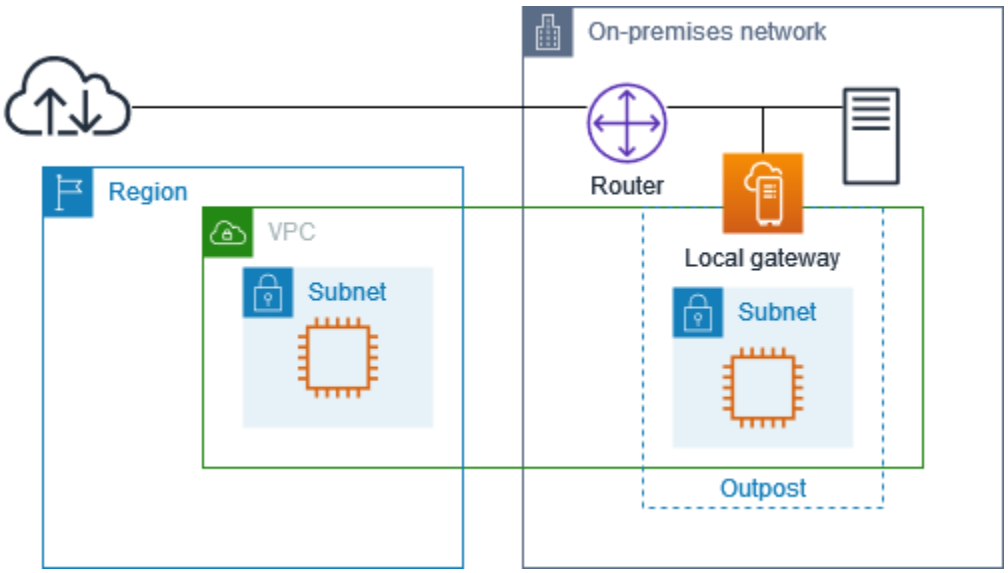
예: 온프레미스 네트워크를 통한 인터넷 연결

Outpost 서브넷의 인스턴스는 온프레미스 네트워크를 통해 인터넷에 액세스할 수 있습니다.

다음 구성을 고려합니다.

- Outpost 서브넷에는 EC2 인스턴스가 있습니다.
- 고객 소유의 IP 주소 풀이 있습니다.
- 로컬 게이트웨이는 BGP 광고를 사용하여 고객 소유 IP 주소 풀을 온프레미스 네트워크에 알립니다.
- 10.0.3.112를 10.1.0.2로 매핑하는 탄력적 IP 주소 연결입니다.

- 고객 온프레미스 네트워크의 라우터는 NAT를 수행합니다.



로컬 게이트웨이를 통해 인터넷에 연결하려면 Outpost 서브넷의 라우팅 테이블에 다음 경로가 있어야 합니다.

대상 주소	대상	설명
VPC CIDR	로컬	VPC의 서브넷 간 연결을 제공합니다.
0.0.0.0/0	*local-gateway-id*	인터넷으로 향하는 트래픽을 로컬 게이트웨이로 보냅니다.

인터넷에 대한 아웃바운드 액세스

Outpost 서브넷의 EC2 인스턴스에서 시작된 트래픽은 인터넷 대상으로 하는 Outpost 서브넷의 EC2 인스턴스에서 시작된 트래픽은 0.0.0.0/0 에 대한 라우팅을 수행합니다. 로컬 게이트웨이는 인스턴스의 프라이빗 IP 주소를 고객 소유 IP 주소에 매핑한 다음 트래픽을 라우터로 보냅니다. 라우터는 NAT를 사용하여 고객 소유 IP 주소를 라우터의 공용 IP 주소로 변환한 다음 트래픽을 대상으로 보냅니다.

온프레미스 네트워크에 대한 아웃바운드 액세스

온프레미스 네트워크가 목적지인 Outpost 서브넷의 EC2 인스턴스에서 시작된 트래픽은 0.0.0.0/0의 경로를 사용하여 트래픽을 로컬 게이트웨이로 라우팅합니다. 로컬 게이트웨이는 EC2 인스턴스의 IP 주소를 고객 소유 IP 주소(탄력적 IP 주소)로 변환한 다음 목적지로 트래픽을 보냅니다.

온프레미스 네트워크를 통한 인바운드 액세스

Outpost 서브넷의 인스턴스 목적지가 있는 온프레미스 네트워크에서 들어오는 트래픽은 인스턴스의 고객 소유 IP 주소(탄력적 IP 주소)를 사용합니다. 트래픽이 로컬 게이트웨이에 도달하면 로컬 게이트웨이는 고객 소유 IP 주소(탄력적 IP 주소)를 인스턴스 IP 주소에 매핑한 후 트래픽을 VPC의 대상으로 보냅니다. 또한 로컬 게이트웨이 라우팅 테이블은 탄력적 네트워크 인터페이스를 대상으로 하는 모든 경로를 평가합니다. 목적지 주소가 고정 경로의 목적지 CIDR과 일치하면 트래픽이 해당 탄력적 네트워크 인터페이스로 전송됩니다. 트래픽이 정적 경로를 따라 탄력적 네트워크 인터페이스스로 전달되는 경우, 대상 주소는 보존되며 네트워크 인터페이스의 프라이빗 IP 주소로 변환되지 않습니다.

로컬 게이트웨이 라우팅 테이블 사용

랙 설치의 일부로 로컬 게이트웨이를 AWS 만들고 VIF 및 VIF 그룹을 구성합니다. 로컬 게이트웨이 라우팅 테이블을 생성합니다. 로컬 게이트웨이 라우팅 테이블은 VIF 그룹 및 VPC와 연결되어 있어야 합니다. VIF 그룹과 VPC의 연결을 생성하고 관리합니다. 로컬 게이트웨이 라우팅 테이블에 대한 다음 정보를 고려합니다.

- VIF 그룹과 로컬 게이트웨이 라우팅 테이블은 관계가 있어야 합니다. one-to-one
- 로컬 게이트웨이는 Outpost와 연결된 AWS 계정이 소유하며 소유자만 로컬 게이트웨이 라우팅 테이블을 수정할 수 있습니다.
- 를 사용하여 AWS Resource Access Manager로컬 게이트웨이 라우팅 테이블을 다른 AWS 계정 또는 조직 구성 단위와 공유할 수 있습니다. 자세한 내용은 AWS Outposts 리소스 사용을 참조하세요.
- 로컬 게이트웨이 라우팅 테이블에는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크(직접 VPC 라우팅)와 통신할지 아니면 고객 소유 IP 주소 풀(CoIP) 과 통신할지를 결정하는 모드가 있습니다. 직접 VPC 라우팅과 CoIP는 상호 배타적인 옵션이며, 라우팅은 선택에 따라 다르게 작동합니다. 자세한 내용은 ??? 단원을 참조하세요.
- 직접 VPC 라우팅 모드는 중복되는 CIDR 범위를 지원하지 않습니다.

Tasks

- 로컬 게이트웨이 라우팅 테이블 세부 정보 보기
- 사용자 지정 로컬 게이트웨이 라우팅 테이블 생성
- 로컬 게이트웨이 라우팅 테이블을 관리합니다.
- 로컬 게이트웨이 라우팅 테이블 관리
- 로컬 게이트웨이 라우팅 테이블 모드 전환 또는 로컬 게이트웨이 라우팅 테이블 삭제
- CoIP 풀을 관리합니다.

- VIF 그룹 연결
- VPC 연결

로컬 게이트웨이 라우팅 테이블 세부 정보 보기

콘솔 또는 AWS CLI을(를) 사용하여 로컬 게이트웨이 라우팅 테이블의 세부 정보를 볼 수 있습니다.

AWS Outposts console

로컬 게이트웨이 라우팅 테이블 세부 정보를 보려면

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 로컬 게이트웨이 라우팅 테이블을 선택한 다음 작업, 세부 정보 보기를 선택합니다.

AWS CLI

로컬 게이트웨이 라우팅 테이블 세부 정보를 보려면

describe-local-gateway-route-tables 명령을 사용하십시오. AWS CLI

예

```
aws ec2 describe-local-gateway-route-tables --region us-west-2
```

출력

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available",
            "Tags": []
        }
    ]
```

```
}
```

> **Note**
>
> 보고 있는 기본 로컬 게이트웨이 라우팅 테이블이 CoIP 모드를 사용하는 경우 로컬 게이트웨이 라우팅 테이블은 각 VIF에 대한 기본 경로와 풀 CoIP 풀의 연결된 각 고객 소유 IP 주소로 전파된 경로로 구성됩니다.

사용자 지정 로컬 게이트웨이 라우팅 테이블 생성

AWS Outposts 콘솔을 사용하여 로컬 게이트웨이에 대한 사용자 지정 라우팅 테이블을 생성할 수 있습니다.

콘솔을 사용하여 사용자 지정 로컬 게이트웨이 라우팅 테이블을 생성하려면

1. https://console.aws.amazon.com/outposts/ AWS Outposts 에서 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 로컬 게이트웨이 라우팅 테이블 생성을 선택합니다.
5. (선택 사항) 이름에 로컬 게이트웨이 라우팅 테이블의 이름을 입력합니다.
6. 로컬 게이트웨이에서 로컬 게이트웨이를 선택합니다.
7. (선택 사항) VIF 그룹 연결을 선택하고 VIF 그룹을 선택합니다.
8. 모드에서 온프레미스 네트워크와 통신하기 위한 모드를 선택합니다.
   - 인스턴스의 프라이빗 IP 주소를 사용하려면 직접 VPC 라우팅을 선택합니다.
   - 고객 소유 IP 주소를 사용하려면 CoIP를 선택합니다.
     - (선택 사항) CoIP 풀 및 추가 CIDR 블록 추가 또는 제거

       [CoIP 풀 추가] 새 풀 추가를 선택하고 다음을 수행합니다.
       - 이름에서 CoIP 풀의 이름을 입력합니다.
       - CIDR의 경우, 고객 소유 IP 주소로 구성된 CIDR 블록을 입력합니다.
     - [CIDR 블록 추가] 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.
     - [CoIP 풀 또는 추가 CIDR 블록 제거] CIDR 블록 오른쪽 또는 CoIP 풀 아래에서 제거를 선택합니다.

최대 10개의 CoIP 풀과 100개의 CIDR 블록을 지정할 수 있습니다.

9. (선택) 태그를 추가하거나 제거할 수 있습니다.

   [태그 추가] 새 태그 추가를 선택하고 다음을 수행합니다.

   - 키에서 키 이름을 입력합니다.
   - 값에 키 값을 입력합니다.

   [태그 제거] 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.

10. 로컬 게이트웨이 라우팅 테이블 생성을 선택합니다.

로컬 게이트웨이 라우팅 테이블을 관리합니다.

Outpost에서 로컬 게이트웨이 라우팅 테이블과 탄력적 네트워크 인터페이스에 대한 인바운드 경로를 생성할 수 있습니다. 기존 로컬 게이트웨이 인바운드 경로를 수정하여 대상 탄력적 네트워크 인터페이스를 변경할 수도 있습니다.

대상 탄력적 네트워크 인터페이스가 실행 중인 인스턴스에 연결된 경우에만 경로가 활성 상태입니다. 인스턴스가 중지되거나 인터페이스가 분리되면 경로가 활성 상태에서블랙홀 상태로 바뀝니다.

로컬 게이트웨이에는 다음과 같은 요구 사항과 제한 사항이 적용됩니다.

- 대상 탄력적 네트워크 인터페이스는 Outpost의 서브넷에 속해야 하며 해당 Outpost의 인스턴스에 연결되어야 합니다. 로컬 게이트웨이 경로는 다른 Outpost나 상위 AWS 리전에 있는 Amazon EC2 인스턴스를 대상으로 할 수 없습니다.
- 서브넷은 로컬 게이트웨이 라우팅 테이블에 연결된 VPC에 속해야 합니다.
- 동일한 라우팅 테이블에서 탄력적 네트워크 인터페이스 라우트는 100개를 초과할 수 없습니다.
- AWS 가장 구체적인 경로에 우선 순위를 지정하고, 경로가 일치하면 전파된 경로보다 정적 경로의 우선 순위를 지정합니다.
- 인터페이스 VPC 엔드포인트는 지원되지 않습니다.
- BGP 광고는 로컬 게이트웨이를 대상으로 하는 라우팅 테이블에 경로가 있는 Outpost의 서브넷에만 해당됩니다. 라우팅 테이블에 로컬 게이트웨이를 대상으로 하는 라우팅이 서브넷에 없는 경우 해당 서브넷은 BGP로 광고되지 않습니다.
- Outpost 인스턴스에 연결된 ENI만 해당 Outpost의 로컬 게이트웨이를 통해 통신할 수 있습니다. Outpost 서브넷에 속하지만 해당 리전의 인스턴스에 연결된 ENI는 해당 Outpost의 로컬 게이트웨이를 통해 통신할 수 없습니다.

- VPCE 엔드포인트 또는 인터페이스와 같은 관리형 인터페이스는 온프레미스에서 로컬 게이트웨이를 통해 연결할 수 없습니다. Outpost 내에 있는 인스턴스에서만 연결할 수 있습니다.

다음 NAT 고려 사항이 적용됩니다.

- 로컬 게이트웨이는 탄력적 네트워크 인터페이스 경로와 일치하는 트래픽에 대해 NAT를 수행하지 않습니다. 대신 대상 IP 주소는 보존됩니다.
- 대상 탄력적 네트워크 인터페이스에 대한 원본, 대상 확인을 끕니다. 자세한 내용은 Amazon EC2 사용 설명서의 네트워크 인터페이스 기본 사항을 참조하십시오.
- 대상 CIDR의 트래픽이 네트워크 인터페이스에서 받아들여질 수 있도록 운영 체제를 구성합니다.

AWS Outposts console

로컬 게이트웨이 라우팅의 경로를 편집하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 로컬 게이트웨이 라우팅 테이블을 선택한 다음 작업, 라우팅 편집을 선택합니다.
5. 라우팅을 추가하려면 라우팅 추가를 선택합니다. 대상에서 대상 CIDR 블록, 단일 IP 주소 또는 접두사 목록의 ID를 입력합니다.
6. 기존 라우팅을 수정하려면 대상에서 대상 CIDR 블록 또는 단일 IP 주소를 바꿉니다. 대상에서 대상을 선택합니다.
7. 라우팅 저장을 선택합니다.

AWS CLI

로컬 게이트웨이 라우팅 테이블의 경로를 생성하려면 다음과 같이 하세요.

- create-local-gateway-route 명령을 사용하십시오. AWS CLI

예

```
aws ec2 create-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
```

```
    --destination-cidr-block 192.0.2.0/24
```

출력

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

로컬 게이트웨이 라우팅 테이블의 경로를 수정하려면 다음과 같이 하세요.

기존 경로를 대상으로 하는 탄력적 네트워크 인터페이스를 수정할 수 있습니다. 수정 작업을 사용하려면 라우팅 테이블에 지정된 대상 CIDR 블록이 있는 경로가 이미 있어야 합니다.

- modify-local-gateway-route AWS CLI 명령을 사용합니다.

예

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

출력

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
```

```
        "OwnerId": "111122223333"
    }
}
```

로컬 게이트웨이 라우팅 테이블 관리

로컬 게이트웨이 라우팅 테이블에 태그를 지정하면 조직의 요구에 따라 이를 식별 또는 분류할 수 있습니다.

로컬 게이트웨이 라우팅 테이블 태그를 관리하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ AWS Outposts 에서 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 로컬 게이트웨이 라우팅 테이블을 선택한 다음 작업, 태그 관리를 선택합니다.
5. 태그를 추가하거나 제거합니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

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

   태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
6. 변경 사항 저장을 선택합니다.

로컬 게이트웨이 라우팅 테이블 모드 전환 또는 로컬 게이트웨이 라우팅 테이블 삭제

모드를 전환하려면 로컬 게이트웨이 라우팅 테이블을 삭제하고 다시 생성해야 합니다. 로컬 게이트웨이 라우팅 테이블을 삭제하면 네트워크 트래픽이 중단됩니다.

모드를 전환하거나 로컬 게이트웨이 라우팅 테이블을 삭제하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 입력이 올바른지 확인하십시오 AWS 리전.

   지역을 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하세요.
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.

4. 로컬 게이트웨이 라우팅 테이블이 VIF 그룹과 연결되어 있는지 확인합니다. 연결되어 있는 경우 로컬 게이트웨이 라우팅 테이블과 VIF 그룹 간의 연결을 제거해야 합니다.

   a. 로컬 게이트웨이 라우팅 테이블의 ID를 선택합니다.
   b. VIF 그룹 연결 탭을 선택합니다.
   c. 하나 이상의 VIF 그룹이 로컬 게이트웨이 라우팅 테이블에 연결된 경우 VIF 그룹 연결 편집을 선택합니다.
   d. VIF 그룹 연결 확인란의 선택을 취소하십시오.
   e. 변경 사항 저장를 선택합니다.
5. 로컬 게이트웨이 라우팅 테이블 삭제를 선택합니다.
6. 확인 대화 상자에 **delete**을(를) 입력한 다음 삭제를 선택합니다.
7. (선택 사항) 새 모드로 로컬 게이트웨이 라우팅 테이블을 생성합니다.

   a. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
   b. 로컬 게이트웨이 라우팅 테이블 생성을 선택합니다.
   c. 새 모드를 사용하여 로컬 게이트웨이 라우팅 테이블을 구성합니다. 자세한 내용은 사용자 지정 로컬 게이트웨이 라우팅 테이블 생성을 참조하세요.

CoIP 풀을 관리합니다.

온프레미스 네트워크와 VPC 인스턴스 간의 통신을 용이하게 하기 위해 IP 주소 범위를 제공할 수 있습니다. 자세한 내용은 고객 소유 IP 주소를 참조하세요.

고객 소유 IP 풀은 CoIP 모드의 로컬 게이트웨이 라우팅 테이블에 사용할 수 있습니다. 로컬 게이트웨이 라우팅 테이블 모드 간에 전환하려면 로컬 게이트웨이 라우팅 테이블 모드 전환)을 참조하세요.

CoIP 풀을 생성하려면 다음 절차를 따릅니다.

CoIP 풀을 생성하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.
5. 세부 정보 창에서 CoIP 풀 탭을 선택한 다음 CoIP 풀 생성을 선택합니다.
6. (선택 사항) 이름에서 CoIP 풀의 이름을 입력합니다.

7. 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.
8. (선택 사항) CIDR 블록을 추가하거나 제거할 수 있습니다.

   [CIDR 블록 추가] 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.

   [CIDR 블록 제거] CIDR 블록 오른쪽에 있는 제거를 선택합니다.
9. CoIP 풀 생성을 선택합니다.

CoIP 풀을 편집하려면 다음 절차를 따릅니다.

CoIP 풀을 편집하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.
5. 세부 정보 창에서 CoIP 풀 탭을 선택한 다음 CoIP 풀을 선택합니다.
6. 작업, CoIP 풀 편집을 선택합니다.
7. 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.
8. (선택 사항) CIDR 블록을 추가하거나 제거할 수 있습니다.

   [CIDR 블록 추가] 새 CIDR 추가를 선택하고 고객 소유 IP 주소 범위를 입력합니다.

   [CIDR 블록 제거] CIDR 블록 오른쪽에 있는 제거를 선택합니다.
9. 변경 사항 저장를 선택합니다.

다음 절차를 사용하여 태그를 관리하거나 CoIP 풀에 이름 태그를 추가할 수 있습니다.

CoIP 풀의 태그를 관리하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.
5. 세부 정보 창에서 CoIP 풀 탭을 선택한 다음 CoIP 풀을 선택합니다.

6. 작업, 태그 관리를 선택합니다.
7. 태그를 추가하거나 제거합니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

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

   태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.
8. 변경 사항 저장을 선택합니다.

CoIP 풀을 삭제하려면 다음 절차를 따릅니다.

CoIP 풀을 삭제하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.
5. 세부 정보 창에서 CoIP 풀 탭을 선택한 다음 CoIP 풀을 선택합니다.
6. 작업, CoIP 풀 삭제를 선택합니다.
7. 확인 대화 상자에 **delete**을(를) 입력한 다음 삭제를 선택합니다.

VIF 그룹 연결

VIF 그룹은 VIF(가상 인터페이스)의 논리적 그룹입니다. VIF 그룹이 로컬 게이트웨이 라우팅 테이블과 연결되도록 바꿀 수 있습니다. 로컬 게이트웨이 라우팅 테이블에서 VIF 그룹을 연결 해제하면 라우팅 테이블에서 모든 경로가 삭제되고 네트워크 트래픽이 중단됩니다.

VIF 그룹의 연결을 변경하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택합니다.

5. 세부 정보 창에서 VIF 그룹 연결 탭을 선택한 다음 VIF 그룹 연결 편집을 선택합니다.
6. VIF 그룹 설정의 경우 다음 작업 중 하나를 수행합니다.
   - VIF 그룹을 로컬 게이트웨이 라우팅 테이블에 연결하려면 VIF 그룹 연결을 선택하고 VIF 그룹을 선택합니다.
   - 로컬 게이트웨이 라우팅 테이블에서 VIF 그룹의 연결을 끊으려면 VIF 그룹 연결을 해제합니다.

   > **Important**
   >
   > 로컬 게이트웨이 라우팅 테이블에서 VIF 그룹을 분리하면 모든 경로가 자동으로 삭제되고 네트워크 트래픽이 중단됩니다.

7. 변경 사항 저장를 선택합니다.

VPC 연결

VPCs를 로컬 게이트웨이 라우팅 테이블과 연결해야 합니다. 기본적으로 연결되지 않습니다.

VPC 연결 생성

다음 절차를 사용하여 VPC를 로컬 게이트웨이 라우팅 테이블과 연결합니다.

선택적으로 연결에 태그를 지정하여 조직의 필요에 따라 연결을 식별하거나 분류할 수 있습니다.

AWS Outposts console

VPC를 연결하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택한 다음 작), VPC 연결을 선택합니다.
5. VPC ID의 경우 로컬 게이트웨이 라우팅 테이블에 연결할 VPC를 선택합니다.
6. (선택) 태그를 추가하거나 제거할 수 있습니다.

   태그를 추가하기 위해 새 태그 추가를 선택하고 다음을 수행합니다.

   - 키에서 키 이름을 입력합니다.

- 값에서 키 값을 입력합니다.

태그를 제거하려면 태그의 키와 값 오른쪽에 있는 제거를 선택합니다.

7. VPC 연결을 선택합니다.

AWS CLI

VPC를 연결하려면 다음과 같이 하세요.

create-local-gateway-route-table-route-table-vpc-association 명령을 사용합니다.

예

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

출력

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

VPC 연결을 삭제하려면 다음과 같이 하세요.

다음 절차를 사용하여 로컬 게이트웨이 라우팅 테이블에서 VPC의 연결을 해제합니다.

AWS Outposts console

VPC를 연결 해제하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전

3. 탐색 창에서 로컬 게이트웨이 라우팅 테이블을 선택합니다.
4. 라우팅 테이블을 선택한 후 작업), 세부 정보 보기를 선택합니다.
5. VPC 연결에서 연결을 끊을 VPC를 선택한 다음 연결 해제를 선택합니다.
6. 연결 해제를 선택합니다.

AWS CLI

VPC를 연결 해제하려면 다음과 같이 하세요.

delete-local-gateway-route-table-vpc-association 명령을 사용합니다.

예

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

출력

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

랙용 로컬 네트워크 연결

Outpost 랙을 온프레미스 네트워크에 연결하려면 다음 구성 요소가 필요합니다.

- Outpost 패치 패널에서 고객 로컬 네트워크 장치로의 물리적 연결
- Outpost 네트워크 장치 및 로컬 네트워크 장치에 대한 두 개의 링크 집계 그룹(LAG) 연결을 설정하는 링크 집계 제어 프로토콜(LACP)
- Outpost와 고객 로컬 네트워크 장치 간의 가상 LAN(VLAN) 연결
- 각 VLAN의 레이어 3 point-to-point 연결.
- Outpost와 온프레미스 서비스 링크 간의 경로 광고를 위한 Border Gateway Protocol(BGP).
- Outpost와 온프레미스 로컬 네트워크 장치 간의 로컬 게이트웨이 연결을 위한 경로 광고용 BGP

내용

- 물리적 연결
- 링크 집계
- 가상 LAN.
- 네트워크 계층 연결
- 에이스 랙 커넥티비티
- 서비스 링크 BGP 연결
- 서비스 링크 인프라, 서브넷 광고 및 IP 범위
- 로컬 게이트웨이 BGP 연결
- 로컬 게이트웨이 고객 소유의 IP 서브넷 광고

물리적 연결

Outpost 랙에는 로컬 네트워크로 연결되는 두 개의 물리적 네트워크 장치가 있습니다.

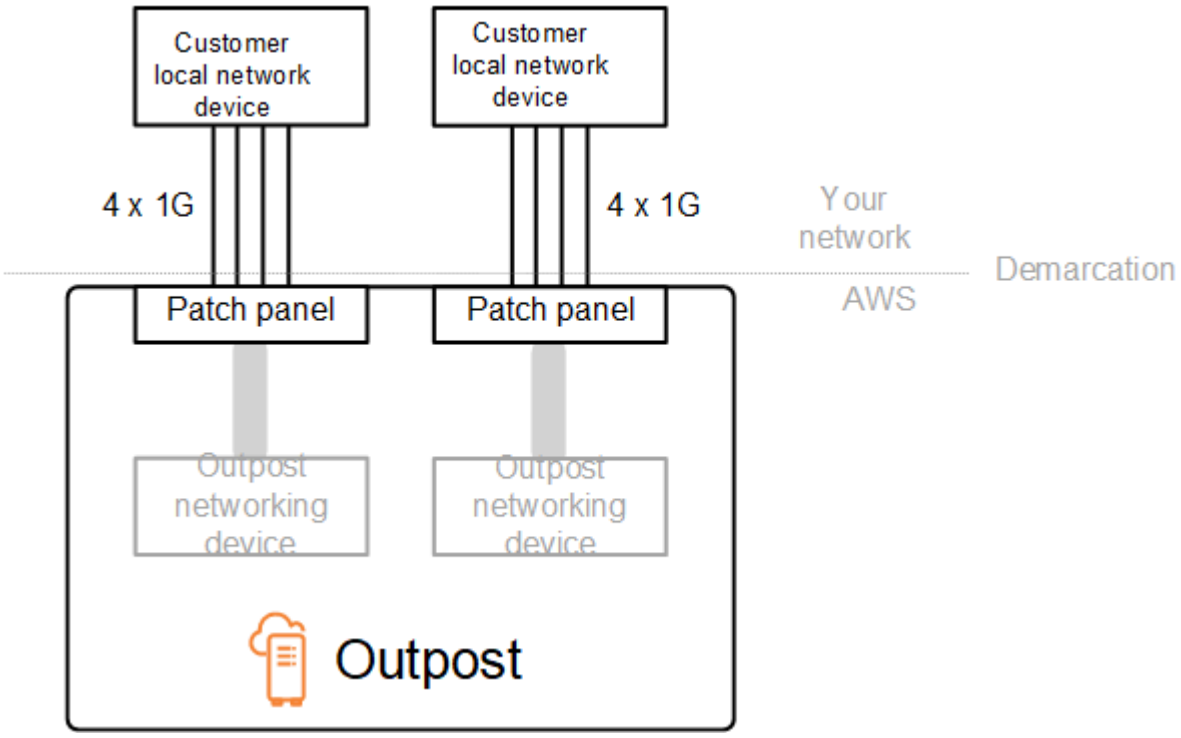
Outpost에는 이러한 Outpost 네트워크 장치와 로컬 네트워크 장치 사이에 최소 두 개의 물리적 링크가 필요합니다. Outpost는 각 Outpost 네트워크 장치에 대해 다음과 같은 업링크 속도 및 수량을 지원합니다.

업링크 속도	업링크 수
1Gbps	1, 2, 4, 6 또는 8
10Gbps	1, 2, 4, 8, 12 또는 16
40Gbps 또는 100Gbps	1, 2, 또는 4

업링크 속도와 수량은 각 Outpost 네트워크 장치에서 대칭입니다. 업링크 속도로 100Gbps를 사용하는 경우 순방향 오류 수정(FEC CL91)을 사용하여 링크를 구성해야 합니다.

아웃포스트 랙은 루슨트 커넥터 (LC) 가 있는 단일 모드 파이버 (SMF), 멀티모드 파이버 (MMF) 또는 LC가 있는 MMF OM4를 지원할 수 있습니다. AWS 랙 위치에 제공하는 광섬유와 호환되는 광학 장치를 제공합니다.

다음 다이어그램에서 물리적 경계는 각 Outpost의 파이버 패치 패널입니다. Outpost를 패치 패널에 연결하는 데 필요한 광섬유 케이블을 제공합니다.



링크 집계

AWS Outposts LACP (링크 집계 제어 프로토콜) 를 사용하여 각 Outpost 네트워크 장치에서 각 로컬 네트워크 장치까지 하나씩 두 개의 LAG (링크 집계 그룹) 연결을 설정합니다. 각 Outpost 네트워크 장

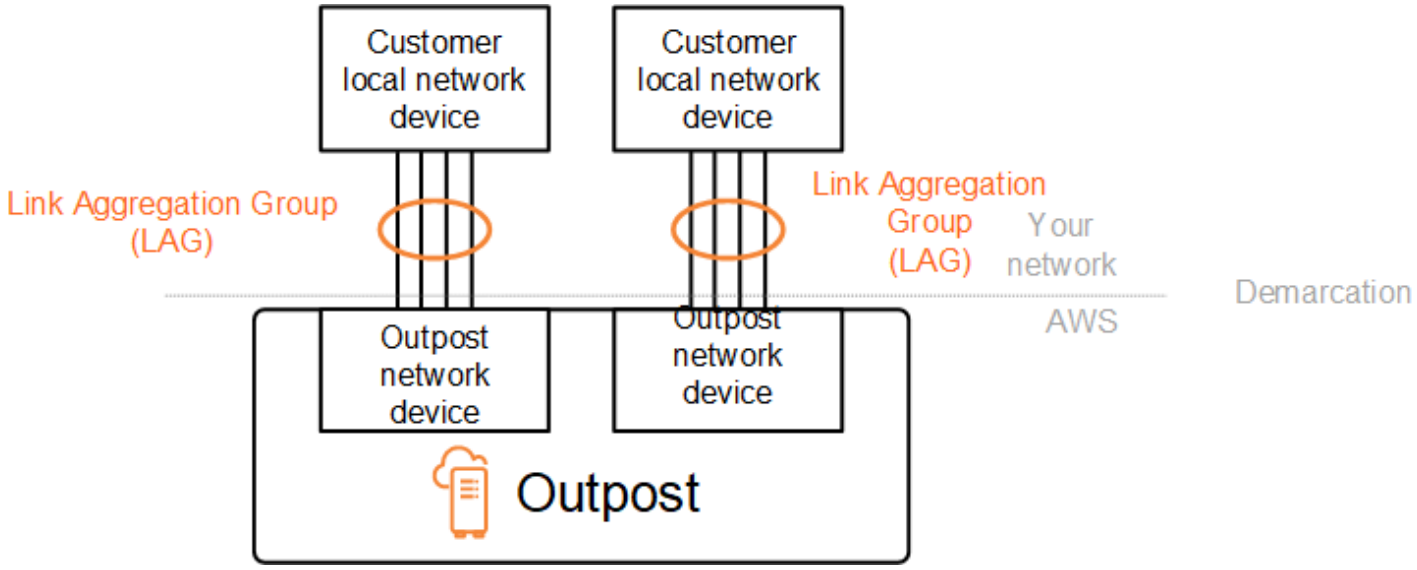
치의 링크는 이더넷 LAG로 집계되어 단일 네트워크 연결을 나타냅니다. 이러한 LAG는 표준 고속 타이머와 함께 LACP를 사용합니다. 슬로우 타이머를 사용하도록 LAG를 구성할 수 없습니다.

사이트에서 Outpost 설치를 활성화하려면 네트워크 장치에서 LAG 연결 쪽을 구성해야 합니다.

논리적인 관점에서 보면 Outpost 패치 패널을 경계점으로 무시하고 Outpost 네트워킹 장치를 사용합니다.

랙이 여러 개 있는 배포의 경우 Outpost에는 Outpost 네트워크 장치의 집계 계층과 로컬 네트워크 장치 사이에 4개의 LAG가 있어야 합니다.

다음 다이어그램은 각 Outpost 네트워크 장치와 연결된 로컬 네트워크 장치 간의 네 가지 물리적 연결을 보여줍니다. 당사는 이더넷 LAG를 사용하여 Outpost 네트워크 장치와 고객 로컬 네트워크 장치를 연결하는 물리적 링크를 집계합니다.



가상 LAN.

Outpost 네트워크 장치와 로컬 네트워크 장치 간의 각 LAG는 IEEE 802.1q 이더넷 트렁크로 구성되어야 합니다. 이를 통해 데이터 경로 간 네트워크 분리에 여러 VLANs를 사용할 수 있습니다.

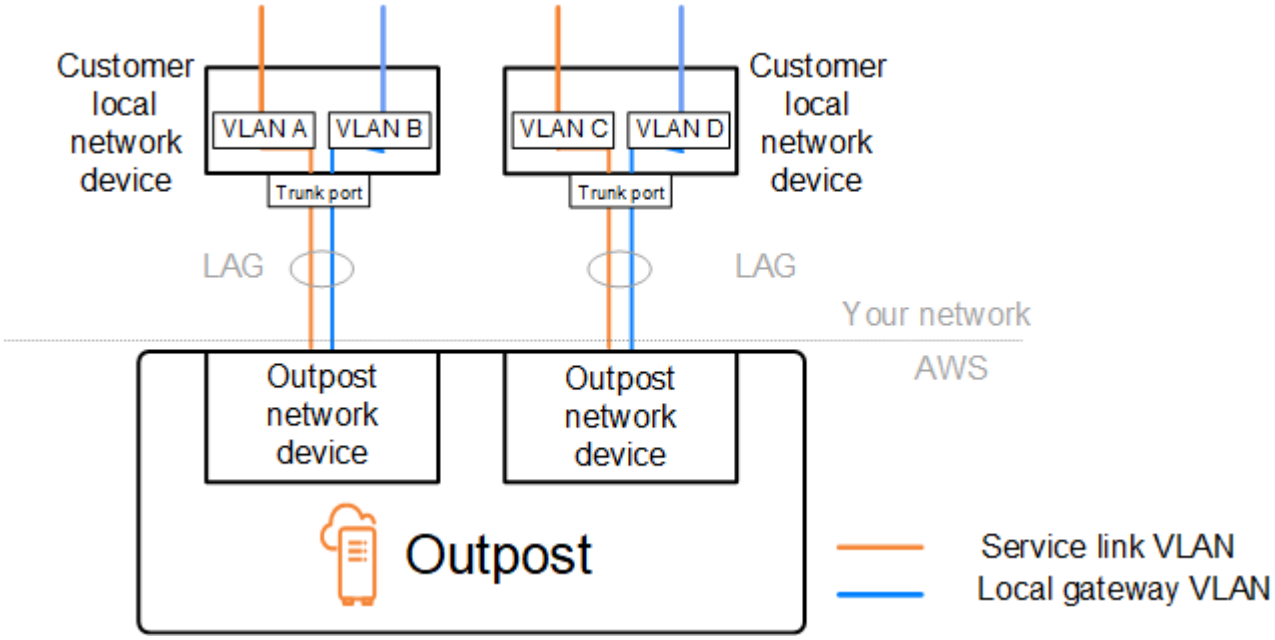
각 Outpost에는 로컬 네트워크 장치와 통신하기 위한 다음과 같은 VLAN이 있습니다.

- 서비스 링크 VLAN — 서비스 링크 연결을 위한 서비스 링크 경로를 설정하기 위해 Outpost와 로컬 네트워크 장치 간의 통신을 가능하게 합니다. 자세한 내용은 지역 AWS Outposts 연결을 AWS 참조하십시오.
- 로컬 게이트웨이 VLAN — Outpost와 로컬 네트워크 장치 간의 통신을 활성화하여 Outpost 서브넷과 근거리 통신망을 연결하는 로컬 게이트웨이 경로를 설정합니다. Outpost 로컬 게이트웨이는 이

VLAN을 활용하여 인스턴스에 온프레미스 네트워크에 대한 연결을 제공합니다. 여기에는 네트워크를 통한 인터넷 액세스가 포함될 수 있습니다. 자세한 내용은 로컬 게이트웨이를 참조하십시오.

Outpost와 고객 로컬 네트워크 장치 간에만 서비스 링크 VLAN과 로컬 게이트웨이 VLAN을 구성할 수 있습니다.

Outpost는 서비스 링크와 로컬 게이트웨이 데이터 경로를 분리된 두 개의 네트워크로 분리하도록 설계되었습니다. 이를 통해 Outpost에서 실행되는 서비스와 통신할 수 있는 네트워크를 선택할 수 있습니다. 또한 일반적으로 가상 라우팅 및 전달 인스턴스(VRF)라고 하는 고객 로컬 네트워크 장치의 여러 라우팅 테이블을 사용하여 서비스 링크를 로컬 게이트웨이 네트워크와 분리된 네트워크로 만들 수 있습니다. 경계선은 Outpost 네트워크 디바이스의 포트에 있습니다. AWS 연결 AWS 측의 모든 인프라를 관리하고 회선 측의 모든 인프라를 관리합니다.



설치 및 운영 중에 Outpost를 온프레미스 네트워크와 통합하려면 Outpost 네트워크 장치와 고객 로컬 네트워크 장치 간에 사용되는 VLAN을 할당해야 합니다. 설치 AWS 전에 이 정보를 제공해야 합니다. 자세한 정보는 the section called “네트워크 준비 체크리스트”을 참조하세요.

네트워크 계층 연결

네트워크 계층 연결을 설정하기 위해 각 Outpost 네트워크 디바이스는 각 VLAN의 IP 주소를 포함하는 가상 인터페이스 (VIF) 로 구성됩니다. AWS Outposts 네트워크 장치는 이러한 VIF를 통해 로컬 네트워크 장비와의 IP 연결 및 BGP 세션을 설정할 수 있습니다.

다음과 같이 하는 것이 좋습니다:

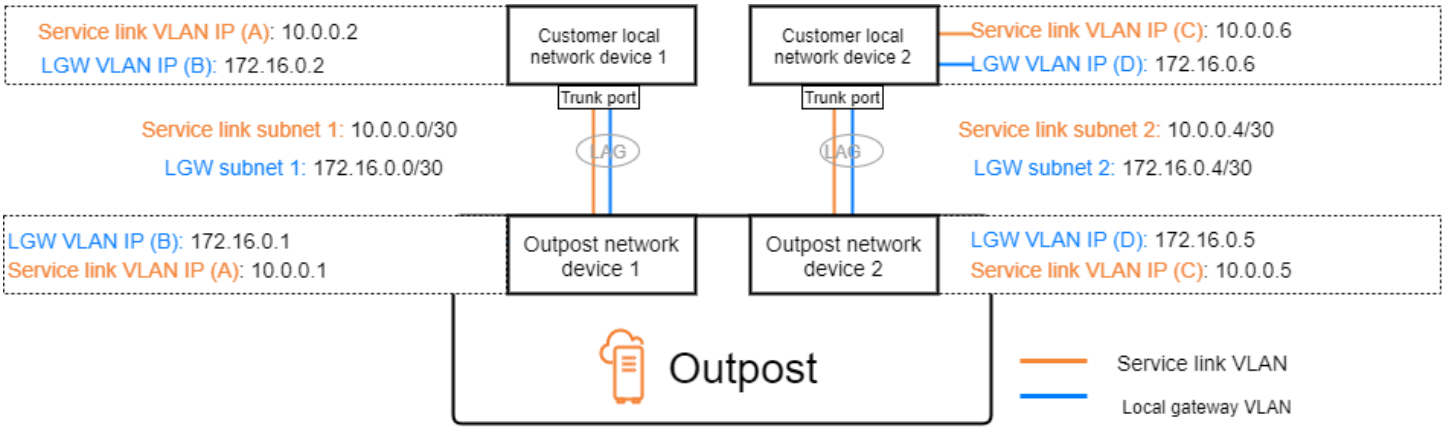
- /30 또는 /31 CIDR과 함께 전용 서브넷을 사용하여 이러한 논리적 연결을 나타내십시오. point-to-point
- 로컬 네트워크 장치 간에 VLAN을 연결하지 마십시오.

네트워크 계층 연결의 경우 두 경로를 설정해야 합니다.

- 서비스 링크 경로 - 이 경로를 설정하려면 범위가 /30 또는 /31인 VLAN 서브넷을 지정하고 네트워크 디바이스의 각 서비스 링크 VLAN에 대한 IP 주소를 지정합니다. AWS Outposts 이 경로에 서비스 링크 가상 인터페이스 (VIF) 를 사용하여 Outpost와 로컬 네트워크 장치 간에 서비스 링크 연결을 위한 IP 연결 및 BGP 세션을 설정합니다. 자세한 내용은 지역 연결을 참조하십시오AWS Outposts . AWS
- 로컬 게이트웨이 경로 - 이 경로를 설정하려면 범위가 /30 또는 /31인 VLAN 서브넷과 네트워크 디바이스의 로컬 게이트웨이 VLAN에 대한 IP 주소를 지정합니다. AWS Outposts 이 경로에서 로컬 게이트웨이 VIF는 Outpost와 로컬 네트워크 디바이스 간에 로컬 리소스 연결을 위한 IP 연결 및 BGP 세션을 설정하는 데 사용됩니다.

다음 다이어그램은 서비스 링크 경로 및 로컬 게이트웨이 경로에 대한 각 Outpost 네트워크 장치에서 고객 로컬 네트워크 장치로의 연결을 보여줍니다. 이 예제에는 VLAN이 네 개 있습니다.

- VLAN A는 Outpost 네트워크 장치 1을 고객 로컬 네트워크 장치 1과 연결하는 서비스 링크 경로를 위한 것입니다.
- VLAN B는 Outpost 네트워크 장치 1을 고객 로컬 네트워크 장치 1과 연결하는 로컬 게이트웨이 경로용입니다.
- VLAN C는 Outpost 네트워크 장치 2를 고객 로컬 네트워크 장치 2와 연결하는 서비스 링크 경로용입니다.
- VLAN D는 Outpost 네트워크 장치 2를 고객 로컬 네트워크 장치 2와 연결하는 로컬 게이트웨이 경로용입니다.



다음 표는 Outpost 네트워크 장치 1을 고객 로컬 네트워크 장치 1에 연결하는 서브넷의 예제 값을 보여 줍니다.

VLAN	서브넷	고객 장치 1 IP	AWS OND 1 IP
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	172.16.0.2	172.16.0.1

다음 표는 Outpost 네트워크 장치 2를 고객 로컬 네트워크 장치 2에 연결하는 서브넷의 예제 값을 보여 줍니다.

VLAN	서브넷	고객 장치 2 IP	AWS 하나 - 두 개의 IP
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

에이스 랙 커넥티비티

> **Note**
>
> ACE 랙이 필요하지 않으면 이 섹션을 건너뛰십시오.

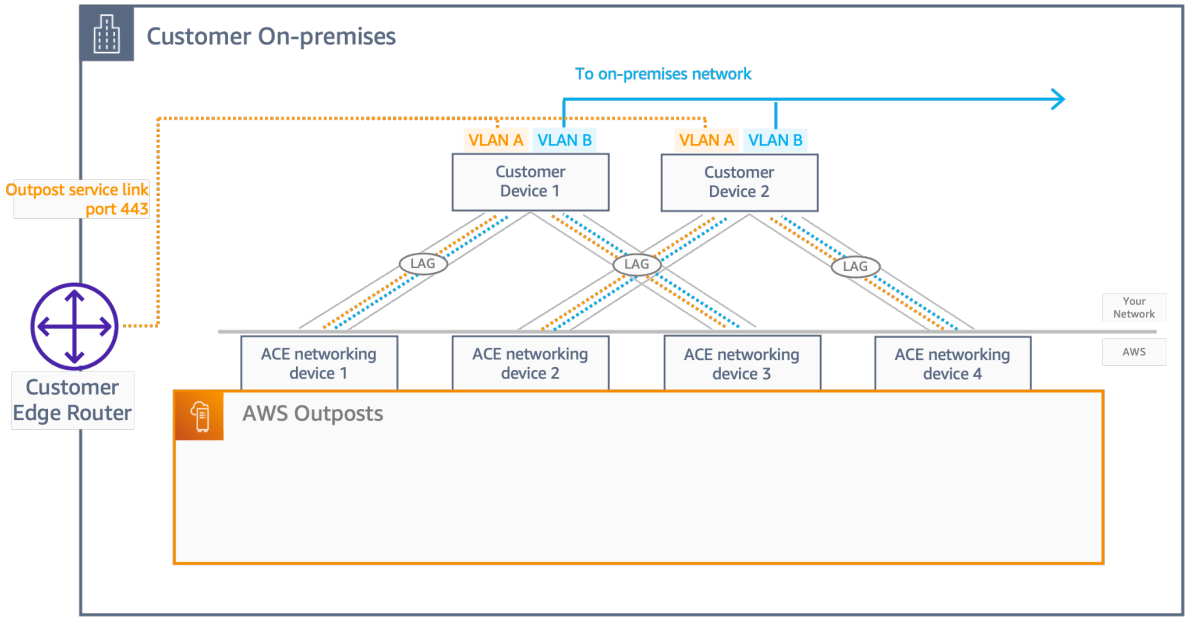
어그리게이션, 코어, 에지 (ACE) 랙은 멀티랙 아웃포스트 배포를 위한 네트워크 어그리게이션 포인트 역할을 합니다. 컴퓨팅 랙이 5개 이상인 경우 ACE 랙을 사용해야 합니다. 컴퓨팅 랙이 5개 미만이지만 향후 랙을 5개 이상으로 확장할 계획이라면 최대한 빨리 ACE 랙을 설치하는 것이 좋습니다.

ACE 랙을 사용하면 Outposts 네트워킹 장치가 더 이상 온-프레미스 네트워킹 장치에 직접 연결되지 않습니다. 대신 ACE 랙에 연결되어 Outpost 랙에 연결할 수 있습니다. 이 토폴로지에서는 Outposts 네트워킹 디바이스와 AWS ACE 네트워킹 디바이스 간의 VLAN 인터페이스 할당 및 컨피그레이션을 소유합니다.

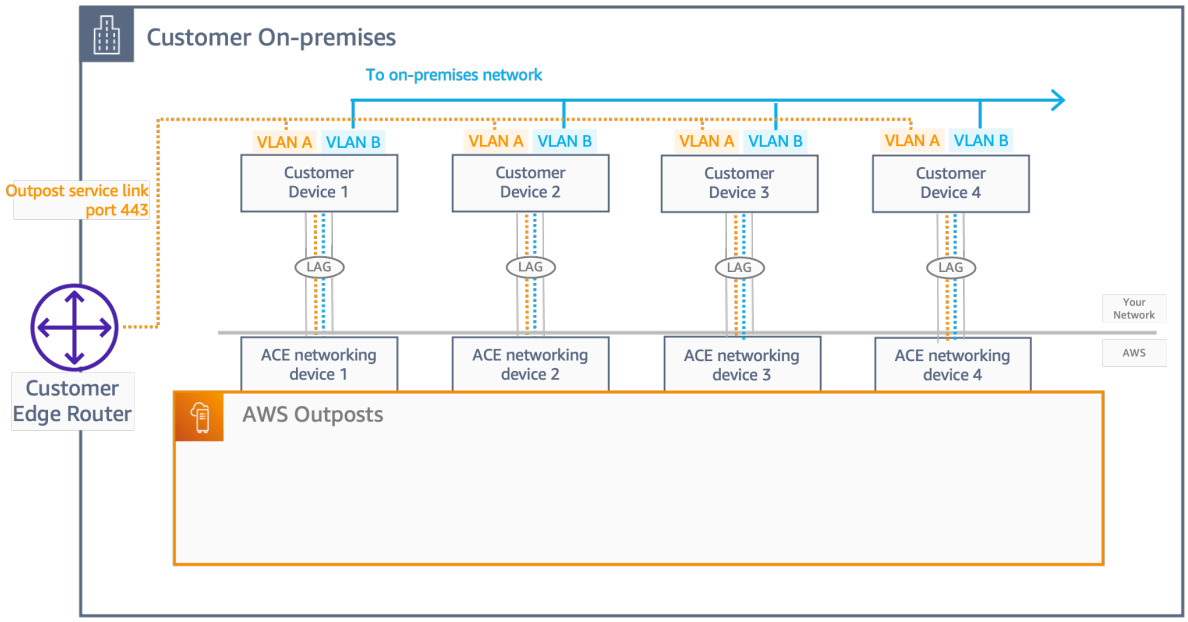
ACE 랙에는 복원력을 극대화하기 위해 고객 온프레미스 네트워크의 업스트림 고객 디바이스 2개 또는 업스트림 고객 디바이스 4개에 연결할 수 있는 네트워킹 디바이스 4개가 포함되어 있습니다.

다음 이미지는 두 네트워킹 토폴로지를 보여줍니다.

다음 이미지는 업스트림 고객 장치 2개에 연결된 ACE 랙의 ACE 네트워킹 장치 4개를 보여줍니다.



다음 이미지는 업스트림 고객 장치 4개에 연결된 ACE 랙의 ACE 네트워킹 장치 4개를 보여줍니다.

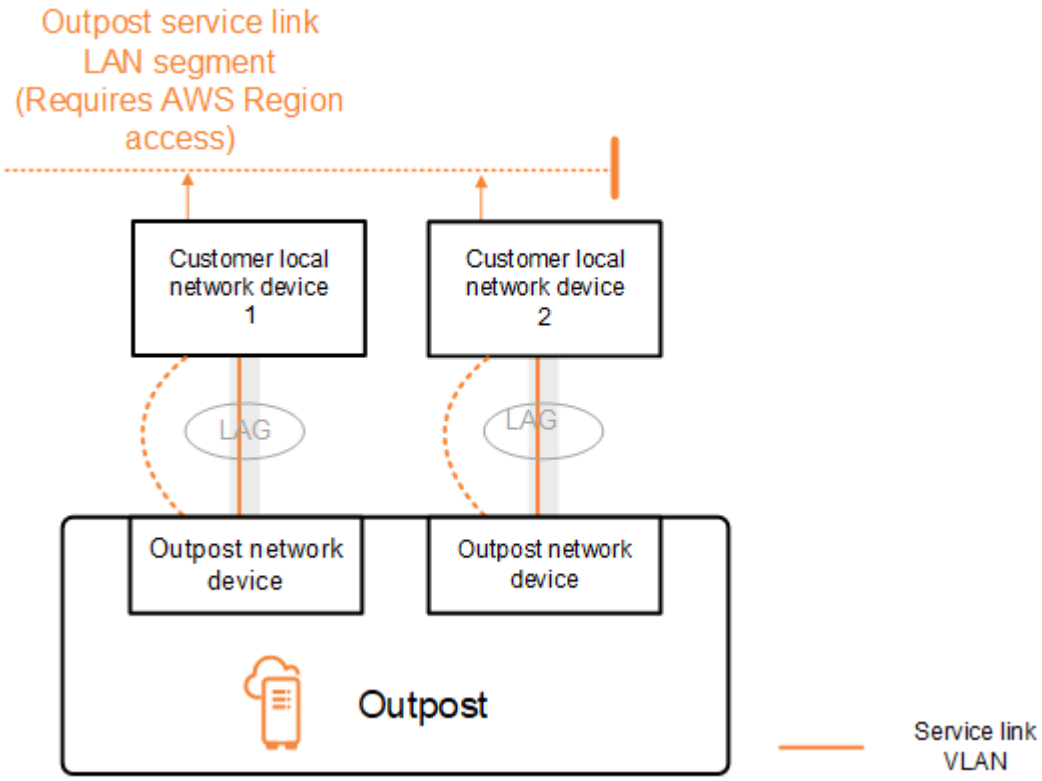


서비스 링크 BGP 연결

Outpost는 서비스 링크 VLAN을 통한 서비스 링크 연결을 위해 각 Outpost 네트워크 장치와 고객 로컬 네트워크 장치 간에 외부 BGP 피어링 세션을 설정합니다. BGP 피어링 세션은 VLAN에 제공된 /30 또는 /31 IP 주소 간에 설정됩니다. point-to-point 각 BGP 피어링 세션은 Outpost 네트워크 장치의 사설 Autonomous System Number(ASN)과 고객 로컬 네트워크 장치용으로 선택한 ASN을 사용합니다. AWS 은(는) 설치 프로세스의 일부로 속성을 제공합니다.

Outpost 네트워크 장치 두 개가 서비스 링크 VLAN을 통해 두 개의 고객 로컬 네트워크 장치에 연결된 Outpost가 있는 시나리오를 고려합니다. 각 서비스 링크에 대해 다음과 같은 인프라 및 고객 로컬 네트워크 장치 BGP ASN 속성을 구성합니다.

- 서비스 링크 BGP 피어 ASN. 2바이트(16비트) 또는 4바이트(32비트). 유효한 값은 64512-65535 또는 4200000000-4294967294입니다.
- 인프라 CIDR. 랙당 /26 CIDR이어야 합니다.
- 고객 로컬 네트워크 장치 1 서비스 링크 BGP 피어 IP 주소입니다.
- 고객 로컬 네트워크 장치 1 서비스 링크 BGP 피어 ASN입니다. 유효한 값은 1-4294967294입니다.
- 고객 로컬 네트워크 장치 2 서비스 링크 BGP 피어 IP 주소입니다.
- 고객 로컬 네트워크 장치 2 서비스 링크 BGP 피어 ASN입니다. 유효한 값은 1-4294967294입니다. 자세한 내용은 RFC4893을 참조하세요.



Outpost는 다음 프로세스를 사용하여 서비스 링크 VLAN을 통해 외부 BGP 피어링 세션을 설정합니다.

1. 각 Outpost 네트워크 장치는 ASN을 사용하여 연결된 로컬 네트워크 장치와 BGP 피어링 세션을 설정합니다.
2. Outpost 네트워크 장치는 링크 및 장치 장애를 지원하기 위해 /26 CIDR 범위를 2개의 /27 CIDR 범위로 광고합니다. 각 OND는 AS-Path 길이가 1인 자체 /27 접두사와 AS-Path 길이가 4인 다른 모든 OND의 /27 접두사를 백업으로 광고합니다.
3. 서브넷은 아웃포스트에서 지역으로 연결하는 데 사용됩니다. AWS

BGP 속성을 변경하지 않고 Outposts에서 BGP 광고를 수신하도록 고객 네트워크 장비를 구성하는 것이 좋습니다. 고객 네트워크는 AS-Path 길이가 1인 Outpost에서 출발하는 경로를 AS-Path 길이가 4인 경로보다 선호해야 합니다.

고객 네트워크는 모든 OND에 동일한 속성을 가진 동일한 BGP 접두사를 알려야 합니다. Outpost 네트워크는 기본적으로 모든 업링크 간에 아웃바운드 트래픽의 부하를 분산합니다. 유지 관리가 필요한 경우 Outpost 측에서는 라우팅 정책을 사용하여 트래픽을 OND에서 다른 곳으로 이동합니다. 이러한 트래픽 이동에는 모든 OND의 고객 측에서 동일한 BGP 접두사가 필요합니다. 고객 네트워크에서 유지 관리가 필요한 경우 AS-Path 프리펜딩을 사용하여 특정 업링크에서 일시적으로 트래픽 배열을 이동하는 것이 좋습니다.

서비스 링크 인프라, 서브넷 광고 및 IP 범위

서비스 링크 인프라 서브넷의 사전 설치 프로세스 중에 /26 CIDR 범위를 제공합니다. Outpost 인프라는 이 범위를 사용하여 서비스 링크를 통해 리전에 대한 연결을 설정합니다. 서비스 링크 서브넷은 연결을 시작하는 Outpost 소스입니다.

Outpost 네트워크 장치는 링크 및 장치 오류를 지원하기 위해 /26 CIDR 범위를 2개의 /27 CIDR 블록으로 광고합니다.

Outpost에 대한 서비스 링크 BGP ASN과 인프라 서브넷 CIDR(/26)을 제공해야 합니다. 각 Outpost 네트워크 장치에 대해 로컬 네트워크 장치의 VLAN에 있는 BGP 피어링 IP 주소와 로컬 네트워크 장치의 BGP ASN을 제공합니다.

랙을 여러 개 배포하는 경우 랙당 하나의 /26 서브넷이 있어야 합니다.

로컬 게이트웨이 BGP 연결

Outpost는 로컬 게이트웨이에 연결하기 위해 각 Outpost 네트워크 장치에서 로컬 네트워크 장치로의 외부 BGP 피어링을 설정합니다. 외부 BGP 세션을 설정하기 위해 사용자가 할당하는 프라이빗 자율 시스템 번호(ASN)를 사용합니다. 각 Outpost 네트워크 장치에는 로컬 게이트웨이 VLAN을 사용하여 로컬 네트워크 장치에 대한 단일 외부 BGP 피어링이 있습니다.

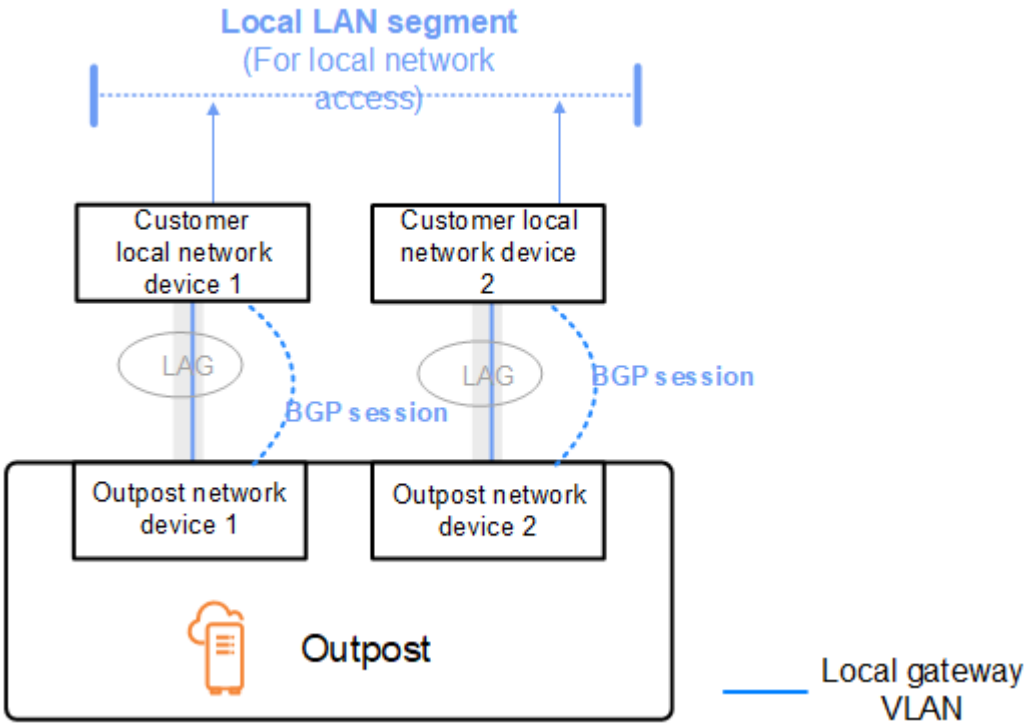
Outpost는 로컬 게이트웨이 VLAN을 통해 각 Outpost 네트워크 장치와 연결된 고객 로컬 네트워크 장치 간에 외부 BGP 피어링 세션을 설정합니다. 피어링 세션은 네트워크 연결을 설정할 때 제공한 /30 또는 /31 IP 간에 설정되며 Outpost 네트워크 장치와 고객 로컬 네트워크 point-to-point 장치 간의 연결을 사용합니다. 자세한 정보는 the section called “네트워크 계층 연결”을 참조하세요.

각 BGP 세션은 Outpost 네트워크 디바이스 측의 프라이빗 ASN과 고객 로컬 네트워크 디바이스 측에서 선택한 ASN을 사용합니다. AWS 설치 전 프로세스의 일부로 속성을 제공합니다.

Outpost 네트워크 장치 두 개가 서비스 링크 VLAN을 통해 두 개의 고객 로컬 네트워크 장치에 연결된 Outpost가 있는 시나리오를 고려합니다. 각 서비스 링크에 대해 다음 로컬 게이트웨이 및 고객 로컬 네트워크 장치 BGP ASN 속성을 구성합니다.

- AWS 로컬 게이트웨이 BGP ASN을 제공합니다. 2바이트 (16비트) 또는 4바이트 (32비트). 유효한 값은 64512-65535 또는 4200000000-4294967294입니다.
- (선택 사항) 광고되는 고객 소유의 CIDR(공개 또는 비공개, 최소 2/26)을 제공합니다.
- 고객에게 로컬 네트워크 장치 1 로컬 게이트웨이 BGP 피어 IP 주소를 제공합니다.

- 고객에게 로컬 네트워크 장치 1 로컬 게이트웨이 BGP 피어 ASN을 제공합니다. 유효한 값은 1-4294967294입니다. 자세한 내용은 RFC4893을 참조하세요.
- 고객에게 로컬 네트워크 장치 2 로컬 게이트웨이 BGP 피어 IP 주소를 제공합니다.
- 고객에게 로컬 네트워크 장치 2 로컬 게이트웨이 BGP 피어 ASN을 제공합니다. 유효한 값은 1-4294967294입니다. 자세한 내용은 RFC4893을 참조하세요.



BGP 속성을 변경하지 않고 Outpost에서 BGP 광고를 수신하도록 고객 네트워크 장비를 구성하고 BGP 다중 경로 및 부하 분산을 활성화하여 최적의 인바운드 트래픽 흐름을 달성하는 것이 좋습니다. AS-Path 사전 지정은 유지 관리가 필요한 경우 트래픽을 OND에서 다른 곳으로 이동시키기 위해 로컬 게이트웨이 접두사에 사용됩니다. 고객 네트워크는 AS-Path 길이가 1인 Outpost에서 출발하는 경로를 AS-Path 길이가 4인 경로보다 선호해야 합니다.

고객 네트워크는 모든 OND에 동일한 속성을 가진 동일한 BGP 접두사를 알려야 합니다. Outpost 네트워크는 기본적으로 모든 업링크 간에 아웃바운드 트래픽의 부하를 분산합니다. 유지 관리가 필요한 경우 Outpost 측에서는 라우팅 정책을 사용하여 트래픽을 OND에서 다른 곳으로 이동합니다. 이러한 트래픽 이동에는 모든 OND의 고객 측에서 동일한 BGP 접두사가 필요합니다. 고객 네트워크에서 유지 관리가 필요한 경우 AS-Path 프리펜딩을 사용하여 특정 업링크에서 일시적으로 트래픽 배열을 이동하는 것이 좋습니다.

로컬 게이트웨이 고객 소유의 IP 서브넷 광고

기본적으로 로컬 게이트웨이는 VPC 내 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와의 통신을 용이하게 합니다. 하지만 고객 소유의 IP 주소 풀(CoIP)을 제공할 수 있습니다.

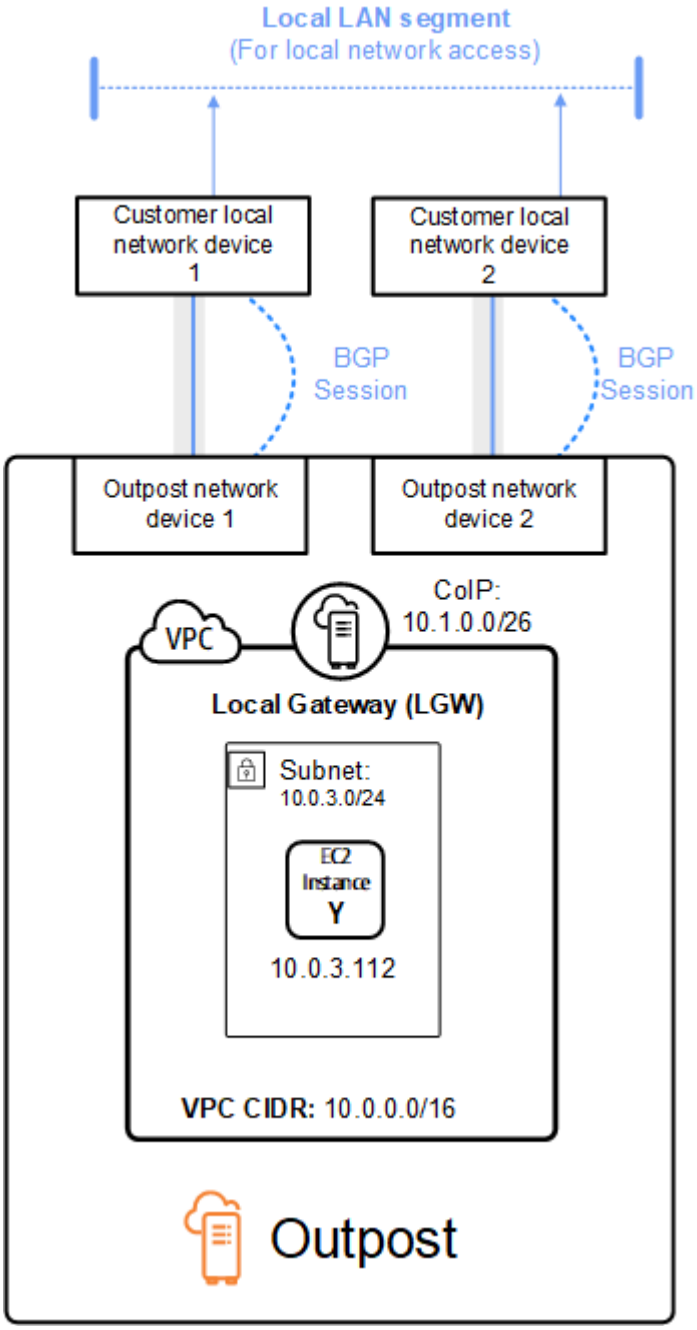
CoIP를 선택하면 설치 프로세스 중에 제공한 정보로 풀이 AWS 생성됩니다. 이 풀에서 탄력적 IP 주소를 생성한 다음, 해당 주소를 Outpost의 리소스(예: EC2 인스턴스)에 할당할 수 있습니다.

로컬 게이트웨이는 탄력적 IP 주소를 고객 소유 풀의 주소로 변환합니다. 로컬 게이트웨이는 변환된 주소를 온프레미스 네트워크 및 Outpost와 통신하는 기타 네트워크에 알립니다. 주소는 두 로컬 게이트웨이 BGP 세션 모두에서 로컬 네트워크 장치에 광고됩니다.

> **Tip**
>
> CoIP를 사용하지 않는 경우 BGP는 로컬 게이트웨이를 대상으로 하는 라우팅 테이블에 경로가 있는 Outpost의 모든 서브넷의 프라이빗 IP 주소를 광고합니다.

Outpost 네트워크 장치 두 개가 서비스 링크 VLAN을 통해 두 개의 고객 로컬 네트워크 장치에 연결된 Outpost가 있는 시나리오를 고려합니다. 다음과 같이 구성되어 있습니다.

- CIDR 블록 10.0.0.0/16과의 VPC
- CIDR 블록 10.0.3.0/24가 있는 VPC의 서브넷입니다.
- 프라이빗 IP 주소가 10.0.3.112인 서브넷의 EC2 인스턴스
- 고객 소유 IP 풀(10.1.0.0/26).
- 10.0.3.112를 10.1.0.2에 연결하는 탄력적 IP 주소 연결입니다.
- BGP를 사용하여 로컬 장치를 통해 온프레미스 네트워크에 10.1.0.0/26을 알리는 로컬 게이트웨이입니다.
- Outpost와 온프레미스 네트워크 간의 통신은 CoIP 탄력적 IP를 사용하여 Outpost의 인스턴스를 처리하며, VPC CIDR 범위는 사용되지 않습니다.


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

공유 AWS Outposts리소스로 작업하기

Outpost 공유를 통해 Outpost 소유자는 Outpost 사이트 및 서브넷을 포함한 Outpost 및 Outpost 리소스를 동일한 AWS 조직의 다른 AWS 계정과 공유할 수 있습니다. Outpost 소유자는 Outpost 리소스를 중앙에서 생성 및 관리하고 AWS 조직 내 여러 AWS 계정에서 리소스를 공유할 수 있습니다. 이를 통해 다른 소비자가 Outpost 사이트를 사용하고, VPC를 구성하고, 공유 Outpost에서 인스턴스를 시작 및 실행할 수 있습니다.

이 모델에서는 Outpost 리소스(소유자)를 소유한 AWS 계정을 사용하거나, 다음 리소스를 동일한 조직의 다른 AWS 계정(소비자)과 공유해야 합니다. 소비자는 자신의 계정으로 생성하는 Outpost에서 동일한 방식으로 공유된 Outpost의 리소스를 생성할 수 있습니다. 소유자는 생성한 Outpost의 관리 및 리소스를 관리할 책임이 있습니다. 소유자는 언제든지 공유 액세스를 변경하거나 취소할 수 있습니다. 용량 예약을 사용하는 인스턴스를 제외하고, 소유자는 소비자가 공유 Outpost에서 생성하는 리소스를 보고 수정하고 삭제할 수 있습니다. 소유자는 공유한 용량 예약으로 소비자가 시작한 인스턴스를 수정할 수 없습니다.

소비자는 용량 예약을 소비하는 리소스를 포함하여 공유된 Outpost의 리소스를 관리할 책임이 있습니다. 소비자는 다른 소비자 또는 용량 예약 소유자가 소유한 인스턴스를 보거나 수정할 수 없습니다. 또한 공유된 Outpost를 수정할 수 없습니다.

Outpost 소유자는 다음과 같이 Outpost 리소스를 공유할 수 있습니다.

- AWS Organizations 내 조직 내부의 특정 AWS 계정
- AWS Organizations 내 조직 내부의 조직 단위
- AWS Organizations의 전체 조직.

목차

- 공유 가능한 Outpost 리소스
- Outpost의 리소스 공유를 위한 사전 조건
- 관련 서비스
- 가용 영역 공유
- Outpost 리소스 공유
- 공유된 Outpost 리소스 공유 해제
- 공유 Outpost 리소스 식별
- 공유 Outpost 리소스 권한

- 결제 및 측정
- 제한 사항

공유 가능한 Outpost 리소스

Outpost 소유주는 이 섹션에 나열된 Outpost 자원을 소비자와 공유할 수 있습니다.

Outpost 랙 에 사용할 수 있는 리소스는 다음과 같습니다. 서버 리소스에 대해서는 Outpost 서버용 AWS Outposts 사용 설명서의 공유 AWS Outposts 리소스 사용을 참조하십시오.

- 할당된 전용 호스트 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 전용 호스트에서 EC2 인스턴스를 시작 및 실행합니다.
- 용량 예약 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 그들과 공유된 용량 예약을 식별합니다.
  - 용량 예약을 사용하는 인스턴스를 시작하고 관리합니다.
- 고객 소유 IP 주소(CoIP) 풀 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 고객 소유 IP 주소를 할당하고 인스턴스에 연결합니다.
- 로컬 게이트웨이 라우팅 테이블 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 로컬 게이트웨이에 대한 VPC 연결을 생성하고 관리합니다.
  - 로컬 게이트웨이 라우팅 테이블 및 가상 인터페이스의 구성을 볼 수 있습니다.
- Outpost – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - Outpost에서 서브넷을 생성하고 관리합니다.
  - Outpost에서 EBS 볼륨을 생성하고 관리합니다.
  - AWS Outposts API를 사용하여 Outpost에 대한 정보를 봅니다.
- Outpost의 S3 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - Outpost에서 S3 버킷, 액세스 포인트 및 엔드포인트를 생성하고 관리합니다.
- 사이트 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 사이트에서 Outpost를 생성하고, 관리하고, 제어합니다.
- 서브넷 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 서브넷에 대한 정보 보기
  - 서브넷에서 EC2 인스턴스를 시작하고 실행합니다.

Amazon VPC 콘솔을 사용하여 Outpost 서브넷을 공유합니다. 자세한 내용은 Amazon VPC 사용 설명서의 서브넷 공유를 참조하십시오.

Outpost의 리소스 공유를 위한 사전 조건

- AWS Organizations의 조직 또는 조직 단위와 Outpost 리소스를 공유하려면 AWS Organizations과(와) 공유를 활성화해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 AWS Organizations과(와) 공유 활성화를 참조하십시오.
- Outpost 리소스를 공유하려면 AWS 계정에서 소유하고 있어야 합니다. 공유된 Outpost 리소스를 공유할 수 없습니다.
- Outpost 리소스를 공유하려면 조직 내 계정과 공유해야 합니다.

관련 서비스

용량 예약 공유는 AWS Resource Access Manager(AWS RAM)과(와) 통합됩니다. AWS RAM은(는) 모든 AWS 계정 또는 AWS Organizations을(를) 통해 AWS 리소스를 공유하도록 해주는 서비스입니다. AWS RAM을(를) 사용하여 리소스 공유 생성으로 소유한 리소스를 공유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. 소비자는 개인 AWS 계정의 조직 단위 또는 AWS Organizations의 전체 조직일 수 있습니다.

AWS RAM에 대한 자세한 내용은 AWS RAM 사용 설명서를 참조하십시오.

가용 영역 공유

리전의 가용 영역에 걸쳐 리소스가 배포될 수 있도록 각 계정의 이름에 가용 영역을 독립적으로 매핑합니다. 이로 인해 계정 전체에서 가용 영역 이름의 차이가 발생할 수 있습니다. 예를 들어 AWS 계정의 `us-east-1a` 가용 영역은 다른 AWS 계정에 대한 `us-east-1a`로 위치가 동일하지 않을 수 있습니다.

계정과 관련된 Outpost 리소스의 위치를 확인하려면 가용 영역 ID(AZ ID)를 사용해야 합니다. AZ ID는 모든 AWS 계정의 가용 영역에 대한 고유하고 일관된 식별자입니다. 예를 들어, `use1-az1`은 `us-east-1` 리전의 AZ ID이고, 모든 AWS 계정에서 위치가 동일합니다.

계정의 가용 영역에 대한 AZ ID 보려면

1. https://console.aws.amazon.com/ramAWS RAM에서 콘솔을 엽니다.
2. 현재 지역의 AZ ID는 화면의 오른쪽에 있는 사용자 AZ ID 패널에 표시됩니다.

> **Note**
>
> 로컬 게이트웨이 라우팅 테이블은 Outpost와 동일한 AZ에 있으므로 라우팅 테이블에 AZ ID를 지정할 필요가 없습니다.

Outpost 리소스 공유

소유주가 소비자와 Outpost를 공유하는 경우, 소비자는 자신의 계정으로 Outpost에 리소스를 생성하는 것과 동일한 방식으로 Outpost에서 리소스를 생성할 수 있습니다. 공유 로컬 게이트웨이 라우팅 테이블에 액세스할 수 있는 소비자는 VPC 연결을 생성하고 관리할 수 있습니다. 자세한 내용은 공유 가능한 Outpost 리소스 단원을 참조하십시오.

Outpost 리소스를 공유하려면 리소스 공유에 추가해야 합니다. 리소스 공유는 여러 AWS 계정에서 리소스를 공유할 수 있게 해주는 AWS RAM 리소스입니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. AWS Outposts 콘솔을 사용하여 Outpost 리소스를 공유하면 기존 리소스 공유에 추가합니다. 새 리소스 공유에 Outpost 리소스를 추가하려면, 우선 AWS RAM 콘솔을 사용해 리소스 공유를 생성해야 합니다.

AWS Organizations의 조직에 속해 있고 조직 내의 공유가 활성화되어 있으면, 조직의 소비자에게 AWS RAM 콘솔에서 공유 Outpost 리소스에 대한 액세스 권한을 부여할 수 있습니다. 그렇지 않으면 소비자는 리소스 공유에 가입하라는 초대장을 받고 초대를 수락한 후 공유된 리소스의 액세스 권한을 받습니다.

AWS Outposts 콘솔, AWS RAM 콘솔 또는 AWS CLI을(를) 사용하여 소유하고 있는 Outpost 리소스를 공유할 수 있습니다.

AWS Outposts 콘솔을 사용하여 소유하고 있는 Outpost를 공유하려면

1. https://console.aws.amazon.com/outposts/에서 AWS Outposts 콘솔을 엽니다.
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 리소스 공유를 선택합니다.
5. 리소스 공유 생성을 선택합니다.

다음 절차에 따라 Outpost 공유를 완료할 수 있는 AWS RAM 콘솔로 리디렉션됩니다. 소유한 로컬 게이트웨이 라우팅 테이블을 공유하려면 다음 절차도 사용합니다.

AWS RAM 콘솔을 사용하여 소유한 Outpost 또는 로컬 게이트웨이 라우팅 테이블을 공유하려면

AWS RAM 사용 설명서의 리소스 공유 생성을 참조하십시오.

AWS CLI을(를) 사용하여 소유한 Outpost 또는 로컬 게이트웨이 라우팅 테이블을 공유하려면

create-resource-share 명령을 사용합니다.

공유된 Outpost 리소스 공유 해제

공유 Outpost가 공유되지 않으면 소비자는 AWS Outposts 콘솔에서 더 이상 Outpost를 볼 수 없습니다. Outpost에서 새 서브넷을 생성하거나, Outpost에 새 EBS 볼륨을 생성하거나, AWS Outposts 콘솔 또는 AWS CLI을(를) 사용하여 Outpost 세부 정보 및 인스턴스 유형을 볼 수 없습니다. 소비자가 만든 기존 서브넷, 볼륨 또는 인스턴스는 삭제되지 않습니다. 소비자가 Outpost에서 생성한 기존 서브넷은 여전히 새 인스턴스를 시작하는 데 사용할 수 있습니다.

공유된 로컬 게이트웨이 라우팅 테이블이 공유되지 않는 경우, 소비자는 더 이상 새 VPC 연결을 생성할 수 없습니다. 소비자가 생성한 기존 VPC 연결은 모두 라우팅 테이블과 연결된 상태로 유지됩니다. 이러한 VPC의 리소스는 계속해서 트래픽을 로컬 게이트웨이로 라우팅할 수 있습니다.

소유하고 있는 공유 Outpost리소스의 공유를 해제하려면 리소스 공유에서 제거해야 합니다. 이를 위해 AWS RAM 콘솔이나 AWS CLI을(를) 사용할 수 있습니다.

AWS RAM 콘솔을 사용하여 소유하고 있는 공유 Outpost 리소스를 공유 해제하려면

AWS RAM 사용 설명서의 리소스 공유 업데이트를 참조하십시오.

AWS CLI를 사용하여 소유하고 있는 공유 Outpost 리소스를 공유 해제하려면

disassociate-resource-share 명령을 사용합니다.

공유 Outpost 리소스 식별

소유자와 소비자는 AWS Outposts 콘솔 및 AWS CLI을(를) 사용하여 공유 Outpost를 식별할 수 있습니다. AWS CLI을(를) 사용하여 공유 로컬 게이트웨이 라우팅 테이블을 식별할 수 있습니다.

AWS Outposts 콘솔을 사용하여 공유 Outpost를 식별하려면

1. https://console.aws.amazon.com/outposts/에서 AWS Outposts 콘솔을 엽니다.

2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 소유자 ID를 보고 Outpost 소유자의 AWS 계정 ID를 식별합니다.

AWS CLI를 사용하여 공유 Outpost 리소스를 식별하려면

list-outposts 및 describe-local-gateway-route-tables 명령을 사용합니다. 이 명령은 사용자가 소유한 Outpost 리소스 및 사용자와 공유하는 Outpost 리소스를 반환합니다. `OwnerId`은(는) Outpost 소유자의 AWS 계정 ID를 보여줍니다.

공유 Outpost 리소스 권한

소유자에 대한 권한

소유자는 Outpost의 관리 및 자원을 관리할 책임이 있습니다. 소유자는 언제든지 공유 액세스를 변경하거나 취소할 수 있습니다. 공유 Outpost에서 소비자가 생성한 리소스를 보고 수정하고 삭제하는 데 AWS Organizations을(를) 사용할 수 있습니다.

소비자에 대한 권한

소비자는 자신의 계정으로 생성하는 Outpost에서 동일한 방식으로 공유된 Outpost의 리소스를 생성할 수 있습니다. 소비자는 공유된 Outpost에서 시작된 리소스를 관리할 책임이 있습니다. 소비자는 다른 소비자나 Outpost 소유자가 소유한 인스턴스를 보거나 수정할 수 없으며 공유된 Outpost를 수정할 수 없습니다.

결제 및 측정

공유하는 Outpost의 리소스에 대한 비용이 소유자에게 청구됩니다. 또한 AWS 리전에서 유입되는 Outpost의 서비스 링크 VPN 트래픽과 관련된 모든 데이터에 대한 전송 요금도 청구됩니다.

로컬 게이트웨이 라우팅 테이블 공유에 대한 추가 비용은 없습니다. 공유 서브넷의 경우 VPN 연결, NAT 게이트웨이, 프라이빗 링크 연결 AWS Direct Connect 등의 VPC 수준 리소스에 대한 요금이 VPC 소유자에게 청구됩니다.

소비자는 로드 밸런서 및 Amazon RDS 데이터베이스와 같은 공유 Outpost에서 생성한 애플리케이션 리소스에 대해 요금이 청구됩니다. 또한 소비자는 AWS 리전에서 데이터를 전송할 때 요금이 청구됩니다.

제한 사항

다음 제한은 AWS Outposts 공유를 사용한 작업에 적용됩니다.

- 공유 서브넷에 대한 제한은 AWS Outposts 공유 작업에 적용됩니다. Amazon VPC에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 제한 사항을 참조하십시오.
- 서비스 할당량은 개별 계정별로 적용됩니다.

보안 내부 AWS Outposts

AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오. AWS Outposts
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

보안 및 규정 준수에 대한 자세한 내용은 AWS Outposts 랙 FAQ 참조하십시오. AWS Outposts

이 설명서는 공동 책임 모델을 사용할 AWS Outposts때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 구성하는 방법을 보여줍니다. 또한 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

내용

- 데이터 보호: AWS Outposts
- ID 및 액세스 관리 (IAM) 에 대한 AWS Outposts
- 의 인프라 보안 AWS Outposts
- 탄력성: AWS Outposts
- 규정 준수 검증: AWS Outposts
- AWS Outposts 워크로드를 위한 인터넷 액세스

데이터 보호: AWS Outposts

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Outposts. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서

호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 AWS 서비스 사용하는 보안 구성 및 관리 작업이 포함됩니다.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이러한 방식에는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다.

데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

유휴 시 암호화

AWS Outposts를 사용하면 저장된 모든 데이터가 암호화됩니다. 키 자료는 이동식 장치에 저장된 외부 키인 Nitro 보안 키(NSK)에 래핑됩니다. Outpost 랙의 데이터를 해독하려면 NSK가 필요합니다.

Amazon EBS 암호화를 EBS 볼륨과 스냅샷에 사용할 수 있습니다. Amazon EBS 암호화는 AWS Key Management Service (AWS KMS) 및 KMS 키를 사용합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 암호화를 참조하세요.

전송 중 데이터 암호화

AWS Outpost와 해당 지역 간의 전송 데이터를 암호화합니다. AWS 자세한 정보는 서비스 링크를 통한 연결을 참조하세요.

TLS(전송 계층 보안)와 같은 암호화 프로토콜을 사용하여 로컬 게이트웨이를 통해 로컬 네트워크로 전송 중인 민감한 데이터를 암호화할 수 있습니다.

데이터 삭제

인스턴스를 중지하거나 종료하면 인스턴스에 할당된 메모리는 새 인스턴스에 할당되기 전에 하이퍼바이저에서 스크러빙(0으로 설정)되며 스토리지의 모든 블록은 재설정됩니다.

Nitro 보안 키를 파괴하면 Outpost의 데이터가 암호적으로 파기됩니다.

ID 및 액세스 관리 (IAM) 에 대한 AWS Outposts

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. AWS IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인)

및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS Outposts IAM은 추가 요금 없이 사용할 수 있습니다.

내용

- AWS Outposts와 IAM의 작동 방식
- AWS Outposts 정책 예제
- AWS Outposts의 서비스 링크 역할 사용
- AWS 관리형 정책 대상 AWS Outposts

AWS Outposts와 IAM의 작동 방식

IAM을 사용하여 Outposts에 대한 액세스를 관리하기 전에 AWS Outposts에서 사용할 수 있는 IAM 기능에 대해 알아보십시오. AWS

Outposts와 함께 AWS 사용할 수 있는 IAM 기능

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

Outposts에 대한 ID 기반 정책 AWS

ID 기반 정책 지원	예

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

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

Outposts의 ID 기반 정책 예제 AWS

AWS Outposts ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Outposts 정책 예제

Outposts 내의 리소스 기반 정책 AWS

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 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

AWS Outposts를 위한 정책 조치

정책 작업 지원	예

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

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

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

AWS Outposts 작업 목록을 보려면 서비스 권한 부여 AWS Outposts 참조에 정의된 작업을 참조하십시오.

AWS Outposts의 정책 조치는 조치 앞에 다음 접두사를 사용합니다.

```
outposts
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

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

```
"Action": "outposts:List*"
```

AWS Outposts를 위한 정책 리소스

정책 리소스 지원	예

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

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

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

일부 AWS Outposts API 액션은 여러 리소스를 지원합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
    "resource1",
    "resource2"
]
```

AWS Outposts 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 AWS Outposts참조에 정의된 리소스 유형을 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Outposts가 정의한 작업을 참조하십시오.

AWS Outposts의 정책 조건 키

서비스별 정책 조건 키 지원	예

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

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

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

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

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

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

AWS Outposts 조건 키 목록을 보려면 서비스 권한 부여 참조의 조건 키를 참조하십시오 AWS Outposts. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 작업 정의 기준을 참조하십시오. AWS Outposts

AWS Outposts ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Outposts 정책 예제

Outposts의 AWS 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.

ABAC (아웃포스트 포함) AWS

ABAC 지원(정책의 태그)	예

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

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

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

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

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

AWS Outposts에서 임시 자격 증명 사용

임시 보안 인증 지원	예

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

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

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

Outposts에 대한 AWS 서비스 간 사용자 권한

전달 액세스 세션(FAS) 지원	예

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

AWS Outpost의 서비스 역할

서비스 역할 지원	아니요

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

Outposts의 서비스 연계 역할 AWS

서비스 링크 역할 지원	예

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

AWS Outposts 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS Outposts의 서비스 링크 역할 사용

AWS Outposts 정책 예제

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

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

각 리소스 유형의 ARN 형식을 비롯하여 AWS AWS Outposts Outposts에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 작업, 리소스 및 조건 키를 참조하십시오.

내용

- 정책 모범 사례
- 예제: 리소스 수준 권한 사용

정책 모범 사례

ID 기반 정책은 누군가가 계정에서 AWS Outposts 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 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 설명서에 있는 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. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 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 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

예제: 리소스 수준 권한 사용

다음 예에서는 리소스 수준 권한을 사용하여 지정된 Outpost에 대한 정보를 가져올 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

다음 예제에서는 리소스 수준 권한을 사용하여 지정된 사이트에 대한 정보를 가져올 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

AWS Outposts의 서비스 링크 역할 사용

AWS Outposts AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Outposts서비스 연결 역할은 사전 정의되며 서비스가 사용자를 AWS Outposts 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS Outposts 보다 효율적으로 설정할 수 있습니다. AWS Outposts 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 역할만 맡을 AWS Outposts 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 링크 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Outposts 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

AWS Outposts에 대한 서비스 링크 역할 권한

AWS Outposts AWSServiceRoleForOutposts_ ***OutpostId ## ### ## ### #####. – Outposts#*** 사용자를 대신하여 개인 연결을 위한 리소스에 AWS 액세스할 수 있도록 합니다. 이 서비스 링크 역할은 프라이빗 연결 구성을 허용하고, 네트워크 인터페이스를 생성하고, 이를 서비스 링크 엔드포인트 인스턴스에 연결합니다.

AWSServiceRoleForOutposts_ *OutpostID ### ## ### ## #### ####* 역할을 수임합니다.

- `outposts.amazonaws.com`

AWSServiceRoleForOutposts_ ***OutpostID*** 서비스 연결 역할에는 다음 정책이 포함됩니다.

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ 아웃포스트ID

AWSOutpostsServiceRolePolicy정책은 에서 관리하는 리소스에 액세스할 수 있도록 하는 서비스 연결 역할 정책입니다. AWS AWS Outposts

이 정책을 통해 지정된 리소스에서 다음 작업을 AWS Outposts 완료할 수 있습니다.

- 작업: `all AWS resources`에 대한 `ec2:DescribeNetworkInterfaces`
- 작업: `all AWS resources`에 대한 `ec2:DescribeSecurityGroups`
- 작업: `all AWS resources`에 대한 `ec2:CreateSecurityGroup`
- 작업: `all AWS resources`에 대한 `ec2:CreateNetworkInterface`

AWSOutpostsPrivateConnectivityPolicy_ ***OutPostId*** 정책을 사용하면 지정된 리소스에서 다음 작업을 AWS Outposts 완료할 수 있습니다.

- 작업: `all AWS resources that match the following Condition:`에 대한 `ec2:AuthorizeSecurityGroupIngress`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: `all AWS resources that match the following Condition:`에 대한 `ec2:AuthorizeSecurityGroupEgress`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: `all AWS resources that match the following Condition:`에 대한 `ec2:CreateNetworkInterfacePermission`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: `all AWS resources that match the following Condition:`에 대한 `ec2:CreateTags`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

AWS Outposts에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 Outpost의 개인 연결을 구성하면 서비스 연결 AWS Management Console역할이 AWS Outposts 자동으로 생성됩니다.

자세한 정보는 VPC를 사용한 서비스 링크 프라이빗 연결을 참조하세요.

AWS Outposts에 대한 서비스 링크 역할 편집

AWS Outposts AWSServiceRoleForOutposts_ *OutpostID* 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 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 링크 역할 편집을 참조하세요.

AWS Outposts에 대한 서비스 링크 역할 삭제

서비스 링크 역할이 필요한 기능이나 서비스가 더 이상 필요하지 않으면 그 역할을 삭제하는 것이 좋습니다. 이렇게 하면 적극적으로 모니터링되거나 유지 관리되지 않는 미사용 개체를 피할 수 있습니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> AWS Outposts 서비스가 이 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

> **Warning**
>
> AWSServiceRoleForOutposts_ OutpostID 서비스 연결 역할을 삭제하려면 먼저 *Outpost#* 삭제해야 합니다. 다음 절차에 따라 Outpost가 삭제됩니다.

시작하기 전에 Outpost가 () 를 사용하여 공유되고 있지 않은지 확인하세요. AWS Resource Access Manager AWS RAM자세한 정보는 공유된 Outpost 리소스 공유 해제을 참조하세요.

AWSServiceRoleForOutposts_ ***AWS Outposts OutPostId## #### #### #####***

- Outpost를 삭제하려면 AWS 기업 지원팀에 문의하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForOutposts _ *OutpostID* 서비스 연결 역할을 삭제하십시오. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

AWS Outposts 서비스 링크 역할이 지원되는 리전

AWS Outposts 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할을 사용할 수 있습니다. 자세한 내용은 AWS Outposts 엔드포인트 및 할당량을 참조하세요.

AWS 관리형 정책 대상 AWS Outposts

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

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

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSOutpostsServiceRolePolicy

이 정책은 사용자를 AWS Outposts 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결됩니다. 자세한 정보는 서비스 링크 역할 사용을 참조하세요.

AWS 관리형 정책: AWSOutpostsPrivateConnectivityPolicy

이 정책은 사용자를 AWS Outposts 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결됩니다. 자세한 정보는 서비스 링크 역할 사용을 참조하세요.

AWS OutpostsAWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Outposts 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다.

변경 사항	설명	날짜
AWS Outposts 변경 내용 추적 시작	AWS Outposts AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2019년 12월 3일

의 인프라 보안 AWS Outposts

관리형 서비스인 AWS Outposts는 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS Outposts에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Outpost에서 실행되는 EC2 인스턴스 및 EBS 볼륨에 제공되는 인프라 보안에 대한 자세한 내용은 Amazon EC2의 인프라 보안을 참조하세요.

VPC 흐름 로그는 지역에서와 동일한 방식으로 작동합니다. AWS 즉, 분석을 GuardDuty 위해 CloudWatch 로그, Amazon S3 또는 Amazon에 게시할 수 있습니다. Outpost가 연결이 끊긴 상태일 때는 데이터를 다른 서비스에서 CloudWatch 볼 수 없도록 이러한 서비스에 게시하려면 해당 지역으로 데이터를 다시 보내야 합니다.

장비에 대한 변조 모니터링 AWS Outposts

아무도 장비를 개조, 변경, 역설계 또는 변조하지 않도록 하십시오. AWS Outposts AWS Outposts 장비에 서비스 약관 준수를 보장하기 위해 변조 모니터링 기능을 장착할 수 있습니다.AWS

탄력성: AWS Outposts

AWS Outposts 가용성이 높도록 설계되었습니다. Outpost 랙은 예비 전원 및 네트워킹 장비를 사용하도록 설계되었습니다. 추가적인 복원력을 위해서는 Outpost에 이중 전력과 중복 네트워크 연결을 제공하는 것이 좋습니다.

고가용성을 위해, Outpost 랙에서 추가 내장 용량과 상시 활성 용량을 프로비저닝하여 . Outpost 용량 구성은 프로덕션 환경에서 작동하도록 설계되었으며, 용량을 프로비저닝하면 각 인스턴스 패밀리에 대해 N+1 인스턴스를 지원합니다. AWS 은(는) 기본 호스트 문제가 있는 경우 복구 및 장애 조치를 수행할 수 있도록 미션 크리티컬 애플리케이션에 충분한 추가 용량을 할당할 것을 권장합니다. Amazon CloudWatch 용량 가용성 지표를 사용하고 경보를 설정하여 애플리케이션 상태를 모니터링하고, 자동 복구 옵션을 구성하는 CloudWatch 작업을 생성하고, 시간 경과에 따른 Outposts의 용량 사용률을 모니터링할 수 있습니다.

Outpost를 생성할 때는 지역에서 가용 영역을 선택합니다. AWS 이 가용 영역은 API 호출에 대한 응답, Outpost 모니터링, Outpost 업데이트와 같은 컨트롤 플레인 작업을 지원합니다. 가용 영역이 제공하는 복원력을 활용하려면 각각 다른 가용 영역에 연결된 여러 Outpost에 애플리케이션을 배포할 수 있습니다. 이를 통해 추가 애플리케이션 복원력을 구축하고 단일 가용 영역에 대한 의존성을 피할 수 있습니다. 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

배치 그룹을 분산 전략과 함께 사용하여 인스턴스가 서로 다른 Outpost 랙에 배치되도록 할 수 있습니다. 이렇게 하면 상호 관련된 장애를 줄이는 데 도움이 될 수 있습니다. 자세한 내용은 Outpost의 배치 그룹을(를) 참조하세요.

Amazon EC2 Auto Scaling을 사용하여 Outpost에서 인스턴스를 시작하고 Application Load Balancer를 생성하여 인스턴스 간에 트래픽을 분산할 수 있습니다. 자세한 내용은 AWS Outposts에서 Application Load Balancer 구성을 참조하세요.

규정 준수 검증: AWS Outposts

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.

- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 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 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

AWS Outposts 워크로드를 위한 인터넷 액세스

이 섹션에서는 AWS Outposts 워크로드가 다음과 같은 방식으로 인터넷에 액세스하는 방법을 설명합니다.

- 상위 AWS 지역을 통해
- 로컬 데이터 센터 네트워크를 통해

상위 AWS 지역을 통한 인터넷 액세스

이 옵션에서 Outposts의 워크로드는 서비스 링크를 통해 인터넷에 액세스한 다음 상위 지역의 인터넷 게이트웨이 (IGW) 를 통해 인터넷에 액세스합니다. AWS 인터넷으로 향하는 아웃바운드 트래픽은 VPC에서 인스턴스화된 NAT 게이트웨이를 통해 이루어질 수 있습니다. 수신 및 송신 트래픽에 대한 추가 보안을 위해 해당 CloudFront 지역의, 및 Amazon과 같은 AWS AWS WAF보안 서비스를 사용할 수 있습니다. AWS Shield AWS

Outposts 서브넷의 라우팅 테이블 설정은 로컬 게이트웨이 라우팅 테이블을 참조하십시오.

고려 사항

- 다음과 같은 경우 이 옵션을 사용하십시오.
  - AWS 지역 내 여러 AWS 서비스를 통해 인터넷 트래픽을 보호하려면 유연성이 필요합니다.
  - 데이터 센터 또는 코로케이션 시설에는 인터넷 지점이 없습니다.
- 이 옵션에서는 트래픽이 상위 AWS 지역을 통과해야 하므로 지연 시간이 발생합니다.
- AWS 지역별 데이터 전송 요금과 마찬가지로 상위 가용 영역에서 Outpost로 데이터를 전송하는 경우에도 요금이 부과됩니다. 데이터 전송에 대한 자세한 내용은 Amazon EC2 온디맨드 요금을 참조하십시오.
- 서비스 링크 대역폭의 사용률이 증가할 것입니다.

다음 이미지는 상위 AWS 지역을 통과하는 Outposts 인스턴스의 워크로드와 인터넷 간의 트래픽을 보여줍니다.

로컬 데이터 센터 네트워크를 통한 인터넷 액세스

이 옵션에서는 Outposts에 있는 워크로드가 로컬 데이터 센터를 통해 인터넷에 액세스합니다. 인터넷에 액세스하는 워크로드 트래픽은 로컬 인터넷 접속 지점 및 송신을 통해 로컬로 이동합니다. 로컬 데이터 센터 네트워크의 보안 계층은 Outposts 워크로드 트래픽을 보호하는 역할을 합니다.

Outposts 서브넷의 라우팅 테이블 설정은 로컬 게이트웨이 라우팅 테이블을 참조하십시오.

고려 사항

- 다음과 같은 경우 이 옵션을 사용하십시오.
  - 워크로드를 처리하려면 지연 시간이 짧은 인터넷 서비스 액세스가 필요합니다.
  - 데이터 전송 (DTO) 요금은 발생하지 않는 것이 좋습니다.
  - 컨트롤 플레인 트래픽에 대한 서비스 링크 대역폭을 보존하고 싶습니다.
- 보안 계층은 Outposts 워크로드 트래픽을 보호하는 역할을 합니다.
- 직접 VPC 라우팅 (DVR) 을 선택하는 경우 Outposts CIDR이 온프레미스 CIDR과 충돌하지 않도록 해야 합니다.
- 기본 경로 (0/0) 가 로컬 게이트웨이 (LGW) 를 통해 전파되는 경우 인스턴스가 서비스 엔드포인트에 도달하지 못할 수 있습니다. 또는 VPC 엔드포인트를 선택하여 원하는 서비스에 연결할 수 있습니다.

다음 이미지는 Outposts 인스턴스의 워크로드와 로컬 데이터 센터를 통과하는 인터넷 간의 트래픽을 보여줍니다.

Outpost 모니터링

AWS Outposts은(는) 모니터링 및 로깅 기능을 제공하는 다음 서비스와 통합됩니다.

CloudWatch 측정 항목

CloudWatch Amazon을 사용하면 Outposts의 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 집합으로 가져올 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 CloudWatch 측정치는 다음과 같습니다. AWS Outposts 단원을 참조하십시오.

CloudTrail 로그

AWS CloudTrail을(를) 사용하여 AWS API 호출에 대한 자세한 정보를 캡처합니다. Amazon S3에 이러한 호출을 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하여 어떤 전화가 걸렸는지, 어떤 소스 IP 주소, 전화를 걸었는지, 언제 전화를 걸었는지 등의 정보를 확인할 수 있습니다.

CloudTrail 로그에는 API 작업에 대한 호출에 대한 정보가 포함됩니다AWS Outposts. 또한 Amazon EC2 및 Amazon EBS와 같은 Outpost에 있는 서비스에서 API 작업을 호출하는 데 대한 정보도 포함되어 있습니다. 자세한 내용은 AWS Outposts자세한 내용은 CloudTrail 단원을 참조하십시오.

VPC 흐름 로그

VPC 흐름 로그를 사용하여 Outpost와 Outpost 내에서 들어오고 나가는 트래픽에 대한 자세한 정보를 캡처합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하십시오.

트래픽 미러링

트래픽 미러링을 사용하여 Outpost의 네트워크 트래픽을 복사하고 Outpost의 out-of-band 보안 및 모니터링 어플라이언스로 전달할 수 있습니다. 미러링된 트래픽을 콘텐츠 검사, 위협 모니터링 또는 문제 해결에 사용할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud용 트래픽 미러링 가이드를 참조하십시오.

AWS Health Dashboard

AWS Health Dashboard은(는) 정보를 표시하고 AWS 리소스의 상태 변경에 따라 작동되는 알림도 제공합니다. 이 정보는 최근 이벤트와 예정된 이벤트를 카테고리별로 보여주는 대시보드와 지난 90일간의 모든 이벤트를 보여주는 전체 이벤트 로그의 두 가지 방법으로 표시됩니다. 예를 들어 서비스 링크의 연결 문제가 발생하면 대시보드와 이벤트 로그에 나타나는 이벤트가 시작되고 이벤트 로그에 90일 동안 남아 있게 됩니다. AWS Health 서비스 부분은 설정이 AWS Health Dashboard

필요하지 않으며, 계정에서 인증된 사용자면 누구나 볼 수 있습니다. 자세한 내용은 AWS Health Dashboard 시작하기를 참조하십시오.

CloudWatch 측정치는 다음과 같습니다. AWS Outposts

AWS OutpostsOutposts를 CloudWatch 위해 Amazon에 데이터 포인트를 게시합니다. CloudWatch 이러한 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 예를 들어, 지정된 기간 동안 Outpost에 사용 가능한 인스턴스 용량을 모니터링할 수 있습니다. 각 데이터 포인트에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어, `ConnectedStatus` 지표를 모니터링하는 CloudWatch 경보를 만들 수 있습니다. 평균 지표가 다음 보다 1 작으면 이메일 주소로 알림을 보내는 등의 작업을 시작할 CloudWatch 수 있습니다. 그런 다음 Outpost 운영에 영향을 미칠 수 있는 잠재적인 온프레미스 또는 업링크 네트워킹 문제를 조사할 수 있습니다. 일반적인 문제로는 방화벽 및 NAT 규칙에 대한 최근의 온프레미스 네트워크 구성 변경 또는 인터넷 연결 문제 등이 있습니다. `ConnectedStatus` 문제의 경우, 온프레미스 네트워크 내에서 AWS 리전 연결을 확인하고 문제가 지속되면 AWS Support에 문의하는 것이 좋습니다.

CloudWatch 경보 생성에 대한 자세한 내용은 Amazon 사용 설명서의 Amazon CloudWatch Alarms 사용을 참조하십시오. CloudWatch 에 대한 CloudWatch 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

내용

- Outpost 지표
- Outpost 지표 차원
- 전초 기지의 CloudWatch 지표 보기

Outpost 지표

`AWS/Outposts` 네임스페이스에 포함된 지표는 다음과 같습니다.

`ConnectedStatus`

Outpost의 서비스 링크 연결 상태. 평균 통계가 1 이하이면 연결이 손상된 것입니다.

단위: 수

최대 해상도: 1분

통계: 가장 유용한 통계는 Average입니다.

차원: OutpostId

CapacityExceptions

인스턴스 시작에 대한 용량 부족 오류 수입니다.

단위: 수

최대 해상도: 5분

통계: 가장 유용한 통계는 Maximum 및 Minimum입니다.

치수: InstanceType 및 OutpostId

IfTrafficIn

Outposts 가상 인터페이스 (VIF) 가 연결된 로컬 네트워크 디바이스로부터 수신하는 데이터의 비트 전송률입니다.

단위: 초당 비트

최대 해상도: 5분

통계: 가장 유용한 통계는 Max 및 Min입니다.

로컬 게이트웨이 VIF (lgw-vif) 의 크기:, 및 OutpostsId VirtualInterfaceGroupId VirtualInterfaceId

서비스 링크 VIF (sl-vif) 의 크기: 및 OutpostsId VirtualInterfaceId

IfTrafficOut

Outposts 가상 인터페이스 (VIF) 가 연결된 로컬 네트워크 장치로 전송하는 데이터의 비트 전송률입니다.

단위: 초당 비트

최대 해상도: 5분

통계: 가장 유용한 통계는 Max 및 Min입니다.

로컬 게이트웨이 VIF (lgw-vif) 의 크기:, 및 `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

서비스 링크 VIF (sl-vif) 의 크기: 및 `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

사용 가능한 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 `Average` 및 `pNN.NN`입니다(백분위수).

치수: 및 `InstanceFamily` `OutpostId`

`InstanceFamilyCapacityUtilization`

사용 중인 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 `Average` 및 `pNN.NN`입니다(백분위수).

차원: `Account`, `InstanceFamily`, `OutpostId`

`InstanceTypeCapacityAvailability`

사용 가능한 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 `Average` 및 `pNN.NN`입니다(백분위수).

치수: `InstanceType` 및 `OutpostId`

`InstanceTypeCapacityUtilization`

사용 중인 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 `Average` 및 `pNN.NN`입니다(백분위수).

차원: `Account`, `InstanceType`, `OutpostId`

`UsedInstanceType_Count`

Amazon RDS(관계형 데이터베이스 서비스) 또는 Application Load Balancer와 같은 관리형 서비스에서 사용하는 모든 인스턴스 유형을 포함하여 현재 사용 중인 인스턴스 유형의 수입니다. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 수

최대 해상도: 5분

차원: `Account`, `InstanceType`, `OutpostId`

`AvailableInstanceType_Count`

사용 가능한 인스턴스 유형 수. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 수

최대 해상도: 5분

치수: `InstanceType` 및 `OutpostId`

`AvailableReservedInstances`

Outpost에서 온디맨드 용량 예약(ODCR)을 위해 사용할 수 있는 인스턴스 수. 이 지표는 Amazon EC2 예약 인스턴스를 측정하지 않습니다.

단위: 수

최대 해상도: 5분

치수: `InstanceType` 및 `OutpostId`

`UsedReservedInstances`

Outpost에서 온디맨드 용량 예약(ODCR)을 위해 사용할 수 있는 인스턴스 수. 이 지표는 Amazon EC2 예약 인스턴스를 측정하지 않습니다.

단위: 수

최대 해상도: 5분

치수: `InstanceType` 및 `OutpostId`

`TotalReservedInstances`

Outpost에서 온디맨드 용량 예약(ODCR)을 위해 사용할 수 있는 인스턴스 수. 이 지표는 Amazon EC2 예약 인스턴스를 측정하지 않습니다.

단위: 수

최대 해상도: 5분

치수: `InstanceType` 및 `OutpostId`

`EBSVolumeTypeCapacityUtilization`

사용 중인 EBS 볼륨 유형 용량의 백분율.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 `Average` 및 `pNN.NN`입니다(백분위수).

치수: `VolumeType` 및 `OutpostId`

`EBSVolumeTypeCapacityAvailability`

사용 가능한 EBS 볼륨 유형 용량의 비율입니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

치수: VolumeType 및 OutpostId

EBSVolumeTypeCapacityUtilizationGB

EBS 볼륨 유형에 사용 중인 기가바이트 수입니다.

단위: 기가바이트

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

치수: VolumeType 및 OutpostId

EBSVolumeTypeCapacityAvailabilityGB

EBS 볼륨 유형에 사용할 수 있는 용량의 기가바이트 수입니다.

단위: 기가바이트

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

치수: VolumeType 및 OutpostId

Outpost 지표 차원

Outpost의 지표를 필터링하려면 다음 차원을 사용합니다.

측정기준	설명
Account	용량을 사용하는 계정 또는 서비스.
InstanceFamily	인스턴스 패밀리.
InstanceType	인스턴스 유형.
OutpostId	Outpost의 ID.

측정기준	설명
VolumeType	EBS 볼륨 유형.
VirtualInterfaceId	로컬 게이트웨이 또는 서비스 링크 가상 인터페이스 (VIF) 의 ID.
VirtualInterfaceGroupId	로컬 게이트웨이 VIF (가상 인터페이스) 의 가상 인터페이스 그룹 ID.

전초 기지의 CloudWatch 지표 보기

콘솔을 사용하여 로드 밸런서의 CloudWatch 지표를 볼 수 있습니다. CloudWatch

콘솔을 CloudWatch 사용하여 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표를 선택합니다.
3. Outposts 네임스페이스를 선택합니다.
4. (선택 사항)모든 차원의 지표를 보려면 검색 상자에 이름을 입력합니다.

AWS CLI을(를) 사용하여 지표를 보려면

사용 가능한 지표의 목록을 표시하려면 다음 list-metrics 명령을 사용합니다.

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

AWS CLI을(를) 사용하여 지표에 대한 통계를 구하려면

다음 get-metric-statistics명령을 사용하여 지정된 지표 및 차원에 대한 통계를 가져올 수 있습니다. CloudWatch 고유한 차원 조합을 각각 별도의 지표로 취급합니다. 특별 게시가 되지 않은 차원의 조합을 사용해 통계를 검색할 수는 없습니다. 지표 생성 시 사용한 것과 동일하게 차원을 지정해야 합니다.

```
aws cloudwatch get-metric-statistics --namespace AWS/Outposts \
--metric-name InstanceTypeCapacityUtilization --statistics Average  --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef \
Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

AWS CloudTrail을(를) 사용하여 AWS Outposts API 호출 로깅

AWS Outposts에서 사용자AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다AWS Outposts. CloudTrail 모든 API 호출을 AWS Outposts 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Outposts 콘솔로부터의 호출과 AWS Outposts API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 에 대한 이벤트를 포함하여 S3 버킷에 CloudTrail 이벤트를 지속적으로 전송할 수 AWS Outposts 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람AWS Outposts, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

에 대한 CloudTrail 자세한 내용은 AWS CloudTrail사용 설명서를 참조하십시오.

AWS Outposts자세한 내용은 CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. 에서 AWS Outposts 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

AWS Outposts에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. 트레일을 사용하면 CloudTrail 상위 항목의 S3 버킷에 로그 파일을 전송할 수 AWS 리전 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 AWS Outposts 작업은 에 의해 기록됩니다 CloudTrail. 이는 AWS Outposts API 참조에 문서로 작성됩니다. 예를 들어, `CreateOutpost`, `GetOutpostInstanceTypes`, 및 `ListSites` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 다음 중 어떤 자격 증명 정보를 사용하여 요청이 수행되었는지 여부를 확인할 수 있습니다:

- 루트 또는 사용자 자격 증명 사용.
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명 사용.
- 다른 AWS 서비스 사용.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

AWS Outposts 로그 파일 항목 이해

트레일은 지정한 S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스로부터 단일 요청을 나타냅니다. 여기에는 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보가 포함됩니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateOutpost` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Outpost 유지 관리

공동 책임 모델 하에서는 AWS AWS 서비스를 실행하는 하드웨어와 소프트웨어를 담당합니다. 이는 AWS 지역과 AWS Outposts마찬가지로 에도 적용됩니다. 예를 들어, 보안 패치를 AWS 관리하고, 펌웨어를 업데이트하고, Outpost 장비를 유지 관리합니다. AWS 또한 Outpost의 성능, 상태 및 지표를 모니터링하고 유지 관리가 필요한지 여부를 결정합니다.

> **Warning**
>
> 기본 디스크 드라이브에 장애가 발생하거나 인스턴스가 중지되거나 최대 절전 모드로 전환되거나 종료되면 인스턴스 스토어 볼륨의 데이터가 손실됩니다. 데이터 손실을 방지하려면 인스턴스 스토어 볼륨의 장기 데이터를 Amazon S3 버킷, Amazon EBS 볼륨 또는 온프레미스 네트워크의 네트워크 스토리지 장치와 같은 영구 스토리지에 백업하는 것이 좋습니다.

콘텐츠

- 하드웨어 유지 관리
- 펌웨어 업데이트
- 네트워크 장비 유지 관리
- AWS Outposts 전력 및 네트워크 이벤트 모범 사례
- 다음을 위해 Amazon EC2를 최적화합니다. AWS Outposts
- AWS Outposts 랙 네트워크 문제 해결 체크리스트

하드웨어 유지 관리

Outpost에서 실행 중인 Amazon EC2 인스턴스를 호스팅하는 하드웨어에서 복구할 수 없는 문제가 AWS 발견되면 Outpost 소유자와 인스턴스 소유자에게 영향을 받는 인스턴스가 사용 중지될 예정임을 알립니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 사용 중지를 참조하세요.

Outpost 소유자와 인스턴스 소유자가 협력하여 문제를 해결할 수 있습니다. 인스턴스 소유자는 영향을 받는 인스턴스를 중지했다가 시작하여 가용 용량으로 마이그레이션할 수 있습니다. 인스턴스 소유자는 자신에게 편리한 시간에 영향을 받는 인스턴스를 중지하고 시작할 수 있습니다. 그렇지 않으면 인스턴스 사용 AWS 중지일에 영향을 받는 인스턴스를 중지했다가 다시 시작합니다. Outpost에 추가 용량이 없는 경우 인스턴스는 중지된 상태로 유지됩니다. Outpost 소유자는 사용 용량을 늘리거나 마이그레이션을 완료할 수 있도록 Outpost에 추가 용량을 요청해 볼 수 있습니다.

하드웨어 유지 관리가 필요한 경우 AWS Outpost 사이트 관리자에게 연락하여 AWS 설치 팀이 방문할 날짜와 시간을 확인합니다. 사이트 관리자가 AWS 팀과 통화한 시점으로부터 영업일 기준 2일 이내에 방문 일정을 잡을 수 있습니다.

AWS 설치 팀이 현장에 도착하면 상태가 좋지 않은 호스트, 스위치 또는 랙 요소를 교체하고 새 용량을 온라인 상태로 전환합니다. 사이트에서는 하드웨어 진단이나 수리를 수행하지 않습니다. 호스트를 교체하면 NIST 규격을 준수하는 물리적 보안 키를 제거하고 파기하여 하드웨어에 남아 있을 수 있는 모든 데이터를 효과적으로 파쇄합니다. 이렇게 하면 데이터가 사이트를 떠나지 않도록 할 수 있습니다. Outpost 네트워킹 장치를 대체하는 경우, 사이트에서 장치를 제거하면 해당 장치에 네트워크 구성 정보가 표시될 수 있습니다. 이 정보에는 로컬 네트워크 또는 리전으로 돌아가는 경로를 구성하기 위한 가상 인터페이스를 설정하는 데 사용되는 IP 주소 및 ASN이 포함될 수 있습니다.

펌웨어 업데이트

Outpost 펌웨어 업데이트는 일반적으로 Outpost의 인스턴스에는 영향을 주지 않습니다. 업데이트를 설치하기 위해 Outpost 장비를 재부팅해야 하는 드문 경우에는 해당 용량으로 실행되는 모든 인스턴스에 대해 인스턴스 사용 중지 통지를 받게 됩니다.

네트워크 장비 유지 관리

Outpost 네트워킹 장치(OND)의 유지 관리는 정기적인 Outpost 운영 및 트래픽에 영향을 주지 않고 수행됩니다. 유지 보수가 필요한 경우 트래픽이 OND에서 멀어집니다. AS-Path 사전 지정과 같은 BGP 광고가 일시적으로 변경되고 Outpost 업링크의 트래픽 패턴이 이에 따라 변경되는 것을 확인할 수 있습니다. OND 펌웨어 업데이트를 사용하면 BGP가 펄럭이는 것을 볼 수 있습니다.

BGP 속성을 변경하지 않고 Outpost에서 BGP 광고를 수신하도록 고객 네트워크 장비를 구성하고 BGP 다중 경로 및 부하 분산을 활성화하여 최적의 인바운드 트래픽 흐름을 달성하는 것이 좋습니다. AS-Path 사전 지정은 유지 관리가 필요한 경우 트래픽을 OND에서 다른 곳으로 이동시키기 위해 로컬 게이트웨이 접두사에 사용됩니다. 고객 네트워크는 AS-Path 길이가 1인 Outpost에서 출발하는 경로를 AS-Path 길이가 4인 경로보다 선호해야 합니다.

고객 네트워크는 모든 OND에 동일한 속성을 가진 동일한 BGP 접두사를 알려야 합니다. Outpost 네트워크는 기본적으로 모든 업링크 간에 아웃바운드 트래픽의 부하를 분산합니다. 유지 관리가 필요한 경우 Outpost 측에서는 라우팅 정책을 사용하여 트래픽을 OND에서 다른 곳으로 이동합니다. 이러한 트래픽 이동에는 모든 OND의 고객 측에서 동일한 BGP 접두사가 필요합니다. 고객 네트워크에서 유지 관리가 필요한 경우 AS-Path 프리펜딩을 사용하여 특정 업링크에서 일시적으로 트래픽 배열을 이동하는 것이 좋습니다.

AWS Outposts 전력 및 네트워크 이벤트 모범 사례

AWS Outposts 고객 AWS 서비스 약관에 명시된 바와 같이 Outposts 장비가 위치한 시설은 Outposts 장비의 설치, 유지 관리 및 사용을 지원하기 위한 최소 전력 및 네트워크 요구 사항을 충족해야 합니다. Outposts 랙 전원 및 네트워크 연결이 중단되지 않는 경우에만 제대로 작동할 수 있습니다.

전력 이벤트

정전이 완전히 중단되면 AWS Outposts 리소스가 자동으로 서비스 상태로 돌아가지 않을 수 있는 위험이 내재되어 있습니다. 중복 전원 및 백업 전원 솔루션을 배포하는 것 외에도 다음과 같은 작업을 미리 수행하여 일부 최악의 시나리오의 영향을 완화하는 것이 좋습니다.

- DNS 기반 또는 랙 외부 로드 밸런싱 변경을 사용하여 통제된 방식으로 Outpost 장비 외부로 서비스와 애플리케이션을 이동하세요.
- 컨테이너, 인스턴스, 데이터베이스를 순서대로 증분 방식으로 중지하고 복원 시 역순으로 사용합니다.
- 서비스의 통제된 이동 또는 중지에 대한 계획을 테스트합니다.
- 중요한 데이터와 구성을 백업하고 Outpost 외부에 저장합니다.
- 전력 가동 중지 시간을 최소화합니다.
- 유지 관리 중에는 전원 공급 장치를 반복적으로 전환(껐다가 켰다가)하지 마십시오.
- 유지 관리 기간 내에 예상치 못한 상황에 대처할 수 있도록 여분의 시간을 할애합니다.
- 일반적으로 필요한 것보다 더 넓은 유지 관리 기간을 전달하여 사용자와 고객의 기대치를 관리합니다.

네트워크 연결 이벤트

Outpost와 AWS 지역 또는 Outposts 홈 지역 간의 서비스 링크 연결은 일반적으로 네트워크 유지 관리가 완료되면 업스트림 회사 네트워크 장치 또는 타사 연결 공급자의 네트워크에서 발생할 수 있는 네트워크 중단이나 문제로부터 자동으로 복구됩니다. 서비스 링크 연결이 끊기는 동안에는 Outpost 작업이 로컬 네트워크 활동으로 제한됩니다.

자세한 내용은 AWS Outposts 랙 FAQ 페이지에 있는 시설의 네트워크 연결이 끊어지면 어떻게 되나요? 질문을 참조하세요.

현장 전원 문제 또는 네트워크 연결 손실로 인해 서비스 링크가 중단된 경우 Outposts를 소유한 계정으로 알림을 AWS Health Dashboard 보냅니다. 서비스 링크 중단이 예상되더라도 사용자나 사용자 모두

서비스 링크 중단 알림을 표시하지 않을 AWS 수 없습니다. 자세한 내용은 AWS Health 사용 설명서의 AWS Health Dashboard시작하기를 참조하세요.

계획된 서비스 유지 관리가 네트워크 연결에 영향을 미칠 경우 다음과 같은 사전 조치를 취하여 잠재적인 문제 시나리오의 영향을 제한합니다.

- Outposts 랙을 인터넷 또는 공용 Direct Connect를 통해 상위 AWS 지역에 연결하는 경우 계획된 유지 관리 전에 추적 경로를 캡처하십시오. 작동 중인(네트워크 유지 관리 전) 네트워크 경로와 문제가 있는 (네트워크 유지 관리 후) 네트워크 경로를 통해 차이점을 식별하면 문제 해결에 도움이 됩니다. 유지 관리 후 문제를 AWS ISP나 ISP에 에스컬레이션하는 경우 이 정보를 포함할 수 있습니다.

  다음 사이의 추적 경로를 캡처합니다.

  - Outpost 위치의 공용 IP 주소 및 `outposts.region.amazonaws.com`에서 반환한 IP 주소 `### ## ###` 이름으로 바꾸십시오. AWS
  - Outpost 위치의 공용 인터넷 연결 및 공용 IP 주소를 사용하는 상위 리전의 모든 인스턴스
- 네트워크 유지 관리를 관리할 수 있는 경우 서비스 링크의 가동 중지 시간을 제한합니다. 네트워크가 복구되었는지 확인하는 단계를 유지 관리 프로세스에 포함시킵니다.
- 네트워크 유지 관리를 관리할 수 없는 경우, 공지된 유지 관리 기간과 관련하여 서비스 링크 다운타임을 모니터링하고 공지된 유지 관리 기간이 끝나도 서비스 링크가 백업되지 않으면 계획된 네트워크 유지 관리 담당자에게 조기에 에스컬레이션합니다.

리소스

다음은 계획된 또는 예상치 못한 전력 또는 네트워크 사고 이후 Outposts가 정상적으로 작동하고 있는지 확인할 수 있는 몇 가지 모니터링 관련 리소스입니다.

- AWS 블로그 모니터링 모범 사례에서는 Outposts와 관련된 옵저버빌리티 및 이벤트 관리 모범 사례를 AWS Outposts다룹니다.
- Amazon VPC의 네트워크 연결을 위한 디버깅 도구 AWS 블로그에서는 AWSSupportMonitoringFrom-SetupIP VPC 도구에 대해 설명합니다. 이 도구는 사용자가 지정한 서브넷에 Amazon EC2 Monitor 인스턴스를 생성하고 대상 IP 주소를 모니터링하는 AWS Systems Manager 문서(SSM 문서)입니다. 이 문서는 ping, MTR, TCP 추적 경로 및 추적 경로 진단 테스트를 실행하고 결과를 Amazon CloudWatch Logs에 저장합니다. 이 테스트는 CloudWatch 대시보드에서 시각화할 수 있습니다 (예: 지연 시간, 패킷 손실). Outposts 모니터링의 경우 Monitor 인스턴스는 상위 AWS 지역의 한 서브넷에 있어야 하며 해당 프라이빗 IP를 사용하여 하나 이상의 Outpost 인스턴스를 모니터링하도록 구성해야 합니다. 그러면 상위 지역 간의 AWS Outposts 패킷 손실 그래프와 지연 시간이 제공됩니다. AWS

- AWS Outposts 사용을 위한 자동 Amazon CloudWatch 대시보드 배포 AWS 블로그에서는 자동화된 대시보드 배포와 관련된 단계를 AWS CDK설명합니다.
- 질문이 있거나 자세한 정보가 필요한 경우, AWS 지원 사용 설명서의 지원 사례 생성를 참조하세요.

다음을 위해 Amazon EC2를 최적화합니다. AWS Outposts

이와 대조적으로 AWS 리전, 전초 기지의 Amazon Elastic Compute Cloud (Amazon EC2) 용량은 한정되어 있습니다. 주문한 컴퓨팅 용량의 총 볼륨에 제약을 받습니다. 이 항목에서는 AWS Outposts에서 Amazon EC2 용량을 최대한 활용하는 데 도움이 되는 모범 사례와 최적화 전략을 제공합니다.

내용

- Outpost의 전용 호스트
- 인스턴스 복구 설정
- Outpost의 배치 그룹

Outpost의 전용 호스트

Amazon EC2 전용 호스트는 고객 전용의 EC2 인스턴스 용량을 갖춘 물리적 서버입니다. Outpost는 이미 전용 하드웨어를 제공하고 있지만 전용 호스트를 사용하면 단일 호스트에 대한 소켓당, 코어당 또는 VM당 라이선스 제한이 있는 기존 소프트웨어 라이선스를 사용할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 전용 호스팅을 참조하십시오. AWS Outposts Windows의 경우 Amazon EC2 사용 설명서의 전용 호스팅 AWS Outposts켜기를 참조하십시오.

라이선스 외에도 Outpost 소유자는 전용 호스트를 사용하여 다음과 같은 두 가지 방법으로 Outpost 배포 시 서버를 최적화할 수 있습니다.

- 서버의 용량 레이아웃 변경
- 하드웨어 수준에서 인스턴스 배치를 제어합니다.

서버의 용량 레이아웃 변경

전용 호스팅은 Outpost 배포 시 별도의 연락 없이 서버 레이아웃을 변경할 수 있는 기능을 제공합니다. AWS Support Outpost의 용량을 구매할 때는 각 서버가 제공하는 EC2 용량 레이아웃을 지정해야 합니다. 각 서버는 단일 인스턴스 유형 패밀리를 지원합니다. 레이아웃은 단일 인스턴스 유형 또는 여러 인스턴스 유형을 제공할 수 있습니다. 전용 호스트를 사용하면 초기 레이아웃에 대해 선택한 모든 것을 변경할 수 있습니다. 전체 용량에 대해 단일 인스턴스 유형을 지원하도록 호스트를 할당하는 경우, 해

당 호스트에서 단일 인스턴스 유형만 시작할 수 있습니다. 다음 그림은 동종 레이아웃의 m5.24xlarge 서버를 나타냅니다.

여러 인스턴스 유형에 동일한 용량을 할당할 수 있습니다. 여러 인스턴스 유형을 지원하도록 호스트를 할당하면 명시적인 용량 레이아웃이 필요하지 않은 다차원의 레이아웃을 얻게 됩니다. 다음 그림은 총 용량에서 다차원의 레이아웃을 포함한 동종 레이아웃의 m5.24xlarge 서버를 나타냅니다.

자세한 내용은 Amazon EC2 사용 설명서의 전용 호스트 할당 또는 Amazon EC2 사용 설명서의 전용 호스트 할당을 참조하십시오.

하드웨어 수준에서 인스턴스 배치를 제어합니다.

전용 호스트를 사용하여 하드웨어 수준에서 인스턴스 배치를 제어할 수 있습니다. 전용 호스트에 대한 자동 배치를 사용하면 시작하는 인스턴스가 특정 호스트에서 시작되는지, 아니면 구성이 일치하는 사용 가능한 호스트에서 시작되는지 관리할 수 있습니다. 호스트 선호도를 사용하여 인스턴스와 전용 호스트 간에 관계를 설정합니다. Outpost 랙이 있는 경우 이러한 전용 호스트 기능을 사용하여 상호 관련된 하드웨어 오류의 영향을 최소화할 수 있습니다. 인스턴스 복구에 대한 자세한 내용은 Amazon EC2 사용 설명서의 자동 배치 및 선호도 이해 또는 Amazon EC2 사용 설명서의 자동 배치 및 선호도 이해를 참조하십시오.

를 사용하여 전용 호스트를 공유할 수 있습니다. AWS Resource Access Manager전용 호스트를 공유하면 AWS 계정전반에서 Outpost 배포 시 호스트를 분산할 수 있습니다. 자세한 정보는 공유 리소스로 작업하기을 참조하세요.

인스턴스 복구 설정

Outpost에서 하드웨어 장애로 인해 비정상 상태가 된 인스턴스는 정상 호스트로 마이그레이션해야 합니다. 인스턴스 상태 확인에 따라 이 마이그레이션이 자동으로 수행되도록 자동 복구를 설정할 수 있습니다. 자세한 내용은 Linux 인스턴스 복구 또는 Windows 인스턴스 복구를 참조하세요.

Outpost의 배치 그룹

AWS Outposts 배치 그룹을 지원합니다. 배치 그룹을 사용하여 Amazon EC2가 Outpost 하드웨어에 상호 종속적인 인스턴스 그룹을 배치하려고 시도하는 방식에 영향을 줄 수 있습니다. 다양한 전략 (클러스터, 파티션 또는 스프레드)을 사용하여 다양한 워크로드의 요구 사항을 충족할 수 있습니다. 단일 랙 Outpost를 사용하는 경우 분산 전략을 사용하여 랙 대신 호스트 전반에서 인스턴스를 배치할 수 있습니다.

분산형 배치 그룹

분산형 배치 그룹을 사용하여 개별 하드웨어에 단일 인스턴스를 배포할 수 있습니다. 분산형 배치 그룹에서 인스턴스를 시작하면 인스턴스가 동일한 장비를 공유할 때 장애가 동시에 발생할 수 있는 위험이 줄어듭니다. 배치 그룹은 랙 또는 호스트 간에 인스턴스를 분산시킬 수 있습니다. 호스트 수준 스프레드 배치 그룹은 에서만 사용할 수 있습니다 AWS Outposts.

랙 분산 레벨 배치 그룹

랙 분산 레벨 배치 그룹은 Outpost 배포에 있는 랙 수만큼의 인스턴스를 보유할 수 있습니다. 다음 그림은 랙 분산 레벨 배치 그룹에서 인스턴스 3개를 실행하는 3-랙 Outpost 배포를 보여줍니다.

호스트 분산 레벨 배치 그룹

호스트 분산 레벨 배치 그룹은 Outpost 배포에 있는 호스트의 개수만큼의 인스턴스를 보유할 수 있습니다. 다음 그림은 호스트 분산 레벨 배치 그룹에서 인스턴스 3개를 실행하는 단일 랙 Outpost 배포를 보여줍니다.

파티션 배치 그룹

파티션 배치 그룹을 사용하면 파티션이 있는 랙 전반에서 여러 인스턴스를 분산할 수 있습니다. 각 파티션은 여러 인스턴스를 보유할 수 있습니다. 자동 배포를 사용하여 파티션 전반에서 인스턴스를 분산하거나 인스턴스를 대상 파티션에 배포할 수 있습니다. 다음 그림은 자동 배포를 사용하는 파티션 배치 그룹을 보여줍니다.

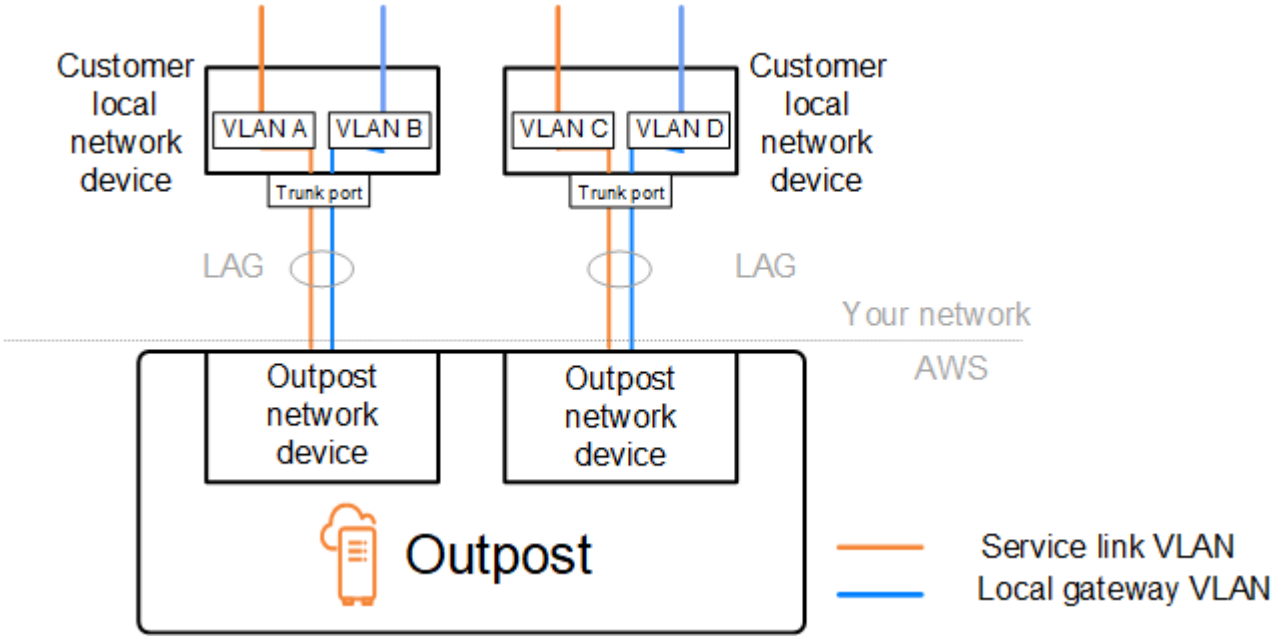
인스턴스를 대상 파티션에 배포할 수도 있습니다. 다음 그림은 대상 지정 배포를 사용하는 파티션 배치 그룹을 보여줍니다.

배치 그룹 작업에 대한 자세한 내용은 Amazon EC2 사용 설명서의배치 그룹 및 배치 그룹을 참조하십시오. AWS OutpostsWindows의 경우 Amazon EC2 사용 설명서의배치 그룹 및 배치 그룹을 참조하십시오. AWS Outposts

고가용성에 대한 자세한 내용은 AWS Outposts AWS Outposts 고가용성 설계 및 아키텍처 고려 사항을 참조하십시오.

AWS Outposts 랙 네트워크 문제 해결 체크리스트

이 체크리스트를 사용하면 상태가 DOWN인 서비스 링크의 문제를 해결하는 데 도움이 됩니다.



Outpost 네트워크 장치와의 연결

Outpost 네트워크 장치에 연결된 고객 로컬 네트워크 장치에서 BGP 피어링 상태를 확인합니다. BGP 피어링 상태가 DOWN인 경우 다음 단계를 따르세요.

1. 고객 장치에서 Outpost 네트워크 장치의 원격 피어 IP 주소를 핑합니다. 피어 IP 주소는 장치의 BGP 구성에서 찾을 수 있습니다. 설치 시 네트워크 준비 체크리스트에 제공된 정보를 참조할 수도 있습니다.
2. 핑에 실패한 경우 물리적 연결을 확인하고 연결 상태가 UP인지 확인합니다.
   a. 고객 로컬 네트워크 장치의 LACP 상태를 확인합니다.
   b. 장치의 인터페이스 상태를 확인합니다. UP 상태인 경우 3단계로 건너뜁니다.
   c. 고객 로컬 네트워크 장치를 확인하고 광 모듈이 작동하는지 확인합니다.
   d. 결함이 있는 광케이블을 교체하고 표시등(Tx/Rx)이 허용 범위 내에 있는지 확인하세요.
3. 핑이 성공하면 고객의 로컬 네트워크 장치를 확인하고 다음 BGP 구성이 올바른지 확인합니다.
   a. 로컬 자율 시스템 번호(고객 ASN)가 올바르게 구성되었는지 확인합니다.
   b. 원격 자율 시스템 번호(Outpost ASN)가 올바르게 구성되었는지 확인합니다.
   c. 인터페이스 IP와 원격 피어 IP 주소가 올바르게 구성되었는지 확인합니다.
   d. 광고된 경로와 수신된 경로가 올바른지 확인하세요.

4. BGP 세션이 활성 상태와 연결 상태 사이에서 펄럭이는 경우 고객 로컬 네트워크 장치에서 TCP 포트 179 및 기타 관련 임시 포트가 차단되지 않았는지 확인합니다.
5. 추가 문제 해결이 필요한 경우 고객 로컬 네트워크 장치에서 다음을 확인합니다.
   a. BGP 및 TCP 디버그 로그
   b. BGP 로그
   c. 패킷 캡처
6. 문제가 지속되면 Outpost에 연결된 라우터에서 Outpost 네트워크 장치 피어 IP 주소로 MTR / traceroute / packet 캡처를 수행하세요. 엔터프라이즈 AWS 지원 플랜을 사용하여 Support와 테스트 결과를 공유하십시오.

고객 로컬 네트워크 장치와 Outpost 네트워크 장치 간의 BGP 피어링 상태가 UP이지만 서비스 링크가 여전히 DOWN 상태인 경우 고객 로컬 네트워크 장치에서 다음 장치를 확인하여 추가 문제를 해결할 수 있습니다. 서비스 링크 연결이 프로비저닝된 방식에 따라 다음 체크리스트 중 하나를 사용합니다.

- 연결된 에지 라우터 AWS Direct Connect — 서비스 링크 연결에 사용 중인 공용 가상 인터페이스 자세한 정보는 AWS Direct Connect 지역에 대한 AWS 공용 가상 인터페이스 연결을 참조하세요.
- 연결된 에지 라우터 AWS Direct Connect — 서비스 링크 연결에 사용 중인 사설 가상 인터페이스 자세한 정보는 AWS Direct ConnectAWS 지역에 대한 프라이빗 가상 인터페이스 연결을 참조하세요.
- 인터넷 서비스 제공자(ISP)와 연결된 에지 라우터 – 서비스 링크 연결에 사용 중인 공용 가상 인터페이스. 자세한 정보는 AWS 리전에 대한 ISP 공용 인터넷 연결을 참조하세요.

AWS Direct Connect 지역에 대한 AWS 공용 가상 인터페이스 연결

다음 체크리스트를 사용하여 서비스 링크 연결에 공용 가상 인터페이스를 사용할 AWS Direct Connect 때 연결된 에지 라우터 문제를 해결하십시오.

1. Outpost 네트워크 장치에 직접 연결하는 장치가 BGP를 통해 서비스 링크 IP 주소 범위를 수신하고 있는지 확인합니다.
   a. 장치에서 BGP를 통해 수신되는 경로를 확인합니다.
   b. 서비스 링크 가상 라우팅 및 포워딩 인스턴스(VRF)의 라우팅 테이블을 확인하세요. IP 주소 범위를 사용하고 있다고 표시되어야 합니다.
2. 리전 연결을 보장하려면 라우팅 테이블에서 서비스 링크 VRF를 확인하세요. 여기에는 AWS 퍼블릭 IP 주소 범위 또는 기본 경로가 포함되어야 합니다.

3. 서비스 링크 VRF에서 AWS 퍼블릭 IP 주소 범위를 수신하지 못하는 경우 다음 항목을 확인하십시오.
   a. 에지 라우터 또는 에서 AWS Direct Connect 링크 상태를 확인합니다. AWS Management Console
   b. 물리적 링크가 UP인 경우, 엣지 라우터에서 BGP 피어링 상태를 확인하세요.
   c. BGP 피어링 DOWN 상태인 경우 피어 AWS IP 주소를 ping하고 에지 라우터에서 BGP 컨피그레이션을 확인합니다. 자세한 내용은 AWS Direct Connect 사용 설명서의 문제 해결 및 AWS Direct Connect콘솔에서 내 가상 인터페이스 BGP 상태가 다운되었음을 참조하십시오. AWS 어떻게 해야 할까요?
   d. BGP가 설정되었는데 VRF에 기본 경로 또는 AWS 퍼블릭 IP 주소 범위가 표시되지 않는 경우 엔터프라이즈 AWS 지원 플랜을 사용하여 Support에 문의하십시오.
4. 온프레미스 방화벽을 사용하는 경우 다음 항목을 확인하세요.
   a. 서비스 링크 연결에 필요한 포트가 네트워크 방화벽에 허용되는지 확인하세요. 포트 443의 traceroute 또는 기타 네트워크 문제 해결 도구를 사용하여 방화벽과 네트워크 장치를 통한 연결을 확인합니다. 서비스 링크 연결을 위해 방화벽 정책에서 다음 포트를 구성해야 합니다.
      - TCP 프로토콜 - 소스 포트: TCP 1025-65535, 대상 포트: 443.
      - UDP 프로토콜 - 소스 포트: TCP 1025-65535, 대상 포트: 443.
   b. 방화벽이 스테이트풀 상태인 경우 아웃바운드 규칙이 Outpost의 서비스 링크 IP 주소 범위를 퍼블릭 IP 주소 범위로 허용하는지 확인하십시오. AWS 자세한 정보는 AWS OutpostsAWS 지역과의 연결성을 참조하세요.
   c. 방화벽이 스테이트풀 방식이 아닌 경우 AWS 퍼블릭 IP 주소 범위에서 서비스 링크 IP 주소 범위까지의 인바운드 흐름도 허용해야 합니다.
   d. 방화벽에 가상 라우터를 구성한 경우 Outpost와 AWS 리전 간의 트래픽에 대해 적절한 라우팅이 구성되어 있는지 확인하세요.
5. Outpost의 서비스 링크 IP 주소 범위를 자체 공용 IP 주소로 변환하도록 온프레미스 네트워크에서 NAT를 구성한 경우 다음 항목을 확인하세요.
   a. NAT 장치에 과부하가 걸리지 않았는지, 새 세션에 할당할 수 있는 빈 포트가 있는지 확인합니다.
   b. NAT 장치가 주소 변환을 수행하도록 올바르게 구성되었는지 확인합니다.
6. 문제가 지속되면 에지 라우터에서 피어 IP 주소로 MTR/traceroute/패킷 캡처를 수행하십시오. AWS Direct Connect 엔터프라이즈 AWS 지원 플랜을 사용하여 Support와 테스트 결과를 공유하십시오.

AWS Direct ConnectAWS 지역에 대한 프라이빗 가상 인터페이스 연결

다음 체크리스트를 사용하여 서비스 링크 연결에 프라이빗 가상 인터페이스를 사용할 AWS Direct Connect 때 연결된 에지 라우터 문제를 해결하십시오.

1. Outpost 랙과 AWS 지역 간 연결에서 AWS Outposts 개인 연결 기능을 사용하는 경우 다음 항목을 확인하십시오.
   a. 에지 라우터에서 원격 피어링 AWS IP 주소를 ping하고 BGP 피어링 상태를 확인합니다.
   b. 서비스 링크 엔드포인트 VPC와 온프레미스에 설치된 Outpost 간의 AWS Direct Connect 프라이빗 가상 인터페이스를 통한 BGP 피어링이 가능한지 확인하십시오. UP 자세한 내용은 AWS Direct Connect 사용 설명서의 문제 해결을 참조하십시오. AWS Direct Connect콘솔에서 내 가상 인터페이스 BGP 상태가 다운되었습니다. AWS 어떻게 해야 할까요?, 그리고 Direct Connect를 통한 BGP 연결 문제를 해결하려면 어떻게 해야 할까요?를 참조하세요.
   c. AWS Direct Connect 프라이빗 가상 인터페이스는 선택한 AWS Direct Connect 위치의 에지 라우터에 대한 프라이빗 연결이며 BGP를 사용하여 경로를 교환합니다. Virtual Private Cloud(VPC) CIDR 범위는 이 BGP 세션을 통해 에지 라우터에 알려집니다. 마찬가지로 Outpost 서비스 링크의 IP 주소 범위도 엣지 라우터의 BGP를 통해 해당 리전에 알려집니다.
   d. VPC의 서비스 링크 프라이빗 엔드포인트와 연결된 네트워크 ACL이 관련 트래픽을 허용하는지 확인합니다. 자세한 내용은 네트워크 준비 체크리스트 단원을 참조하세요.
   e. 온프레미스 방화벽을 사용하는 경우, 방화벽에 서비스 링크 IP 주소 범위와 VPC 또는 VPC CIDR에 있는 Outpost 서비스 엔드포인트 (네트워크 인터페이스 IP 주소)를 허용하는 아웃바운드 규칙이 있는지 확인하세요. TCP 1025-65535 및 UDP 443 포트가 차단되지 않았는지 확인합니다. 자세한 내용은 AWS Outposts 프라이빗 연결 소개를 참조하십시오.
   f. 방화벽이 상태 저장 상태가 아닌 경우, 방화벽에 VPC의 Outpost 서비스 엔드포인트에서 Outpost로 들어오는 인바운드 트래픽을 허용하는 규칙과 정책이 있는지 확인하세요.
2. 온-프레미스 네트워크에 100개가 넘는 네트워크가 있는 경우 BGP 세션을 통한 기본 경로를 개인 가상 AWS 인터페이스에 알릴 수 있습니다. 기본 경로를 알리고 싶지 않은 경우 알려지는 경로 수가 100개 미만이 되도록 경로를 요약합니다.
3. 문제가 지속되면 에지 라우터에서 피어 IP 주소로 MTR/traceroute/패킷 캡처를 수행하십시오. AWS Direct Connect 엔터프라이즈 AWS 지원 플랜을 사용하여 Support와 테스트 결과를 공유하십시오.

AWS 리전에 대한 ISP 공용 인터넷 연결

서비스 링크 연결에 공용 인터넷을 사용할 때 다음 체크리스트를 사용하여 ISP를 통해 연결된 엣지 라우터 문제를 해결하세요.

- 인터넷 링크가 작동 중인지 확인합니다.
- ISP를 통해 연결된 엣지 장치에서 공용 서버에 액세스할 수 있는지 확인합니다.

ISP 링크를 통해 인터넷 또는 공용 서버에 액세스할 수 없는 경우 다음 단계를 완료하세요.

1. ISP 라우터와의 BGP 피어링 상태가 설정되었는지 확인하세요.
   a. BGP가 플래핑되지 않는지 확인하세요.
   b. BGP가 ISP로부터 필요한 경로를 수신하고 광고하고 있는지 확인합니다.
2. 고정 경로 구성의 경우 엣지 장치에 기본 경로가 제대로 구성되어 있는지 확인합니다.
3. 다른 ISP 연결을 사용하여 인터넷에 연결할 수 있는지 확인하세요.
4. 문제가 지속되면 엣지 라우터에서 MTR / traceroute / packet 캡처를 수행하세요. 추가 문제 해결을 위해 ISP 기술 지원 팀과 결과를 공유합니다.

ISP 링크를 통해 인터넷 및 공용 서버에 액세스할 수 있는 경우 다음 단계를 완료합니다.

1. Outpost 홈 리전에서 공개적으로 액세스할 수 있는 EC2 인스턴스 또는 로드 밸런서가 엣지 장치에서 액세스할 수 있는지 확인합니다. 핑 또는 텔넷을 사용하여 연결을 확인한 다음 traceroute를 사용하여 네트워크 경로를 확인할 수 있습니다.
2. VRF를 사용하여 네트워크에서 트래픽을 분리하는 경우 서비스 링크 VRF에 트래픽을 ISP(인터넷) 및 VRF로 보내고 받는 경로 또는 정책이 있는지 확인하세요. 다음 체크포인트를 참조하세요.
   a. ISP에 연결된 에지 라우터. 엣지 라우터의 ISP VRF 라우팅 테이블을 확인하여 서비스 링크 IP 주소 범위가 존재하는지 확인합니다.
   b. Outpost에 연결하는 고객 로컬 네트워크 장치. VRF의 구성을 확인하고 서비스 링크 VRF와 ISP VRF 간의 연결에 필요한 라우팅 및 정책이 제대로 구성되었는지 확인합니다. 일반적으로 인터넷 트래픽의 경우 ISP VRF에서 서비스 링크 VRF로 기본 경로가 전송됩니다.
   c. Outpost에 연결된 라우터에서 소스 기반 라우팅을 구성한 경우 구성이 올바른지 확인하세요.
3. 온프레미스 방화벽이 Outpost 서비스 링크 IP 주소 범위에서 퍼블릭 IP 주소 범위로의 아웃바운드 연결 (TCP 1025-65535 및 UDP 443 포트) 을 허용하도록 구성되어 있는지 확인하십시오. AWS 방화벽이 상태 저장 방식이 아닌 경우 Outpost에 대한 인바운드 연결도 구성되었는지 확인하세요.
4. Outpost의 서비스 링크 IP 주소 범위를 공용 IP 주소로 변환하도록 온프레미스 네트워크에 NAT가 구성되어 있는지 확인하세요. 또한 다음 항목을 확인하세요.
   a. NAT 장치에 과부하가 걸리지 않았고 새 세션에 할당할 수 있는 빈 포트가 있습니다.
   b. NAT 장치가 주소 변환을 수행하도록 올바르게 구성되었습니다.

문제가 지속되면 MTR / traceroute / packet 캡처를 수행하세요.

- 결과 온프레미스 네트워크에서 패킷이 삭제되거나 차단된 것으로 나타나면 네트워크 또는 기술팀에 문의하여 추가 지침을 확인하세요.
- 결과가 ISP 네트워크에서 패킷이 삭제되거나 차단된 것으로 나타나면 ISP 기술 지원 팀에 문의하십시오.
- 결과에 문제가 없는 경우 모든 테스트 결과 (예: MTR, 텔넷, 추적 경로, 패킷 캡처, BGP 로그) 를 수집하고 Enterprise AWS Support 플랜을 사용하여 Support에 문의하십시오.

Outposts는 두 개의 방화벽 장치 뒤에 있습니다.

Outpost를 고가용성 동기화 방화벽 쌍이나 독립형 방화벽 두 개 뒤에 설치한 경우 서비스 링크의 비대칭 라우팅이 발생할 수 있습니다. 즉, 인바운드 트래픽은 방화벽-1을 통과하고 아웃바운드 트래픽은 방화벽-2를 통과할 수 있습니다. 다음 체크리스트를 사용하여 서비스 링크의 잠재적인 비대칭 라우팅을 식별하십시오. 특히 이전에 제대로 작동하고 있었다면 더욱 그렇습니다.

- 회사 네트워크 라우팅 설정에 최근 변경 사항이나 지속적인 유지 관리로 인해 방화벽을 통한 서비스 링크의 비대칭 라우팅이 발생했을 수 있는 부분이 있는지 확인하십시오.
  - 방화벽 트래픽 그래프를 사용하여 서비스 연결 문제의 시작과 일치하는 트래픽 패턴의 변경 사항을 확인하세요.
  - 방화벽 간의 연결 테이블을 더 이상 동기화하지 못하게 하는 원인이 될 수 있는 부분적인 방화벽 장애 또는 분리형 방화벽 쌍 시나리오가 있는지 확인하세요.
  - 회사 네트워크에서 링크가 다운되었거나 최근 라우팅 변경 사항 (OSPF/ISIS/EIGRP 지표 변경, BGP 경로 맵 변경) 이 서비스 링크 문제의 시작과 일치하는지 확인하십시오.
- 홈 지역으로의 서비스 링크에 공용 인터넷 연결을 사용하는 경우 서비스 제공업체 유지 관리로 인해 방화벽을 통한 서비스 링크가 비대칭적으로 라우팅될 수 있습니다.
  - ISP로 연결되는 링크의 트래픽 그래프에서 서비스 연결 문제의 시작과 일치하는 트래픽 패턴의 변경 사항을 확인하십시오.
- 서비스 링크에 AWS Direct Connect 연결을 사용하는 경우 AWS 계획된 유지 관리로 인해 서비스 링크의 비대칭 라우팅이 트리거되었을 수 있습니다.
  - AWS Direct Connect 서비스에 예정된 유지 관리 알림이 있는지 확인하세요.
  - 중복 AWS Direct Connect 서비스가 있는 경우 유지 관리 조건에서 가능한 각 네트워크 경로를 통해 Outposts 서비스 링크의 라우팅을 사전에 테스트할 수 있습니다. 이를 통해 서비스 중 하나가 중단되면 AWS Direct Connect 서비스 링크가 비대칭적으로 라우팅될 수 있는지 테스트할 수 있습니다. end-to-end 네트워크 연결 AWS Direct Connect 부분의 복원력은 Resiliency with AWS

Direct Connect Resiliency Toolkit에서 테스트할 수 있습니다. 자세한 내용은 복원력 도구 키트를 사용한 AWS Direct Connect 복원력 테스트 — 장애 조치 테스트를 참조하십시오.

위의 체크리스트를 살펴보고 서비스 링크의 비대칭 라우팅을 가능한 근본 원인으로 지목한 후 다음과 같은 추가 조치를 취할 수 있습니다.

- 회사 네트워크 변경 사항을 되돌리거나 제공업체가 계획한 유지 관리가 완료될 때까지 기다려 대칭 라우팅을 복원하십시오.
- 방화벽 중 하나 또는 둘 다에 로그인하고 명령줄에서 모든 흐름에 대한 모든 흐름 상태 정보를 지우십시오 (방화벽 공급업체에서 지원하는 경우).
- 다른 방화벽을 통해 대칭 라우팅을 강제하려면 방화벽 중 하나를 통해 BGP 알림을 일시적으로 필터링하거나 한 방화벽의 인터페이스를 종료하십시오.
- 각 방화벽을 차례로 재부팅하여 방화벽 메모리의 서비스 링크 트래픽의 흐름 상태 추적에서 잠재적인 손상을 방지하십시오.
- 방화벽 벤더에 문의하여 포트 443에서 공급되고 포트 443으로 향하는 UDP 연결의 UDP 흐름 상태 추적을 확인하거나 완화하십시오.

AWS Outposts end-of-term 옵션

AWS Outposts 학기가 끝나면 다음과 같은 세 가지 옵션이 있습니다.

- 구독을 갱신하고 기존 Outpost를 유지하세요.
- 구독을 종료하고 Outpost 랙을 반환할 수 있도록 준비하세요.
- month-to-month 구독으로 전환하고 기존 Outpost를 유지하세요.

주제

- 구독 갱신
- 구독을 종료하고 랙을 반환할 수 있도록 준비하세요.
- 구독으로 전환하세요. month-to-month

구독 갱신

구독을 갱신하고 기존 Outpost를 유지하려면 다음과 같이 하세요.

Outpost 기간이 끝나기 최소 30일 전에 다음 단계를 완료하세요.

1. AWS Support 센터 콘솔로 로그인합니다.
2. 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 서비스에서 결제를 선택합니다.
5. 카테고리에서 기타 결제 질문을 선택합니다.
6. 심각도에서 중요 질문을 선택합니다.
7. 다음 단계: 추가 정보를 선택합니다
8. 추가 정보 페이지의 제목에 **`Renew my Outpost subscription`**다음과 같이 갱신 요청을 입력합니다.
9. 설명에 다음 결제 옵션 중 하나를 입력합니다.
    - 선수금 없음
    - 부분 선결제
    - 전체 선결제

요금에 대한 내용은 AWS Outposts 랙 요금을 참조하세요. 가격 견적을 요청할 수도 있습니다.

10. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.
11. 문의처 페이지에서 선호하는 언어를 선택합니다.
12. 선호하는 연락 방법을 선택합니다.
13. 사례 세부 정보를 검토한 다음 제출을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.

AWS 고객 지원 부서에서 구독 갱신 프로세스를 시작합니다. 새 구독은 현재 구독이 종료된 다음 날에 시작됩니다.

구독을 갱신하거나 Outpost 랙을 반품하겠다는 의사를 표시하지 않으면 자동으로 구독으로 전환됩니다. month-to-month Outpost는 구성에 해당하는 선결제 없음 결제 옵션의 요율로 월 단위로 갱신됩니다. AWS Outposts 새 월별 구독은 현재 구독이 종료된 다음 날에 시작됩니다.

구독을 종료하고 랙을 반환할 수 있도록 준비하세요.

> **Important**
>
> AWS 다음 절차를 완료하기 전에는 반품 프로세스를 시작할 수 없습니다. 구독을 종료하기 위해 지원 케이스를 연 후에는 반환 프로세스를 중단할 수 없습니다.

구독을 종료하려면 다음과 같이 하세요.

Outpost 기간이 끝나기 최소 30일 전에 다음 단계를 완료하세요.

1. AWS Support 센터 콘솔로 로그인합니다.
2. 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 서비스에서 결제를 선택합니다.
5. 카테고리에서 기타 결제 질문을 선택합니다.
6. 심각도에서 중요 질문을 선택합니다.
7. 다음 단계: 추가 정보를 선택합니다
8. 추가 정보 페이지에서, 제목에 **`End my Outpost subscription`**와(과) 같이 명백한 요청을 입력합니다.

9. 설명에 Outpost를 가져오길 원하는 날짜를 입력합니다.
10. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.
11. 문의처 페이지에서 선호하는 언어를 선택합니다.
12. 선호하는 연락 방법을 선택합니다.
13. 사례 세부 정보를 검토한 다음 제출을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.

AWS 고객 지원 부서에서 연락하여 검색을 조율할 것입니다.

AWS Outposts 랙 반품을 준비하려면:

> **Important**
> 예정된 회수를 위해 현장에 도착하기 AWS 전까지는 Outpost 랙의 전원을 끄지 마십시오.

1. Outpost의 리소스를 공유하는 경우 해당 리소스의 공유를 해제해야 합니다.

   다음 방법 중 하나로 공유 Outpost 리소스의 공유를 취소할 수 있습니다.

   - 콘솔을 사용하세요. AWS RAM 자세한 내용은 AWS RAM 사용 설명서에서 리소스 공유 업데이트를 참조하세요.
   - 를 AWS CLI 사용하여 연결 해제-리소스-공유 명령을 실행합니다.

   공유할 수 있는 Outpost 리소스 목록은 공유 가능한 Outpost 리소스를 참조하세요.
2. Outpost의 서브넷과 연결된 활성 인스턴스를 종료하세요. 인스턴스를 종료하려면 Amazon EC2 사용 설명서의 인스턴스 종료에 있는 지침을 따르십시오.

   > **Note**
   > 애플리케이션 로드 밸런서 또는 Amazon RDatabase Service (RDS) 와 같이 Outpost에서 실행되는 일부 AWS관리형 서비스는 EC2 용량을 소비합니다. 하지만 Amazon EC2 대시보드에는 관련 인스턴스가 표시되지 않습니다. 용량을 확보하려면 이러한 서비스에 연결된 리소스를 종료해야 합니다. 자세한 내용은 Outpost에서 일부 EC2 인스턴스 용량이 누락된 이유를 참조하십시오. .
3. 계정에 있는 instance-capacity-availability Amazon EC2 인스턴스가 있는지 확인하십시오. AWS

a. https://console.aws.amazon.com/outposts/ 에서 AWS Outposts 콘솔을 엽니다.

b. Outposts를 선택합니다.

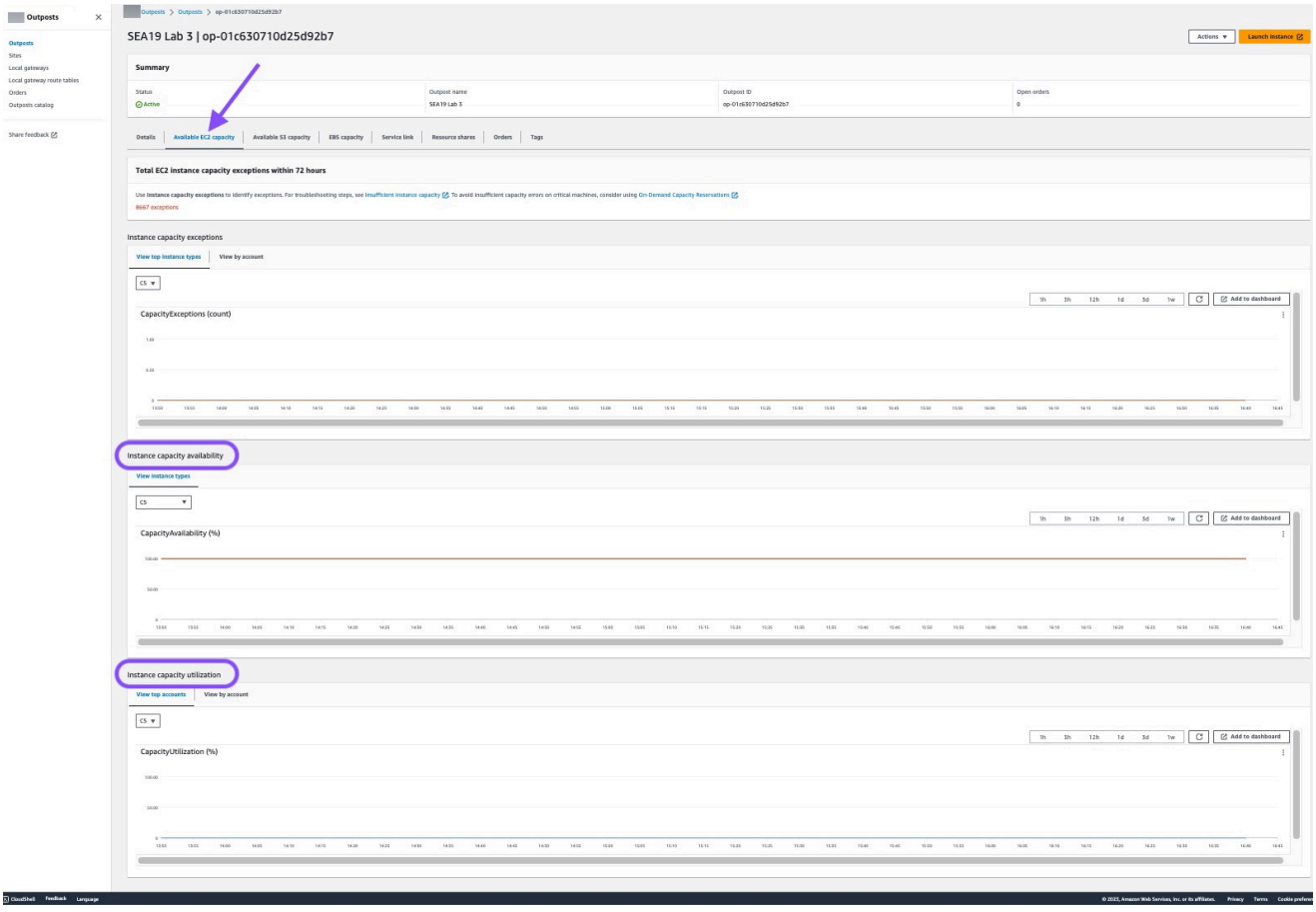
c. 반환할 특정 Outpost를 선택하세요.

d. Outpost 페이지에서 사용 가능한 EC2 용량 탭을 선택합니다.

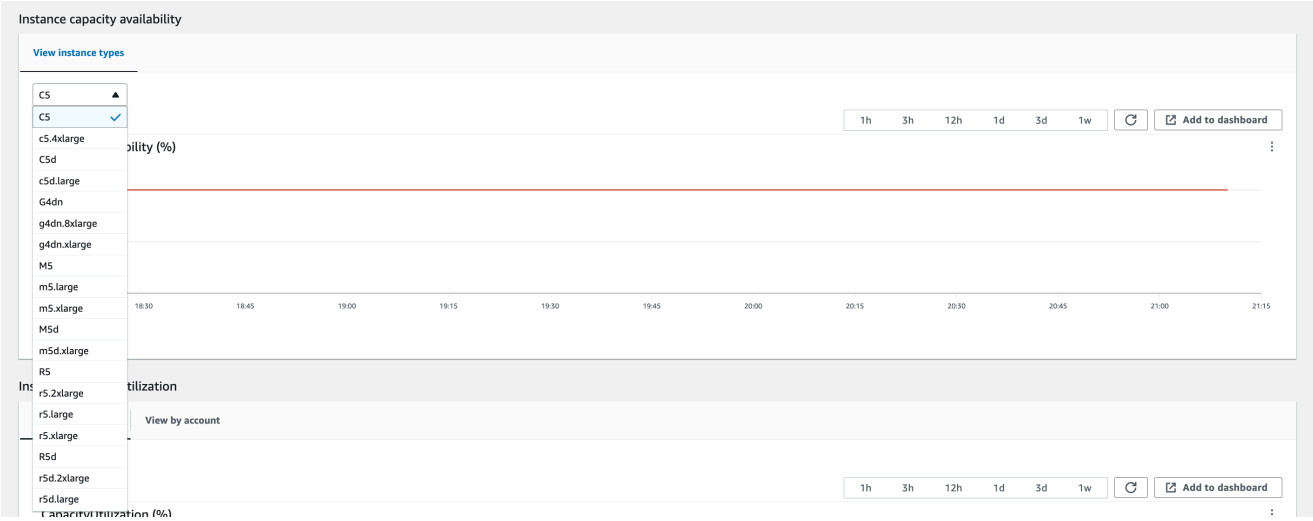
e. 각 인스턴스 패밀리의 인스턴스 용량 가용성이 100%인지 확인하세요.

f. 각 인스턴스 패밀리의 인스턴스 용량 사용률이 0%인지 확인하세요.

다음 이미지는 가용 EC2 용량 탭의 인스턴스 용량 가용성 및 인스턴스 용량 사용률 그래프를 보여줍니다.



다음 이미지는 인스턴스 유형의 목록을 보여줍니다.



4. Amazon EC2 인스턴스 및 서버 볼륨의 백업을 생성합니다. 백업을 생성하려면 AWS 권장 지침 가이드에서 EBS 볼륨으로 Amazon EC2를 백업 및 복구의 지침을 따르세요.
5. Outpost와 연결된 Amazon EBS 볼륨을 삭제하세요.
   a. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
   b. 탐색 창에서 볼륨을 선택합니다.
   c. 작업을 선택한 후 볼륨 삭제을 선택합니다.
   d. 확인 대화 상자에서 Delete(삭제)를 선택합니다.
6. Outpost에 Amazon S3가 있는 경우, Outpost에 있는 로컬 스냅샷을 모두 삭제하세요.
   a. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
   b. 탐색 창에서 스냅샷을 선택합니다.
   c. Outpost ARN을 사용하여 스냅샷을 선택합니다.
   d. 작업 및 스냅샷 삭제를 선택합니다.
   e. 확인 대화 상자에서 Delete(삭제)를 선택합니다.
7. Outpost와 연결된 모든 Amazon S3 버킷을 삭제하세요. 버킷을 삭제하려면 Amazon 심플 스토리지 서비스 사용 설명서의 Outpost 버킷에서 Amazon S3 삭제의 지침을 따르세요.
8. Outpost에 연결된 VPC 연결 및 고객 소유 IP 주소 풀 (COIP) CIDR을 삭제하세요.

AWS 검색 팀이 랙의 전원을 끌 것입니다. 전원이 꺼진 후 AWS Nitro 보안 키를 파기하거나 AWS 검색 팀이 대신 파기할 수 있습니다.

구독으로 전환하세요. month-to-month

month-to-month 구독으로 전환하고 기존 Outpost를 유지하려면 별도의 조치가 필요하지 않습니다. 궁금한 점은 청구 지원 사례를 여세요.

Outpost는 구성에 해당하는 선결제 없음 결제 옵션의 요율로 월 단위로 갱신됩니다. AWS Outposts 새 월별 구독은 현재 구독이 종료된 다음 날에 시작됩니다.

AWS Outposts에 대한 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 모든 할당량에 대한 증가를 요청할 수 없습니다.

AWS Outposts에 대한 할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스을(를) 선택한 다음 AWS Outposts을(를) 선택합니다.

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

AWS 계정에는 AWS Outposts와 관련하여 다음과 같은 할당량이 있습니다.

리소스	기본값	조정 가능	설명
Outpost 사이트	100	예	Outpost 사이트는 Outpost 장비에 전원을 공급하고 네트워크에 연결하는 고객이 관리하는 물리적 건물입니다. AWS 계정의 각 리전에는 100개의 Outpost 사이트를 만들 수 있습니다.
사이트당 Outpost	10	예	AWS Outposts은(는) Outpost라고 하는 하드웨어 및 가상 리소스를 포함합니다. 이 할당량은 Outpost 가상 리소스를 제한합니다. 각 Outpost 내에 10개의 Outpost를 생성할 수 있습니다.

AWS Outposts 그리고 다른 서비스에 대한 할당량

AWS Outposts은(는) 다른 서비스의 리소스에 의존하며 해당 서비스에는 자체 기본 할당량이 있을 수 있습니다. 예를 들어, 로컬 네트워크 인터페이스의 할당량은 네트워크 인터페이스의 Amazon VPC 할당량에서 나옵니다.

문서 기록

아래 표에 AWS Outposts 사용 설명서의 주요 변경 사항이 설명되어 있습니다.

변경 사항	설명	날짜
용량 관리	새 Outposts 주문에 대한 기본 용량 구성을 수정할 수 있습니다.	2024년 4월 16일
AWS Outposts 랙은 서비스 링크 인터페이스 처리량 메트릭을 지원합니다.	이제 및 메트릭을 활용하여 `IfTrafficIn` Outpost 랙 서비스 링크 가상 인터페이스(VIF) 와 로컬 네트워크 장치 간의 처리량 사용량을 모니터링할 수 있습니다. `IfTrafficOut` Amazon CloudWatch	2023년 11월 17일
로컬 게이트웨이를 통한 VPC 내 통신 AWS Outposts	로컬 게이트웨이를 사용하여 여러 Outpost 전반의 동일한 VPC에 있는 서브넷 간 통신을 설정할 수 있습니다.	2023년 8월 30일
랙용 AWS Outposts E nd-of-term 옵션	AWS Outposts 기간이 끝나면 구독을 갱신, 종료 또는 전환할 수 있습니다.	2023년 8월 1일
Outposts의 Amazon Route 53은 랙에서 사용할 수 있습니다. AWS Outposts	Outposts의 Amazon Route 53에는 AWS Outposts에서 발생하는 모든 DNS 쿼리를 캐싱하는 해석기가 포함되어 있습니다. 또한 인바운드 및 아웃바운드 엔드포인트를 배포할 때 Outpost와 온프레미스 DNS 해석기 간에 하이브리드 연결을 설정할 수 있습니다.	2023년 7월 20일

로컬 게이트웨이 인바운드 경로	Outpost에서 탄력적 네트워크 인터페이스에 대한 로컬 게이트웨이 인바운드 경로를 생성하고 수정할 수 있습니다.	2022년 9월 15일
에 대한 직접 VPC 라우팅 소개 AWS Outposts	VPC에 있는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와의 통신을 용이하게 합니다.	2022년 9월 14일
AWS Outposts Outposts 랙용 사용 설명서 작성	AWS Outposts 사용 설명서는 랙과 서버에 대한 별도의 안내서로 구성되었습니다.	2022년 9월 14일
로컬 게이트웨이 라우팅 테이블 생성 및 관리	로컬 게이트웨이 라우팅 테이블 및 CoIP 풀을 생성하고 수정합니다. VIF 그룹 연결을 관리합니다.	2022년 9월 14일
배치 그룹은 다음과 같습니다. AWS Outposts	분산 전략을 사용하는 배치 그룹은 호스트 전반에서 인스턴스를 분산할 수 있습니다.	2022년 6월 30일
전용 호스트 켜짐 AWS Outposts	이제 Outposts의 전용 호스트를 사용할 수 있습니다.	2022년 5월 31일
공유 Outpost 사이트	Outpost 사이트를 만들고 관리하고 조직의 다른 AWS 계정과 공유하세요.	2021년 10월 18일
새로운 차원 CloudWatch	AWS Outposts 네임스페이스의 메트릭에 대한 새 CloudWatch 차원.	2021년 10월 13일
S3 버킷 공유	Outpost에서 S3 버킷을 공유하고 관리합니다.	2021년 8월 5일

일부 배치 그룹 지원	리전에서와 마찬가지로, 클러스터, 파티션 또는 스프레드 배치 전략을 사용할 수 있습니다.	2021년 7월 28일
추가 지표 CloudWatch	예약 인스턴스에는 추가 CloudWatch 측정치를 사용할 수 있습니다.	2021년 5월 24일
네트워크 문제 해결 체크리스트	네트워크 문제 해결 체크리스트를 사용할 수 있습니다.	2021년 2월 22일
추가 CloudWatch 지표	EBS 볼륨에 대한 추가 CloudWatch 지표를 사용할 수 있습니다.	2021년 2월 2일
콘솔 주문 업데이트	콘솔 주문 프로세스가 업데이트되었습니다.	2021년 1월 14일
프라이빗 연결	AWS Outposts 콘솔에서 Outpost를 생성할 때 Outpost의 프라이빗 연결을 구성할 수 있습니다.	2020년 12월 21일
네트워크 준비 체크리스트	Outpost 구성을 위한 정보를 수집할 때는 네트워크 준비 체크리스트를 사용합니다.	2020년 10월 28일
공유 리소스 AWS Outposts	Outpost 공유를 통해 Outpost 소유자는 로컬 게이트웨이 라우팅 테이블을 포함한 Outposts 및 Outpost 리소스를 동일한 조직의 다른 AWS 계정과 공유할 수 있습니다. AWS	2020년 10월 15일
CloudWatch 추가 지표	인스턴스 유형 수에 대한 추가 CloudWatch 측정치를 사용할 수 있습니다.	2020년 9월 21일

추가 지표 CloudWatch	서비스 링크 연결 상태에 대한 추가 CloudWatch 지표를 사용할 수 있습니다.	2020년 9월 11일
고객 소유 IPv4 주소 공유 지원	고객 소유 IPv4 주소를 공유하는 AWS Resource Access Manager 데 사용합니다.	2020년 4월 20일
CloudWatch 추가 지표	EBS 볼륨에 대한 추가 CloudWatch 지표를 사용할 수 있습니다.	2020년 4월 4일
최초 릴리스	의 초기 릴리스입니다. AWS Outposts	2019년 12월 3일

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