



를 사용하여 하이브리드 클라우드 아키텍처를 구축하는 모범 사례 AWS 서비스

AWS 권장 가이드



AWS 권장 가이드: 를 사용하여 하이브리드 클라우드 아키텍처를 구축하는 모범 사례 AWS 서비스

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

소개	1
개요	3
하이브리드 클라우드 워크숍	3
PoCs	3
원칙	4
사전 조건 및 제한 사항	5
사전 조건	5
AWS Outposts	5
AWS 로컬 영역	5
제한 사항	6
AWS Outposts	6
AWS 로컬 영역	6
하이브리드 클라우드 채택 프로세스	7
엣지에서의 네트워킹	7
VPC 아키텍처	7
엣지-리전 트래픽	8
엣지-온프레미스 트래픽	10
엣지의 보안	13
데이터 보호	14
ID 및 액세스 관리	18
인프라 보안	19
인터넷 액세스	20
인프라 거버넌스	22
엣지의 복원력	23
인프라 고려 사항	24
네트워킹 고려 사항	26
Outpost 및 로컬 영역에 인스턴스 배포	29
의 Amazon RDS 다중 AZ AWS Outposts	30
장애 조치 메커니즘	31
엣지에서의 용량 계획	35
Outposts의 용량 계획	35
로컬 영역에 대한 용량 계획	36
엣지 인프라 관리	36
엣지에서 서비스 배포	37

Outposts별 CLI 및 SDK	38
리소스	41
AWS 참조	41
AWS 블로그 게시물	41
기여자	42
작성	42
검토	42
기술 작성	42
문서 기록	43
.....	xliv

를 사용하여 하이브리드 클라우드 아키텍처를 구축하는 모범 사례 AWS 서비스

Amazon Web Services([기여자](#))

2025년 6월([문서 기록](#))

많은 기업과 조직이 기술 전략의 주요 측면으로 클라우드 컴퓨팅을 채택했습니다. 일반적으로 워크로드를 로 마이그레이션 AWS 클라우드 하여 민첩성, 비용 절감, 성능, 가용성, 복원력 및 확장성을 높입니다. 대부분의 애플리케이션은 쉽게 마이그레이션할 수 있지만, 일부 애플리케이션은 온프레미스 환경의 짧은 지연 시간과 로컬 데이터 처리를 활용하거나, 높은 데이터 전송 비용을 피하거나, 규정 준수를 위해 온프레미스에 남아 있어야 합니다. 또한 애플리케이션 하위 집합을 클라우드로 이동하기 전에 다시 설계하거나 현대화해야 할 수 있습니다. 이를 통해 많은 조직이 하이브리드 클라우드 아키텍처를 찾아 온프레미스 및 클라우드 운영을 통합하여 광범위한 사용 사례를 지원할 수 있습니다. 이 하이브리드 접근 방식은 온프레미스 및 클라우드 기반 컴퓨팅의 이점을 제공할 수 있으며 엣지 컴퓨팅 시나리오에 특히 유용할 수 있습니다.

를 사용하여 하이브리드 클라우드를 구축할 때는 하이브리드 클라우드 전략과 기술 전략을 결정하는 것이 AWS 좋습니다.

- 하이브리드 클라우드 전략은 비즈니스 목표를 지원하기 위해 클라우드 및 온프레미스 리소스의 소비를 관리하는 지침을 제공합니다. 이 지침에서는 클라우드로의 지속적인 마이그레이션 지원, 재해 발생 시 비즈니스 연속성 보장, 지연 시간이 짧은 애플리케이션을 지원하기 위해 클라우드 인프라를 온프레미스 환경으로 확장, 국제적 입지 확장 등 하이브리드 클라우드 구축을 위한 일반적인 사용 사례를 설명합니다 AWS. 이 전략을 정의하면 하이브리드 클라우드 구축을 위한 비즈니스 목표를 식별하고 정의하는 데 도움이 되며 하이브리드 클라우드에서의 워크로드 배치에 대한 지침을 제공합니다.
- 하이브리드 클라우드에 대한 기술 전략은 하이브리드 클라우드 아키텍처의 기본 원칙을 식별하고 구현 프레임워크를 정의합니다. 이 지침에서는 계획된 하이브리드 클라우드 구현의 원칙을 정의하는 데 도움이 되는 일관되게 배포되고 관리되는 하이브리드 클라우드 아키텍처의 공통 요구 사항을 간략하게 설명합니다. 이러한 요구 사항에는 클라우드 인프라 전반의 리소스 프로비저닝 및 관리를 위한 표준화된 인터페이스가 포함됩니다.

이 가이드에서는 솔루션 아키텍트와 운영자가 하이브리드 클라우드를 구현하기 위한 구성 요소, 모범 사례, AWS 하이브리드 클라우드 및 리전 내 서비스를 식별하는 데 도움이 되는 운영 및 관리 프레임워크를 설명합니다 AWS.

많은 조직에서이 가이드에 설명된 솔루션을 사용하여에서 제공하는 규모, 민첩성, 혁신 및 글로벌 공간을 활용하는 하이브리드 클라우드 환경을 성공적으로 배포했습니다 AWS 클라우드. ([사례 연구](#) 참조) [AWS 하이브리드 클라우드 서비스](#)는 클라우드에서 온프레미스 및 엣지로 일관된 AWS 경험을 제공합니다. 최종 사용자 디바이스 또는 기존 온프레미스 데이터 센터와 워크로드 서버 간에 짧은 지연 시간이 필요한 경우 AWS Outposts 및 AWS 로컬 영역 장소 컴퓨팅, 스토리지, 데이터베이스 및 기타와 같은 서비스는 대규모 인구 및 산업 센터와 AWS 서비스 가깝습니다.

이 가이드에서는 다음 주제를 다룹니다.

- [개요](#)
- [사전 조건 및 제한 사항](#)
- 하이브리드 클라우드 채택 프로세스:
 - [엣지에서의 네트워킹](#)
 - [엣지의 보안](#)
 - [엣지의 복원력](#)
 - [엣지에서의 용량 계획](#)
 - [엣지 인프라 관리](#)
- [리소스](#)
- [기여자](#)
- [문서 기록](#)

개요

이 가이드에서는 하이브리드 클라우드에 대한 AWS 권장 사항을 [네트워킹](#), [보안](#), [복원력](#), [용량 계획](#) 및 [인프라 관리](#)의 5가지 원칙으로 분류합니다. 또는와 같은 AWS 하이브리드 엣지 서비스를 사용하여 준비 상태를 개선하고 마이그레이션 전략을 개발하는 데 도움이 AWS Outposts 되는 지침을 제공합니다 AWS 로컬 영역. 이 가이드를 따르고 프로세스를 개발할 때 AWS 계정 팀과 협력하거나 AWS 하이브리드 클라우드 전문가가 도움을 줄 수 AWS Partner 있도록 하는 것이 좋습니다.

Note

AWS Outposts 및 로컬 영역은 유사한 문제를 해결하지만 사용 사례와 사용 가능한 서비스 및 기능을 검토하여 필요에 가장 적합한 제품을 결정하는 것이 좋습니다. 자세한 내용은 AWS 블로그 게시물 [AWS 로컬 영역 및 엣지 워크로드에 적합한 기술 AWS Outposts](#) 선택을 참조하세요.

하이브리드 클라우드 워크숍

AWS 하이브리드 클라우드 주제 전문가(SME)의 지원을 받아 하이브리드 클라우드 워크숍을 실행하여 이 가이드에서 설명하는 5가지 원칙과 관련하여 회사의 성숙도를 평가할 수 있습니다.

워크숍은 네트워킹, 보안, 규정 준수, DevOps, 가상화 및 사업부와 같은 조직 내 내부 영역에 중점을 둡니다. 이 가이드의 하이브리드 클라우드 [채택 프로세스 섹션에 있는 단계에 따라 조직의 요구 사항을 충족하고 구현 세부 정보를 정의하는 하이브리드 클라우드](#) 아키텍처를 설계하는 데 도움이 됩니다.

PoCs

특정 요구 사항이 있는 경우 개념 증명(PoCs)을 사용하여 로컬 영역에서 해당 요구 사항에 AWS Outposts 맞게 기능을 검증할 수 있습니다.

AWS 는 PoCs 사용하여 Outpost 또는 Local Zone으로 이동하려는 워크로드를 테스트하여 워크로드가 테스트 아키텍처에서 작동할지 여부를 결정하는 데 도움이 됩니다. 테스트를 위해 로컬 영역에 액세스하려면 [로컬 영역 설명서](#)의 지침을 따릅니다. 에서 워크로드를 테스트하려면 팀과 AWS Outposts 협력 AWS 계정 하거나 AWS Outposts 테스트 실험실 AWS Partner 에 액세스하고 솔루션 아키텍트로부터 AWS 지침을 받으세요. 모든 시나리오에서 PoC를 개발하려면 다음을 포함하는 테스트 문서를 생성해야 합니다.

- AWS 서비스 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Block Store(Amazon EBS), Amazon Virtual Private Cloud(Amazon VPC) 및 Amazon Elastic Kubernetes Service(Amazon EKS)와 같은를 사용하려면
- 사용할 인스턴스의 크기 및 수(예: m5.xlarge 또는 c5.2xlarge)
- 테스트 아키텍처 다이어그램
- 테스트 성공 기준
- 실행할 각 테스트의 세부 정보 및 목표

원칙

다음 섹션에서는이 가이드에서 설명하는 아키텍처를 사용하기 위한 [사전 조건 및 제한](#) 사항을 다룹니다. 이후 섹션에서는 하이브리드 클라우드 워크숍 중에 생성하는 권장 사항 문서가 구현에 필요한 설계 세부 정보를 반영할 수 있도록 각 요소의 세부 정보를 다룹니다.

- [엣지에서의 네트워킹](#)
- [엣지의 보안](#)
- [엣지의 복원력](#)
- [엣지에서의 용량 계획](#)
- [엣지 인프라 관리](#)

사전 조건 및 제한 사항

이 가이드를 따르기 전에 AWS 계정 팀과 협력하거나 AWS Outposts 및 로컬 영역을 사용하여 엣지 아키텍처를 구현 AWS Partner 하기 위한 사전 조건 및 제한 사항을 검토하세요.

사전 조건

AWS Outposts

- 기존 데이터 센터는 시설, 네트워킹 및 전력에 대한 [AWS Outposts 요구 사항을](#) 충족해야 합니다. AWS Outposts 는 5~15kVA의 중복 전원 입력, 분당 입방 피트(CFM) 공기 흐름의 145.8배, 41°F(5°C)~95°F(35°C)의 주변 온도가 있는 데이터 센터 환경에서 작동하도록 설계되었습니다.
- [AWS Outposts 랙 FAQs](#)를 참조하여 해당 국가에서 AWS Outposts 서비스를 사용할 수 있는지 확인합니다. 질문을 참조하세요. Outpost 랙을 사용할 수 있는 국가 및 지역은 어디인가요?
- 조직에 4개 이상의 [AWS Outposts 랙이](#) 필요한 경우 데이터 센터는 [집계, 코어, 엣지\(ACE\) 랙 요구 사항을](#) 충족해야 합니다.
- 사용 사례에 필요한 경우 적절한 백업 연결을 통해 [AWS Outposts 에 AWS 리전](#) 연결하려면 인터넷 또는 500Mbps(1Gbps가 더 좋음) 이상의 AWS Direct Connect 링크를 제공하고 유지해야 합니다. 에서 리전 AWS Outposts 까지의 왕복 시간 지연 시간은 최대 175밀리초여야 합니다.
- [AWS Enterprise Support](#) 또는 [AWS 통합 운영](#) 플랜에 대한 활성 계약이 있어야 합니다.

AWS 로컬 영역

- AWS 로컬 영역은 데이터 센터 또는 사용자와 가까운 곳에서 사용할 수 있어야 합니다. [AWS 로컬 영역 위치를](#) 참조하세요.
- 온프레미스 인프라에서 로컬 영역으로 네트워크가 연결되어 있는지 확인합니다.
 - 옵션 1: 데이터 센터에서 로컬 영역에 가장 가까운 [Direct Connect 존재 지점\(PoP\)](#)으로 연결되는 Direct Connect 링크입니다. 자세한 내용은 로컬 영역 설명서의 [Direct Connect](#)를 참조하세요.
 - 옵션 2: 온프레미스 Virtual Private Network(VPN) 어플라이언스와 로컬 영역의 Amazon EC2에서 소프트웨어 기반 VPN 어플라이언스를 시작하는 데 필요한 라이선스 외에도 인터넷 링크입니다. 자세한 내용은 로컬 영역 설명서의 [VPN 연결을](#) 참조하세요.

추가 연결 옵션은 [로컬 영역 설명서를 참조하세요](#).

제한 사항

AWS Outposts

- AWS Outposts 다중 AZ 배포의 Amazon Relational Database Service(Amazon RDS)에는 고객 소유 IP(CoIP) 주소 풀이 필요합니다. 자세한 내용은 [Amazon RDS on의 고객 소유 IP 주소를 참조하세요 AWS Outposts](#).
- 의 다중 AZ AWS Outposts 는 Amazon RDS on에서 지원되는 모든 버전의 MySQL 및 PostgreSQL 에 사용할 수 있습니다 AWS Outposts. 자세한 내용은 [Amazon RDS 기능에 대한 AWS Outposts 기반 Amazon RDS 지원](#)을 참조하세요. [의 AWS Outposts Amazon RDS는 SQL Server, Amazon RDS for MySQL 및 Amazon RDS for PostgreSQL 데이터베이스를 지원합니다](#). MySQL PostgreSQL
- AWS Outposts 는에서 연결이 끊어졌을 때 작동하도록 설계되지 않았습니다 AWS 리전. 자세한 내용은 백서 고가용성 설계 및 아키텍처 고려 사항 [의 실패 모드 측면에서 생각](#) 섹션을 AWS 참조하세요. AWS Outposts
- 의 Amazon Simple Storage Service(Amazon S3) AWS Outposts 에는 몇 가지 제한 사항이 있습니다. 이에 대해서는 [Amazon S3 on Outposts가 Amazon S3와 어떻게 다른가요?](#)에서 설명합니다. Amazon S3 on Outposts 사용 설명서의 섹션.
- 의 Application Load Balancer AWS Outposts 는 상호 TLS(mTLS) 또는 고정 세션을 지원하지 않습니다.
- ACE 랙은 완전히 둘러싸여 있지 않으며 전면 또는 후면 도어가 포함되어 있지 않습니다.
- 인스턴스 용량 도구는 새 주문에만 적용할 수 있습니다.

AWS 로컬 영역

- 로컬 영역에는 AWS Site-to-Site VPN 엔드포인트가 없습니다. 대신 Amazon EC2에서 소프트웨어 기반 VPN을 사용합니다.
- 로컬 영역은 지원하지 않습니다 AWS Transit Gateway. 대신 Direct Connect 프라이빗 가상 인터페이스(VIF)를 사용하여 로컬 영역에 연결합니다.
- 모든 로컬 영역이 Amazon RDS, Amazon FSx, Amazon EMR 또는 Amazon ElastiCache 또는 NAT 게이트웨이와 같은 서비스를 지원하는 것은 아닙니다. 자세한 내용은 [AWS 로컬 영역 features](#)를 참조하세요.
- 로컬 영역의 Application Load Balancer는 mTLS 또는 고정 세션을 지원하지 않습니다.

하이브리드 클라우드 채택 프로세스

다음 섹션에서는 AWS 하이브리드 클라우드의 각 요소에 대한 아키텍처 및 설계 세부 정보에 대해 설명합니다.

- [엣지에서의 네트워킹](#)
- [엣지의 보안](#)
- [엣지의 복원력](#)
- [엣지에서의 용량 계획](#)
- [엣지 인프라 관리](#)

엣지에서의 네트워킹

AWS Outposts 또는 로컬 영역과 같은 AWS 엣지 인프라를 사용하는 솔루션을 설계할 때는 네트워크 설계를 신중하게 고려해야 합니다. 네트워크는 이러한 엣지 로케이션에 배포된 워크로드에 도달하기 위한 연결의 기반을 형성하며 짧은 지연 시간을 보장하는 데 매우 중요합니다. 이 섹션에서는 하이브리드 엣지 연결의 다양한 측면을 간략하게 설명합니다.

VPC 아키텍처

Virtual Private Cloud(VPC)는 모든 가용 영역에 걸쳐 있습니다 AWS 리전. AWS 콘솔 또는 AWS Command Line Interface (AWS CLI)를 사용하여 Outpost 또는 로컬 영역 서브넷을 추가하여 리전의 모든 VPC를 Outpost 또는 로컬 영역으로 원활하게 확장할 수 있습니다. 다음 예제에서는를 사용하여 AWS Outposts 및 로컬 영역에서 서브넷을 생성하는 방법을 보여줍니다 AWS CLI.

- AWS Outposts: VPC에 Outpost 서브넷을 추가하려면 Outpost의 Amazon 리소스 이름(ARN)을 지정합니다.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:111111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

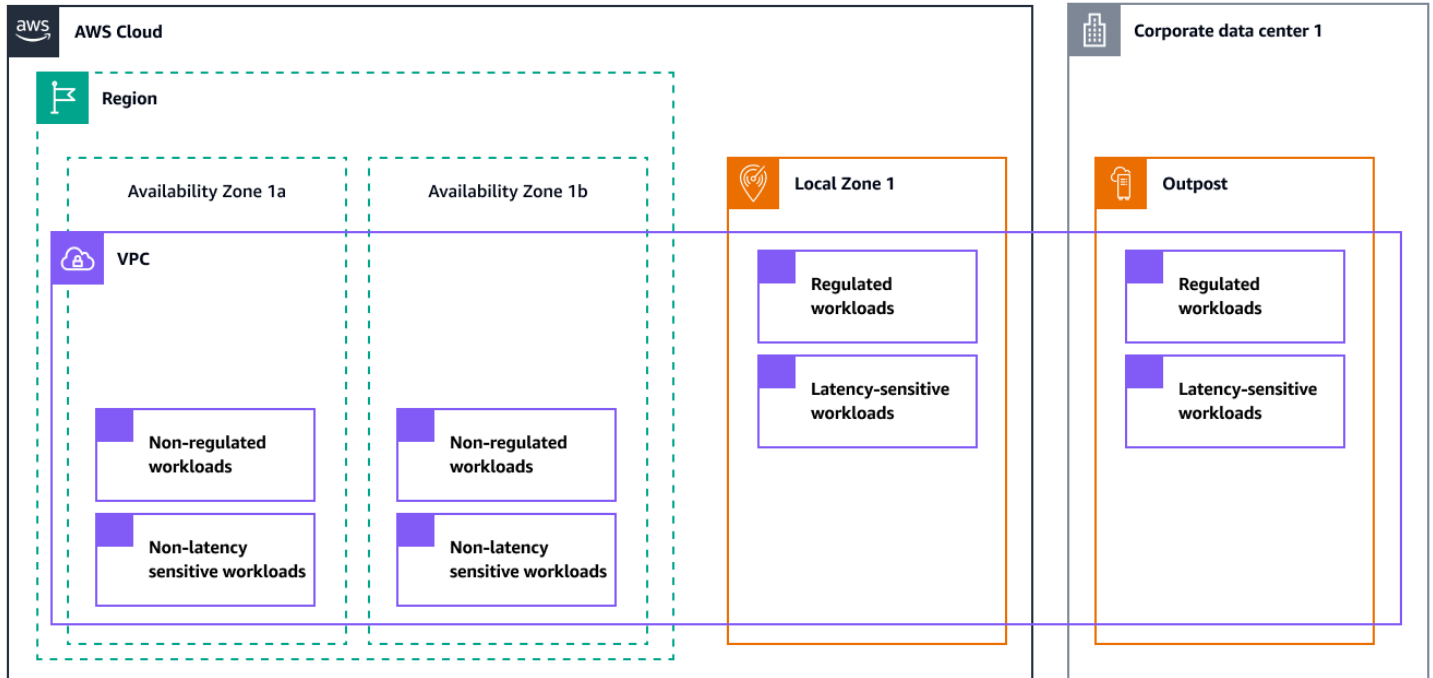
자세한 내용은 [AWS Outposts 설명서](#)를 참조하세요.

- 로컬 영역: VPC에 로컬 영역 서브넷을 추가하려면 가용 영역에 사용하는 것과 동일한 절차를 따르되 로컬 영역 ID(<local-zone-name>다음 예제에서는)를 지정합니다.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

자세한 내용은 [Local Zones 설명서를 참조하세요](#).

다음 다이어그램은 Outpost 및 Local Zone 서브넷을 포함하는 AWS 아키텍처를 보여줍니다.



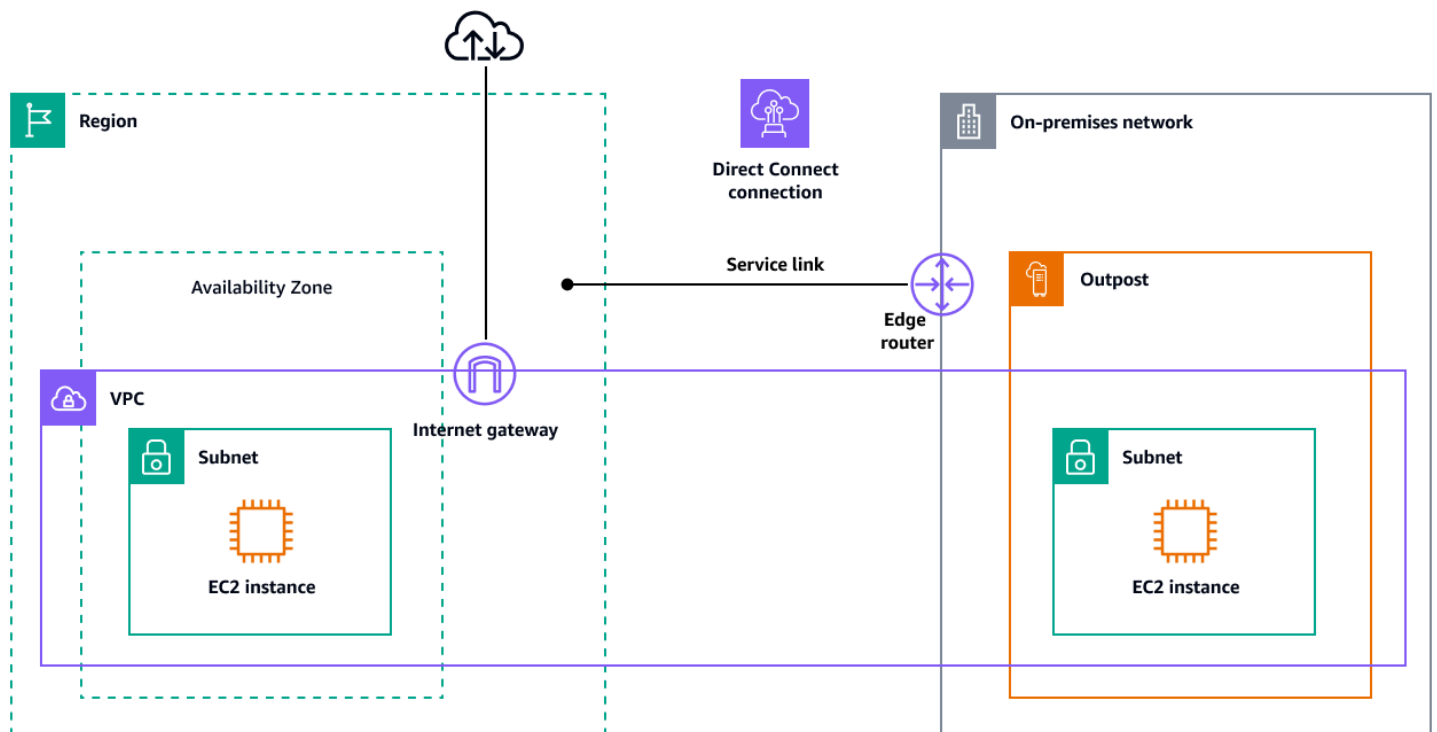
엣지-리전 트래픽

로컬 영역 및와 같은 서비스를 사용하여 하이브리드 아키텍처를 설계할 때는 엣지 인프라와 간의 제어 흐름과 데이터 트래픽 흐름을 모두 AWS Outposts고려하세요 AWS 리전. 엣지 인프라 유형에 따라 사용자의 책임이 달라질 수 있습니다. 일부 인프라에서는 상위 리전에 대한 연결을 관리해야 하는 반면, AWS 글로벌 인프라를 통해 이를 처리하는 인프라도 있습니다. 이 섹션에서는 로컬 영역 및에 대한 컨트롤 플레인 및 데이터 영역 연결 영향을 살펴봅니다 AWS Outposts.

AWS Outposts 컨트롤 플레인

AWS Outposts 는 서비스 링크라는 네트워킹 구조를 제공합니다. 서비스 링크는 AWS Outposts 와 선택한 리전 AWS 리전 또는 상위 리전(홈 리전이라고도 함) 간의 필수 연결입니다. 이를 통해 Outpost를 관리하고 Outpost와 간의 트래픽을 교환할 수 있습니다 AWS 리전. 서비스 링크는 암호화된 VPN 연

결 세트를 사용하여 홈 리전과 통신합니다. AWS 리전 인터넷 링크 또는 Direct Connect 퍼블릭 가상 인터페이스(퍼블릭 VIF) 또는 Direct Connect 프라이빗 가상 인터페이스(프라이빗 VIF)를 통해 AWS Outposts 와 간의 연결을 제공해야 합니다. 최적의 경험과 복원력을 AWS 위해는에 대한 서비스 링크 연결에 최소 500Mbps(1Gbps가 더 좋음)의 중복 연결을 사용할 것을 권장합니다 AWS 리전. 최소 500Mbps 서비스 링크 연결을 사용하면 Amazon EC2 인스턴스를 시작하고, Amazon EBS 볼륨을 연결하고, Amazon EKS, Amazon EMR 및 Amazon CloudWatch 지표와 AWS 서비스 같은 액세스를 수행할 수 있습니다. 네트워크는 Outpost와 상위의 서비스 링크 엔드포인트 간에 1,500바이트의 최대 전송 단위(MTU)를 지원해야 합니다 AWS 리전. 자세한 내용은 Outposts 설명서의 [AWS Outposts 에 대한 연결을 AWS 리전](#) 참조하세요.



Direct Connect 및 퍼블릭 인터넷을 사용하는 서비스 링크에 대한 복원력이 뛰어난 아키텍처를 생성하는 방법에 대한 자세한 내용은 AWS 백서 AWS Outposts 고가용성 설계 및 아키텍처 고려 사항의 [앵커 연결](#) 섹션을 참조하세요.

AWS Outposts 데이터 영역

AWS Outposts 와 사이의 데이터 영역은 컨트롤 플레인에서 사용하는 것과 동일한 서비스 링크 아키텍처에서 AWS 리전 지원됩니다. AWS Outposts 와 간의 데이터 영역 서비스 링크 대역폭은 교환해야 하는 데이터의 양과 상관관계가 AWS 리전 있어야 합니다. 데이터 종속성이 클수록 링크 대역폭이 커집니다.

대역폭 요구 사항은 다음 특성에 따라 달라집니다.

- AWS Outposts 랙 수 및 용량 구성
- AMI 크기, 애플리케이션 탄력성 및 버스트 속도 요구 사항과 같은 워크로드 특성
- 리전에 대한 VPC 트래픽

의 EC2 인스턴스 AWS Outposts 와의 EC2 인스턴스 AWS 리전 간 트래픽의 MTU는 1,300바이트입니다. 리전과 간에 상호 종속성이 있는 아키텍처를 제안하기 전에 AWS 하이브리드 클라우드 전문가와 이러한 요구 사항에 대해 논의하는 것이 좋습니다 AWS Outposts.

로컬 영역 데이터 영역

로컬 영역과 간의 데이터 영역은 글로벌 인프라를 통해 AWS 지원 AWS 리전 됩니다. 데이터 영역은 VPC를 통해에서 로컬 영역 AWS 리전 으로 확장됩니다. 또한 로컬 영역은에 대한 높은 대역폭의 보안 연결을 제공하며 동일한 APIs AWS 리전및 도구 세트를 통해 전체 리전 서비스에 원활하게 연결할 수 있습니다.

다음 표에는 연결 옵션과 관련 MTUs.

시작	로	MTU
리전의 Amazon EC2	로컬 영역의 Amazon EC2	1,300바이트
Direct Connect	Local Zones	1,468바이트
인터넷 게이트웨이	Local Zones	1,500바이트
로컬 영역의 Amazon EC2	로컬 영역의 Amazon EC2	9,001바이트

로컬 영역은 AWS 글로벌 인프라를 사용하여 연결합니다 AWS 리전. 인프라에서 완벽하게 관리 AWS되므로이 연결을 설정할 필요가 없습니다. 리전과 로컬 영역 간에 공동 종속성이 있는 아키텍처를 설계하기 전에 AWS 하이브리드 클라우드 전문가와 로컬 영역 요구 사항 및 고려 사항에 대해 논의하는 것이 좋습니다.

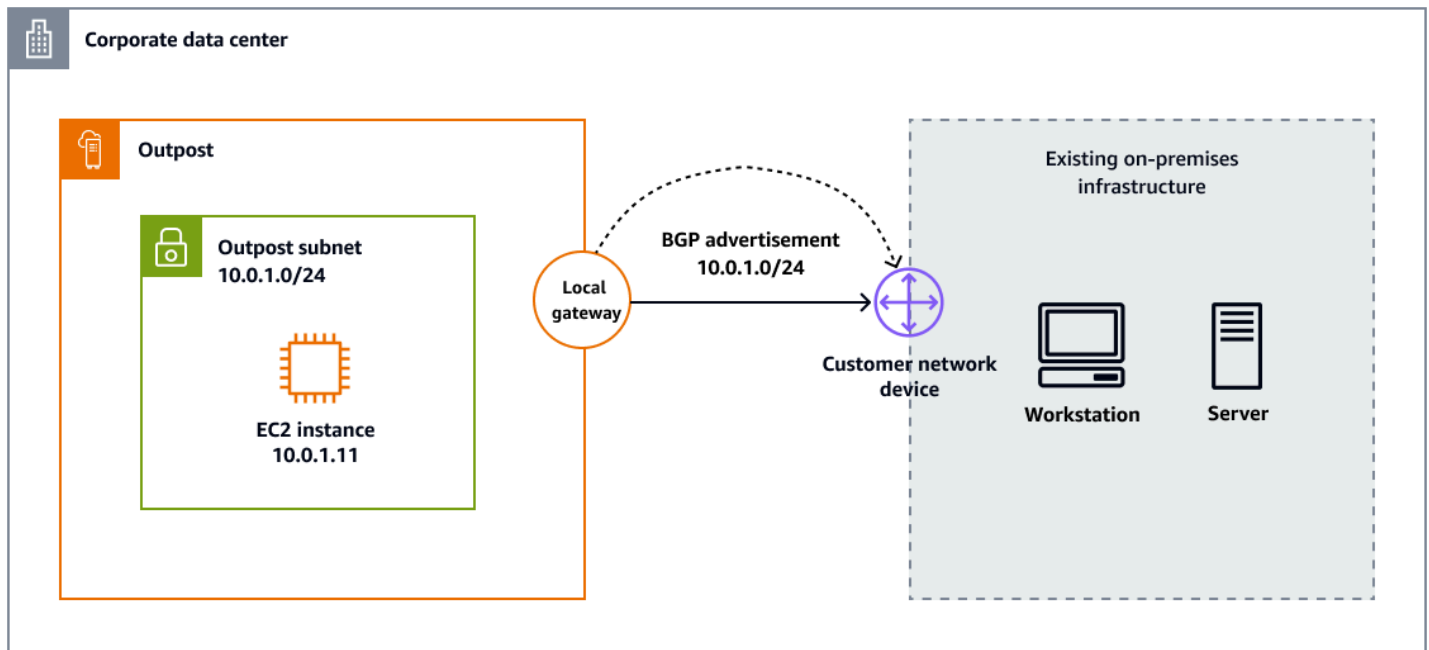
엣지-온프레미스 트래픽

AWS 하이브리드 클라우드 서비스는 짧은 지연 시간, 로컬 데이터 처리 또는 데이터 레지던시 규정 준수가 필요한 사용 사례를 해결하도록 설계되었습니다. 이 데이터에 액세스하기 위한 네트워크 아키텍처는 중요하며 워크로드가 AWS Outposts 또는 로컬 영역에서 실행 중인지에 따라 달라집니다. 로컬 연결에는 다음 섹션에서 설명하는 대로 잘 정의된 범위도 필요합니다.

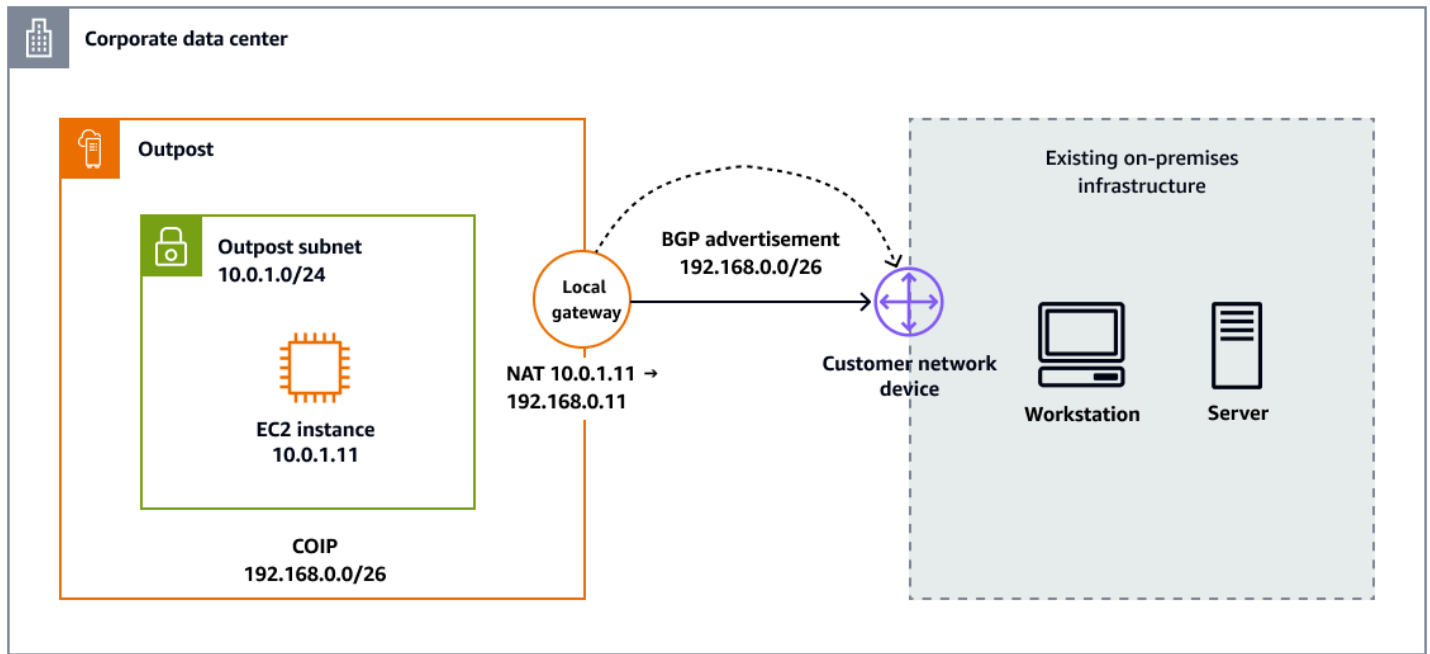
AWS Outposts 로컬 게이트웨이

로컬 게이트웨이(LGW)는 AWS Outposts 아키텍처의 핵심 구성 요소입니다. 로컬 게이트웨이는 Outpost 서브넷과 온프레미스 네트워크를 연결할 수 있게 해줍니다. LGW의 주요 역할은 Outpost에서 로컬 온프레미스 네트워크로의 연결을 제공하는 것입니다. 또한 [직접 VPC 라우팅](#) 또는 [고객 소유 IP 주소](#)를 통해 온프레미스 네트워크를 통해 인터넷에 대한 연결을 제공합니다.

- 직접 VPC 라우팅은 VPC에 있는 인스턴스의 프라이빗 IP 주소를 사용하여 온프레미스 네트워크와의 통신을 용이하게 합니다. 이러한 주소는 BGP(Border Gateway Protocol)를 사용하여 온프레미스 네트워크에 광고됩니다. BGP 광고는 Outpost 랙의 서브넷에 속하는 프라이빗 IP 주소에만 해당됩니다. 이 유형의 라우팅이 기본 모드입니다 AWS Outposts. 이 모드에서는 로컬 게이트웨이가 인스턴스에 대해 NAT를 수행하지 않으므로 EC2 인스턴스에 탄력적 IP 주소를 할당할 필요가 없습니다. 다음 다이어그램은 직접 VPC 라우팅을 사용하는 AWS Outposts 로컬 게이트웨이를 보여줍니다.



- 고객 소유 IP 주소를 사용하면 중복 CIDR 범위 및 기타 네트워크 토폴로지를 지원하는 고객 소유 IP(CoIP) 주소 풀이라고 하는 주소 범위를 제공할 수 있습니다. CoIP를 선택할 때는 주소 풀을 생성하고 로컬 게이트웨이 라우팅 테이블에 할당한 다음 BGP를 통해 이러한 주소를 네트워크에 다시 알려야 합니다. CoIP 주소는 온프레미스 네트워크의 리소스에 로컬 또는 외부 연결을 제공합니다. CoIP에서 새 탄력적 IP 주소를 할당한 다음 리소스에 할당하여 EC2 인스턴스와 같은 Outpost의 리소스에 이러한 IP 주소를 할당할 수 있습니다. 다음 다이어그램은 CoIP 모드를 사용하는 AWS Outposts 로컬 게이트웨이를 보여줍니다.



에서 로컬 네트워크 AWS Outposts 로의 로컬 연결에는 BGP 라우팅 프로토콜 활성화 및 BGP 피어 간의 광고 접두사와 같은 일부 파라미터 구성이 필요합니다. Outpost와 로컬 게이트웨이 간에 지원할 수 있는 MTU는 1,500바이트입니다. 자세한 내용은 AWS 하이브리드 클라우드 전문가에게 문의하거나 [AWS Outposts 설명서](#)를 검토하세요.

로컬 영역 및 인터넷

저지연 또는 로컬 데이터 레지던시가 필요한 산업(예: 게임, 라이브 스트리밍, 금융 서비스 및 정부)은 로컬 영역을 사용하여 인터넷을 통해 최종 사용자에게 애플리케이션을 배포하고 제공할 수 있습니다. 로컬 영역을 배포하는 동안 로컬 영역에서 사용할 퍼블릭 IP 주소를 할당해야 합니다. 탄력적 IP 주소를 할당할 때 IP 주소를 알릴 위치를 지정할 수 있습니다. 이 위치를 네트워크 경계 그룹이라고 합니다. 네트워크 경계 그룹은 퍼블릭 IP 주소를 AWS 광고하는 가용 영역, 로컬 영역 또는 AWS Wavelength 영역의 모음입니다. 이렇게 하면 AWS 네트워크와 이러한 영역의 리소스에 액세스하는 사용자 간의 지연 시간 또는 물리적 거리를 최소화할 수 있습니다. 로컬 영역에 대한 모든 네트워크 경계 그룹을 보려면 [로컬 영역 설명서의 사용 가능한](#) 로컬 영역을 참조하세요.

로컬 영역의 Amazon EC2 호스팅 워크로드를 인터넷에 노출하려면 EC2 인스턴스를 시작할 때 퍼블릭 IP 자동 할당 옵션을 활성화하면 됩니다. Application Load Balancer를 사용하는 경우 로컬 영역에 할당된 퍼블릭 IP 주소가 로컬 영역과 연결된 경계 네트워크에 의해 전파될 수 있도록 인터넷 경계로 정의할 수 있습니다. 또한 탄력적 IP 주소를 사용하는 경우 시작 후 이러한 리소스 중 하나를 EC2 인스턴스와 연결할 수 있습니다. 로컬 영역의 인터넷 게이트웨이를 통해 트래픽을 전송하면 리전에서 사용하는 것과 동일한 [인스턴스 대역폭](#) 사양이 적용됩니다. 로컬 영역 네트워크 트래픽은 지연 시간이 짧은 컴퓨

팅에 액세스할 수 있도록 로컬 영역의 상위 리전을 통과하지 않고 인터넷 또는 PoPs(존재 지점)로 직접 이동합니다.

로컬 영역은 인터넷을 통해 다음과 같은 연결 옵션을 제공합니다.

- 퍼블릭 액세스: 인터넷 게이트웨이를 통해 탄력적 IP 주소를 사용하여 워크로드 또는 가상 어플라이언스를 인터넷에 연결합니다.
- 아웃바운드 인터넷 액세스: 리소스가 직접적인 인터넷 노출 없이 연결된 탄력적 IP 주소가 있는 NAT(네트워크 주소 변환) 인스턴스 또는 가상 어플라이언스를 통해 퍼블릭 엔드포인트에 도달할 수 있습니다.
- VPN 연결: 연결된 탄력적 IP 주소가 있는 가상 어플라이언스를 통해 IPsec(인터넷 프로토콜 보안) VPN을 사용하여 프라이빗 연결을 설정합니다.

자세한 내용은 [로컬 영역 설명서의 로컬 영역에 대한 연결 옵션](#)을 참조하세요.

로컬 영역 및 Direct Connect

로컬 영역은 프라이빗 네트워크 연결을 통해 트래픽을 라우팅할 수 Direct Connect있는 도 지원합니다. 자세한 내용은 [로컬 영역 설명서의 로컬 영역의 Direct Connect](#)를 참조하세요.

로컬 영역 및 전송 게이트웨이

AWS Transit Gateway 는 로컬 영역 서브넷에 대한 직접 VPC 연결을 지원하지 않습니다. 그러나 동일한 VPC의 상위 가용 영역 서브넷에서 Transit Gateway 연결을 생성하여 로컬 영역 워크로드에 연결할 수 있습니다. 이 구성을 사용하면 여러 VPCs와 로컬 영역 워크로드 간의 상호 연결이 가능합니다. 자세한 내용은 [로컬 영역 설명서의 로컬 영역 간 전송 게이트웨이 연결](#)을 참조하세요.

로컬 영역 및 VPC 피어링

새 서브넷을 생성하고 로컬 영역에 할당하여 상위 리전에서 로컬 영역으로 VPC를 확장할 수 있습니다. 로컬 영역으로 확장되는 VPCs 피어링을 설정할 수 있습니다. 피어링된 VPCs가 동일한 로컬 영역에 있는 경우 트래픽은 로컬 영역 내에 유지되고 상위 리전을 통해 헤어핀되지 않습니다.

엣지의 보안

에서는 AWS 클라우드보안이 최우선 순위입니다. 조직이 클라우드의 확장성과 유연성을 채택함에 따라 보안, 자격 증명 및 규정 준수를 주요 비즈니스 요소로 채택하도록 AWS 지원합니다.는 보안을 핵심 인프라에 AWS 통합하고 고유한 클라우드 보안 요구 사항을 충족하는 데 도움이 되는 서비스를 제공합니다. 아키텍처 범위를 로 확장하면 Local Zones 및 Outposts와 같은 인프라를 통합하는 이점을

AWS 클라우드에 누릴 수 있습니다 AWS 리전. 이 통합 AWS 을 통해서는 선택한 코어 보안 서비스 그룹을 엣지로 확장할 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. [AWS 공동 책임 모델](#)은 클라우드의 보안과 클라우드의 보안을 구분합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#)의 일환으로 AWS 보안의 효과를 정기적으로 테스트하고 확인합니다.
- 클라우드의 보안 - 사용자의 책임은 AWS 서비스 사용하는에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

데이터 보호

AWS 공동 책임 모델은 AWS Outposts 및의 데이터 보호에 적용됩니다 AWS 로컬 영역. 이 모델에 설명된 대로 AWS 는 AWS 클라우드 (클라우드의 보안)를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라(클라우드의 보안)에서 호스팅되는 콘텐츠를 제어할 책임은 사용자에게 있습니다. 이 콘텐츠에는 AWS 서비스 사용하는에 대한 보안 구성 및 관리 작업이 포함됩니다.

데이터 보호를 위해 자격 AWS 계정 증명을 보호하고 [AWS Identity and Access Management \(IAM\)](#) 또는를 사용하여 개별 사용자를 설정하는 것이 좋습니다 [AWS IAM Identity Center](#). 이렇게 하면 각 사용자에게 직무를 수행하는 데 필요한 권한만 부여됩니다.

저장 시 암호화

EBS 볼륨의 암호화

AWS Outposts를 사용하면 모든 데이터가 저장 시 암호화됩니다. 키 구성 요소는 외부 키인 Nitro 보안 키(NSK)로 래핑되며,이 키는 이동식 디바이스에 저장됩니다. NSK는 Outpost 랙의 데이터를 복호화하는 데 필요합니다. Amazon EBS 암호화를 EBS 볼륨과 스냅샷에 사용할 수 있습니다. Amazon EBS 암호화는 [AWS Key Management Service \(AWS KMS\)](#) 및 KMS 키를 사용합니다.

로컬 영역의 경우 계정에 암호화가 활성화되지 않은 한 [AWS 로컬 영역 FAQ](#)에 설명된 목록(질문: 로컬 영역에서 EBS 볼륨의 기본 암호화 동작은 무엇입니까? 참조)을 제외하고 모든 로컬 영역에서 모든 EBS 볼륨이 기본적으로 암호화됩니다.

Amazon S3 on Outposts의 암호화

기본적으로, Amazon S3 on Outposts에 저장된 모든 데이터는 Amazon S3 관리형 암호화 키를 통한 서버 측 암호화(SSE-S3)를 사용하여 암호화됩니다. 원한다면 고객 제공 암호화 키(SSE-C)로 서버 측

암호화를 사용할 수도 있습니다. SSE-C를 사용하려면 객체 API 요청의 일부로 암호화 키를 지정합니다. 서버 측 암호화는 객체 메타데이터가 아닌 객체 데이터만 암호화합니다.

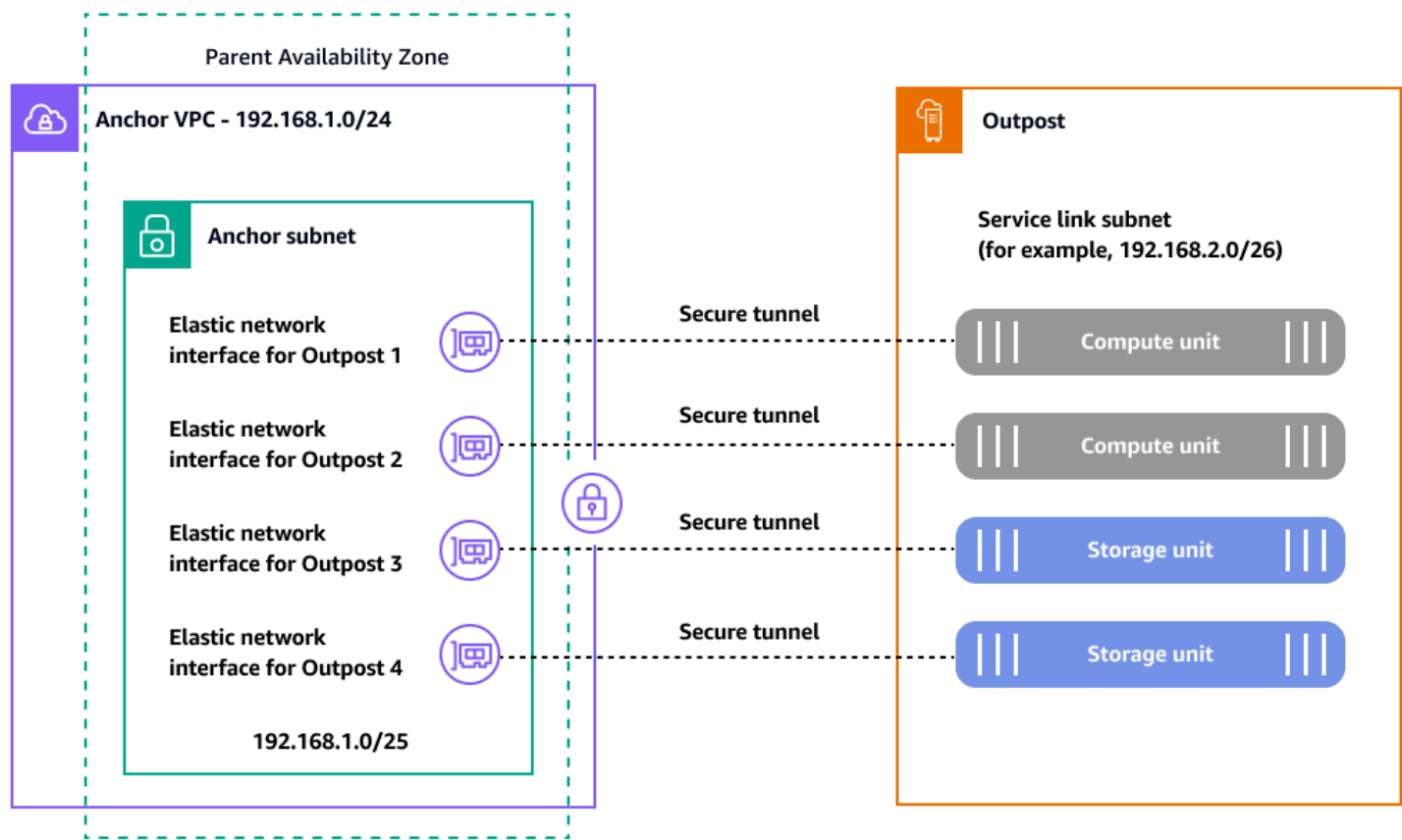
 Note

Amazon S3 on Outposts는 KMS 키를 사용한 서버 측 암호화(SSE-KMS)를 지원하지 않습니다.

전송 중 암호화

AWS Outposts의 경우 서비스 링크는 Outpost 서버와 선택한 AWS 리전 (또는 홈 리전) 간의 필수 연결이며 Outpost를 관리하고와 트래픽을 주고받을 수 있도록 합니다 AWS 리전. 서비스 링크는 AWS 관리형 VPN을 사용하여 홈 리전과 통신합니다. 내부의 각 호스트는 컨트롤 플레인 트래픽과 VPC 트래픽을 분할하는 VPN 터널 세트를 AWS Outposts 생성합니다. 에 대한 서비스 링크 연결(인터넷 또는 Direct Connect)에 따라 AWS Outposts 해당 터널 위에 오버레이를 생성하려면 서비스 링크에 대해 방화벽 포트를 열어야 합니다. 및 서비스 링크의 보안에 대한 자세한 기술 정보는 AWS Outposts 설명서의 AWS Outposts의 [서비스 링크를 통한 연결](#) 및 [인프라 보안을 AWS Outposts](#) 참조하세요.

AWS Outposts 서비스 링크는 다음 다이어그램과 AWS 리전같이 상위에 대한 컨트롤 플레인 및 데이터 플레인 연결을 설정하는 암호화된 터널을 생성합니다.



Anchor VPC CIDR: /25 or larger that doesn't conflict with 10.1.0.0/16
IAM role: `AWSServiceRoleForOutposts_<OutpostID>`

각 AWS Outposts 호스트(컴퓨팅 및 스토리지)는 상위 리전과 통신하려면 잘 알려진 TCP 및 UDP 포트를 통해 암호화된 터널이 필요합니다. 다음 표에는 UDP 및 TCP 프로토콜의 소스 및 대상 포트와 주소가 나와 있습니다.

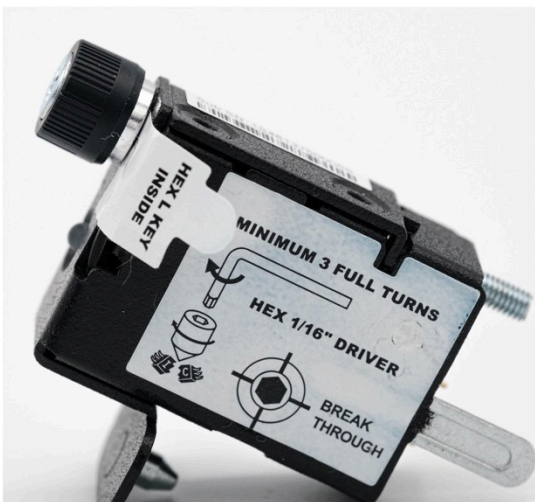
프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	443	AWS Outposts 서비스 링크 /26	443	AWS Outposts 리전의 퍼블릭 경로 또는 앵커 VPC CIDR
TCP	1025-65535	AWS Outposts 서비스 링크 /26	443	AWS Outposts 리전의 퍼블릭

프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
				경로 또는 앵커 VPC CIDR

또한 로컬 영역은 Amazon의 매우 높은 대역폭의 중복 글로벌 프라이빗 백본을 통해 상위 리전에 연결됩니다. 이 연결을 통해 Local Zones에서 실행되는 애플리케이션이 다른에 빠르고 안전하며 원활하게 액세스할 수 있습니다 AWS 서비스. 로컬 영역이 AWS 글로벌 인프라의 일부인 한 글로벌 AWS 네트워크를 통해 흐르는 모든 데이터는 AWS 보안 시설을 떠나기 전에 물리적 계층에서 자동으로 암호화됩니다. 온프레미스 위치와 Direct Connect PoPs 간에 전송 중인 데이터를 암호화하여 로컬 영역에 액세스해야 하는 특정 요구 사항이 있는 경우 온프레미스 라우터 또는 스위치와 Direct Connect 엔드포인트 간에 MAC 보안(MACsec)을 활성화할 수 있습니다. 자세한 내용은 AWS 블로그 게시물 [Direct Connect 연결에 MACsec 보안 추가를 참조하세요](#).

데이터 삭제

에서 EC2 인스턴스를 중지하거나 종료하면 새 인스턴스에 할당되기 전에 하이퍼바이저가 인스턴스에 할당된 AWS Outposts 메모리를 스크러빙(0으로 설정)하고 모든 스토리지 블록을 재설정합니다. Outpost 하드웨어에서 데이터를 삭제하려면 특수 하드웨어를 사용해야 합니다. NSK는 다음 사진에 표시된 소형 디바이스로, Outpost의 모든 컴퓨팅 또는 스토리지 유닛의 전면에 연결됩니다. 데이터 센터 또는 콜로케이션 사이트에서 데이터가 노출되지 않도록 하는 메커니즘을 제공하도록 설계되었습니다. Outpost 디바이스의 데이터는 디바이스를 암호화하는 데 사용되는 키 지정 구성 요소를 래핑하고 래핑된 구성 요소를 NSK에 저장하여 보호됩니다. Outpost 호스트를 반환할 때 NSK를 깨뜨리고 칩을 물리적으로 파괴하는 칩에 작은 나사를 돌려 NSK를 파괴합니다. NSK를 폐기하면 Outpost에서 데이터를 암호화 방식으로 파쇄합니다.



ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 누가 AWS Outposts 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. 가 있는 경우 추가 비용 없이 IAM을 사용할 AWS 계정 수 있습니다.

다음 표에는 사용할 수 있는 IAM 기능이 나열되어 있습니다 AWS Outposts.

IAM 기능	AWS Outposts 지원
자격 증명 기반 정책	예
리소스 기반 정책	예*
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
액세스 제어 목록(ACL)	아니요
속성 기반 액세스 제어(ABAC)(정책 태그)	예
임시 보안 인증	예
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	예

* Amazon S3 on Outposts는 IAM 자격 증명 기반 정책 외에도 버킷 및 액세스 포인트 정책을 모두 지원합니다. 이는 Amazon S3 on Outposts 리소스에 연결된 리소스 [기본 정책](#)입니다.

에서 이러한 기능을 지원하는 방법에 대한 자세한 내용은 [AWS Outposts 사용 설명서](#)를 AWS Outposts참조하세요.

인프라 보안

인프라 보호는 정보 보안 프로그램의 핵심 요소입니다. 이를 통해 워크로드 시스템 및 서비스가 의도하지 않은 무단 액세스 및 잠재적 취약성으로부터 보호됩니다. 예를 들어 신뢰 경계(예: 네트워크 및 계층 경계), 시스템 보안 구성 및 유지 관리(예: 강화, 최소화 및 패치 적용), 운영 체제 인증 및 권한 부여(예: 사용자, 키 및 액세스 수준), 기타 적절한 정책 적용 지점(예: 웹 애플리케이션 방화벽 또는 API 게이트웨이)을 정의합니다.

AWS 는 다음 단원에서 설명한 대로 인프라 보호에 대한 다양한 접근 방식을 제공합니다.

네트워크 보호

사용자는 작업 인력 또는 고객의 일부일 수 있으며 어디에나 위치할 수 있습니다. 따라서 네트워크에 액세스할 수 있는 모든 사람을 신뢰할 수는 없습니다. 모든 계층에 보안을 적용하는 원칙을 따를 때는 [제로 트러스트](#) 접근 방식을 사용합니다. 제로 트러스트 보안 모델에서 애플리케이션 구성 요소 또는 마이크로서비스는 개별 구성 요소로 간주되며 다른 구성 요소 또는 마이크로서비스를 신뢰하는 구성 요소 또는 마이크로서비스는 없습니다. 제로 트러스트 보안을 달성하려면 다음 권장 사항을 따르세요.

- [네트워크 계층을 생성합니다](#). 계층화된 네트워크는 유사한 네트워킹 구성 요소를 논리적으로 그룹화하는 데 도움이 됩니다. 또한 무단 네트워크 액세스의 잠재적 영향 범위를 줄입니다.
- [트래픽 계층을 제어](#)합니다. 인바운드 및 아웃바운드 트래픽 모두에 대해 defense-in-depth 접근 방식을 사용하여 여러 제어를 적용합니다. 여기에는 보안 그룹(상태 저장 검사 방화벽), 네트워크 ACLs, 서브넷 및 라우팅 테이블의 사용이 포함됩니다.
- [검사 및 보호를 구현](#)합니다. 각 계층에서 트래픽을 검사하고 필터링합니다. [Network Access Analyzer](#)를 사용하여 VPC 구성에 의도하지 않은 잠재적 액세스가 있는지 검사할 수 있습니다. 네트워크 액세스 요구 사항을 지정하고 해당 요구 사항을 충족하지 않는 잠재적 네트워크 경로를 식별할 수 있습니다.

컴퓨팅 리소스 보호

컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lambda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다. 각 컴퓨팅 리소스 유형에는 보안에 대한 다른 접근 방식이 필요합니다. 그러나 이러한 리소스는 심층 방어, 취약성 관리, 공격 표면 감소, 구성 및 운영 자동화, 원격 작업 수행 등 고려해야 할 일반적인 전략을 공유합니다.

다음은 주요 서비스의 컴퓨팅 리소스를 보호하기 위한 일반적인 지침입니다.

- [취약성 관리 프로그램을 생성하고 유지](#) 관리합니다. EC2 인스턴스, Amazon Elastic Container Service(Amazon ECS) 컨테이너, Amazon Elastic Kubernetes Service(Amazon EKS) 워크로드와 같은 리소스를 정기적으로 스캔하고 패치합니다.
- [컴퓨팅 보호를 자동화합니다](#). 취약성 관리, 공격 표면 감소, 리소스 관리를 비롯한 보호 컴퓨팅 메커니즘을 자동화합니다. 이 자동화를 통해 워크로드의 다른 측면을 보호하는 데 사용할 수 있는 시간을 확보하고 인적 오류 위험을 줄일 수 있습니다.
- [공격 표면을 줄입니다](#). 운영 체제를 강화하고 사용하는 구성 요소, 라이브러리 및 외부 소모성 서비스를 최소화하여 의도하지 않은 액세스에 대한 노출을 줄입니다.

또한 사용하는 각 AWS 서비스 에 대해 [서비스 설명서](#)의 특정 보안 권장 사항을 확인합니다.

인터넷 액세스

AWS Outposts 및 로컬 영역 모두 워크로드에 인터넷 액세스 권한을 부여하는 아키텍처 패턴을 제공합니다. 이러한 패턴을 사용하는 경우 패치 적용, 업데이트, 외부의 Git 리포지토리 액세스 AWS 및 유사한 시나리오에 사용할 경우에만 리전의 인터넷 소비를 실행 가능한 옵션으로 고려하세요. 이 아키텍처 패턴의 경우 중앙 집중식 [인바운드 검사](#) 및 [중앙 집중식 인터넷 송신](#)의 개념이 적용됩니다. 이러한 액세스 패턴은 AWS Transit Gateway에 상주하지만 리전과 엣지 간의 데이터 경로를 통해 AWS Outposts 또는 로컬 영역에 연결된 NAT 게이트웨이 AWS 리전, 네트워크 방화벽 및 기타 구성 요소를 사용합니다.

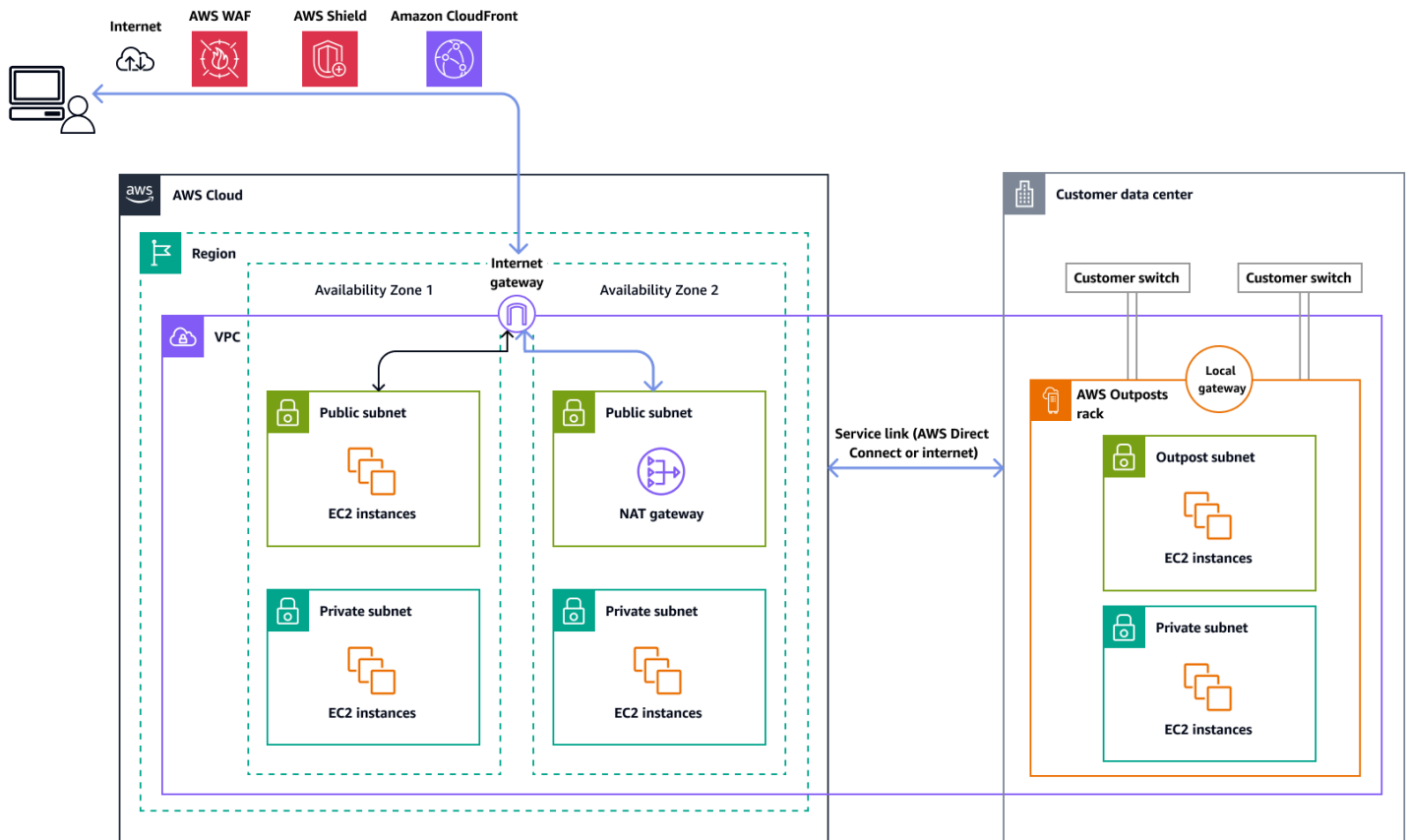
Local Zones는 네트워크 경계 그룹이라는 네트워크 구성을 채택합니다. 이 네트워크 경계 그룹은에 사용됩니다 AWS 리전. 이 네트워크 경계 그룹은 이러한 고유 그룹의 퍼블릭 IP 주소를 AWS 광고합니다. 네트워크 경계 그룹은 가용 영역, 로컬 영역 또는 Wavelength 영역으로 구성됩니다. 네트워크 경계 그룹에 사용할 퍼블릭 IP 주소 풀을 명시적으로 할당할 수 있습니다. 네트워크 경계 그룹을 사용하여 그룹에서 탄력적 IP 주소를 제공하도록 허용하여 인터넷 게이트웨이를 로컬 영역으로 확장할 수 있습니다. 이 옵션을 사용하려면 로컬 영역에서 사용할 수 있는 핵심 서비스를 보완하기 위해 다른 구성 요소를 배포해야 합니다. 이러한 구성 요소는 ISVs에서 가져온 것일 수 있으며 AWS 블로그 게시물 [Hybrid inspection architectures with](#)에 설명된 대로 [로컬 영역에서 검사 AWS 로컬 영역](#) 계층을 구축하는 데 도움이 될 수 있습니다.

에서 로컬 게이트웨이(LGW)를 사용하여 네트워크에서 인터넷에 연결 AWS Outposts하려면 AWS Outposts 서브넷과 연결된 사용자 지정 라우팅 테이블을 수정해야 합니다. 라우팅 테이블에는 LGW를 다음 홉으로 사용하는 기본 라우팅 항목(0.0.0.0/0)이 있어야 합니다. 방화벽, 침입 방지 시스템 또는 침입 탐지 시스템(IPS/IDS)과 같은 경계 방어를 포함하여 로컬 네트워크에 나머지 보안 제어를 구현하는 것은 사용자의 책임입니다. 이는 사용자와 클라우드 공급자 간의 보안 의무를 나누는 공동 책임 모델에 부합합니다.

상위를 통한 인터넷 액세스 AWS 리전

이 옵션에서는 Outpost의 워크로드가 [서비스 링크](#)와 상위의 인터넷 게이트웨이를 통해 인터넷에 액세스합니다 AWS 리전. 인터넷으로의 아웃바운드 트래픽은 VPC에서 인스턴스화된 NAT 게이트웨이를 통해 라우팅할 수 있습니다. 수신 및 송신 트래픽에 대한 추가 보안을 위해에서 AWS WAF AWS Shield 및 Amazon CloudFront와 같은 AWS 보안 서비스를 사용할 수 있습니다 AWS 리전.

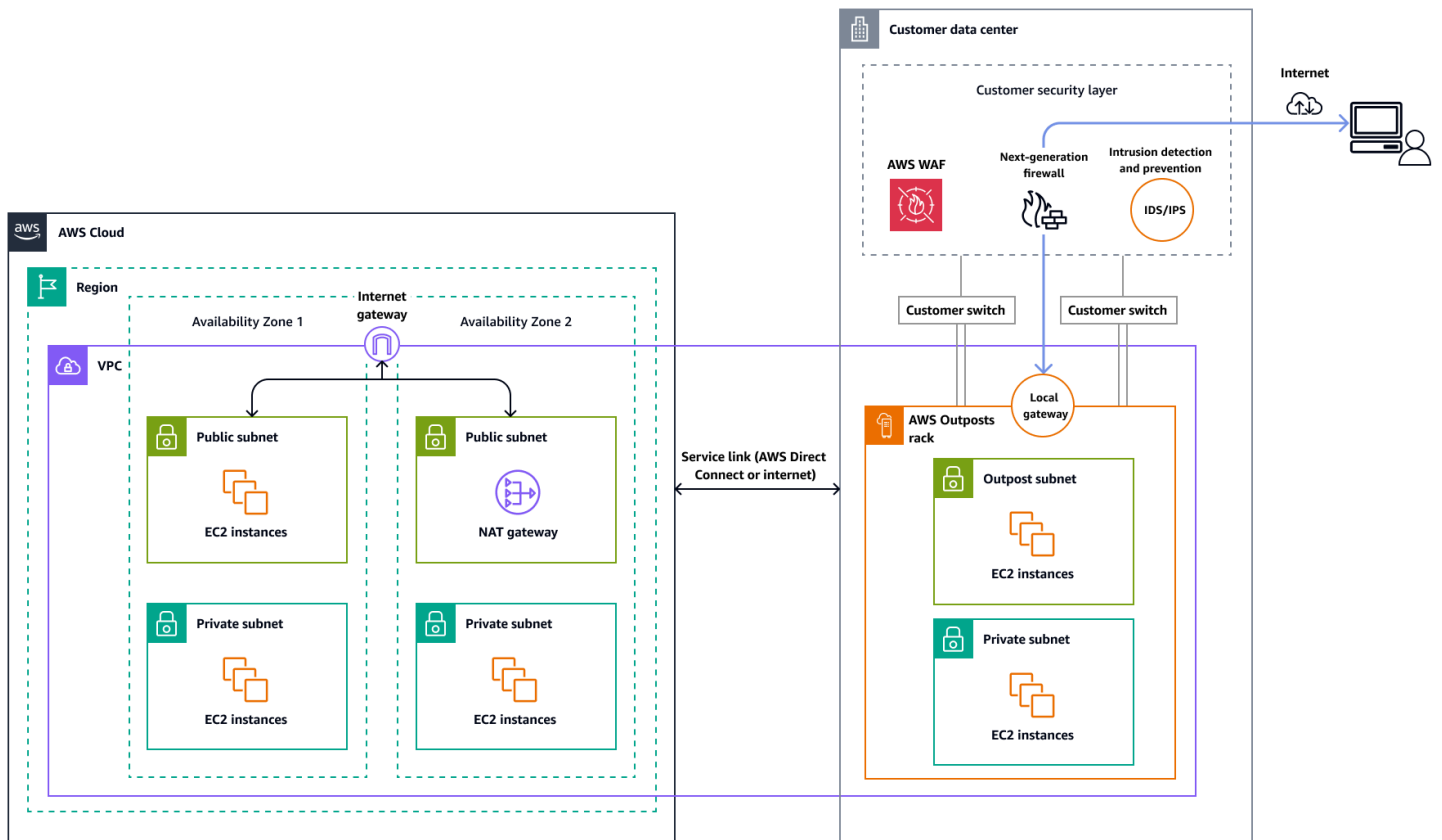
다음 다이어그램은 AWS Outposts 인스턴스의 워크로드와 상위를 통과하는 인터넷 간의 트래픽을 보여줍니다 AWS 리전.



로컬 데이터 센터의 네트워크를 통한 인터넷 액세스

이 옵션에서는 Outpost의 워크로드가 로컬 데이터 센터를 통해 인터넷에 액세스합니다. 인터넷에 액세스하는 워크로드 트래픽은 로컬 인터넷 접속 지점을 통과하여 로컬로 송신합니다. 이 경우 로컬 데이터 센터의 네트워크 보안 인프라가 워크로드 트래픽을 보호할 AWS Outposts 책임이 있습니다.

다음 이미지는 AWS Outposts 서브넷의 워크로드와 데이터 센터를 통과하는 인터넷 간의 트래픽을 보여줍니다.



인프라 거버넌스

워크로드가 AWS 리전, 로컬 영역 또는 Outpost에 배포되었는지 여부에 관계없이 인프라 거버넌스 AWS Control Tower 에를 사용할 수 있습니다.는 규범적 모범 사례를 따라 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 AWS Control Tower 제공합니다.는 AWS Organizations AWS Service Catalog 및 IAM Identity Center([모든 통합 서비스](#) 참조)를 AWS 서비스포함한 여러 다른의 기능을 AWS Control Tower 조정하여 1시간 이내에 랜딩 존을 구축합니다. 리소스는 사용자를 대신하여 설정 및 관리됩니다.

AWS Control Tower 는 리전, 로컬 영역(저지연 확장) 및 Outpost(온프레미스 인프라)를 포함한 모든 AWS 환경에서 통합 거버넌스를 제공합니다. 이를 통해 전체 하이브리드 클라우드 아키텍처에서 일관된 보안 및 규정 준수를 보장할 수 있습니다. 자세한 내용은 [AWS Control Tower 설명서](#)를 참조하세요.

정부 AWS Control Tower 및 금융 서비스 기관(FSIs. 옛지에서 데이터 레지던시를 위한 가드레일을 배포하는 방법을 이해하려면 다음을 참조하세요.

- [랜딩 존 제어를 AWS 로컬 영역 사용하여에서 데이터 레지던시를 관리하는 모범 사례](#)(AWS 블로그 게시물)
- [AWS Outposts 랙 및 랜딩 존 가드레일을 사용한 데이터 레지던시 설계](#)(AWS 블로그 게시물)

- [하이브리드 클라우드 서비스 렌즈를 사용한 데이터 레지던시](#)(AWS Well-Architected Framework 설명서)

Outposts 리소스 공유

Outpost는 데이터 센터 또는 코로케이션 공간에 있는 유한한 인프라므로 중앙 집중식 거버넌스를 위해서는 AWS Outposts 공유되는 계정을 중앙에서 제어 AWS Outposts해야 합니다.

Outpost 공유를 사용하면 Outpost 소유자는 Outpost 사이트 및 서브넷을 포함한 Outpost 및 Outpost 리소스를 동일한 조직에 AWS 계정 있는 다른와 공유할 수 있습니다 AWS Organizations. Outpost 소유자는 중앙 위치에서 Outpost 리소스를 생성 및 관리하고 AWS 조직 AWS 계정 내 여러에서 리소스를 공유할 수 있습니다. 이를 통해 다른 소비자가 Outpost 사이트를 사용하고, VPC를 구성하고, 공유 Outpost에서 인스턴스를 시작 및 실행할 수 있습니다.

에서 공유 가능한 리소스는 다음과 AWS Outposts 같습니다.

- 할당된 전용 호스트
- 용량 예약
- 고객 소유 IP(CoIP) 주소 풀
- 로컬 게이트웨이 라우팅 테이블
- Outpost
- Outposts에서의 Amazon S3
- Sites
- 서브넷

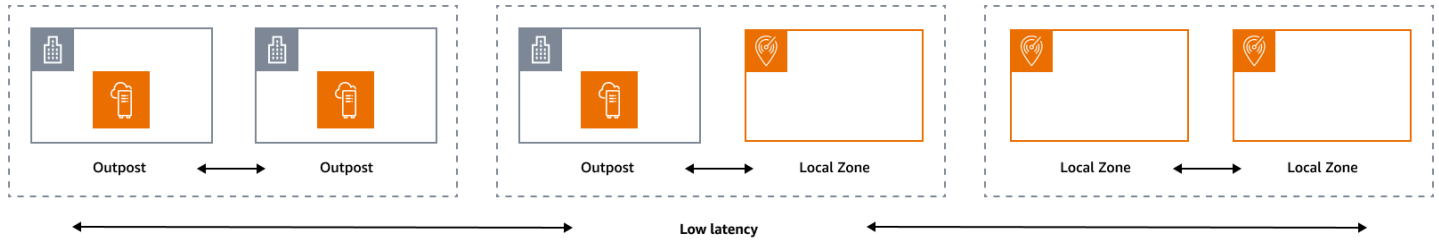
다중 계정 환경에서 Outpost 리소스를 공유하는 모범 사례를 따르려면 다음 AWS 블로그 게시물을 참조하세요.

- [AWS Outposts 다중 계정 AWS 환경에서 공유: 1부](#)
- [AWS Outposts 다중 계정 AWS 환경에서 공유: 2부](#)

엣지의 복원력

신뢰성 원칙은 워크로드가 의도한 기능을 예상대로 올바르게 일관되게 수행할 수 있는 능력을 포함합니다. 여기에는 수명 주기 동안 워크로드를 운영하고 테스트하는 기능이 포함됩니다. 이러한 의미에서 엣지에서 복원력이 뛰어난 아키텍처를 설계할 때는 먼저 해당 아키텍처를 배포하는 데 사용할 인프라

를 고려해야 합니다. 다음 다이어그램과 같이 AWS 로컬 영역 Outpost에서 AWS Outposts Outpost로, Outpost에서 Local Zone으로, Local Zone에서 Local Zone으로 3가지 조합을 사용하여 구현할 수 있습니다. AWS 엣지 서비스를 기존 온프레미스 인프라 또는와 결합하는 등 복원력이 뛰어난 아키텍처에 대한 다른 가능성이 있지만 AWS 리전,이 가이드는 하이브리드 클라우드 서비스 설계에 적용되는 이러한 세 가지 조합에 중점을 둡니다.



인프라 고려 사항

에서 서비스 설계의 핵심 원칙 AWS중 하나는 기본 물리적 인프라에서 단일 장애 지점을 방지하는 것입니다. 이 원칙 AWS 때문에 소프트웨어와 시스템은 여러 가용 영역을 사용하며 단일 영역의 장애에 대해 복원력이 있습니다. 엣지에서는 로컬 영역 및 Outpost를 기반으로 하는 인프라를 AWS 제공합니다. 따라서 인프라 설계의 복원력을 보장하는 중요한 요소는 애플리케이션의 리소스가 배포되는 위치를 정의하는 것입니다.

Local Zones

로컬 영역은 서브넷 및 EC2 인스턴스와 같은 영역 AWS 리소스의 배치 위치로 선택할 수 AWS 리전있으므로 해당 영역 내의 가용 영역과 유사하게 작동합니다. 그러나 현재는 AWS 리전 인구 AWS 리전, 산업 및 IT 센터가 거의 없는데 위치하지 않습니다. 그럼에도 불구하고 로컬 영역의 로컬 워크로드와에서 실행 중인 워크로드 간에 높은 대역폭의 보안 연결을 유지합니다 AWS 리전. 따라서 지연 시간이 짧은 요구 사항을 위해 로컬 영역을 사용하여 사용자에게 더 가깝게 워크로드를 배포해야 합니다.

Outpost

AWS Outposts 는 AWS 인프라, AWS 서비스, APIs 및 도구를 데이터 센터로 확장하는 완전관리형 서비스입니다. 에서 사용되는 것과 동일한 하드웨어 인프라 AWS 클라우드 가 데이터 센터에 설치됩니다. 그런 다음 Outpost가 가장 가까운 연결됩니다 AWS 리전. Outposts를 사용하여 지연 시간이 짧거나 로컬 데이터 처리 요구 사항이 있는 워크로드를 지원할 수 있습니다.

상위 가용 영역

각 로컬 영역 또는 Outpost에는 상위 리전(홈 리전이라고도 함)이 있습니다. 상위 리전은 AWS 엣지 인프라(Outpost 또는 로컬 영역)의 컨트롤 플레인인 고정되는 곳입니다. 로컬 영역의 경우 상위 리전은

로컬 영역의 기본 아키텍처 구성 요소이며 고객이 수정할 수 없습니다. 온프레미스 환경 AWS 클라우드 으로 AWS Outposts 확장되므로 주문 프로세스 중에 특정 리전 및 가용 영역을 선택해야 합니다. 이 선택은 Outposts 배포의 컨트롤 플레인을 선택한 AWS 인프라에 고정합니다.

엣지에서 고가용성 아키텍처를 개발하는 경우 VPC를 확장할 수 있도록 Outpost 또는 로컬 영역과 같은 이러한 인프라의 상위 리전이 동일해야 합니다. 이 확장 VPC는 이러한 고가용성 아키텍처를 생성하기 위한 기반입니다. 복원력이 뛰어난 아키텍처를 정의할 때는 상위 리전과 서비스가 고정될(또는 고정될) 리전의 가용 영역을 검증해야 합니다. 다음 다이어그램에 설명된 대로 두 Outpost 사이에 고가용성 솔루션을 배포하려면 두 개의 서로 다른 가용 영역을 선택하여 Outpost를 고정해야 합니다. 이를 통해 컨트롤 플레인 관점에서 다중 AZ 아키텍처를 사용할 수 있습니다. 하나 이상의 로컬 영역을 포함하는 고가용성 솔루션을 배포하려면 먼저 인프라가 고정되는 상위 가용 영역을 검증해야 합니다. 이를 위해 다음 명령을 사용합니다 AWS CLI .

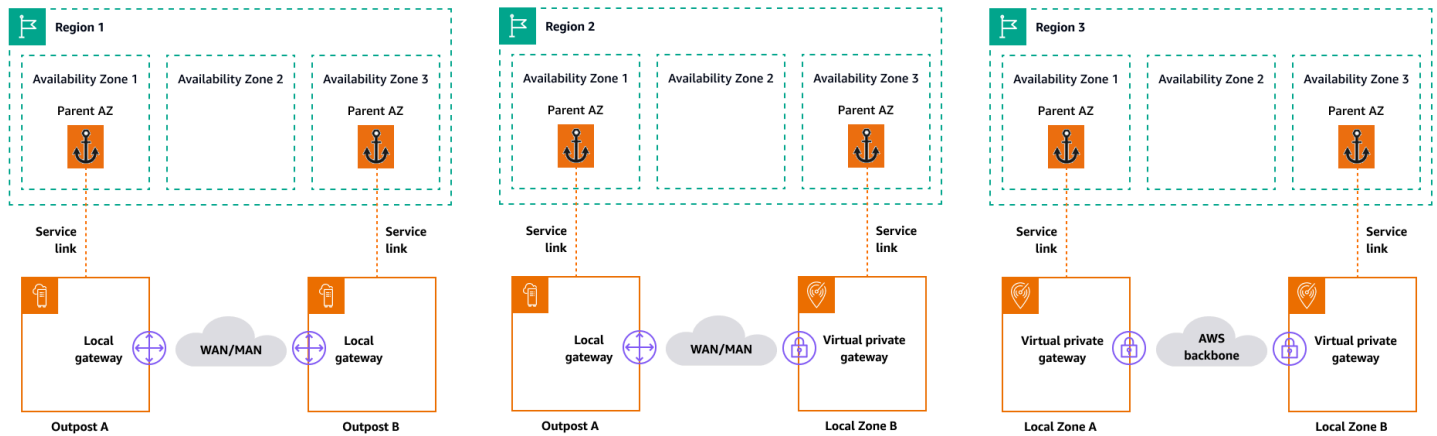
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

이전 명령의 출력:

```
{
  "AvailabilityZones": [
    {
      "State": "available",
      "OptInStatus": "opted-in",
      "Messages": [],
      "RegionName": "us-east-1",
      "ZoneName": "us-east-1-mia-1a",
      "ZoneId": "use1-mia1-az1",
      "GroupName": "us-east-1-mia-1",
      "NetworkBorderGroup": "us-east-1-mia-1",
      "ZoneType": "local-zone",
      "ParentZoneName": "us-east-1d",
      "ParentZoneId": "use1-az2"
    }
  ]
}
```

이 예제에서는 마이애미 로컬 영역(us-east-1d-mia-1a1)이 us-east-1d-az2 가용 영역에 고정되어 있습니다. 따라서 엣지에서 복원력이 뛰어난 아키텍처를 생성해야 하는 경우 보조 인프라 (Outpost 또는 로컬 영역)가 이외의 가용 영역에 고정되어 있는지 확인해야 합니다 us-east-1d-az2. 예를 들어 us-east-1d-az1는 유효합니다.

다음 다이어그램은 고가용성 엣지 인프라의 예를 제공합니다.



네트워킹 고려 사항

이 섹션에서는 엣지에서의 네트워킹, 주로 엣지 인프라에 액세스하기 위한 연결에 대한 초기 고려 사항을 설명합니다. 서비스 링크에 복원력이 뛰어난 네트워크를 제공하는 유효한 아키텍처를 검토합니다.

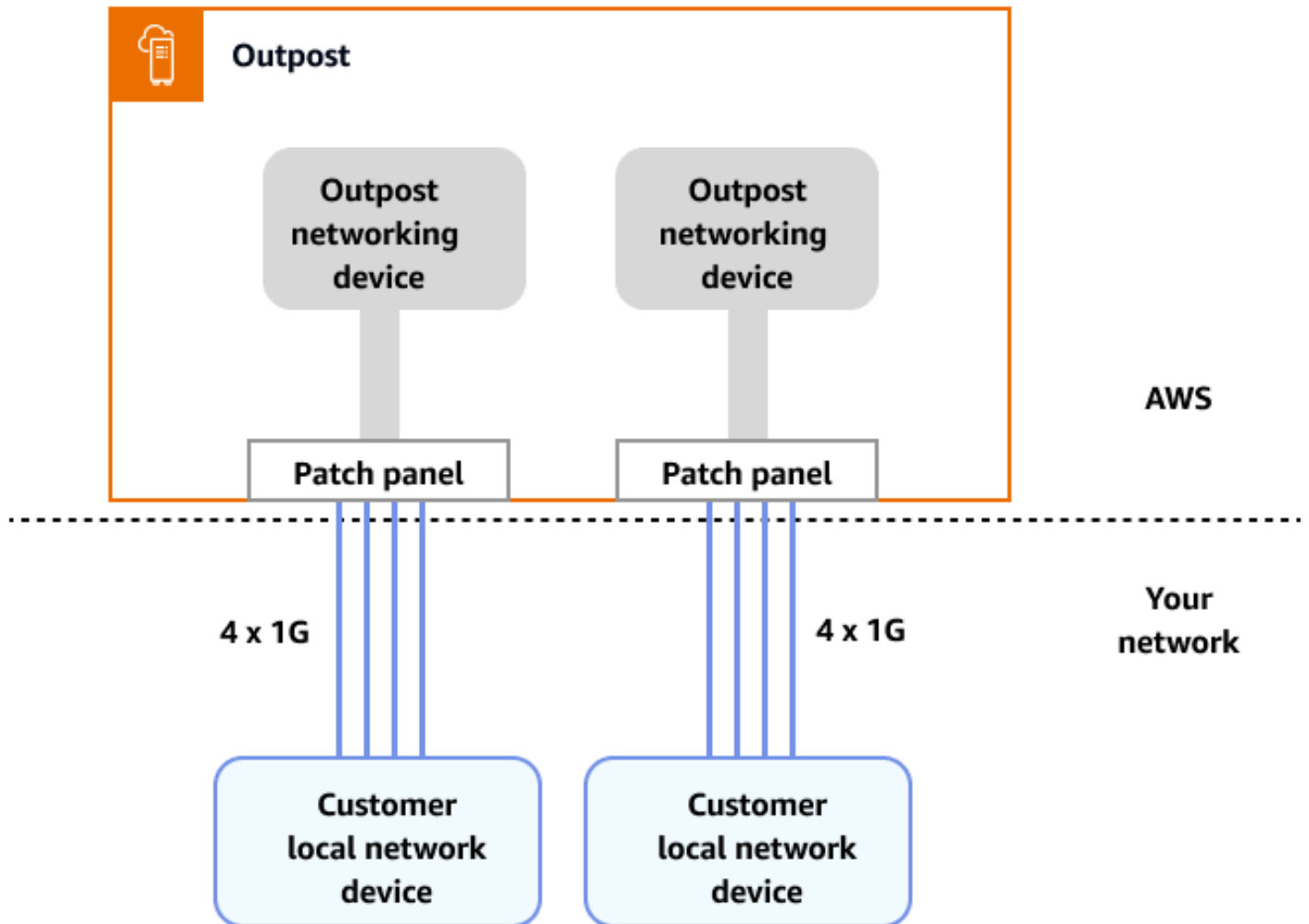
로컬 영역에 대한 복원력 네트워킹

로컬 영역은 Amazon S3 및 Amazon RDS와 같은 모든 리전 서비스를 원활하게 사용할 수 있는 여러 개의 안전한 고속 중복 링크를 통해 상위 리전에 연결됩니다. 온프레미스 환경 또는 사용자에서 로컬 영역으로의 연결을 제공할 책임은 사용자에게 있습니다. 선택한 연결 아키텍처(예: VPN 또는 Direct Connect)에 관계없이 기본 링크에서 장애가 발생할 경우 애플리케이션 성능에 영향을 주지 않도록 네트워크 링크를 통해 달성해야 하는 지연 시간은 동일해야 합니다. Direct Connect를 사용하는 경우 해당 복원력 아키텍처는 [Direct Connect 복원력 권장 사항](#)에 설명된 AWS 리전대로 액세스하기 위한 아키텍처와 동일합니다. 그러나 대부분의 경우 국제 로컬 영역에 적용되는 시나리오가 있습니다. 로컬 영역이 활성화된 국가에서는 단일 Direct Connect PoP만 있으면 Direct Connect 복원력에 권장되는 아키텍처를 생성할 수 없습니다. 단일 Direct Connect 위치에만 액세스할 수 있거나 단일 연결 이상의 복원력이 필요한 경우 AWS 블로그 게시물 [온프레미스에서 로 고가용성 연결 활성화에 설명된 Direct Connect](#)대로 Amazon EC2에서 VPN 어플라이언스를 생성할 수 있습니다. [AWS 로컬 영역](#)

Outposts의 복원력 네트워킹

로컬 영역과 달리 Outposts에는 로컬 네트워크에서 Outposts에 배포된 워크로드에 액세스하기 위한 중복 연결이 있습니다. 이 중복성은 두 개의 Outpost 네트워크 디바이스(ONDs). 각 OND에는 로컬 네트워크에 대한 1Gbps, 10Gbps, 40Gbps 또는 100Gbps의 광섬유 연결이 두 개 이상 필요합니다. 이러한 연결은 더 많은 링크를 확장 가능하게 추가할 수 있도록 링크 집계 그룹(LAG)으로 구성해야 합니다.

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

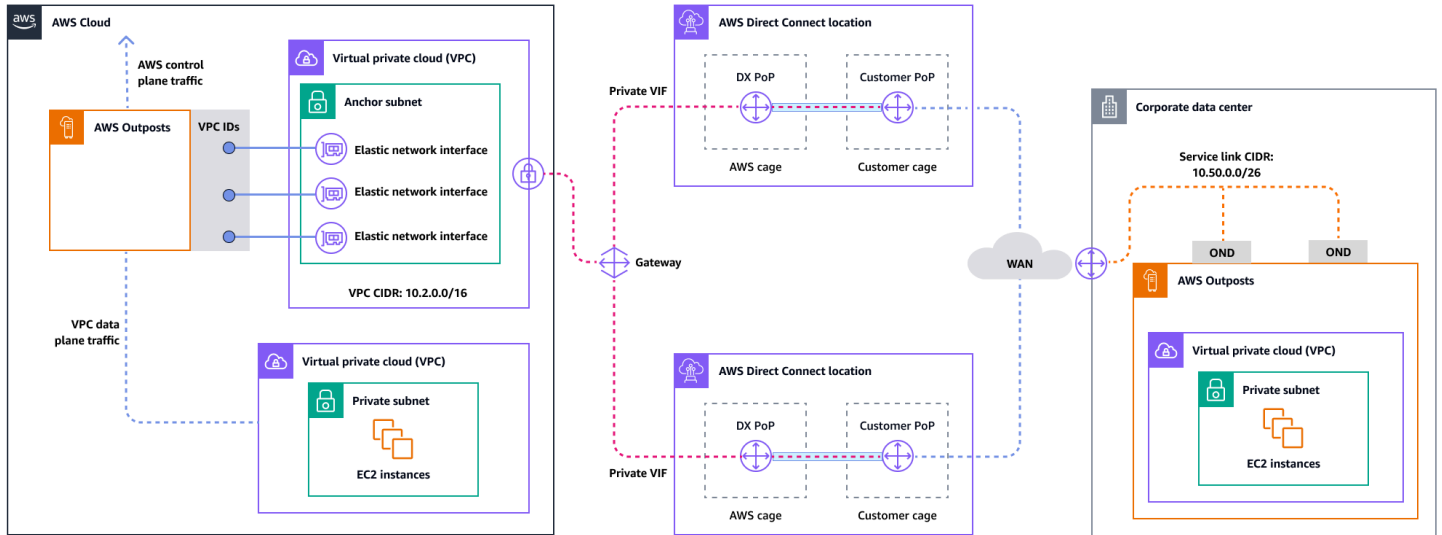


이 연결에 대한 자세한 내용은 AWS Outposts 설명서의 [Outpost 랙에 대한 로컬 네트워크 연결을 참조하세요](#).

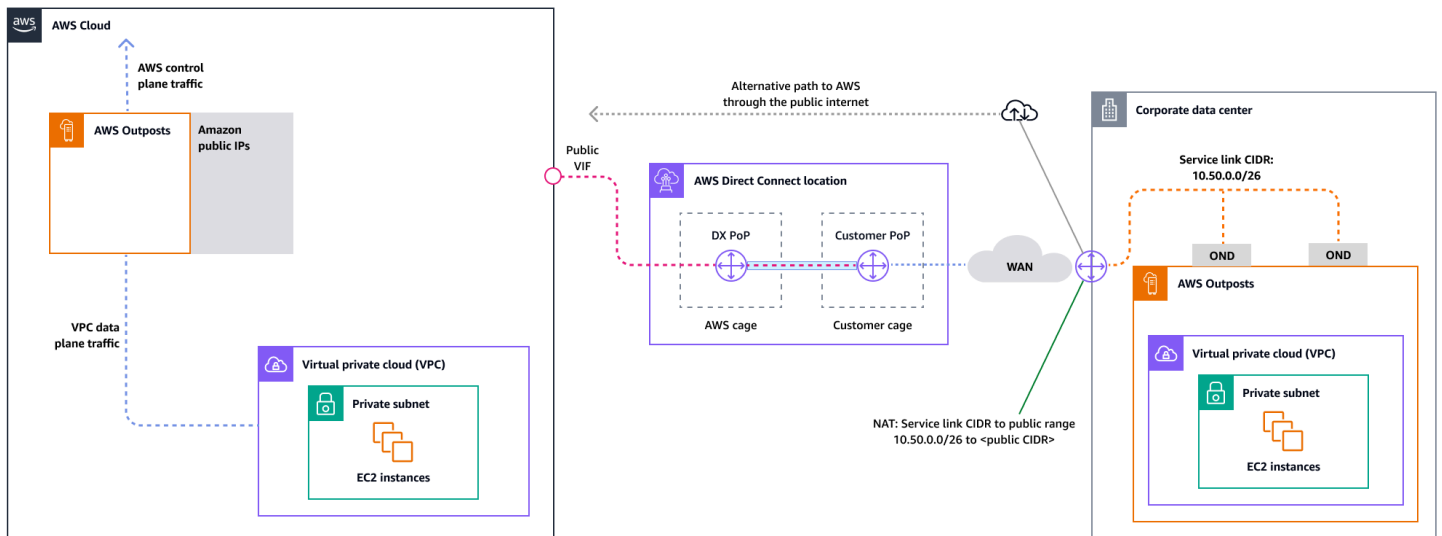
최적의 경험과 복원력을 위해는에 대한 서비스 링크 연결에 최소 500Mbps(1Gbps가 더 좋음)의 중복 연결을 사용할 것을 AWS권장합니다 AWS 리전. 서비스 링크에 Direct Connect 또는 인터넷 연결을 사

용할 수 있습니다. 이 최소값을 사용하면 EC2 인스턴스를 시작하고, EBS 볼륨을 연결하고, Amazon EKS AWS 서비스, Amazon EMR 및 CloudWatch 지표와 같은에 액세스할 수 있습니다.

다음 다이어그램은 고가용성 프라이빗 연결을 위한 이 아키텍처를 보여줍니다.



다음 다이어그램은 고가용성 퍼블릭 연결을 위한 이 아키텍처를 보여줍니다.



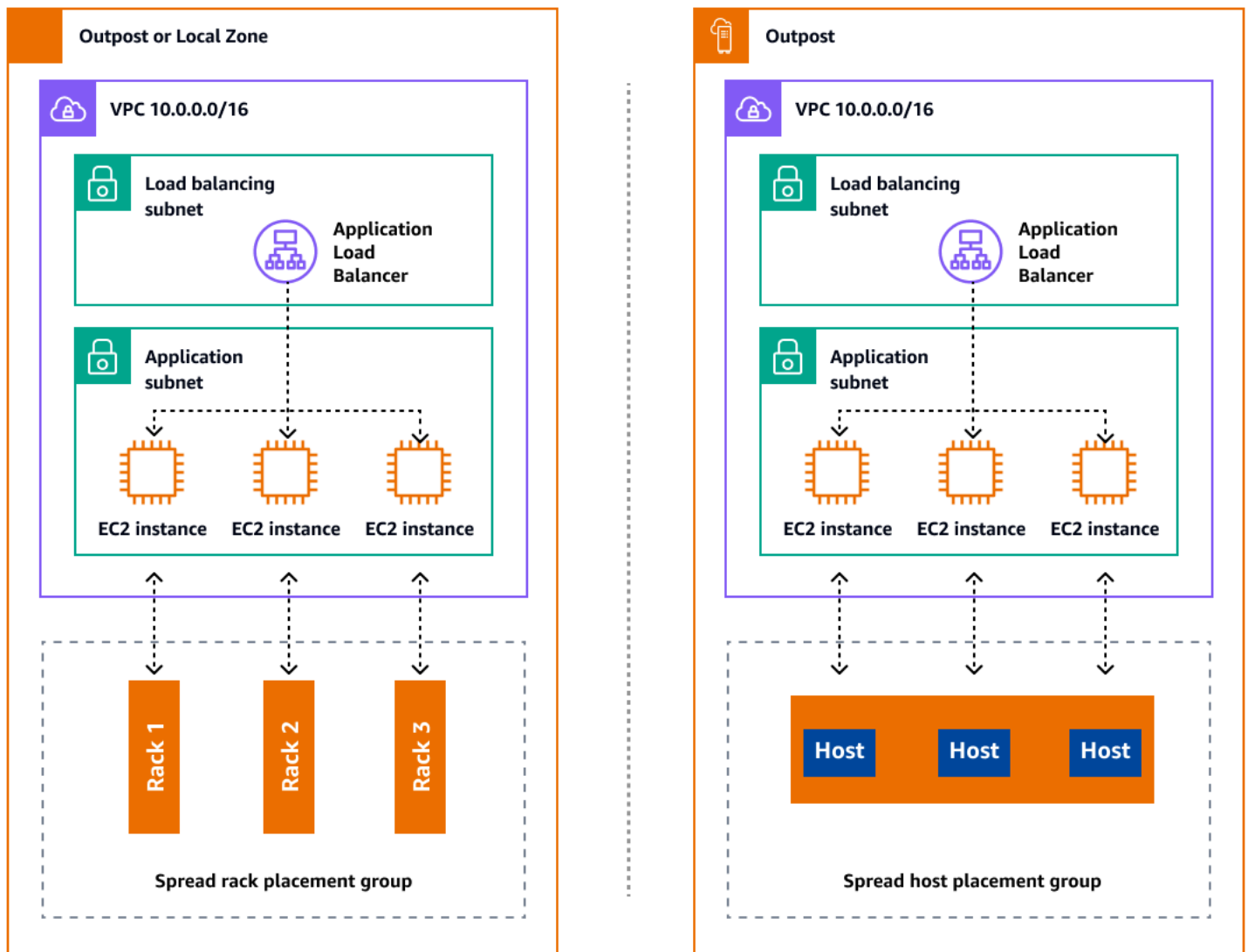
ACE 랙을 사용하여 Outpost 랙 배포 확장

집계, 코어, 엣지(ACE) 랙은 AWS Outposts 다중 랙 배포의 중요한 집계 지점 역할을 하며, 랙 3개를 초과하는 설치 또는 향후 확장 계획에 주로 권장됩니다. 각 ACE 랙에는 10Gbps, 40Gbps 및 100Gbps 연결을 지원하는 4개의 라우터가 있습니다(100Gbps가 최적임). 각 랙은 최대 4개의 업스트림 고객 디바이스에 연결하여 중복성을 극대화할 수 있습니다. ACE 랙은 최대 10kVA의 전력을 소비하고 최대 705 파운드의 무게를 갖습니다. 주요 이점으로는 물리적 네트워킹 요구 사항 감소, 광섬유 케이블 업링크

감소, VLAN 가상 인터페이스 감소 등이 있습니다.는 VPN 터널을 통해 원격 측정 데이터를 통해 이러한 랙을 AWS 모니터링하고 설치 중에 고객과 긴밀하게 협력하여 적절한 전력 가용성, 네트워크 구성 및 최적의 배치를 보장합니다. ACE 랙 아키텍처는 배포 규모에 따라 가치를 높이고 연결을 효과적으로 간소화하는 동시에 대규모 설치에서 복잡성과 물리적 포트 요구 사항을 줄입니다. 자세한 내용은 AWS 블로그 게시물 [Scaling AWS Outposts rack deployments with ACE Rack](#)을 참조하세요.

Outpost 및 로컬 영역에 인스턴스 배포

Outpost 및 로컬 영역에는 컴퓨팅 서버 수가 유한합니다. 애플리케이션이 여러 관련 인스턴스를 배포하는 경우 이러한 인스턴스는 다르게 구성되지 않는 한 동일한 서버 또는 동일한 랙의 서버에 배포될 수 있습니다. 기본 옵션 외에도 서버 간에 인스턴스를 분산 하여 동일한 인프라에서 관련 인스턴스를 실행할 위험을 완화할 수 있습니다. 파티션 배치 그룹을 사용하여 여러 랙에 인스턴스를 배포할 수도 있습니다. 이를 스프레드 랙 배포 모델이라고 합니다. 자동 배포를 사용하여 그룹의 파티션 간에 인스턴스를 분산하거나 선택한 대상 파티션에 인스턴스를 배포합니다. 대상 파티션에 인스턴스를 배포하면 선택한 리소스를 동일한 랙에 배포하는 동시에 다른 리소스를 랙에 배포할 수 있습니다. 또한 Outposts는 호스트 수준에서 워크로드를 분산할 수 있는 분산 호스트라는 또 다른 옵션을 제공합니다. 다음 다이어그램은 스프레드 랙 및 스프레드 호스트 배포 옵션을 보여줍니다.



의 Amazon RDS 다중 AZ AWS Outposts

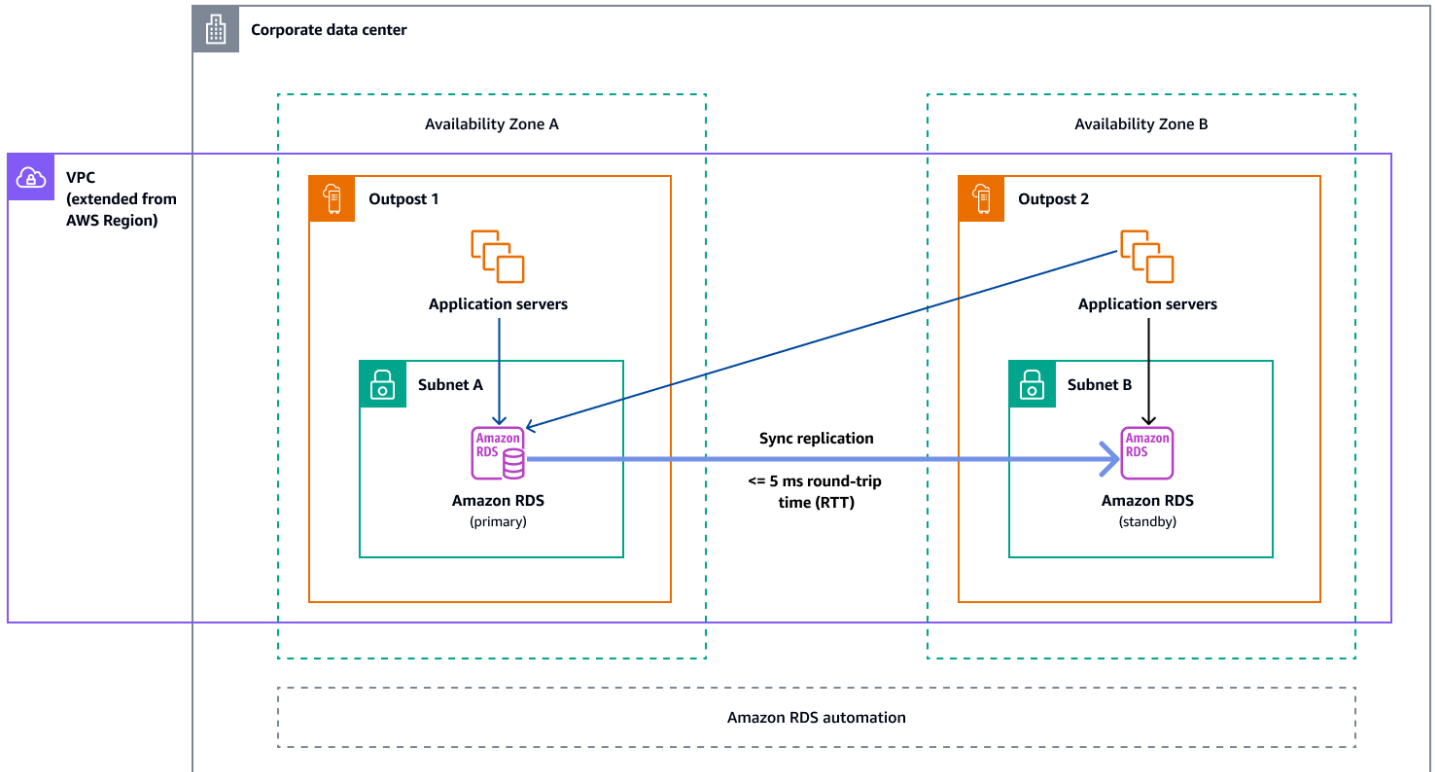
Outposts에서 다중 AZ 인스턴스 배포를 사용하는 경우 Amazon RDS는 두 Outposts에 두 개의 데이터베이스 인스턴스를 생성합니다. 각 Outpost는 자체 물리적 인프라에서 실행되며고가용성을 위해 리전의 여러 가용 영역에 연결됩니다. 고객 관리형 로컬 연결을 통해 두 개의 Outpost가 연결되면 Amazon RDS는 기본 데이터베이스 인스턴스와 대기 데이터베이스 인스턴스 간의 동기식 복제를 관리합니다. 소프트웨어 또는 인프라에 장애가 발생하는 경우 Amazon RDS는 자동으로 대기 인스턴스를 기본 역할로 승격하고 DNS 레코드를 업데이트하여 새 기본 인스턴스를 가리킵니다. 다중 AZ 배포의 경우 Amazon RDS는 하나의 Outpost에 기본 DB 인스턴스를 생성하고 다른 Outpost에 있는 대기 DB 인스턴스에 데이터를 동기식으로 복제합니다. Outposts의 다중 AZ 배포는 다중 AZ 배포 AWS 리전과 같이 작동하며 다음과 같은 차이점이 있습니다.

- 두 개 이상의 Outposts 사이에 로컬 연결이 필요합니다.

- 여기에는 고객 소유 IP(CoIP) 주소 풀이 필요합니다. 자세한 내용은 [Amazon RDS 설명서의 Amazon RDS에 대한 고객 소유 IP 주소를 AWS Outposts](#) 참조하세요.
- 로컬 네트워크에서 복제가 실행됩니다.

Amazon RDS on Outposts에서 지원되는 모든 버전의 MySQL 및 PostgreSQL에 다중 AZ 배포를 사용할 수 있습니다. 다중 AZ 배포에는 로컬 백업이 지원되지 않습니다.

다음 다이어그램은 Amazon RDS on Outposts 다중 AZ 구성의 아키텍처를 보여줍니다.



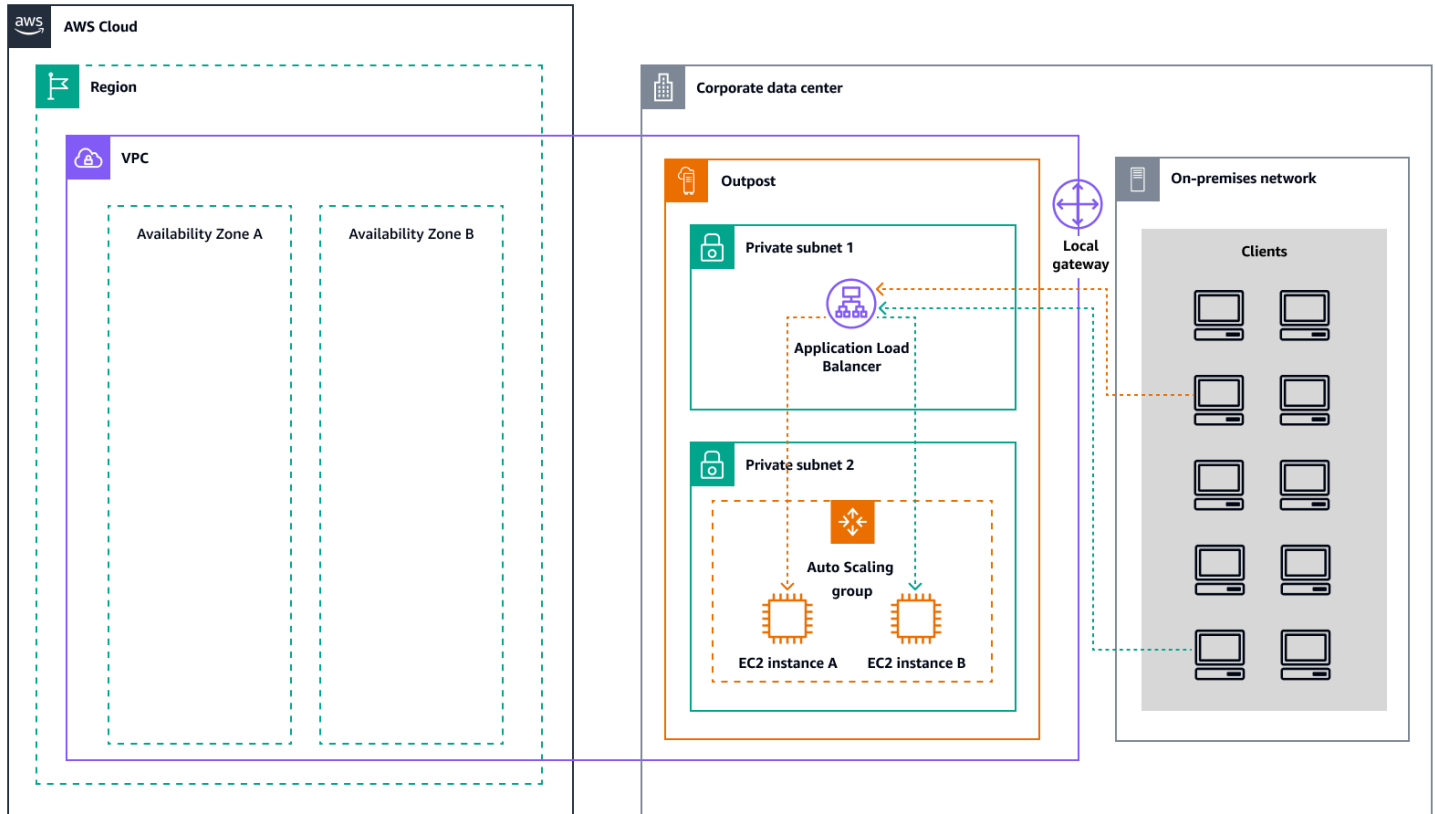
장애 조치 메커니즘

로드 밸런싱 및 자동 조정

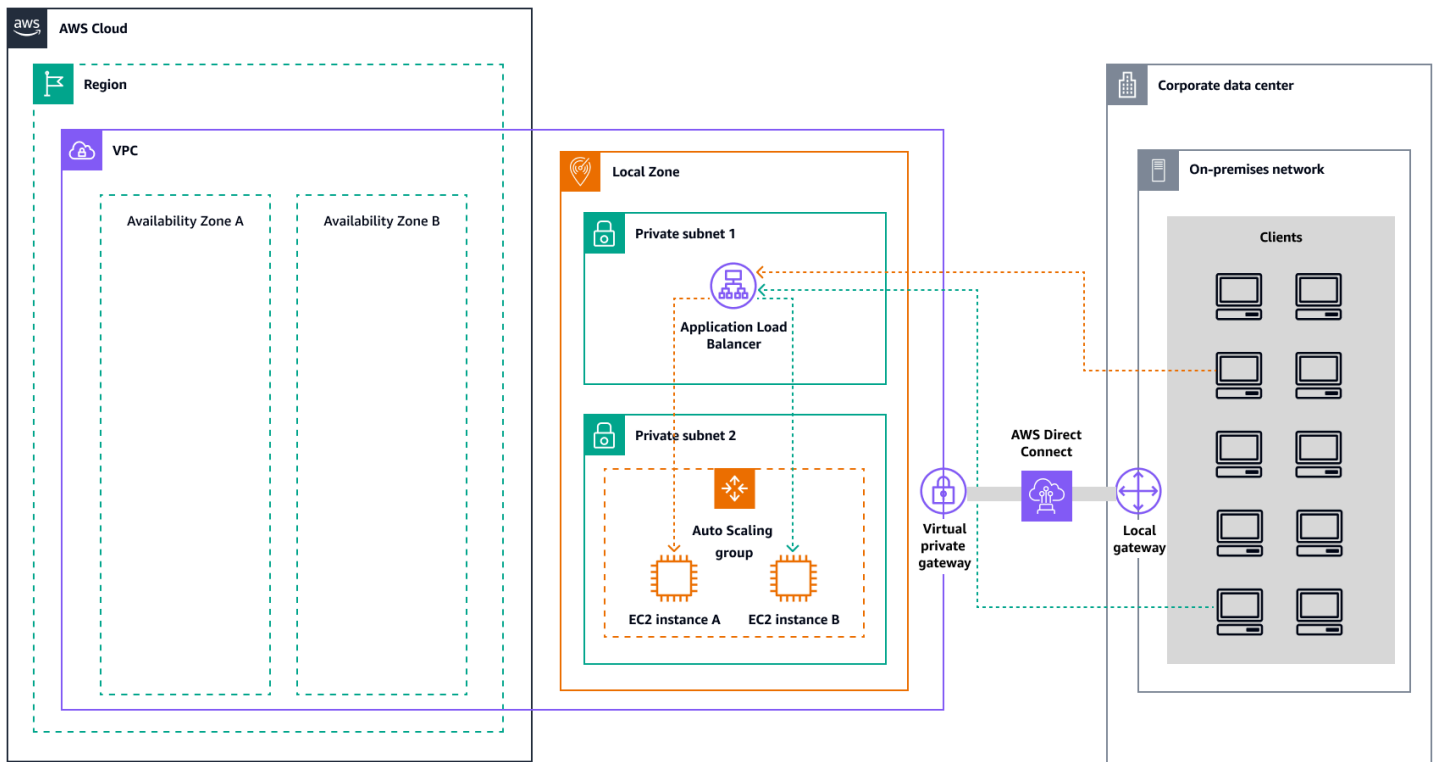
Elastic Load Balancing(ELB)은 실행 중인 모든 EC2 인스턴스에 수신 애플리케이션 트래픽을 자동으로 분산합니다. ELB는 단일 인스턴스가 압도되지 않도록 트래픽을 최적으로 라우팅하여 수신 요청을 관리하는 데 도움이 됩니다. Amazon EC2 Auto Scaling 그룹에서 ELB를 사용하려면 Auto Scaling 그룹에 로드 밸런서를 연결합니다. 이렇게 하면 그룹으로 들어오는 모든 웹 트래픽에 대한 단일 연락 지점 역할을 하는 로드 밸런서에 그룹이 등록됩니다. Auto Scaling 그룹에서 ELB를 사용하는 경우 로드 밸런서에 개별 EC2 인스턴스를 등록할 필요가 없습니다. Auto Scaling 그룹에서 시작되는 인스턴스가 로드 밸런서에 자동으로 등록됩니다. 마찬가지로 Auto Scaling 그룹에 의해 종료된 인스턴스는 로드 밸

런서에서 자동으로 등록 취소됩니다. Auto Scaling 그룹에 로드 밸런서를 연결한 후 ELB 지표(예: 대상 당 Application Load Balancer 요청 수)를 사용하여 수요 변동에 따라 그룹의 인스턴스 수를 조정하도록 그룹을 구성할 수 있습니다. 선택적으로 Amazon EC2 Auto Scaling이 이러한 상태 확인을 기반으로 비정상 인스턴스를 식별하고 교체할 수 있도록 Auto Scaling 그룹에 ELB 상태 확인을 추가할 수 있습니다. 대상 그룹의 정상 호스트 수가 허용보다 낮은 경우 이를 알리는 Amazon CloudWatch 경보를 생성할 수도 있습니다.

다음 다이어그램은 Application Load Balancer가에서 Amazon EC2의 워크로드를 관리하는 방법을 보여줍니다 AWS Outposts.



다음 다이어그램은 로컬 영역의 Amazon EC2에 대한 유사한 아키텍처를 보여줍니다.



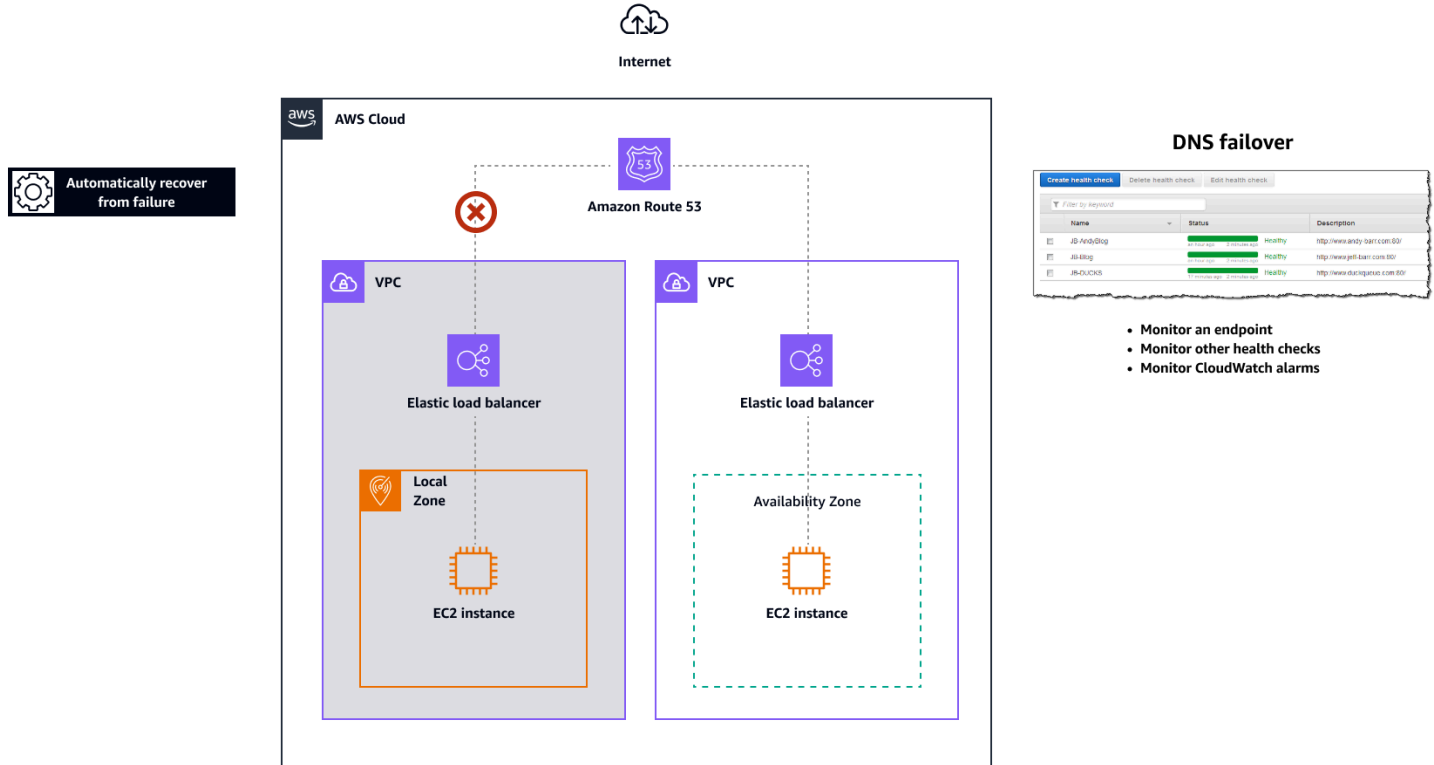
Note

Application Load Balancer는 AWS Outposts 및 로컬 영역 모두에서 사용할 수 있습니다. 그러나에서 Application Load Balancer를 사용하려면 로드 밸런서에 필요한 확장성을 제공하기 위해 Amazon EC2 용량의 크기를 조정 AWS Outposts해야 합니다. 의 로드 밸런서 크기 조정 에 대한 자세한 내용은 AWS 블로그 게시물 [Configure an Application Load Balancer on AWS Outposts](#)을 AWS Outposts참조하세요.

DNS 장애 조치를 위한 Amazon Route 53

여러 HTTP 또는 메일 서버와 같이 동일한 기능을 수행하는 리소스가 두 개 이상 있는 경우 [Amazon Route 53](#)을 구성하여 리소스의 상태를 확인하고 정상 리소스만 사용하여 DNS 쿼리에 응답할 수 있습니다. 예를 들어 웹 사이트 example.com가 두 서버에서 호스팅된다고 가정해 보겠습니다. 한 서버는 로컬 영역에 있고 다른 서버는 Outpost에 있습니다. 해당 서버의 상태를 확인하고 현재 정상 상태인 서버만 사용하여에 대한 DNS 쿼리example.com에 응답하도록 Route 53를 구성할 수 있습니다. 별칭 레코드를 사용하여 ELB 로드 밸런서와 같은 선택한 AWS 리소스로 트래픽을 라우팅하는 경우 리소스의 상태를 평가하고 정상인 리소스로만 트래픽을 라우팅하도록 Route 53을 구성할 수 있습니다. 리소스의 상태를 평가하도록 별칭 레코드를 구성할 때 해당 리소스에 대한 상태 확인을 생성할 필요가 없습니다.

다음 다이어그램은 Route 53 장애 조치 메커니즘을 보여줍니다.



참고

- 프라이빗 호스팅 영역에서 장애 조치 레코드를 생성하는 경우 CloudWatch 지표를 생성하고 경보를 지표와 연결한 다음 경보의 데이터 스트림을 기반으로 하는 상태 확인을 생성할 수 있습니다.
- Application Load Balancer를 AWS Outposts 사용하여 애플리케이션에 공개적으로 액세스할 수 있도록 하려면 퍼블릭 IPs에서 로드 밸런서의 정규화된 도메인 이름(FQDN)으로 대상 네트워크 주소 변환(DNAT)을 활성화하는 네트워킹 구성을 설정하고 노출된 퍼블릭 IP를 가리키는 상태 확인이 포함된 Route 53 장애 조치 규칙을 생성합니다. 이 조합은 Outposts 호스팅 애플리케이션에 대한 안정적인 퍼블릭 액세스를 보장합니다.

Amazon Route 53 Resolver 의 AWS Outposts

[Amazon Route 53 Resolver](#)는 Outpost 랙에서 사용할 수 있습니다. Outposts에서 직접 로컬 DNS 확인을 온프레미스 서비스 및 애플리케이션에 제공합니다. 로컬 Route 53 Resolver 엔드포인트를 사용하면 Outposts와 온프레미스 DNS 서버 간의 DNS 확인도 가능합니다. Outposts의 Route 53 Resolver는 온프레미스 애플리케이션의 가용성과 성능을 개선하는 데 도움이 됩니다.

Outposts의 일반적인 사용 사례 중 하나는 공장 장비, 고주파 거래 애플리케이션 및 의료 진단 시스템과 같은 온프레미스 시스템에 대한 지연 시간이 짧은 액세스가 필요한 애플리케이션을 배포하는 것입니다.

Outposts에서 로컬 Route 53 Resolver를 사용하도록 옵트인하면 상위에 대한 연결이 AWS 리전 끊어지더라도 애플리케이션 및 서비스는 로컬 DNS 확인의 이점을 계속 누릴 수 있습니다. 또한 로컬 해석기는 쿼리 결과가 Outpost에서 로컬로 캐싱되고 제공되므로 DNS 확인 지연 시간을 줄이는 데 도움이 되므로 상위 항목으로의 불필요한 왕복이 제거됩니다 AWS 리전. 프라이빗 DNS를 사용하는 Outposts VPCs의 애플리케이션에 대한 모든 DNS 확인은 로컬에서 제공됩니다. <https://docs.aws.amazon.com/managedservices/latest/userguide/set-dns.html>

이 시작은 로컬 해석기를 활성화하는 것 외에도 로컬 해석기 엔드포인트도 활성화합니다. Route 53 Resolver 아웃바운드 엔드포인트를 사용하면 Route 53 Resolver가 온프레미스 네트워크와 같이 관리하는 DNS 해석기에 DNS 쿼리를 전달할 수 있습니다. 반대로 Route 53 Resolver 인바운드 엔드포인트는 VPC 외부에서 수신한 DNS 쿼리를 Outposts에서 실행 중인 Resolver로 전달합니다. 이를 통해 VPC 외부에서 프라이빗 Outposts VPC에 배포된 서비스에 대한 DNS 쿼리를 전송할 수 있습니다. 인바운드 및 아웃바운드 엔드포인트에 대한 자세한 내용은 Route 53 설명서의 [VPCs와 네트워크 간의 DNS 쿼리 해결을 참조하세요](#).

엣지에서의 용량 계획

용량 계획 단계에는 아키텍처를 배포하기 위한 vCPU, 메모리 및 스토리지 요구 사항을 수집하는 작업이 포함됩니다. [AWS Well-Architected Framework](#)의 비용 최적화 원칙에서 올바른 크기 조정은 계획부터 시작하는 지속적인 프로세스입니다. AWS 도구를 사용하여 내의 리소스 소비를 기반으로 최적화를 정의할 수 있습니다 AWS.

로컬 영역의 엣지 용량 계획은의와 동일합니다 AWS 리전. 일부 인스턴스 유형은의 유형과 다를 수 있으므로 각 로컬 영역에서 인스턴스를 사용할 수 있는지 확인해야 합니다 AWS 리전. Outposts의 경우 워크로드 요구 사항에 따라 용량을 계획해야 합니다. Outpost는 호스트당 고정된 수의 인스턴스로 슬롯화되며 필요에 따라 다시 슬롯화할 수 있습니다. 워크로드에 예비 용량이 필요한 경우 용량 요구 사항을 계획할 때 이를 고려하세요.

Outposts의 용량 계획

AWS Outposts 용량 계획에는 리전별 적정 크기 조정을 위한 특정 입력과 애플리케이션 가용성, 성능 및 성장에 영향을 미치는 엣지별 요소가 필요합니다. 자세한 지침은 고가용성 설계 및 아키텍처 고려 사항 백서의 AWS [용량 계획](#)을 참조하세요. AWS Outposts

로컬 영역에 대한 용량 계획

로컬 영역은 사용자와 AWS 리전 지리적으로 가까운 확장입니다. 로컬 영역에서 생성된 리소스는 지연 시간이 매우 짧은 통신을 로컬 사용자에게 제공할 수 있습니다. 에서 로컬 영역을 활성화하려면 AWS 설명서의 [시작하기 AWS 로컬 영역](#)를 AWS 계정검토하세요. 각 로컬 영역에는 EC2 인스턴스 패밀리에 사용할 수 있는 슬롯이 다릅니다. 사용하기 전에 [각 로컬 영역에서 사용 가능한 인스턴스](#)를 검증합니다. 사용 가능한 EC2 인스턴스를 확인하려면 다음 AWS CLI 명령을 실행합니다.

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

예상 결과:

```
{
  "InstanceTypeOfferings": [
    {
      "InstanceType": "m5.2xlarge",
      "LocationType": "availability-zone",
      "Location": "<local-zone-name>"
    },
    {
      "InstanceType": "t3.micro",
      "LocationType": "availability-zone",
      "Location": "local.zone-name"
    },
    ...
  ]
}
```

엣지 인프라 관리

AWS 는 AWS 인프라, 서비스, APIs 및 도구를 최종 사용자 및 데이터 센터에 더 가깝게 확장하는 완전 관리형 서비스를 제공합니다. Outposts 및 Local Zones에서 사용할 수 있는 서비스는에서 사용할 수 있는 서비스와 동일 AWS 리전하므로 동일한 AWS 콘솔 AWS CLI또는 AWS APIs. 지원되는 서비스는 [AWS Outposts 기능 비교](#) 표 및 [AWS 로컬 영역 기능](#)을 참조하세요.

엣지에서 서비스 배포

AWS 콘솔 AWS CLI, 또는 API를 AWS 리전 사용하여 로컬 영역 및 Outposts에서 사용할 수 있는 서비스를 구성하는 것과 동일한 방식으로 구성할 수 있습니다. AWS APIs 리전 배포와 엣지 배포의 주요 차이점은 리소스가 프로비저닝될 서브넷입니다. [엣지의 네트워킹](#) 섹션에서는 서브넷이 Outpost 및 로컬 영역에 배포되는 방법을 설명했습니다. 엣지 서브넷을 식별한 후 엣지 서브넷 ID를 파라미터로 사용하여 Outpost 또는 로컬 영역에 서비스를 배포합니다. 다음 섹션에서는 엣지 서비스 배포의 예를 제공합니다.

엣지의 Amazon EC2

다음 run-instances 예시에서는 현재 리전의 엣지 서브넷 m5.2xlarge로 유형의 단일 인스턴스를 시작합니다. Linux의 SSH 또는 Windows의 RDP(원격 데스크톱 프로토콜)를 사용하여 인스턴스에 연결할 계획이 없는 경우 키 페어는 선택 사항입니다.

```
aws ec2 run-instances \  
  --image-id ami-id \  
  --instance-type m5.2xlarge \  
  --subnet-id <subnet-edge-id> \  
  --key-name MyKeyPair
```

엣지의 Application Load Balancer

다음 create-load-balancer 예시에서는 내부 Application Load Balancer를 생성하고 지정된 서브넷에 대해 로컬 영역 또는 Outposts를 활성화합니다.

```
aws elbv2 create-load-balancer \  
  --name my-internal-load-balancer \  
  --scheme internal \  
  --subnets <subnet-edge-id>
```

인터넷 경계 Application Load Balancer를 Outpost의 서브넷에 배포하려면 다음 예제와 같이 --scheme 옵션에서 internet-facing 플래그를 설정하고 [CoIP 풀 ID](#)를 제공합니다.

```
aws elbv2 create-load-balancer \  
  --name my-internal-load-balancer \  
  --scheme internet-facing \  
  --customer-owned-ipv4-pool <coip-pool-id> \  
  --subnets <subnet-edge-id>
```

옛지에서 다른 서비스를 배포하는 방법에 대한 자세한 내용은 다음 링크를 참조하세요.

서비스	AWS Outposts	AWS 로컬 영역
Amazon EKS	를 사용하여 Amazon EKS 온프레미스 배포 AWS Outposts	를 사용하여 지연 시간이 짧은 EKS 클러스터 시작 AWS 로컬 영역
Amazon ECS	의 Amazon ECS AWS Outposts	공유 서브넷, 로컬 영역 및 Wavelength 영역의 Amazon ECS 애플리케이션
Amazon RDS	의 Amazon RDS AWS Outposts	로컬 영역 서브넷 선택
Amazon S3	Amazon S3 on Outposts 시작하기	사용할 수 없음
Amazon ElastiCache	ElastiCache에서 Outposts 사용	ElastiCache에서 로컬 영역 사용
Amazon EMR	의 EMR 클러스터 AWS Outposts	의 EMR 클러스터 AWS 로컬 영역
Amazon FSx	사용할 수 없음	로컬 영역 서브넷 선택
AWS Elastic Disaster Recovery	AWS Elastic Disaster Recovery 및 작업 AWS Outposts	사용할 수 없음
AWS Transform MGN	사용할 수 없음	로컬 영역 서브넷을 스테이징 서브넷으로 선택

Outposts별 CLI 및 SDK

AWS Outposts에는 서비스 주문을 생성하거나 로컬 게이트웨이와 로컬 네트워크 간의 라우팅 테이블을 조작하기 위한 두 가지 명령 및 APIs 그룹이 있습니다.

Outposts 주문 프로세스

[AWS CLI](#) 또는 [Outposts APIs](#)를 사용하여 Outposts 사이트를 생성하고, Outpost를 생성하고, Outpost 주문을 생성할 수 있습니다. AWS Outposts 주문 프로세스 중에 하이브리드 클라우드 전문가와 협력하여 구현 요구 사항에 맞는 적절한 리소스 IDs 선택과 최적의 구성을 보장하는 것이 좋습니다. 전체 리소스 ID 목록은 [AWS Outposts 랙 요금 페이지를 참조하세요](#).

로컬 게이트웨이 관리

Outposts에서 로컬 게이트웨이(LGW)를 관리하고 운영하려면이 작업에 사용할 수 있는 AWS CLI 및 SDK 명령에 대한 지식이 필요합니다. AWS CLI 및 AWS SDKs를 사용하여 다른 작업 중에서도 LGW 경로를 생성하고 수정할 수 있습니다. LGW 관리에 대한 자세한 내용은 다음 리소스를 참조하세요.

- [AWS CLI Amazon EC2용](#)
- 의 EC2.Client [AWS SDK for Python \(Boto\)](#)
- 의 Ec2Client [AWS SDK for Java](#)

CloudWatch 지표 및 로그

Outpost와 로컬 영역 모두에서 사용할 수 AWS 서비스 있는의 경우 지표와 로그는 리전과 동일한 방식으로 관리됩니다. Amazon CloudWatch는 다음 차원에서 Outpost 모니터링 전용 지표를 제공합니다.

차원	설명
Account	용량을 사용하는 계정 또는 서비스
InstanceFamily	인스턴스 패밀리
InstanceType	인스턴스 유형
OutpostId	Outpost의 ID
VolumeType	EBS 볼륨 유형
VirtualInterfaceId	로컬 게이트웨이 또는 서비스 링크 가상 인터페이스(VIF)의 ID
VirtualInterfaceGroupId	로컬 게이트웨이 VIF에 대한 VIF 그룹의 ID

자세한 내용은 [Outposts 설명서의 Outpost 랙에 대한 CloudWatch 지표](#)를 참조하세요.

리소스

AWS 참조

- [를 사용한 하이브리드 클라우드 AWS](#)
- [AWS Outposts Outpost 랙 사용 설명서](#)
- [AWS 로컬 영역 사용 설명서](#)
- [AWS Outposts 패밀리](#)
- [AWS 로컬 영역](#)
- [VPC를 로컬 영역, Wavelength Zone 또는 Outpost로 확장](#)(Amazon VPC 설명서)
- [로컬 영역의 Linux 인스턴스](#)(Amazon EC2 설명서)
- [Outposts의 Linux 인스턴스](#)(Amazon EC2 설명서)
- [를 사용하여 저지연 애플리케이션 배포 시작하기 AWS 로컬 영역](#)(자습서)

AWS 블로그 게시물

- [Amazon EC2를 사용하여 온프레미스 AWS 인프라 실행](#)
- [Amazon EC2에서 Amazon EKS를 사용하여 최신 애플리케이션 구축](#)
- [Amazon EC2 랙에서 CoIP 및 직접 VPC 라우팅 모드 중에서 선택하는 방법](#)
- [Amazon EC2의 네트워크 스위치 선택](#)
- [에서 데이터의 로컬 복사본 유지 관리 AWS 로컬 영역](#)
- [Amazon EC2의 Amazon ECS](#)
- [용 Amazon EKS를 사용하여 엣지 인식 서비스 메시 관리 AWS 로컬 영역](#)
- [Amazon EC2에 로컬 게이트웨이 수신 라우팅 배포](#)
- [에서 워크로드 배포 자동화 AWS 로컬 영역](#)
- [다중 계정 환경에서 Amazon EC2 공유 AWS : 1부](#)
- [다중 계정 환경에서 Amazon EC2 공유 AWS : 2부](#)
- [AWS Direct Connect 및 AWS 로컬 영역 상호 운용성 패턴](#)
- [다중 AZ 고가용성을 사용하여 Amazon EC2에 Amazon RDS 배포](#)

기여자

다음은 이 가이드에 기여한 사람입니다.

작성

- Leonardo Solano, Principal Hybrid Cloud Solutions Architect, AWS
- Len Gomes, 파트너 솔루션 아키텍트, AWS
- Matt Price, 선임 엔터프라이즈 지원 엔지니어, AWS
- Tom Gadomski, 솔루션 아키텍트, AWS
- Obed Gutierrez, 솔루션 아키텍트, AWS
- Dionysios Kakalettris, 기술 계정 관리자, AWS
- Vamsi Krishna, Principal Outposts Specialist, AWS

검토

- David Fillatrault, 전송 컨설턴트, AWS

기술 작성

- Handan Selamoglu, Sr. Documentation Manager, AWS

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 [RSS 피드](#)를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2025년 6월 10일

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