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

Table of Contents

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 컴퓨팅과 클라우드 기반 컴퓨팅의 이점을 모두 제공할 수 있으며 엣지 컴퓨팅 시나리오에 특히 유용할 수 있습니다.

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

- 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 클라우드에서 워크로드 배치에 대한 지침을 제공합니다.
- 하이브리드 클라우드의 기술 전략은 하이브리드 클라우드 아키텍처의 기본 원칙을 식별하고 구현 프레임워크를 정의합니다. 이 지침에서는 계획된 하이브리드 클라우드 구현에 대한 원칙을 정의하는 데 도움이 되도록 일관되게 배포되고 관리되는 하이브리드 클라우드 아키텍처에 대한 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 서비스는 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 다음을 수행합니다.

개요

이 가이드에서는 하이브리드 클라우드에 대한 AWS 권장 사항을 네트워킹, 보안, 복원력, 용량 계획 및 인프라 관리의 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 Outposts선택을 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 설명서의 지침을 따릅니다. 에서 워크로드를 테스트하려면 팀과 AWS Outposts협력 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 FAQs를 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 리전연결하려면 500Mbps(1Gbps가 더 좋음) 이상의 인터넷 또는 AWS Direct Connect 링크를 제공하고 유지해야 합니다. 에서 리전 AWS Outposts 까지의 왕복 시간 지연 시간은 최대 175밀리초여야 합니다.
- AWS Enterprise Support 또는 AWS Enterprise On-Ramp에 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 AWS Direct Connect 존재 지점(PoP)으로 연결되는 AWS Direct Connect 링크입니다. 자세한 내용은 로컬 영역 설명서의 Direct Connect를 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 지원을 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 사항의 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 Outposts 사용 설명서의 Amazon S3 on Outposts가 Amazon S3와 어떻게 다른가요? 섹션에서 설명합니다. Amazon S3
- 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 영역은를 지원하지 않습니다 AWS Transit Gateway. 대신 AWS Direct Connect 프라이빗 가상 인터페이스(VIF)를 사용하여 로컬 영역에 연결합니다.
- 모든 로컬 영역이 Amazon RDS, Amazon FSx, Amazon EMR, Amazon ElastiCache 또는 NAT 게이트웨이와 같은 서비스를 지원하는 것은 아닙니다. 자세한 내용은 AWS 로컬 영역 기능을 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)는의 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.

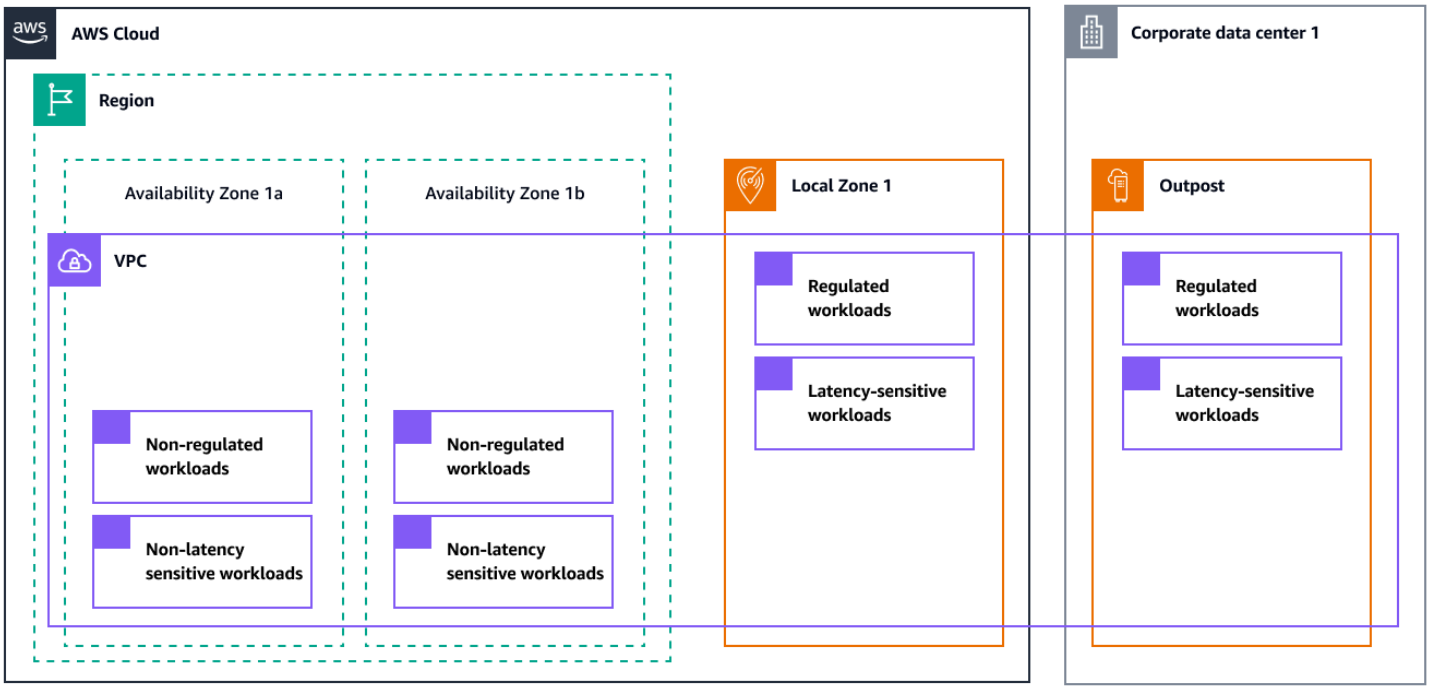
```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  자세한 내용은 AWS Outposts 설명서를 참조하십시오.
- 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 로컬 영역 서브넷을 포함하는 AWS 아키텍처를 보여줍니다.



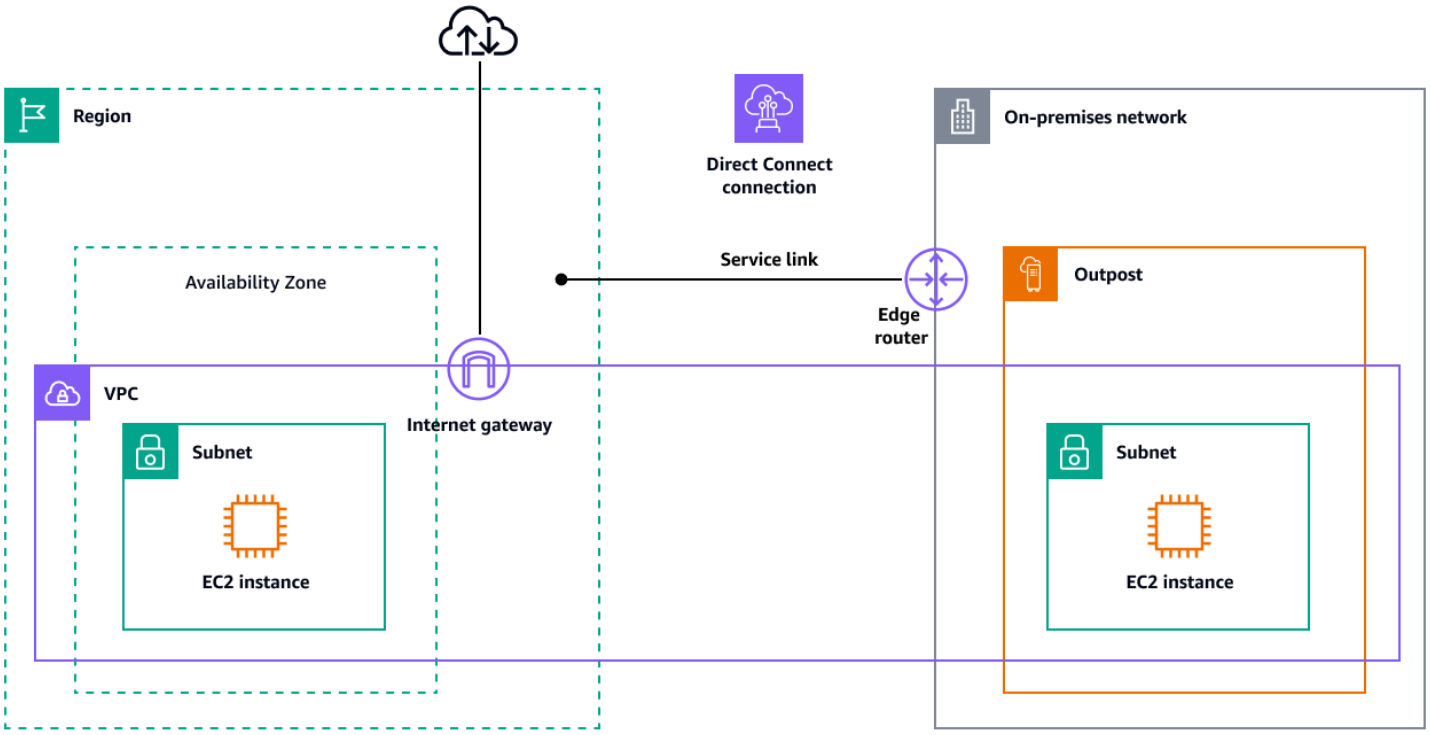
엣지-리전 트래픽

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 연결

세트를 사용하여 홈 리전과 통신합니다. AWS 리전 인터넷 링크 또는 AWS Direct Connect 퍼블릭 가상 인터페이스(퍼블릭 VIF) 또는 AWS 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 Outposts에 대한 연결을 AWS 리전 참조하세요.



AWS Direct Connect 및 퍼블릭 인터넷을 사용하는 서비스 링크에 대한 복원력이 뛰어난 아키텍처를 생성하는 방법에 대한 자세한 내용은 AWS 백서의 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	대상	MTU
리전의 Amazon EC2	로컬 영역의 Amazon EC2	1,300바이트
AWS Direct Connect	로컬 영역	1,468바이트
인터넷 게이트웨이	로컬 영역	1,500바이트
로컬 영역의 Amazon EC2	로컬 영역의 Amazon EC2	9,001바이트

로컬 영역은 AWS 글로벌 인프라를 사용하여 연결합니다 AWS 리전. 인프라는에서 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.

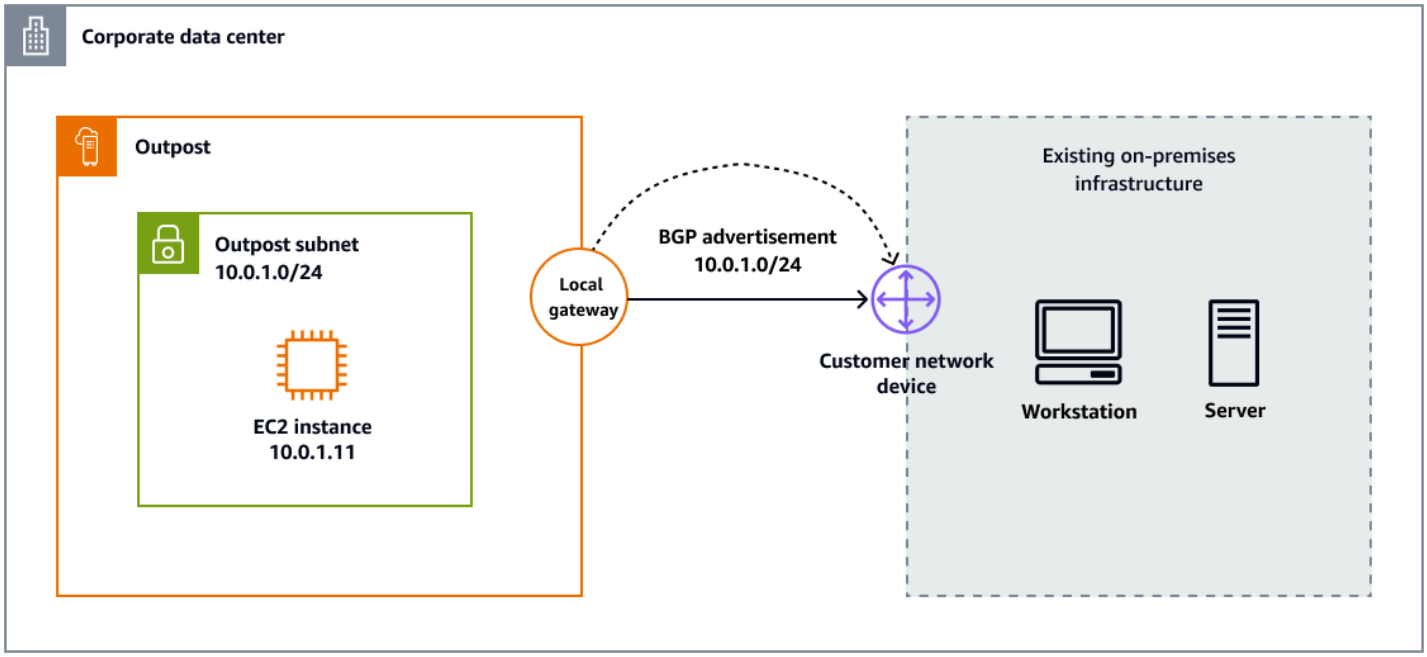
엣지-온프레미스 트래픽

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.

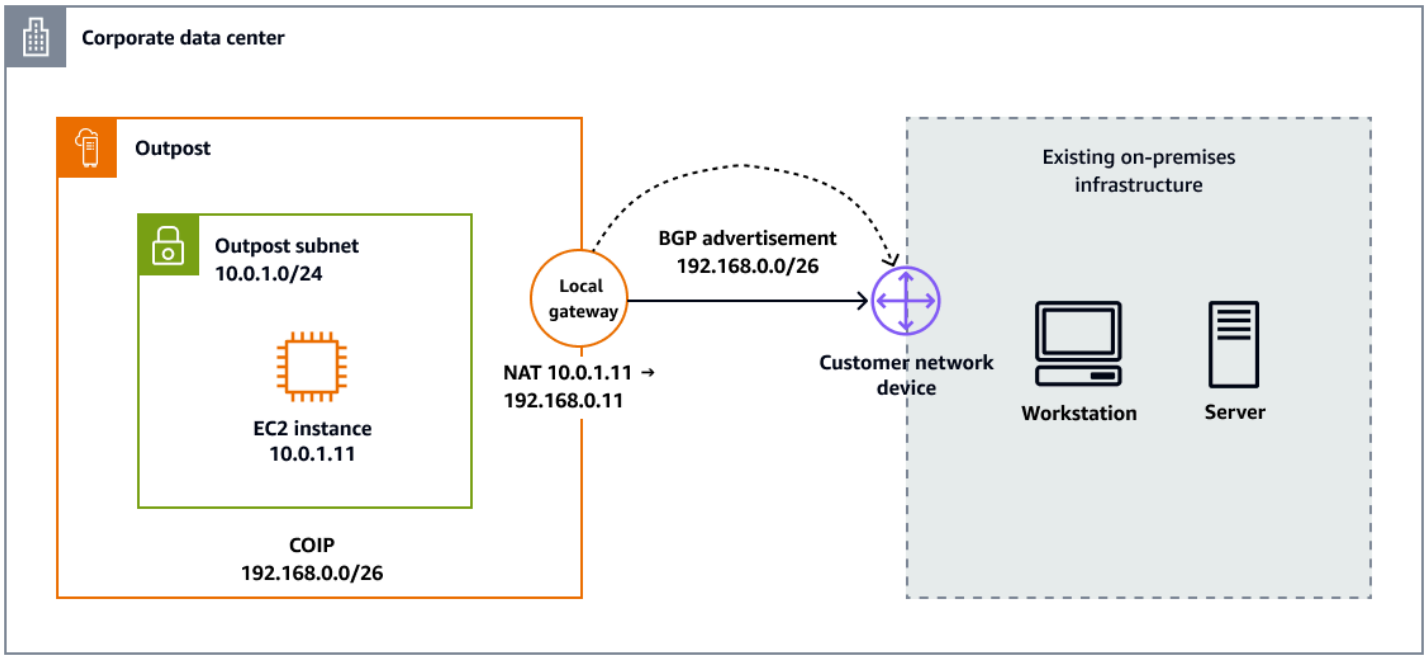
AWS Outposts 로컬 게이트웨이

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 주소를 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 몇 가지 파라미터 구성이 필요합니다. Outpost와 로컬 게이트웨이 간에 지원할 수 있는 MTU는 1,500바이트입니다. 자세한 내용은 AWS 하이브리드 클라우드 전문가에게 문의하거나AWS Outposts 설명서를 검토하세요.

로컬 영역 및 인터넷

지연 시간이 짧거나 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 그룹은가 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 옵션을 참조하세요.

로컬 영역 및 AWS Direct Connect

로컬 영역은 프라이빗 네트워크 연결을 통해 트래픽을 라우팅할 수 AWS Direct Connect있는 도 지원합니다. 자세한 내용은 로컬 영역 설명서의 로컬 영역의 Direct Connect를 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 서브넷에 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 연결을 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 따라는 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 로 통합하는 AWS

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

보안은 AWS 와 사용자 간의 공동 책임입니다. AWS 공동 책임 모델은 클라우드의 보안과 클라우드의 보안을 구분합니다.

- 클라우드 보안 - AWS 서비스 에서 실행되는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 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. 사용자는이 인프라(클라우드의 보안)에서 호스팅되는 콘텐츠에 대한 제어를 유지할 책임이 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 좋습니다AWS IAM Identity Center. 이렇게 하면 각 사용자에게 직무를 수행하는 데 필요한 권한만 부여됩니다.

유휴 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 FAQ에 설명된 목록(질문: 로컬 영역에서 EBS 볼륨의 기본 암호화 동작은 무엇입니까? 참조)을 제외하고모든 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

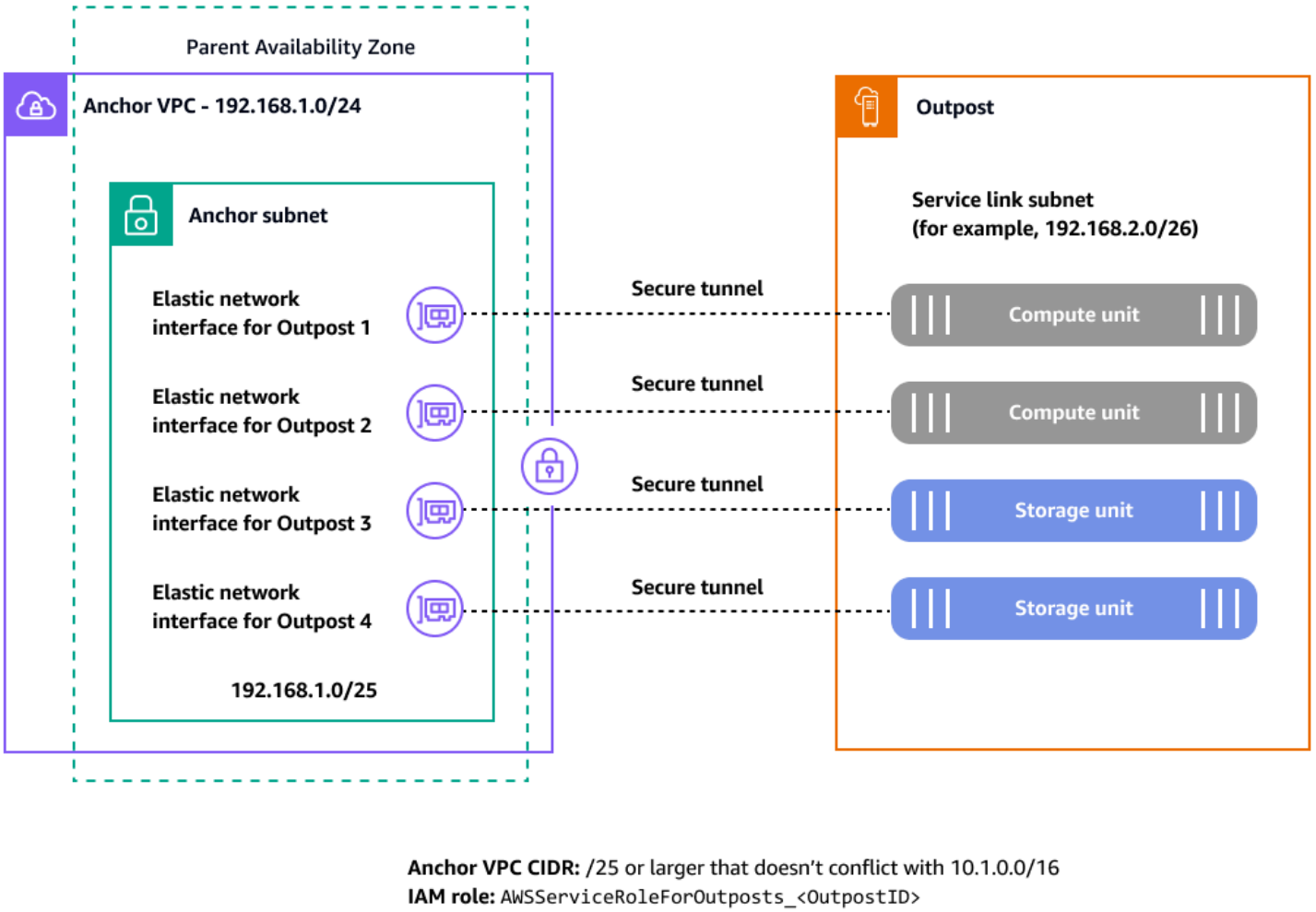
암호화를 사용할 수도 있습니다. SSE-C를 사용하려면 객체 API 요청의 일부로 암호화 키를 지정합니다. 서버 측 암호화는 객체 메타데이터가 아닌 객체 데이터만 암호화합니다.

> **Note**
>
> Amazon S3 on Outposts는 KMS 키(SSE-KMS)를 사용한 서버 측 암호화를 지원하지 않습니다.

전송 중 데이터 암호화

AWS Outposts의 경우 서비스 링크는 Outpost 서버와 선택한 AWS 리전 (또는 홈 리전) 간의 필수 연결이며 Outpost를 관리하고와 트래픽을 주고받을 수 있습니다 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 AWS Direct Connect)에 따라 AWS Outposts해당 터널 위에 오버레이를 생성하려면 서비스 링크에 대해 방화벽 포트를 열어야 합니다. 및 서비스 링크의 AWS Outposts 보안에 대한 자세한 기술 정보는 AWS Outposts 설명서의의 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.



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

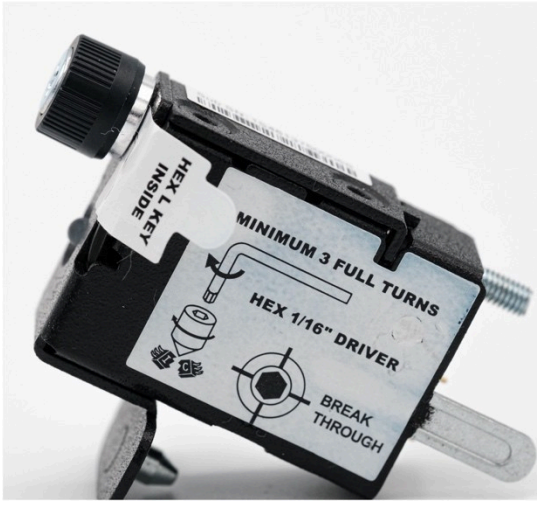
프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	443	AWS Outposts 서비스 링크 /26	443	AWS Outposts 리전의 퍼블릭 경로 또는 앵커 VPC CIDR
TCP	1025-65535	AWS Outposts 서비스 링크 /26	443	AWS Outposts 리전의 퍼블릭

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 AWS Direct Connect PoPs 간에 전송 중인 데이터를 암호화하여 로컬 영역에 액세스해야 하는 특정 요구 사항이 있는 경우 온프레미스 라우터 또는 스위치와 AWS Direct Connect 엔드포인트 간에 MAC 보안(MACsec)을 활성화할 수 있습니다. 자세한 내용은 AWS 블로그 게시물 AWS Direct Connect 연결에 MACsec 보안 추가를 참조하세요.

데이터 삭제

에서 EC2 인스턴스를 중지하거나 종료하면 새 인스턴스에 할당되기 전에 하이퍼바이저가 인스턴스에 할당된 AWS Outposts메모리를 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.



자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. 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 계정수 있습니다.

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

IAM 기능	AWS Outposts 지원
ID 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
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 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 기반 정책입니다.

에서 이러한 기능을 지원하는 방법에 대한 자세한 내용은 AWS Outposts 사용 설명서를 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 계정 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 불연속적인 것으로 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 제어합니다. 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 구현합니다. 각 계층에서 트래픽을 검사하고 필터링합니다. Network Access Analyzer를 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 설명서의 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, 외부 Git 리포지토리 액세스 AWS및 유사한 시나리오에 사용할 경우에만 리전의 인터넷 소비를 실행 가능한 옵션으로 고려하세요. 이 아키텍처 패턴의 경우 중앙 집중식 인바운드 검사 및 중앙 집중식 인터넷 송신의 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.

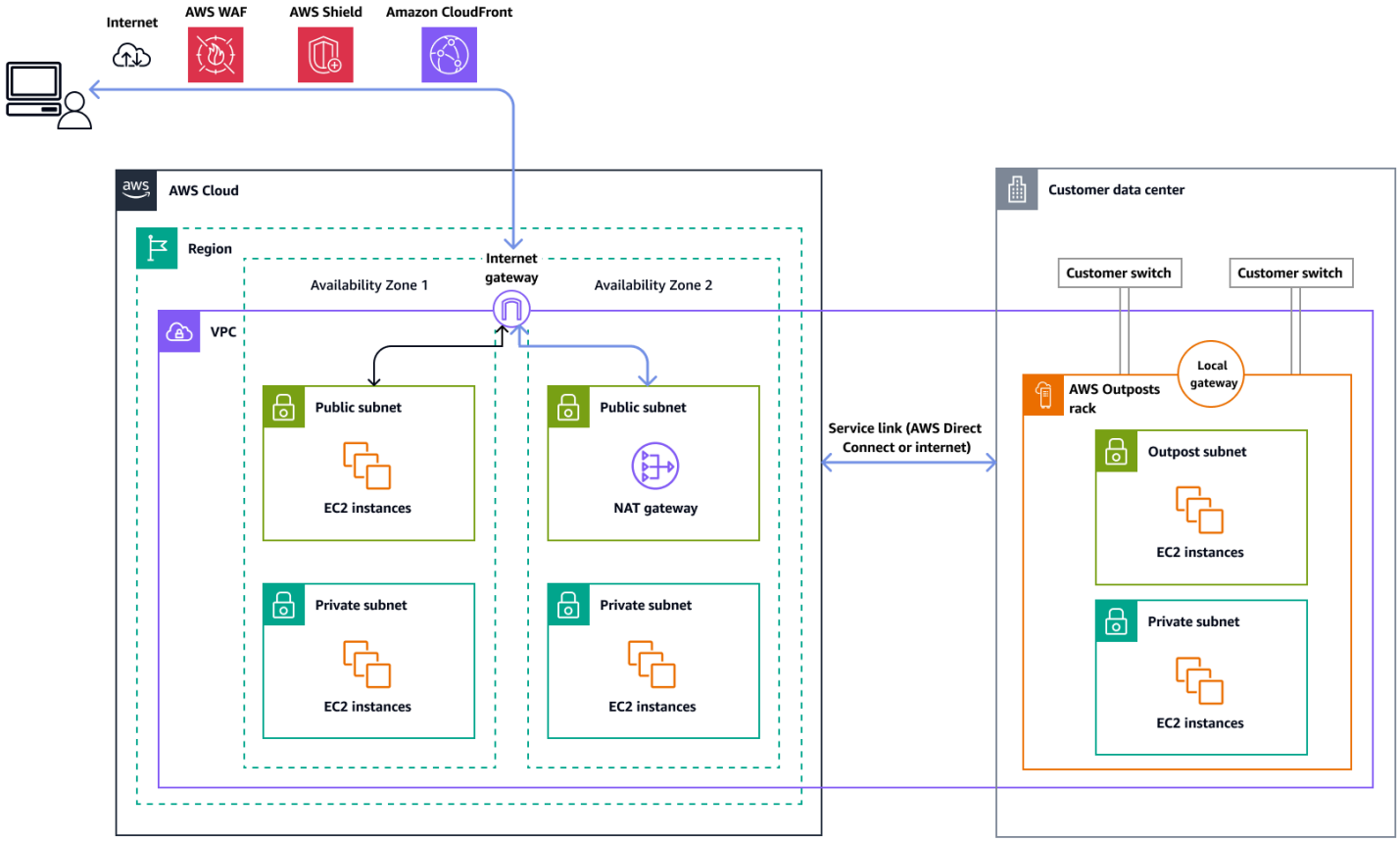
Local Zones는 네트워크 경계 그룹이라는 네트워크 구성을 채택합니다.이 네트워크 경계 그룹은에 사용됩니다 AWS 리전.이 네트워크 경계 그룹은 이러한 고유 그룹의 퍼블릭 IP 주소를 AWS 광고합니다. 네트워크 경계 그룹은 가용 영역, 로컬 영역 또는 Wavelength 영역으로 구성됩니다. 네트워크 경계 그룹에 사용할 퍼블릭 IP 주소 풀을 명시적으로 할당할 수 있습니다. 네트워크 경계 그룹을 사용하여 그룹에서 탄력적 IP 주소를 제공하도록 허용하여 인터넷 게이트웨이를 로컬 영역으로 확장할 수 있습니다. 이 옵션을 사용하려면 로컬 영역에서 사용할 수 있는 핵심 서비스를 보완하기 위해 다른 구성 요소를 배포해야 합니다. 이러한 구성 요소는 ISVs에서 가져올 수 있으며 AWS 블로그 게시물 Hybrid inspection architectures with에 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 링크와 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.

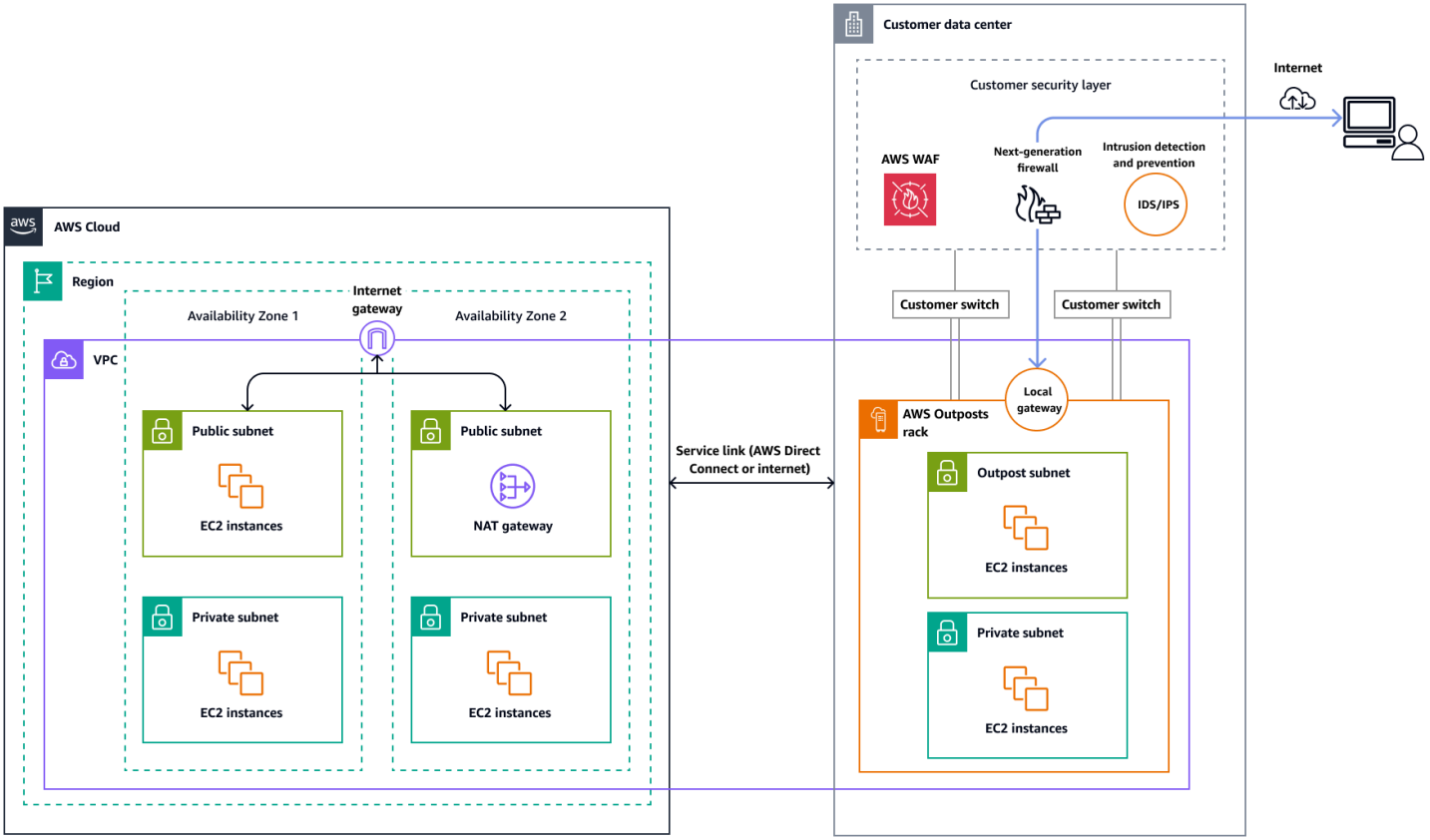
다음 다이어그램은 AWS Outposts 인스턴스의 워크로드와 상위를 통과하는 인터넷 간의 트래픽을 보여줍니다 AWS 리전.



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 Catalog및 IAM Identity Center(모든 통합 서비스 참조)를 AWS 서비스포함하여 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 설명서를 참조하십시오.

정부 AWS Control Tower 및 금융 서비스 기관(FSIs. 엣지에서 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 인프라이므로 중앙 집중식 거버넌스를 위해서는 어떤 계정 AWS Outposts 리소스가 공유되는지 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

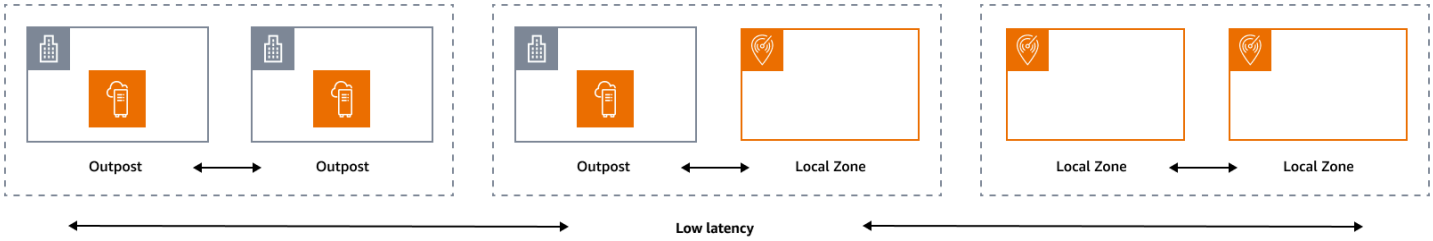
다중 계정 환경에서 Outpost 리소스를 공유하는 모범 사례를 따르려면 다음 AWS 블로그 게시물을 참조하세요.

- AWS Outposts 다중 계정 AWS 환경에서 공유: 1부
- AWS Outposts 다중 계정 AWS 환경에서 공유: 2부

엣지의 복원력

신뢰성 원칙은 워크로드가 의도한 기능을 예상대로 올바르고 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 인프라를 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 리전이 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.

로컬 영역

로컬 영역은 서브넷 및 EC2 인스턴스와 같은 영역 AWS 리소스의 배치 위치로 선택할 수 AWS 리전있으므로 해당 영역 내의 가용 영역과 유사하게 작동합니다. 그러나 이들은에 위치하지 AWS 리전않고 현재 AWS 리전 존재하지 않는 대규모 인구, 산업 및 IT 센터에 가깝습니다. 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 가까운에 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 플레인이 고정되는 곳입니다. 로컬 영역의 경우 상위 리전은 로컬 영역의 기본 아키텍처 구성 요소이며 고객이 수정할 수 없습니다.는 온프레미스 환경 AWS 클라우드 으로 AWS Outposts 확장되므로 주문 프로세스 중에 특정 리전 및 가용 영역을 선택해야 합니다. 이 선택은 Outpost 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
```

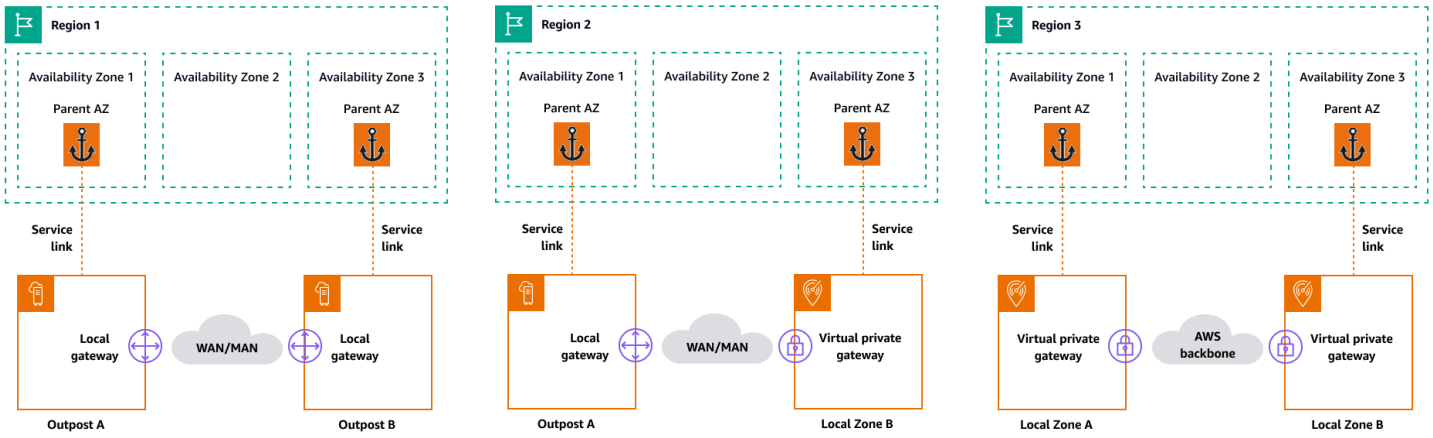
이전 명령의 출력:

```
{     "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 합니다us-east-1d-az2. 예를 들어 us-east-1d-az1는 유효합니다.

다음 다이어그램은 가용성이 높은 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

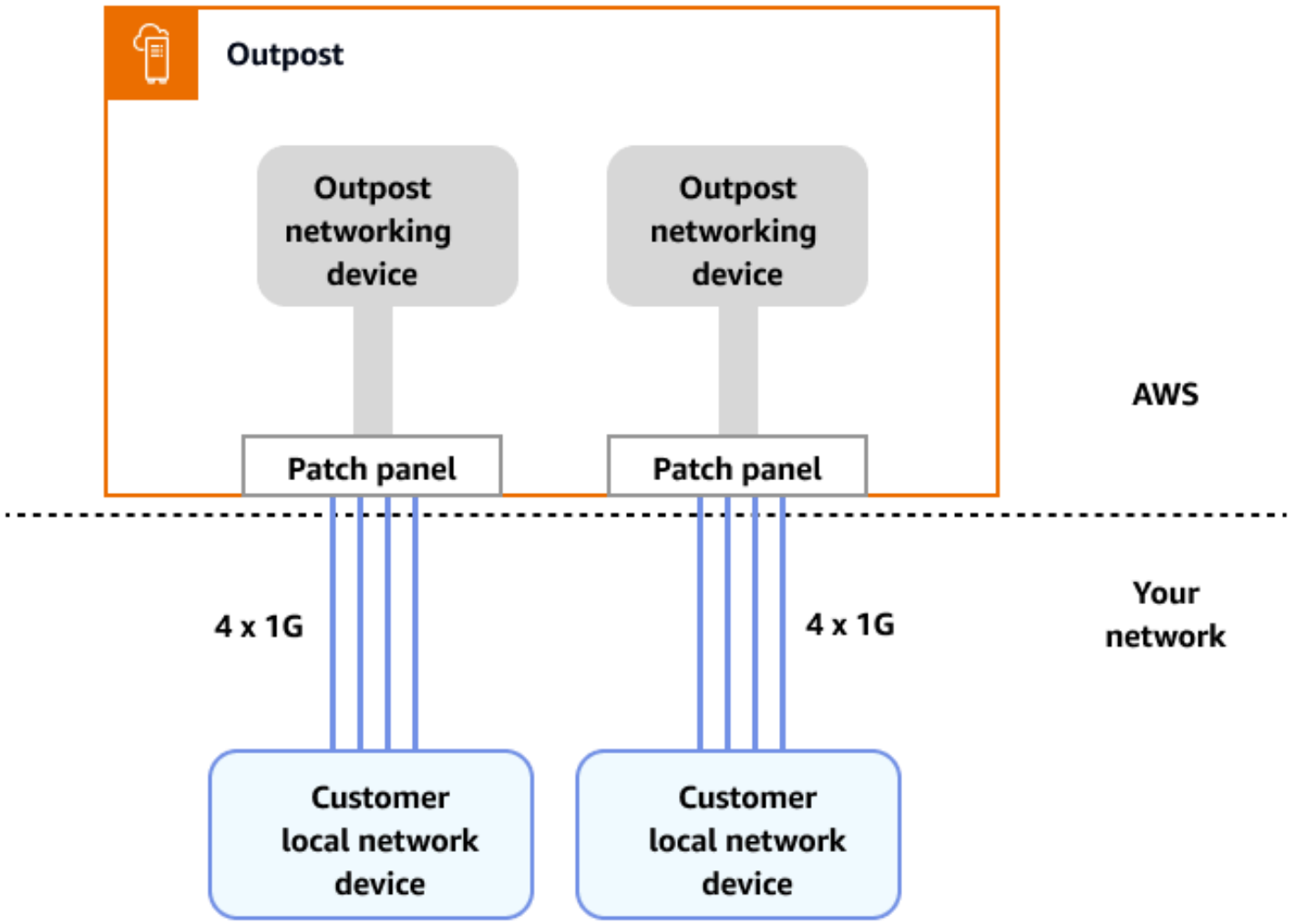
로컬 영역은 Amazon S3 및 Amazon RDS와 같은 모든 리전 서비스를 원활하게 사용할 수 있는 여러 개의 안전하고 중복된 고속 링크를 통해 상위 리전에 연결됩니다. 온프레미스 환경 또는 사용자에서 로컬 영역으로의 연결을 제공할 책임은 사용자에게 있습니다. 선택한 연결 아키텍처(예: VPN 또는 AWS Direct Connect)에 관계없이 기본 링크에서 장애가 발생할 경우 애플리케이션 성능에 영향을 주지 않도록 네트워크 링크를 통해 달성해야 하는 지연 시간은 동일해야 합니다. AWS Direct Connect를 사용하는 경우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

워크에 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.

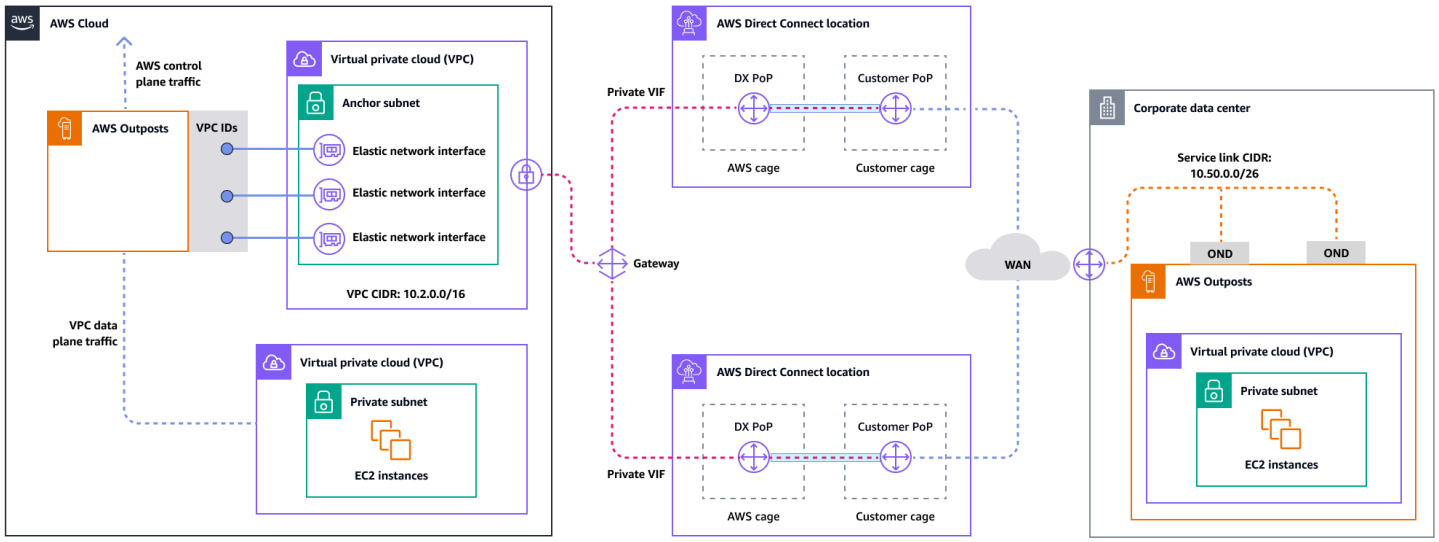
업링크 속도	업링크 수
1Gbps	1, 2, 4, 6 또는 8
10Gbps	1, 2, 4, 8, 12 또는 16
40 또는 100Gbps	1, 2, 또는 4



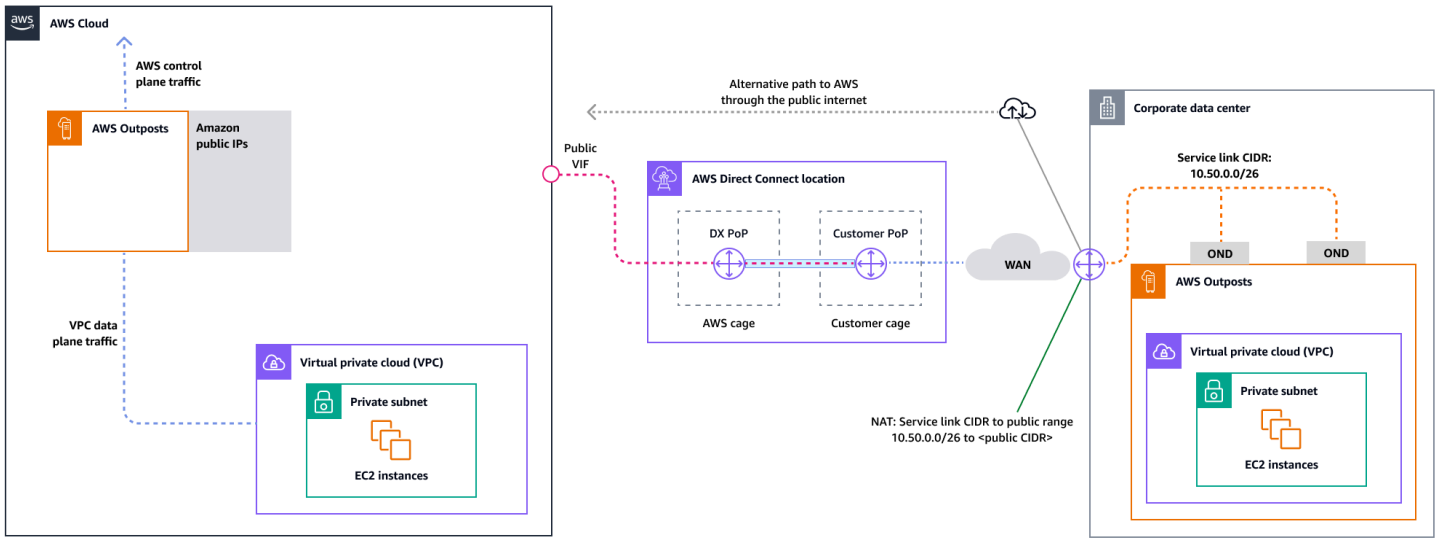
이 연결에 대한 자세한 내용은 AWS Outposts 설명서의 Outpost 랙에 대한 로컬 네트워크 연결을 참조하세요.

최적의 경험과 복원력을 위해는에 대한 서비스 링크 연결에 최소 500Mbps(1Gbps가 더 좋음)의 중복 연결을 사용할 것을 AWS권장합니다 AWS 리전. 서비스 링크에 AWS Direct Connect 또는 인터넷 연결을 사용할 수 있습니다. 이 최소값을 사용하면 EC2 인스턴스를 시작하고, EBS 볼륨을 연결하고, Amazon EKS AWS 서비스, Amazon EMR 및 CloudWatch 지표와 같은 액세스를 수행할 수 있습니다.

다음 다이어그램은 고가용성 프라이빗 연결을 위한이 아키텍처를 보여줍니다.



다음 다이어그램은 고가용성 퍼블릭 연결을 위한이 아키텍처를 보여줍니다.



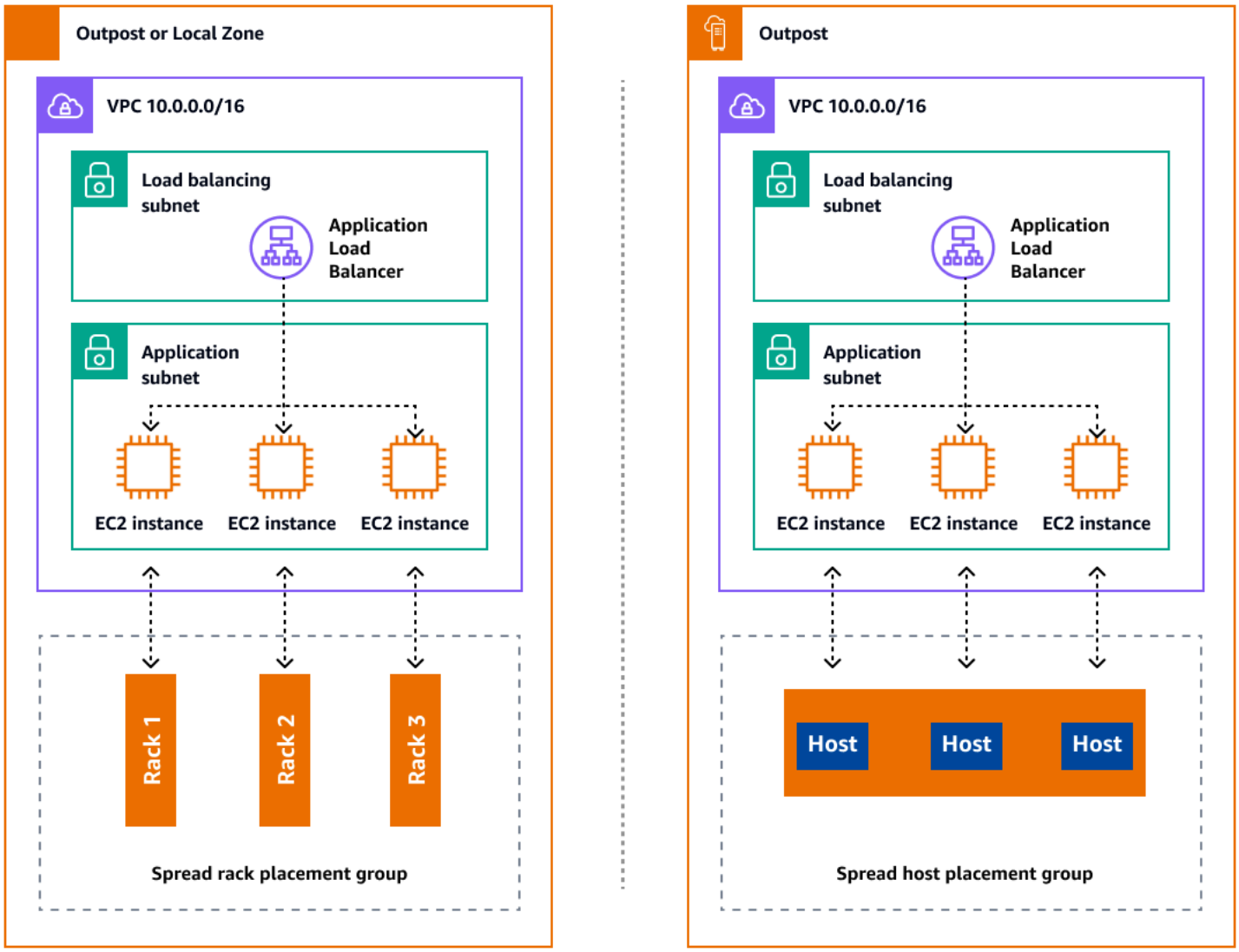
ACE 랙을 사용하여 Outpost 랙 배포 규모 조정

집계, 코어, 엣지(ACE) 랙은 AWS Outposts 다중 랙 배포에 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 디바

이스에 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 Rack을 참조하세요.

Outpost 및 로컬 영역에 인스턴스 배포

Outpost와 로컬 영역에는 컴퓨팅 서버 수가 한정되어 있습니다. 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 분산하여 동일한 인프라에서 관련 인스턴스를 실행할 위험을 완화할 수 있습니다. 파티션 배치 그룹을 사용하여 여러 랙에 인스턴스를 배포할 수도 있습니다. 이를 스프레드 랙 분산 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

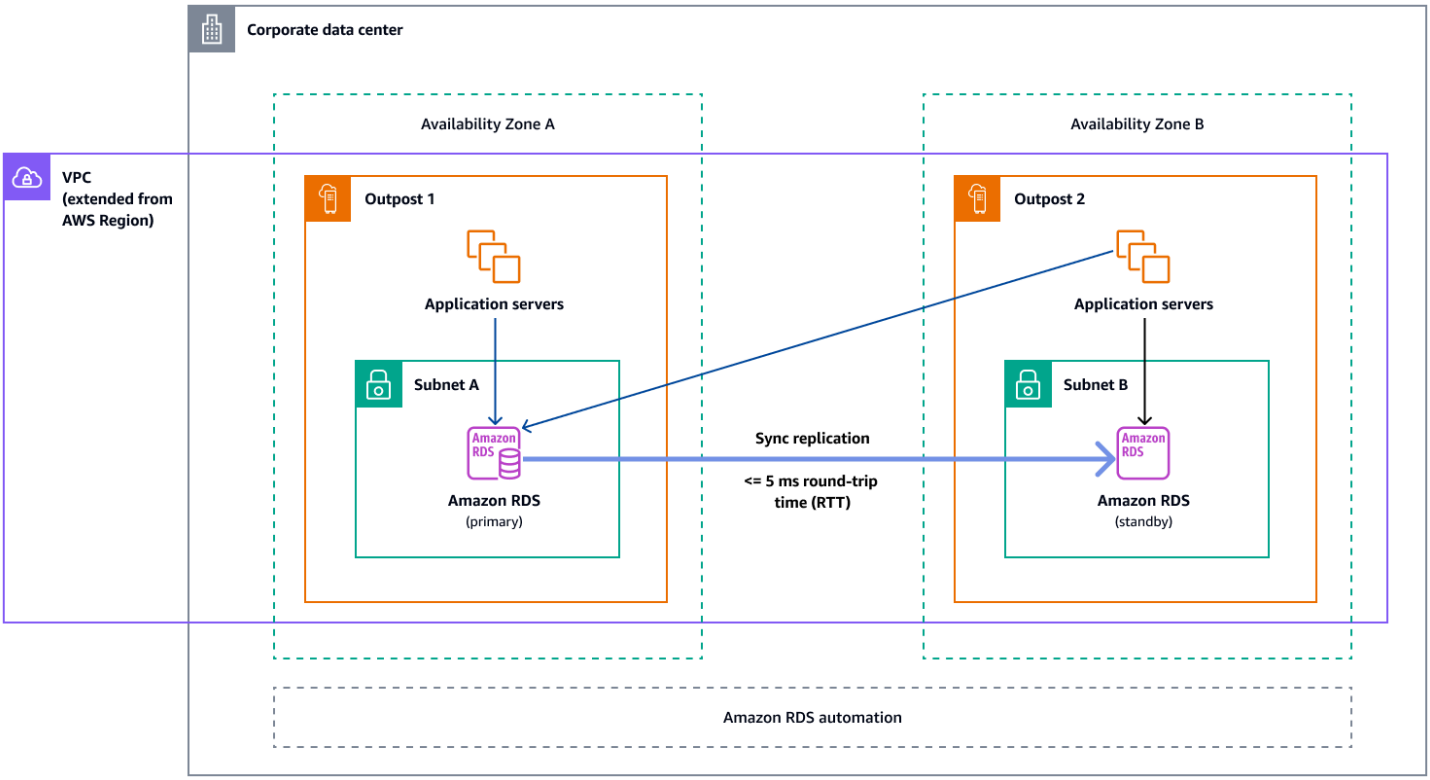
Outposts에서 다중 AZ 인스턴스 배포를 사용하는 경우 Amazon RDS는 두 Outposts에 두 개의 데이터베이스 인스턴스를 생성합니다. 각 Outpost는 자체 물리적 인프라에서 실행되며 고가용성을 위해 리전의 여러 가용 영역에 연결됩니다. 고객 관리형 로컬 연결을 통해 두 개의 Outpost가 연결되면 Amazon RDS는 기본 데이터베이스 인스턴스와 대기 데이터베이스 인스턴스 간의 동기식 복제를 관리합니다. 소프트웨어 또는 인프라에 장애가 발생하는 경우 Amazon RDS는 자동으로 대기 인스턴스를 기본 역할로 승격하고 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 배포는의 다중 AZ 배포 AWS 리전와 같이 작동하지만 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.



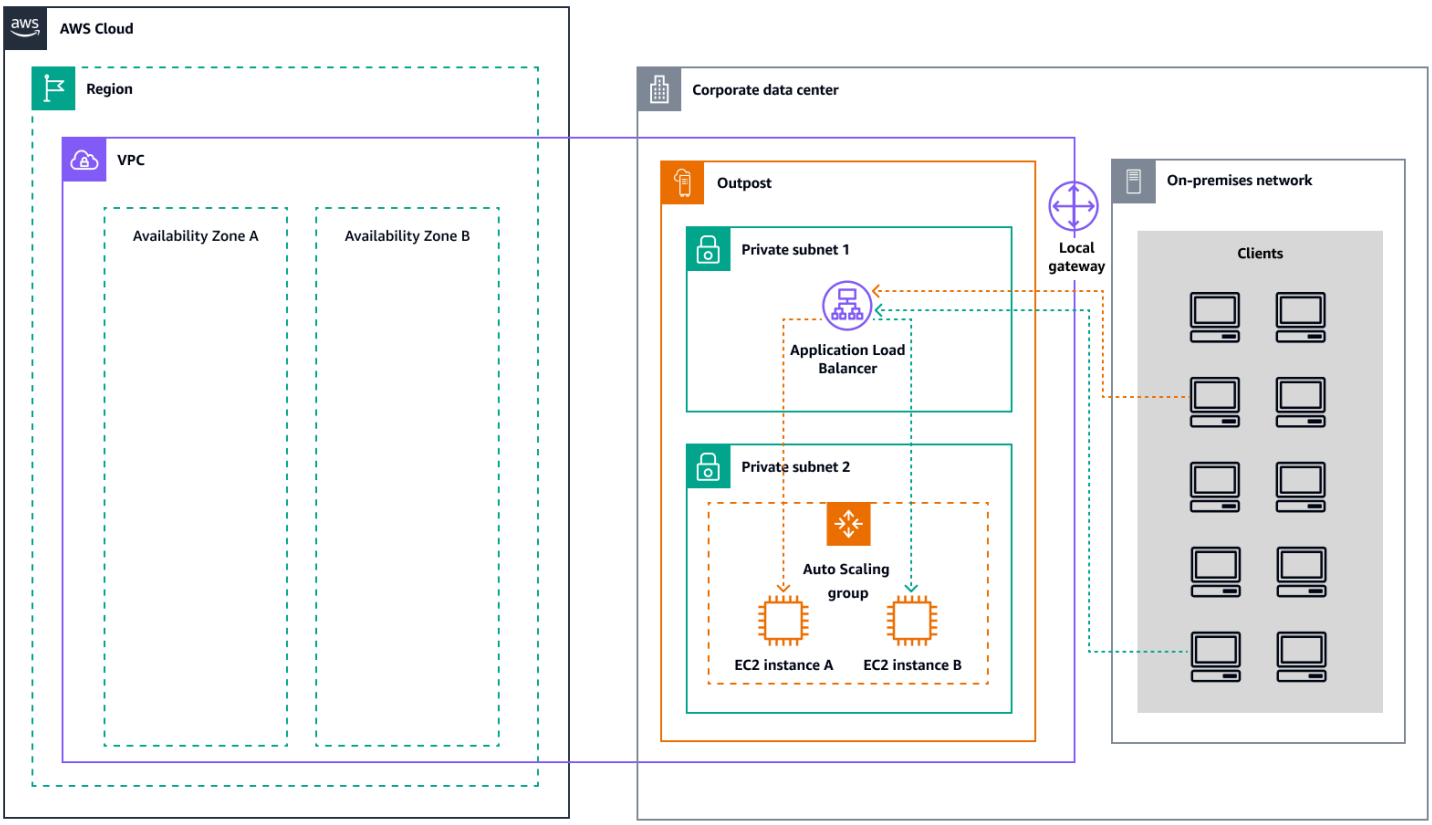
장애 조치 메커니즘

로드 밸런싱 및 자동 조정

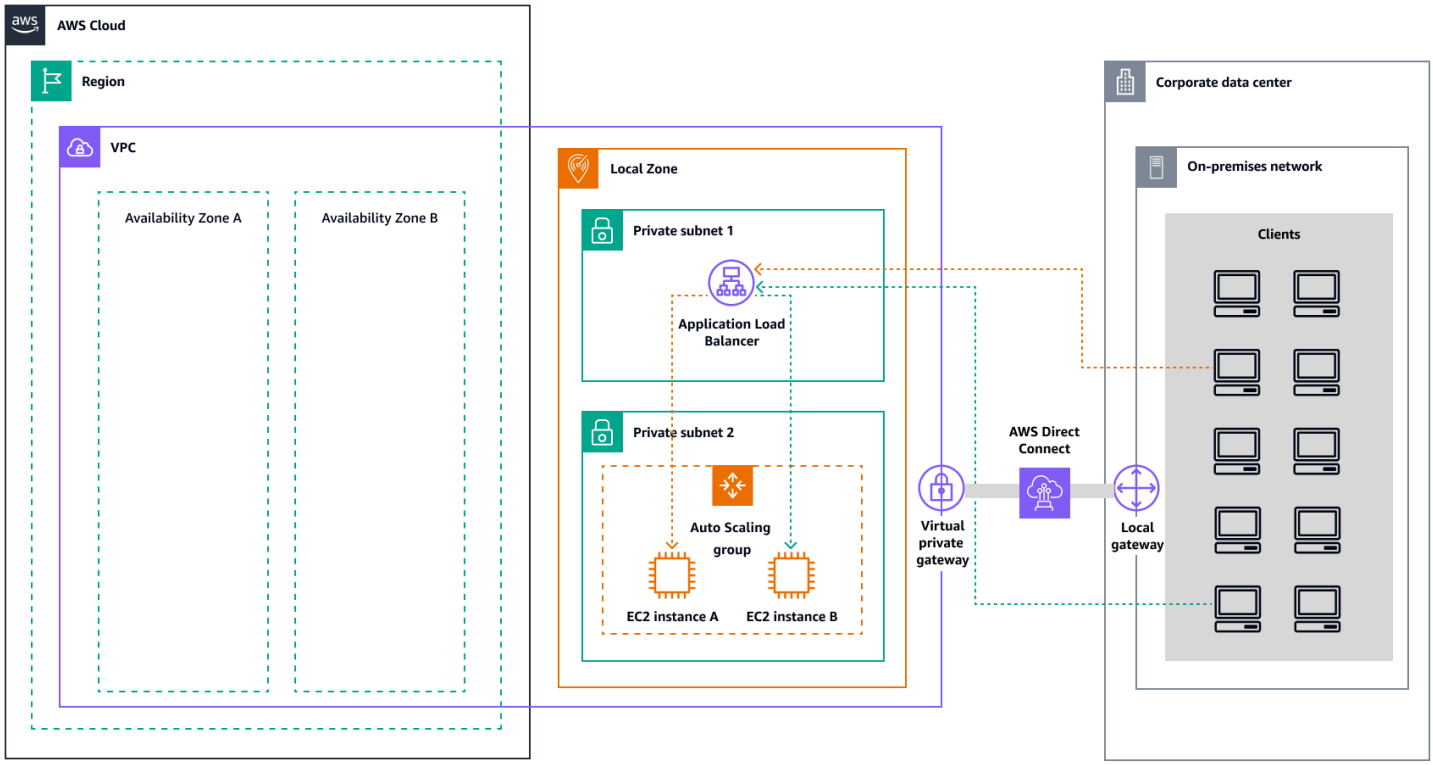
Elastic Load Balancing(ELB)은 실행 중인 모든 EC2 인스턴스에 수신 애플리케이션 트래픽을 자동으로 분산합니다. ELB는 단일 인스턴스가 압도되지 않도록 트래픽을 최적으로 라우팅하여 수신 요청을 관리하는 데 도움이 됩니다. Amazon EC2 Auto Scaling 그룹에서 ELB를 사용하려면 Auto Scaling 그룹에 로드 밸런서를 연결합니다. 이렇게 하면 그룹으로 들어오는 모든 웹 트래픽에 대한 단일 연락 지점 역할을 하는 로드 밸런서에 그룹이 등록됩니다. Auto Scaling 그룹에서 ELB를 사용하는 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: 대상당 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 알려주는 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.

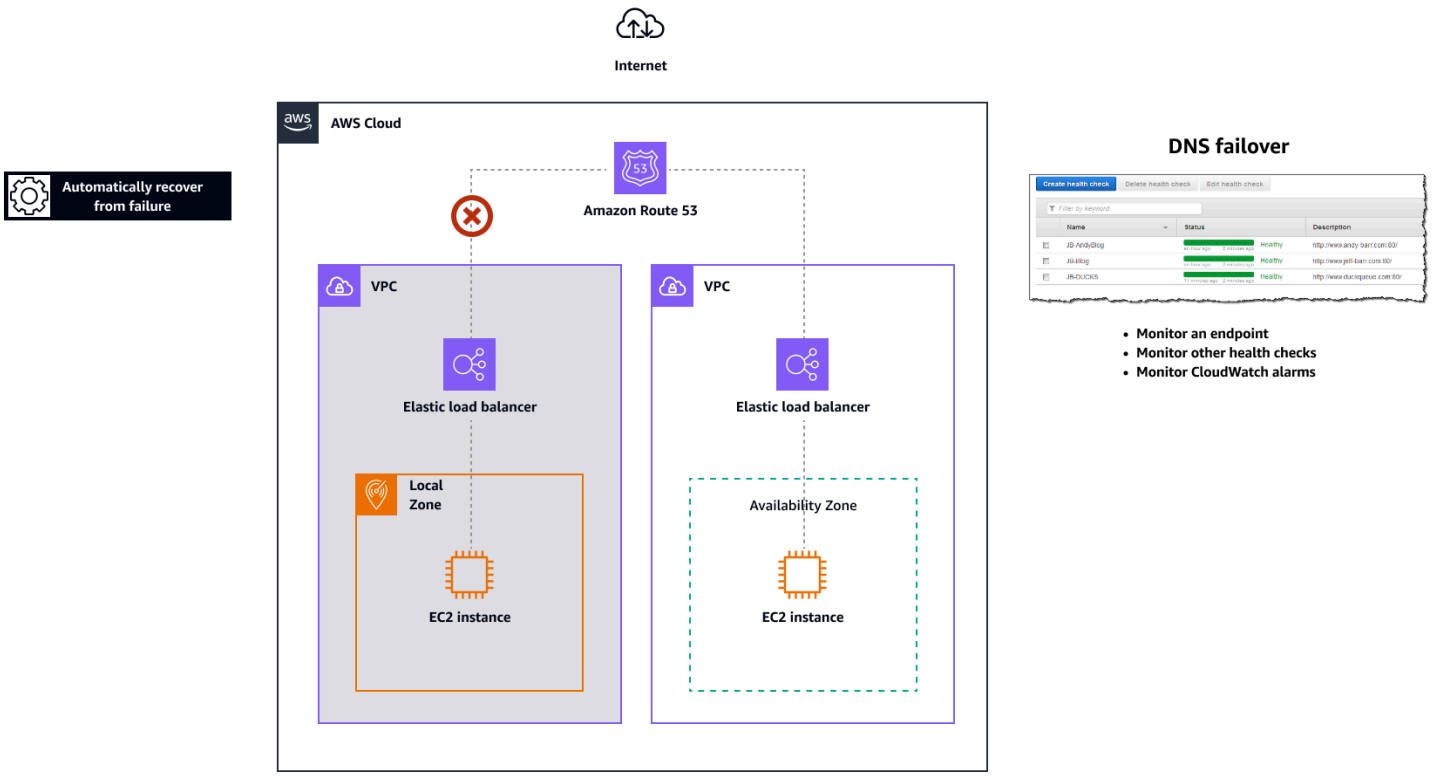


> **Note**
>
> Application Load Balancer는 AWS Outposts 및 로컬 영역 모두에서 사용할 수 있습니다. 그러나에서 Application Load Balancer를 사용하려면 로드 밸런서에 필요한 확장성을 제공하기 위해 Amazon EC2 용량의 크기를 조정 AWS Outposts해야 합니다. 의 로드 밸런서 크기 조정에 대한 자세한 내용은 AWS 블로그 게시물 Configure an Application Load Balancer on AWS Outposts을 AWS Outposts참조하세요.

DNS 장애 조치를 위한 Amazon Route 53

여러 HTTP 또는 메일 서버와 같이 동일한 기능을 수행하는 리소스가 두 개 이상 있는 경우 Amazon Route 53을 구성하여 리소스의 상태를 확인하고 정상 리소스만 사용하여 DNS 쿼리에 응답할 수 있습니다. 예를 들어 웹 사이트 `example.com`가 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 쿼리`example.com`에 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 사용하여에서 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 조합을 통해 Outposts 호스팅 애플리케이션에 대한 안정적인 퍼블릭 액세스를 보장합니다.

Amazon Route 53 Resolver 의 AWS Outposts

Amazon Route 53 Resolver는 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 상위 항목에 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 Framework의 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 계획을 참조하세요. AWS Outposts

로컬 영역에 대한 용량 계획

로컬 영역은 사용자와 AWS 리전 지리적으로 가까운의 확장입니다. 로컬 영역에서 생성된 리소스는 지연 시간이 매우 짧은 통신을 로컬 사용자에게 제공할 수 있습니다. 에서 로컬 영역을 활성화하려면 AWS 설명서의 시작하기 AWS 로컬 영역를 AWS 계정검토하세요. 각 로컬 영역에는 EC2 인스턴스 패밀리에 사용할 수 있는 슬롯이 다릅니다. 사용하기 전에 각 로컬 영역에서 사용 가능한 인스턴스를 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 기능을 참조하세요.

엣지에서 서비스 배포

AWS 콘솔 AWS CLI, 또는 API를 AWS 리전사용하여 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`m5.2xlarge`으로 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 ID를 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>
```

엣지에서 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 Application Migration Service	사용할 수 없음	로컬 영역 서브넷을 스테이징 서브넷으로 선택

Outposts별 CLI 및 SDK

AWS Outposts 에는 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 APIs를 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 지표를 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

다음 개인이이 가이드에 기여했습니다.

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 Kakaletris, 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 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2025년 6월 10일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 버전으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예:에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(RDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예:의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

속성 기반 액세스 제어를 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 액티브-패시브 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 데이터가 대상 데이터베이스에 복제되는 동안 소스 데이터베이스만 애플리케이션 연결의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 `SUM` 및가 있습니다`MAX`.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 작업을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용할 수 있는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 검색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 용 ABAC AWS를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환하기 위한 효율적이고 효과적인 계획을 개발하는 AWS 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹 사이트와 AWS CAF 백서를 참조하십시오.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

잘못된 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

별개의 동일한 두 환경을 생성하는 배포 전략입니다. 현재 애플리케이션 버전은 한 환경(파란색)에서 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 빠르게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇이라고 하는 다른 일부 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 것입니다.

봇넷

맬웨어에 감염되어 있고 봇 셰이더 또는 봇 운영자라고 하는 단일 당사자가 제어하는 봇 네트워크입니다. Botnet은 봇과 봇의 영향을 확장하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 About branches(GitHub 설명서)를 참조하십시오.

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 중고안경 절차 구현 표시기를 AWS 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

AWS 클라우드 채택 프레임워크를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

Cloud Center of Excellence를 참조하세요.

CDC

변경 데이터 캡처를 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템 복원력을 테스트하기 위해 의도적으로 장애 또는 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전달을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술과 연결됩니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 로 마이그레이션할 때 일반적으로 거치는 4단계: AWS 클라우드

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 – 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리에는 GitHub 또는가 포함됩니다Bitbucket Cloud. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정 미준수가 될 수 있으며 일반적으로 점진적이고 의도하지 않습니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 검색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 분산된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 일반적으로 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터베이스 정의 언어를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 컨트롤을 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Detective controls를 참조하십시오.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서는 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 일반적으로 쿼리 제약, 필터링 및 결과 집합 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간과 데이터 손실을 최소화하는 데 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준 구성과의 편차 추적. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 값 스트림 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 클라우드 컴퓨팅과 비교할 때 엣지 컴퓨팅은 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간의 비즈니스 문서 자동 교환. 자세한 내용은 전자 데이터 교환이란 무엇입니까?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

별표 스키마의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외래 키가 포함된 열의 두 가지 유형이 포함됩니다.

빠른 실패

개발 수명 주기를 줄이기 위해 빈번한 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용

할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

몇 장의 샷 프롬프트

유사한 작업을 수행하도록 요청하기 전에 LLM에 작업과 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 컨텍스트 내 학습을 적용하여 모델이 프롬프트에 포함된 예제(샷)에서 학습합니다. 퓨샷 프롬프트는 특정 형식 지정, 추론 또는 도메인 지식이 필요한 작업에 효과적일 수 있습니다. 제로샷 프롬프트도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 연속 데이터 복제를 사용하여 최대한 짧은 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화되고 레이블이 지정되지 않은 데이터의 대규모 데이터 세트에 대해 훈련된 대규모 딥 러닝 신경망입니다. FMs은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 작업을 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란 무엇입니까?를 참조하세요.

G

생성형 AI

대량의 데이터에 대해 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트 및 오디오와 같은 새 콘텐츠 및 아티팩트를 생성할 수 있는 AI 모델의 하위 집합입니다. 자세한 내용은 생성형 AI란 무엇입니까?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 현대적이고 선호하는 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조업에서는 골든 이미지를 사용하여 여러 디바이스에 소프트웨어를 프로비저닝할 수 있으며 디바이스 제조 작업의 속도, 확장성 및 생산성을 개선하는 데 도움이 됩니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터 세트에서 보류된 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교하여 모델 성능을 평가할 수 있습니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

정보

IaC

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하십시오.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 적용 또는 수정하는 대신 프로덕션 워크로드를 위한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용한 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 참조하기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷(IoT) 디지털 트랜스포메이션 전략 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(TIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(TSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터를 기반으로 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문 답변, 문서 요약, 텍스트를 다른 언어로 변환, 문장 완성과 같은 여러 작업을 수행할 수 있습니다. 자세한 내용은 LLMs 참조하십시오.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 개인 정보 보호를 손상하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 중단하거나, 민감한 정보를 유출하거나, 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB는 관리형 서비스의 예입니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원재료를 작업 현장의 완성된 제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

마이그레이션 가속화 프로그램을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동 시 자체를 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 대기열 원격 측정 전송(MQTT)

리소스가 제한된 IoT 디바이스에 대한 게시/구독 패턴을 기반으로 하는 경량 M2M(machine-to-machine) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 실행 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은이 용어집의 7R 항목을 참조하고 대규모 마이그레이션을 가속화하기 위해 조직 동원을 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

마이그레이션 포트폴리오 평가를 참조하세요.

MQTT

메시지 대기열 원격 측정 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework에서는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

작업 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

Open Process Communications - Unified Architecture를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 M2M(Machinemachine-to-machine) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조업에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 혁신의 핵심 초점입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

개인 식별 정보를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능한 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한을 정의하거나(자격 증명 기반 정책 참조), 액세스 조건을 지정하거나(리소스 기반 정책 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체 AWS Organizations 입니다(서비스 제어 정책 참조).

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 마이크로서비스에서 데이터 지속성 활성화를 참조하십시오.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

`WHERE` 절에서 `false`일반적으로 위치한 `true` 또는를 반환하는 쿼리 조건입니다.

조건자 푸시다운

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄어들고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

설계에 따른 개인 정보 보호

전체 개발 프로세스를 통해 개인 정보를 고려하는 시스템 엔지니어링 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 리소스를 스캔합니다. 리소스가 컨트롤을 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

제조에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체인

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 작업을 하위 작업으로 나누거나 예비 응답을 반복적으로 구체화하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

마이크로서비스 간의 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 지침과 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RAG

Retrieval Augmented Generation을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

재설계

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 지정을 참조 AWS 리전 하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7R을 참조하세요.

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 고가용성 및 재해 복구가 일반적인 고려 사항입니다 AWS 클라우드. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 Implementing security controls on AWS의 Responsive controls를 참조하십시오.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 의미 검색을 수행할 수 있습니다. 자세한 내용은 RAG란 무엇입니까?를 참조하십시오.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

복구 시점 목표를 참조하세요.

RTO

복구 시간 목표를 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

secret

에는 암호화된 형식으로 저장하는 암호 또는 사용자 자격 증명과 같은 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?를 참조하세요.

설계별 보안

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 예방, 탐지, 대응 및 사전 예방의 네 가지 주요 유형이 있습니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동 응답 작업의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

대상에서 데이터를 AWS 서비스 수신하는에 의한 데이터 암호화.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 표시기(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 대상 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애 지점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 장애가 발생한 경우.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 표시기를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드.

SPOF

단일 장애 지점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스 또는 비즈니스 인텔리전스용으로 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도

하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 운영을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 시스템을 테스트합니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 지침 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

전송 게이트웨이

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 Quantifying uncertainty in deep learning systems 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란?을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대 위치를 기반으로 행 값에 액세스하는 등의 작업을 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

쓰기를 한 번, 많이 읽기를 참조하세요.

WQF

AWS 워크로드 검증 프레임워크를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 데이터를 읽을 수 있지만 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경할 수 없는 것으로 간주됩니다.

Z

제로데이 익스플로잇

제로데이 취약성을 활용하는 공격, 일반적으로 맬웨어입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프트

LLM에 작업을 수행하기 위한 지침을 제공하지만 작업에 도움이 될 수 있는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 작업을 처리해야 합니다. 제로샷 프롬프트의 효과는 작업의 복잡성과 프롬프트의 품질에 따라 달라집니다. 스크린샷이 거의 없는 프롬프트도 참조하세요.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

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