AWS 백서

AWS장애 격리 경계

AWS장애 격리 경계: AWS 백서

Table of Contents

AWS

출판 날짜: 2022년 11월 16일 (문서 수정)

요약

Amazon Web Services (AWS) 는 가용 영역 (AZ), 지역, 컨트롤 플레인 및 데이터 플레인과 같은 다양한 격리 경계를 제공합니다. 이 AWS 백서에서는 이러한 경계를 사용하여 영역별, 지역별 및 글로벌 서비스를 만드는 방법을 자세히 설명합니다. 또한 이러한 다양한 서비스에 대한 종속성을 고려하는 방법과 이를 사용하여 구축하는 워크로드의 레질리언스를 개선하는 방법에 대한 규범적 지침도 포함되어 있습니다.

Dyl-Architected To

AWSWell-Architected 프레임워크는 클라우드에 시스템을 구축할 때 내리는 의사 결정의 장단점을 이해하는 데 도움이 됩니다. 프레임워크의 6가지 기둥을 통해 신뢰할 수 있고 안전하며 효율적이고 비용 효율적이며 지속 가능한 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 배울 수 있습니다. 에서 무료로 제공되는 를 사용하면 각 기둥에 대한 일련의 질문에 답하여 이러한 모범 사례와 비교하여 워크로드를 검토할 수 있습니다. AWS Well-Architected ToolAWS Management Console

참조 아키텍처 배포, 다이어그램, 백서 등 클라우드 아키텍처에 대한 더 많은 전문가 지침과 모범 사례는 아키텍처 센터를 참조하십시오. AWS

소개

AWS글로벌 인프라를 운영하여 고객이 유연하고 안전하며 확장 가능하고 가용성이 높은 방식으로 워크로드를 배포하는 데 도움이 되는 클라우드 서비스를 제공합니다. 이 AWS 인프라는 여러 장애 격리 구조를 사용하여 고객이 레질리언스 목표를 달성할 수 있도록 지원합니다. 이러한 장애 격리 경계를 통해 고객은 자신이 제공하는 예측 가능한 영향 억제 범위를 활용하도록 워크로드를 설계할 수 있습니다. 또한 워크로드에 대해 선택한 종속성을 의도적으로 선택할 수 있도록 이러한 경계를 사용하여 AWS 서비스를 설계하는 방법을 이해하는 것도 중요합니다.

이 백서에서는 먼저 AWS 글로벌 인프라와 해당 인프라가 제공하는 장애 격리 경계뿐만 아니라 서비스 설계에 사용되는 몇 가지 패턴을 요약합니다. 이 이해 기준을 바탕으로 이 백서에서는 다음으로 지역별, 지역별 및 전 세계적으로 AWS 제공되는 다양한 서비스 범위를 간략하게 설명합니다. 또한 이러한 격리 경계와 다양한 서비스 범위를 사용하여 실행 중인 워크로드의 복원력을 개선하는 아키텍처를 구

축하는 모범 사례를 제시합니다. AWS 특히 단일 장애 지점을 최소화하면서 글로벌 서비스에 대한 의존도를 높이는 방법에 대한 규범적인 지침을 제공합니다. 이렇게 하면 AWS 종속성과 고가용성 (HA) 및 재해 복구 (DR) 를 위한 워크로드 설계 방법에 대해 정보에 입각한 선택을 내리는 데 도움이 됩니다.

AWS 인프라

이 섹션에서는 AWS 글로벌 인프라와 인프라가 제공하는 장애 격리 경계에 대한 요약을 제공합니다. 또한 이 섹션에서는 서비스 AWS 설계 방식의 중요한 차이점인 컨트롤 플레인과 데이터 플레인의 개념에 대한 개요를 제공합니다. 이 정보는 장애 격리 경계와 서비스의 컨트롤 플레인 및 데이터 플레인이 다음 섹션에서 설명하는 AWS 서비스 유형에 어떻게 적용되는지를 이해하기 위한 기준을 제공합니다.

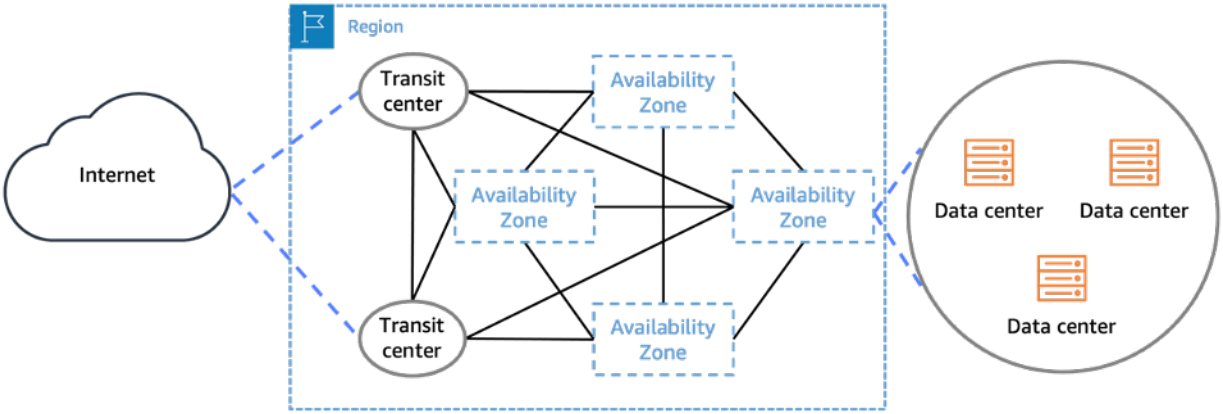
주제

가용 영역

AWS전 세계 여러 지역에서 100개 이상의 가용 영역을 운영합니다 (현재 수치는 AWS글로벌 인프라 참조). 가용 영역은 독립적이고 이중화된 전원 인프라, 네트워킹 및 연결을 갖춘 하나 이상의 개별 데이터 센터입니다. AWS 리전 한 지역의 가용 영역은 상호 연관된 장애를 방지하기 위해 최대 60마일 (~100km) 까지 서로 상당히 떨어져 있지만 지연 시간이 10밀리초인 동기 복제를 사용할 수 있을 정도로 가깝습니다. 전력 공급, 단수, 광케이블 격리, 지진, 화재, 토네이도 또는 홍수와 같은 공동 운명 시나리오의 영향을 동시에 받지 않도록 설계되었습니다. 발전기 및 냉각 장비와 같은 일반적인 장애 지점은 가용 구역 간에 공유되지 않으며 독립된 변전소에서 공급되도록 설계되었습니다. 서비스 업데이트를 AWS 배포할 때 동일한 지역의 가용 영역에 대한 배포를 시간적으로 구분하여 상호 관련된 장애를 방지합니다.

한 지역의 모든 가용 영역은 완전 이중화된 전용 메트로 파이버를 통해 고대역폭, 저지연 네트워킹으로 상호 연결됩니다. 한 지역의 각 가용 영역은 여러 계층 1 인터넷 AWS 공급자와 동료가 있는 두 개의 트랜짓 센터를 통해 인터넷에 연결됩니다 (자세한 내용은 Amazon Web Services 개요 참조).

이러한 기능을 통해 가용 영역을 서로 강력하게 격리할 수 있으며, 이를 가용 영역 독립성 (AZI) 이라고 합니다. 가용 영역의 논리적 구조와 가용 영역의 인터넷 연결성은 다음 그림에 나와 있습니다.



가용 영역은 상호 및 인터넷에 중복 연결된 하나 이상의 물리적 데이터 센터로 구성됩니다.

리전

각 가용 영역은 지리적 영역 내에 독립적이고 물리적으로 분리된 여러 개의 가용 영역으로 AWS 리전 구성되어 있습니다. 현재 모든 지역에는 3개 이상의 가용 영역이 있습니다. 지역 자체는 다른 지역과 격리되어 있으며 독립적입니다. 단, 이 문서의 뒷부분에서 설명하는 몇 가지 예외가 있습니다 (글로벌 단일 지역 운영 참조). 이러한 지역 간 분리로 인해 서비스 장애가 발생할 경우 단일 지역에서만 서비스 장애가 발생할 수 있습니다. 이 경우 다른 지역의 정상 운영에는 영향을 미치지 않습니다. 또한 AWS 서비스에서 제공하는 복제 또는 복사 기능을 명시적으로 사용하거나 리소스를 직접 복제하지 않는 한 한 한 한 지역에서 생성한 리소스 및 데이터는 다른 지역에 존재하지 않습니다.

2022년 12월 현재 및 예정된 AWS 지역

AWSLocal Zones

AWSLocal Zone은 컴퓨팅, 스토리지, 데이터베이스 및 기타 일부 AWS 서비스를 대규모 인구 및 산업 센터 근처에 배치하는 인프라 배포 유형입니다. 로컬 영역의 컴퓨팅 및 스토리지 서비스와 같은 AWS 서비스를 사용하여 엣지에서 지연 시간이 짧은 애플리케이션을 실행하거나 하이브리드 클라우드 마이그레이션을 단순화할 수 있습니다. Local Zone은 지연 시간을 줄이기 위해 로컬 인터넷 수신 및 송신을 지원하지만 Amazon의 중복 고대역폭 사설망을 통해 상위 지역과 연결되어 있어 Local AWS Zones에서 실행되는 애플리케이션이 전체 범위의 서비스에 빠르고 안전하며 원활하게 액세스할 수 있습니다.

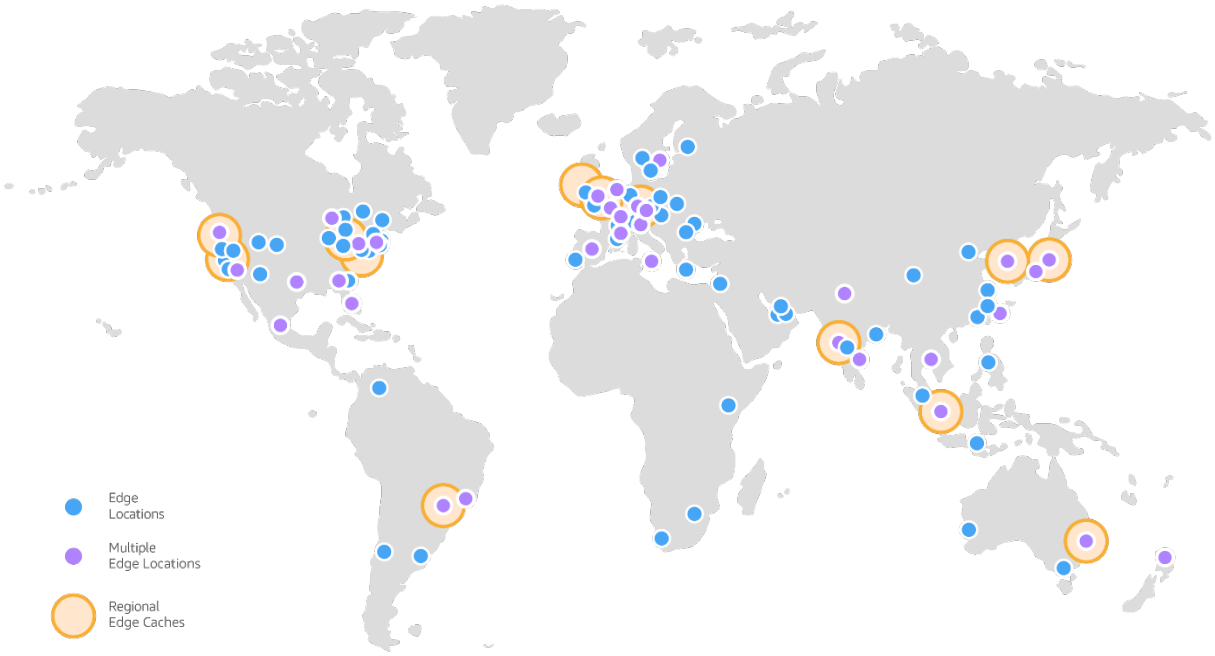
AWS Outposts

AWS Outposts진정한 일관성 있는 하이브리드 경험을 위해 거의 모든 온프레미스 또는 엣지 로케이션에 AWS 인프라와 서비스를 제공하는 완전 관리형 솔루션 제품군입니다. Outposts 솔루션을 사용하면 네이티브 AWS 서비스를 온프레미스로 확장하고 실행할 수 있으며, 1U 및 2U Outposts 서버에서 42U Outposts 랙, 다중 랙 배포에 이르기까지 다양한 폼 팩터로 제공됩니다.

를 사용하면 일부 AWS 서비스를 로컬에서 실행하고 상위 서비스에서 사용할 수 있는 광범위한 서비스에 연결할 수 있습니다. AWS Outposts AWS 리전 AWS Outposts고객이 온프레미스에서 컴퓨팅 및 스토리지를 실행하는 동시에 AWS 클라우드의 다양한 서비스에 원활하게 연결할 수 AWS 있도록 설계된 하드웨어로 구축된 완전 관리형 및 구성 가능한 컴퓨팅 및 스토리지 랙입니다.

접속 지점

AWS 리전및 가용 영역 외에도 전 세계적으로 분산된 PoP (PoP) AWS 네트워크도 운영합니다. 이들은 콘텐츠 전송 네트워크 (CDN) 인 Amazon CloudFront, 퍼블릭 도메인 이름 시스템 (DNS) 확인 서비스인 Amazon Route 53, 엣지 네트워킹 최적화 서비스인 AWS 글로벌 액셀러레이터 (AGA) 를 PoPs 호스팅합니다. 글로벌 엣지 네트워크는 현재 400개 이상의 엣지 로케이션을 포함한 410개 PoPs 이상의 엣지 로케이션과 48개국 90개 이상의 도시에 있는 13개의 지역 미드티어 캐시로 구성되어 있습니다 (현재 상태는 Amazon CloudFront 주요 기능 참조).



Amazon CloudFront 글로벌 엣지 네트워크

각 PoP는 다른 PoP와 격리되어 있으므로 단일 PoP 또는 대도시 지역에 영향을 미치는 장애가 나머지 글로벌 네트워크에는 영향을 미치지 않습니다. 이 AWS 네트워크는 전 세계 수천 개의 Tier 1/2/3 통신 사업자와 경쟁하고 있으며, 최적의 성능을 위해 모든 주요 액세스 네트워크와 잘 연결되어 있으며 수백 테라비트의 배치 용량을 갖추고 있습니다. 엣지 로케이션은 전 세계를 돌며 수만 개의 AWS 네트워크와 연결되는 완전 이중화된 다중 100GbE 병렬 파이버인 네트워크 백본을 AWS 리전 통해 연결되어 오리진 페치 개선과 동적 콘텐츠 가속을 제공합니다.

파티션

AWS지역을 파티션으로 그룹화합니다. 모든 지역은 정확히 하나의 파티션에 있으며 각 파티션에는 하나 이상의 지역이 있습니다. 파티션에는 IAM AWS Identity and Access Management (독립 인스턴스)

이 있으며 서로 다른 파티션의 지역 간에 엄격한 경계를 제공합니다. AWS상업 지역은 aws 파티션에, 중국의 지역은 aws-cn 파티션에, AWS GovCloud 지역은 aws-us-gov 파티션에 있습니다. Amazon S3 지역 간 복제 또는 AWSTransit Gateway 지역 간 피어링과 같은 일부 AWS 서비스는 지역 간 기능을 제공하도록 설계되었습니다. 이러한 유형의 기능은 동일한 파티션의 지역 간에서만 지원됩니다. 한 파티션의 IAM 자격 증명을 사용하여 다른 파티션의 리소스와 상호 작용할 수는 없습니다.

컨트롤 플레인 및 데이터 영역

AWS대부분의 서비스를 컨트롤 플레인 및 데이터 플레인 개념으로 구분합니다. 이러한 용어는 네트워킹, 특히 라우터의 세계에서 유래했습니다. 라우터의 주요 기능인 데이터 플레인은 규칙에 따라 패킷을 이동시킵니다. 하지만 라우팅 정책을 만들고 어딘가에서 배포해야 하기 때문에 컨트롤 플레인이 필요합니다.

컨트롤 플레인은 CRUDL (리소스를 생성, 읽기/설명, 업데이트, 삭제, 나열) 하는 데 사용되는 관리 API를 제공합니다. 예를 들어, 새 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 시작, 아마존 심플 스토리지 서비스 (Amazon S3) 버킷 생성, 아마존 심플 큐 서비스 (Amazon SQS) 대기열 설명 등 모든 컨트롤 플레인 작업이 여기에 해당합니다. EC2 인스턴스를 시작할 때 컨트롤 플레인은 용량이 있는 물리적 호스트 찾기, 네트워크 인터페이스 할당, Amazon Elastic Block Store (Amazon EBS) 볼륨 준비, IAM 자격 증명 생성, 보안 그룹 규칙 추가 등과 같은 여러 작업을 수행해야 합니다. 컨트롤 플레인은 복잡한 오케스트레이션 및 집계 시스템인 경향이 있습니다.

데이터 플레인은 서비스의 주요 기능을 제공합니다. 예를 들어, 실행 중인 EC2 인스턴스 자체, EBS 볼륨 읽기 및 쓰기, S3 버킷에 객체 가져오기 및 넣기, DNS 쿼리에 응답하고 상태 확인을 수행하는 Route 53 등 관련된 각 서비스에 대한 데이터 플레인의 모든 부분이 다음과 같습니다.

데이터 플레인은 일반적으로 복잡한 워크플로, 비즈니스 로직 및 데이터베이스 시스템을 구현하는 컨트롤 플레인에 비해 움직이는 부분이 적어 의도적으로 덜 복잡합니다. 따라서 컨트롤 플레인보다 데이터 플레인에서 장애 이벤트가 발생할 가능성이 통계적으로 낮아집니다. 데이터와 컨트롤 플레인 모두 서비스의 전반적인 운영과 성공에 기여하지만, 이를 AWS 별개의 구성 요소로 간주합니다. 이러한 분리는 성능과 가용성에 모두 도움이 됩니다.

정적 안정성

AWS서비스의 가장 중요한 복원력 특성 중 하나는 정적 AWS 안정성입니다. 이 용어가 의미하는 바는 시스템이 정적 상태에서 작동하며 장애가 발생하거나 종속성을 사용할 수 없는 경우에도 변경할 필요 없이 정상적으로 계속 작동한다는 의미입니다. 이를 위한 한 가지 방법은 서비스의 순환 종속성으로 인해 해당 서비스 중 하나가 성공적으로 복구되지 못하게 할 수 있는 것을 방지하는 것입니다. 이를 위한 또 다른 방법은 기존 상태를 유지하는 것입니다. 우리는 컨트롤 플레인이 데이터 플레인보다 실패할 확

률이 통계적으로 더 높다는 사실을 고려합니다. 데이터 플레인은 일반적으로 컨트롤 플레인으로부터 수신되는 데이터에 의존하지만, 데이터 플레인은 컨트롤 플레인이 손상된 경우에도 기존 상태를 유지하고 계속 작동합니다. 일단 프로비저닝된 리소스에 대한 데이터 플레인 액세스는 컨트롤 플레인에 종속되지 않으므로 컨트롤 플레인 손상의 영향을 받지 않습니다. 즉, 리소스를 생성, 수정 또는 삭제하는 기능이 손상되더라도 기존 리소스는 계속 사용할 수 있습니다. 따라서 AWS 데이터 플레인은 컨트롤 플레인의 손상에 대해 정적으로 안정적입니다. 다양한 유형의 종속성 장애에 대해 정적으로 안정적이도록 다양한 패턴을 구현할 수 있습니다.

정적 안정성의 예는 Amazon EC2에서 찾을 수 있습니다. EC2 인스턴스가 시작되면 데이터 센터의 물리적 서버처럼 사용할 수 있습니다. 실행 상태를 유지하거나 재부팅 후 다시 실행하기 위해서는 컨트롤 플레인 API에 의존하지 않습니다. VPC, Amazon S3 버킷 및 객체, Amazon EBS 볼륨과 같은 다른 AWS 리소스에도 동일한 속성이 적용됩니다.

정적 안정성은 서비스 AWS 설계 방식에 깊이 뿌리내리고 있는 개념이지만 고객이 사용할 수 있는 패턴이기도 합니다. 실제로 다양한 유형의 AWS 서비스를 탄력적인 방식으로 사용하기 위한 모범 사례 지침의 대부분은 프로덕션 환경에 정적 안정성을 구현하는 것입니다. 가장 신뢰할 수 있는 복구 및 완화 메커니즘은 변경을 최소화하여 복구할 수 있는 메커니즘입니다. 장애가 발생한 가용 영역에서 복구하기 위해 EC2 컨트롤 플레인에 의존하여 새 EC2 인스턴스를 시작하는 대신, 추가 용량을 미리 프로비저닝하면 정적 안정성을 확보할 수 있습니다. 따라서 복구 경로에서 컨트롤 플레인 (리소스 변경을 구현하는 API) 에 대한 종속성을 제거하면 보다 탄력적인 워크로드를 생성하는 데 도움이 됩니다. 정적 안정성, 컨트롤 플레인 및 데이터 플레인에 대한 자세한 내용은 Amazon Builders 라이브러리 문서 가용 영역을 사용한 정적 안정성을 참조하십시오.

요약

AWS인프라 내 다양한 장애 컨테이너를 활용하여 결함을 격리합니다. 핵심 인프라 장애 컨테이너는 파티션, 지역, 가용 영역, 컨트롤 플레인, 데이터 플레인입니다. 다음으로 다양한 유형의 AWS 서비스를 살펴보고, 이러한 장애 컨테이너가 설계에 어떻게 활용되는지, 그리고 이러한 장애 컨테이너를 사용하여 탄력성을 갖도록 워크로드를 설계하는 방법을 살펴보겠습니다.

AWS 서비스 유형

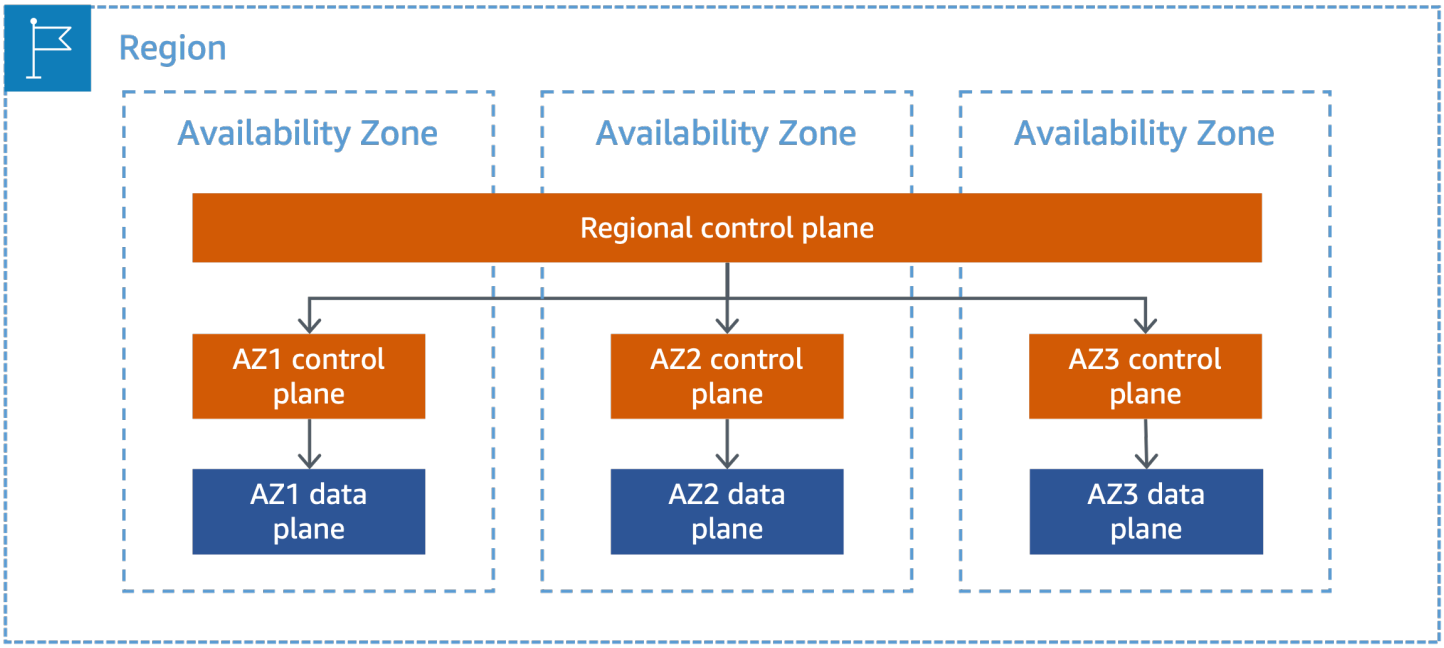
AWS 장애 격리 경계에 따라 영역, 지역, 글로벌 등 세 가지 범주의 서비스를 운영합니다. 이 섹션에서는 특정 서비스 유형의 장애가 실행 중인 워크로드에 어떤 영향을 미치는지 확인할 수 있도록 이러한 다양한 유형의 서비스가 어떻게 설계되었는지 자세히 설명합니다. AWS또한 탄력적인 방식으로 이러한 서비스를 사용하도록 워크로드를 설계하는 방법에 대한 높은 수준의 지침을 제공합니다. 글로벌 서비스의 경우, 이 문서는 서비스의 컨트롤 플레인 장애로 인한 워크로드 영향을 방지하는 데 도움이 부록 B - 에지 네트워크 글로벌 서비스 지침 되는 규범적 지침도 제공합니다. 이를 통해 단일 장애 지점으로 인한 영향을 최소화하면서 글로벌 AWS 서비스에 대한 의존도를 안전하게 유지할 수 있습니다. 부록 A - 부분 서비스 지침

주제

- 영역별 서비스
- 지역 서비스
- 글로벌 서비스

영역별 서비스

가용 영역 독립성 (AZI) AWS 을 통해 Amazon EC2 EBS 및 Amazon과 같은 영역 서비스를 제공할 수 있습니다. 영역 서비스는 리소스를 배포할 가용 영역을 지정할 수 있는 기능을 제공하는 서비스입니다. 이러한 서비스는 지역 내 각 가용 영역에서 독립적으로 작동하며, 더 중요한 것은 각 가용 영역에서도 독립적으로 장애가 발생한다는 것입니다. 즉, 한 가용 영역에 있는 서비스의 구성 요소는 다른 가용 영역의 구성 요소에 종속되지 않습니다. 영역 서비스에는 영역 데이터 플레인이 있기 때문에 이렇게 할 수 있습니다. 와 같은 일부 경우에는 인스턴스 시작과 EC2 같이 영역별로 정렬된 작업을 위한 영역 컨트롤 플레인도 서비스에 포함됩니다. EC2 AWS 또한 이러한 서비스의 경우 서비스와 쉽게 상호 작용할 수 있도록 지역 컨트롤 플레인 엔드포인트를 제공합니다. 또한 지역 제어 플레인은 지역 범위 기능을 제공할 뿐만 아니라 영역 제어 플레인 상단의 집계 및 라우팅 계층 역할도 합니다. 이는 다음 그림에 나와 있습니다.



영역별로 분리된 컨트롤 플레인과 데이터 플레인이 있는 영역 서비스.

가용 영역을 통해 고객은 단일 데이터 센터에서보다 가용성이 높고 내결함성이 뛰어나며 확장 가능한 프로덕션 워크로드를 운영할 수 있습니다. 워크로드가 여러 가용 영역을 사용하는 경우 단일 가용 영역의 물리적 인프라에 영향을 미치는 문제로부터 고객을 더 잘 격리하고 보호할 수 있습니다. 이를 통해 고객은 가용 영역 전반에 걸쳐 중복되는 서비스를 구축할 수 있으며, 올바르게 설계되면 한 가용 영역에 장애가 발생하더라도 운영 상태를 유지할 수 있습니다. 고객은 이를 활용하여 가용성이 높고 복원력이 뛰어난 AZI 워크로드를 만들 수 있습니다. 아키텍처에 AZI 구현하면 한 가용 영역의 리소스가 다른 가용 영역의 리소스와의 상호 작용을 최소화하거나 제거하므로 격리된 가용 영역 장애로부터 빠르게 복구할 수 있습니다. 이를 통해 가용 영역 간 종속성을 제거하여 가용 영역 대피를 단순화할 수 있습니다. 가용 영역 제거 메커니즘 생성에 대한 자세한 내용은 고급 다중 AZ 복원 패턴을 참조하십시오. 또한 가용 영역을 한 번에 단일 가용 영역에만 배포하거나 해당 가용 영역의 변경이 잘못된 경우 서비스에서 가용 영역을 제거하는 등 자체 서비스에 AWS 사용되는 것과 동일한 모범 사례를 따라 가용 영역을 더욱 활용할 수 있습니다.

정적 안정성은 다중 가용 영역 아키텍처에서도 중요한 개념입니다. 다중 가용 영역 아키텍처에서 대비해야 하는 장애 모드 중 하나는 가용 영역의 손실이며, 이로 인해 가용 영역의 가치가 손실될 수 있습니다. 가용 영역 손실을 처리할 수 있을 만큼 충분한 용량을 미리 프로비저닝하지 않은 경우 현재 부하로 인해 남은 용량이 과다하게 될 수 있습니다. 또한 손실된 용량을 대체하려면 사용하는 영역 서비스의 컨트롤 플레인에 의존해야 하는데, 이는 정적으로 안정적인 설계보다 안정성이 떨어질 수 있습니다. 이 경우 충분한 추가 용량을 사전 프로비저닝하면 동적으로 변경할 필요 없이 정상 운영을 계속할 수 있으므로 가용 영역과 같은 장애 도메인이 손실되어도 정적으로 안정적으로 대처할 수 있습니다.

여러 가용 영역에 배포된 Auto Scaling EC2 인스턴스 그룹을 사용하여 워크로드의 필요에 따라 동적으로 규모를 확장 및 축소할 수 있습니다. Auto Scaling은 몇 분에서 수십 분에 걸쳐 점진적으로 사용량이 변경되는 경우에 적합합니다. 하지만 새 EC2 인스턴스를 시작하는 데는 시간이 걸립니다. 특히 인스턴스에 부트스트래핑 (예: 에이전트, 애플리케이션 바이너리 또는 구성 파일 설치) 이 필요한 경우에는 더욱 그렇습니다. 이 기간 동안에는 현재 부하로 인해 남은 용량이 과다해질 수 있습니다. 또한 Auto Scaling을 통한 새 인스턴스 배포는 EC2 컨트롤 플레인에 의존합니다. 이는 단점이 있습니다. 단일 가용 영역이 손실되어도 정적으로 안정적으로 작동하려면 Auto Scaling을 사용하여 새 EC2 인스턴스를 프로비저닝하는 대신 손상된 가용 영역에서 이동된 부하를 처리할 수 있을 만큼 충분한 인스턴스를 다른 가용 영역에 미리 프로비저닝해야 합니다. 하지만 추가 용량을 사전 프로비저닝하면 추가 비용이 발생할 수 있습니다.

예를 들어 정상 운영 중에 워크로드에 3개의 가용 영역에서 고객 트래픽을 처리하기 위해 6개의 인스턴스가 필요하다고 가정해 보겠습니다. 단일 가용 영역 장애에 대해 정적 안정성을 유지하려면 각 가용 영역에 총 9개의 인스턴스를 배포해야 합니다. 가용 영역 상당의 인스턴스 중 하나에 장애가 발생하더라도 여전히 6개 남았기 때문에 장애 발생 시 새 인스턴스를 프로비저닝하고 구성할 필요 없이 고객 트래픽을 계속 제공할 수 있습니다. 이 경우 50% 의 추가 인스턴스를 실행하기 때문에 EC2 용량의 정적 안정성을 확보하려면 추가 비용이 듭니다. 리소스를 사전 프로비저닝할 수 있는 모든 서비스 (예: S3 버킷 또는 사용자 사전 프로비저닝) 에 추가 비용이 발생하는 것은 아닙니다. 원하는 워크로드 복구 시간을 초과할 위험과 정적 안정성 구현의 절충점을 비교해야 합니다.

AWS Local Zones 및 Outposts는 일부 AWS 서비스의 데이터 플레인을 최종 사용자에게 더 가깝게 제공합니다. 이러한 서비스의 컨트롤 플레인은 상위 지역에 있습니다. Local Zone 또는 Outposts 인스턴스는 로컬 영역 또는 Outposts 서브넷을 생성한 가용 EC2 영역과 같은 영역 서비스에 EBS 대한 컨트롤 플레인 종속성을 갖게 됩니다. 또한 Elastic Load Balancing (ELB), 보안 그룹, 아마존 엘라스틱 쿠버네티스 서비스 (Amazon) 에서 관리하는 쿠버네티스 컨트롤 플레인 EKS (사용하는 경우) 과 같은 리전 서비스에 대한 리전 컨트롤 플레인에도 종속됩니다. EKS Outposts와 관련된 추가 정보는 설명서와 지원 및 유지 관리를 참조하십시오. FAQ Local Zones 또는 Outposts를 사용할 때 정적 안정성을 구현하면 상위 지역에 대한 네트워크 연결 중단이나 컨트롤 플레인 장애에 대한 복원력을 개선할 수 있습니다.

지역 서비스

지역 서비스는 여러 가용 영역을 기반으로 AWS 구축된 서비스이므로 고객이 영역 서비스를 최대한 활용하는 방법을 고민하지 않아도 됩니다. 여러 가용 영역에 배포된 서비스를 논리적으로 그룹화하여 고객에게 단일 지역 엔드포인트를 제공합니다. 아마존 SQS 및 아마존 DynamoDB는 지역 서비스의 예입니다. 이들은 가용 영역의 독립성과 중복성을 사용하여 가용성 및 내구성 위험 범주로 인프라 장애를 최소화합니다. 예를 들어 Amazon S3는 요청과 데이터를 여러 가용 영역에 분산하고 가용 영역 장애로부터 자동으로 복구하도록 설계되었습니다. 하지만 서비스의 리전 엔드포인트와만 상호 작용합니다.

AWS 대부분의 고객은 영역 서비스를 사용하는 지역 서비스 또는 다중 AZ 아키텍처를 사용하여 단일 지역에서 복원력 목표를 달성할 수 있다고 생각합니다. 그러나 일부 워크로드에는 추가 중복성이 필요할 수 있으며, 이를 분리하여 HA 또는 비즈니스 연속성을 위한 다중 지역 AWS 리전 아키텍처를 만들 수 있습니다. 물리적/논리적 분리를 통해 둘 사이의 상호 AWS 리전 관련된 장애를 방지할 수 있습니다. 즉, EC2 고객으로서 가용 영역 전체에 배포하여 가용 영역 격리의 이점을 누릴 수 있는 경우와 마찬가지로 여러 지역에 배포하면 지역 서비스에서도 동일한 이점을 얻을 수 있습니다. 이를 위해서는 애플리케이션에 다중 지역 아키텍처를 구현해야 하며, 이를 통해 지역 서비스의 장애에 대한 복원력을 확보할 수 있습니다.

그러나 다중 지역 아키텍처의 이점을 달성하는 것은 어려울 수 있습니다. 응용 프로그램 수준에서 어떤 것도 취소하지 않으면서 지역적 격리를 활용하려면 세심한 작업이 필요합니다. 예를 들어, 지역 간에 애플리케이션을 페일오버하는 경우 각 지역의 애플리케이션 스택을 엄격하게 구분하고, 모든 애플리케이션 종속성을 파악하고, 애플리케이션의 모든 부분을 함께 페일오버해야 합니다. 애플리케이션 간 종속성이 많은 복잡한 마이크로서비스 기반 아키텍처로 이를 달성하려면 많은 엔지니어링 및 비즈니스 팀 간의 계획과 조정이 필요합니다. 개별 워크로드가 자체적으로 페일오버 결정을 내리도록 허용하면 조정이 덜 복잡해지지만 단일 지역 내에서와 비교하여 지역 간에 발생하는 지연 시간의 현저한 차이로 인해 모달 동작이 발생합니다.

AWS 은 현재 지역 간 동기식 복제 기능을 제공하지 않습니다. 지역 간에 비동기적으로 복제된 데이터스토어 (에서 제공 AWS) 를 사용하는 경우 지역 간에 애플리케이션을 페일오버하면 데이터 손실이나 불일치가 발생할 수 있습니다. 발생할 수 있는 불일치를 줄이려면 신뢰할 수 있고 워크로드 포트폴리오의 여러 데이터 저장소에서 운영해야 하는 신뢰할 수 있는 데이터 조정 프로세스가 필요합니다. 그렇지 않으면 데이터 손실을 감수할 수 있어야 합니다. 마지막으로, 페일오버를 연습하여 필요할 때 제대로 작동하는지 확인해야 합니다. 페일오버를 실행하기 위해 애플리케이션을 지역 간에 정기적으로 교체하려면 상당한 시간과 리소스가 투자됩니다. 여러 지역에서 동시에 실행되는 애플리케이션을 지원하기 위해 여러 지역에서 동기식으로 복제된 데이터스토어를 사용하기로 결정한 경우, 100마일 또는 1000마일에 걸친 이러한 데이터베이스의 성능 특성 및 지연 시간은 단일 지역에서 운영되는 데이터베이스와는 매우 다릅니다. 이를 위해서는 이 동작을 고려하여 처음부터 애플리케이션 스택을 계획해야 합니다. 또한 두 지역의 가용성이 크게 종속되어 워크로드의 복원력이 저하될 수 있습니다.

글로벌 서비스

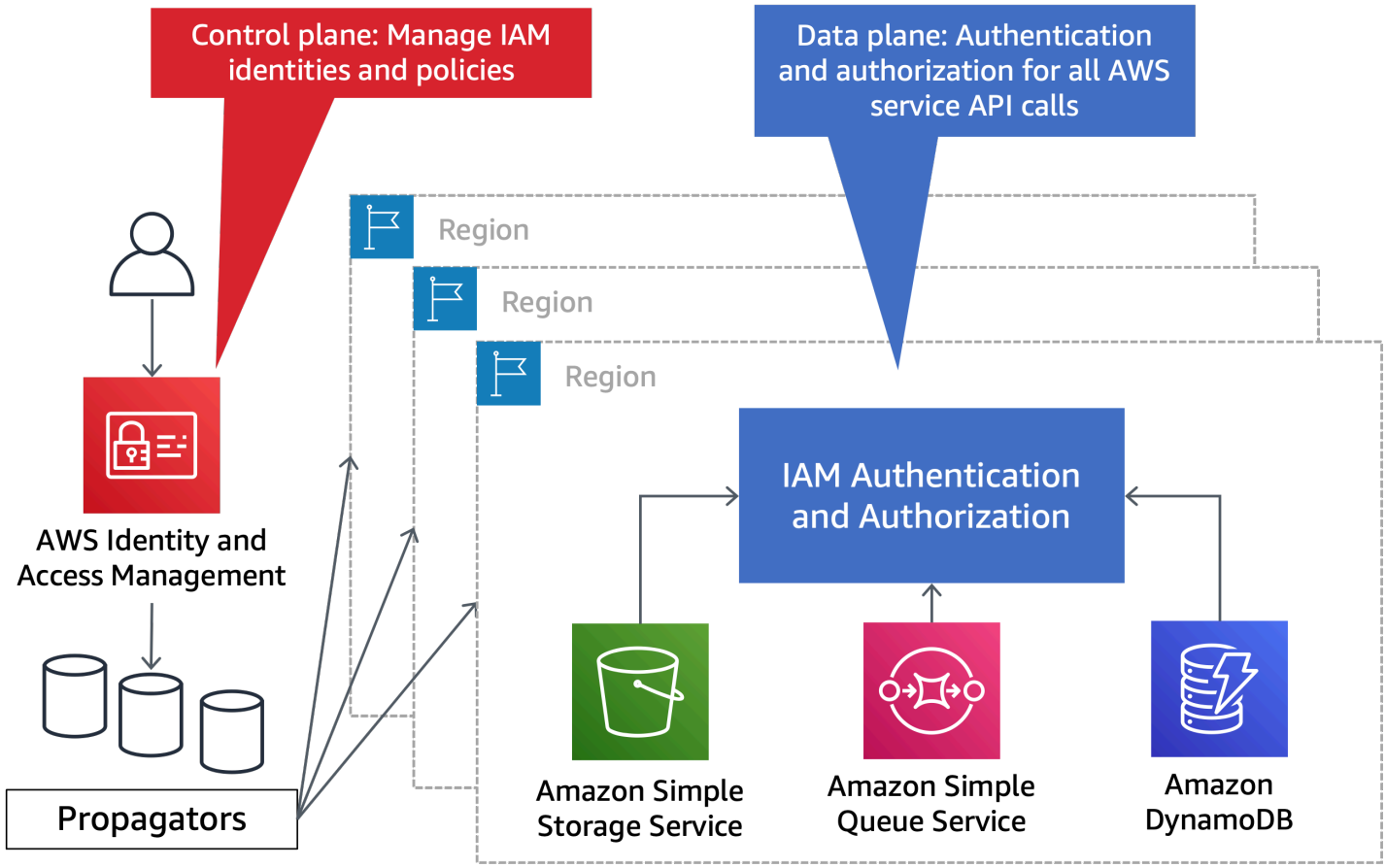
지역 및 영역 AWS 서비스 외에도 컨트롤 플레인과 데이터 플레인이 각 지역에 독립적으로 존재하지 않는 소수의 AWS 서비스가 있습니다. 리소스가 지역별로 한정되지 않기 때문에 일반적으로 글로벌 리소스라고 합니다. 글로벌 AWS 서비스는 여전히 정적 안정성을 확보하기 위해 컨트롤 플레인과 데이터 플레인을 분리하는 기존의 AWS 설계 패턴을 따릅니다. 대부분의 글로벌 서비스가 크게 다른 점은 컨트롤 플레인이 한 AWS 리전곳에서 호스팅되는 반면 데이터 플레인은 전 세계에 분산되어 있다는 점입

니다. 세 가지 유형의 글로벌 서비스가 있으며, 선택한 구성에 따라 글로벌처럼 보일 수 있는 서비스 집합도 있습니다.

다음 섹션에서는 각 글로벌 서비스 유형과 해당 제어 플레인과 데이터 플레인이 분리되는 방식을 설명합니다. 이 정보를 사용하면 글로벌 서비스 컨트롤 플레인에 의존하지 않고도 신뢰할 수 있는 고가용성 (HA) 및 재해 복구 (DR) 메커니즘을 구축하는 방법을 안내할 수 있습니다. 이 접근 방식은 글로벌 서비스 컨트롤 플레인이 호스팅되는 지역과 다른 지역에서 운영하는 경우에도 아키텍처의 단일 장애 지점을 제거하고 지역 간 잠재적 영향을 방지하는 데 도움이 됩니다. 또한 글로벌 서비스 컨트롤 플레인에 의존하지 않는 페일오버 메커니즘을 안전하게 구현하는 데도 도움이 됩니다.

파티션별로 고유한 글로벌 서비스

일부 글로벌 AWS 서비스는 각 파티션에 존재합니다 (이 백서에서는 파티션 서비스라고 함). 파티셔널 서비스는 컨트롤 플레인을 하나로 제공합니다. AWS 리전 AWS Network Manager와 같은 일부 파티션 서비스는 컨트롤 플레인 전용이며 다른 서비스의 데이터 플레인을 오케스트레이션합니다. 예를 들어 다른 파티셔널 서비스에는 파티션의 모든 영역에 격리되어 분산되는 자체 데이터 플레인이 있습니다. IAM AWS 리전 파티션 서비스에 장애가 발생해도 다른 파티션에는 영향을 주지 않습니다. aws파티션에서 IAM 서비스의 컨트롤 플레인은 us-east-1 지역에 있으며 파티션의 각 리전에는 분리된 데이터 플레인이 있습니다. 또한 파티셔널 서비스는 및 aws-cn 파티션에 독립적인 컨트롤 플레인과 데이터 플레인을 aws-us-gov 갖추고 있습니다. 컨트롤 플레인과 데이터 플레인의 분리는 다음 다이어그램에 나와 있습니다. IAM



IAM단일 컨트롤 플레인과 지역화된 데이터 플레인이 있습니다.

다음은 파티션 서비스와 파티션 내 해당 컨트롤 플레인 위치입니다. aws

- AWS IAM (us-east-1)
- AWS Organizations (us-east-1)
- AWS 계정 관리 () us-east-1
- Route 53 애플리케이션 복구 컨트롤러 (ARCus-west-2) () - 이 서비스는 aws 파티션에만 있습니다.
- AWS 네트워크 관리자 (us-west-2)
- 루트 53 프라이빗 DNS (us-east-1)

이러한 서비스 컨트롤 플레인 중 가용성에 영향을 미치는 이벤트가 발생하는 경우 이러한 서비스에서 제공하는 CRUDL -type 작업을 사용하지 못할 수 있습니다. 따라서 복구 전략이 이러한 작업에 종속되어 있는 경우 컨트롤 플레인 또는 컨트롤 플레인을 호스팅하는 지역에 대한 가용성에 영향을 미치면 복

구 성공 가능성이 낮아집니다. 부록 A - 부분 서비스 지침복구 중에 글로벌 서비스 컨트롤 플레인에 대한 종속성을 제거하기 위한 전략을 제공합니다.

> **권장 사항**
>
> 복구 경로에서 파티션 서비스의 컨트롤 플레인에 의존하지 마십시오. 대신 이러한 서비스의 데이터 플레인 운영에 의존하세요. 파티셔널 서비스를 설계하는 방법에 부록 A - 부분 서비스 지침 대한 자세한 내용은 을 참조하십시오.

에지 네트워크의 글로벌 서비스

차세대 글로벌 AWS 서비스 세트는 aws 파티션에 컨트롤 플레인을 두고 글로벌 PoP (AWS 리전 PoS) 인프라에서 데이터 플레인을 호스팅합니다 (아마도 그럴 수도 있음). 호스팅된 데이터 플레인은 인터넷뿐만 아니라 모든 파티션의 리소스에서 액세스할 PoPs 수 있습니다. 예를 들어 Route 53은 리전에서 컨트롤 플레인을 운영하지만 데이터 플레인은 PoPs 리전 세계 수백 개 us-east-1 지역과 각 지역 AWS 리전 (지역 DNS 내 Route 53 퍼블릭 및 프라이빗 지원) 에 분산되어 있습니다. Route 53 상태 확인도 데이터 플레인의 일부이며 aws 파티션에 AWS 리전 있는 8개부터 수행됩니다. 클라이언트는 AWS 가상 사설 클라우드 (VPC) 와 같은 GovCloud 다른 파티션을 포함하여 인터넷상의 어느 곳에서나 Route 53 퍼블릭 호스팅 영역을 DNS 사용하여 문제를 해결할 수 있습니다. 다음은 글로벌 에지 네트워크 서비스와 aws 파티션 내 해당 컨트롤 플레인 위치입니다.

- Route 53 퍼블릭 DNS (us-east-1)
- 아마존 CloudFront (us-east-1)
- AWS WAF 클래식 포 CloudFront (us-east-1)
- AWS WAF 용 CloudFront (us-east-1)
- Amazon 인증서 관리자 (ACM) 용 CloudFront (us-east-1)
- AWS글로벌 액셀러레이터 (AGA) (us-west-2)
- AWS Shield Advanced (us-east-1)

EC2인스턴스 또는 엘라스틱 IP 주소에 대한 AGA 상태 확인을 사용하는 경우 Route 53 상태 확인을 사용합니다. AGA상태 확인의 생성 또는 업데이트는 Route 53 컨트롤 플레인에 따라 달라집니다us-east-1. AGA상태 점검 실행에는 Route 53 상태 점검 데이터 플레인이 사용됩니다.

이러한 서비스의 컨트롤 플레인을 호스팅하는 지역에 영향을 미치는 장애 또는 컨트롤 플레인 자체에 영향을 미치는 장애가 발생하는 경우 이러한 서비스에서 제공하는 CRUDL -type 작업을 사용하지 못할

수 있습니다. 복구 전략에서 이러한 작업에 의존했다면 이러한 서비스의 데이터 플레인에만 의존하는 경우보다 해당 전략의 성공 가능성이 낮을 수 있습니다.

> **권장 사항**
>
> 복구 경로에서 에지 네트워크 서비스의 컨트롤 플레인에 의존하지 마십시오. 대신 이러한 서비스의 데이터 플레인 운영에 의존하십시오. 에지 네트워크에서 글로벌 서비스를 설계하는 방법에 부록 B - 에지 네트워크 글로벌 서비스 지침 대한 자세한 내용은 을 참조하십시오.

글로벌 단일 지역 운영

최종 카테고리는 이전 카테고리처럼 전체 서비스가 아닌 글로벌 영향 범위를 갖는 서비스 내의 특정 컨트롤 플레인 운영으로 구성됩니다. 지정한 지역의 영역 및 지역 서비스와 상호 작용하는 동안 특정 작업에는 리소스가 위치한 곳과는 다른 단일 지역에 대한 근본적인 종속성이 있습니다. 이러한 서비스는 단일 지역에서만 제공되는 서비스와는 다릅니다. 해당 서비스 목록은 을 부록 C - 단일 지역 서비스 참조하십시오.

기본 글로벌 종속성에 영향을 미치는 오류가 발생하는 경우 종속 작업의 CRUDL -type 작업을 사용하지 못할 수 있습니다. 복구 전략에서 이러한 작업에 종속된 경우 이러한 서비스의 데이터 영역에만 의존하는 경우보다 해당 전략의 성공 가능성이 낮을 수 있습니다. 복구 전략을 위해 이러한 작업에 종속되지 않도록 해야 합니다.

다음은 글로벌 범위를 가진 다른 서비스가 의존할 수 있는 서비스 목록입니다.

- Route 53

  일부 AWS 서비스는 리소스별 DNS 이름을 제공하는 리소스를 생성합니다. 예를 들어 Elastic Load Balancer (ELB) 를 프로비저닝하면 서비스가 Route 53에서 에 대한 공개 DNS 기록과 상태 확인을 생성합니다. ELB 이는 Route 53 컨트롤 플레인에 의존합니다. `us-east-1` 사용하는 다른 서비스도 컨트롤 플레인 워크플로의 일부로 Route 53 레코드를 프로비저닝하거나ELB, 공개 Route 53 DNS 레코드를 생성하거나, Route 53 상태 확인을 생성해야 할 수 있습니다. 예를 들어, 아마존 API 게이트웨이 REST API 리소스, 아마존 관계형 데이터베이스 서비스 (Amazon) 데이터베이스 또는 RDS OpenSearch 아마존 서비스 도메인을 프로비저닝하면 모두 Route 53에 레코드가 DNS 생성됩니다. 다음은 Route 53 컨트롤 플레인을 사용하여 DNS 레코드, 호스팅 영역을 생성, 업데이트 또는 삭제하거나 Route 53 상태 확인을 생성하는 `us-east-1` 데 컨트롤 플레인이 의존하는 서비스 목록입니다. 이 목록은 완전한 것이 아니며, 리소스를 생성, 업데이트 또는 삭제하기 위한 컨트롤 플레인 작업이 Route 53 컨트롤 플레인에 따라 달라지는 가장 일반적으로 사용되는 서비스 중 일부를 강조하기 위한 것입니다.

- 아마존 API 게이트웨이 REST 및 HTTP APIs
- 아마존 RDS 인스턴스
- 아마존 Aurora 데이터베이스
- 아마존 ELB 로드 밸런서
- AWS PrivateLink VPC엔드포인트
- AWS Lambda URLs
- 아마존 ElastiCache
- 아마존 OpenSearch 서비스
- 아마존 CloudFront
- Amazon MemoryDB
- Amazon Neptune
- 아마존 다이나모DB 액셀러레이터 () DAX
- AGA
- DNS기반 서비스 검색 (Route 53을 관리하는 AWS Cloud Map API 데 사용ECS) 을 지원하는 Amazon Elastic 컨테이너 서비스 (AmazonDNS)
- Amazon EKS 쿠버네티스 컨트롤 플레인

  EC2인스턴스 호스트 이름에 대한 VPC DNS 서비스는 각각 독립적으로 AWS 리전 존재하며 Route 53 컨트롤 플레인에 의존하지 않는다는 점에 유의해야 합니다. ,, `ip-10-0-10.ec2.internal` `ip-10-0-1-5.compute.us-west-2.compute.internali-0123456789abcdef.ec2.internal`, 등과 같이 VPC DNS 서비스의 EC2 인스턴스에 대해 AWS 생성되는 레코드는 Route 53 컨트롤 플레인을 사용하지 않습니다. `i-0123456789abcdef.us-west-2.compute.internal` `us-east-1`

  > **권장 사항**
  >
  > 복구 경로에서 Route 53 리소스 레코드, 호스팅 영역 또는 상태 확인의 생성, 업데이트 또는 삭제가 필요한 리소스의 생성, 업데이트 또는 삭제에만 의존하지 마십시오. 예를 들어 복구 경로에서 Route 53 컨트롤 플레인에 대한 종속성을 방지하기 위해 이러한 리소스를 사전 프로비저닝하십시오. ELBs

- Amazon S3

다음 Amazon S3 컨트롤 플레인 작업은 기본적으로 us-east-1 aws 파티션에 종속되어 있습니다. Amazon S3 또는 기타 서비스에 영향을 미치는 장애로 인해 다른 지역에서 이러한 컨트롤 플레인 작업이 손상될 수 있습니다. us-east-1

```
PutBucketCors
DeleteBucketCors
PutAccelerateConfiguration
PutBucketRequestPayment
PutBucketObjectLockConfiguration
PutBucketTagging
DeleteBucketTagging
PutBucketReplication
DeleteBucketReplication
PutBucketEncryption
DeleteBucketEncryption
PutBucketLifecycle
DeleteBucketLifecycle
PutBucketNotification
PutBucketLogging
DeleteBucketLogging
PutBucketVersioning
PutBucketPolicy
DeleteBucketPolicy
PutBucketOwnershipControls
DeleteBucketOwnershipControls
PutBucketAcl
PutBucketPublicAccessBlock
DeleteBucketPublicAccessBlock
```

Amazon S3 다중 지역 액세스 포인트 (MRAP) 의 컨트롤 플레인은 해당 지역을 직접 MRAPs 대상으로 생성, 업데이트 또는 삭제를 요청하는 요청에서만 us-west-2 호스팅됩니다. MRAP또한 컨트롤 플레인에는 콘텐츠를 제공하도록 구성된 각 지역의 AGA inus-west-2, Route 53 내부 및 ACM 각 리전에 대한 기본 종속성이 있습니다. us-east-1 MRAP 복구 경로나 자체 시스템의 데이터 플레인에 있는 MRAP 컨트롤 플레인의 가용성에 의존해서는 안 됩니다. 이는 에 있는 각 버킷의 액티브 또는 패시브 라우팅 상태를 지정하는 데 사용되는 MRAP페일오버 컨트롤과는 다릅니다. MRAP APIs 이들은 5개로 AWS 리전 호스팅되며 서비스의 데이터 플레인을 사용하여 트래픽을 효과적으로 전환하는 데 사용할 수 있습니다.

또한 Amazon S3 버킷 이름은 전 세계적으로 `CreateBucket` 고유하며 `DeleteBucket` APIsus-east-1, 호출이 버킷을 생성하려는 특정 지역으로 전달되더라도 aws 파티션에 대한 모든 API 호출은 이름의 고유성을 보장하기 위해 파티션에서 이를 기반으로 합니다. 마지막으로, 중요한 버킷 생성 워크플로가 있는 경우 버킷 이름의 특정 철자, 특히 식별 가능한 패턴을 따르는 버킷 이름의 사용 가능 여부에 의존해서는 안 됩니다.

> **권장 사항**
>
> 복구 경로의 일부로 S3 버킷을 삭제 또는 새로 만들거나 S3 버킷 구성을 업데이트하는 데 의존하지 마십시오. 필요한 모든 S3 버킷을 필요한 구성으로 사전 프로비저닝하여 장애를 복구하기 위해 변경할 필요가 없도록 하십시오. 이 접근 방식은 MRAPs 에도 적용됩니다.

- CloudFront

  Amazon API Gateway는 엣지에 최적화된 API 엔드포인트를 제공합니다. 이러한 엔드포인트 생성은 게이트웨이 엔드포인트 앞에 us-east-1 배포를 생성하는 CloudFront 컨트롤 플레인에 따라 달라집니다.

  > **권장 사항**
  >
  > 복구 경로의 일부로 엣지에 최적화된 API 게이트웨이 엔드포인트를 새로 생성하는 것에 의존하지 마십시오. 필요한 모든 게이트웨이 엔드포인트를 사전 프로비저닝하십시오. API

  이 섹션에서 설명하는 모든 종속성은 데이터 플레인 작업이 아니라 컨트롤 플레인 작업입니다. 워크로드가 정적으로 안정되도록 구성된 경우 이러한 종속성이 복구 경로에 영향을 주지 않아야 합니다. 정적 안정성을 구현하려면 추가 작업이나 서비스가 필요하다는 점을 염두에 두세요.

기본 글로벌 엔드포인트를 사용하는 서비스

일부 경우에는 AWS 서비스가 AWS 보안 토큰 서비스 (AWS STS) 와 같은 기본 글로벌 엔드포인트를 제공합니다. 다른 서비스는 이 기본 글로벌 엔드포인트를 기본 구성으로 사용할 수 있습니다. 즉, 사용 중인 지역 서비스가 단일 AWS 리전지역에 대한 글로벌 종속성을 가질 수 있습니다. 다음 세부 정보는 기본 글로벌 엔드포인트에서 의도하지 않은 종속성을 제거하여 지역적 방식으로 서비스를 사용하는 데 도움이 되는 방법을 설명합니다.

AWS STS: STS 는 IAM 사용자 또는 인증한 사용자 (페더레이션 사용자) 를 위해 권한이 제한된 임시 자격 증명을 요청할 수 있는 웹 서비스입니다. STS AWS 소프트웨어 개발 키트 (SDK) 및 명령줄 인터페이스 () 에서의 사용 기본값은 입니다. CLI `us-east-1` 이 STS 서비스는 지역별 엔드포인트도 제공합니다. 이러한 엔드포인트는 기본적으로 활성화되며, 지역에서도 기본적으로 활성화됩니다. AWS STS지역화된 엔드포인트를 SDK 구성하거나 CLI 다음 지침에 따라 언제든지 이러한 이점을 활용할 수 있습니다. 또한 SigV4A를 사용하려면 지역 엔드포인트에서 요청한 임시 자격 증명이 필요합니다. STS 이 작업에는 글로벌 STS 엔드포인트를 사용할 수 없습니다.

> **권장 사항**
>
> 지역 STS 엔드포인트를 사용하도록 SDK 및 CLI 구성을 업데이트하십시오.

보안 어설션 마크업 언어 (SAML) 로그인: SAML 서비스는 어디에나 존재합니다. AWS 리전이 서비스를 사용하려면 적절한 지역 SAML 엔드포인트 (예: https://us-west-2.signin.aws.amazon.com/saml) 를 선택하십시오. 지역 엔드포인트를 사용하려면 신뢰 정책 및 ID 공급자 (IdP) 의 구성을 업데이트해야 합니다. 자세한 내용은 AWS SAML설명서를 참조하십시오.

호스팅되는 IdP를 사용하는 경우 장애 이벤트 중에 IdP가 영향을 받을 위험이 있습니다. AWS AWS 이로 인해 IdP 구성을 업데이트할 수 없거나 완전히 페더레이션하지 못할 수 있습니다. IdP가 손상되거나 사용할 수 없는 경우에 대비하여 “브레이크글라스” 사용자를 사전 프로비저닝해야 합니다. 정적으로 안정적인 방식으로 Break-Glass 사용자를 생성하는 방법에 부록 A - 부분 서비스 지침 대한 자세한 내용은 를 참조하십시오.

> **권장 사항**
>
> 여러 지역의 로그인을 IAM 허용하도록 역할 신뢰 정책을 업데이트하세요. SAML 장애가 발생한 경우 선호 엔드포인트가 손상된 경우 다른 지역 SAML 엔드포인트를 사용하도록 IdP 구성을 업데이트하십시오. IdP가 손상되었거나 사용할 수 없는 경우에 대비하여 브레이크-글래스 사용자를 생성하세요.

AWS IAMIdentity Center: Identity Center는 고객 및 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 중앙에서 쉽게 관리할 수 있는 클라우드 기반 서비스입니다. AWS 계정 Identity Center는 선택한 단일 지역에 배포해야 합니다. 하지만 서비스의 기본 동작은 에서 호스팅되는 글로벌 SAML 엔드포인트 (https://signin.aws.amazon.com/saml) 를 사용하는 `us-east-1` 것입니다. Identity Center를 다른 AWS 리전곳에 배포한 경우 Identity Center 배포와 동일한 지역 콘솔 엔드포인트를 대상으로 하도록 모든 권한 세트의 릴레이 상태를 URL 업데이트해야 합니다. 예를 들어 Identity Center를 에 us-

west-2 배포한 경우 https://us-west-2.console.aws.amazon.com 을 사용하도록 권한 집합의 릴레이 상태를 업데이트해야 합니다. 이렇게 하면 Identity Center 배포에 대한 us-east-1 종속성이 모두 제거됩니다.

또한 IAM Identity Center는 단일 지역에만 배포할 수 있으므로 배포에 장애가 발생할 경우를 대비하여 "브레이크글라스" 사용자를 미리 프로비전해야 합니다. 정적으로 안정적인 방식으로 Break-Glass 사용자를 생성하는 방법에 부록 A - 부분 서비스 지침 대한 자세한 내용은 를 참조하십시오.

> 권장 사항
>
> 서비스가 배포된 지역과 일치하도록 IAM Identity Center에서 권한 URL 집합의 릴레이 상태를 설정하십시오. IAMIdentity Center 배포를 사용할 수 없는 경우를 대비하여 유용한 사용자를 생성하십시오.

Amazon S3 스토리지 렌즈: 스토리지 렌즈는 라는 기본 대시보드를 제공합니다 default-account-dashboard. 대시보드 구성 및 관련 지표는 에 저장됩니다us-east-1. 대시보드 구성 및 지표 데이터의 홈 지역을 지정하여 다른 지역에 추가 대시보드를 생성할 수 있습니다.

> 권장 사항
>
> 의 서비스에 영향을 미치는 장애 발생 중에 기본 S3 Storage Lens 대시보드의 데이터가 필요한 경우 대체 홈 지역에 us-east-1 추가 대시보드를 생성하십시오. 추가 지역에서 생성한 다른 사용자 지정 대시보드를 복제할 수도 있습니다.

글로벌 서비스 요약

글로벌 서비스를 위한 데이터 플레인은 지역 AWS 서비스와 유사한 격리 및 독립 원칙을 적용합니다. 한 지역의 데이터 플레인에 영향을 미치는 장애가 다른 AWS 리전지역의 IAM 데이터 플레인 작동에는 영향을 미치지 않습니다. IAM 마찬가지로 PoP에서 Route 53의 데이터 플레인에 영향을 미치는 장애는 나머지 Route 53 데이터 플레인의 작동에는 영향을 미치지 않습니다. PoPs 따라서 컨트롤 플레인이 운영되는 지역 또는 컨트롤 플레인 자체에 영향을 미치는 서비스 가용성 이벤트를 고려해야 합니다. 각 글로벌 서비스에는 컨트롤 플레인이 하나뿐이므로 해당 컨트롤 플레인에 영향을 미치는 장애가 발생할 경우 CRUDL -type 작업 (서비스를 직접 사용하는 대신 서비스를 설정하거나 구성하는 데 일반적으로 사용되는 구성 작업) 에 지역 간 영향을 미칠 수 있습니다.

글로벌 서비스를 탄력적으로 사용하도록 워크로드를 설계하는 가장 효과적인 방법은 정적 안정성을 사용하는 것입니다. 장애 시나리오에서는 영향을 완화하거나 다른 위치로의 장애 조치를 취하기 위해

컨트롤 플레인을 사용하여 변경할 필요가 없도록 워크로드를 설계하십시오. 컨트롤 플레인 종속성을 제거하고 단일 장애 지점을 제거하기 위해 이러한 유형의 글로벌 서비스를 활용하는 방법에 대한 규범적 지침은 및 을 참조하십시오. 부록 A - 부분 서비스 지침 부록 B - 에지 네트워크 글로벌 서비스 지침 복구를 위해 컨트롤 플레인 작업의 데이터가 필요한 경우 AWS Systems Manager Parameter Store (SSMParameter Store) 파라미터, DynamoDB 테이블 또는 S3 버킷과 같은 데이터 플레인을 통해 액세스할 수 있는 데이터 스토어에 이 데이터를 캐시하십시오. 중복성을 위해 해당 데이터를 추가 지역에 저장하도록 선택할 수도 있습니다. 예를 들어, Route 53 애플리케이션 복구 컨트롤러 (ARC) 의 모범 사례에 따라 5개의 지역 클러스터 엔드포인트를 하드코딩하거나 북마크해야 합니다. 장애 이벤트 중에는 매우 안정적인 데이터 플레인 클러스터에서 호스팅되지 않는 Route 53 ARC API 작업을 비롯한 일부 API 작업에 액세스하지 못할 수 있습니다. `DescribeCluster`API작업을 사용하여 Route 53 ARC 클러스터의 엔드포인트를 나열할 수 있습니다.

다음은 글로벌 서비스의 컨트롤 플레인에 대한 종속성을 유발하는 가장 일반적인 구성 오류 또는 안티패턴 중 일부를 요약한 것입니다.

- Route 53 레코드를 변경하여 A 레코드 값을 업데이트하거나 가중치가 적용된 레코드 세트의 가중치를 변경하여 장애 조치를 수행합니다.
- 장애 조치 중에 IAM 역할 및 정책을 포함한 IAM 리소스 생성 또는 업데이트. 이는 일반적으로 의도적인 것은 아니지만 테스트되지 않은 장애 조치 계획의 결과일 수 있습니다.
- 장애 발생 시 운영자가 운영 환경에 액세스할 수 있도록 IAM Identity Center를 활용합니다.
- IAMIdentity Center를 다른 지역에 배포한 `us-east-1` 경우 기본 ID 센터 구성을 사용하여 콘솔을 활용하십시오.
- AGA트래픽 다이얼 가중치를 변경하여 지역별 장애 조치를 수동으로 수행합니다.
- 손상된 오리진에서 장애가 발생되지 않도록 CloudFront 배포의 오리진 구성을 업데이트합니다.
- Route 53에서의 DNS 레코드 생성에 따라 장애 발생 시 ELBs 및 RDS 인스턴스와 같은 재해 복구 (DR) 리소스를 프로비저닝합니다.

다음은 이전의 일반적인 안티패턴을 방지하는 데 도움이 되는 탄력적인 방식으로 글로벌 서비스를 사용하기 위해 이 섹션에 제공된 권장 사항을 요약한 것입니다.

> **권장 사항 요약**
>
> 복구 경로에서 파티션 서비스의 컨트롤 플레인에 의존하지 마십시오. 대신 이러한 서비스의 데이터 플레인 운영에 의존하세요. 파티셔널 서비스를 설계하는 방법에 부록 A - 부분 서비스 지침 대한 자세한 내용은 을 참조하십시오.

복구 경로에서 에지 네트워크 서비스의 컨트롤 플레인에 의존하지 마십시오. 대신 이러한 서비스의 데이터 플레인 운영에 의존하십시오. 에지 네트워크에서 글로벌 서비스를 설계하는 방법에 부록 B - 에지 네트워크 글로벌 서비스 지침 대한 자세한 내용은 을 참조하십시오.
복구 경로에서 Route 53 리소스 레코드, 호스팅 영역 또는 상태 확인의 생성, 업데이트 또는 삭제가 필요한 리소스의 생성, 업데이트 또는 삭제에만 의존하지 마십시오. 예를 들어 복구 경로에서 Route 53 컨트롤 플레인에 대한 종속성을 방지하기 위해 이러한 리소스를 사전 프로비저닝하십시오. ELBs
복구 경로의 일부로 S3 버킷을 삭제 또는 새로 만들거나 S3 버킷 구성을 업데이트하는 데 의존하지 마십시오. 필요한 모든 S3 버킷을 필요한 구성으로 사전 프로비저닝하여 장애를 복구하기 위해 변경할 필요가 없도록 하십시오. 이 접근 방식은 MRAPs 에도 적용됩니다.
복구 경로의 일부로 엣지에 최적화된 API 게이트웨이 엔드포인트를 새로 만드는 것에 의존하지 마십시오. 필요한 모든 게이트웨이 엔드포인트를 사전 프로비저닝하십시오. API
지역 STS 엔드포인트를 사용하도록 SDK 및 CLI 구성을 업데이트하십시오.
여러 지역의 SAML 로그인을 허용하도록 IAM 역할 신뢰 정책을 업데이트하세요. 장애가 발생한 경우 선호 엔드포인트가 손상된 경우 다른 지역 SAML 엔드포인트를 사용하도록 IdP 구성을 업데이트하십시오. IdP가 손상되었거나 사용할 수 없는 경우를 대비하여 브레이크글래스 사용자를 생성하세요.
서비스가 배포된 지역과 일치하도록 IAM Identity Center에서 권한 URL 집합의 릴레이 상태를 설정하십시오. Identity Center 배포를 사용할 수 없는 경우를 대비하여 유용한 사용자를 생성하십시오.
에서 서비스에 영향을 미치는 장애 발생 중에 기본 S3 Storage Lens 대시보드의 데이터가 필요한 경우 대체 `us-east-1` 홈 지역에 추가 대시보드를 생성하십시오. 추가 지역에서 생성한 다른 사용자 지정 대시보드를 복제할 수도 있습니다.

결론

AWS장애 격리 경계를 위한 여러 가지 다른 구조를 제공합니다. 컨트롤 플레인 장애 시 워크로드의 복구 능력과 워크로드에 미치는 잠재적 영향뿐만 아니라 영역, 지역 및 글로벌 서비스를 위한 설계 방법을 고려해야 합니다. 정적 안정성은 서비스를 사용할 AWS 때 컨트롤 플레인 종속성을 피하고 안정적이고 탄력적인 HA 및 DR 메커니즘을 만들 수 있는 주요 방법 중 하나입니다.

부록 A - 부분 서비스 지침

분할 서비스의 경우 AWS 서비스 컨트롤 플레인 장애 시 워크로드의 레질리언스를 유지하려면 정적 안정성을 구현해야 합니다. 다음은 부분 서비스에 대한 종속성을 고려하는 방법과 컨트롤 플레인 장애 시 작동할 수 있는 것과 작동하지 않을 수 있는 사항에 대한 규범적인 지침을 제공합니다.

AWS Identity and Access Management(IAM)

AWS Identity and Access Management(IAM) 컨트롤 플레인은 모든 퍼블릭 IAM API (액세스 어드바이저 포함, 액세스 분석기 또는 IAM 역할 애니웨어는 제외) 로 구성됩니다. 여기에는`CreateRole`, `AttachRolePolicy` `ChangePasswordUpdateSAMLProvider`, 및 같은 동작이 포함됩니다`UpdateLoginProfile`. IAM 데이터 플레인은 각각의 IAM 보안 주체에 대한 인증 및 권한 부여를 제공합니다. AWS 리전 컨트롤 플레인 장애 중에는 IAM에 대한 CRUDL 유형 작업이 작동하지 않을 수 있지만 기존 보안 주체에 대한 인증 및 권한 부여는 계속 작동합니다. STS는 IAM과 별개이며 IAM 컨트롤 플레인에 의존하지 않는 데이터 플레인 전용 서비스입니다.

즉, IAM에 대한 종속성을 계획할 때는 복구 경로에서 IAM 컨트롤 플레인에 의존해서는 안 됩니다. 예를 들어, “브레이크-글래스 (break-glass)” 관리자를 위한 정적으로 안정적인 설계는 적절한 권한이 첨부된 사용자를 생성하고, 암호를 설정하고, 액세스 키와 비밀 액세스 키를 제공한 다음, 해당 자격 증명을 실제 또는 가상 볼트에 잠그는 것입니다. 긴급 상황에서 필요할 경우 볼트에서 사용자 자격 증명을 검색하고 필요에 따라 사용하십시오. non-statically-stable설계는 장애 발생 시 사용자를 프로비저닝하거나 사용자가 미리 프로비저닝하도록 하되 필요한 경우에만 관리 정책을 연결하는 것입니다. 이러한 접근 방식은 IAM 컨트롤 플레인에 따라 달라집니다.

AWS Organizations

AWS Organizations컨트롤 플레인은`AcceptHandshake`, `AttachPolicy` `CreateAccountCreatePolicy`, 및 `ListAccounts` 같은 모든 공개 Organizations API로 구성됩니다. 에 대한 데이터 플레인이 없습니다AWS Organizations. IAM과 같은 다른 서비스를 위한 데이터 플레인을 오케스트레이션합니다. 컨트롤 플레인 장애 중에는 Organizations 대한 CRUDL 유형의 작업이 작동하지 않을 수 있지만 서비스 제어 정책 (SCP) 및 태그 정책과 같은 정책은 계속 작동하며 IAM 권한 부여 프로세스의 일부로 평가됩니다. Organizations에서 지원하는 다른 AWS 서비스의 위임된 관리자 기능 및 다중 계정 기능도 계속 사용할 수 있습니다.

즉AWS Organizations, 종속 관계를 계획할 때는 복구 경로에서 Organizations 컨트롤 플레인에 의존해서는 안 됩니다. 대신 복구 계획에 정적 안정성을 구현하세요. 예를 들어 SCP를 업데이트하여 Allowed AWS 리전 via `aws:RequestedRegion` 조건에 대한 제한을 제거하거나 특정 IAM 역할에 대한 관리

자 권한을 활성화하는 non-statically-stable 접근 방식이 될 수 있습니다. 이를 위해서는 Organizations 컨트롤 플레인이 이러한 업데이트를 수행합니다. 세션 태그를 사용하여 관리자 권한을 부여하는 것이 더 나은 접근 방식입니다. IdP (Identity Provider) 는 조건을 기준으로 평가할 수 있는 세션 태그를 포함할 수 있습니다. 세션 태그는 특정 주체에 대한 권한을 동적으로 구성하는 동시에 SCP가 정적 `aws:PrincipalTag` 상태를 유지할 수 있도록 도와줍니다. 이렇게 하면 컨트롤 플레인에 대한 종속성이 제거되고 데이터 플레인 액션만 활용됩니다.

AWS 계정 관리

AWS계정 관리 컨트롤 플레인은 us-east-1에서 호스팅되며 관리를 위한 모든 공개 API (예: `GetContactInformation` 및 `PutContactInformation`) 로 AWS 계정 구성됩니다. 또한 관리 콘솔을 AWS 계정 통해 새로 만들거나 닫는 것도 포함됩니다. `CloseAccount`, `CreateAccount`, `CreateGovCloudAccount`, 및 `DescribeAccount` 에 대한 API는 us-east-1에서도 호스팅되는 AWS Organizations 컨트롤 플레인의 일부입니다. 또한 외부에서 GovCloud 계정을 만들려면 AWS Organizations us-east-1의 AWS 계정 관리 컨트롤 플레인이 필요합니다. 또한 GovCloud 계정은 `aws` 파티션에 1:1 로 AWS 계정 연결되어 있어야 합니다. `aws-cn`파티션에 계정을 만들 때는 us-east-1을 사용하지 않습니다. 데이터 플레인은 계정 AWS 계정 자체입니다. 컨트롤 플레인 장애 중에는 CRUDL 유형의 작업 (예: 새 계정 생성 또는 연락처 정보 가져오기 및 업데이트) 이 작동하지 않을 수 있습니다. AWS 계정 IAM 정책에서 계정에 대한 참조는 계속 사용할 수 있습니다.

즉, 계정 관리 종속 관계를 계획할 때는 복구 경로에서 AWS 계정 관리 컨트롤 플레인에 의존해서는 안 됩니다. Account Management 컨트롤 플레인은 복구 상황에서 일반적으로 사용하는 직접적인 기능을 제공하지는 않지만 경우에 따라 사용할 수 있습니다. 예를 들어, 정적으로 안정적인 설계는 페일오버에 필요한 모든 것을 미리 프로비저닝하는 것입니다. AWS 계정 non-statically-stable설계는 장애 발생 AWS 계정 시 DR 리소스를 호스팅하기 위해 새로 만드는 것입니다.

Route 53 애플리케이션 복구 컨트롤러

Route 53 ARC의 컨트롤 플레인은 복구 제어 및 복구 준비를 위한 API로 구성되며, Amazon Route 53 애플리케이션 복구 컨트롤러 엔드포인트 및 할당량에서 확인할 수 있습니다. 컨트롤 플레인을 사용하여 준비 검사, 라우팅 제어 및 클러스터 작업을 관리합니다. ARC의 데이터 플레인은 Route 53 상태 확인에서 쿼리되는 라우팅 제어 값을 관리하고 안전 규칙도 구현하는 복구 클러스터입니다. Route 53 ARC의 데이터 플레인 기능은 다음과 같은 `https://aaaaaaaa.route53-recovery-cluster.eu-west-1.amazonaws.com` 복구 클러스터 API를 통해 액세스할 수 있습니다.

즉, 복구 경로에서 Route 53 ARC 컨트롤 플레인에 의존해서는 안 됩니다. 이 지침을 구현하는 데 도움이 되는 두 가지 모범 사례가 있습니다.

- 먼저 5개의 지역 클러스터 엔드포인트를 북마크하거나 하드 코딩합니다. 따라서 페일오버 시나리오 중에 DescribeCluster 컨트롤 플레인 작업을 사용하여 엔드포인트 값을 검색할 필요가 없습니다.
- 둘째, CLI 또는 SDK를 사용하여 Route 53 ARC 클러스터 API를 사용하여 라우팅 컨트롤에 대한 업데이트를 수행하되 업데이트는 수행하지 마십시오. AWS Management Console 이렇게 하면 페일오버 계획에 대한 종속성이 관리 콘솔을 제거하고 데이터 플레인 작업에만 종속되도록 할 수 있습니다.

AWS Network Manager

AWS네트워크 관리자 서비스는 주로 us-west-2에서 호스팅되는 컨트롤 플레인 전용 시스템입니다. AWS 클라우드전체 리전 및 온프레미스 위치에서 WAN 코어 네트워크와 AWS Transit Gateway 네트워크의 구성을 중앙에서 AWS 계정 관리하는 것이 목적입니다. 또한 us-west-2의 클라우드 WAN 메트릭을 집계하며, 데이터 플레인을 통해서도 액세스할 수 있습니다. CloudWatch Network Manager가 손상되어도 이 관리자가 오케스트레이션하는 서비스의 데이터 플레인은 영향을 받지 않습니다. 클라우드 WAN에 대한 CloudWatch 지표는 us-west-2에서도 확인할 수 있습니다. 지역별 수신 및 송신 바이트 수와 같은 기간별 지표 데이터를 통해 us-west-2에 영향을 미치는 장애 발생 시 또는 기타 운영 목적으로 다른 지역으로 이동할 수 있는 트래픽 양을 파악하려는 경우 CloudWatch 콘솔에서 직접 또는 Amazon CloudWatch 지표를 CSV 파일에 게시하는 방법을 사용하여 해당 지표를 CSV 데이터로 내보낼 수 있습니다. 데이터는 `AWS/Network Manager` 네임스페이스에서 찾을 수 있으며, 선택한 일정에 따라 이 작업을 수행하고 S3 또는 선택한 다른 데이터 스토어에 저장할 수 있습니다. 정적으로 안정적인 복구 계획을 구현하려면 AWS Network Manager를 사용하여 네트워크를 업데이트하거나 컨트롤 플레인 작업의 데이터에 의존하여 페일오버 입력을 수행하지 마십시오.

루트 53 프라이빗 DNS

Route 53 프라이빗 호스팅 영역이 각 파티션에서 지원되지만 Route 53의 프라이빗 호스팅 영역과 퍼블릭 호스팅 영역에 대한 고려 사항은 동일합니다. 부록 B - 엣지 네트워크 글로벌 서비스 지침의 Amazon Route 53을 참조하십시오.

부록 B - 에지 네트워크 글로벌 서비스 지침

에지 네트워크 글로벌 서비스의 경우 AWS 서비스 컨트롤 플레인 장애 시 워크로드의 복원력을 유지하려면 정적 안정성을 구현해야 합니다.

Route 53

Route 53 컨트롤 플레인은 호스팅 영역, 레코드, 상태 확인, DNS 쿼리 로그, 재사용 가능한 위임 세트, 트래픽 정책 및 비용 할당 태그에 대한 기능을 포함하는 모든 퍼블릭 Route 53 API로 구성됩니다. us-east-1. 데이터 영역은 200개 이상의 PoP 위치에서 실행되는 신뢰할 수 있는 DNS 서비스로서 호스팅 영역 및 상태 확인 데이터를 기반으로 DNS 쿼리에 응답합니다. AWS 리전 또한 Route 53에는 상태 점검을 위한 데이터 플레인이 있으며 이 데이터 플레인도 여러 곳에 걸쳐 전 세계적으로 분산된 서비스입니다. AWS 리전 이 데이터 영역은 상태 확인을 수행하고 결과를 집계하여 Rou53 공용 및 프라이빗 DNS와 AGA와 AGA의 데이터 영역에 전달합니다. 컨트롤 플레인 장애 중에는 Route 53에 대한 CRUDL 유형의 작업이 작동하지 않을 수 있지만 상태 확인의 변경으로 인한 DNS 확인 및 상태 확인과 라우팅 업데이트는 계속 작동합니다.

즉, Route 53에 대한 종속성을 계획할 때는 복구 경로에서 Route 53 컨트롤 플레인에 의존해서는 안 됩니다. 예를 들어, 상태 확인 상태를 사용하여 지역 간 장애 조치를 수행하거나 가용 영역을 제거하는 것이 정적으로 안정적인 설계라고 할 수 있습니다. Route 53 ARC (애플리케이션 복구 컨트롤러) 라우팅 컨트롤을 사용하여 상태 확인 상태를 수동으로 변경하고 DNS 쿼리에 대한 응답을 변경할 수 있습니다. 요구 사항에 따라 구현할 수 있는 ARC에서 제공하는 것과 유사한 패턴이 있습니다. 이러한 패턴 중 일부는 Route 53을 사용한 재해 복구 메커니즘 만들기 및 고급 다중 AZ 레질리언스 패턴 상태 점검 회로 차단기 섹션에 요약되어 있습니다. 다중 지역 DR 플랜을 사용하기로 선택한 경우 ELB 및 RDS 인스턴스와 같이 DNS 레코드를 생성해야 하는 리소스를 미리 프로비저닝하십시오. non-statically-stable설계는 `ChangeResourceRecordSets` API를 통해 Route 53 리소스 레코드의 값을 업데이트하거나, 가중치 기반 레코드의 가중치를 변경하거나, 새 레코드를 생성하여 장애 조치를 수행하는 것입니다. 이러한 접근 방식은 Route 53 컨트롤 플레인에 따라 달라집니다.

Amazon CloudFront

Amazon CloudFront 컨트롤 플레인은 배포 관리를 위한 모든 퍼블릭 CloudFront API로 구성되며 us-east-1에서 호스팅됩니다. 데이터 플레인이란 엣지 네트워크에서 제공되는 배포판 그 자체입니다. PoPs 오리진 콘텐츠의 요청 처리, 라우팅 및 캐싱을 수행합니다. 컨트롤 플레인 장애 시 CRUDL 유형의 작업 CloudFront (무효화 요청 포함) 이 작동하지 않을 수 있지만 콘텐츠는 계속 캐시 및 서비스되며 원본 장애 조치는 계속 작동합니다.

즉CloudFront, 종속 관계를 계획할 때 복구 경로에서 CloudFront 컨트롤 플레인에 의존해서는 안 됩니다. 예를 들어, 정적으로 안정적인 설계는 자동화된 오리진 페일오버를 사용하여 장애가 오리진 중 하나에 미치는 영향을 완화하는 것입니다. Lamda @Edge 를 사용하여 오리진 로드 밸런싱 또는 장애 복구를 구축할 수도 있습니다. 해당 패턴에 대한 자세한 내용은 Amazon을 사용하는 고가용성 애플리케이션을 위한 세 가지 고급 설계 패턴 CloudFront 및 Amazon CloudFront 및 Amazon S3를 사용하여 다중 지역 액티브-액티브 지역 근접 애플리케이션 구축을 참조하십시오. 오리진 장애에 대응하여 배포 구성을 수동으로 업데이트하는 것이 non-statically-stable 설계일 것입니다. 이 접근 방식은 CloudFront 컨트롤 플레인에 따라 달라집니다.

Amazon Certificate Manager

CloudFront배포와 함께 사용자 지정 인증서를 사용하는 경우 ACM에도 종속됩니다. CloudFront배포에서 사용자 지정 인증서를 사용하려면 us-east-1 리전의 ACM 제어 영역에 의존합니다. 컨트롤 플레인 장애가 발생하더라도 배포판에 구성된 기존 인증서는 계속 작동하며 자동 인증서 갱신도 가능합니다. 배포 구성을 변경하거나 복구 경로의 일부로 새 인증서를 만드는 데 의존하지 마십시오.

AWS웹 애플리케이션 방화벽 (WAF) 및 WAF 클래식

CloudFront배포판과 AWS WAF 함께 사용하는 경우 us-east-1 지역에서도 호스팅되는 WAF 컨트롤 플레인에 종속됩니다. 컨트롤 플레인 장애가 발생해도 구성된 웹 ACL (액세스 제어 목록) 과 관련 규칙은 계속 작동합니다. 복구 경로의 일부로 WAF 웹 ACL 업데이트에 의존하지 마십시오.

AWS Global Accelerator

AGA 컨트롤 플레인은 모든 퍼블릭 AGA API로 구성되며 us-west-2에서 호스팅됩니다. 데이터 플레인이란 AGA에서 제공하는 애니캐스트 IP 주소를 등록된 엔드포인트로 네트워크로 라우팅하는 것입니다. 또한 AGA는 Route 53 상태 검사를 활용하여 Route 53 데이터 플레인의 일부인 AGA 엔드포인트의 상태를 확인합니다. 컨트롤 플레인 장애 중에는 AGA에 대한 CRUDL 유형의 작업이 작동하지 않을 수 있습니다. 기존 엔드포인트로의 라우팅은 물론 다른 엔드포인트 및 엔드포인트 그룹으로 트래픽을 라우팅하거나 이동하는 데 사용되는 기존 상태 확인, 트래픽 다이얼 및 엔드포인트 가중치 구성은 계속 작동합니다.

즉, AGA 종속성을 계획할 때 복구 경로에서 AGA 컨트롤 플레인에 의존해서는 안 됩니다. 예를 들어, 정적으로 안정적인 설계는 구성된 상태 검사의 상태를 사용하여 비정상 엔드포인트에서 페일아웃하는 것입니다. 이 구성의 예는 AWSGlobal AWS Accelerator를 사용하여 다중 지역 응용 프로그램 배포를 참조하십시오. non-statically-stable설계는 장애가 발생한 동안 AGA 트래픽 다이얼 백분율을 수정하거나, 엔드포인트 그룹을 편집하거나, 엔드포인트 그룹에서 엔드포인트를 제거하는 것입니다. 이러한 접근 방식은 AGA 컨트롤 플레인에 따라 달라집니다.

Amazon Shield 사용

아마존 Shield 어드밴스드 컨트롤 플레인은 모든 퍼블릭 Shield 어드밴스드 API로 구성되며 us-east-1에서 호스팅됩니다. 여기에는`CreateProtection`, `CreateProtectionGroup` `AssociateHealthCheck`, `DesribeDRTAccess`, 및 같은 기능이 포함됩니다`ListProtections`. 데이터 플레인이란 Shield 어드밴스가 제공하는 DDoS 보호와 Shield 어드밴스드 메트릭스 생성을 말합니다. 또한 Shield 어드밴스드는 Route 53 상태 확인 (Route 53 데이터 플레인의 일부) 을 구성한 경우 이를 활용합니다. 컨트롤 플레인 장애 중에는 Shield Advanced에 대한 CRUDL 유형의 작업이 작동하지 않을 수 있지만 리소스에 대해 구성된 DDoS 보호와 상태 점검 변경에 대한 대응은 계속 작동합니다.

즉, 복구 경로에서 Shield Advanced 컨트롤 플레인에 의존해서는 안 됩니다. Shield Advanced 컨트롤 플레인은 일반적으로 복구 상황에서 사용할 수 있는 직접적인 기능을 제공하지는 않지만 경우에 따라 사용할 수 있습니다. 예를 들어, 장애 발생 후 보호를 구성하는 것과는 대조적으로 DR 리소스가 보호 그룹에 포함되도록 이미 구성되고 관련 상태 점검을 받는 것이 정적으로 안정적인 설계라고 할 수 있습니다. 이렇게 하면 복구 시 Shield 어드밴스드 컨트롤 플레인에 의존하는 것을 방지할 수 있습니다.

부록 C - 단일 지역 서비스

다음은 단일 지역에서만 사용할 수 있는 서비스 또는 해당 서비스의 특정 기능 (서비스 이름 뒤에 괄호 안에 나열됨) 의 목록입니다. 제어 영역 및 데이터 플레인에 대한 종속성을 계획해야 하는 경우 다른 글로벌 서비스에 제공된 정적 안정성을 구현하기 위한 동일한 지침이 이러한 서비스에도 적용됩니다.

- Alexa for Business
- AWS Marketplace(AWS Marketplace 카탈로그API, AWS Marketplace 커머스 애널리틱스, AWS Marketplace 권한 서비스)
- 청구 및 비용 관리 (AWS Cost Explorer, AWS 비용 및 사용 보고서, AWS 예산, Savings Plan)
- AWS BugBust
- Amazon Mechanical Turk
- Amazon Chime
- Amazon Chime SDK (PSTN오디오, 메시징, 아이덴티티)
- AWS 챗봇
- AWS DeepRacer
- AWS Device Farm
- 아마존 GameSparks

기여자

이 문서의 기여자는 다음과 같습니다.

- 마이클 하켄, Amazon Web Services 수석 솔루션 아키텍트

문서 수정

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
사소한 수정	IAM 모범 실무에 따라 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례를 참조하세요.	2023년 2월 9일
초기 간행물	백서 발행.	2022년 11월 16일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하십시오.

고지 사항

고객은 이 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서: (a) 는 정보 제공만을 목적으로 하며, (b) 사전 통지 없이 변경될 수 있는 현재 AWS 제품 제공 및 관행을 나타내며, (c) 해당 계열사, 공급업체 또는 라이선스 제공자로부터 AWS 어떠한 약속이나 보증도 하지 않습니다. AWS제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 “있는 그대로” 제공됩니다. AWS고객에 대한 책임과 책임은 AWS 계약에 의해 통제되며, 이 문서는 고객 간의 AWS 계약의 일부가 아니며 이를 수정하지도 않습니다.

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