백업 및 복구 접근 방식 AWS

AWS 규범적 지침

AWS 규범적 지침: 백업 및 복구 접근 방식 AWS

Table of Contents

백업 및 복구 접근 방식 AWS

Khurram Nizami, Amazon Web Services(AWS)

2024년 6월 (문서 기록)

본 가이드에서는 Amazon Web Services(AWS) 서비스를 사용하여 온프레미스, 클라우드 네이티브 및 하이브리드 아키텍처를 위한 백업 및 복구 접근 방식을 구현하는 방법을 설명합니다. 이러한 접근 방식은 Recovery Time Objective(RTO), Recovery Point Objective(RPO) 및 규정 준수 요건을 충족할 수 있도록 비용 절감, 확장성 및 내구성을 제공합니다.

본 가이드는 기업 IT 및 클라우드 환경의 데이터 보호를 담당하는 기술 리더를 대상으로 합니다.

이 가이드는 다양한 백업 아키텍처(클라우드 네이티브 애플리케이션, 하이브리드 및 온프레미스 환경)를 다룹니다. 또한 아키텍처의 변경할 수 없는 구성 요소를 위한 확장 가능하고 신뢰할 수 있는 데이터 보호 솔루션을 구축하는 데 사용할 수 있는 관련 Amazon Web Services(AWS) 서비스도 다룹니다.

또 다른 접근 방식은 변경 불가능한 아키텍처를 사용하도록 워크로드를 현대화하여 구성 요소의 백업 및 복구 필요성을 줄이는 것입니다. AWS 변경할 수 없는 아키텍처를 구현하고 백업 및 복구의 필요성을 줄이기 위한 다음과 같은 다양한 서비스를 제공합니다.

- 다음과 같은 서버리스 AWS Lambda
- 아마존 Elastic Container 서비스 (Amazon ECS), 아마존 Elastic Kubernetes 서비스 (Amazon EKS)를 사용하는 컨테이너, AWS Fargate
- Amazon Elastic Compute Cloud(Amazon EC2)를 사용하는 Amazon Compute Cloud(AMI)

엔터프라이즈 데이터의 성장이 가속화됨에 따라 데이터를 보호하는 작업은 더욱 어려워지고 있습니다. 백업 접근 방식의 내구성과 확장성에 대한 질문은 흔한데, 여기에는 다음과 같은 질문이 포함됩니다. 클라우드가 백업 및 복원 요건을 충족하는 데 어떻게 도움이 됩니까?

이 가이드에는 다음 주제가 포함되어 있습니다.

- 데이터 보호를 위한 AWS 서비스 선택
- 백업 및 복구 솔루션 설계
- AWS Backup을 사용하여 백업 및 복구
- Amazon S3를 사용한 백업 및 복구
- EBS 볼륨을 사용하는 Amazon EC2의 백업 및 복구

데이터 보호 플랫폼으로 사용하는 AWS 이유는 무엇입니까?

AWS는 안전하고 성능이 뛰어나며 유연하며 비용을 절감하는 easy-to-use 클라우드 컴퓨팅 플랫폼입니다. AWS 확장 가능한 백업 및 복구 솔루션을 생성, 구현 및 관리하는 데 필요한 차별화되지 않은 무거운 작업을 처리합니다.

데이터 보호 전략의 AWS 일부로 사용하면 다음과 같은 많은 이점이 있습니다.

- 내구성: 아마존 심플 스토리지 서비스 (Amazon S3) 와 S3 글레이셔 딥 아카이브 Glacier Deep Archive Archive는 99.999999999% (11나인) 의 내구성을 제공하도록 설계되었습니다. 두 플랫폼 모두 지리적으로 분산된 3개 이상의 가용 영역에 객체를 복제하여 안정적인 데이터 백업을 제공합니다. 많은 AWS 서비스가 Amazon S3를 스토리지 및 내보내기/가져오기 작업에 사용합니다. 예컨대, Amazon Elastic Block Store(Amazon EBS)는 Amazon S3를 스냅샷 스토리지로 사용합니다.
- 보안: 전송 중 및 미사용 시 액세스 제어 및 데이터 암호화를 위한 다양한 옵션을 AWS 제공합니다.
- 글로벌 인프라: 전 세계에서 AWS 서비스를 이용할 수 있으므로 규정 준수 및 워크로드 요구 사항을 충족하는 지역에 데이터를 백업하고 저장할 수 있습니다.
- 규정 준수: AWS 인프라는 다음 표준을 준수하도록 인증되었으므로 백업 솔루션을 기존 규정 준수 체제에 쉽게 맞출 수 있습니다.
  - SOC(Service Organization Controls)
  - SSAE(Statement on Standards for Attestation Engagements) 16
  - ISO(국제표준화기구) 27001
  - Payment Card Industry Data Security Standard(PCI DSS)
  - HIPAA(미국 건강 보험 양도 및 책임에 관한 법)
  - SEC1
  - 연방정부의 위험 및 인증 관리 프로그램(FedRAMP)
- 확장성: 사용하면 AWS용량에 대해 걱정할 필요가 없습니다. 요건이 변경되면 관리 부담 없이 사용량을 늘리거나 줄일 수 있습니다.

- 총소유비용 (TCO) 절감: AWS 운영 규모가 커지면 서비스 비용이 절감되고 서비스의 TCO를 낮추는 데 도움이 됩니다. AWS AWS 가격 인하를 통해 이러한 비용 절감 효과를 고객에게 전가합니다.
- P ay-as-you-go 가격 책정: 필요한 만큼 AWS 서비스를 구매하고 사용하려는 기간 동안만 서비스를 구매합니다. AWS 가격에는 선결제 수수료, 해지 위약금 또는 장기 계약이 없습니다.

목표 비즈니스 성과

이 설명서의 목적은 다음과 같은 백업 및 복구 접근 방식을 지원하는 데 사용할 수 있는 AWS 서비스의 개요를 제공하는 것입니다.

- 온프레미스 아키텍처
- 클라우드 네이티브 아키텍처
- 하이브리드 아키텍처
- AWS 네이티브 서비스
- 재해 복구(DR)

모범 사례 및 고려 사항은 서비스 개요와 함께 다룹니다. 또한, 이 설명서에서는 백업 및 복구에 대해 한 접근 방식을 사용하는 것과 또 다른 방법 간의 장단점을 설명합니다.

데이터 보호를 위한 AWS 서비스 선택

> **알림**
>
> 2024년 4월 30일부터 VMware Cloud AWS on은 더 이상 채널 AWS 파트너나 채널 파트너에 의해 재판매되지 않습니다. 이 서비스는 Broadcom을 통해 계속 제공될 예정입니다. 자세한 내용은 AWS 담당자에게 문의하시기 바랍니다.

AWS 백업 및 복구 접근 방식의 일부로 사용할 수 있는 다양한 스토리지 및 보완 서비스를 제공합니다. 이러한 서비스는 클라우드 네이티브 아키텍처와 하이브리드 아키텍처를 모두 지원할 수 있습니다. 사용 사례에 따라 다양하게 설계된 서비스를 제공하고 있습니다.

- Amazon S3는 하이브리드 및 클라우드 네이티브 사용 사례 모두에 적합합니다. 개별 파일, 서버 또는 전체 데이터 센터를 백업하는 데 적합한 내구성이 뛰어난 범용 객체 스토리지 솔루션을 제공합니다.
- AWS Storage Gateway은(는) 하이브리드 사용 사례에 적합합니다. Storage Gateway는 일반적인 온프레미스 백업 및 스토리지 요구 사항에 Amazon S3의 성능을 사용합니다. 사용자의 애플리케이션은 다음 표준 스토리지 프로토콜을 사용하는 가상 머신(VM) 또는 하드웨어 게이트웨이 어플라이언스를 통해 서비스에 연결됩니다.
  - 네트워크 파일 시스템 () NFS
  - 서버 메시지 블록 (SMB)
  - 인터넷 소형 컴퓨터 시스템 인터페이스 (iSCSI)

  게이트웨이는 이러한 일반 온프레미스 프로토콜을 다음과 같은 AWS 스토리지 서비스에 연결합니다.
  - Amazon S3
  - S3 Glacier Deep Archive
  - 아마존 EBS

  Storage Gateway를 사용하면 파일, 볼륨, 스냅샷 및 가상 테이프를 위한 탄력적인 고성능 스토리지를 더 쉽게 제공할 수 있습니다. AWS
- AWS Backup서비스 전반의 데이터 백업을 중앙 집중화하고 자동화하기 위한 완전 관리형 백업 서비스입니다. AWS AWS Backup을(를) 사용하면 중앙에서 백업 정책을 구성하고 다음과 같은 AWS 리소스의 백업 활동을 모니터링할 수 있습니다.

- EBS볼륨
- EC2인스턴스 (Windows 애플리케이션 포함)
- 아마존 RDS 및 아마존 Aurora 데이터베이스
- DynamoDB 테이블
- Amazon Neptune 데이터베이스
- Amazon DocumentDB(MongoDB 호환) 데이터베이스
- 아마존 EFS 파일 시스템
- Amazon FSx for Lustre 파일 시스템 및 Amazon FSx Windows 파일 서버 파일 시스템
- VMware온프레미스 및 클라우드 온의 워크로드 VMware AWS
- Storage Gateway 볼륨

  AWSBackup 비용은 한 달에 사용하고, 복원하고, 전송하는 스토리지를 기준으로 합니다. 자세한 내용은 AWS Backup 요금을 참조하십시오.

- AWS Elastic Disaster Recovery대상 AWS 계정 및 선호 지역의 저렴한 스테이징 영역에 시스템을 지속적으로 복제합니다. DR 및 교차 리전 premises-to-cloud DR에 Elastic DR 복구를 사용할 수 있습니다.
- AWS Config AWS 계정의 AWS 리소스 구성을 자세히 볼 수 있습니다. 여기에는 리소스가 서로 어떻게 관련되는지, 과거에 어떻게 구성되었는지 등이 포함됩니다. 이 보기에서는 시간이 지남에 따라 리소스 구성 및 관계가 어떻게 변했는지 확인할 수 있습니다.

  AWS 리소스에 대한 AWS Config 구성 기록을 켜면 시간 경과에 따른 리소스 관계 기록이 유지됩니다. 이를 통해 최대 7년간 AWS 리소스 관계 (삭제된 리소스 포함) 를 식별하고 추적할 수 있습니다. 예를 들어, Amazon EBS 스냅샷 볼륨과 볼륨이 연결된 EC2 인스턴스의 관계를 추적할 AWS Config 수 있습니다.
- AWS Lambda을(를) 사용하여 워크로드의 백업 및 복구 절차를 프로그래밍 방식으로 정의하고 자동화할 수 있습니다. 를 사용하여 AWS 서비스 및 해당 AWS SDKs 데이터와 상호 작용할 수 있습니다. 또한 Amazon CloudWatch Events를 사용하여 Lambda 함수를 일정에 따라 실행할 수 있습니다.

AWS 서비스는 백업 및 복원을 위한 특정 기능을 제공합니다. 사용 중인 각 AWS 서비스에 대해 AWS 설명서를 참조하여 서비스에서 제공하는 백업, 복원 및 데이터 보호 기능을 확인하십시오. AWS Command Line Interface (AWS CLI) AWS SDKs, 및 API 작업을 사용하여 AWS 서비스별 데이터 백업 및 복구 기능을 자동화할 수 있습니다.

백업 및 복구 솔루션 설계

데이터 백업 및 복원을 위한 포괄적인 전략을 개발할 때는 먼저 발생 가능한 장애 또는 재해 상황과 이로 인한 비즈니스에 미치는 잠재적인 영향을 파악해야 합니다. 일부 산업에서는 데이터 보안, 개인 정보 보호 및 기록 보존에 대한 규제 요구 사항을 고려해야 합니다.

백업 및 복구 프로세스에는 다음을 포함하여 워크로드 및 지원 비즈니스 프로세스에 대한 Recovery Point Objective(RPO)와 Recovery Point Objective(RPO)를 충족할 수 있는 적절한 수준의 세분화가 포함되어야 합니다.

- 파일 레벨 복구(예: 애플리케이션의 구성 파일)
- 애플리케이션 데이터 레벨 복구(예: MySQL 내의 특정 데이터베이스)
- 애플리케이션 레벨 복구(예: 특정 웹 서버 애플리케이션 버전)
- Amazon EC2 볼륨 레벨 복구(예: EBS 볼륨)
- EC2 인스턴스 레벨 복구(예: EC2 인스턴스)
- 관리형 서비스 복구(예: DynamoDB 테이블)

솔루션의 모든 복구 요구 사항과 더불어 아키텍처 내 다양한 구성 요소 간의 데이터 종속성을 고려해야 합니다. 성공적인 복원 프로세스를 촉진하려면 아키텍처 내 다양한 구성 요소 간의 백업 및 복구를 조정하세요.

다음 항목은 인프라 구성에 따른 백업 및 복구 접근 방식을 설명합니다. IT 인프라는 크게 온프레미스, 하이브리드, 클라우드 네이티브로 분류할 수 있습니다.

AWS Backup을 사용하여 백업 및 복구

AWS Backup은 AWS 서비스 전반에 걸친 데이터 백업을 중앙 집중화하고 자동화하는 종합 관리형 백업 서비스입니다. AWS Backup은 Amazon CloudWatch, AWS CloudTrail, AWS Identity and Access Management(IAM), AWS Organizations 및 기타 서비스를 통합하는 오케스트레이션 계층을 제공합니다. 이 중앙 집중식 AWS 클라우드 네이티브 솔루션은 재해 복구 및 규정 준수 요구 사항을 달성하는 데 도움이 되는 글로벌 백업 기능을 제공합니다. AWS Backup를 사용하여 중앙에서 백업 정책을 구성하고 AWS 리소스의 백업 활동을 모니터링할 수 있습니다.

AWS Backup은 AWS 계정 및 지역 전반의 AWS 리소스에 대한 표준 백업 계획을 구현하는 데 이상적인 솔루션입니다. AWS Backup이 여러 AWS 리소스 유형을 지원하므로 일괄 백업해야 하는 여러 AWS 리소스를 사용하는 워크로드에 대한 백업 전략을 쉽게 유지 관리하고 구현할 수 있습니다.또한 AWS Backup는 여러 AWS 리소스가 포함된 백업 및 복원 작업을 종합적으로 모니터링할 수 있게 합니다.

규정 준수 및 감사 요구 사항이 있는 경우 AWS Backup Audit Manager 기능을 사용하여 규정 준수 요구 사항을 지원하는 감사 프레임워크 및 보고서를 만들 수 있습니다. 또한 AWS Backup 저장소 잠금 기능은 AWS Backup의 백업 저장소에 저장된 모든 백업에 대해 WORM(Write-Once, Read-Many) 구성을 적용하여 규정 준수 요구 사항을 지원합니다.

AWS Backup의 주요 차별화 요소는 Organizations에 대한 지원입니다. 이 지원을 사용하면 조직 또는 조직 단위 수준에서 백업 정책을 정의 및 관리하고 각 관련 AWS 계정 및 지역에 해당 정책을 자동으로 구현할 수 있습니다. 새 AWS 계정과 지역을 온보딩할 때 백업 계획을 별도로 정의하고 관리할 필요가 없습니다.

AWS Backup은 태그를 사용하여 조직 전체의 백업 정책을 더 쉽게 구현할 수 있게 합니다. 각각 고유한 빈도와 보존 설정이 있는 별도의 백업 계획을 만든 다음 백업에 포함할 리소스를 선택하는 고유한 키-값 페어 태그를 만들 수 있습니다.

예를 들어, 매일 05:00 UTC에 백업을 시작하고 35일 보존 정책이 적용되는 일일 백업 계획을 생성할 수 있습니다. 이 백업 계획에는 매일 태그 키 백업과 태그 값이 있는 지원되는 모든 AWS 리소스를 이 계획에 따라 백업하도록 지정하는백업 리소스 할당이 포함될 수 있습니다. 또한 매월 첫째 날 05:00 UTC에 시작하고 366일 보존 정책이 적용되는 월별 백업 계획을 만들 수도 있습니다. 이 백업 계획에는 매월 태그 키 백업과 태그 값이 있는 지원되는 모든 AWS 리소스를 이 계획에 따라 백업하도록 지정하는 백업 리소스 할당이 포함될 수 있습니다.

그런 다음 태그 정책과 필수 태그 AWS Config 규칙을 사용하여 AWS 지원되는 모든 리소스에 이 태그 키와 이러한 태그 값 중 하나가 있는지 확인할 수 있습니다. 이 접근 방식을 사용하면 지원되는 AWS

Backup 리소스에 대한 AWS의 표준 백업 접근 방식을 일관되게 구현하고 유지할 수 있습니다. 이 접근 방식을 확장하여 Recovery Point Objective(RPO) 요구 사항이 서로 다른 애플리케이션 및 아키텍처 계층의 백업을 표준화할 수 있습니다.

백업 저장소를 보호하기 위한 단계를 취하는 것이 좋습니다. 예를 들어, 백업 저장소가 삭제되거나 의도하지 않은 AWS 계정과 공유되는 것을 방지하는 조직 서비스 제어 정책(SCP)를 구현할 수 있습니다. 자세한 내용 및 기타 중요한 보안 고려 사항은 블로그 게시물의 AWS의 백업 보안을 위한 10가지 보안 모범 사례를 검토하세요.

AWS Backup는 종합적으로 처리할 수 있는 여러 AWS 리소스를 지원하므로 AWS의 재해 복구(DR) 계획 구현을 단순화할 수 있습니다. 예를 들어 AWS Backup에서 지원하는 대부분의 AWS 리소스 유형에 대해 지역 간 및 계정 간 백업을 구현할 수 있습니다. 계정 간 백업은 별도의 계정에서 사본을 사용할 수 있으므로 백업 보안을 개선합니다. 지역 간 백업은 백업을 둘 이상의 지역에서 사용할 수 있으므로 가용성이 향상됩니다. 지원되는 AWS 리소스 유형에 대한 자세한 내용은 리소스별 기능 가용성 표를 참조하세요.

AWS Backup 오픈 소스 솔루션과 함께 Backup and Recovery의 예를 사용하여 코드형 인프라(IaC) 및 지속적 통합 및 지속적 전달(CI/CD) 접근 방식을 구현하여 AWS Organizations 조직의 백업을 관리할 수 있습니다. 이 솔루션에는 복원된 AWS 리소스에 자동으로 AWS 태그를 재적용하는 것은 물론 재해 복구 목적으로 별도의 계정 및 지역에 보조 백업 저장소를 설정하는 등의 사용자 지정 기능이 포함되어 있습니다.

Amazon S3를 사용한 백업 및 복구

Amazon Simple Storage 서비스 (Amazon S3) 를 사용하여 언제든지 원하는 양의 데이터를 저장하고 검색할 수 있습니다. Amazon S3를 애플리케이션 데이터와 파일 수준 백업 및 복원 프로세스를 위한 내구성 있는 저장소로 사용할 수 있습니다. 예를 들어, AWS CLI 또는 AWS SDK를 사용하여 백업 스크립트를 사용하여 데이터베이스 인스턴스에서 Amazon S3로 데이터베이스 백업을 복사할 수 있습니다.

AWS 서비스 Amazon S3를 사용하면 다음 예와 같이 내구성이 뛰어나고 안정적인 스토리지를 만들 수 있습니다.

- Amazon EC2는 Amazon S3를 사용하여 EBS 볼륨 및 EC2 인스턴스 스토어용 Amazon EBS 스냅샷을 저장합니다.
- Storage Gateway는 Amazon S3와 통합되어 Amazon S3가 지원하는 파일 공유, 볼륨 및 테이프 라이브러리가 있는 온프레미스 환경을 제공합니다.
- Amazon RDS는 데이터베이스 스냅샷에 Amazon S3를 사용합니다.

많은 타사 백업 솔루션도 Amazon S3를 사용합니다. 예를 들어. Arcserve Unified Data Protection은 온프레미스 및 클라우드 네이티브 서버의 내구성 있는 백업을 위해 Amazon S3를 지원합니다.

이러한 서비스의 Amazon S3 통합 기능을 사용하여 백업 및 복구 접근 방식을 단순화할 수 있습니다. 동시에 Amazon S3가 제공하는 높은 내구성 및 가용성을 활용할 수 있습니다.

Amazon S3는 버킷이라 불리는 리소스 내에 객체로 데이터를 저장합니다. 버킷에 객체를 원하는 만큼 저장할 수 있습니다. 세분화된 액세스 제어를 통해 버킷에서 객체를 쓰고, 읽고, 삭제할 수 있습니다. 단일 객체의 크기는 최대 5TB까지 가능합니다.

Amazon S3 스토리지 클래스를 사용하여 백업 데이터 스토리지 비용 절감

Amazon S3는 온프레미스, 하이브리드 및 클라우드 네이티브 아키텍처에서 사용할 수 있는 여러 스토리지 클래스를 제공합니다. 모든 스토리지 클래스는 확장 가능한 용량을 제공하므로 백업 데이터 세트가 증가함에 따라 볼륨이나 미디어를 관리할 필요가 없습니다. pay-for-what-you-use 모델과 저렴한 GB/월 비용 덕분에 Amazon S3 스토리지 클래스는 광범위한 데이터 보호 사용 사례에 적합합니다. Amazon S3 스토리지 클래스는 다음 범주를 포함하여 다양한 사용 사례에 맞게 설계되었습니다.

- 자주 액세스하는 데이터 (예: 구성 파일, 계획되지 않은 백업, 일일 백업) 의 범용 스토리지를 위한 빈번한 액세스 스토리지 클래스. 여기에는 모든 Amazon S3 객체의 기본값인 S3 표준 스토리지 클래스가 포함됩니다.
- 수명이 길지만 자주 액세스하지 않는 데이터를 위한 비액세스 스토리지 클래스 (예: 월별 백업). 여기에는 S3 스탠다드-IA 스토리지 클래스가 포함됩니다. IA는 Infrequent Access(빈번하지 않은 액세스)의 약어입니다.
- 거의 액세스할 필요가 없는 매우 수명이 긴 데이터 (예: 연간 백업) 를 위한 S3 Glacier 스토리지 클래스. 여기에는 가장 저렴한 스토리지를 제공하는 S3 Glacier Deep Archive도 포함됩니다. AWS

액세스 패턴을 알 수 없거나 변경되는 백업의 경우 S3 인텔리전트 티어링 스토리지 클래스를 사용할 수 있습니다. S3 Intelligent-Tiering은 객체에 마지막으로 액세스한 지 며칠을 기준으로 객체를 가장 비용 효율적인 계층으로 자동 전환합니다.

> **Note**
>
> 일부 스토리지 클래스에는 최소 기간 요금이 부과됩니다. 자세한 내용은 Amazon S3 요금을 참조하고 웹 페이지 검색을 사용하여 찾아보십시오`duration`.

또한 Amazon S3는 수명 주기 전반에 걸쳐 데이터를 관리하기 위한 구성 가능한 수명 주기 정책을 제공합니다. 정책이 설정되면 애플리케이션을 변경하지 않고도 데이터가 적절한 스토리지 클래스로 자동 마이그레이션됩니다. 자세한 내용을 알아보려면 Amazon S3 객체 수명 주기 관리 설명서를 참조하십시오.

백업 비용을 줄이려면 다음 예와 같이 RPO(복구 시점 목표) 및 RTO(복구 시간 목표)를 기반으로 계층형 스토리지 클래스 접근 방식을 사용하십시오.

- S3 Standard를 사용한 지난 2주 동안의 일일 백업
- S3 Standard-IA를 사용한 지난 3개월 동안의 주간 백업
- S3 Glacier Flexible Retrieval의 지난해 분기별 백업
- S3 Glacier Deep Archive의 지난 5년 동안의 연간 백업
- S3 Glacier Deep Archive에서 5년이 지난 후 백업이 삭제됨

백업 및 아카이브를 위한 표준 S3 버킷 생성

S3 수명 주기 정책을 통해 구현된 회사의 백업 및 보존 정책을 사용하여 백업 및 아카이브를 위한 표준 S3 버킷을 생성할 수 있습니다. 비용 할당 태깅 및 AWS 청구 보고는 버킷 수준에서 할당된 태그를 기반으로 합니다. 비용 할당이 중요한 경우 각 프로젝트 또는 사업부에 대해 별도의 백업 및 아카이브 S3 버킷을 만들어 그에 따라 비용을 할당할 수 있습니다.

백업 스크립트와 애플리케이션은 생성한 백업 및 아카이브 S3 버킷을 사용하여 애플리케이션 및 워크로드 데이터용 point-in-time 스냅샷을 저장할 수 있습니다. 표준 S3 접두사를 생성하여 point-in-time 데이터 스냅샷을 구성하는 데 도움이 될 수 있습니다. 예를 들어, 시간별 백업을 생성하는 경우 `YYYY/MM/DD/HH/<WorkloadName>/<files...>`와 같은 백업 접두사를 사용하는 것이 좋습니다. 이렇게 하면 수동 또는 프로그래밍 방식으로 point-in-time 백업을 빠르게 검색할 수 있습니다.

Amazon S3 버전 관리를 사용하여 롤백 기록 자동 유지 관리

S3 객체 버전 관리를 활성화하여 이전 버전으로 되돌리는 기능을 포함하여 객체 변경 기록을 유지 관리할 수 있습니다. 이는 point-in-time 백업 일정보다 더 자주 변경될 수 있는 구성 파일 및 기타 객체에 유용합니다. 또한 개별적으로 되돌려야 하는 파일에도 유용합니다.

Amazon S3를 사용하여 AMI용 사용자 지정 구성 파일 백업 및 복구

객체 버전 관리를 사용하는 Amazon S3는 워크로드 구성 및 옵션 파일의 레코드 시스템이 될 수 있습니다. 예를 들어 ISV에서 유지 관리하는 표준 AWS Marketplace Amazon EC2 이미지를 사용할 수 있습니다. 이 이미지에는 여러 구성 파일에서 구성이 유지되는 소프트웨어가 포함될 수 있습니다. Amazon S3에서 사용자 지정 구성 파일을 유지 관리할 수 있습니다. 인스턴스가 시작되면 이러한 구성 파일을 인스턴스 사용자 데이터의 일부로 인스턴스에 복사할 수 있습니다. 이러한 접근 방식을 적용하면 업데이트된 버전을 사용하기 위해 AMI를 사용자 지정하고 다시 생성할 필요가 없습니다.

사용자 지정 백업 및 복원 프로세스에서 Amazon S3의 사용

Amazon S3는 기존의 사용자 지정 백업 프로세스에 빠르게 통합할 수 있는 범용 백업 저장소를 제공합니다. AWS CLI, AWS SDK 및 API 작업을 사용하여 Amazon S3를 사용하는 백업 및 복원 스크립트와 프로세스를 통합할 수 있습니다. 예를 들어, 야간 데이터베이스 내보내기를 수행하는 데이터베이스 백업 스크립트가 있을 수 있습니다. 이 스크립트를 사용자 지정하여 야간 백업을 Amazon S3에 복사하여 오프사이트 저장소에 저장할 수 있습니다. 이 작업을 수행하는 방법에 대한 개요는 Batch upload files to the cloud 자습서를 참조하십시오.

개별 RPO에 따라 다양한 애플리케이션의 데이터를 내보내고 백업하는 유사한 접근 방식을 사용할 수 있습니다. 또한 를 AWS Systems Manager 사용하여 관리형 인스턴스에서 백업 스크립트를 실행할 수 있습니다. Systems Manager는 개별 백업 프로세스에 대한 자동화, 액세스 제어, 일정 예약, 로깅 및 알림을 제공합니다.

Amazon S3의 백업 데이터 보안

데이터 보안은 보편적인 관심사이며 AWS 보안을 매우 중요하게 생각합니다. 보안은 모든 것의 AWS 서비스기초입니다. Amazon S3는 저장 및 전송 중 액세스 제어 및 암호화 기능을 제공합니다. 모든 Amazon S3 엔드포인트는 전송 데이터를 암호화하기 위해 SSL/TLS를 지원합니다. 다음을 수행하여 유휴 객체에 대한 암호화를 설정할 수 있습니다.

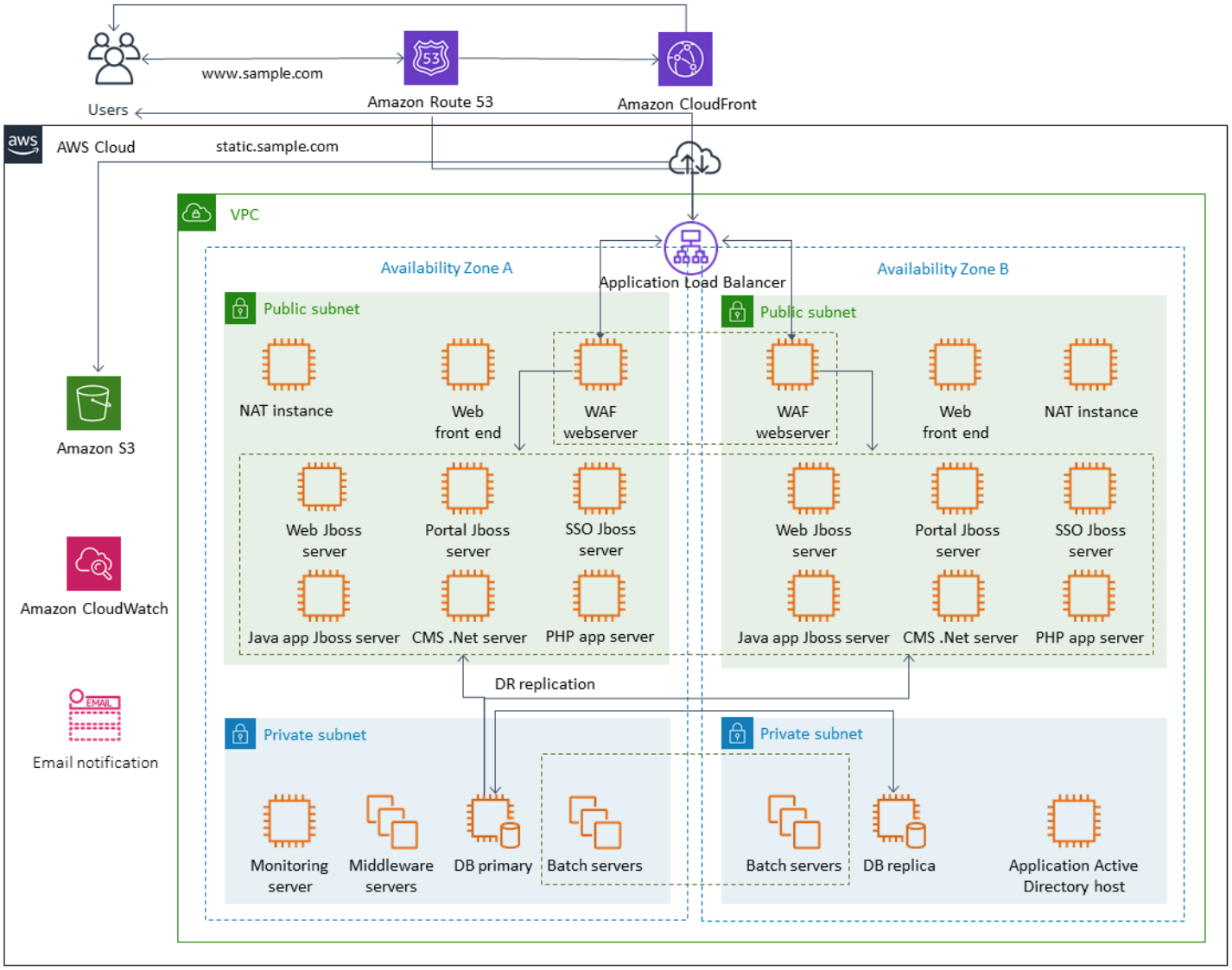
- Amazon S3 관리 암호화 키를 통한 서버 측 암호화 사용 (기본값)
- AWS Key Management Service ()AWS KMS키가 저장된 서버 측 암호화 사용 AWS KMS
- 클라이언트 측 암호화 사용

AWS Identity and Access Management (IAM) 을 사용하여 S3 객체에 대한 액세스를 제어할 수 있습니다. IAM은 S3 버킷 내 개별 객체 및 특정 접두사 경로에 대한 권한을 제어합니다. 에서 객체 수준 로깅을 사용하여 S3 객체에 대한 액세스를 감사할 수 있습니다. AWS CloudTrail

EBS 볼륨을 사용하는 Amazon EC2의 백업 및 복구

AWS Amazon EC2 인스턴스를 백업하는 여러 방법을 제공합니다. 이 단원에서는 Amazon Elastic Block Store(Amazon EBS) 볼륨 또는 스토리지용 인스턴스 스토어 볼륨을 백업하는 데 있어서의 다양한 측면을 다룹니다. 요구 사항을 충족하는 AWS 경우 백업을 관리하기 위한 첫 번째 AWS Backup 선택으로 고려해 보십시오. 백업은 원래 기능으로 복원할 수 있는 경우에만 유효하다는 점을 기억하십시오. 복원 및 복구 기능을 정기적으로 테스트하여 이를 확인해야 합니다.

다음 다이어그램의 솔루션 아키텍처는 Amazon EC2를 기반으로 하는 대부분의 아키텍처에 전적으로 존재하는 워크로드 환경을 설명합니다. AWS 다음 그림에서 볼 수 있듯이 시나리오에는 웹 서버, 애플리케이션 서버, 모니터링 서버, 데이터베이스 및 Active Directory가 포함됩니다.



AWS 는 이 아키텍처에 포함된 많은 Amazon EC2 서버가 인스턴스 및 스토리지를 생성, 프로비저닝, 백업, 복원 및 최적화하는 차별되지 않은 작업을 수행할 수 있도록 다양한 기능을 갖춘 서비스를 제공합니다. 이러한 서비스가 아키텍처에서 복잡성과 관리를 줄이는 데 적합한지 생각해 보십시오. AWS 또한 Amazon EC2 기반 아키텍처의 가용성을 개선하는 서비스를 제공합니다. 특히 Amazon EC2의 워크로드를 보완하기 위해 Amazon EC2 Auto Scaling 및 Elastic Load Balancing을 고려해 보십시오. 이러한 서비스를 사용하면 아키텍처의 가용성과 내결함성을 개선하고 사용자에게 미치는 영향을 최소화하면서 손상된 인스턴스를 복원할 수 있습니다.

EC2 인스턴스는 영구 스토리지용 Amazon EBS 볼륨을 주로 사용합니다. Amazon EBS는 이 단원에서 자세히 설명하는 다양한 백업 및 복구 기능을 제공합니다.

주제

스냅샷과 AMI를 사용한 Amazon EC2 백업 및 복구

Amazon Machine Image(AMI)를 사용하여 EC2 인스턴스의 전체 백업을 생성해야 하는지 아니면 개별 볼륨의 스냅샷을 생성해야 하는지 고려해 보십시오.

AMI 또는 Amazon EBS 스냅샷을 백업에 사용

AMI는 다음을 포함합니다.

- 하나 이상의 스냅샷 I nstance-store-backed AMI에는 인스턴스의 루트 볼륨 (예: 운영 체제, 애플리케이션 서버, 애플리케이션) 을 위한 템플릿이 포함되어 있습니다.
- AMI를 사용하여 인스턴스를 시작할 수 있는 AWS 계정을 제어하는 시작 권한.
- 시작될 때 인스턴스에 연결할 볼륨을 지정하는 블록 디바이스 매핑

AMI를 사용하여 미리 구성된 소프트웨어 및 데이터로 새 인스턴스를 시작할 수 있습니다. 더 많은 인스턴스를 시작하기 위한 재사용 가능한 구성이 되는 기준을 설정하려는 경우 AMI를 생성할 수 있습니다. 기존 EC2 인스턴스의 AMI를 생성하면 인스턴스에 연결된 모든 볼륨의 스냅샷이 생성됩니다. 스냅샷에는 디바이스 매핑이 포함됩니다.

스냅샷을 사용하여 새 인스턴스를 시작할 수는 없지만 기존 인스턴스의 볼륨을 대체하는 데는 스냅샷을 사용할 수 있습니다. 데이터 손상이나 볼륨 장애가 발생하는 경우, 생성한 스냅샷으로 볼륨을 생성

하고 이전 볼륨을 교체할 수 있습니다. 스냅샷을 사용하여 새 볼륨을 프로비저닝하고 새 인스턴스 시작 중에 연결할 수도 있습니다.

에서 유지 AWS 관리하거나 에서 게시한 플랫폼 및 애플리케이션 AMI를 사용하는 경우 데이터에 대해 별도의 볼륨을 유지하는 것이 좋습니다. AWS Marketplace 데이터 볼륨을 운영 체제 및 애플리케이션 볼륨과 분리된 스냅샷으로 백업할 수 있습니다. 그런 다음 에서 AWS 게시하거나 에서 게시한 새로 업데이트된 AMI와 함께 데이터 볼륨 스냅샷을 사용하십시오. AWS Marketplace 이 방법을 사용하려면 새로 게시된 AMI에서 구성 정보를 포함한 모든 사용자 지정 데이터를 백업하고 복원하기 위한 신중한 테스트와 계획이 필요합니다.

복원 프로세스는 AMI 백업과 스냅샷 백업 중에서 어떤 것을 선택하느냐에 영향을 받습니다. 인스턴스 백업으로 사용할 AMI를 생성하는 경우 복원 프로세스의 일부로 AMI에서 EC2 인스턴스를 시작해야 합니다. 잠재적 충돌을 방지하기 위해 기존 인스턴스를 종료해야 할 수도 있습니다. 잠재적 충돌의 예로는 도메인에 가입된 Windows 인스턴스의 SID(보안 식별자)를 들 수 있습니다. 스냅샷의 복원 프로세스에서는 기존 볼륨을 분리하고 새로 복원된 볼륨을 연결해야 할 수 있습니다. 또는 애플리케이션이 새로 연결된 볼륨을 가리키도록 구성을 변경해야 할 수도 있습니다.

AWS Backup AMI로서의 인스턴스 수준 백업과 별도의 스냅샷으로서의 볼륨 수준 백업을 모두 지원합니다.

- 인스턴스의 모든 EBS 볼륨을 전체 백업하려면 Linux 또는 Windows에서 실행되는 EC2 인스턴스의 AMI를 생성하십시오. 롤백하려면 인스턴스 시작 마법사를 사용하여 인스턴스를 생성하십시오. 인스턴스 시작 마법사에서 My AMI를 선택합니다.
- 개별 볼륨을 백업하려면 스냅샷을 생성하십시오. 스냅샷을 복원하려면 스냅샷에서 볼륨 만들기를 참조하십시오. AWS Management Console 또는 AWS Command Line Interface (AWS CLI) 를 사용할 수 있습니다.

인스턴스 AMI의 비용은 인스턴스에 있는 모든 볼륨의 스토리지이지만 메타데이터는 아닙니다. EBS 스냅샷 비용은 개별 볼륨의 스토리지입니다. 볼륨 스토리지 비용에 대한 자세한 내용은 Amazon EBS 요금 페이지를 참조하십시오.

서버 볼륨

EBS 볼륨은 Amazon EC2의 기본 영구 스토리지 옵션입니다. 이 블록 스토리지는 데이터베이스와 같은 정형 데이터나 볼륨의 파일 시스템에 있는 파일과 같은 비정형 데이터에 사용할 수 있습니다.

EBS 볼륨은 특정 사용 가능 영역에 배치됩니다. 볼륨은 여러 서버에 복제되어 단일 구성 요소의 장애로 인한 데이터 손실을 방지합니다. 장애란 볼륨의 크기와 성능에 따라 볼륨이 완전히 또는 부분적으로 손실되는 것을 말합니다.

EBS 볼륨은 0.1~0.2% 의 AFR(연간 고장률)을 제공하도록 설계되었습니다. 따라서 EBS 볼륨의 안정성은 약 4%의 AFR로 실패하는 일반적인 상용 디스크 드라이브보다 20배 더 안정적입니다. 예를 들어, 1년 동안 1,000개의 EBS 볼륨을 실행한다면 한두 개의 볼륨에서 장애가 발생할 것으로 예상해야 합니다.

Amazon EBS는 데이터 point-in-time 백업을 위한 스냅샷 기능도 지원합니다. 모든 EBS 볼륨 유형은 내구적 스냅샷 기능을 제공하고 99.999% 가용성으로 설계되었습니다. 자세한 내용은 Amazon 컴퓨팅 서비스 수준 계약을 참조하십시오.

Amazon EBS는 모든 EBS 볼륨의 스냅샷(백업)을 생성할 수 있는 기능을 제공합니다. 스냅샷은 EBS 볼륨의 백업을 생성하기 위한 기본 기능입니다. 스냅샷은 EBS 볼륨의 사본을 복수 가용 영역에 중복 저장되는 Amazon S3에 저장합니다. 초기 스냅샷은 볼륨의 전체 사본이며, 진행 중인 스냅샷은 블록 수준의 증분 변경 사항만 저장합니다. Amazon EBS 스냅샷을 생성하는 방법에 대한 자세한 내용은 Amazon EC2 설명서를 참조하십시오.

스냅샷을 촬영한 동일한 리전의 Amazon EC2 콘솔에서 복원 작업을 수행하거나, 스냅샷을 삭제하거나, 스냅샷과 관련된 스냅샷 메타데이터(예: 태그)를 업데이트할 수 있습니다.

스냅샷을 복원하면 전체 볼륨 데이터가 포함된 새 Amazon EBS 볼륨이 생성됩니다. 부분 복원만 필요한 경우 다른 디바이스 이름으로 실행 중인 인스턴스에 볼륨을 연결할 수 있습니다. 그런 다음 마운트하고 운영 체제 복사 명령을 사용하여 백업 볼륨의 데이터를 프로덕션 볼륨으로 복사합니다.

Amazon EC2 설명서에 설명된 대로 Amazon EBS 스냅샷 복사 기능을 사용하여 AWS 지역 간에 Amazon EBS 스냅샷을 복사할 수도 있습니다. 이 기능을 사용하면 기본 복제 기술을 관리할 필요 없이 백업을 다른 리전에 저장할 수 있습니다.

별도의 서버 볼륨 설정

운영 체제, 로그, 애플리케이션 및 데이터에 대해 별도의 표준 볼륨 세트를 이미 사용하고 있을 수 있습니다. 별도의 서버 볼륨을 설정하면 디스크 공간 소진으로 인한 애플리케이션 또는 플랫폼 장애 발생 시 영향 범위를 줄일 수 있습니다. 물리적 하드 드라이브는 볼륨을 빠르게 확장할 수 있는 유연성이 없기 때문에 일반적으로 이러한 위험은 더 큽니다. 물리적 드라이브의 경우 새 드라이브를 구입하여 데이터를 백업한 다음 새 드라이브에 데이터를 복원해야 합니다. 를 사용하면 AWS Amazon EBS를 사용하여 프로비저닝된 볼륨을 확장할 수 있으므로 이러한 위험이 크게 줄어듭니다. 자세한 내용은 AWS 설명서를 참조하십시오.

애플리케이션 데이터, 사용자 데이터, 로그 및 스왑 파일을 위한 별도의 볼륨을 유지하여 이러한 리소스에 대해 별도의 백업 및 복원 정책을 사용할 수 있습니다. 데이터의 볼륨을 분리하여 데이터의 성능 및 스토리지 요구 사항에 따라 다양한 볼륨 유형을 사용할 수도 있습니다. 그런 다음 다양한 워크로드에 맞게 비용을 최적화하고 세밀하게 조정할 수 있습니다.

인스턴스 스토어 볼륨에 대한 고려 사항

인스턴스 스토어는 인스턴스에 블록 수준의 임시 스토리지를 제공합니다. 스토리지는 호스트 컴퓨터에 물리적으로 연결된 디스크에 위치합니다. 인스턴스 스토어는 버퍼, 캐시, 스크래치 데이터, 기타 임시 콘텐츠와 같이 자주 변경되는 정보의 임시 저장에 적합합니다. 또한 로드 밸런싱된 웹 서버 풀과 같은 인스턴스 플릿 전체에 복제되는 데이터에도 적합합니다.

인스턴스 스토리지의 데이터는 관련 인스턴스의 수명 기간 동안만 지속됩니다. 인스턴스가 재부팅(의도적 또는 의도적이지 않게)되면 인스턴스 스토어의 데이터는 유지됩니다. 그러나 다음 상황에서는 인스턴스 스토어의 데이터가 손실됩니다.

- 기본 드라이브 오류
- 인스턴스가 중지됩니다.
- 인스턴스가 종료됩니다.

그러므로 중요한 장기 데이터의 경우 인스턴스 스토어에 의존하지 마십시오. 오히려 Amazon S3, Amazon EBS 또는 Amazon EFS 등 내구성이 뛰어난 데이터 스토리지를 사용하는 것이 좋습니다.

인스턴스 스토어 볼륨의 일반적인 전략은 RPO(복구 시점 목표) 및 RTO(복구 시간 목표)를 기반으로 필요에 따라 필요한 데이터를 Amazon S3에 정기적으로 보관하는 것입니다. 그러면 새 인스턴스가 시작될 때 Amazon S3에서 인스턴스 스토어로 데이터를 다운로드할 수 있습니다. 인스턴스가 중지되기 전에 Amazon S3에 데이터를 업로드할 수도 있습니다. 지속성을 위해 EBS 볼륨을 생성하여 인스턴스에 연결하고 인스턴스 스토어 볼륨의 데이터를 주기적으로 EBS 볼륨으로 복사하십시오. 자세한 정보는 AWS 지식 센터를 참조하십시오.

EBS 스냅샷 및 AMI에 대한 태그 지정 및 표준 적용

모든 AWS 리소스에 태그를 지정하는 것은 비용 할당, 감사, 문제 해결 및 알림을 위한 중요한 관행입니다. EBS 볼륨에서는 볼륨을 관리하고 복원하는 데 필요한 관련 정보가 표시되도록 하기 위해 태그를 지정하는 것이 중요합니다. 태그는 EC2 인스턴스에서 AMI로 또는 소스 볼륨에서 스냅샷으로 자동으로 복사되지 않습니다. 백업 프로세스에 이러한 소스의 관련 태그가 포함되어 있는지 확인하십시오. 그러면 액세스 정책, 연결 정보, 비용 할당 등의 스냅샷 메타데이터를 설정하여 나중에 이러한 백업을 사용하는 데 도움이 됩니다. AWS 리소스에 태그를 지정하는 방법에 대한 자세한 내용은 태깅 모범 사례 기술 문서를 참조하십시오.

모든 AWS 리소스에 사용하는 태그 외에도 다음과 같은 백업별 태그를 사용하십시오.

- 소스 인스턴스 ID

- 소스 볼륨 ID(스냅샷용)
- 복구 시점 설명

규칙 및 IAM 권한을 사용하여 AWS Config 태깅 정책을 적용할 수 있습니다. IAM은 강제 태그 사용을 지원하므로 Amazon EBS 스냅샷에서 작업할 때 특정 태그의 사용을 의무화하는 IAM 정책을 작성할 수 있습니다. IAM 권한 정책에 정의된 태그에 권한을 부여하지 않고 `CreateSnapshot` 작업을 시도하면 액세스가 거부되면서 스냅샷 생성이 실패합니다. 자세한 내용은 Amazon EBS 스냅샷 생성 시 태그 지정 및 더 강력한 보안 정책 구현에 관한 블로그 게시물을 참조하십시오.

AWS Config 규칙을 사용하여 리소스의 구성 설정을 자동으로 평가할 수 AWS 있습니다. 시작하는 데 도움이 되도록 관리형 규칙이라는 사용자 지정 가능하고 사전 정의된 규칙을 AWS Config 제공합니다. 고유의 사용자 지정 규칙을 만들 수도 있습니다. 리소스 간의 구성 변경을 AWS Config 지속적으로 추적하면서 이러한 변경이 규칙의 조건을 위반하는지 확인합니다. 리소스가 규칙을 위반하는 경우 해당 리소스와 규칙을 준수하지 않는 것으로 AWS Config 플래그를 지정합니다. 필수 태그 관리형 규칙은 현재 스냅샷과 AMI를 지원하지 않습니다.

AMI와 EBS 스냅샷을 사용하여 EBS 볼륨 백업 생성

AWS AMI와 스냅샷을 생성하고 관리하기 위한 다양한 옵션을 제공합니다. 사용자는 필요에 맞는 접근 방식을 사용할 수 있습니다. 많은 고객이 직면하는 일반적인 문제는 스냅샷 수명 주기를 관리하고 용도, 보존 정책 등에 따라 스냅샷을 명확하게 정렬하는 것입니다. 적절한 태그를 지정하지 않으면 스냅샷이 실수로 또는 자동화된 클린업 프로세스의 일부로 삭제될 위험이 있습니다. 또한 더 이상 사용되지 않는 스냅샷이 여전히 필요한지 여부를 명확하게 파악할 수 없기 때문에 보관된 스냅샷에 대해 비용을 지불해야 할 수도 있습니다.

스냅샷 또는 AMI를 생성하기 전의 EBS 볼륨 준비

스냅샷을 만들거나 AMI를 생성하기 전에 EBS 볼륨에 필요한 준비를 하십시오. AMI를 생성하면 인스턴스에 연결된 각 EBS 볼륨에 대한 새 스냅샷이 생성되므로 이러한 준비는 AMI에도 적용됩니다.

구동되는 EC2 인스턴스에서 사용 중인 연결된 EBS 볼륨의 스냅샷을 생성할 수 있습니다. 하지만 스냅샷은 snapshot 명령을 실행할 때 EBS 볼륨에 기록된 데이터만 캡처합니다. 이때 애플리케이션이나 운영 체제에 의해 캐시된 데이터가 제외될 수 있습니다. 시스템에서 I/O를 수행하지 않는 상태를 유지하는 것이 가장 좋습니다. 시스템이 트래픽을 수신하지 않고 중지된 상태에 있는 것이 이상적이지만, 연중무휴 IT 운영이 일반화되면서 이러한 경우는 드뭅니다. 시스템 메모리의 모든 데이터를 애플리케이션에서 사용 중인 디스크로 플러시하고 스냅샷을 만들기에 충분한 시간 동안 볼륨에 대한 파일 쓰기 작업을 일시 중지할 수 있는 경우 스냅샷이 완전해야 합니다.

클린 백업을 만들려면 데이터베이스 또는 파일 시스템을 중단해야 합니다. 이 작업을 수행하는 방법은 데이터베이스 또는 파일 시스템에 따라 다릅니다.

데이터베이스 프로세스는 다음과 같습니다.

1. 가능하면 데이터베이스를 핫 백업 모드로 전환합니다.
2. Amazon EBS 스냅샷 명령을 실행합니다.
3. 데이터베이스를 핫 백업 모드에서 해제하거나 읽기 전용 복제본을 사용하는 경우 읽기 전용 복제본 인스턴스를 종료합니다.

파일 시스템의 프로세스는 비슷하지만 운영 체제 또는 파일 시스템의 기능에 따라 다릅니다. 예를 들어, XFS는 일관적 백업을 위해 데이터를 플러시할 수 있는 파일 시스템입니다. 자세한 내용은 xfs_freeze를 참조하십시오. 또는 I/O 정지를 지원하는 논리 볼륨 관리자를 사용하여 이 프로세스를 용이하게 할 수 있습니다.

하지만 볼륨에 대한 모든 파일 쓰기를 플러시하거나 일시 중지할 수 없는 경우 다음을 수행하십시오.

1. 운영 체제에서의 볼륨 마운트를 해제합니다.
2. 스냅샷 명령을 실행합니다.
3. 일관되고 완전한 스냅샷을 만들려면 볼륨을 다시 마운트합니다. 스냅샷 상태가 대기 중인 상태에서 볼륨을 다시 마운트하고 사용할 수 있습니다.

스냅샷 프로세스는 배경에서 계속되며 스냅샷 생성은 빠르며 특정 시점을 캡처합니다. 백업하는 볼륨은 단 몇 초 만에 마운트 해제됩니다. 운영 중단이 예상되고 클라이언트가 정상적으로 처리하는 짧은 백업 기간을 예약할 수 있습니다.

루트 디바이스 역할을 하는 EBS 볼륨의 스냅샷을 생성할 때는 인스턴스를 중지한 후 스냅샷을 생성해야 합니다. Windows는 애플리케이션 정합성이 보장되는 스냅샷을 만들 수 있도록 VSS (볼륨 섀도 복사본 서비스) 를 제공합니다. AWS 는 VSS 인식 애플리케이션의 이미지 레벨 백업을 수행하기 위해 실행할 수 있는 Systems Manager 문서를 제공합니다. 스냅샷에는 이러한 애플리케이션과 디스크 간에 대기 중인 트랜잭션의 데이터가 포함됩니다. 연결된 볼륨을 모두 백업하는 경우 인스턴스를 종료하거나 연결을 해제할 필요가 없습니다. 자세한 내용은 AWS 설명서를 참조하십시오.

> **Note**
>
> 다른 유사한 인스턴스를 배포할 수 있도록 Windows AMI를 생성하는 경우 EC2Config 또는 EC2Launch를 사용하여 인스턴스를 Sysprep하십시오. 그런 다음, 중지된 인스턴스에서 AMI를

생성합니다. Sysprep은 SID, 컴퓨터 이름 및 드라이버 등의 Amazon EC2 Windows 인스턴스에서 고유한 정보를 제거합니다. SID가 중복되면 Active Directory, Windows 서버 업데이트 서비스(WSUS), 로그인 문제, Windows 볼륨 키 활성화, Microsoft Office 및 타사 제품에 문제가 발생할 수 있습니다. AMI가 백업용이고 모든 고유 정보를 그대로 유지한 상태로 동일한 인스턴스를 복원하려는 경우 인스턴스에 Sysprep을 사용하지 마십시오.

콘솔에서 수동으로 EBS 볼륨 스냅샷 생성

인스턴스에서 완전히 테스트되지 않은 주요 변경 사항을 적용하기 전에 적절한 볼륨 또는 전체 인스턴스의 스냅샷을 생성하십시오. 예를 들어, 인스턴스의 애플리케이션 또는 시스템 소프트웨어를 업그레이드하거나 패치를 적용하기 전에 스냅샷을 생성해야 합니다.

콘솔에서 수동으로 스냅샷을 생성할 수 있습니다. Amazon EC2 콘솔의 Elastic Block Store 볼륨 페이지에서 백업하려는 볼륨을 선택합니다. 그런 다음 작업 메뉴에서 스냅샷 생성을 선택합니다. 필터 상자에 인스턴스 ID를 입력하여 특정 인스턴스에 연결된 볼륨을 검색할 수 있습니다.

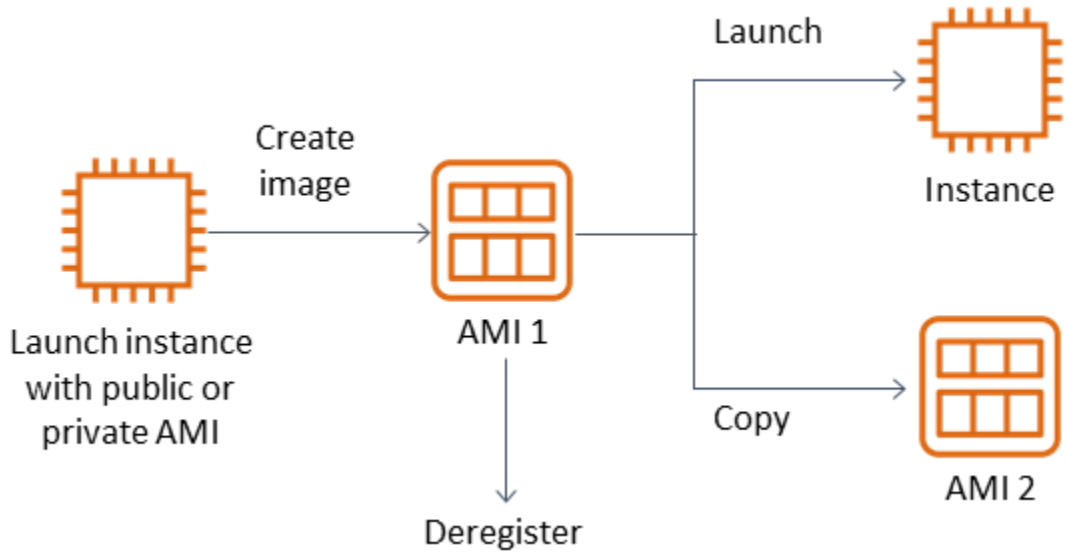
설명을 입력하고 적절한 태그를 추가합니다. 나중에 볼륨을 더 쉽게 찾을 수 있도록 Name 태그를 추가합니다. 태그 지정 전략에 따라 다른 적절한 태그를 추가합니다.

AMI 생성

AMI는 인스턴스를 시작하는 데 필요한 정보를 제공합니다. AMI에는 이미지 생성 시 인스턴스에 연결된 EBS 볼륨의 루트 볼륨과 스냅샷이 포함됩니다. EBS 스냅샷만으로는 새 인스턴스를 시작할 수 없으며 AMI에서 새 인스턴스를 시작해야 합니다.

AMI를 생성하면 사용 중인 계정 및 리전에 생성됩니다. AMI 생성 프로세스는 인스턴스에 연결된 각 볼륨에 대해 Amazon EBS 스냅샷을 생성하고, AMI는 이러한 Amazon EBS 스냅샷을 참조합니다. 이러한 스냅샷은 Amazon S3에 있으며 내구성이 뛰어납니다.

EC2 인스턴스의 AMI를 생성한 후 이 AMI를 사용하여 인스턴스를 다시 생성하거나 인스턴스의 추가 사본을 시작할 수 있습니다. 애플리케이션 마이그레이션 또는 DR을 위해 한 리전에서 다른 리전으로 AMI를 복사할 수도 있습니다.



VMWARE 가상 머신과 같은 가상 머신을 마이그레이션하는 경우가 아니면 EC2 인스턴스에서 AMI를 생성해야 합니다. AWS Amazon EC2 콘솔에서 AMI를 생성하려면 인스턴스를 선택하고 작업, 이미지, 이미지 생성을 차례로 선택합니다.

Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager를 사용하여 Amazon EBS 스냅샷의 생성, 보존 및 삭제를 자동화할 수 있습니다. 스냅샷 관리를 자동화하여 다음과 같은 이점을 누려 보십시오.

- 정기적인 백업 일정을 실행하여 중요한 데이터를 보호합니다.
- 감사 기관이나 내부 규정 준수 부서에서 요구하는 백업을 보관합니다.
- 오래된 백업을 삭제하여 스토리지 비용을 절감합니다.

Amazon Data Lifecycle Manager를 사용하면 EC2 인스턴스(및 연결된 EBS 볼륨) 또는 개별 EBS 볼륨에 대한 스냅샷 관리 프로세스를 자동화할 수 있습니다. 교차 리전 복사와 같은 옵션을 지원하므로 스냅샷을 다른 AWS 리전에 자동으로 복사할 수 있습니다. 대체 리전에 스냅샷을 복사하는 것은 대체 리전의 DR 노력과 복원 옵션을 지원하는 한 가지 방법입니다. 또한 Amazon Data Lifecycle Manager를 사용하여 빠른 스냅샷 복원을 지원하는 스냅샷 수명 주기 정책을 생성할 수 있습니다.

Amazon Data Lifecycle Manager는 Amazon EC2와 Amazon EBS에 포함된 기능입니다. Amazon Data Lifecycle Manager에는 요금이 부과되지 않습니다.

AWS Backup

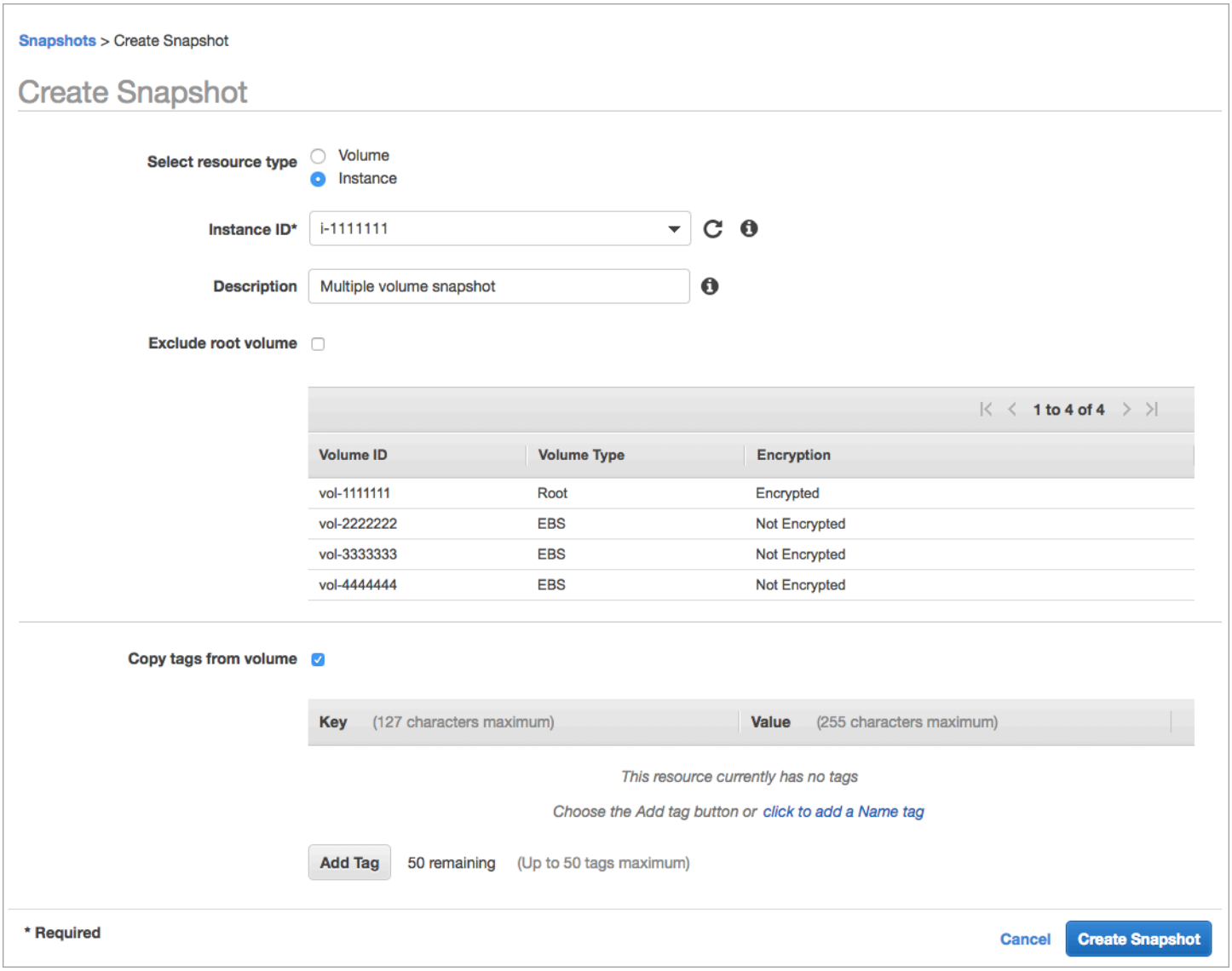
AWS Backup 여러 AWS 서비스의 리소스를 포함하는 백업 계획을 생성할 수 있다는 점에서 Amazon Data Lifecycle Manager와는 다릅니다. 리소스 백업을 개별적으로 조정하는 대신 함께 사용하는 리소스를 포함하도록 백업을 조정할 수 있습니다.

AWS Backup 또한 완료된 백업의 복구 지점에 대한 액세스를 제한할 수 있는 백업 저장소의 개념도 포함되어 있습니다. 각 개별 리소스로 진행하여 생성된 백업을 복원하는 AWS Backup 대신 복원 작업을 바로 시작할 수 있습니다. AWS Backup 감사 관리 및 보고와 같은 다양한 추가 기능도 포함되어 있습니다. 자세한 내용은 이 설명서의 AWS Backup을 사용하여 백업 및 복구 단원을 참조하십시오.

다중 볼륨 백업 수행

스냅샷을 사용하여 RAID 배열의 EBS 볼륨에 데이터를 백업하려는 경우 스냅샷이 일관되어야 합니다. 이러한 볼륨의 스냅샷은 독립적으로 생성되기 때문입니다. 동기화되지 않은 스냅샷을 사용하여 RAID 배열의 EBS 볼륨을 복원할 경우 배열의 무결성이 손상됩니다.

RAID 어레이에 대한 일관된 스냅샷 세트를 생성하려면 CreateSnapshotsAPI 작업을 사용하거나 Amazon EC2 콘솔에 로그인하고 Elastic Block Store, 스냅샷, 스냅샷 생성을 선택합니다.



RAID 구성에서 여러 볼륨이 연결된 인스턴스의 스냅샷은 일괄적으로 다중 볼륨 스냅샷으로 촬영됩니다. 다중 볼륨 스냅샷은 EC2 인스턴스에 연결된 여러 EBS 볼륨에서 데이터가 조정되고 충돌 시에도 정합성이 유지되는 스냅샷을 제공합니다 point-in-time. 스냅샷은 여러 EBS 볼륨에서 자동으로 생성되기 때문에 일관성을 유지하기 위해 인스턴스를 중지하여 볼륨 간을 조정할 필요가 없습니다. 볼륨의 스냅샷이 시작된 후(보통 1~2초) 파일 시스템은 작업을 계속할 수 있습니다.

스냅샷이 생성된 후 각 스냅샷은 개별 스냅샷으로 처리됩니다. 단일 볼륨 스냅샷과 마찬가지로, 복원, 삭제, 교차 리전 및 계정 복사 등의 모든 스냅샷 작업을 수행할 수 있습니다. 또한 단일 볼륨 스냅샷과 마찬가지로 다중 볼륨 스냅샷에도 태그를 지정할 수 있습니다. 복원, 복사 또는 보존 중에 한꺼번에 관리할 수 있도록 다중 볼륨 스냅샷에 태그를 지정하는 것이 좋습니다. 자세한 내용은 AWS 설명서를 참조하십시오.

논리 볼륨 관리자나 파일 시스템 수준 백업에서 이러한 백업을 수행할 수도 있습니다. 이러한 경우 기존 백업 에이전트를 사용하면 네트워크를 통해 데이터를 백업할 수 있습니다. 인터넷과 AWS Marketplace에서 다양한 에이전트 기반 백업 솔루션을 사용할 수 있습니다.

또 다른 방법은 하나의 큰 볼륨에 있는 기본 시스템 볼륨의 복제본을 만드는 것입니다. 이렇게 하면 하나의 큰 볼륨만 백업해야 하고 기본 시스템에서는 백업이 수행되지 않으므로 백업 프로세스가 간소화됩니다. 그러나 먼저 단일 볼륨이 백업 중에 충분한 성능을 발휘할 수 있는지 여부와 최대 볼륨 크기가 애플리케이션에 적합한지 여부를 결정해야 합니다.

Amazon EC2 백업 보호

백업의 보안을 고려하고 백업이 우발적이거나 악의적으로 삭제되는 것을 방지하는 것이 중요합니다. 여러 접근 방식을 일괄적으로 사용하여 이 작업을 수행할 수 있습니다. 보안 침해로 인한 중요한 백업의 손실을 방지하려면 백업을 다른 계정에 복사하는 것이 좋습니다. AWS 여러 AWS 계정이 있는 경우 다른 모든 계정이 백업을 복사할 수 있는 아카이브 계정으로 별도의 계정을 지정할 수 있습니다. 예를 들어, AWS Backup에서 계정 간 백업을 사용하여 이 작업을 수행할 수 있습니다.

또한 재해 복구 계획에 따라 리전별 장애 발생 시 다른 AWS 리전에서 EC2 인스턴스를 복제할 수 있어야 할 수도 있습니다. 백업을 동일한 계정 내의 다른 리전에 복사하여 이 목표를 달성할 수 있습니다. 이를 통해 실수로 인한 삭제 방지를 한층 강화할 수 있을 뿐만 아니라 재해 복구(DR) 목표를 지원할 수 있습니다. AWS Backup은 리전 간 백업을 지원합니다.

ec2: DeleteSnapshot 및 ec2: 작업에 대한 IAM 권한을 차단하는 것을 고려해 보십시오. DeregisterImage 대신 보존 정책 및 메서드로 EBS 스냅샷과 Amazon EC2 AMI의 수명 주기를 관리하도록 할 수 있습니다. 삭제 작업을 차단하는 것은 EBS 스냅샷에 대한 WORM(Write-Once, Read-Many) 전략을 구현하는 한 가지 방법입니다. EBS 스냅샷 및 기타 리소스를 지원하는 AWS Backup Vault Lock을 사용할 수도 있습니다. AWS

또한 ec2: 및 ec2: ModifyImageAttribute IAM 작업을 차단하여 사용자가 AMI와 EBS 스냅샷을 공유하는 기능을 차단하는 것도 고려해 보십시오. ModifySnapshotAttribute 이렇게 하면 AMI와 스냅샷이 조직 외부의 계정과 AWS 공유되지 않습니다. 를 사용하는 AWS Backup 경우 사용자가 백업 저장소에서 유사한 작업을 수행하지 못하도록 제한하십시오. 자세한 내용은 이 설명서의 AWS Backup 단원을 참조하십시오.

Amazon EC2에는 실수로 삭제된 EBS 스냅샷을 복원하는 데 도움이 되는 휴지통 기능이 포함되어 있습니다. 사용자가 스냅샷을 삭제하도록 허용하는 경우 필요한 스냅샷이 영구적으로 삭제되지 않도록 이 기능을 활성화하십시오. Amazon EC2 콘솔에서는 한 번에 여러 스냅샷을 선택하여 삭제할 수 있으므로 사용자는 여러 스냅샷을 삭제할 때 특히 주의해야 합니다. 또한 클린업 스크립트와 자동화를 사용

할 때는 필요한 스냅샷을 실수로 삭제하지 않도록 주의하십시오. 휴지통 기능은 이러한 유형의 상황으로부터 보호하는 데 도움이 됩니다.

EBS 스냅샷 아카이브

EBS 스냅샷 아카이브는 90일 이상 복원할 계획이 없는 참조 목적으로 볼륨 사본을 보관하는 비용 효율적인 방법이 될 수 있습니다. 이는 EBS 볼륨의 모든 관련 스냅샷을 영구 삭제하기 전에 좋은 중간 단계가 될 수 있습니다. 예를 들어 더 이상 사용되지 않는 EBS 볼륨을 위한 end-of-lifecycle 단계로 스냅샷을 보관하는 것을 고려할 수 있습니다. 삭제보다는 아카이브하는 것이 휴지통을 사용하는 것보다 더 비용 효율적인 삭제 보존 방법일 수도 있습니다.

Systems Manager, 및 SDK를 사용하여 스냅샷 및 AMI 생성을 자동화합니다. AWS CLIAWS

백업 접근 방식에는 스냅샷 또는 AMI를 생성하기 전후에 작업이 필요할 수 있습니다. 예를 들어, 파일 시스템을 중단하려면 서비스를 중지한 후 다시 시작해야 할 수 있습니다. 또는 AMI 생성 중에 인스턴스를 중지한 후 다시 시작해야 할 수도 있습니다. 또한 아키텍처에 있는 여러 구성 요소의 백업을 일괄적으로 생성해야 할 수도 있으며, 각 구성 요소에는 별도의 사전 생성 및 사후 생성 단계가 있습니다.

프로세스를 자동화하고 백업 프로세스가 일관되게 적용되는지 확인하여 백업의 유지 관리 기간을 줄일 수 있습니다. 사용자 지정 사전 생성 및 사후 생성 작업을 자동화하려면 및 SDK를 사용하여 백업 프로세스를 스크립팅하십시오. AWS CLI

자동화는 요청 시 또는 Systems Manager 유지 관리 기간 중에 실행할 수 있는 Systems Manager 런북에서 정의할 수 있습니다. Amazon EC2를 방해하는 명령에 대한 권한을 부여할 필요 없이 사용자에게 Systems Manager 런북을 실행할 수 있는 액세스 권한을 부여할 수 있습니다. 또한 이를 통해 백업 프로세스와 태그가 사용자에 의해 일관되게 적용되는지 확인할 수 있습니다. AWS CreateSnapshot 및 AWS CreateImage Runbook을 사용하여 스냅샷과 AMI를 생성하거나 다른 사용자에게 사용 권한을 부여할 수 있습니다. Systems Manager에는 AMI 패치 UpdateLinuxAmi 및 AMI 생성을 자동화하는 AWS 및 AWS UpdateWindowsAmi 런북도 포함되어 있습니다.

및 를 사용하여 스냅샷 AWS CLI 및 AWS Tools for Windows PowerShellAMI 생성 프로세스를 자동화할 수도 있습니다. aws ec2 create-snapshot AWS CLI 명령을 사용하여 자동화의 한 단계로 EBS 볼륨의 스냅샷을 생성할 수 있습니다. aws ec2 create-snapshots 명령을 사용하여 EC2 인스턴스에 연결된 모든 볼륨의 충돌 시에도 일관되고 동기화된 스냅샷을 생성할 수 있습니다.

AWS CLI를 사용하여 새 AMI를 생성할 수 있습니다. aws ec2 register-image 명령을 사용하여 EC2 인스턴스용 새 이미지를 생성할 수 있습니다. 인스턴스의 종료, 이미지 생성 및 재시작을 자동화하려면 이 명령을 aws ec2 stop-instances 및 aws ec2 start-instances 명령과 함께 사용하십시오.

Amazon EBS 볼륨 또는 EC2 인스턴스 복원

EC2 인스턴스에 연결된 단일 볼륨만 복원해야 하는 경우 해당 볼륨을 별도로 복원하고 기존 볼륨을 분리한 다음 복원된 볼륨을 EC2 인스턴스에 연결할 수 있습니다. 모든 관련 볼륨을 포함하여 전체 EC2 인스턴스를 복원해야 하는 경우 인스턴스의 Amazon Machine Image(AMI) 백업을 사용해야 합니다.

복구 시간을 줄이고 종속 애플리케이션 및 프로세스에 미치는 영향을 줄이려면 복원 프로세스에서 대체하는 리소스를 고려해야 합니다. 최상의 결과를 얻으려면 낮은 환경(예: 비 프로덕션 환경)에서 정기적으로 복원 프로세스를 테스트하여 프로세스가 RPO(복구 시점 목표) 및 RTO(복구 시간 목표)를 충족하는지와 복원 프로세스가 예상대로 작동하는지 확인하십시오. 복원 프로세스가 복원 중인 인스턴스에 의존하는 애플리케이션과 서비스에 어떤 영향을 미칠지 생각해 본 다음 필요에 따라 복원을 조정하십시오. 복원 프로세스를 최대한 자동화하고 테스트하여 복원 프로세스가 실패하거나 일관되지 않게 구현될 위험을 줄이십시오.

트래픽을 처리하는 여러 인스턴스와 함께 Elastic Load Balancing을 사용하는 경우 장애가 발생하거나 손상된 인스턴스의 서비스 중단시킬 수 있습니다. 그러면 다른 인스턴스가 사용자에게 영향을 주지 않고 트래픽을 계속 서비스하는 동안 새 인스턴스를 복원하여 이를 대체할 수 있습니다.

설명된 다음 복원 프로세스는 Elastic Load Balancing을 사용하지 않는 인스턴스를 위한 것입니다.

- EBS 스냅샷에서 개별 파일 및 디렉터리 복원
- Amazon EBS 스냅샷에서 EBS 볼륨 복원
- EBS 스냅샷에서 EC2 인스턴스 생성 또는 복원
- AMI에서 실행 중인 인스턴스 복원

EBS 스냅샷에서 파일 및 디렉터리 복원

EBS 스냅샷은 스냅샷을 생성하는 데 사용된 원본 볼륨의 point-in-time 정확한 복제본을 제공합니다. 개별 파일 또는 디렉터리를 복원하려면 다음을 수행해야 합니다.

1. 먼저, 파일 또는 디렉터리가 포함된 EBS 스냅샷에서 볼륨을 복원합니다.
2. 파일을 복원하려는 EC2 인스턴스에 볼륨을 연결합니다.
3. 복원된 볼륨의 파일을 EC2 인스턴스 볼륨으로 복사합니다.
4. 복원된 볼륨을 분리하고 삭제합니다.

Amazon EBS 스냅샷에서 EBS 볼륨 복원

스냅샷에서 볼륨을 생성하고 인스턴스에 연결하여 기존 EC2 인스턴스에 연결된 볼륨을 복원할 수 있습니다. 콘솔 AWS CLI, 또는 API 작업을 사용하여 기존 스냅샷에서 볼륨을 생성할 수 있습니다. 그런 다음 운영 체제를 사용하여 인스턴스에 볼륨을 마운트할 수 있습니다.

Amazon EBS 스냅샷의 데이터는 비동기적으로 EBS 볼륨에 로드된다는 점에 유의하십시오. 애플리케이션이 데이터가 로드되지 않는 볼륨에 액세스하는 경우 Amazon S3에서 데이터를 로드하는 동안 지연 시간이 평소보다 길어집니다. 지연 시간에 민감한 애플리케이션에 이러한 영향을 미치지 않도록 하려면 다음 두 가지 옵션이 있습니다.

- EBS 볼륨을 초기화할 수 있습니다.
- Amazon EBS는 추가 비용을 지불하면 빠른 스냅샷 복원을 지원하므로 볼륨을 초기화할 필요가 없습니다.

동일한 마운트 지점을 사용해야 하는 볼륨을 교체하는 경우, 새 볼륨을 제자리에 마운트할 수 있도록 해당 볼륨을 마운트 해제하십시오. 볼륨을 마운트 해제하려면 먼저 해당 볼륨을 사용하는 모든 프로세스를 중지합니다. 루트 볼륨을 교체하는 경우 루트 볼륨을 분리하기 전에 인스턴스를 먼저 중지해야 합니다.

예를 들어 콘솔을 사용하여 볼륨을 이전 point-in-time 백업으로 복원하려면 다음 단계를 따르십시오.

1. Amazon EC2 콘솔의 Elastic Block Store 메뉴에서 스냅샷을 선택합니다.
2. 복원할 스냅샷을 검색하고 선택합니다.
3. 작업, 볼륨 생성을 차례대로 선택합니다.
4. EC2 인스턴스와 동일한 가용 영역에서 새 볼륨을 생성합니다.
5. Amazon EC2 콘솔에서 인스턴스를 선택합니다.
6. 인스턴스 세부 정보에서 루트 디바이스 항목 또는 블록 디바이스 항목의 교체하려는 디바이스 이름을 기록해 둡니다.
7. 볼륨을 연결합니다. 프로세스는 루트 볼륨과 비루트 볼륨에 따라 다릅니다.

   루트 볼륨의 경우:

   a. EC2 인스턴스를 중지합니다.

   b. EC2 Elastic Block Store 볼륨 메뉴에서 교체하려는 루트 볼륨을 선택합니다.

   c. 작업을 선택한 후 볼륨 분리를 선택합니다.

   d. EC2 Elastic Block Store 볼륨 메뉴에서 새 볼륨을 선택합니다.

   e. 작업을 선택한 후 볼륨 연결을 선택합니다.

f. 볼륨을 연결할 인스턴스를 선택하고 앞서 언급한 것과 동일한 디바이스 이름을 사용합니다.

비루트 볼륨의 경우:

a. EC2 Elastic Block Store 볼륨 메뉴에서 교체하려는 비루트 볼륨을 선택합니다.

b. 작업을 선택한 후 볼륨 분리를 선택합니다.

c. EC2 Elastic Block Store 볼륨 메뉴에서 새 볼륨을 선택한 다음 작업, 볼륨 연결을 선택하여 새 볼륨을 연결합니다. 연결할 인스턴스를 선택한 다음 사용 가능한 디바이스 이름을 선택합니다.

d. 인스턴스의 운영 체제를 사용하여 기존 볼륨을 마운트 해제한 다음 새 볼륨을 제자리에 마운트합니다.

   Linux에서 `umount` 명령을 사용할 수 있습니다. Windows에서는 디스크 관리 시스템 유틸리티와 같은 LVM(논리 볼륨 관리자)을 사용할 수 있습니다.

e. EC2 Elastic Block Store 볼륨 메뉴에서 이전 볼륨을 선택한 다음 작업, 볼륨 분리를 선택하여 교체할 이전 볼륨을 분리합니다.

를 운영 체제 명령과 함께 사용하여 이러한 단계를 자동화할 수도 있습니다. AWS CLI

EBS 스냅샷에서 EC2 인스턴스 생성 또는 복원

전체 EC2 인스턴스를 복원하는 데 사용할 백업을 생성하려면 Amazon Machine Image(AMI)를 생성하는 것이 좋습니다. AMI는 가상화 유형과 같은 머신 정보를 캡처합니다. 또한 디바이스 매핑을 포함하여 EC2 인스턴스에 연결된 각 볼륨에 대한 스냅샷을 생성하므로 동일한 구성으로 복원할 수 있습니다.

하지만 EBS 스냅샷을 사용하여 인스턴스를 복원해야 하는 경우 먼저 새 EC2 인스턴스의 루트 볼륨이 될 EBS 스냅샷에서 AMI를 생성하십시오.

1. Amazon EC2 콘솔의 Elastic Block Store 메뉴에서 스냅샷을 선택합니다.
2. 새 EC2 인스턴스의 루트 볼륨을 생성하는 데 사용할 스냅샷을 검색하고 선택합니다.
3. 작업을 선택한 후 스냅샷에서 이미지 생성을 선택합니다.
4. 이미지 이름(예:`YYYYMMDD-restore-for-i-012345678998765de`)을 입력하고 새 이미지에 적합한 옵션을 선택합니다.

이미지를 생성하여 사용할 수 있게 되면 해당 EBS 스냅샷을 루트 볼륨에 사용할 새 EC2 인스턴스를 시작할 수 있습니다.

AMI에서 실행 중인 인스턴스 복원

AMI 백업에서 새 인스턴스를 가져와서 실행 중인 기존 인스턴스를 대체할 수 있습니다. 한 가지 접근 방식은 기존 인스턴스를 중지하고 AMI에서 새 인스턴스를 시작하는 동안 오프라인 상태로 유지하면서 필요한 업데이트를 수행하는 것입니다. 이러한 접근 방식을 사용하면 두 인스턴스가 동시에 실행될 때 충돌이 발생할 위험이 줄어듭니다. 인스턴스가 제공하는 서비스가 중단되거나 유지 관리 기간 중에 복원을 수행하는 경우 적합한 접근 방식입니다. 새 인스턴스를 테스트한 후 이전 인스턴스에 할당되었던 탄력적 IP 주소를 재할당할 수 있습니다. 그런 다음 새 인스턴스를 가리키도록 모든 도메인 이름 시스템(DNS) 레코드를 업데이트할 수 있습니다.

그러나 복원 중에 서비스 중인 인스턴스의 가동 중지 시간을 최소화해야 하는 경우 AMI 백업에서 새 인스턴스를 시작하고 테스트해 보십시오. 그런 다음 기존 인스턴스를 새 인스턴스로 교체합니다.

두 인스턴스가 모두 실행 중일 때는 새 인스턴스가 플랫폼 수준 또는 애플리케이션 수준 충돌을 일으키지 않도록 해야 합니다. 예를 들어, 동일한 SID와 컴퓨터 이름으로 실행되는 도메인에 가입된 Windows 인스턴스에서 문제가 발생할 수 있습니다. 고유 식별자가 필요한 네트워크 애플리케이션 및 서비스에서도 비슷한 문제가 발생할 수 있습니다.

준비가 되기 전에 다른 서버 및 서비스가 새 인스턴스에 연결하지 못하도록 하려면 보안 그룹을 사용하여 액세스 및 테스트용 자체 IP 주소를 제외한 새 인스턴스의 모든 인바운드 연결을 일시적으로 차단하십시오. 또한 새 인스턴스의 아웃바운드 연결을 일시적으로 차단하여 서비스와 애플리케이션이 다른 리소스에 대한 연결이나 업데이트를 시작하지 못하게 할 수 있습니다. 새 인스턴스가 준비되면 기존 인스턴스를 중지하고 새 인스턴스에서 서비스와 프로세스를 시작한 다음 구현한 인바운드 또는 아웃바운드 네트워크 연결의 차단을 해제하십시오.

온프레미스 인프라에서 AWS로 백업 및 복구

온프레미스 인프라 AWS 백업의 내구성이 뛰어난 오프사이트 스토리지로 사용할 수 있습니다. 이 시나리오에서 AWS 스토리지 서비스를 사용하면 백업 및 보관 작업에 집중할 수 있습니다. 백업 작업을 위한 스토리지 인프라 프로비저닝, 확장 또는 인프라 용량에 대해 걱정할 필요가 없습니다.

Amazon S3는 신규 및 기존 백업 및 복구 접근 방식에 통합할 수 있는 광범위한 API 작업 및 SDK를 제공합니다. 또한 백업 소프트웨어 공급업체는 애플리케이션을 AWS 스토리지 솔루션과 직접 통합할 수 있는 방법을 백업 소프트웨어 공급업체에 제공합니다.

이 시나리오에서는 온프레미스 인프라에서 사용하는 백업 및 아카이브 소프트웨어가 API 작업을 AWS 통해 직접 인터페이스합니다. 백업 소프트웨어는 AWS-인식을 하기 때문에 온프레미스 서버의 데이터를 Amazon S3로 직접 백업합니다.

기존 백업 소프트웨어가 AWS 클라우드를 기본적으로 지원하지 않는 경우 Storage Gateway를 사용할 수 있습니다. 클라우드 스토리지 서비스인 Storage Gateway는 온프레미스 시스템에 확장 가능한 클라우드 스토리지에 대한 액세스를 제공합니다. Amazon S3에 데이터를 암호화하여 안전하게 저장하면서 기존 애플리케이션과 함께 작동하는 개방형 표준 스토리지 프로토콜을 지원합니다. Storage Gateway를 온프레미스 블록 기반 스토리지 워크로드에 대한 백업 및 복구 접근 방식의 일부로 사용할 수 있습니다.

Storage Gateway는 백업을 위해 클라우드 기반 스토리지로 전환하려는 하이브리드 시나리오에서 유용합니다. 또한, Storage Gateway는 온프레미스 스토리지에 대한 자본 투자를 줄이는 데 도움이 됩니다. 사용자는 Storage Gateway를 VM 또는 전용 하드웨어 어플라이언스로 배포합니다. 이 설명서에서는 Storage Gateway가 백업 및 복구에 적용되는 방식을 중점적으로 다룹니다.

Storage Gateway는 다양한 요구 사항을 충족할 수 있는 세 가지 옵션을 제공합니다.

- SMB 기반 또는 NFS 기반 액세스를 사용하여 Amazon S3 클라우드 스토리지에 애플리케이션 데이터 파일 및 백업 이미지를 내구성 있는 객체로 저장하기 위한 파일 게이트웨이입니다.
- 클라우드 기반 iSCSI 블록 스토리지 볼륨을 온프레미스 애플리케이션에 제공하기 위한 볼륨 게이트웨이입니다. 볼륨 게이트웨이는 로컬 캐시 또는 전체 볼륨을 온프레미스로 제공하는 동시에 볼륨의 전체 사본을 AWS 클라우드에 저장합니다.
- 신뢰할 수 있는 백업 소프트웨어가 온 프레미스 스토리지 게이트웨이를 가리키도록 하고, 이를 Amazon S3에 연결하는 테이프 게이트웨이입니다. 이 옵션은 기존 투자 또는 프로세스를 중단하지 않고 안전하게 장기간 보존할 수 있도록 클라우드의 확장성과 내구성을 제공합니다.

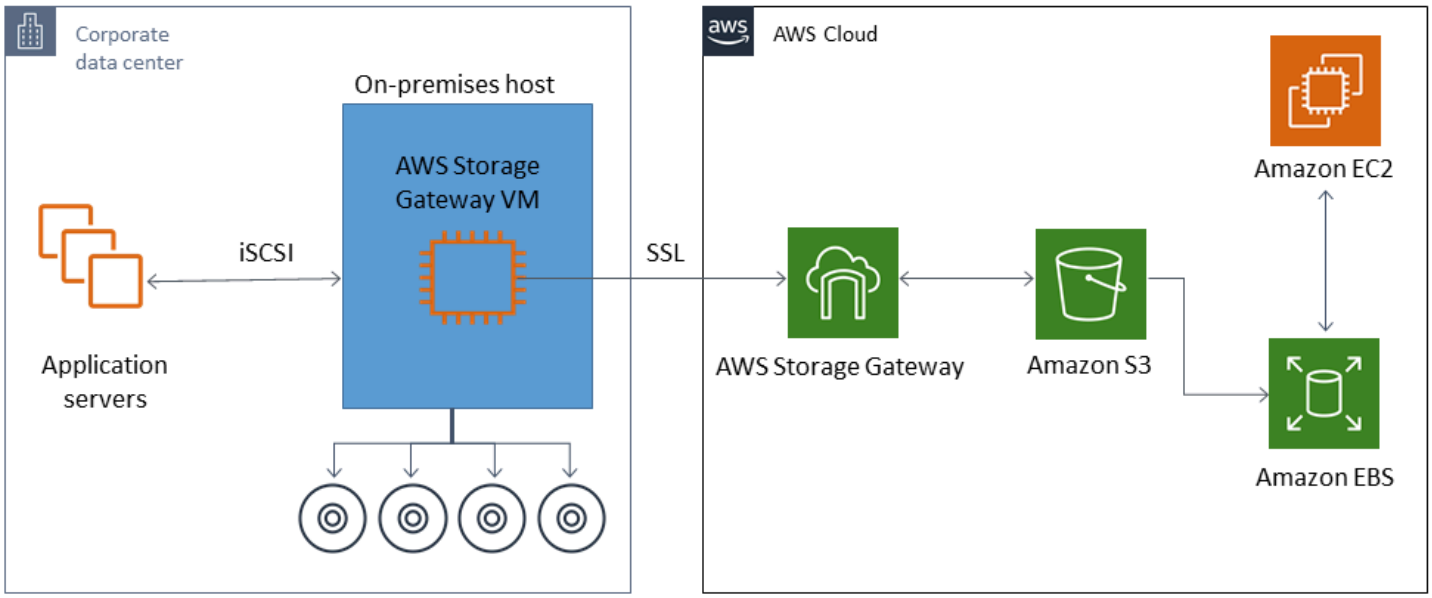
파일 게이트웨이

많은 조직이 백업과 같은 2차 및 3차 데이터를 클라우드로 이동하는 것으로 클라우드 여정을 시작합니다. 파일 게이트웨이의 SMB 및 NFS 인터페이스 지원을 통해 IT 그룹은 기존 온프레미스 백업 시스템에서 클라우드로 백업 작업을 전환할 수 있습니다. SMB 또는 NFS에 쓸 수 있는 백업 애플리케이션, 네이티브 데이터베이스 툴 또는 스크립트는 파일 게이트웨이에 쓸 수 있습니다. 파일 게이트웨이는 백업을 최대 5TiB 크기의 Amazon S3 객체로 저장합니다. 적절한 크기의 로컬 캐시로 최근 백업을 사용하여 현장에서 빠르게 복구할 수 있습니다. 장기 보존 요구 사항은 백업을 저렴한 S3 스탠다드-인프레시언트 액세스 및 S3 Glacier 스토리지 클래스로 계층화하여 해결합니다.

파일 게이트웨이는 Amazon S3에 블록 기반 스토리지를 위한 온램프를 제공하여 내구성이 뛰어난 오프사이트 백업을 제공합니다. 이는 최근에 백업한 파일을 빠르게 복원해야 하는 시나리오에 특히 유용합니다. 파일 게이트웨이는 SMB 및 NFS 프로토콜을 지원하므로 사용자는 네트워크 파일 공유에 액세스하는 것과 같은 방식으로 파일에 액세스할 수 있습니다. Amazon S3 객체의 버전 관리 기능을 활용할 수도 있습니다. 객체 버전 관리를 사용하면 파일의 이전 객체 버전을 복원한 후에 SMB 또는 NFS를 사용하여 쉽게 액세스할 수 있습니다.

볼륨 게이트웨이

볼륨 게이트웨이를 사용하면 온프레미스 서버에 대해 클라우드 기반 iSCSI 블록 스토리지 볼륨을 프로비저닝할 수 있습니다. 볼륨 게이트웨이는 안정적이고 확장 가능한 클라우드 기반 오프사이트 스토리지를 위해 볼륨 데이터를 Amazon S3에 저장합니다. 볼륨 게이트웨이를 사용하면 볼륨의 전체 point-in-time 스냅샷을 손쉽게 생성하여 클라우드에 Amazon EBS 스냅샷으로 저장할 수 있습니다. 스냅샷으로 저장한 후에는 전체 볼륨을 EBS 볼륨으로 복원하고 EC2 인스턴스에 연결할 수 있으므로 클라우드 기반 DR 솔루션을 가속화할 수 있습니다. 또한, 볼륨을 Storage Gateway로 복원하여 온프레미스 애플리케이션을 이전 상태로 되돌릴 수 있습니다.



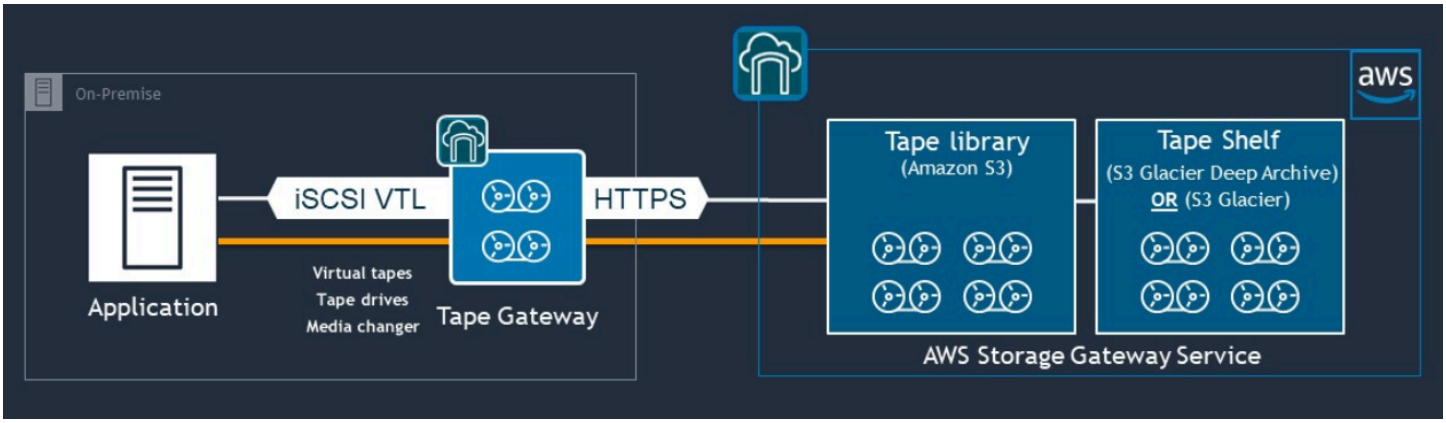
볼륨 게이트웨이는 Amazon EC2의 Amazon EBS 볼륨 기능과 통합되므로 스냅샷 프로세스를 자동화하고 일정을 잡는 데 AWS Backup 사용할 수 있습니다. 볼륨 게이트웨이는 내구성이 뛰어난 Amazon S3–backed Amazon EBS 스냅샷 및 태깅 기능의 이점을 추가로 제공합니다. 자세한 내용은 Amazon EBS 스냅샷 설명서를 참조하십시오.

Tape Gateway

테이프 게이트웨이는 오프사이트 가상 테이프 백업 스토어를 위한 Amazon S3의 뛰어난 내구성, 저렴한 계층형 스토리지 및 광범위한 기능을 제공합니다. Amazon S3에 저장된 모든 가상 테이프는 지리적으로 분산된 3개 이상의 가용 영역에 복제 및 저장됩니다. 가상 테이프는 99.999999999%의 내구성으로 보호됩니다.

AWS 또한 정기적으로 수정 검사를 수행하여 데이터를 읽을 수 있고 오류가 발생하지 않았는지 확인합니다. Amazon S3에 저장된 모든 테이프는 기본 키 또는 사용자 키를 사용하는 서버 측 암호화로 보호됩니다. AWS KMS 또한, 테이프 휴대성과 관련된 물리적 보안 위험을 피할 수 있습니다. 테이프 게이트웨이를 사용하면 복원 중에 부정확하거나 손상된 테이프를 받을 수 있는 테이프의 오프사이트 웨어하우징에 비해 정확한 데이터를 얻을 수 있습니다.

Amazon S3에 데이터를 저장하면 매달 스토리지 비용을 절약할 수 있습니다. S3 Glacier Deep Archive를 사용하면 장기 보관이 필요할 때 훨씬 더 많은 비용을 절약할 수 있습니다.



테이프 게이트웨이는 온프레미스 환경에서부터 Amazon S3, S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive와 같이 확장성, 중복성, 내구성이 뛰어난 스토리지 서비스까지 아우르는 가상 테이프 라이브러리(VTL)의 역할을 합니다.

테이프 게이트웨이는 Storage Gateway를 기존 백업 애플리케이션에 가상 미디어 체인저 및 가상 테이프 드라이브가 포함된 개방형 표준 iSCSI 기반 VTL로 제공합니다. 대규모로 확장 가능한 Amazon S3에 저장된 가상 테이프 컬렉션에 기록하면서 기존의 백업 애플리케이션과 워크플로우를 계속 사용할 수 있습니다. 더 이상 가상 테이프의 데이터에 즉시 또는 자주 액세스할 필요가 없는 경우, 백업 애플리케이션이 해당 데이터를 S3 Glacier Flexible Retrival 또는 S3 Glacier Deep Archive에 보관할 수 있으므로 스토리지 비용을 더욱 절감할 수 있습니다.

S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브된 테이프는 일반적으로 각각 3~5시간 또는 12시간 내에 검색할 수 있습니다. 테이프 게이트웨이는 가상 테이프에 액세스하기 위한 iSCSI 기반 테이프 라이브러리 인터페이스와 호환되는 백업 애플리케이션과 함께 사용할 수 있습니다. 또한, 테이프당 최소 100GB의 스토리지 크기도 고려해 보십시오. 자세한 내용은 테이프 게이트웨이를 지원하는 타사 백업 애플리케이션 목록을 검토해 보십시오.

AWS에서 데이터 센터로 애플리케이션 백업 및 복구

클라우드 기반 워크로드 및 온프레미스 인프라를 위한 DR 또는 비즈니스 연속성과 같은 시나리오를 구현하도록 요구하는 정책이 있을 수 있습니다. 온프레미스 서버용 데이터 백업 프레임워크가 이미 있는 경우 이를 VPN 연결 또는 AWS Direct Connect를 통해 AWS 리소스까지 확장할 수 있습니다. EC2 인스턴스에 백업 에이전트를 설치하고 데이터 보호 정책에 따라 데이터와 애플리케이션을 백업할 수 있습니다. 또한 Amazon S3를 애플리케이션 수준 백업을 저장하는 중간 서비스로 사용할 수 있습니다. 그런 다음 API 작업, SDK 또는 AWS CLI를 사용하여 데이터를 온프레미스 환경에 복원할 수 있습니다.

Amazon EC2 이외의 AWS 서비스에 데이터를 백업하려면 AWS CLI, SDK 및 API 작업을 사용하여 데이터를 원하는 형식으로 추출하십시오. 그런 다음 Amazon S3로 데이터를 복사하고, Amazon S3에서 온프레미스 환경으로 데이터를 복사합니다. 일부 서비스는 Amazon S3로 직접 내보냅니다. 예를 들어, Amazon RDS는 Microsoft SQL Server 데이터베이스를 Amazon S3에 네이티브 백업할 수 있도록 지원합니다.

클라우드 네이티브 AWS 서비스의 백업 및 복구

백업 및 복구 접근 방식에는 워크로드에 사용되는 AWS 서비스가 포함되어야 합니다. AWS은(는) 데이터 관리 및 상호 작용을 위한 서비스별 기능과 옵션을 제공합니다. 콘솔, AWS CLI, SDK 및 API 작업을 사용하여 사용 중인 AWS 서비스에 대한 백업 및 복구를 구현할 수 있습니다. 이 가이드는 Amazon RDS와 Amazon DynamoDB를 예로 들어 설명합니다. AWS Backup은(는) DynamoDB와 Amazon RDS를 모두 지원하므로 요구 사항을 충족하는 경우 사용하시기 바랍니다.

Amazon RDS의 백업 및 복구

Amazon RDS에는 데이터베이스 백업을 자동화하는 기능이 포함되어 있습니다. Amazon RDS는 데이터베이스 인스턴스의 스토리지 볼륨 스냅샷을 생성하여 개별 데이터베이스만 백업하는 것이 아니라 전체 DB 인스턴스를 백업합니다. Amazon RDS를 사용하면 자동 백업을 위한 백업 기간을 설정하고, 데이터베이스 인스턴스 스냅샷을 생성하고, 리전 및 계정 간에 스냅샷을 공유하고 복사할 수 있습니다.

Amazon RDS는 DB 인스턴스를 백업하고 복원하기 위한 두 가지 옵션을 제공합니다.

- 자동 백업은 DB 인스턴스의 특정 시점 복구(PITR)를 제공합니다. 새 DB 인스턴스를 생성할 때 자동 백업이 기본적으로 활성화됩니다.

  Amazon RDS는 DB 인스턴스를 생성할 때 사용자가 정의한 백업 기간 동안 데이터를 매일 전체 백업합니다. 자동 백업에 대해 최대 35일까지 보존 기간을 구성할 수 있습니다. 또한 Amazon RDS는 5분마다 DB 인스턴스에 대한 트랜잭션 로그를 Amazon S3에 업로드합니다. Amazon RDS는 데이터베이스 트랜잭션 로그와 함께 일일 백업을 사용하여 DB 인스턴스를 복원합니다. 보존 기간 중 최대 `LatestRestorableTime`까지(일반적으로 최근 5분) 인스턴스를 복원할 수 있습니다.

  DB 인스턴스의 복원 가능한 최신 시간을 찾으려면 `DescribeDBInstances` API 호출을 사용하세요. 또는 Amazon RDS 콘솔에서 데이터베이스의 설명 탭을 찾아보세요.

  PITR을 시작하면 트랜잭션 로그가 가장 적절한 일일 백업과 결합되어 DB 인스턴스를 요청한 시간으로 복원합니다.
- DB 스냅샷은 DB 인스턴스를 원하는 만큼 알려진 상태로 복원하는 데 사용할 수 있는 사용자 시작 백업입니다. 그러면 언제든지 해당 상태로 복원할 수 있습니다. Amazon RDS 콘솔 또는 `CreateDBSnapshot` API 호출을 사용하여 DB 스냅샷을 생성할 수 있습니다. 이러한 스냅샷은 콘솔이나 `DeleteDBSnapshot` API 호출을 사용하여 명시적으로 삭제할 때까지 보관됩니다.

이 두 백업 옵션 모두 AWS Backup의 Amazon RDS에서 지원되며 다른 기능도 제공합니다. Amazon RDS 데이터베이스의 표준 백업 계획을 설정하는 데 AWS Backup을(를) 사용하고, 특정 데이터베이스의 백업 계획이 다르면 사용자가 시작한 인스턴스 백업 옵션을 사용하는 것이 좋습니다.

Amazon RDS는 DB 인스턴스가 사용하는 기본 스토리지에 직접 액세스하는 것을 방지합니다. 또한 이렇게 하면 RDS DB 인스턴스의 데이터베이스를 로컬 디스크로 직접 내보낼 수 없습니다. 경우에 따라 클라이언트 유틸리티를 사용하여 기본 백업 및 복원 기능을 사용할 수 있습니다. 예를 들어, Amazon RDS MySQL 데이터베이스와 함께 mysqldump 명령을 사용하여 데이터베이스를 로컬 클라이언트 시스템으로 내보낼 수 있습니다. 경우에 따라 Amazon RDS는 데이터베이스의 기본 백업 및 복원을 수행할 수 있는 확장된 옵션도 제공합니다. 예를 들어 Amazon RDS는 SQL Server 데이터베이스의 RDS 데이터베이스 백업을 내보내고 가져오기 위한 저장 프로시저를 제공합니다.

전반적인 백업 및 복원 접근 방식의 일환으로 데이터베이스 복원 프로세스와 데이터베이스 클라이언트에 미치는 영향을 철저하게 테스트해야 합니다.

DNS CNAME 레코드를 사용하면 데이터베이스 복구 중에 클라이언트에 미치는 영향을 줄일 수 있습니다.

PITR 또는 RDS DB 인스턴스 스냅샷을 사용하여 데이터베이스를 복원하면 새 엔드포인트가 있는 새 DB 인스턴스가 생성됩니다. 이렇게 하면 특정 DB 스냅샷 또는 특정 시점에서 여러 DB 인스턴스를 만들 수 있습니다. 라이브 RDS DB 인스턴스를 대체하기 위해 RDS DB 인스턴스를 복원할 때는 특히 고려해야 할 사항이 있습니다. 예를 들어 중단과 수정을 최소화하면서 기존 데이터베이스 클라이언트를 새 인스턴스로 리디렉션할 방법을 결정해야 합니다. 새 인스턴스가 쓰기를 받기 시작할 때의 복원된 데이터 시간과 복구 시간을 고려하여 데이터베이스 내 데이터의 연속성과 일관성을 보장해야 합니다.

DB 인스턴스 엔드포인트를 가리키는 별도의 DNS CNAME 레코드를 만들고 클라이언트가 이 DNS 이름을 사용하도록 할 수 있습니다. 그러면 데이터베이스 클라이언트를 업데이트할 필요 없이 CNAME이 복원된 새 엔드포인트를 가리키도록 업데이트할 수 있습니다.

CNAME 레코드의 Time to Live(TTL)를 적절한 값으로 설정합니다. 지정하는 TTL에 따라 다른 요청이 이루어지기 전에 DNS 해석기로 레코드를 캐시하는 데 걸리는 시간이 결정됩니다. 참고로 일부 DNS 해석기 또는 애플리케이션은 TTL을 준수하지 않을 수 있으며 TTL보다 더 오래 레코드를 캐시할 수 있습니다. Amazon Route 53의 경우, 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간이 줄어들고 Route 53 서비스에 대한 요금이 절감됩니다. 자세한 내용은 Amazon Route 53이 도메인의 트래픽을 라우팅하는 방법을 참조하세요.

애플리케이션과 클라이언트 운영 체제는 새 DNS 확인 요청을 시작하고 업데이트된 CNAME 레코드를 검색하기 위해 플러시하거나 다시 시작해야 하는 DNS 정보를 캐시할 수도 있습니다.

데이터베이스 복원을 시작하고 복원된 인스턴스로 트래픽을 이동할 때는 모든 클라이언트가 이전 인스턴스 대신 복원된 인스턴스에 쓰고 있는지 확인하세요. 데이터 아키텍처는 데이터베이스를 복원하고, 복원된 인스턴스로 트래픽을 이동하도록 DNS를 업데이트하며, 이전 인스턴스에 아직 기록되어 있을 수 있는 모든 데이터를 수정하는 것을 지원할 수 있습니다. 그렇지 않은 경우 DNS CNAME 레코드를 업데이트하기 전에 기존 인스턴스를 중지할 수 있습니다. 그러면 새로 복원된 인스턴스에서 모든 액세스가 이루어집니다. 이로 인해 일부 데이터베이스 클라이언트에 일시적으로 연결 문제가 발생할 수 있으며, 이는 개별적으로 처리할 수 있습니다. 클라이언트에 미치는 영향을 줄이려면 유지 관리 기간 중에 데이터베이스 복원을 수행하시기 바랍니다.

지수 백오프를 사용한 재시도를 통해 데이터베이스 연결 실패를 적절하게 처리하도록 애플리케이션을 작성하세요. 이렇게 하면 복원 중에 데이터베이스 연결을 사용할 수 없게 되어도 애플리케이션이 예기치 않게 충돌하지 않고 복구할 수 있습니다.

복원 프로세스를 완료한 후 이전 인스턴스를 중지된 상태로 유지할 수 있습니다. 또는 보안 그룹 규칙을 사용하여 더 이상 필요하지 않다고 판단될 때까지 이전 인스턴스에 대한 트래픽을 제한할 수 있습니다. 점진적인 서비스 해제 방식을 취하려면 먼저 보안 그룹이 실행 중인 데이터베이스에 대한 액세스를 제한하세요. 더 이상 필요하지 않은 인스턴스는 결국 중지할 수 있습니다. 마지막으로 데이터베이스 인스턴스의 스냅샷을 만들고 삭제합니다.

DynamoDB의 백업 및 복구

DynamoDB는 DynamoDB 테이블 데이터를 거의 연속적으로 백업하는 PITR을 제공합니다. 활성화되면 DynamoDB는 사용자가 명시적으로 비활성화할 때까지 지난 35일 간 테이블의 증분 백업을 유지합니다.

또한 DynamoDB 콘솔 AWS CLI 또는 DynamoDB API를 사용하여 DynamoDB 테이블의 온디맨드 백업을 생성할 수 있습니다. 자세한 내용은 DynamoDB 테이블 백업을 참조하세요. AWS Backup을(를) 사용하여 정기적인 백업이나 향후 백업을 예약하거나, Lambda 함수를 사용하여 백업 접근 방식을 사용자 지정 및 자동화할 수 있습니다. DynamoDB 백업에 Lambda 함수를 사용하는 방법에 대한 자세한 내용은 블로그 게시물 Amazon DynamoDB 온디맨드 백업 예약을 위한 서버리스 솔루션을 참조하세요. 예약 스크립트 및 정리 작업을 생성하지 않으려면 AWS Backup을(를) 사용하여 백업 계획을 생성할 수 있습니다. 백업 계획에는 DynamoDB 테이블의 일정 및 보존 정책이 포함됩니다. AWS Backup은(는) 보존 일정에 따라 백업을 생성하고 이전 백업을 삭제합니다. AWS Backup에는 또한 저렴한 계층형 스토리지, 계정 간 및 리전 간 복사를 포함하여 DynamoDB 서비스에서는 사용할 수 없는 고급 DynamoDB 백업 옵션도 포함되어 있습니다. 자세한 내용은 고급 DynamoDB 백업을 참조하세요.

복원된 DynamoDB 테이블에서 다음을 수동으로 설정해야 합니다.

- 자동 규모 조정 정책

- IAM 정책
- Amazon CloudWatch 지표 및 경보
- 태그
- 스트림 설정
- TTL 설정

전체 테이블 데이터만 백업에서 새 테이블로 복원할 수 있습니다. 복원된 테이블은 활성 상태가 된 이후에만 쓸 수 있습니다.

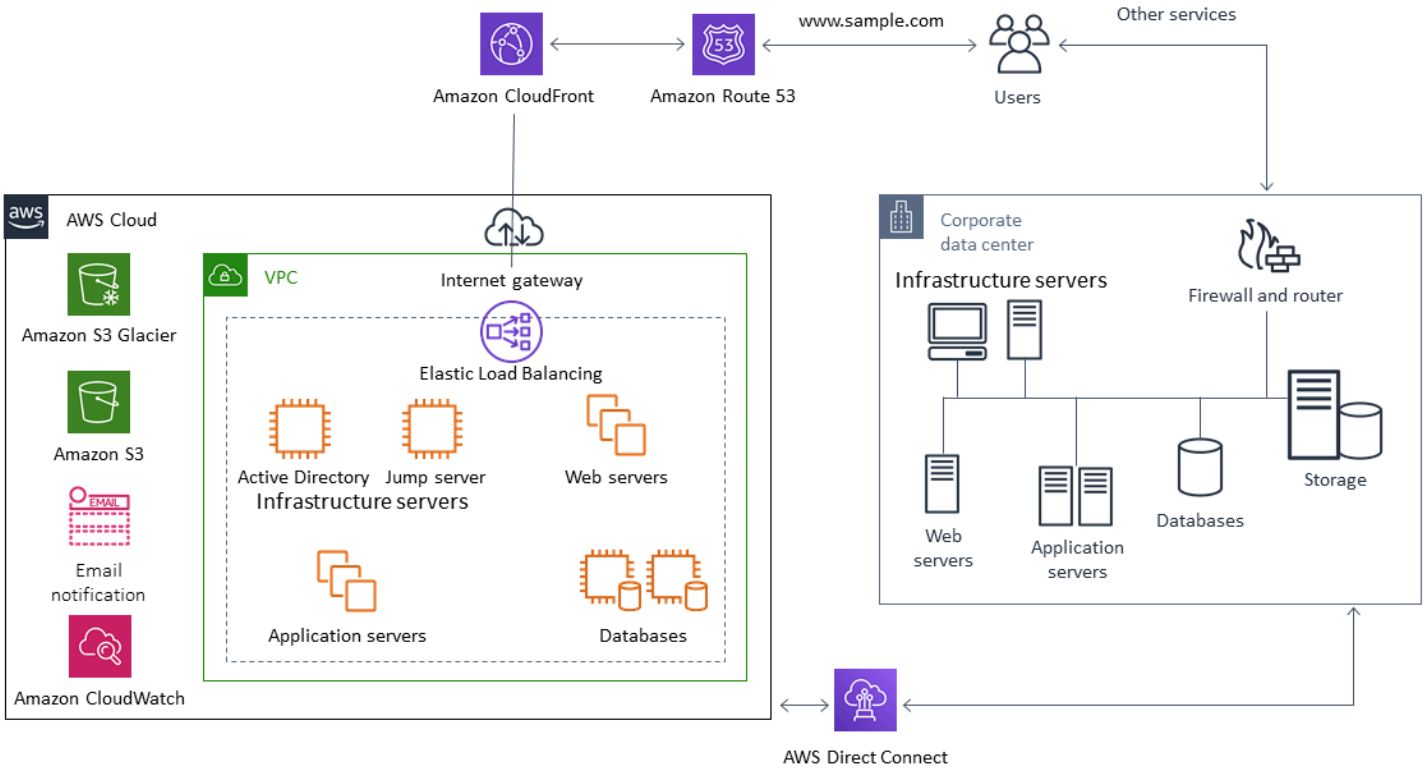
복원 프로세스는 클라이언트가 새로 복원된 테이블 이름을 사용하도록 지시하는 방법을 고려해야 합니다. 구성 파일, AWS Systems Manager Parameter Store 값 또는 클라이언트가 사용해야 하는 테이블 이름을 반영하도록 동적으로 업데이트할 수 있는 다른 참조에서 DynamoDB 테이블 이름을 검색하도록 애플리케이션과 클라이언트를 구성할 수 있습니다.

복원 프로세스의 일환으로 전환 프로세스를 신중하게 고려해야 합니다. IAM 권한을 통해 기존 DynamoDB 테이블에 대한 액세스를 거부하고 새 테이블에 대한 액세스를 허용하도록 선택할 수 있습니다. 그런 다음 새 테이블을 사용하도록 애플리케이션과 클라이언트 구성을 업데이트할 수 있습니다. 기존 DynamoDB 테이블과 새로 복원된 DynamoDB 테이블 간의 차이를 조정해야 할 수도 있습니다.

하이브리드 아키텍처를 위한 백업 및 복구

이 가이드에서 설명하는 클라우드 네이티브 및 온프레미스 배포는 워크로드 환경에 온프레미스 및 인프라 구성 요소가 있는 하이브리드 시나리오로 결합할 수 있습니다. AWS 웹 서버, 애플리케이션 서버, 모니터링 서버, 데이터베이스 및 Microsoft Active Directory를 비롯한 리소스는 고객 데이터 센터 또는 AWS에서 호스팅됩니다. AWS 클라우드에서 실행되는 애플리케이션은 온프레미스에서 실행되는 애플리케이션에 연결됩니다.

이것은 엔터프라이즈 워크로드의 일반적인 시나리오가 되고 있습니다. 많은 기업이 자체 데이터 센터를 보유하고 있으며 용량을 늘리는 AWS 데 사용합니다. 이러한 고객 데이터 센터는 대용량 네트워크 링크를 통해 AWS 네트워크에 연결되는 경우가 많습니다. 예를 AWS Direct Connect들어 를 사용하면 온프레미스 데이터 센터에서 사설 전용 연결을 설정할 수 있습니다. AWS이는 데이터 보호를 위해 데이터를 클라우드에 업로드할 수 있는 대역폭과 일관된 지연 시간을 제공합니다. 또한, 하이브리드 워크로드에 일관된 성능과 지연 시간을 제공합니다. 아래의 다이어그램은 하이브리드 환경 접근 방식의 한 가지 예를 제공합니다.



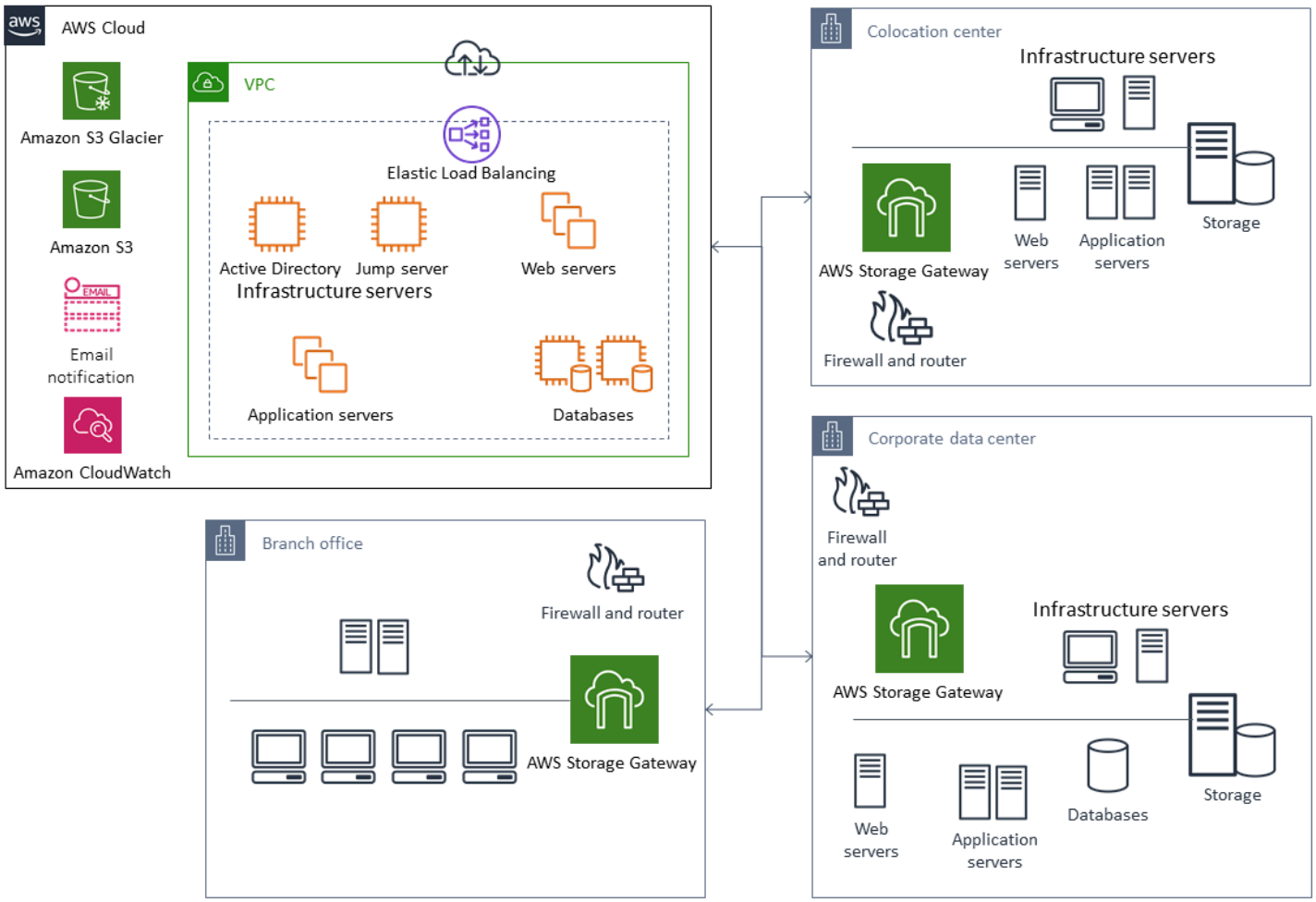
잘 설계된 데이터 보호 솔루션은 일반적으로 이 설명서의 클라우드 네이티브 솔루션과 온프레미스 솔루션에서 설명된 옵션을 조합하여 사용합니다. 많은 ISV는 온프레미스 인프라를 위해 업계 최고의 백업 및 복원 솔루션을 제공하며 하이브리드 접근 방식을 지원하도록 솔루션을 확장했습니다.

가용성을 높이기 위해 중앙 집중식 백업 관리 솔루션을 클라우드로 이전합니다.

에 투자한 기존 백업 관리 솔루션을 사용하면 접근 방식의 복원력과 아키텍처를 개선할 수 있습니다. AWS기본 백업 서버와 하나 이상의 미디어 또는 스토리지 서버가 보호 중인 서버 및 서비스와 가까운 여러 위치 전반에서 온프레미스에 있을 수 있습니다. 이 경우 온프레미스 재해로부터 보호하고 고가용성을 확보하기 위해 기본 백업 서버를 EC2 인스턴스로 이동하는 것을 고려해 보십시오.

백업 데이터 플로우를 관리하기 위해 보호할 서버와 동일한 리전의 EC2 인스턴스에 미디어 서버를 하나 이상 생성할 수 있습니다. EC2 인스턴스 근처의 미디어 서버를 사용하면 인터넷 전송 비용을 절약할 수 있습니다. Amazon S3에 백업하면 미디어 서버가 전반적인 백업 및 복구 성능을 향상시킵니다.

또한, Storage Gateway를 사용하여 지리적으로 분산된 데이터 센터 및 사무실의 데이터에 중앙 집중식 클라우드 액세스를 제공할 수 있습니다. 예를 들어, 파일 게이트웨이를 사용하면 전 세계에 걸쳐 있는 애플리케이션 워크플로에 AWS 대해 저장된 데이터에 온디맨드로 짧은 지연 시간으로 액세스할 수 있습니다. 캐시 새로 고침과 같은 기능을 사용하여 지리적으로 분산된 위치의 데이터를 새로 고쳐 사무실 전체에서 콘텐츠를 쉽게 공유할 수 있습니다.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Web servers
Infrastructure servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
AWS Storage Gateway
Infrastructure servers
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

를 통한 재해 복구 AWS

백업 및 복원 접근 방식과 지원 서비스 및 기술을 사용하여 재해 복구(DR) 솔루션을 구현할 수 있습니다. 많은 기업이 AWS 클라우드를 백업 및 복원과 DR 사이트로 사용하고 있습니다. AWS DR 및 비즈니스 연속성을 지원하는 다양한 서비스와 기능을 제공합니다.

주제

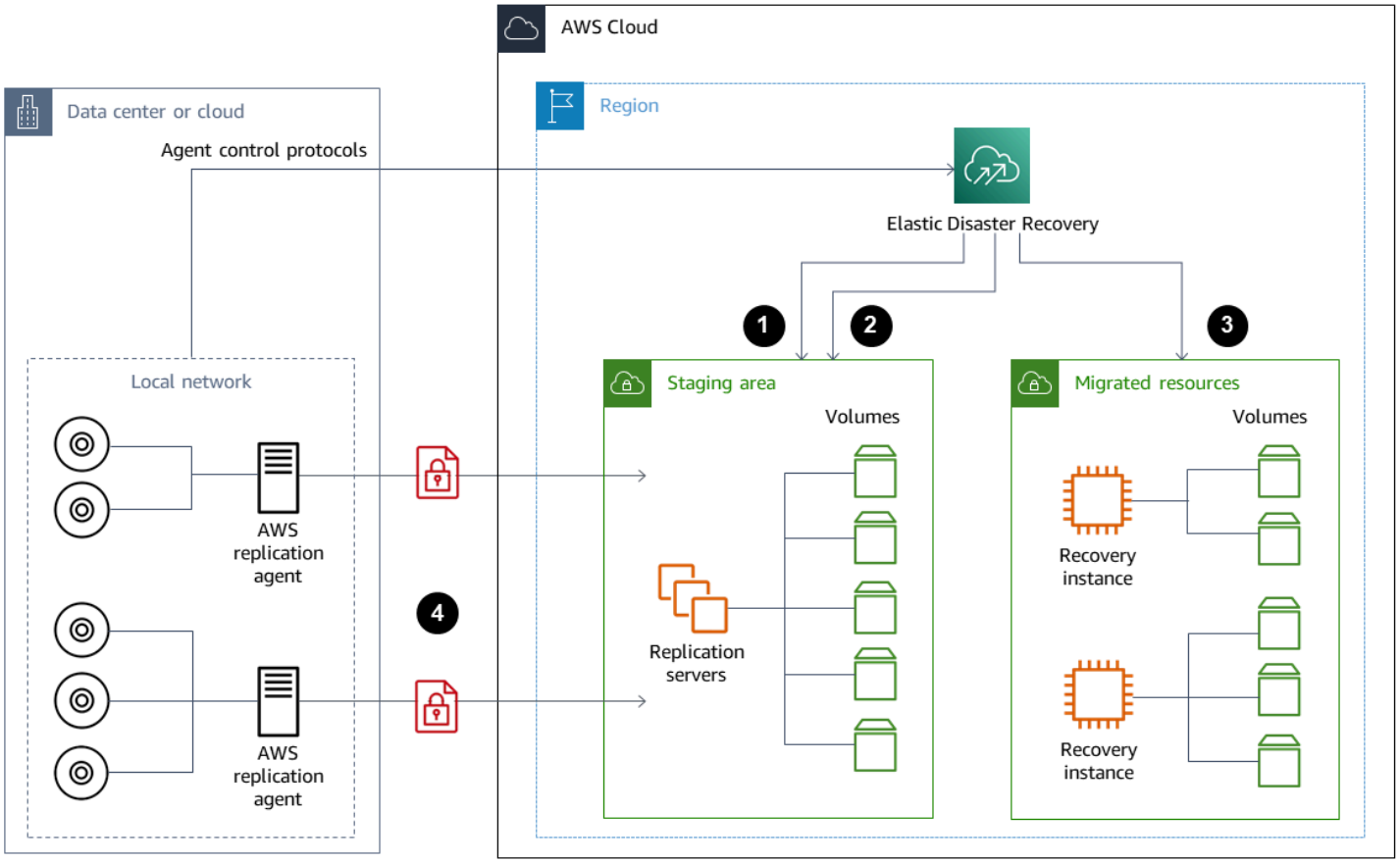
온프레미스 DR - AWS

온프레미스 워크로드를 위한 오프사이트 재해 복구 (DR) AWS 환경으로 사용하는 것은 일반적인 하이브리드 시나리오입니다. 사용할 기술을 선택하기 전에 필요한 복구 시간 및 복구 지점 목표를 비롯한 DR 목표를 정의하십시오. 이러한 정의에 도움이 되는 DR 계획 체크리스트를 활용할 수 있습니다.

AWS에 DR 환경을 신속하게 설정하고 프로비저닝하는 데 도움이 되는 다양한 옵션이 있습니다. 모든 워크로드 종속성을 고려하고, 정기적으로 DR 계획과 솔루션을 철저하게 테스트하여 무결성을 확인하십시오.

AWS 에서 루트 볼륨 및 운영 체제를 포함한 온프레미스 서버의 전체 복제본을 생성할 수 있습니다. AWS Elastic Disaster Recovery AWS Elastic Disaster Recovery는 대상 AWS 계정과 선호하는 AWS 리전에 있는 저렴한 스테이징 영역에 머신을 지속적으로 복제합니다. 블록 수준 복제는 운영 체제, 시스템 상태 구성, 데이터베이스, 애플리케이션 및 파일을 포함한 서버 스토리지의 완벽한 복제본입니다. 재해가 발생하는 경우 Elastic Disaster Recovery에 지시하여 몇 분 안에 수천 대의 머신을 완전히 프로비저닝된 상태로 신속하게 시작하도록 할 수 있습니다.

Elastic Disaster Recovery는 각 온프레미스 서버에 설치된 에이전트를 사용합니다. 에이전트는 온프레미스 서버의 상태를 AWS에서 실행 중인 저전력 Amazon EC2 서버와 동기화합니다. 또한 Elastic Disaster Recovery를 사용하여 DR 장애 조치 및 페일백 프로세스를 자동화할 수 있습니다. 장애 조치 및 페일백 프로세스를 자동화하면 더 낮고 일관된 Recovery Time Objective(RTO)를 달성하는 데 도움이 될 수 있습니다.



1. 복제 서버 상태 보고
2. 스테이징 영역 리소스가 자동으로 생성되고 종료됨
3. 분 단위의 RTO와 초 단위의 RPO로 복구 인스턴스가 시작됨
4. 지속적인 블록 수준 복제(압축 및 암호화)

DR 프로세스를 테스트하고 라이브 스테이징 환경이 온프레미스 환경과 충돌을 일으키지 않는지 확인하는 것이 중요합니다. 예를 들어 온프레미스, 스테이징 및 시작된 DR 환경에서 적절한 라이선스가 사용 가능하고 작동하는지 확인하십시오. 또한 중앙 데이터베이스에서 작업을 폴링하고 가져올 수 있는 모든 작업자 유형 프로세스가 중복이나 충돌을 방지하도록 적절하게 구성되어 있는지 확인하십시오. DR 프로세스에 복구 서버 인스턴스가 온라인 상태가 되기 전에 수행해야 하는 모든 필수 단계를 포함시키십시오. 또한 복구 서버 인스턴스가 온라인 상태이고 사용 가능한 상태가 된 후에 수행할 단계도 포함하십시오. AWS Elastic Disaster Recovery 계획 자동화 솔루션과 같은 솔루션이나 DR 계획을 자동화하는 데 도움이 되는 다른 접근 방식을 사용할 수 있습니다.

Storage Gateway Volume Gateway를 사용하여 온프레미스 서버에 클라우드 기반 볼륨을 제공할 수 있습니다. 또한 Amazon EBS 스냅샷을 사용하여 Amazon EC2에서 사용할 수 있도록 이러한 볼륨을

빠르게 프로비저닝할 수 있습니다. 특히, 저장된 볼륨 게이트웨이는 온프레미스 애플리케이션에서 전체 데이터 세트에 액세스할 때 지연 시간을 단축합니다. 또한 Volume Gateway는 온프레미스에서 사용하거나 Amazon EC2에서 사용하기 위해 복원할 수 있는 견고한 스냅샷 기반 백업을 제공합니다. 워크로드의 복구 시점 목표 (RPO) 에 따라 point-in-time 스냅샷을 예약할 수 있습니다.

> **Important**
>
> Volume Gateway 볼륨은 부팅 볼륨이 아닌 데이터 볼륨으로 사용하기 위한 것입니다.

온프레미스 서버와 일치하고 데이터 볼륨을 별도로 지정하는 구성으로 Amazon EC2 Amazon Machine Image(AMI)를 사용할 수 있습니다. AMI를 구성하고 테스트한 후에는 Volume Gateway 스냅샷을 기반으로 데이터 볼륨과 함께 AMI의 EC2 인스턴스를 프로비저닝합니다. 이 접근법을 사용하려면 환경을 철저하게 테스트하여 EC2 인스턴스가 제대로 작동하고 있는지, 특히 Windows 워크로드의 경우 제대로 작동하는지 확인해야 합니다.

클라우드 네이티브 워크로드용 DR

클라우드 네이티브 워크로드가 DR 목표에 어떻게 부합하는지 생각해 보세요. AWS 전 세계 지역에 여러 가용 영역을 제공합니다. AWS 클라우드를 사용하는 많은 기업은 가용 영역의 손실을 견딜 수 있도록 워크로드 아키텍처와 DR 목표를 조정합니다. AWS Well-Architected 프레임워크의 안정성 기둥은 이러한 모범 사례를 지원합니다. 여러 가용 영역을 사용하도록 워크로드와 서비스 및 애플리케이션 종속성을 설계할 수 있습니다. 그러면 개입을 최소화하거나 전혀 하지 않고도 DR을 자동화하고 DR 목표를 달성할 수 있습니다.

하지만 실제로는 모든 구성 요소에 대해 중복되고 활성화 상태이며 자동화된 아키텍처를 구축하지 못할 수도 있습니다. 아키텍처의 모든 계층을 검토하여 목표를 달성하는 데 필요한 DR 프로세스를 파악하십시오. 이는 아키텍처 및 서비스 요구 사항이 다르므로 워크로드마다 달라질 수 있습니다. 이 안내서는 Amazon EC2 고려 사항 및 옵션을 다룹니다. 다른 AWS 서비스의 경우 AWS 설명서를 참조하여 고가용성 및 DR 옵션을 결정할 수 있습니다.

단일 가용 영역의 Amazon EC2에 대한 DR

여러 가용 영역의 클라이언트를 적극적으로 지원하고 서비스하도록 워크로드를 설계해 보십시오. Amazon EC2 Auto Scaling 및 Elastic Load Balancing을 사용하여 Amazon EC2 및 기타 서비스를 위한 다중 AZ 서버 아키텍처를 구현할 수 있습니다.

아키텍처에 로드 밸런싱이 불가능하고 특정 시점에 단일 인스턴스만 실행할 수 있는 EC2 인스턴스가 있는 경우 다음 옵션 중 하나를 사용할 수 있습니다.

- 최소, 최대 및 원하는 크기가 1이고 여러 가용 영역에 대해 구성된 오토 스케일링을 생성합니다. 장애가 발생할 경우 인스턴스를 대체하는 데 사용할 AMI를 생성합니다. AMI에서 새로 프로비저닝된 인스턴스를 자동으로 구성하고 서비스를 제공할 수 있도록 적절한 자동화 및 구성을 정의해야 합니다. 오토 스케일링을 가리키고 여러 가용 영역에 대해 구성된 로드 밸런서를 생성합니다. 로드 밸런서 엔드포인트를 가리키는 Amazon Route 53 별칭을 생성할 수도 있습니다.
- 활성 인스턴스에 대한 Route 53 레코드를 생성하고 클라이언트가 이 레코드를 사용하여 연결하도록 하십시오. 활성 인스턴스의 새 AMI를 생성하고 이 AMI를 사용하여 별도의 가용 영역에 중지된 상태의 새 EC2 인스턴스를 프로비저닝하는 스크립트를 생성합니다. 주기적으로 실행하고 이전에 중지된 인스턴스를 종료하도록 스크립트를 구성합니다. 가용 영역에 장애가 발생한 경우 대체 가용 영역에서 백업 인스턴스를 시작하십시오. 그런 다음 이 새 인스턴스를 가리키도록 Route 53 레코드를 업데이트하십시오.

솔루션이 보호하도록 설계된 오류를 시뮬레이션하여 솔루션을 철저하게 테스트하십시오. 또한 워크로드 아키텍처가 변경됨에 따라 DR 솔루션이 필요로 할 업데이트도 고려해 보십시오.

리전별 장애 발생 시 Amazon EC2에 대한 DR

가용성 요구 사항이 매우 높은 고객 (예: 다운타임을 허용할 수 없는 업무상 중요한 애플리케이션) 은 AWS 여러 지역에서 사용하여 지역 수준의 문제에 대한 복원력을 강화할 수 있습니다. 고객은 여러 지역 DR 계획을 수립하고 유지하는 데 필요한 복잡성, 비용 및 노력을 이점과 비교하여 신중하게 평가해야 합니다. AWS 글로벌 가용성, 장애 조치 및 DR을 위한 다중 지역 아키텍처를 지원하는 기능을 제공합니다. 이 안내서에서는 Amazon EC2의 백업 및 복구와 관련하여 사용 가능한 몇 가지 기능을 다룹니다.

AWS AMI와 Amazon EBS 스냅샷은 단일 지역 내에서 새 인스턴스를 프로비저닝하는 데 사용할 수 있는 지역 리소스입니다. 하지만 스냅샷과 AMI를 다른 리전에 복사하고 이를 사용하여 해당 리전에서 새 인스턴스를 프로비저닝할 수 있습니다. 지역별 장애 DR 계획을 지원하기 위해 AMI와 스냅샷을 다른 지역으로 복사하는 프로세스를 자동화할 수 있습니다. AWS Backup Amazon Data Lifecycle Manager는 백업 구성의 일부로 지역 간 복사를 지원합니다.

AWS Elastic Disaster Recovery을(를) 한 리전의 Amazon EC2 서버를 자동화하고 다른 DR 리전으로 지속적으로 복제하는 데 사용할 수 있습니다. Elastic Disaster Recovery는 다중 리전 DR 접근 방식을 단순화하고, 드릴을 사용하여 리전 간 Amazon EC2 DR 계획을 정기적으로 테스트하는 데 도움이 됩니다. Elastic Disaster Recovery는 백업 및 복구로 RTO 및 RPO 목표를 달성할 수 없을 때 도움이 될 수 있습니다. Elastic Disaster Recovery를 사용하면 RTO를 분 단위로, RPO를 1초 이하로 낮출 수 있습니다.

어떤 솔루션을 사용하든 정전 발생 시 사용할 프로비저닝, 장애 조치 및 페일백 프로세스를 결정해야 합니다. Route 53을 상태 확인 및 Domain Name System 장애 조치와 함께 사용하면 솔루션을 지원하는 데 도움이 될 수 있습니다.

백업 정리

비용을 줄이려면 복구 또는 보존 목적으로 더 이상 필요하지 않은 백업을 정리하세요. AWS Backup 및 Amazon Data Lifecycle Manager를 사용하여 백업의 일부에 대한 보관 정책을 자동화할 수 있습니다. 하지만 이러한 도구를 갖추고 있더라도 별도로 생성되는 백업에 대해서는 여전히 정리 접근 방식이 필요합니다.

태그 지정 전략은 정리 전략의 전제 조건입니다. 태그 지정을 사용하여 정리해야 할 리소스를 파악하고, 소유자에게 적절하게 알리고, 정리 프로세스를 자동화하세요. AWS에서 만든 백업에는 생성 날짜가 정리되어 있지만 백업을 워크로드, 보존 요건 및 복원 지점 식별과 연관시키려면 태그 지정이 중요합니다.

자동화를 사용하여 스냅샷에 대한 정리 프로세스를 구현할 수 있습니다. 예를 들어 계정에 스냅샷이 있는지 스캔하고 해당 볼륨이 연결된 상태인지 또는 사용 가능한 상태인지 확인할 수 있습니다. 지정한 시간 임계값을 기준으로 결과를 추가로 필터링할 수 있습니다. 볼륨에 첨부된 태그를 사용하여 스냅샷 소유자에게 자동으로 이메일을 보내고, 해당 스냅샷이 삭제될 예정임을 경고할 수 있습니다. AWS Config 규칙을 사용하거나 AWS CLI을(를) 사용하는 스크립트 또는 AWS SDK를 사용하는 Lambda 함수를 사용하여 이 자동 해결을 구현할 수 있습니다.

Systems Manager는 Amazon EBS 스냅샷 정리를 시작하고 자동화하는 데 도움이 되는 AWS-DeleteEBSVolumeSnapshots 및 AWS-DeleteSnapshot 문서를 제공합니다. 또한 AWS CLI 및 AWS SDK를 사용하여 Amazon RDS 스냅샷과 같은 다른 AWS 리소스의 정리를 자동화할 수 있습니다.

백업 및 복구 FAQ

어떤 백업 일정을 선택해야 하나요?

사용자의 Recovery Point Objective(RPO)에 맞는 백업 스케줄 빈도를 파악하시기 바랍니다. 워크로드의 부하가 가장 적고 사용자에게 미치는 영향을 줄일 수 있는 백업 시간을 파악하세요. 워크로드를 크게 변경해야 할 때마다 특정 시점 스냅샷을 생성하세요.

개발 계정에서 백업을 만들어야 하나요?

워크로드에 맞게 개발 계정의 잠재적 주요 변경 사항을 테스트하고 주요 변경을 수행하기 전에 백업을 생성하세요. 개발 계정과 비프로덕션 계정에 개발 및 테스트 활동을 통해 얻은 시점 복구(PITR) 백업이 더 많이 있을 수 있습니다.

스냅샷이 생성되는 동안 아무런 영향 없이 애플리케이션을 업그레이드하고 EBS 볼륨을 계속 사용할 수 있나요?

스냅샷은 비동기적으로 생성됩니다. 특정 시점 스냅샷은 즉시 생성되지만 수정된 블록이 Amazon S3로 모두 이동할 때까지 스냅샷 상태는 보류 상태입니다. 대규모 초기 스냅샷이나 블록 수가 많이 변경된 후속 스냅샷의 경우 전송하는 데 몇 시간이 걸릴 수 있습니다. 전송하는 동안 진행 중인 스냅샷은 볼륨에 대한 지속적인 읽기 및 쓰기의 영향을 받지 않습니다. 자세한 내용은 AWS 설명서를 참조하세요.

다음 단계

비프로덕션 환경에서 백업 및 복구 접근 방식을 평가, 구현 및 테스트하는 것부터 시작하십시오. 복구 프로세스를 철저하게 테스트하고 복원된 워크로드가 추정대로 작동하는지 확인하는 것이 중요합니다.

아키텍처의 모든 구성 요소뿐 아니라 아키텍처의 단일 구성 요소에 대한 복원 프로세스를 테스트하십시오. 각각의 복구 시간을 확인하십시오. 또한 백업 및 복원 프로세스가 업스트림 및 다운스트림 종속성에 미치는 영향을 검증하십시오. 서비스 중단이 업스트림 종속성에 미치는 영향을 확인하고 다운스트림이 백업에 미치는 영향을 확인하십시오.

추가 리소스

AWS 리소스

- AWS 규범적 지침
- 설명서
- AWS 일반 참조
- AWS 용어집

서비스

- AWS Backup
- 아마존 CloudWatch
- 아마존 CloudWatch 이벤트
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Storage Gateway
- AWS Systems Manager

기타 리소스

- AWS Backup을(를) 이용한 백업 및 복구(솔루션)
- 워크로드 재해 복구 AWS: 클라우드에서의 복구 (백서)
- 재해 복구 시리즈(AWS 아키텍처 블로그 게시물)
- DR 계획 체크리스트
- AWS을(를) 사용한 백업 및 복구 접근 방식(기술 문서 – 보관)
- 시작하기 AWS Backup

- AWS 마켓플레이스 – 백업 및 복원

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
업데이트된 정보	Amazon S3 섹션의 지침이 업데이트되었습니다.	2024년 6월 28일
업데이트된 정보	AWS대상 온프레미스 DR 섹션의 정보가 업데이트되었습니다.	2023년 4월 13일
섹션이 추가됨	스냅샷에서 인스턴스를 만들거나 복원하기 위한 지침 및 단계가 추가되었습니다.	2023년 3월 7일
Elastic 재해 복구에 대한 정보 추가 및 설명 추가	데이터 보호를 위한 재해 복구 AWS 및 AWS 서비스 선택 섹션에 다음과 같은 정보가 AWS Elastic Disaster Recovery추가되었습니다. 스냅샷과 AMI를 사용한 Amazon EC2 백업 및 복구, 스냅샷 또는 AMI를 생성하기 전에 EBS 볼륨 준비하기, Amazon EBS 스냅샷 또는 AMI에서 복원 섹션에 설명이 추가되었습니다. 백업 및 복구 FAQ에 추가되었습니다.	2023년 1월 19일
링크 추가됨	Amazon Data Lifecycle Manager 섹션에 Amazon Data Lifecycle Manager 설명서로 연결되는 링크를 추가했습니다.	2022년 10월 31일

업데이트된 정보	볼륨 복원에 대한 정보가 업데이트되었습니다.	2022년 8월 30일
정보가 업데이트되고 새 섹션이 추가되었습니다.	데이터 보호를 위한 AWS 서비스 선택 섹션에 서비스가 추가되었습니다. AWS Backup을 사용한 백업 및 복구 섹션이 추가되었습니다. Amazon S3 및 Amazon S3 Glacier를 사용한 백업 및 복구 섹션에 새로운 Amazon S3 Glacier 스토리지 클래스에 대한 정보가 추가되었습니다. EBS 볼륨을 사용하는 Amazon EC2의 백업 및 복구 섹션에 설명서 및 추가 정보로 연결되는 링크가 추가되었습니다. 클라우드 네이티브 AWS 서비스의 백업 및 복구 섹션에 사용 AWS Backup권장 사항을 추가했습니다. 추가 리소스 섹션에 리소스가 추가되었습니다.	2022년 1월 28일
업데이트된 정보	S3 Glacier Flexible Retrieval 섹션에 스토리지 클래스 설정에 대한 정보가 추가되었습니다. 스냅샷 및 AMI를 사용한 Amazon EC2 백업 및 복구 섹션에 스냅샷 검색에 대한 정보가 추가되었습니다.	2021년 9월 9일
업데이트된 정보	AWS Backup섹션에는 AWS Backup 지원하는 AWS 서비스에 대한 정보가 추가되었습니다.	2021년 6월 1일
최초 게시	—	2020년 7월 29일

AWS 규범적 지침 용어집

다음은 규범적 지침에서 제공하는 AWS 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 에디션으로 마이그레이션하십시오.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 오라클용 Amazon RDS (Amazon 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.com으로 마이그레이션하십시오.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 의 EC2 인스턴스에서 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 다음으로 마이그레이션하십시오. 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 참조하십시오.

추상화된 서비스

관리형 서비스를 참조하십시오.

산

원자성, 일관성, 격리성, 내구성을 참조하십시오.

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 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 연산을 수행하고 그룹에 대한 단일 반환값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 및 등이 `SUM` 있습니다. `MAX`

AI

인공 지능을 참조하십시오.

AIOps

인공 지능 운영을 참조하십시오.

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

시스템을 멀웨어로부터 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 AWS ABAC for를 참조하십시오.

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 격리되고 동일한 지역 내 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 별도의 위치. AWS 리전

AWS 클라우드 채택 프레임워크 (AWS CAF)

조직이 클라우드로 성공적으로 AWS 전환하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 관점이라고 하는 6가지 중점 영역, 즉 비즈니스, 사람, 거버넌스, 플랫폼, 보안, 운영으로 분류합니다. 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 조직이 성공적인 클라우드 채택을 준비할 수 있도록 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 권장하며 작업 예상치를 제공하는 도구입니다. AWS WQF는 () 에 포함됩니다. AWS Schema Conversion Tool AWS SCT데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

배드 봇

개인이나 조직을 방해하거나 피해를 입히려는 의도를 가진 봇입니다.

BCP

비즈니스 연속성 계획을 참조하십시오.

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. 엔디안도 참조하십시오.

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

서로 다르지만 동일한 환경을 두 개 만드는 배포 전략입니다. 현재 애플리케이션 버전을 한 환경 (파란색) 에서 실행하고 다른 환경 (녹색) 에서 새 애플리케이션 버전을 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 신속하게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 작업을 실행하고 사람의 활동이나 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 배드 봇으로 알려진 일부 다른 봇은 개인이나 조직을 방해하거나 피해를 입히기 위한 것입니다.

봇넷

멀웨어에감염되어 봇 허더 또는 봇 운영자로 알려진 단일 당사자의 통제 하에 있는 봇 네트워크. 봇넷은 봇과 그 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 브랜치 정보 (문서) 를 참조하십시오. GitHub

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스 권한이 없는 데이터에 빠르게 액세스할 수 AWS 계정 있는 수단입니다. 자세한 내용은 Well-Architected AWS 지침의 브레이크 글래스 절차 구현 표시기를 참조하십시오.

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

클라우드 채택 프레임워크를 참조하십시오AWS .

카나리아 배포

최종 사용자에게 버전을 느리고 점진적으로 릴리스하는 것입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

클라우드 센터 오브 엑설런스를 참조하십시오.

CDC

변경 데이터 캡처를 참조하십시오.

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

시스템의 복원력을 테스트하기 위해 의도적으로 장애나 장애를 일으키는 이벤트를 발생시키는 행위 AWS Fault Injection Service (AWS FIS) 를 사용하여 AWS 워크로드에 스트레스를 주는 실험을 수행하고 응답을 평가할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전달을 참조하십시오.

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 데이터를 로컬로 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 기업 전략 블로그의 CCoE 게시물을 참조하십시오.

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 마이그레이션할 때 일반적으로 거치는 4단계는 다음과 같습니다. 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

Stephen Orban은 기업 전략 블로그의 클라우드 우선주의를 향한 여정 및 채택 단계에 대한 블로그 게시물에서 이러한 단계를 정의했습니다. AWS 클라우드 이들이 AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오.

CMDB

구성 관리 데이터베이스를 참조하십시오.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반 클라우드 리포지토리에는 또는 이 포함됩니다 GitHub . AWS CodeCommit코드의 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 분야. 예를 들어 AWS Panorama 는 온프레미스 카메라 네트워크에 CV를 추가하는 디바이스를 제공하고, SageMaker Amazon은 CV용 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않게 될 수 있으며, 일반적으로 점진적이고 의도하지 않은 방식으로 진행됩니다.

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

AWS Config 규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 규칙 및 수정 조치 모음입니다. YAML 템플릿을 사용하여 한 AWS 계정 및 지역 또는 조직 전체에 단일 엔티티로 적합성 팩을 배포할 수 있습니다. 자세한 내용은 설명서의 적합성 팩을 참조하십시오. AWS Config

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 참조하십시오.

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 프레임워크의 보안 핵심 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 거버넌스와 함께 분산되고 분산된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터 최소화를 실천하면 개인 정보 보호 위험, 비용 및 분석에 따른 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 ID만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경 내 일련의 예방 가드레일입니다. 자세한 내용은 데이터 경계 구축을 참조하십시오. 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 시스템. 데이터 웨어하우스에는 일반적으로 대량의 과거 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 참조하십시오.

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.

defense-in-depth

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 AWS여러 컨트롤을 추가하여 리소스를 보호하는 데 도움이 됩니다. 예를 들어 다단계 인증, 네트워크 세분화, 암호화를 결합한 defense-in-depth 접근 방식을 사용할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환 가능한 서비스는 AWS 구성원 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 참조하십시오.

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.

치수 표

스타 스키마에서 팩트 테이블의 양적 데이터에 대한 데이터 속성을 포함하는 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트처럼 동작하는 텍스트 필드 또는 불연속형 숫자입니다. 이러한 속성은 일반적으로 쿼리 제한, 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 다운타임과 데이터 손실을 최소화하기 위해 사용하는 전략과 프로세스입니다. 자세한 내용은 워크로드의 재해 복구 AWS: AWS Well-Architected 프레임워크에서의 클라우드 복구를 참조하십시오.

DML

데이터베이스 조작 언어를 참조하십시오.

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 참조하십시오.

드리프트 감지

기준 구성으로부터의 편차 추적. 예를 들어 시스템 리소스의 편차를 감지하는 AWS CloudFormation 데 사용하거나 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 착륙 지대의 변경 사항을 탐지하는 AWS Control Tower 데 사용할 수 있습니다.

DVSM

개발 가치 흐름 매핑을 참조하십시오.

E

EDA

탐색적 데이터 분석을 참조하십시오.

엣지 컴퓨팅

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

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 암호문으로 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 참조하십시오.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 다른 주체 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 부여하여 엔드포인트 서비스를 생성하고 권한을 부여할 수 있습니다. AWS PrivateLink 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니

다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

ERP (전사적 자원 관리)

기업의 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 참조하십시오.

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, 사고 대응 등이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하십시오.

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

[스타 스키마의](#) 중앙 테이블. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블의 외부 키가 포함된 열 등 두 가지 유형의 열이 포함됩니다.

빨리 실패하세요

빈번하고 점진적인 테스트를 통해 개발 라이프사이클을 단축하는 철학. 이는 애자일 접근 방식의 중요한 부분입니다.

장애 격리 경계

장애 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역 AWS 리전, 컨트롤 플레인 또는 데이터 플레인과 같은 경계 AWS 클라우드자세한 내용은 [AWS 장애 격리](#) 경계를 참조하십시오.

기능 브랜치

[브랜치를](#) 참조하십시오.

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 [다음을AWS사용한 기계 학습 모델 해석 가능성을](#) 참조하십시오.

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 활용할 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.

FGAC

[세분화된 액세스 제어를](#) 참조하십시오.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계별 접근 방식 대신 변경 데이터 캡처를 통한 지속적인 데이터 복제를 통해 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

G

지리적 차단

지리적 제한을 참조하십시오.

지리적 제한(지리적 차단)

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

Gitflow 워크플로

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

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, 이들은, Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

하

고가용성을 확인하세요.

이기종 데이터베이스 마이그레이션

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

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. 긴급성 때문에 핫픽스는 일반적으로 일반적인 DevOps 릴리스 워크플로 외부에서 만들어집니다.

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.

I

IaC

인프라를 코드로 보세요.

자격 증명 기반 정책

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

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.

불변의 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드용 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 기본적으로 변경 가능한 인프라보다 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 Well-Architected AWS 프레임워크의 변경 불가능한 인프라를 사용한 배포 모범 사례를 참조하십시오.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 VPC는 애플리케이션 외부에서 네트워크 연결을 허용, 검사 및 라우팅합니다. 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 것

이 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

Klaus Schwab이 연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통한 제조 프로세스의 현대화를 지칭하기 위해 2016년 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 아키텍처에서 VPC (동일하거나 AWS 리전다른), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPC입니다. 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 Machine learning model interpretability with AWS를 참조하십시오.

IoT

사물 인터넷을 참조하십시오.

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 참조하십시오.

ITSM

IT 서비스 관리를 참조하십시오.

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

Landing Zone은 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 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하십시오.

최소 권한

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

리프트 앤드 시프트

7 R을 참조하십시오.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안 참조.

하위 환경

환경 참조.

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

브랜치 참조.

악성 코드

컴퓨터 보안 또는 개인 정보를 침해하도록 설계된 소프트웨어 멀웨어는 컴퓨터 시스템을 방해하거나, 민감한 정보를 유출하거나, 무단 액세스를 얻을 수 있습니다. 멀웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

매니지드 서비스

AWS 서비스 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로는 아마존 심플 스토리지 서비스 (Amazon S3) 와 아마존 DynamoDB가 있습니다. 이러한 서비스를 추상화된 서비스라고도 합니다.

제조 실행 시스템 (MES)

제조 현장에서 원자재를 완제품으로 전환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

Migration Acceleration 프로그램을 참조하십시오.

기구

도구를 만들고 도구 채택을 유도한 다음 결과를 검토하여 조정하는 전체 프로세스입니다. 메커니즘은 작동하면서 자체적으로 강화되고 개선되는 사이클입니다. 자세한 내용은 AWS Well-Architected 프레임워크에서의 메커니즘 구축을 참조하십시오.

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 참조하십시오.

메시지 큐 텔레메트리 전송 (MQTT)

퍼블리시/구독 패턴을 기반으로 하는 리소스가 제한된 IoT 디바이스를 위한 경량 machine-to-machine (M2M) 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 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하십시오. AWS

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 마이크로서비스 구현을 참조하십시오. AWS

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄할 수 있도록 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 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자 및 스프린트에서 일하는 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, 계정 등이 있습니다. AWS

마이그레이션 패턴

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

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 컨설턴트와 APN 파트너 AWS 컨설턴트에게 무료로 제공됩니다.

마이그레이션 준비 상태 평가(MRA)

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

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용된 접근 방식. AWS 클라우드자세한 내용은 이 용어집의 7R 항목 및 대규모 마이그레이션 가속화를 위한 조직 동원을 참조하십시오.

ML

기계 학습을 참조하십시오.

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 AWS 클라우드애플리케이션 현대화 전략을 참조하십시오.

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 에서 애플리케이션의 현대화 준비 상태 평가를 참조하십시오. 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 참조하십시오.

MQTT

메시지 큐 원격 분석 전송을 참조하십시오.

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, 안정성 및 예측 가능성을 개선하기 위해 AWS Well-Architected Framework는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

원본 액세스 제어를 참조하십시오.

좋아요

원본 액세스 ID를 참조하십시오.

OCM

조직 변경 관리를 참조하십시오.

오프라인 마이그레이션

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

OI

운영 통합을 참조하십시오.

안녕하세요.

운영 수준 계약을 참조하십시오.

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

오픈 프로세스 커뮤니케이션 - 통합 아키텍처를 참조하십시오.

오픈 프로세스 커뮤니케이션 - 통합 아키텍처 (OPC-UA)

산업 machine-to-machine 자동화를 위한 (M2M) 통신 프로토콜. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 함께 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 검토 (ORR)

인시던트 및 발생 가능한 실패의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 및 관련 모범 사례로 구성된 체크리스트입니다. 자세한 내용은 Well-Architected AWS 프레임워크의 운영 준비 상태 검토 (ORR) 를 참조하십시오.

운영 기술 (OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템. 제조 분야에서는 OT와 정보 기술 (IT) 시스템의 통합이 인더스트리 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

이를 통해 AWS CloudTrail 생성되는 트레일은 조직 AWS 계정 내 모든 사용자의 모든 이벤트를 기록합니다. AWS Organizations이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서에서 조직을 위한 트레일 만들기를 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. 클라우드 채택 프로젝트에 필요한 변화 속도 때문에 AWS 마이그레이션 전략에서는 이 프레임워크를 사용자 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서는 Amazon Simple Storage Service (Amazon S3) 콘텐츠의 보안을 위해 액세스를 제한하는 향상된 옵션을 제공합니다. OAC는 모든 S3 버킷 AWS 리전, AWS KMS (SSE-KMS) 를 사용한 서버 측 암호화, S3 버킷에 대한 동적 및 요청을 모두 지원합니다. PUT DELETE

오리진 액세스 ID(OAI)

CloudFront에서는 Amazon S3 콘텐츠 보안을 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 Amazon S3가 인증할 수 있는 보안 주체를 CloudFront 생성합니다. 인증된 보안 주체는 특정 배

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

또는

운영 준비 상태 검토를 참조하십시오.

아니요

운영 기술을 참조하십시오.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작되는 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 참조하십시오.

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

프로그래머블 로직 컨트롤러를 참조하십시오.

PLM

제품 라이프사이클 관리를 참조하십시오.

정책

권한을 정의 (ID 기반 정책 참조) 하거나, 액세스 조건을 지정 (리소스 기반 정책 참조) 하거나, 조직 내 모든 계정에 대한 최대 권한을 정의 AWS Organizations (서비스 제어 정책 참조) 할 수 있는 개체입니다.

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

일반적으로 조항에 있는 `true` `false` OR를 반환하는 쿼리 조건입니다. `WHERE`

조건부 푸시다운

전송하기 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 있는 엔티티 이 엔티티는 일반적으로 IAM 역할의 루트 사용자 또는 사용자입니다. AWS 계정자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

개인 정보 보호 중심 설계

전체 엔지니어링 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 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 예방 제어

규정을 준수하지 않는 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 컨트롤은 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 컨트롤과 호환되지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 컨트롤 참조 안내서를 참조하고 보안 제어 구현의 사전 제어를 참조하십시오. AWS

제품 라이프사이클 관리 (PLM)

설계, 개발, 출시부터 성장 및 성숙도, 폐기 및 제거에 이르는 전체 라이프사이클에 걸쳐 제품에 대한 데이터 및 프로세스를 관리하는 것입니다.

프로덕션 환경

환경을 참조하십시오.

프로그래머블 로직 컨트롤러 (PLC)

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

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 (게시/구독)

마이크로서비스 간의 비동기 통신을 통해 확장성과 응답성을 개선할 수 있는 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 일련의 단계 (예: 지침).

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

RACI (책임, 책임, 상담, 정보 제공) 를 참조하십시오.

랜섬웨어

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

RASCI 매트릭스

책임, 책임, 상담, 정보 제공 (RACI) 을 참조하십시오.

RCAC

행 및 열 액세스 제어를 참조하십시오.

읽기 전용 복제본

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

재설계

7 R을 참조하십시오.

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

7 R을 참조하십시오.

리전

지리적 AWS 영역별 리소스 모음. AWS 리전 각각은 격리되어 있고 서로 독립적이므로 내결함성, 안정성 및 복원력을 제공합니다. 자세한 내용은 사용할 수 있는 AWS 리전 계정 지정을 참조하십시오.

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

7 R을 참조하십시오.

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

고쳐 놓다

7 R을 참조하십시오.

리플랫포밍

7 R을 참조하십시오.

환매

7 R을 참조하십시오.

복원력

장애를 견디거나 장애를 복구할 수 있는 애플리케이션의 능력 고가용성 및 재해 복구는 복원력을 계획할 때 일반적으로 고려해야 할 사항입니다. AWS 클라우드자세한 내용은 AWS 클라우드 복원력을 참조하십시오.

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 결

정권자 (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

7 R을 참조하십시오.

은퇴

7 R을 참조하십시오.

회전

공격자가 자격 증명에 액세스하는 것을 더 어렵게 만들기 위해 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 지점 목표를 참조하십시오.

RTO

복구 시간 목표를 참조하십시오.

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 (IdPs) 가 사용하는 개방형 표준입니다. 이 기능을 사용하면 페더레이션 싱글 사인온 (SSO) 이 가능하므로 조직의 모든 사용자를 위해 IAM에서 사용자를 생성하지 않고도 사용자가 AWS API 작업에 AWS Management Console 로그인하거나 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 수집을 참조하십시오.

SCP

서비스 제어 정책을 참조하십시오.

secret

에는 AWS Secrets Manager암호화된 형태로 저장하는 비밀번호나 사용자 자격 증명과 같은 기밀 또는 제한된 정보. 비밀 값과 해당 메타데이터로 구성됩니다. 비밀 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 Secrets Manager 시크릿에는 무엇이 들어 있나요? 를 참조하십시오. Secrets Manager 설명서에서 확인할 수 있습니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 예방적, 탐정적, 대응적, 사전 예방적 제어의 네 가지 기본 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 대응 자동화

보안 이벤트에 자동으로 대응하거나 보안 이벤트를 해결하도록 설계된 사전 정의되고 프로그래밍된 조치입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응형 보안 제어 역할을 합니다. AWS 자동 응답 조치의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치, 자격 증명 교체 등이 있습니다.

서버 측 암호화

수신자에 의한 목적지의 데이터 암호화 AWS 서비스

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 참조하십시오.

서비스 엔드포인트

의 진입점 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 측면을 측정하는 것입니다.

서비스 수준 목표 (SLO)

서비스 수준 지표로 측정되는 서비스 상태를 나타내는 대상 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수에 AWS 대한 책임을 공유하는 것을 설명하는 모델입니다. AWS 클라우드의 보안을 책임지는 반면, 사용자는 클라우드에서의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

시엠

보안 정보 및 이벤트 관리 시스템을 참조하십시오.

단일 장애 지점 (SPOF)

응용 프로그램의 중요한 단일 구성 요소에서 발생한 오류로 인해 시스템이 중단될 수 있습니다.

SLA

SLA (서비스 수준 계약) 를 참조하십시오.

SLI

서비스 수준 표시기 참조.

SLO

서비스 수준 목표를 참조하십시오.

split-and-seed 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 의 애플리케이션 현대화를 위한 단계별 접근 방식을 참조하십시오. AWS 클라우드

SPOF

단일 장애 지점 보기.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 구성 구조입니다. 이 구조는 데이터 웨어하우스에서 사용하거나 비즈니스 인텔리전스 용도로 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 압도하고 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 통제 및 데이터 수집 (SCADA)

제조 시 하드웨어와 소프트웨어를 사용하여 물리적 자산과 생산 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

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

T

tags

리소스 구성을 위한 메타데이터 역할을 하는 키-값 쌍. AWS 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 참조하십시오.

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 트랜짓 게이트웨이란 무엇입니까? 를 참조하십시오.

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

조직 내 AWS Organizations 및 해당 계정에서 사용자를 대신하여 작업을 수행하도록 지정한 서비스에 권한 부여 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관

리 작업을 수행합니다. 자세한 내용은 AWS Organizations 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하십시오.

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 판만 들고 배불리 먹을 수 있는 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 보세요.

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.

윈도우 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 윈도우 함수는 이동 평균을 계산하거나 현재 행의 상대적 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.

웜

한 번 쓰고, 많이 읽으세요.

WQF

AWS 워크로드 검증 프레임워크를 참조하십시오.

한 번 작성하고 여러 번 읽기 (WORM)

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

Z

제로데이 익스플로잇

제로데이 취약점을 악용하는 공격 (일반적으로 멀웨어) 입니다.

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.

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.