의 백업 및 복구 접근 방식 AWS

AWS 권장 가이드

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

AWS 권장 가이드: 의 백업 및 복구 접근 방식 AWS

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

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

Table of Contents

소개 ... 1
를 데이터 보호 플랫폼 AWS 으로 사용하는 이유는 무엇입니까? ... 2
목표 비즈니스 성과 ... 4
AWS 서비스 선택 ... 5
백업 및 복구 솔루션 설계 ... 7
AWS Backup ... 8
Amazon S3 ... 10
Amazon S3 스토리지 클래스 사용 ... 10
표준 S3 버킷 생성 ... 12
Amazon S3 버전 관리 사용 ... 12
AMI용 사용자 지정 구성 파일 백업 및 복구 ... 12
사용자 지정 백업 및 복원 ... 12
백업 데이터 보안 유지 ... 13
EBS 볼륨을 사용하는 Amazon EC2 ... 14
Amazon EC2 백업 및 복구 ... 15
AMI 또는 스냅샷 ... 15
서버 볼륨 ... 17
별도의 서버 볼륨 ... 18
인스턴스 저장소 볼륨 ... 18
태그 지정 및 표준 적용 ... 19
EBS 볼륨 백업 생성 ... 19
EBS 볼륨 준비 ... 20
콘솔에서 스냅샷 생성 ... 21
AMI 생성 ... 22
Amazon Data Lifecycle Manager ... 22
AWS Backup ... 23
다중 볼륨 백업 ... 23
백업 보호 ... 25
스냅샷 아카이브 ... 26
스냅샷 및 AMI 생성 자동화 ... 26
볼륨 또는 인스턴스 복원 ... 27
EBS 스냅샷에서 파일 및 디렉터리 복원 ... 27
Amazon EBS 스냅샷에서 EBS 볼륨 복원 ... 27
EBS 스냅샷에서 EC2 인스턴스 생성 또는 복원 ... 29

AMI에서 실행 중인 인스턴스 복원 30
온프레미스에서 백업 및 복구 31
File Gateway 32
볼륨 게이트웨이 32
Tape Gateway 33
애플리케이션 백업 및 복구 35
클라우드 네이티브 AWS 서비스 36
Amazon RDS 36
DNS CNAME 사용 37
DynamoDB 38
하이브리드 아키텍처 40
중앙 집중식 백업 관리 솔루션 이동하기 41
재해 복구 43
에 대한 온프레미스 DR AWS 43
클라우드 네이티브 워크로드용 DR 45
단일 가용 영역의 DR 45
리전별 장애 발생 시 DR 46
백업 정리 48
FAQ 49
어떤 백업 일정을 선택해야 하나요? 49
개발 계정에서 백업을 만들어야 하나요? 49
스냅샷이 생성되는 동안 아무런 영향 없이 애플리케이션을 업그레이드하고 EBS 볼륨을 계속 사용할 수 있나요? 49
다음 단계 50
리소스 51
문서 기록 52
..... liv

의 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 목표 복구 시간(RTO), 목표 복구 시점(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 요소에 대한 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.는 다음과 같이 변경 불가능한 아키텍처를 구현하고 백업 및 복구 필요성을 줄이는 다양한 서비스를 AWS 제공합니다.

- 를 사용한 서버리스 AWS Lambda
- Amazon Elastic Container Service(Amazon ECS), Amazon Elastic Kubernetes Service(Amazon EKS) 및가 있는 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
- S3을 사용하여 백업 및 복구
- EBS 볼륨을 사용하는 Amazon EC2의 백업 및 복구

- 온프레미스 인프라에서 로 백업 및 복구 AWS
- AWS에서 데이터 센터로 애플리케이션 백업 및 복구
- 클라우드 네이티브 AWS 서비스의 백업 및 복구
- 하이브리드 아키텍처를 위한 백업 및 복구
- 를 사용한 재해 복구 AWS
- 백업 정리

를 데이터 보호 플랫폼 AWS 으로 사용하는 이유는 무엇입니까?

AWS 는 안전하고 유연하며 비용을 절감하고 easy-to-use 고성능 클라우드 컴퓨팅 플랫폼입니다. AWS 는 확장 가능한 백업 및 복구 솔루션을 생성, 구현 및 관리하는 데 필요한 차별화되지 않은 어려운 작업을 처리합니다.

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

- 내구성: Amazon Simple Storage Service(Amazon S3)와 S3 Glacier Deep 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 저장 및 내보내기/가져오기 작업에 Amazon S3를 사용합니다. 예컨대, Amazon Elastic Block Store(Amazon EBS)는 Amazon S3를 스냅샷 스토리지로 사용합니다.
- Security:전송 중 및 유휴 시 액세스 제어 및 데이터 암호화를 위한 다양한 옵션을 AWS 제공합니다.
- 글로벌 인프라: AWS 서비스는 전 세계에서 사용할 수 있으므로 규정 준수 및 워크로드 요구 사항을 충족하는 리전에 데이터를 백업하고 저장할 수 있습니다.
- Compliance: AWS infrastructure는 다음 표준을 준수하는 것으로 인증되었으므로 기존 규정 준수 방식에 백업 솔루션을 쉽게 맞출 수 있습니다.
  - Service Organization Controls(SOC)
  - 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:를 사용하면 용량에 대해 걱정할 필요가 AWS없습니다. 요건이 변경되면 관리 부담 없이 사용량을 늘리거나 줄일 수 있습니다.

- 총 소유 비용(TCO) 절감: AWS 운영 규모는 서비스 비용을 절감하고 AWS 서비스의 TCO를 낮추는 데 도움이 됩니다.는 가격 인하를 통해 이러한 비용 절감을 고객에게 AWS 전달합니다.
- Pay-as-you-go 요금: 필요한 만큼 AWS 서비스를 구매하고 사용하려는 기간 동안만 구매합니다. AWS 요금에는 선결제 요금, 해지 위약금 또는 장기 계약이 없습니다.

목표 비즈니스 성과

이 가이드의 목표는 다음에 대한 백업 및 복구 접근 방식을 지원하는 데 사용할 수 있는 AWS 서비스에 대한 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

AWS 는 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 Gateway는 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.
  - Network File System(NFS)
  - Server Message Block(SMB)
  - Internet Small Computer System Interface(iSCSI)

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

  Storage Gateway를 사용하면 파일, 볼륨, 스냅샷 및 가상 테이프에 탄력적인 고성능 스토리지를 더 쉽게 제공할 수 있습니다 AWS.
- AWS Backup는 서비스 간 데이터 백업을 중앙 집중화하고 자동화하기 위한 완전 관리형 백업 AWS 서비스입니다. AWS Backup을 사용하면 중앙에서 백업 정책을 구성하고 다음과 같은 AWS 리소스의 백업 활동을 모니터링할 수 있습니다.
  - EBS 볼륨
  - EC2 인스턴스(Windows 애플리케이션 포함)
  - Amazon RDS 및 Amazon Aurora 데이터베이스
  - DynamoDB 테이블
  - Amazon Neptune 데이터베이스
  - Amazon DocumentDB(MongoDB 호환) 데이터베이스

- Amazon EFS 파일 시스템
- Amazon FSx for Lustre 파일 시스템 및 Amazon FSx for Windows File Server 파일 시스템
- Storage Gateway 볼륨

의 비용은 한 달에 소비, 복원 및 전송하는 스토리지를 AWS Backup 기준으로 합니다. 자세한 내용은 AWS Backup 요금을 참조하세요.

- AWS Elastic Disaster Recovery는 대상 AWS 계정 및 기본 리전의 스테이징 영역 서브넷에 시스템을 복제합니다. 스테이징 영역 설계는 저렴한 스토리지와 최소한의 컴퓨팅 리소스를 사용하여 지속적인 복제를 유지함으로써 비용을 절감합니다. Elastic Disaster Recovery는 온프레미스에서 클라우드로의 DR 및 리전 간 DR에 모두 사용할 수 있습니다.
- AWS Config는 AWS 계정의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다. 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 기록을 유지합니다. 이를 통해 최대 7년 동안 AWS 리소스 관계(삭제된 리소스 포함)를 식별하고 추적할 수 있습니다. 예를 들어는 Amazon EBS 스냅샷 볼륨과 볼륨이 연결된 EC2 인스턴스의 관계를 AWS Config 추적할 수 있습니다.
- AWS Lambda를 사용하여 워크로드의 백업 및 복구 절차를 프로그래밍 방식으로 정의하고 자동화할 수 있습니다. AWS SDKs를 사용하여 AWS 서비스 및 해당 데이터와 상호 작용할 수 있습니다. 또한 Amazon EventBridge를 사용하여 일정에 따라 Lambda 함수를 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 확인합니다. AWS Command Line Interface (AWS CLI), AWS SDKs 및 API 작업을 사용하여 데이터 백업 및 복구를 위한 AWS 서비스별 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 조정하십시오.

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 검토하십시오.

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 참조하십시오.

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.

S3을 사용하여 백업 및 복구

Amazon Simple Storage Service(Amazon S3)를 사용하면 인터넷을 통해 언제든 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 또는SDK를 사용하여 백업 스크립트를 사용하여 데이터베이스 인스턴스에서 Amazon S3로 데이터베이스 백업을 복사할 수 있습니다. AWS SDKs

AWS 서비스 다음 예제와 같이는 Amazon S3를 사용하여 내구성이 뛰어나고 안정적인 스토리지를 제공합니다.

- Amazon EC2는 Amazon S3를 사용하여 EBS 볼륨 및 EC2 인스턴스 저장소용 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 아키텍처에 사용할 수 있는 여러 스토리지 클래스를 제공합니다. 모든 스토리지 클래스는 백업 데이터세트가 증가하더라도 볼륨이나 미디어를 관리할 필요 없이 확장 가능한 용량을 제공합니다. 사용한 만큼만 지불하는 모델과 저렴한 GB/월 비용 덕분에 Amazon S3 스토리지 클래스는 광범위한 데이터 보호 사용 사례에 적합합니다. Amazon S3 스토리지 클래스는 다음 범주를 포함한 여러 사용 사례에 맞춰 설계된 다양한 스토리지 클래스를 제공합니다.

- 빈번한 액세스 스토리지 클래스: 자주 액세스되는 데이터의 범용 스토리지 용도(예: 구성 파일, 계획되지 않은 백업, 일일 백업). 여기에는 모든 Amazon S3 객체의 기본값인 S3 Standard 스토리지 클래스가 포함됩니다.
- 비정기적 액세스 스토리지 클래스: 오랜 기간 보관하지만 자주 액세스하지 않는 데이터 용도(예: 월간 백업). 여기에는 S3 Standard-IA 스토리지 클래스가 포함됩니다. IA는 Infrequent Access(빈번하지 않은 액세스)의 약어입니다.
- S3 Glacier 스토리지 클래스: 거의 액세스할 필요가 없는 매우 장기 보관 데이터를 위한 용도(예: 연간 백업).https://docs.aws.amazon.com/AmazonS3/latest/userguide/glacier-storage-classes.html 여기에는 가장 저렴한 스토리지를 제공하는 S3 Glacier Deep Archive가 포함됩니다 AWS.

액세스 패턴을 알 수 없거나 변경 중인 백업의 경우 S3 Intelligent-Tiering 스토리지 클래스를 사용할 수 있습니다. S3 Intelligent-Tiering은 객체에 마지막으로 액세스한 일수에 따라 객체를 가장 비용 효율적인 계층으로 자동 전환합니다.

> **Note**
>
> 일부 스토리지 클래스는 최소 스토리지 기간 요금이 있습니다. 자세한 내용은 Amazon S3 요금을 참조하고 웹 페이지 검색을 사용하여 `duration`을 찾아보세요.

또한 Amazon S3는 수명 주기 전반에 걸쳐 데이터를 관리하기 위한 구성 가능한 수명 주기 정책을 제공합니다. 정책이 설정되면 애플리케이션 변경 없이 데이터가 적합한 스토리지 클래스로 자동으로 마이그레이션됩니다. 자세한 내용을 알아보려면 Amazon S3 객체 수명 주기 관리 설명서를 참조하세요.

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

- 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. AWS 청구에 대한 비용 할당 태그 지정 및 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 데이터에 대한 특정 시점 스냅샷을 저장할 수 있습니다. 표준 S3 접두사를 생성하면 특정 시점 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 특정 시점 백업을 수동 또는 프로그래밍 방식으로 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 특정 시점 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 standard 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 SDKs 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 클라우드로 파일 일괄 업로드 자습서를 참조하세요.

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

Amazon S3에서 백업 데이터 보안 유지

데이터 보안은 보편적인 문제이며 보안을 매우 심각하게 AWS 받아들입니다. 보안은 모든 AWS 서비스의 기본입니다. Amazon S3는 저장 중이거나 전송 중일 때 모두 액세스 제어 및 암호화를 위한 기능을 제공합니다. 모든 Amazon S3 엔드포인트는 전송 중 데이터를 암호화하기 위해 SSL/TLS를 지원합니다. 다음을 수행하여 저장된 객체에 대한 암호화를 설정할 수 있습니다.

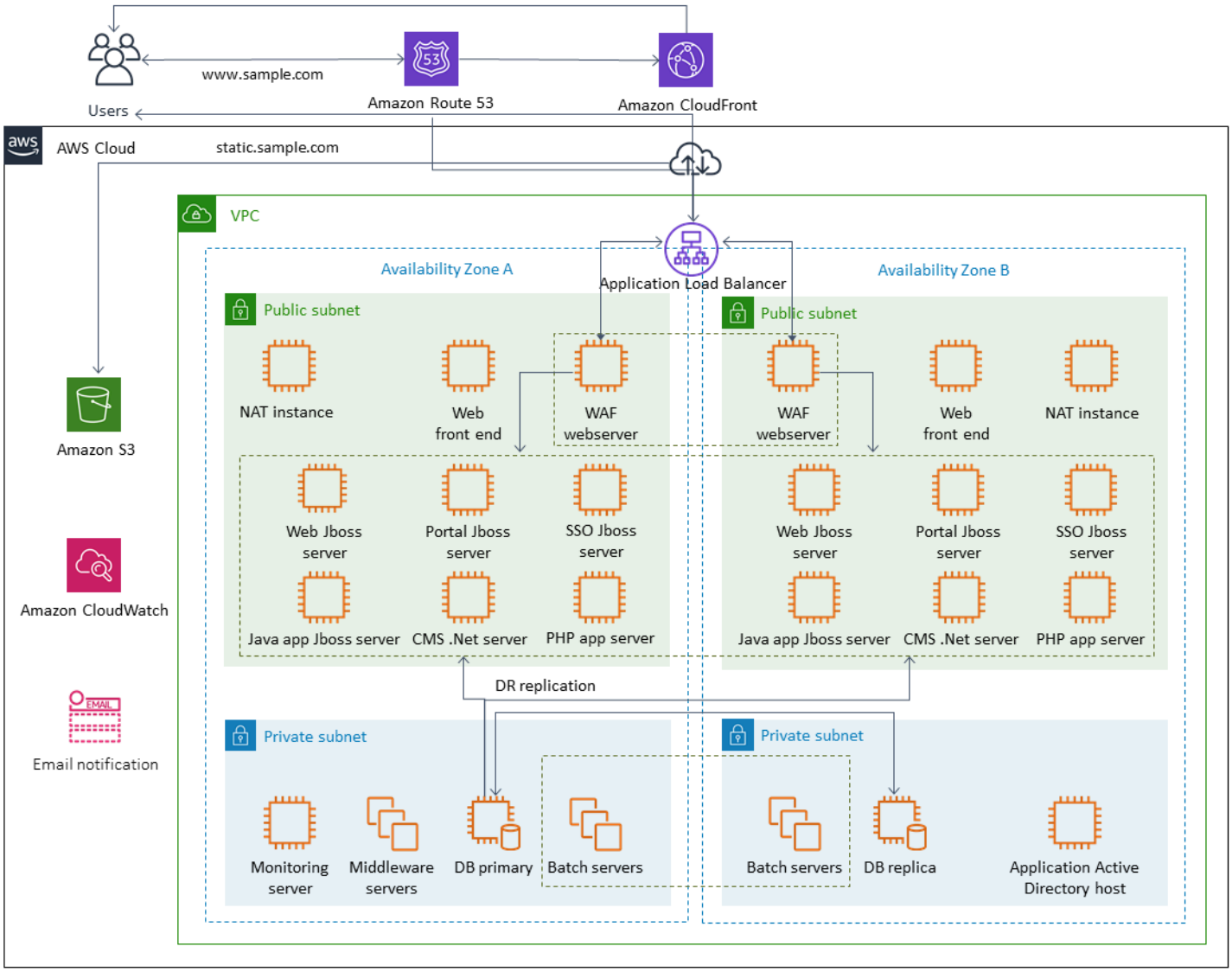
- Amazon S3 관리형 암호화 키로 서버 측 암호화(기본값) 사용
- 에 저장된 AWS Key Management Service (AWS KMS) 키와 함께 서버 측 암호화 AWS KMS 사용
- 클라이언트 측 암호화 사용

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 는 Amazon EC2 인스턴스를 백업하는 여러 방법을 제공합니다. 이 섹션에서는 Amazon Elastic Block Store(Amazon EBS) 볼륨 또는 스토리지용 인스턴스 저장소 볼륨을 백업하는 데 있어서의 다양한 측면을 다룹니다. 요구 사항을 충족하는 AWS 경우에서 백업을 관리하기 위한 첫 번째 선택 AWS Backup 으로를 고려하세요. 백업은 원래 기능으로 복원할 수 있는 경우에만 유효하다는 점을 기억하세요. 복원 및 복구 기능을 정기적으로 테스트하여 이를 확인해야 합니다.

다음 다이어그램의 솔루션 아키텍처는 Amazon EC2를 기반으로 하는 대부분의 아키텍처와 AWS 함께 완전히에 존재하는 워크로드 환경을 설명합니다. 다음 그림에서 볼 수 있듯이 시나리오에는 웹 서버, 애플리케이션 서버, 모니터링 서버, 데이터베이스, Active Directory 및 재해 복구(DR) 복제가 포함됩니다.



AWS 는 인스턴스 및 스토리지를 생성, 프로비저닝, 백업, 복원 및 최적화하는 차별화되지 않은 작업을 수행하기 위해이 아키텍처에 표시된 많은 Amazon EC2 서버에 대해 많은 완전한 기능을 갖춘 서비스를 제공합니다. 이러한 서비스가 복잡성과 관리를 줄이기 위해 아키텍처에 적합한지 고려합니다. AWS 또한는 Amazon EC2 기반 아키텍처의 가용성을 개선하기 위한 서비스를 제공합니다. 특히 Amazon EC2의 워크로드를 보완하기 위해 Amazon EC2 Auto Scaling 및 Elastic Load Balancing을 고려해 보세요. 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 섹션에서 자세히 설명하는 다양한 백업 및 복구 기능을 제공합니다.

주제

- 스냅샷과 AMI를 사용한 Amazon EC2 백업 및 복구
- AMI와 EBS 스냅샷을 사용하여 EBS 볼륨 백업 생성
- Amazon EBS 볼륨 또는 EC2 인스턴스 복원

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 보세요.

AMI 또는 Amazon EBS 스냅샷을 백업에 사용

AMI는 다음을 포함합니다.

- 하나 이상의 스냅샷 인스턴스 저장소 지원 AMI에는 인스턴스의 루트 볼륨(예: 운영 체제, 애플리케이션 서버 및 애플리케이션)에 대한 템플릿이 포함되어 있습니다.
- AMI를 사용하여 인스턴스를 시작할 수 있는 AWS 계정을 제어하는 시작 권한입니다.
- 시작될 때 인스턴스에 연결할 볼륨을 지정하는 블록 디바이스 매핑

> **Note**
>
> 대부분의 경우 Windows, Red Hat, SUSE 및 SQL Server용 AMI를 사용하려면 AMI에 올바른 라이선스 정보가 있어야 합니다. 자세한 내용은 AMI 청구 정보 이해를 참조하세요. 스냅샷에서 AMI를 생성할 때 `RegisterImage` 작업은 스냅샷의 메타데이터에서 올바른 결제 정보를 가져오지만, 이를 위해서는 적절한 메타데이터가 있어야 합니다. 올바른 결제 정보가 적용되었는지

확인하려면 새 AMI의 플랫폼 세부 정보 필드를 확인합니다. 필드가 비어 있거나 예상 운영 체제 코드(예: Windows, Red Hat, SUSE 또는 SQL)와 일치하지 않는 경우 AMI 생성에 실패한 것이므로 AMI를 삭제하고 인스턴스에서 AMI 생성의 지침을 따라야 합니다.

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

에서 유지 관리하고 게시하는 AWS 플랫폼 및 애플리케이션 AMIs를 사용하는 경우 데이터에 대해 별도의 볼륨을 유지하는 것이 AWS Marketplace좋습니다. 데이터 볼륨을 운영 체제 및 애플리케이션 볼륨과 분리된 스냅샷으로 백업할 수 있습니다. 그런 다음에서 AWS 또는에서 게시한 새로 업데이트된 AMIs 함께 데이터 볼륨 스냅샷을 사용합니다 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 는 인스턴스 수준 백업을 AMIs로 지원하고 볼륨 수준 백업을 별도의 스냅샷으로 지원합니다.

- 인스턴스의 모든 EBS 볼륨을 완전히 백업하려면 EC2 인스턴스의 AMI를 생성합니다. 롤백하려면 인스턴스 시작 마법사를 사용하여 인스턴스를 생성합니다. 인스턴스 시작 마법사에서 내 AMI를 선택합니다.
- 개별 볼륨을 백업하려면 스냅샷을 생성합니다. 스냅샷을 복원하려면 스냅샷에서 볼륨 생성을 참조하세요. 또는 AWS Command Line Interface ()를 사용할 AWS Management Console 수 있습니다 AWS CLI.

인스턴스 AMI의 비용은 인스턴스의 모든 볼륨 스토리지에 해당하며, 메타데이터는 포함되지 않습니다. EBS 스냅샷 비용은 개별 볼륨의 스토리지에 해당합니다. 볼륨 스토리지 비용에 대한 자세한 내용은 Amazon EBS 요금 페이지를 참조하세요.

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 데이터의 특정 시점 백업을 위한 스냅샷 기능도 지원합니다. 모든 EBS 볼륨 유형은 내구적 스냅샷 기능을 제공하고 99.999% 가용성으로 설계되었습니다. 자세한 내용은 Amazon 컴퓨팅 서비스 수준 계약을 참조하세요.

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 EBS 설명서를 참조하세요.

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 EBS 설명서에 설명된 대로 Amazon EBS 스냅샷 복사 기능을 사용하여 AWS 리전 간에 Amazon EBS 스냅샷을 복사할 수도 있습니다. https://docs.aws.amazon.com/ebs/latest/userguide/ebs-copy-snapshot.html 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 Amazon EBS를 사용하여 프로비저닝된 볼륨을 확장할 수 있으므로 AWS이 위험이 크게 줄어듭니다. 자세한 내용은 AWS 설명서를 참조하세요.

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 저장소 볼륨에 대한 고려 사항

인스턴스 저장소는 인스턴스에 임시 블록 스토리지를 제공합니다. 스토리지는 호스트 컴퓨터에 물리적으로 연결된 디스크에 위치합니다. 인스턴스 저장소는 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 저장소의 데이터는 관련 인스턴스의 수명 기간 동안만 지속됩니다. 인스턴스가 재부팅(의도적 또는 의도적이지 않게)되면 인스턴스 저장소의 데이터는 유지됩니다. 그러나 다음 상황에서는 인스턴스 저장소의 데이터가 손실됩니다.

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

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

인스턴스 저장소 볼륨의 일반적인 전략은 목표 복구 시점(RPO) 및 목표 복구 시간(RTO)을 기반으로 필요에 따라 필요한 데이터를 Amazon S3에 정기적으로 보관하는 것입니다. 그러면 새 인스턴스가 시작될 때 Amazon S3에서 인스턴스 저장소로 데이터를 다운로드할 수 있습니다. 인스턴스가 중지되기 전에 Amazon S3에 데이터를 업로드할 수도 있습니다. 지속성을 위해 EBS 볼륨을 생성하여 인스턴스

에 연결하고 인스턴스 저장소 볼륨의 데이터를 주기적으로 EBS 볼륨으로 복사하세요. 자세한 정보는 AWS 지식 센터를 참조하세요.

EBS 스냅샷 및 AMI에 대한 태그 지정 및 표준 적용

모든 AWS 리소스에 태그를 지정하는 것은 비용 할당, 감사, 문제 해결 및 알림에 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 확인하세요. 그러면 액세스 정책, 연결 정보, 비용 할당 등의 스냅샷 메타데이터를 설정하여 나중에 이러한 백업을 사용하는 데 도움이 됩니다. AWS 리소스 태그 지정에 대한 자세한 내용은 태그 지정 모범 사례 기술 문서를 참조하세요.

모든 AWS 리소스에 사용하는 태그 외에도 다음 백업별 태그를 사용합니다.

- 소스 인스턴스 ID
- 소스 볼륨 ID(스냅샷용)
- 복구 시점 설명

AWS Config 규칙 및 IAM 권한을 사용하여 태그 지정 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 참조하세요.

AWS Config 규칙을 사용하여 리소스의 구성 설정을 자동으로 평가할 수 있습니다 AWS . 시작하는 데 도움이 되도록는 관리형 규칙이라고 하는 사용자 지정 가능한 사전 정의된 규칙을 AWS Config 제공합니다. 고유의 사용자 지정 규칙을 만들 수도 있습니다. 는 리소스 간의 구성 변경을 AWS Config 지속적으로 추적하지만 이러한 변경 사항이 규칙의 조건을 위반하는지 확인합니다. 리소스가 규칙을 위반하는 경우는 리소스와 규칙을 규정 미준수로 AWS Config 표시합니다. 필수 태그 관리형 규칙은 현재 스냅샷과 AMI를 지원하지 않습니다.

AMI와 EBS 스냅샷을 사용하여 EBS 볼륨 백업 생성

AWS 는 AMIs 및 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 스

냅샷이 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 하세요. 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 참조하세요. 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 수행하세요.

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 일관성 스냅샷을 생성하는 데 도움이 되는 Volume Shadow Copy Service(VSS)를 제공합니다.는 VSS 인식 애플리케이션의 이미지 수준 백업을 수행하기 위해 실행할 수 있는 Systems Manager 문서를 AWS 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 Sysprep하세요. 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 마세요.

콘솔에서 수동으로 EBS 볼륨 스냅샷 생성

인스턴스에서 완전히 테스트되지 않은 주요 변경 사항을 적용하기 전에 적절한 볼륨 또는 전체 인스턴스의 스냅샷을 생성하세요. 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.

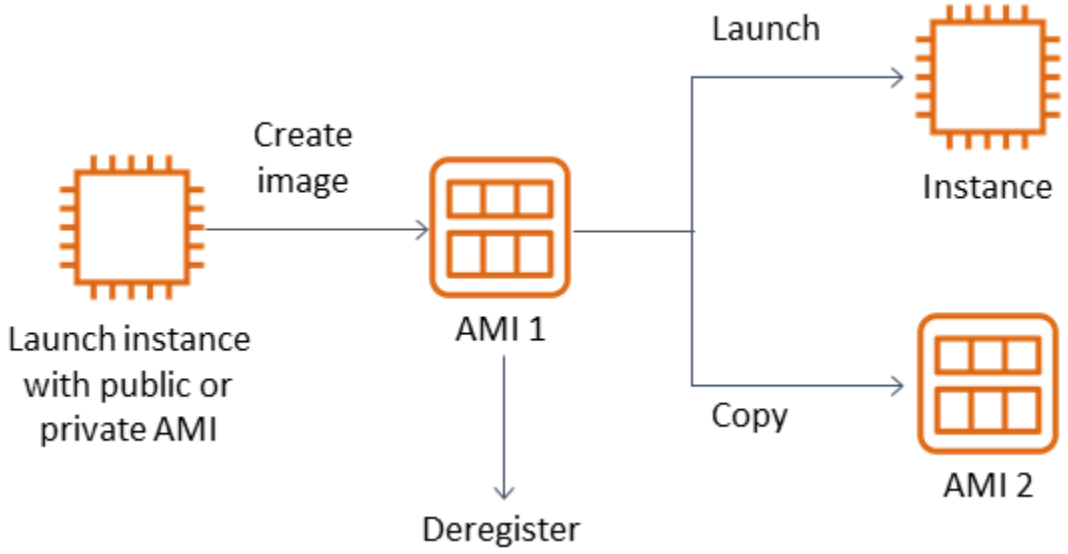
설명을 입력하고 적절한 태그를 추가합니다. 나중에 볼륨을 더 쉽게 찾을 수 있도록 `Name` 태그를 추가합니다. 태그 지정 전략에 따라 다른 적절한 태그를 추가합니다.

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 로 마이그레이션하지 않는 한 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 보세요.

- 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

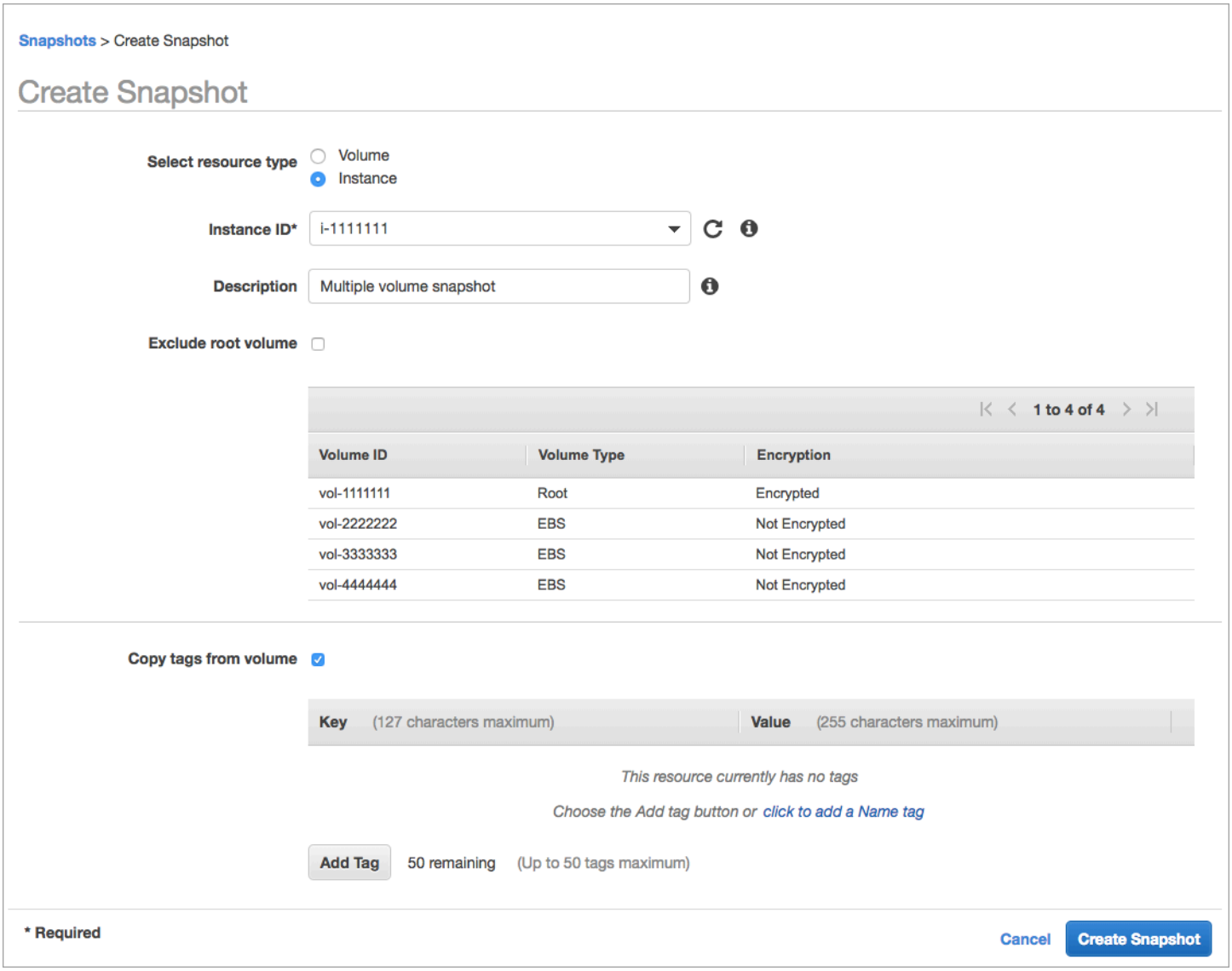
AWS Backup 는 Amazon Data Lifecycle Manager에서 고유합니다. 여러 AWS 서비스의 리소스를 포함하는 백업 계획을 생성할 수 있기 때문입니다. 리소스 백업을 개별적으로 조정하는 대신 함께 사용하는 리소스를 포함하도록 백업을 조정할 수 있습니다.

AWS Backup 에는 완료된 백업의 복구 시점에 대한 액세스를 제한할 수 있는 백업 볼트 개념도 포함되어 있습니다. 각 개별 리소스로 진행하고 생성된 백업을 복원하는 AWS Backup 대신에서 복원 작업을 시작할 수 있습니다. AWS Backup 에는 감사 관리 및 보고와 같은 추가 기능도 포함되어 있습니다. 자세한 내용은 이 설명서의 AWS Backup을 사용하여 백업 및 복구 섹션을 참조하세요.

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 배열을 위한 일관된 스냅샷 세트를 생성하려면 CreateSnapshots API 작업을 사용하거나 Amazon EC2 콘솔에 로그인하여 Elastic Block Store, 스냅샷, 스냅샷 생성을 선택합니다.



RAID 구성에서 여러 볼륨이 연결된 인스턴스의 스냅샷은 일괄적으로 다중 볼륨 스냅샷으로 촬영됩니다. 다중 볼륨 스냅샷을 통해 EC2 인스턴스에 연결된 여러 EBS 볼륨에서 특정 시점, 데이터 조정 및 충돌 일치 스냅샷을 생성할 수 있습니다. 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 참조하세요.

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 위반으로 인해 중요한 백업이 손실되는 것을 방지하려면 백업을 다른 AWS 계정에 복사하는 것이 좋습니다. AWS 계정이 여러 개인 경우 별도의 계정을 다른 모든 계정이 백업을 복사할 수 있는 아카이브 계정으로 지정할 수 있습니다. 예를 들어, AWS Backup에서 계정 간 백업을 사용하여 이 작업을 수행할 수 있습니다.

재해 복구 계획에서는 리전별 장애 AWS 리전 발생 시 다른에서 EC2 인스턴스를 재현해야 할 수도 있습니다. 백업을 동일한 계정 내의 다른 리전에 복사하여 이 목표를 달성할 수 있습니다. 이를 통해 실수로 인한 삭제 방지 계층을 추가로 제공하고 재해 복구(DR) 목표를 지원할 수 있습니다. AWS Backup는 교차 리전 백업을 지원합니다.

ec2:DeleteSnapshot 및 ec2:DeregisterImage 작업에 대한 IAM 권한을 차단하는 것을 고려해 보세요. 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 AWS 리소스를 지원하는 AWS Backup 볼트 잠금을 사용할 수도 있습니다.

또한 ec2:ModifyImageAttribute 및 ec2:ModifySnapshotAttribute IAM 작업을 차단하여 사용자가 AMI와 EBS 스냅샷을 공유하는 기능을 차단하는 것도 고려해 보세요. 이렇게 AMIs 및 스냅샷이 조직 외부의 AWS 계정과 공유되지 않습니다. 를 사용하는 경우 사용자가 백업 볼트에서 유사한 작업을 수행하지 못하도록 AWS Backup제한합니다. 자세한 내용은 이 설명서의 AWS Backup 섹션을 참조하세요.

Amazon EBS에는 실수로 삭제된 EBS 스냅샷을 복원하는 데 도움이 되는 휴지통 기능이 포함되어 있습니다. 사용자가 스냅샷을 삭제하도록 허용하는 경우 필요한 스냅샷이 영구적으로 삭제되지 않도록 이 기능을 활성화하세요. Amazon EC2 콘솔에서는 한 번에 여러 스냅샷을 선택하여 삭제할 수 있으므로 사용자는 여러 스냅샷을 삭제할 때 특히 주의해야 합니다. 또한 클린업 스크립트와 자동화를 사용할 때는 필요한 스냅샷을 실수로 삭제하지 않도록 주의하세요. 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 볼륨의 수명 주기 종료 단계로 스냅샷 아카이브를 고려할 수 있습니다. 삭제보다는 아카이브하는 것이 휴지통을 사용하는 것보다 더 비용 효율적인 삭제 보존 방법일 수도 있습니다.

Systems Manager, 및 AWS SDKs를 사용하여 스냅샷 AWS CLI및 AMI 생성 자동화

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 생성 전 및 생성 후 작업을 자동화하려면 AWS CLI 및 SDK를 사용하여 백업 프로세스를 스크립팅합니다.

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 런북을 사용하여 스냅샷 및 AMIs를 생성하거나 다른 사용자에게 사용할 수 있는 권한을 부여할 수 있습니다. Systems Manager에는 AMI 패치 및 AMI 생성을 자동화하기 위한 AWS-UpdateLinuxAmi 및 AWS-UpdateWindowsAmi 실행서도 포함되어 있습니다.

AWS CLI 및를 사용하여 스냅샷 및 AMI 생성 프로세스를 자동화AWS Tools for Windows PowerShell할 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 AMIs. 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 사용하세요.

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 목표 복구 시점(RPO) 및 목표 복구 시간(RTO)을 충족하는지와 복원 프로세스가 예상대로 작동하는지 확인하세요. 복원 프로세스가 복원 중인 인스턴스에 의존하는 애플리케이션과 서비스에 어떤 영향을 미칠지 생각해 본 다음 필요에 따라 복원을 조정하세요. 복원 프로세스를 최대한 자동화하고 테스트하여 복원 프로세스가 실패하거나 일관되지 않게 구현될 위험을 줄이세요.

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 정확한 특정 시점 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 CLI또는 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 유의하세요. 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 해제하세요. 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 특정 시점 백업으로 복원하려면 다음 단계를 따르세요.

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.

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

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.

> **Note**
>
> 대부분의 경우 Windows, Red Hat, SUSE 및 SQL Server용 AMI를 사용하려면 AMI에 올바른 라이선스 정보가 있어야 합니다. 자세한 내용은 AMI 청구 정보 이해를 참조하세요. 스냅샷에서 AMI를 생성할 때 `RegisterImage` 작업은 스냅샷의 메타데이터에서 올바른 결제 정보를 가져오지만, 이를 위해서는 적절한 메타데이터가 있어야 합니다. 올바른 결제 정보가 적용되었는지 확인하려면 새 AMI의 플랫폼 세부 정보 필드를 확인합니다. 필드가 비어 있거나 예상 운영 체제 코드(예: Windows, Red Hat, SUSE 또는 SQL)와 일치하지 않는 경우 AMI 생성에 실패한 것이므로 AMI를 삭제하고 인스턴스에서 AMI 생성의 지침을 따라야 합니다.

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

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.
5. (Windows, Red Hat, SUSE, SQL Server 전용) 올바른 결제 정보가 적용되었는지 확인하려면 새 AMI의 플랫폼 세부 정보 필드를 확인합니다. 필드가 비어 있거나 예상 운영 체제 코드(예: Windows 또는 Red Hat)와 일치하지 않는 경우 AMI 생성에 실패한 것이므로 AMI를 삭제하고 인스턴스에서 AMI 생성의 지침을 따라야 합니다.

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 보세요. 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 차단하세요. 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 해제하세요.

온프레미스 인프라에서 로 백업 및 복구 AWS

온프레미스 인프라 백업의 내구성 있는 오프사이트 스토리지 AWS 에를 사용할 수 있습니다. 이 시나리오에서 AWS 스토리지 서비스를 사용하면 백업 및 아카이빙 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 통합하기 위한 광범위한 API 작업 및 SDK를 제공합니다. 또한 백업 소프트웨어 공급업체는 애플리케이션을 AWS 스토리지 솔루션과 직접 통합할 수 있습니다.

이 시나리오에서는 온프레미스 인프라에서 사용 중인 백업 및 아카이브 소프트웨어가 API 작업을 AWS 통해와 직접 인터페이스합니다. 백업 소프트웨어는 AWS인식되므로 온프레미스 서버의 데이터를 Amazon S3로 직접 백업합니다.

기존 백업 소프트웨어가 기본적으로 AWS 클라우드를 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 소프트웨어를 온프레미스 스토리지 게이트웨이로 안내하고, 이를 Amazon S3에 연결하는 테이프 게이트웨이입니다. 이 옵션은 기존 투자 또는 프로세스를 중단하지 않고 안전하게 장기간 보존할 수 있도록 클라우드의 확장성과 내구성을 제공합니다.

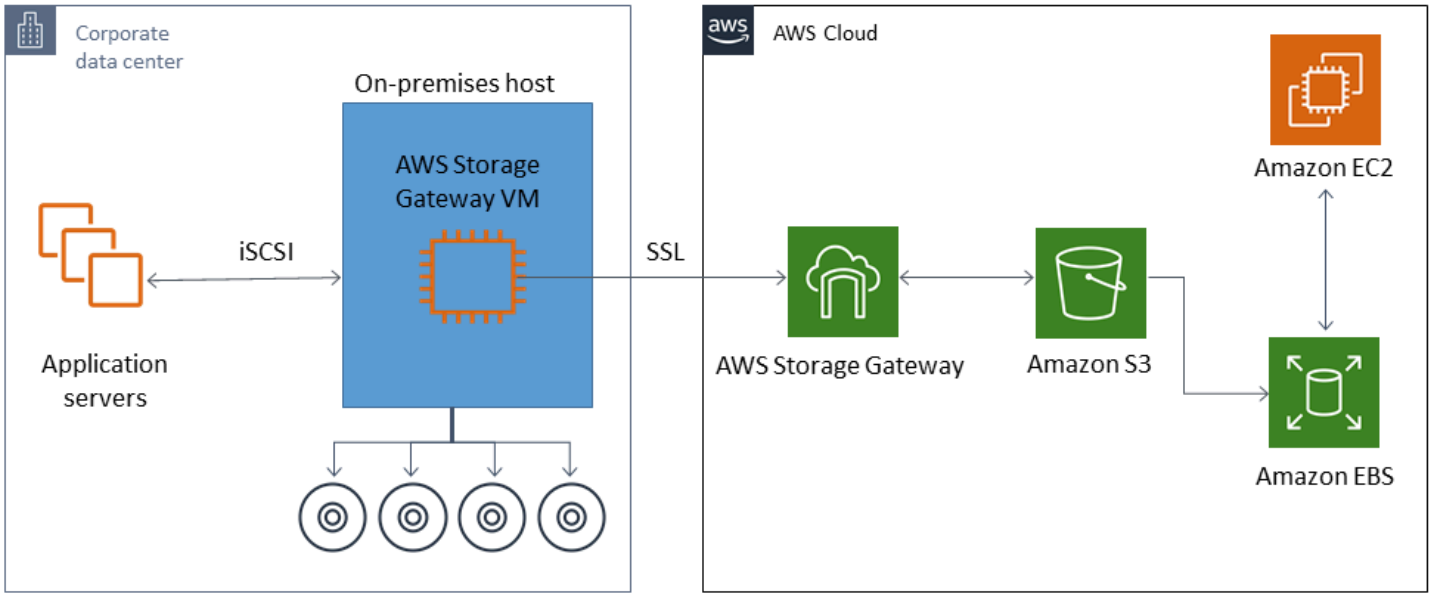
File Gateway

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 도구 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. 백업을 저렴한 S3 Standard-Infrequent Access 및 Amazon Glacier 스토리지 클래스로 계층화하여 장기 보존 요구 사항을 해결할 수 있습니다.

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 볼륨에 대해 전체 PIT(point-in-time) 스냅샷을 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.



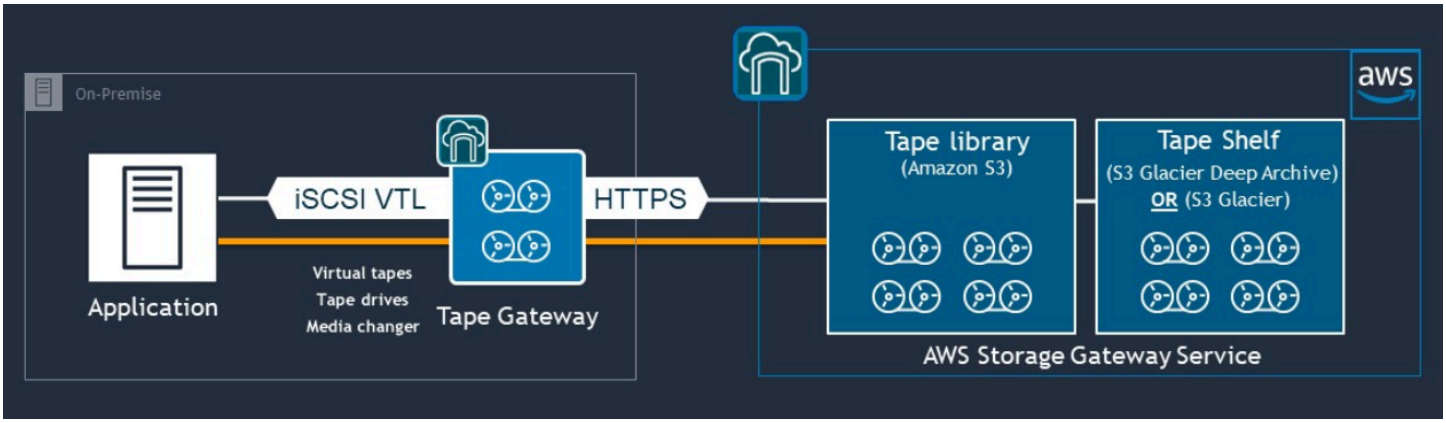
볼륨 게이트웨이는 Amazon EC2의 Amazon EBS 볼륨 기능과 통합되므로 AWS Backup 를 사용하여 스냅샷 프로세스를 자동화하고 예약할 수 있습니다. 볼륨 게이트웨이는 내구성이 뛰어난 Amazon S3–backed Amazon EBS 스냅샷 및 태깅 기능의 이점을 추가로 제공합니다. 자세한 내용은 Amazon EBS 스냅샷 설명서를 참조하세요.

Tape Gateway

테이프 게이트웨이는 오프사이트 가상 테이프 백업 스토어를 위한 Amazon S3의 뛰어난 내구성, 저렴한 계층형 스토리지, 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 또한는 정기적으로 고정성 검사를 수행하여 데이터를 읽을 수 있고 오류가 발생하지 않았는지 확인합니다. Amazon S3에 저장된 모든 테이프는 기본 키 또는 AWS KMS 키를 사용한 서버 측 암호화로 보호됩니다. 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 Retrieval 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 보세요. 자세한 내용은 테이프 게이트웨이를 지원하는 타사 백업 애플리케이션 목록을 검토해 보세요.

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 방식은 워크로드에 사용되는 AWS 서비스를 포함해야 합니다.는 데이터를 관리하고 상호 작용하기 위한 서비스별 기능과 옵션을 AWS 제공합니다. 콘솔, AWS CLI, SDKs 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 Backup 은 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 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 직접 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 직접 호출을 사용하여 DB 스냅샷을 생성할 수 있습니다. 이러한 스냅샷은 콘솔이나 `DeleteDBSnapshot` API 직접 호출을 사용하여 명시적으로 삭제할 때까지 보관됩니다.

이러한 두 백업 옵션 모두 다른 기능 AWS Backup도 제공하는의 Amazon RDS에서 지원됩니다. AWS Backup 를 사용하여 Amazon RDS 데이터베이스에 대한 표준 백업 계획을 설정하고 특정 데이터베이스에 대한 백업 계획이 고유한 경우 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.

DynamoDB 콘솔 AWS CLI, 또는 DynamoDB API를 사용하여 DynamoDB 테이블의 온디맨드 백업을 생성할 수도 있습니다. 자세한 내용은 DynamoDB 테이블 백업을 참조하세요. 를 사용하여 정기 또는 향후 백업을 예약 AWS Backup하거나 Lambda 함수를 사용하여 백업 접근 방식을 사용자 지정하고 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 Backup 를 사용하여 백업 계획을 생성할 수 있습니다. 백업 계획에는 DynamoDB 테이블에 대한 일정 및 보존 정책이 포함됩니다.는 백업을 AWS Backup 생성하고 보존 일정에 따라 이전 백업을 삭제합니다. 또한 DynamoDB 서비스에서 사용할 수 없는 저비용 계층형 스토리지, 교차 계정 및 교차 리전 복사를 포함한 고급 DynamoDB 백업 옵션 AWS Backup 도 포함됩니다. 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.

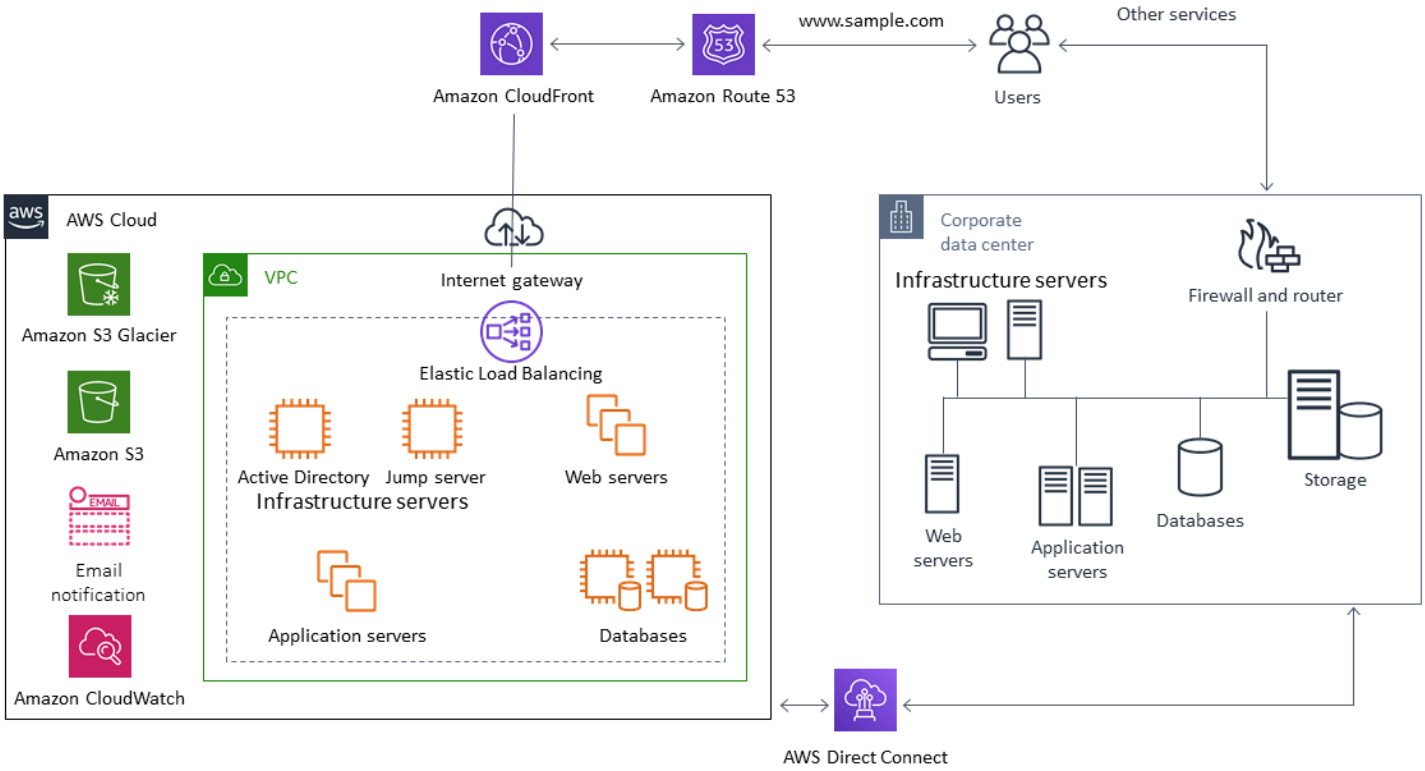
복원 프로세스는 클라이언트가 새로 복원된 테이블 이름을 사용하도록 지시하는 방법을 고려해야 합니다. 구성 파일, AWS Systems Manager 파라미터 스토어 값 또는 클라이언트가 사용해야 하는 테이블 이름을 반영하도록 동적으로 업데이트할 수 있는 다른 참조에서 DynamoDB 테이블 이름을 검색하도록 애플리케이션과 클라이언트를 구성할 수 있습니다.

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 배포를 워크로드 환경에 온프레미스 및 AWS 인프라 구성 요소가 있는 하이브리드 시나리오와 결합할 수 있습니다. 웹 서버, 애플리케이션 서버, 모니터링 서버, 데이터베이스 및 Microsoft Active Directory를 비롯한 리소스는 고객 데이터 센터 또는 AWS에서 호스팅됩니다. AWS 클라우드에서 실행 중인 애플리케이션은 온프레미스에서 실행 중인 애플리케이션에 연결됩니다.

이것은 엔터프라이즈 워크로드의 일반적인 시나리오가 되고 있습니다. 많은 기업이 자체 데이터 센터를 보유하고 있으며 AWS 를 사용하여 용량을 늘리고 있습니다. 이러한 고객 데이터 센터는 대용량 AWS 네트워크 링크를 통해 네트워크에 연결되는 경우가 많습니다. 예를 들어를 Direct Connect사용하면 온프레미스 데이터 센터에서 로 프라이빗 전용 연결을 설정할 수 있습니다 AWS. 이는 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.



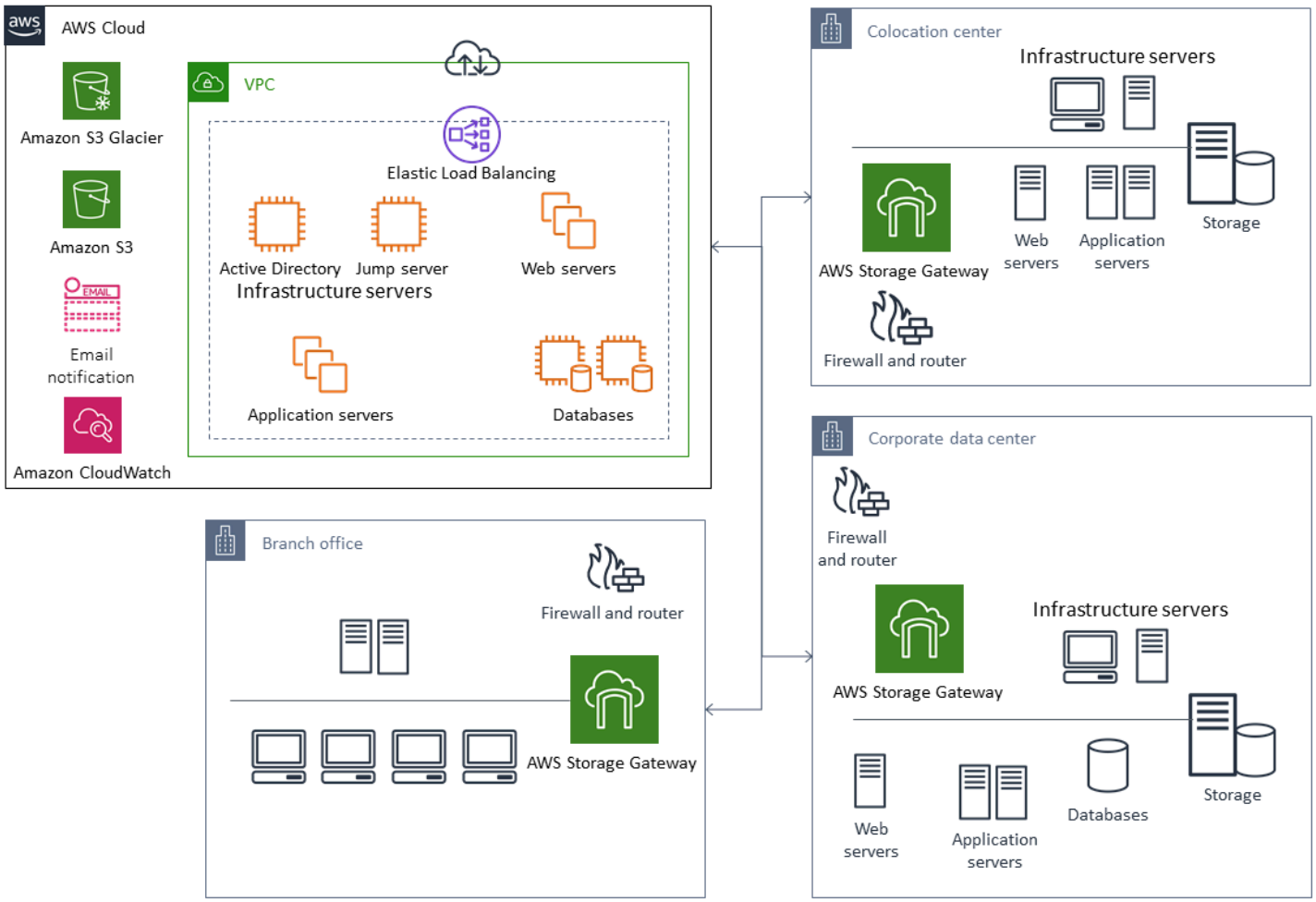
잘 설계된 데이터 보호 솔루션은 일반적으로 이 설명서의 클라우드 네이티브 솔루션과 온프레미스 솔루션에서 설명된 옵션을 조합하여 사용합니다. 많은 ISV는 온프레미스 인프라를 위해 업계 최고의 백업 및 복원 솔루션을 제공하며 하이브리드 접근 방식을 지원하도록 솔루션을 확장했습니다.

가용성을 높이기 위해 중앙 집중식 백업 관리 솔루션을 클라우드로 이전합니다.

기존 백업 관리 솔루션 투자를와 함께 사용하면 접근 방식의 복원력과 아키텍처를 개선할 AWS수 있습니다. 기본 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 보세요.

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 게이트웨이는 전 세계에 걸쳐 있을 수 있는 애플리케이션 워크플로를 AWS 위해에 저장된 데이터에 대한 온디맨드 방식의 지연 시간이 짧은 액세스를 제공합니다. 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
Infrastructure servers
Web 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
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

를 사용한 재해 복구 AWS

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

주제

- 에 대한 온프레미스 DR AWS
- 클라우드 네이티브 워크로드용 DR

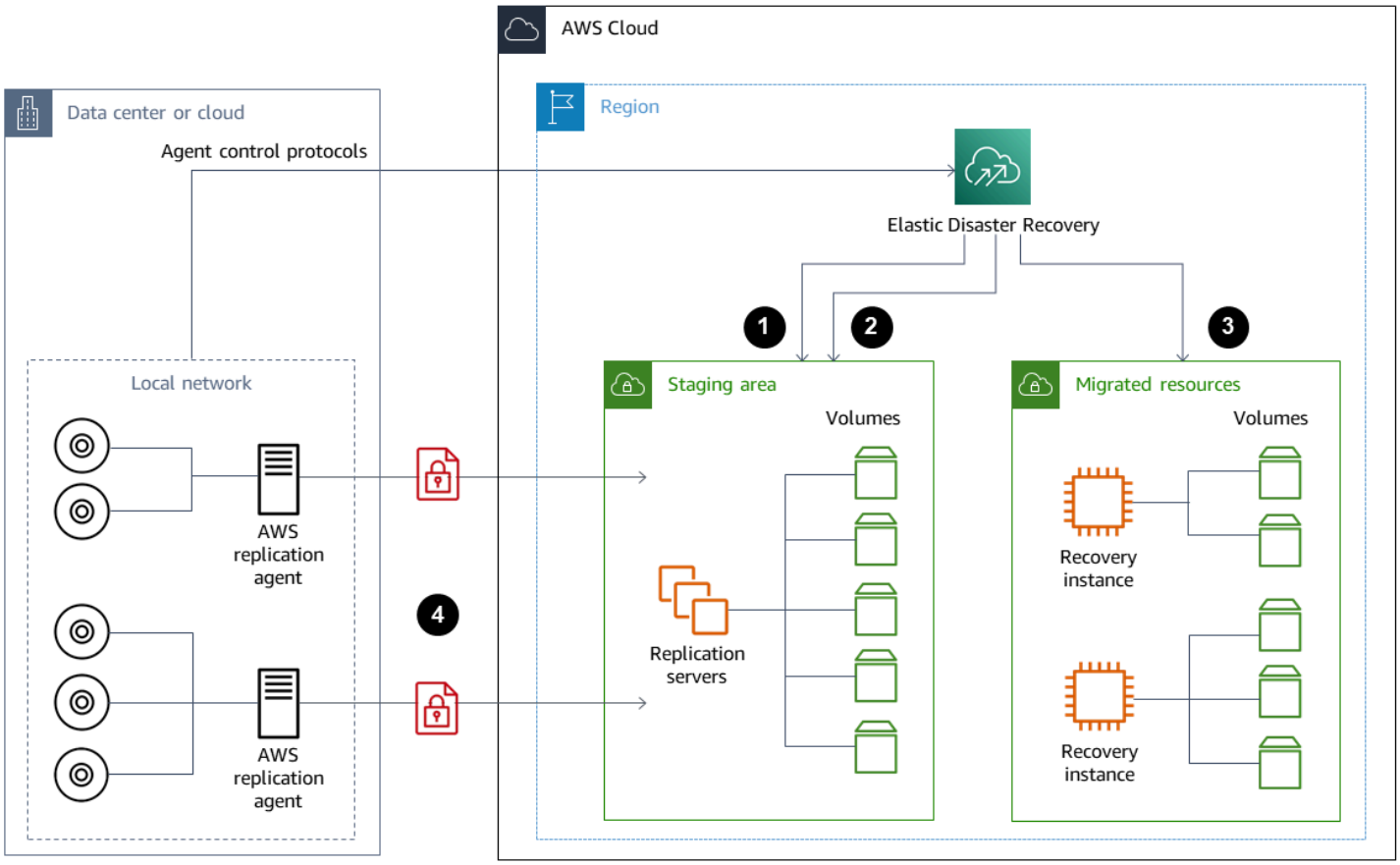
에 대한 온프레미스 DR AWS

를 온프레미스 워크로드에 대한 오프사이트 재해 복구(DR) 환경 AWS 으로 사용하는 것은 일반적인 하이브리드 시나리오입니다. 사용할 기술을 선택하기 전에 필요한 복구 시간 및 복구 지점 목표를 비롯한 DR 목표를 정의하세요. 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 확인하세요.

AWS 에서는 루트 볼륨 및 운영 체제를 포함하여 온프레미스 서버의 전체 복제본을 AWS Elastic Disaster Recovery 생성할 수 있습니다 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 목표 복구 시간(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 확인하세요. 또한 중앙 데이터베이스에서 작업을 폴링하고 가져올 수 있는 모든 작업자 유형 프로세스가 중복이나 충돌을 방지하도록 적절하게 구성되어 있는지 확인하세요. DR 프로세스에 복구 서버 인스턴스가 온라인 상태가 되기 전에 수행해야 하는 모든 필수 단계를 포함시키세요. 또한 복구 서버 인스턴스가 온라인 상태이고 사용 가능한 상태가 된 후에 수행할 단계도 포함하세요. 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 데이터세트에 액세스할 때 지연 시간을 단축합니다. 또한 Volume Gateway는 온프레미스에서 사용하거나 Amazon EC2에서 사용하기 위해 복원할 수 있는 견고한 스냅샷 기반 백업을 제공합니다. 워크로드의 목표 복구 시점(RPO)를 기반으로 시점 스냅샷을 스케줄링할 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 고려하세요.는 전 세계 리전에서 여러 가용 영역을 AWS 제공합니다. AWS 클라우드를 사용하는 많은 기업은 가용 영역의 손실을 견딜 수 있도록 워크로드 아키텍처와 DR 목표를 조정합니다. AWS Well-Architected Framework의 신뢰성 원칙은이 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 파악하세요. 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 보세요. 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 하세요. 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 시작하세요. 그런 다음 이 새 인스턴스를 가리키도록 Route 53 레코드를 업데이트하세요.

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

리전별 장애 발생 시 Amazon EC2에 대한 DR

가용성 요구 사항이 매우 높은 고객(예: 가동 중지 시간을 허용할 수 없는 미션 크리티컬 애플리케이션)은 AWS 여러 리전에서를 사용하여 리전 수준의 문제에 대한 추가 복원력을 제공할 수 있습니다. 고객은 다중 리전 DR 계획을 수립하고 유지하는 데 필요한 복잡성, 비용 및 노력을 이점과 비교하여 신중하게 고려해야 합니다.는 글로벌 가용성, 장애 조치 및 DR을 위한 다중 리전 아키텍처를 지원하는 기능을 AWS 제공합니다. 이 가이드에서는 Amazon EC2의 백업 및 복구와 관련된 몇 가지 사용 가능한 기능을 다룹니다.

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

AWS Elastic Disaster Recovery를 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 보존 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. 에서 생성한 백업 AWS 에는 생성 날짜가 정렬되어 있지만 백업을 워크로드, 보존 요구 사항 및 복원 지점 식별과 상호 연관시키는 데는 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. 이 자동 문제 해결은 AWS Config 규칙,를 사용하는 스크립트 AWS CLI또는 AWS SDK를 사용하는 Lambda 함수를 사용하여 구현할 수 있습니다.

Systems Manager는 Amazon EBS 스냅샷의 정리를 시작하고 자동화하는 데 도움이 되는 AWS-DeleteEBSVolumeSnapshots 및 AWS-DeleteSnapshot 문서를 제공합니다. AWS CLI 및 AWS SDK를 사용하여 Amazon RDS 스냅샷과 같은 다른 AWS 리소스의 정리를 자동화할 수도 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 resources

- AWS 권장 가이드
- AWS 설명서
- AWS 일반 참조
- AWS 용어집

AWS 서비스

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

기타 리소스

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

문서 기록

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

변경 사항	설명	날짜
정보 업데이트	Amazon S3 섹션의 지침이 업데이트되었습니다.	2024년 6월 28일
업데이트된 정보	AWS대상 온프레미스 DR 섹션의 정보가 업데이트되었습니다.	2023년 4월 13일
섹션 추가	스냅샷에서 인스턴스를 만들거나 복원하기 위한 지침 및 단계가 추가되었습니다.	2023년 3월 7일
Elastic 재해 복구에 대한 정보 추가 및 설명 추가	를 사용한 재해 복구 AWS 및 데이터 보호를 위한 AWS 서비스 선택 섹션에서에 대한 정보가 추가되었습니다 AWS Elastic Disaster Recovery. 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 추가	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
정보 업데이트 및 새 섹션 추가	데이터 보호를 위한 AWS 서비스 선택 섹션에서에 서비스가 추가되었습니다. 를 사용한 백업 및 복구 AWS Backup 단원이 추가되었습니다. Amazon S3 및 Amazon Glacier를 사용한 백업 및 복구 섹션에 새로운 Amazon 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 권장 사항이 추가되었습니다 AWS Backup. 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 Backup 섹션에가 AWS Backup 지원하는 AWS 서비스에 대한 정보가 추가되었습니다.	2021년 6월 1일
최초 게시	—	2020년 7월 29일

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