개발자 안내서

AWS Backup

AWS Backup: 개발자 안내서

Table of Contents

이게 뭐야 AWS Backup?

AWS Backup 서비스, 클라우드 및 온프레미스에서 데이터 보호를 쉽게 중앙 집중화하고 자동화할 수 있는 완전 관리형 AWS 서비스입니다. 이 서비스를 사용하면 한 곳에서 백업 정책을 구성하고 AWS 리소스의 활동을 모니터링할 수 있습니다. 이를 통해 이전에 수행했던 백업 작업을 자동화하고 통합할 수 있으며 service-by-service, 사용자 지정 스크립트와 수동 프로세스를 만들 필요가 없습니다. AWS Backup 콘솔에서 클릭 몇 번으로 데이터 보호 정책 및 일정을 자동화할 수 있습니다.

AWS Backup 외부 AWS 환경에서 수행하는 백업에는 적용되지 않습니다. AWS Backup따라서 비즈니스 및 규정 준수 요구 사항을 충족하는 중앙 집중식 end-to-end 솔루션을 원한다면 AWS Backup 지금 바로 사용해 보십시오.

기능 개요

AWS Backup 는 다음을 비롯한 많은 특징과 기능을 제공합니다.

중앙 집중식 백업 관리

AWS Backup 중앙 집중식 백업 콘솔, 백업 API 세트, 그리고 애플리케이션이 사용하는 AWS 서비스 전반의 백업을 관리할 수 있는 AWS Command Line Interface (AWS CLI) 를 제공합니다. 를 사용하면 백업 요구 사항에 맞는 백업 정책을 중앙에서 관리할 수 있습니다. AWS Backup그런 다음 이를 AWS 서비스 전반의 AWS 리소스에 적용하여 일관되고 규정을 준수하는 방식으로 애플리케이션 데이터를 백업할 수 있습니다. AWS Backup 중앙 집중식 백업 콘솔은 백업 및 백업 작업 로그를 통합적으로 보여주므로 백업을 쉽게 감사하고 규정 준수를 보장할 수 있습니다.

정책 기반 백업

를 AWS Backup사용하여 백업 계획이라는 백업 정책을 만들 수 있습니다. 이러한 백업 계획을 사용하여 백업 요구 사항을 정의한 다음 사용하는 AWS 서비스 전반에서 보호하려는 AWS 리소스에 적용할 수 있습니다. 특정 비즈니스 및 규정 준수 요건을 충족하는 별도의 백업 계획을 생성할 수 있습니다. 이렇게 하면 요구 사항에 따라 각 AWS 리소스를 백업할 수 있습니다. 백업 계획을 사용하면 조직 및 애플리케이션 전반에 걸쳐 확장 가능한 방식으로 백업 전략을 쉽게 적용할 수 있습니다.

백업 계획의 모든 구성 옵션은 백업 계획 옵션 및 구성 섹션을 참조하세요.

태그 기반 백업 정책

를 사용하여 AWS Backup 리소스에 태그를 지정하는 등 다양한 방법으로 AWS 리소스에 백업 계획을 적용할 수 있습니다. 태그를 지정하면 모든 애플리케이션에서 백업 전략을 쉽게 구현하고 모든 AWS

리소스를 백업하고 보호할 수 있습니다. AWS 태그는 리소스를 구성하고 분류할 수 AWS 있는 좋은 방법입니다. AWS 태그와의 통합을 통해 백업 계획을 AWS 리소스 그룹에 신속하게 적용하여 일관되고 규정을 준수하는 방식으로 백업할 수 있습니다.

백업 계획에 리소스를 할당할 수 있는 모든 방법은 백업 계획에 리소스 할당 섹션을 참조하세요.

수명 주기 관리 정책

AWS Backup 백업을 저렴한 콜드 스토리지 계층에 저장하여 백업 스토리지 비용을 최소화하면서 규정 준수 요구 사항을 충족할 수 있습니다. 정의한 일정에 따라 백업을 웜 스토리지에서 콜드 스토리지로 자동 전환하도록 수명 주기 정책을 구성할 수 있습니다.

콜드 스토리지로 전환할 수 있는 리소스 목록은 리소스별 기능 가용성 섹션을 참조하세요. 백업 계획에서 콜드 스토리지를 활성화하는 단계는 수명 주기 및 스토리지 계층을 참조하십시오.

교차 리전 백업

를 사용하면 AWS Backup필요에 AWS 리전 따라 백업을 여러 다른 곳에 복사하거나 예약된 백업 계획의 일부로 자동으로 복사할 수 있습니다. 교차 리전 백업은 프로덕션 데이터로부터 최소 거리에 백업을 저장해야 하는 비즈니스 연속성 또는 규정 준수 요구 사항이 있는 경우 특히 유용합니다. 자세한 내용은 AWS 리전에서 백업 복사본 생성 섹션을 참조하세요.

교차 계정 관리 및 교차 계정 백업

를 AWS Backup 사용하여 AWS Organizations구조 AWS 계정 내 모든 항목의 백업을 관리할 수 있습니다. 교차 계정 관리를 사용하면, 백업 정책을 사용하여 조직 내의 AWS 계정 전체에 걸쳐 백업 계획을 자동으로 적용할 수 있습니다. 따라서 규정 준수 및 데이터 보호를 대규모로 효율적으로 수행할 수 있으며 운영 오버헤드를 줄일 수 있습니다. 또한 개별 계정 간에 백업 계획을 수동으로 복제하지 않아도 됩니다. 자세한 내용은 여러 AWS 계정에서 AWS Backup 리소스 관리 섹션을 참조하세요.

또한 AWS Organizations 관리 구조 AWS 계정 내의 여러 다른 위치에 백업을 복사할 수 있습니다. 이렇게 하면 백업을 단일 리포지토리 계정으로 "팬인"한 다음, 백업을 "팬아웃"하여 복원력을 높일 수 있습니다. AWS 계정간 백업 복사본 생성 섹션을 참조하세요.

교차 계정 관리 기능을 사용하려면 우선 AWS Organizations에 구성된 기존 조직 구조가 있어야 합니다. 조직 구성 단위 (OU) 는 단일 엔티티로 관리할 수 있는 계정 그룹입니다. AWS Organizations 조직 단위로 그룹화하고 단일 엔티티로 관리할 수 있는 계정 목록입니다.

Audit Manager를 통한 AWS Backup 감사 및 보고

AWS Backup Audit Manager를 사용하면 전체 백업의 데이터 거버넌스 및 규정 준수 관리를 단순화할 수 AWS있습니다. AWS Backup Audit Manager는 조직의 요구 사항에 맞게 조정할 수 있는 사용자 지정 가능한 기본 제공 제어 기능을 제공합니다. 또한 이러한 컨트롤을 사용하여 백업 작업 및 리소스를 자동으로 추적할 수 있습니다.

AWS Backup Audit Manager는 정의한 제어를 아직 준수하지 않는 특정 활동 및 리소스를 찾는 데 도움을 줄 수 있습니다. 또한 일정 기간 동안 컨트롤을 준수했다는 걸 보여주는 증거 역할을 하는 일일 보고서를 생성할 수 있습니다.

전체 규정 준수 태세와 함께 백업 규정 준수를 포함하려면 AWS Backup Audit Manager 결과를 로 자동으로 가져올 수 AWS Audit Manager있습니다.

증분 백업

AWS Backup 주기적인 백업을 점진적으로 효율적으로 저장합니다. AWS 리소스의 첫 번째 백업은 데이터의 전체 복사본을 백업합니다. 연속되는 각 증분 백업의 경우 AWS 리소스의 변경 사항만 백업됩니다. 증분 백업을 사용하면 스토리지 비용을 최소화하면서 백업을 자주 실행하여 데이터를 보호하는 이점을 누릴 수 있습니다.

증분 백업을 지원하는 리소스 목록은 리소스별 기능 가용성 섹션을 참조하세요.

전체 관리 AWS Backup

일부 리소스 유형은 전체 AWS Backup 관리를 지원합니다. 전체 AWS Backup 관리의 이점은 다음과 같습니다.

- 독립적 암호화. AWS Backup 소스 리소스와 동일한 암호화 키를 사용하는 대신 AWS Backup 볼트의 KMS 키를 사용하여 백업을 자동으로 암호화합니다. 이렇게 하면 방어 계층이 강화됩니다. 자세한 정보는 내 백업을 위한 암호화 AWS Backup을 참조하세요.
- **awsbackup** Amazon Resource 이름(ARN). 백업 ARN은 `arn:aws:source-resource` 대신 `arn:aws:backup`으로 시작합니다. 이렇게 하면 소스 리소스가 아닌 백업에만 적용되는 액세스 정책을 생성할 수 있습니다. 자세한 정보는 액세스 제어을 참조하세요.
- 중앙 집중식 백업 청구 및 Cost Explorer 비용 할당 태그. 스토리지, 데이터 전송, 복원, 조기 삭제 등을 포함한 요금은 AWS Backup 지원되는 각 리소스에 표시되지 않고 Amazon Web Services 청구서의 “Backup”에 표시됩니다. 또한 Cost Explorer 비용 할당 태그를 사용하여 백업 비용을 추적하고 최적화할 수 있습니다. 자세한 정보는 측정, 비용 및 청구을 참조하세요.

전체 AWS Backup 관리에 적합한 리소스 유형을 확인하려면 을 참조하십시오리소스별 기능 가용성.

백업 활동 모니터링

AWS Backup AWS 서비스 전반의 백업 및 복원 활동을 간단하게 감사할 수 있는 대시보드를 제공합니다. AWS Backup 콘솔에서 몇 번만 클릭하면 최근 백업 작업의 상태를 볼 수 있습니다. 또한 여러 AWS 서비스에서 작업을 복원하여 AWS 리소스가 적절하게 보호되도록 할 수 있습니다.

AWS Backup 아마존 CloudWatch 및 EventBridge 아마존과 통합됩니다. CloudWatch 지표를 추적하고 경보를 생성할 수 있습니다. EventBridge AWS Backup 이벤트를 보고 모니터링할 수 있습니다. 자세한 내용은 를 사용하여 AWS Backup 이벤트 모니터링 EventBridge 및 AWS Backup 메트릭 모니터링을 참조하십시오 CloudWatch.

AWS Backup 와 통합됩니다. AWS CloudTrail CloudTrail 백업 작업 로그의 통합 보기를 제공하므로 리소스가 백업되는 방식을 빠르고 쉽게 감사할 수 있습니다. AWS Backup 또한 Amazon Simple Notification Service (Amazon SNS) 와 통합되어 백업이 성공하거나 복원이 시작된 시기와 같은 백업 활동 알림을 제공합니다. 자세한 내용은 Amazon SNS를 통한 AWS Backup API 호출 로깅 CloudTrail 및 Amazon SNS를 사용하여 AWS Backup 이벤트 추적을 참조하십시오.

백업 저장소의 데이터 보호

각 AWS Backup 백업의 콘텐츠는 변경할 수 없습니다. 즉, 아무도 해당 콘텐츠를 변경할 수 없습니다. AWS Backup 백업 저장소의 백업 보안을 더욱 강화하여 백업본을 원본 인스턴스와 안전하게 분리합니다. 예를 들어, 원본 Amazon EC2 인스턴스와 Amazon EBS 볼륨을 삭제하더라도 사용자가 선택한 수명 주기 정책에 따라 저장소에 Amazon EC2 및 Amazon EBS 백업이 보존됩니다.

백업 저장소는 백업에 대한 액세스 권한이 있는 사용자를 정의할 수 있는 암호화 및 리소스 기반 액세스 정책을 제공합니다. 백업 저장소에 대해 저장소 내의 백업에 대한 액세스 권한이 있는 사용자 및 사용자가 수행할 수 있는 작업을 정의하는 액세스 정책을 정의할 수 있습니다. 이를 통해 서비스 전반에서 백업에 대한 액세스를 간단하고 안전하게 제어할 수 있습니다. AWS 고객 관리형 정책을 AWS 검토하고 이에 대한 AWS Backup내용은 관리형 정책을 참조하십시오 AWS Backup.

AWS Backup Vault Lock을 사용하여 본인을 포함한 다른 사람이 백업을 삭제하거나 보존 기간을 변경하지 못하도록 할 수 있습니다. AWS Backup Vault Lock을 사용하면 write-once-read-many(WORM) 모델을 적용하고 심층 방어를 위한 또 다른 계층을 추가할 수 있습니다. 시작하려면 AWS Backup 보관소 잠금 섹션을 참조하세요.

규정 준수 의무 지원

AWS Backup 글로벌 규정 준수 의무를 충족하는 데 도움이 됩니다. AWS Backup 는 다음 AWS 규정 준수 프로그램의 범위에 속합니다.

- FedRAMP High
- GDPR
- SOC 1, 2, 3
- PCI
- HIPAA
- 그 외의 많은 기능

시작하기

에 대해 AWS Backup자세히 알아보려면 부터 시작하는 것이 좋습니다시작하기 AWS Backup.

지원되는 AWS 리소스 및 애플리케이션

다음은 백업 및 복원을 사용하여 사용할 수 있는 AWS 리소스 및 타사 AWS Backup애플리케이션입니다. 자세한 정보는 the section called “기능 가용성”을 참조하세요.

Service	지원되는 리소스 유형
Amazon Elastic Compute Cloud(Amazon EC2)	Amazon EC2 인스턴스(인스턴스 스토어 지원 AMI 제외)
Amazon Simple Storage Service(S3)	Amazon S3 데이터
Amazon Elastic Block Store(Amazon EBS)	Amazon EBS 볼륨
Amazon DynamoDB	Amazon DynamoDB 테이블
Amazon Relational Database Service(RDS)	Amazon RDS 데이터베이스 인스턴스(모든 데이터베이스 엔진 포함), 다중 가용 영역 클러스터

Service	지원되는 리소스 유형
Amazon Aurora	Aurora DB 클러스터
Amazon Elastic File System(Amazon EFS)	Amazon EFS 파일 시스템
FSx for Lustre	FSx for Lustre 파일 시스템
FSx for Windows File Server	FSx for Windows File Server 파일 시스템
ONTAP용 아마존 NetApp FSx	FSx for ONTAP 파일 시스템
Amazon FSx for OpenZFS	FSx for OpenZFS 파일 시스템
AWS Storage Gateway (볼륨 게이트웨이)	AWS Storage Gateway 볼륨
Amazon DocumentDB	아마존 DocumentDB 인스턴스 기반 클러스터
Amazon Neptune	Amazon Neptune 클러스터
Amazon Redshift	Amazon Redshift 클러스터
Amazon Timestream	Amazon Timestream 테이블
VMware 클라우드™ 켜기 AWS	VMware Cloud™ 가상 머신이 켜져 있습니다 AWS
VMware 클라우드™ 켜기 AWS Outposts	VMware Cloud™ 가상 머신이 켜져 있습니다 AWS Outposts
AWS CloudFormation	AWS CloudFormation 스택
SAP HANA 데이터베이스	Amazon EC2 인스턴스의 SAP HANA 데이터베이스

요금

를 사용하면 백업 스토리지 AWS Backup, 데이터 복원, 복원 테스트, 지역 간 데이터 전송, AWS Backup Audit Manager에 대한 비용을 지불합니다. 자세한 내용은 AWS Backup 요금을 참조하세요.

AWS Backup 기능 사용 가능 여부

AWS Backup 기능은 리소스 및 리소스에 따라 제공됩니다 AWS 리전. 아래의 섹션 및 표는 기능 가용성을 확인하는 데 도움이 될 수 있습니다.

내용

지원되는 모든 리소스에 사용할 수 있는 기능

AWS Backup 지원되는 AWS 서비스 및 지원되는 타사 응용 프로그램에 대해 다음과 같은 기능을 제공합니다. 명시적으로 언급되지 않는 한 기능 또는 서비스에 대한 지원이 제공된다고 가정할 수 없습니다.

- 자동 백업 일정 및 보존 관리
- 중앙 집중식 백업 모니터링
- 암호화된 백업
- 증분 백업
- 다음과 같은 교차 계정 관리 AWS Organizations
- Audit Manager를 통한 자동 백업 AWS Backup 감사 및 보고서
- 볼트 잠금을 통한 한 번의 쓰기, 여러 번 읽기 (WORM) AWS Backup

리소스별 기능 가용성

특정 지역에서 지원되는 AWS 서비스와 AWS Backup 함께 사용하려면 해당 지역에서 서비스를 사용할 수 있어야 합니다. 지역의 서비스 가용성을 확인하려면 에서 서비스 엔드포인트를 확인하십시오. AWS 일반 참조

AWS Backup 지원	교차 리전 백업	교차 계정 백업	AWS Backup Audit Manager	증분 백업	지속적인 백업 및 point-in-time 복원	전체 관리	콜드 스토리지까지의 수명 주기	항목 수준 복원 [1]	복원 테스트
Amazon EC2	✓	✓	✓	✓					✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
아마존 RDS 단일 인스턴스	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Amazon RDS 클러스터	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx for Lustre	✓	✓	✓	✓					✓
FSx for	✓	✓	✓	✓					✓

AWS Backup 지원	교차 리전 백업	교차 계정 백업	AWS Backup Audit Manager	증분 백업	지속적인 백업 및 point-in-time 복원	전체 관리	콜드 스토리지까지의 수명 주기	항목 수준 복원 [1]	복원 테스트
Windows File Server									
OnTAP 용 FSx			✓ [2]	✓					✓
FSx OpenZF 용 FSx	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon Docume B	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon Redshift								✓	
Timestre m	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					

AWS Backup 지원	교차 리전 백업	교차 계정 백업	AWS Backup Audit Manager	증분 백업	지속적인 백업 및 point-in-time 복원	전체 관리	콜드 스토리지까지의 수명 주기	항목 수준 복원 [1]	복원 테스트
가상 머신	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation 템플릿	✓	✓		✓ [5]		✓	✓ [5]		
Amazon DynamoDB			✓						✓
AWS Backup 고급 기능이 있는 DynamoDB	✓	✓	✓			✓	✓		✓
Amazon EC2 인스턴스의 SAP HANA 데이터베이스				✓	✓	✓	✓		

일부 리소스 유형에는 연속 백업 기능과 교차 리전 복사 및 교차 계정 복사를 모두 사용할 수 있습니다. 연속 백업의 교차 리전 또는 교차 계정 복사본을 생성하면 복사된 복구 시점(백업)은 스냅샷(정기) 백업

이 됩니다. Amazon RDS와 Amazon S3는 증분 스냅샷 복사를 지원하지만 Amazon Aurora는 전체 스냅샷 복사만 지원합니다. 이러한 복사본에는 PITR(시점 복원)을 사용할 수 없습니다.

[1] 항목 수준 복원의 "항목"은 지원되는 리소스에 따라 다릅니다. 예를 들어 파일 시스템 항목은 파일 또는 디렉터리인 반면, S3 항목은 S3 객체입니다. VMware 항목은 디스크입니다. 자세한 내용은 지원되는 리소스의 백업 복원 섹션을 참조하세요.

[2] AWS Backup Audit Manager는 계정 간 복사 및 지역 간 복사를 제외한 모든 제어에서 이 리소스를 지원합니다.

[3] RDS, Aurora, DocumentDB 및 Neptune은 리전 간 백업과 계정 간 백업을 모두 수행하는 단일 복사 작업을 지원하지 않습니다. 둘 중 하나만 선택할 수 있습니다. AWS Lambda 스크립트를 사용하여 첫 번째 복사가 완료될 때까지 수신하고, 두 번째 복사를 수행한 다음, 첫 번째 사본을 삭제할 수도 있습니다. RDS 다중 가용 영역(다중 AZ) 데이터베이스 인스턴스는 복사할 수 있지만, 현재 다중 AZ 클러스터는 교차 리전 또는 교차 계정 복사를 지원하지 않습니다. 자세한 내용은 특정 리소스를 사용한 지역 간 복사 고려 사항 을 참조하십시오.

[4] Backup Audit Manager 지원이 제공되는 지역의 RDS 다중 가용 영역 백업을 참조하십시오.

[5] CloudFormation 스택 백업에서 중첩된 리소스는 소스 리소스의 기능을 유지합니다. 하지만 스택 내의 리소스는 지정 시간 복원 (PITR) 기능 (예: Amazon S3 및 Amazon RDS) 을 유지하지 않습니다. 위 매트릭스 내의 속성은 CloudFormation 템플릿에만 적용되며 스택 내 리소스에는 적용되지 않습니다.

[6] Aurora의 경우 스냅샷이 가득 차며 PITR을 통해 증분 백업이 제공됩니다.

기능 가용성은 다음과 같습니다. AWS 리전

AWS Backup 다음 모두에서 사용할 수 있습니다 AWS 리전. AWS Backup 다음 표에 달리 명시되지 않는 한 이 모든 지역에서 기능을 사용할 수 있습니다.

AWS Backup 지원	교차 리전 백업	교차 계정 관리	교차 계정 백업	AWS Backup Audit Manager 및 작업 대시보드	복원 테스트
미국 동부(버지니아 북부)	✓	✓	✓	✓	✓

AWS Backup 지원	교차 리전 백업	교차 계정 관리	교차 계정 백업	AWS Backup Audit Manager 및 작업 대시보드	복원 테스트
미국 동부(오하이오)	✓	✓	✓	✓	✓
미국 서부(캘리포니아 북부)	✓	✓	✓	✓	✓
미국 서부(오레곤)	✓	✓	✓	✓	✓
아프리카(케이프타운)	✓		✓	✓	✓
아시아 태평양(홍콩)	✓		✓	✓	✓
아시아 태평양(하이데라바드)	✓		✓		✓
아시아 태평양(자카르타)	✓		✓		✓
아시아 태평양(멜버른)	✓		✓		✓
아시아 태평양(뭄바이)	✓	✓	✓	✓	✓
아시아 태평양(오사카)	✓	✓	✓		✓

AWS Backup 지원	교차 리전 백업	교차 계정 관리	교차 계정 백업	AWS Backup Audit Manager 및 작업 대시보드	복원 테스트
아시아 태평양(서울)	✓	✓	✓	✓	✓
아시아 태평양(싱가포르)	✓	✓	✓	✓	✓
아시아 태평양(시드니)	✓	✓	✓	✓	✓
아시아 태평양(도쿄)	✓	✓	✓	✓	✓
캐나다(중부)	✓	✓	✓	✓	✓
캐나다 서부(캘거리)	✓ (아마존 S3 제외)		✓		
중국(베이징)	✓				
중국(닝샤)	✓				
유럽(프랑크푸르트)	✓	✓	✓	✓	✓
유럽(아일랜드)	✓	✓	✓	✓	✓
유럽(런던)	✓	✓	✓	✓	✓
유럽(밀라노)	✓		✓	✓	✓
유럽(파리)	✓	✓	✓	✓	✓
유럽(스페인)	✓		✓		✓

AWS Backup 지원	교차 리전 백업	교차 계정 관리	교차 계정 백업	AWS Backup Audit Manager 및 작업 대시보드	복원 테스트
유럽(스톡홀름)	✓	✓	✓	✓	✓
유럽(취리히)	✓		✓		✓
이스라엘(텔아비브)	✓		✓		
중동(바레인)	✓		✓	✓	✓
중동(UAE)	✓		✓		✓
남아메리카(상파울루)	✓	✓	✓	✓	✓
AWS GovCloud (미국 동부)	✓	✓	✓	✓	
AWS GovCloud (미국 서부)	✓	✓	✓	✓	

중국(베이징) 및 중국(닝샤)은 이러한 두 가지 리전 중 한 곳에서 다른 리전으로 교차 리전 복사를 지원합니다. 이러한 리전에서 다른 리전으로 또는 이러한 리전으로 교차 리전 복사는 지원되지 않습니다. 이러한 리전에서 교차 계정 복사는 지원되지 않습니다.

AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서는 채용 정보 대시보드를 사용할 수 없습니다. 작업 대시보드 집계는 교차 계정 관리 및 AWS Backup Audit Manager를 지원하는 지역에서만 사용할 수 있습니다.

Windows File Server용 Amazon FSx 및 Amazon Neptune은 옵트인 지역의 지역 간 백업 사본을 지원하지 않습니다.

지원되는 서비스는 다음과 같습니다. AWS 리전

AWS Backup 지원되는 모든 지역에서 다음을 지원합니다.

- Aurora
- DynamoDB
- 고급 기능을 갖춘 DynamoDB AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

다음 표는 AWS 서비스 지역별 기타에 대한 AWS Backup 지원을 나타냅니다.

리전 및 서비스	Amazon FSx	EC2 인스턴스의 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 및 백업 게이트웨이
미국 동부(버지니아 북부)	✓	✓	✓	✓	✓	✓
미국 동부(오하이오)	✓	✓	✓	✓	✓	✓
미국 서부(캘리포니아 북부)	Windows, Lustre, ONTAP	✓	✓	✓		✓
미국 서부(오레곤)	Windows, Lustre, ONTAP	✓	✓	✓	✓	✓

리전 및 서비스	Amazon FSx	EC2 인스턴스의 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 및 백업 게이트웨이
아프리카(케이프타운)	Windows, Lustre, ONTAP	✓	✓ [1]	✓		✓
아시아 태평양(홍콩)	✓	✓	✓ [1]	✓		✓
아시아 태평양(하이데라바드)	Windows, Lustre, ONTAP		✓ [1]	✓		
아시아 태평양(자카르타)	Windows, Lustre, ONTAP		✓	✓		
아시아 태평양(멜버른)	Windows, Lustre, ONTAP		✓ [1]	✓		
아시아 태평양(뭄바이)	✓	✓	✓	✓		✓
아시아 태평양(오사카)	Windows, Lustre	✓	✓ [1]	✓		✓
아시아 태평양(서울)	✓	✓	✓	✓		✓
아시아 태평양(싱가포르)	✓	✓	✓	✓		✓

리전 및 서비스	Amazon FSx	EC2 인스턴스의 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 및 백업 게이트웨이
아시아 태평양(시드니)	✓	✓	✓	✓	✓	✓
아시아 태평양(도쿄)	✓	✓	✓	✓	✓	✓
캐나다(중부)	✓	✓	✓	✓		✓
캐나다 서부(캘거리)						
중국(베이징)	Windows, Lustre		✓ [1]	✓	✓	
중국(닝샤)	Windows, Lustre		✓ [1]	✓	✓	
유럽(프랑크푸르트)	✓	✓	✓	✓	✓	✓
유럽(아일랜드)	✓	✓	✓	✓	✓	✓
유럽(런던)	✓	✓	✓	✓		✓
유럽(밀라노)	Windows, Lustre, ONTAP	✓	✓ [1]	✓		✓
유럽(파리)	Windows, Lustre, ONTAP	✓	✓	✓		✓

리전 및 서비스	Amazon FSx	EC2 인스턴스의 SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware 및 백업 게이트웨이
유럽(스페인)	Windows, Lustre, ONTAP		✓ [1]	✓		
유럽(스톡홀름)	✓	✓	✓	✓		✓
유럽(취리히)	Windows, Lustre, ONTAP		✓ [1]	✓		
이스라엘(텔아비브)	Windows, Lustre, ONTAP		✓ [1]	✓		
중동(바레인)	Windows, Lustre, ONTAP	✓	✓ [1]	✓		✓
중동(UAE)			✓ [1]	✓		
남아메리카(상파울루)		✓	✓	✓		✓
AWS GovCloud(미국 서부)	Windows, Lustre, ONTAP		✓ [1]	✓		✓
AWS GovCloud(미국 동부)	Windows, Lustre, ONTAP		✓ [1]	✓		✓

Amazon FSx에서 확인하면 Windows File Server용 FSx, Lustre용 FSx, ONTAP용 FSx 및 OpenZFS용 FSX가 모두 해당 지역에서 지원되며, 그렇지 않으면 지원되는 구성이 나열됩니다. AWS Backup

[1] 지역 간 및 계정 간 복사는 지원되지 않습니다.

AWS Backup: 작동 방식

AWS Backup 서비스 AWS 전반의 데이터 백업을 쉽게 중앙 집중화하고 자동화할 수 있는 완전 관리형 백업 서비스입니다. 를 사용하여 AWS Backup백업 계획이라는 백업 정책을 만들 수 있습니다. 이러한 계획을 사용하여 데이터 백업 빈도 및 백업 보존 기간과 같은 백업 요구 사항을 정의할 수 있습니다.

AWS Backup 리소스에 태그를 지정하기만 하면 AWS 리소스에 백업 계획을 적용할 수 있습니다. AWS Backup 그런 다음 정의한 백업 계획에 따라 AWS 리소스를 자동으로 백업합니다.

다음 섹션에서는 AWS Backup 작동 방식, 구현 세부 정보 및 보안 고려 사항에 대해 설명합니다.

주제

- 지원되는 AWS 서비스와의 AWS Backup 작동 방식
- 측정, 비용 및 청구
- AWS Backup 블로그, 동영상, 자습서 및 기타 리소스

지원되는 AWS 서비스와의 AWS Backup 작동 방식

AWS Backup지원되는 일부 AWS 서비스는 자체 독립 실행형 백업 기능을 제공합니다. 이러한 기능은 AWS Backup사용 여부와 관계없이 사용할 수 있습니다. 하지만 다른 AWS 서비스에서 만든 백업은 중앙 거버넌스에 사용할 수 없습니다. AWS Backup

지원되는 모든 서비스에 대한 데이터 보호를 중앙에서 AWS Backup 관리하도록 구성하려면 해당 서비스를 관리하도록 선택하고, 온디맨드 백업을 생성하거나 AWS Backup, 백업 계획을 사용하여 백업을 예약하고, 백업을 백업 저장소에 저장해야 합니다.

주제

- 다음과 같은 관리 서비스에 옵트인하십시오. AWS Backup
- Amazon S3 데이터 작업
- VMware 가상 머신 작업
- Amazon DynamoDB 작업
- Amazon FSx 파일 시스템 작업
- Amazon EC2 작업
- Amazon EFS 작업
- Amazon EBS 작업

- Amazon RDS 및 Aurora 작업
- 사용 방법: AWS BackInt
- 다음과 함께 작업하기 AWS Storage Gateway
- Amazon DocumentDB 작업
- Amazon Neptune 작업
- Amazon Timestream 작업
- 다음과 같이 작업하기 AWS Organizations
- 다음과 같이 작업하기 AWS CloudFormation
- SAP 및 SAP HANA와 함께 AWS BackInt 작업하기 AWS Systems Manager
- AWS 서비스가 자체 리소스를 백업하는 방법

다음과 같은 관리 서비스에 옵트인하십시오. AWS Backup

새 AWS 서비스를 사용할 수 있게 되면 해당 서비스를 사용할 수 AWS Backup 있도록 설정해야 합니다. 활성화되지 않은 서비스의 리소스를 사용하여 온디맨드 백업 또는 백업 계획을 생성하려고 하면 오류 메시지가 나타나고 프로세스를 완료할 수 없습니다.

AWS Backup 콘솔에서는 백업 계획에 리소스 유형을 포함하는 두 가지 방법이 있습니다. 즉, 백업 계획에 리소스 유형을 명시적으로 할당하거나 모든 리소스를 포함하는 것입니다. 이러한 선택 항목이 서비스 옵트인과 어떻게 작동하는지 이해하려면 아래 내용을 참조하세요.

- 태그만 기준으로 하여 리소스를 할당할 경우 서비스 옵트인 설정이 적용됩니다.
- 리소스 유형을 백업 계획에 명시적으로 할당하면 해당 특정 서비스에 대해 옵트인이 활성화되지 않은 경우에도 백업에 포함됩니다. Aurora, Neptune 및 Amazon DocumentDB에는 적용되지 않습니다. 이러한 서비스를 포함하려면 옵트인을 활성화해야 합니다.
- 리소스 배정에 리소스 유형과 태그가 모두 지정된 경우 지정된 리소스 유형이 먼저 필터링된 다음 태그가 해당 리소스를 추가로 필터링합니다.

  서비스 옵트인 설정은 대부분의 리소스 유형에서 무시됩니다. 하지만 Aurora, Neptune 및 Amazon DocumentDB에는 서비스 옵트인이 필요합니다.
- Amazon FSx NetApp for ONTAP의 경우, 태그 기반 리소스 선택을 사용하는 경우 전체 파일 시스템 대신 개별 볼륨에 태그를 적용합니다.

서비스 옵트인 설정은 지역별로 다릅니다. 계정이 지역에서 사용 AWS Backup (백업 저장소 또는 백업 계획 생성) 하는 경우, 해당 계정은 해당 시점에 해당 지역에서 지원되는 모든 리소스 유형에 자동으로

옵트인됩니다. AWS Backup 나중에 해당 지역에 추가된 지원 서비스는 백업 계획에 자동으로 포함되지 않습니다. 이러한 리소스 유형이 지원되면 해당 유형을 선택하도록 선택할 수 있습니다.

에서 사용하는 서비스를 구성하려면 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 서비스 옵트인 페이지에서 리소스 구성을 선택합니다.
4. 토글 스위치를 사용하여 에서 사용하는 서비스를 활성화하거나 비활성화할 AWS Backup수 있습니다.

   > **Important**
   >
   > RDS, Aurora, Nepune, DocumentDB는 동일한 Amazon 리소스 이름(ARN)을 공유합니다. 이러한 리소스 유형 중 하나를 관리하도록 선택하면 백업 계획에 할당할 때 모든 리소스에 AWS Backup 옵트인합니다. 그와 상관없이, 옵트인 상태를 정확하게 나타내려면 모두 옵트인하는 것이 좋습니다.

5. 확인을 선택합니다.

Amazon S3 데이터 작업

AWS Backup Amazon S3 백업을 위한 완전 관리형 백업 및 복원을 제공합니다. 자세한 내용은 Amazon S3 버킷 섹션을 참조하세요.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- AWS Backup다음을 사용하여 Amazon S3 데이터를 복원하는 방법 S3 데이터 복원

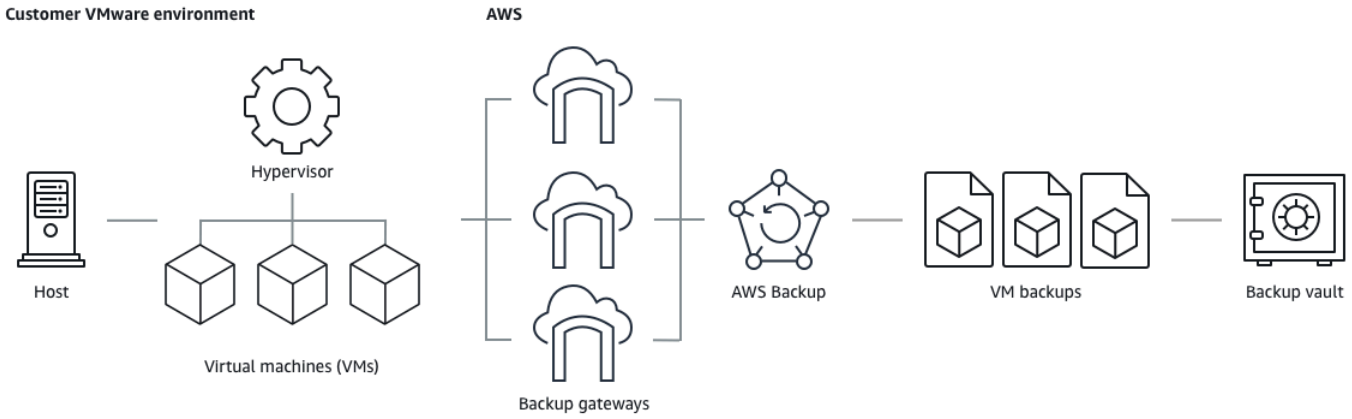
S3 데이터에 대한 자세한 내용은 Amazon S3 설명서를 참조하세요.

VMware 가상 머신 작업

AWS Backup VMware Cloud™ (VMC) 의 VM과 함께 온프레미스 VMware 가상 머신 (VM) 에 대한 중앙 집중식 및 자동 데이터 보호를 지원합니다. AWS온프레미스 및 VMC 가상 시스템에서 로 백업할 수 있습니다. AWS Backup그런 다음 온프레미스 또는 VMC에서 AWS Backup 복원할 수 있습니다.

백업 게이트웨이는 VMware VM에 배포하여 VMware VM을 연결하는 다운로드 가능한 AWS Backup 소프트웨어입니다. AWS Backup이 게이트웨이는 VM을 검색하기 위해 VM 관리 서버에 연결하고, VM

을 검색하고, 데이터를 암호화하고, 데이터를 AWS Backup에 효율적으로 전송합니다. 다음 다이어그램에서는 Backup 게이트웨이가 VM에 연결되는 방식을 보여 줍니다.



- 리소스를 백업하는 방법: 가상 머신 백업
- VM 리소스를 복원하는 방법: 다음을 사용하여 가상 시스템을 복원합니다. AWS Backup

Amazon DynamoDB 작업

AWS Backup Amazon DynamoDB 테이블 백업 및 복원을 지원합니다. DynamoDB는 완전 관리형 NoSQL 데이터베이스 서비스로서 원활한 확장성과 함께 빠르고 예측 가능한 성능을 제공합니다.

출시 이후 항상 DynamoDB를 지원해 AWS Backup 왔습니다. 2021년 11월부터 DynamoDB 백업을 위한 고급 AWS Backup 기능도 도입되었습니다. 이러한 고급 기능에는 계정 간 AWS 리전 백업 복사, 콜드 스토리지로의 백업 계층화, 권한 및 비용 관리를 위한 태그 사용 등이 포함됩니다.

2021년 11월 이후에 온보딩하는 신규 AWS Backup 고객은 고급 DynamoDB 백업 기능이 기본적으로 활성화됩니다.

모든 기존 AWS Backup 고객이 DynamoDB의 고급 기능을 활성화하는 것이 좋습니다. 고급 기능을 활성화한 후에는 원 백업 스토리지 요금에 차이가 없으며, 백업을 콜드 스토리지로 계층화하여 비용을 절감하고 비용 할당 태그를 사용하여 비용을 최적화할 수 있습니다.

고급 기능의 전체 목록 및 이를 활성화하는 방법은 고급 DynamoDB 백업 섹션을 참조하세요.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- DynamoDB 리소스를 복원하는 방법: Amazon DynamoDB 테이블 복원

DynamoDB에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 Amazon DynamoDB란 무엇인가요?를 참조하세요.

Amazon FSx 파일 시스템 작업

AWS Backup Amazon FSx 파일 시스템의 백업 및 복원을 지원합니다. Amazon FSx는 워크로드에 대한 기본 호환성 및 기능 세트를 갖춘 완전 관리형 타사 파일 시스템을 제공합니다. AWS Backup Amazon FSx의 내장된 백업 기능을 사용합니다. 따라서 AWS Backup 콘솔에서 생성한 백업은 Amazon FSx 콘솔로 생성한 백업과 동일한 수준의 파일 시스템 일관성과 성능, 동일한 복원 옵션을 제공합니다.

를 AWS Backup 사용하여 이러한 백업을 관리하면 무제한 보존 옵션, 한 시간마다 예약 백업을 생성할 수 있는 기능과 같은 추가 기능을 이용할 수 있습니다. 또한 소스 파일 시스템이 삭제된 후에도 백업을 AWS Backup 보존합니다. 이렇게 하면 실수로 삭제되거나 악의적으로 삭제되는 것을 방지할 수 있습니다.

다른 서비스에 대한 지원도 AWS Backup 확장하는 중앙 백업 콘솔에서 백업 정책을 구성하고 백업 작업을 모니터링하려는 경우 Amazon FSx 파일 시스템을 보호하는 데 사용합니다. AWS

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon FSx 리소스를 복원하는 방법: FSX 파일 시스템 복원

Amazon FSx 파일 시스템에 대한 자세한 내용은 Amazon FSx 설명서를 참조하세요.

Amazon EC2 작업

AWS Backup Amazon EC2 인스턴스를 지원합니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon EC2 리소스를 복원하는 방법: Amazon EC2 인스턴스 복원

Amazon EBS 볼륨을 포함한 전체 EC2 인스턴스를 포함하는 온디맨드 백업 작업을 예약하거나 수행할 수 있습니다. 따라서 단일 복구 지점에서 루트 볼륨, 데이터 볼륨, 일부 인스턴스 구성 설정 (예: 인스턴스 유형 및 키 쌍) 을 포함한 전체 Amazon EC2 인스턴스를 복원할 수 있습니다.

VSS 지원 Microsoft Windows 애플리케이션을 백업 및 복원할 수도 있습니다. 온디맨드 백업 또는 예약 백업 계획의 일환으로 애플리케이션에 일관되게 적용되는 백업을 예약하고, 수명 주기 정책을 정의하고, 일관된 복원을 수행할 수 있습니다. 자세한 정보는 Windows VSS 백업 생성을 참조하세요.

AWS Backup 언제든지 EC2 인스턴스를 재부팅하지 않습니다.

이미지 및 스냅샷

Amazon EC2 인스턴스를 백업할 때 루트 Amazon EBS 스토리지 볼륨 AWS Backup , 시작 구성 및 모든 관련 EBS 볼륨의 스냅샷을 찍습니다. AWS Backup 인스턴스 유형, 보안 그룹, Amazon VPC, 모니터링 구성, 태그 등 EC2 인스턴스의 특정 구성 파라미터를 저장합니다. 백업 데이터는 Amazon EBS 볼륨 기반 Amazon Machine Image(AMI)로 저장됩니다.

Amazon EC2 휴지통이 구성되어 AWS Backup 있고 에서 관리하는 Amazon 머신 이미지 (AMI) 또는 Amazon EBS 스냅샷을 삭제하는 경우 Amazon EC2 휴지통 정책에 따라 이미지 또는 스냅샷에 요금이 부과될 수 있습니다. AWS Backup Amazon EC2 휴지통에 있는 스냅샷과 이미지는 휴지통에서 복원할 경우 더 이상 정책에 AWS Backup AWS Backup 의해 관리되지 않으며 정책에 의해서도 관리되지 않습니다.

AWS Backup Amazon EBS 스냅샷 잠금이 적용된 관리형 Amazon EBS 스냅샷 및 관리형 AWS Backup Amazon EC2 AMI와 연결된 스냅샷은 스냅샷 잠금 기간이 백업 수명 주기를 초과하는 경우 복구 지점 수명 주기의 일부로 삭제되지 않을 수 있습니다. 대신 이 복구 시점의 상태는 `EXPIRED`가 됩니다. Amazon EBS 스냅샷 잠금을 먼저 제거하면 이러한 복구 시점을 수동으로 삭제할 수 있습니다.

AWS Backup Amazon EC2 백업과 관련된 EBS 스냅샷을 암호화할 수 있습니다. 이는 EBS 스냅샷을 암호화하는 방법과 비슷합니다. AWS Backup Amazon EC2 AMI의 스냅샷을 생성할 때 기본 EBS 볼륨에 적용된 것과 동일한 암호화를 사용하며, 원본 인스턴스의 구성 파라미터는 복원 메타데이터에 유지됩니다.

스냅샷은 볼륨에서 암호화를 가져오고 해당 스냅샷에도 동일한 암호화가 적용됩니다. 복사된 AMI의 EBS 스냅샷은 항상 암호화됩니다. 복사 중에 KMS 키를 지정하면 지정된 키가 적용됩니다. KMS 키를 지정하지 않으면 기본 KMS 키가 적용됩니다.

자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스 및 Amazon EBS 사용 설명서의 Amazon EBS 암호화를 참조하십시오.

Amazon EFS 작업

AWS Backup 아마존 Elastic File System (아마존 EFS) 을 지원합니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon EFS 리소스를 복원하는 방법: Amazon EFS 파일 시스템 복원

Amazon EFS 파일 시스템에 대한 자세한 내용은 Amazon Elastic 파일 시스템 사용 설명서의 What is Amazon Elastic File System? 섹션을 참조하세요.

Amazon EBS 작업

AWS Backup 아마존 엘라스틱 블록 스토어 (아마존 EBS) 볼륨을 지원합니다.

AWS Backup Amazon EBS 스냅샷 잠금이 적용된 관리형 Amazon EBS 스냅샷 및 관리형 AWS Backup Amazon EC2 AMI와 연결된 스냅샷은 스냅샷 잠금 기간이 백업 수명 주기를 초과하는 경우 복구 지점 수명 주기의 일부로 삭제되지 않을 수 있습니다. 대신 이 복구 시점의 상태는 EXPIRED가 됩니다. Amazon EBS 스냅샷 잠금을 먼저 제거하면 이러한 복구 시점을 수동으로 삭제할 수 있습니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon EBS 볼륨을 복원하는 방법: Amazon EBS 볼륨 복원

자세한 내용은 Amazon EBS 사용 설명서의 Amazon EBS 볼륨을 참조하십시오.

Amazon RDS 및 Aurora 작업

AWS Backup Amazon RDS 데이터베이스 엔진 및 Aurora 클러스터를 지원합니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon RDS 리소스를 복원하는 방법: RDS 데이터베이스 복원
- Aurora 클러스터를 복원하는 방법: Amazon Aurora 클러스터 복원

Amazon RDS에 대한 자세한 내용은 Amazon RDS 사용 설명서에서 Amazon Relational Database Service(RDS)란 무엇인가요? 섹션을 참조하세요.

Aurora에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora란 무엇인가요? 섹션을 참조하세요.

> **Note**
>
> Amazon RDS 콘솔에서 백업 작업을 시작할 경우, Aurora 클러스터 백업 작업과 충돌하여 Backup job expired before completion이라는 오류가 발생할 수 있습니다. 이러한 오류가 발생하면 AWS Backup에서 더 긴 백업 기간을 구성하세요.

> **Note**
>
> RDS Custom for SQL Server 및 RDS Custom for Oracle은 현재 AWS Backup에서 지원되지 않습니다.

> **Note**
>
> AWS Aurora에서 자동 백업을 활성화하고 Aurora 자동 백업의 보존 기간이 Aurora 스냅샷의 보존 기간보다 길면 백업 저장소에 저장된 Aurora 스냅샷에 대해서는 요금이 부과되지 않습니다. 스냅샷의 데이터베이스를 삭제하면 백업 저장소 내의 모든 스냅샷에 요금이 부과됩니다(실수로 또는 블루/그린 배포 중에 삭제될 수 있음).
> 스냅샷이 크고 삭제된 데이터베이스에서 자주 백업할 경우 상당한 스토리지 요금이 부과될 수 있습니다. AWS Backup 계산기로 이동하여 예상 AWS Backup 요금을 계산해 보세요.

사용 방법: AWS BackInt

AWS Backup AWS Backint와 함께 작동하여 Amazon EC2 인스턴스에서 SAP HANA 데이터베이스 백업 및 복원을 지원합니다.

- SAP HANA 리소스 백업 및 복원 지침: SAP HANA Amazon EC2 인스턴스 백업 및 복원
- AWS Backint 에이전트 설정 AWS : SAP HANA용 Backint 에이전트

다음과 함께 작업하기 AWS Storage Gateway

AWS Backup Storage Gateway 볼륨 게이트웨이를 지원합니다. Amazon EBS 스냅샷을 Storage Gateway 볼륨으로 복원할 수도 있습니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Storage Gateway 리소스를 복원하는 방법: Storage Gateway 볼륨 복원

Amazon DocumentDB 작업

AWS Backup Amazon DocumentDB 클러스터를 지원합니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup

- Amazon DocumentDB 리소스를 복원하는 방법:. DocumentDB 클러스터 복원

Amazon Neptune 작업

AWS Backup Amazon Neptune 클러스터를 지원합니다.

- 리소스를 백업하는 방법: 시작하기 AWS Backup
- Amazon Neptune 클러스터를 복원하는 방법: Neptune 클러스터 복원.

Amazon Timestream 작업

AWS Backup Amazon Timestream 테이블을 지원합니다.

- Timestream 테이블을 백업하는 방법.
- Timestream 테이블을 복원하는 방법.

다음과 같이 작업하기 AWS Organizations

AWS Backup 와 함께 AWS Organizations 작동하여 계정 간 모니터링 및 관리를 단순화합니다.

- 조직 내 관리 계정을 생성합니다.
- 교차 계정 관리를 켭니다.
- 위임된 관리자 계정을 지정하고 정책을 위임합니다.

다음과 같이 작업하기 AWS CloudFormation

AWS Backup 지원 AWS CloudFormation 템플릿 및 애플리케이션 스택

- AWS CloudFormation 스택 백업

SAP 및 SAP HANA와 함께 AWS BackInt 작업하기 AWS Systems Manager

AWS Backup SAP용 AWS BackInt SSM과 함께 또는 SSM과 함께 작동하여 SAP HANA 백업 및 복원 기능을 지원합니다.

- Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업

- AWS Systems Manager SAP용으로 시작하세요.
- AWS SAP HANA용 Backint 에이전트

AWS 서비스가 자체 리소스를 백업하는 방법

특정 AWS 서비스의 백업 및 복원 프로세스에 대한 기술 설명서를 참조할 수 있습니다. 특히 복원 중에 해당 AWS 서비스의 새 인스턴스를 구성해야 하는 경우에는 더욱 그렇습니다. 다음은 설명서 목록입니다.

- Amazon EC2 관련 서비스
- Amazon AWS Backup EFS와 함께 사용
- DynamoDB에 대한 온디맨드 백업 및 복원
- Amazon EBS 스냅샷
- Amazon RDS DB 인스턴스 백업 및 복원
  - Aurora DB 클러스터 백업 및 복원에 대한 개요
- Windows File Server용 AWS Backup FSx와 함께 사용
- FSx AWS Backup for Lustre와 함께 사용
- 에서 볼륨 백업 AWS Storage Gateway
- Amazon DocumentDB에서 백업 및 복원
- Amazon Neptune 클러스터 백업 및 복원

측정, 비용 및 청구

AWS Backup 가격

현재 AWS Backup 가격은 AWS Backup 가격에서 확인할 수 있습니다.

> **Important**
>
> 추가 요금이 부과되지 않도록 하려면 웜 스토리지 기간을 1주 이상으로 설정하도록 보존 정책을 구성하세요.
> 예를 들어 매일 백업을 생성하여 하루 동안 보관한다고 가정해 보겠습니다. 또한 보호되는 리소스가 너무 커서 백업을 완료하는 데 하루 종일 걸린다고 가정해 보겠습니다. AWS Backup 보존 기간을 하루로 구현하고 백업 작업이 완료되면 웜 스토리지에서 백업을 제거합니다. 다음

날에는 웜 AWS Backup 스토리지에 백업이 없기 때문에 증분 백업을 생성할 수 없습니다. 이 보존 기간은 모범 사례를 따르지 않았으므로, 매일 전체 백업을 생성하는 데 따르는 위험과 비용이 발생합니다.
추가 지원이 AWS Support 필요한 경우 문의하세요.

AWS Backup 청구

리소스 유형이 전체 AWS Backup 관리를 지원하는 경우 스토리지, 데이터 전송, 복원, 조기 삭제 등 AWS Backup 활동에 대한 요금이 Amazon Web Services 청구서의 “백업” 섹션에 표시됩니다. 전체 AWS Backup 관리를 지원하는 서비스 목록은 리소스별 기능 가용성 표의 전체 AWS Backup 관리 섹션을 참조하십시오.

리소스 유형이 전체 AWS Backup 관리를 지원하지 않는 경우 백업에 대한 스토리지 비용과 같은 일부 AWS Backup 활동에 대한 청구가 해당 AWS 서비스에 반영됩니다.

복사 작업 실패

대상 저장소에 복구 시점이 생성된 후에만 요금이 부과됩니다. 복사 작업에 실패하고 복구 시점이 생성되지 않은 경우에는 요금이 부과되지 않습니다.

비용 할당 태그

비용 할당 태그를 사용하여 세부 수준에서 AWS Backup 비용을 추적 및 최적화하고 를 사용하여 해당 태그를 보고 필터링할 수 AWS Cost Explorer있습니다.

비용 할당 태그를 사용하려면 Automating backups and optimizing backup costs for Amazon EFS using AWS Backup 및 비용 할당 태그 사용을 참조하세요.

AWS Backup Audit Manager 가격

AWS Backup Audit Manager는 통제 평가 횟수를 기준으로 사용 요금을 부과합니다. 컨트롤 평가는 한 컨트롤을 기준으로 한 가지 리소스를 평가하는 것입니다. 통제 평가 요금은 AWS Backup 청구서에 표시됩니다. 현재의 컨트롤 평가 요금은 AWS Backup 요금을 참조하세요.

AWS Backup Audit Manager 제어를 사용하려면 백업 활동을 추적할 수 있는 AWS Config 기록을 활성화해야 합니다. AWS Config 각 구성 항목에 대한 요금이 기록되며 이러한 요금은 AWS Config 청구서에 표시됩니다. 현재 구성 항목의 기록된 가격은 AWS Config 요금을 참조하세요.

Amazon Aurora 요금

Aurora 연속 백업을 위해 구성된 보존 기간(최대 35일) 동안 스냅샷에는 스토리지 요금이 발생하지 않습니다. 이 기간 이후에 보존된 스냅샷은 전체 백업으로 청구됩니다.

AWS Backup 블로그, 동영상, 자습서 및 기타 리소스

에 대한 자세한 내용은 AWS Backup다음을 참조하십시오.

- 를 사용하여 온프레미스 VMware 가상 머신을 백업 및 복원합니다. AWS Backup Olumuyiwa Koya 및 Ezekiel Oyerinde 참여(2022년 6월).
- Amazon Aurora 데이터베이스를 보호하는 AWS Backup 데 사용합니다. Chris Hendon, Brandon Rubadou, Thomas Liddle 참여(2022년 5월).
- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups. Evan Peck 및 Sabith Venkitachalapathy 참여(2022년 5월).
- 및 를 사용하여 보안 태세를 자동화하고 개선하십시오 AWS Backup . AWS PrivateLink Bilal Alam 참여(2022년 4월).
- 일일 계정 간 다중 AWS Backup 지역 간 집계된 보고서를 확보하십시오. Wali Akbari 및 Sabith Venkitachalapathy 참여(2022년 2월).
- 및 를 사용하여 백업 결과의 가시성을 자동화합니다. AWS Backup AWS Security Hub Kanishk Mahajan 참여(2022년 1월).
- 에서 AWS백업 보안을 위한 10가지 주요 보안 모범 사례 Ibukun Oyewumi 참여(2022년 1월).
- FSx for AWS Lustre를 통한 SAS 그리드 최적화 (및 재해 복구 최적화) AWS Backup Matt Saeger 및 Shea Lutton 참여(2022년 1월).
- 를 사용하여 Amazon Neptune의 데이터 보호 및 규정 준수를 중앙 집중화합니다. AWS Backup Brian O'Keefe 참여(2021년 11월).
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. Karthik Vijayraghavan 참여(2021년 11월).
- Audit Manager를 사용하여 데이터 보호 정책 AWS Backup 감사를 간소화할 수 있습니다. Jordan Bjorkman 및 Harshitha Putta 참여(2021년 11월).
- AWS Backup Vault Lock을 사용하여 백업의 보안 상태를 강화하십시오. Rolland Miller 참여(2021년 10월).
- AWS Backup 복원 작업에서 리소스 태그를 유지하는 방법 Ibukun Oyewumi, Amee Shah, Sabith Venkitachalapathy 참여(2021년 9월).

- 를 사용하여 서비스 제어 정책을 사용하여 백업에 대한 액세스를 관리합니다 AWS Backup. Sabith Venkitachalapathy 및 Ibukun Oyewumi 참여(2021년 8월).
- 를 사용하여 AWS 서비스 전반에서 대규모 중앙 집중식 백업을 자동화합니다 AWS Backup. Ibukun Oyewumi 및 Sabith Venkitachalapathy 참여(2021년 7월).
- 블로그: VSS를 사용하여 AWS Backup Microsoft SQL Server 백업을 간소화하는 방법 Siavash Irani 및 Sepehr Samiei 참여(2021년 7월).
- 를 사용하여 데이터 복구 검증을 자동화하십시오. AWS Backup Mahanth Jayadeva 참여(2021년 6월).
- AWS Backup 작업을 모니터링하도록 알림을 구성합니다. Virgil Ennes 참여(2021년 6월).
- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup. Prachi Gupta 및 Rohit Verma 참여(2021년 6월).
- Amazon EFS 백업 비용 관리: 비용 할당 태그 AWS Backup 지원. Aditya Maruvada 참여(2021년 5월).
- 를 사용하여 계정 및 지역 간에 암호화된 백업을 생성하고 공유할 수 AWS Backup있습니다. Prachi Gupta 참여(2021년 5월).
- AWS Backup 이제 FedRAMP High의 승인을 받아 규정 준수 및 데이터 보호 요구 사항을 충족할 수 있습니다. Andy Grimes 참여(2021년 5월).
- ZS Associates는 를 통해 백업 효율성을 향상시킵니다. AWS Backup Mitesh Naik, Hiranand Mulchandani, Sushant Jadhav 참여(2021년 5월).
- 자습서: Amazon EBS 백업 및 복원을 사용하여 AWS Backup. Fathima Kamal 참여(2021년 4월).
- 동영상 자습서: Managing Cross-Region Copies of Backups. 데이비드와 함께 DeLuca (2021년 4월)
- 에 대한 AWS 도구를 사용하여 여러 AWS Backup 복구 지점을 삭제합니다. PowerShell Sherif Talaat 참여(2021년 4월).
- Amazon FSx의 지역 간 백업 및 계정 간 백업을 사용합니다. AWS Backup Adam Hunter 및 Fathima Kamal 참여(2021년 4월).
- 에 대한 AWS Backup Amazon CloudWatch 이벤트 및 지표 Rolland Miller 참여(2021년 3월).
- 자습서: Amazon 관계형 데이터베이스 서비스 (RDS) 의 백업 및 복원 사용. AWS Backup Fathima Kamal 참여(2021년 3월).
- Amazon RDS를 위한 P oint-in-time 복구 및 연속 백업 기능을 제공합니다. AWS Backup Kelly Griffin 참여(2021년 3월).
- 존 AWS Backup 하우스몰러와 함께 AWS Service Catalog로 자동화하세요 (2021년 1월).
- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup. Cher Simon 참여(2021년 1월).

- AWS re:Invent 요약: 데이터 보호 및 규정 준수 AWS Backup Nancy Wang 참여(2020년 12월).
- AWS Backup 리소스 전체에 중앙 집중식 데이터 보호를 제공합니다. AWS Nancy Wang 참여(2020년 11월).
- Tech Talk: Data protection at scale with AWS Backup. Kareem Behairy 참여(2020년 9월).
- 지역 간 복사를 통한 중앙 집중식 교차 계정 관리 AWS Backup Cher Simon 참여(2020년 9월).
- 동영상 튜토리얼: 사용 중에 대규모로 백업을 관리하세요. AWS OrganizationsAWS Backup Ildar Sharafeev 참여(2020년 7월).
- AWS Organizations 사용 중에 대규모로 백업을 관리합니다 AWS Backup. Nancy Wang, Avi Drabkin, Ganesh Sundaresan, Vikas Shah 참여(2020년 6월).
- 를 사용하여 Amazon EFS 파일 및 폴더를 복구할 수 AWS Backup 있습니다. Abrar Hussain and Gurudath Pai 참여(2020년 5월).
- Scheduling automated backups using Amazon EFS and AWS Backup. Rob Barnes 참여(2019년 12월).
- re:Invent 레코딩: AWS re:Invent 2019: 딥 다이브 온 피트. AWS Backup 랙스페이스. Nancy Wang 및 Jason Pavao 참여(2019년 12월).
- 로 데이터를 보호합니다. AWS Backup Anthony Fiore 참여(2019년 7월).
- 마케팅 동영상: Introducing AWS Backup. 2019년 1월.
- 동영상: Introduction to AWS Backup. AWS 교육 및 인증 포함.

AWS 처음으로 설정하기

AWS Backup 처음 사용하기 전에 다음 작업을 완료하십시오.

1. 등록하기: AWS
2. IAM 사용자를 생성합니다.
3. IAM 역할 생성

등록하기: AWS

Amazon Web Services (AWS) 에 가입하면 다음을 AWS포함한 모든 서비스에 자동으로 AWS 계정 가입됩니다 AWS Backup. 사용자에게는 사용한 서비스에 대해서만 요금이 청구됩니다.

AWS Backup 사용료에 대한 자세한 내용은 AWS Backup 요금 페이지를 참조하십시오.

AWS 계정 이미 등록한 경우 다음 작업으로 건너뛰세요. AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성합니다.

생성하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

다음 작업에 필요하므로 AWS 계정 번호를 기록해 두세요.

IAM 사용자를 생성합니다.

예를 AWS들어 의 서비스에서는 서비스에 액세스할 때 자격 증명을 제공해야 합니다. 그래야 서비스가 사용자에게 해당 리소스에 액세스할 수 있는 권한이 있는지 여부를 확인할 수 있습니다. AWS Backup

AWS AWS 계정 루트 사용자를 사용하여 요청하지 않는 것이 좋습니다. 대신, IAM 사용자를 생성하고 해당 사용자에게 모든 액세스 권한을 부여합니다. 이러한 사용자를 관리자 사용자라고 합니다. AWS 계정 루트 사용자 자격 증명 대신 관리자 자격 증명을 사용하여 버킷 생성, 사용자 생성, 권한 부여 등의 작업을 AWS 수행하고 상호 작용할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 계정 루트 사용자 보안 인증 및 IAM 사용자 보안 인증과 IAM 사용 설명서의 IAM 모범 사례를 참조하세요.

AWS 가입했지만 직접 IAM 사용자를 생성하지 않은 경우 IAM 콘솔을 사용하여 생성할 수 있습니다.

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center에서 (권장)	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다. 이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM 보안 모범 사례를 참조하세요.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따르세요.	사용 AWS IAM Identity Center 설명서에서 사용하도록 구성하여 프로그래밍 액세스를 구성하십시오. AWS CLI AWS Command Line Interface
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 첫 IAM 관리 사용자 및 사용자 그룹 만들기에 나온 지침을 따릅니다.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리 단계를 수행하여 프로그래밍 방식의 액세스를 구성합니다.

새 IAM 사용자로 로그인하려면 에서 로그아웃하십시오. AWS Management Console그런 다음 다음 URL을 사용하십시오. 여기서 your_aws_account_id는 하이픈이 없는 AWS 계정 번호입니다 (예: 번호가 인 경우 ID는 다음과 같음). AWS 계정 1234-5678-9012 AWS 계정 123456789012

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

방금 생성한 IAM 사용자 이름과 암호를 입력합니다. 로그인하면 탐색 모음에 your_user_name@your_aws_account_id가 표시됩니다.

로그인 페이지의 URL에 ID를 포함하지 않으려면 계정 별칭을 만들 수 있습니다. AWS 계정 IAM 대시보드에서 계정 별칭 생성을 클릭하고 기업명 등의 별칭을 입력합니다. 계정 별칭 생성 후에는 다음 URL에서 로그인하세요.

```
https://your_account_alias.signin.aws.amazon.com/console/
```

본인 계정의 IAM 사용자 로그인 링크를 확인하려면 IAM 콘솔을 열고 대시보드의 AWS 계정 별칭 아래의 확인란을 선택합니다.

IAM 역할 생성

IAM 콘솔을 사용하여 지원되는 리소스에 액세스할 AWS Backup 권한을 부여하는 IAM 역할을 생성할 수 있습니다. IAM 역할을 생성한 후 정책을 생성하여 해당 역할에 연결합니다.

콘솔을 사용하여 IAM 역할을 생성하려면

1. AWS 관리 콘솔에 로그인하고 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. AWS 서비스 역할을 선택한 다음, AWS Backup에 대해 선택을 선택합니다. 다음: 권한을 선택합니다.
4. 권한 정책 연결 페이지에서 AWSBackupServiceRolePolicyForBackup 및 AWSBackupServiceRolePolicyForRestores를 둘 다 선택합니다. 이러한 AWS 관리형 정책은 지원되는 모든 AWS 리소스를 백업하고 복원할 AWS Backup 권한을 부여합니다. 관리형 정책에 대해 자세히 알아보고 예시를 보려면 관리형 정책 섹션을 참조하세요.

   그런 다음 다음: 태그를 선택합니다.
5. 다음: 검토를 선택합니다.
6. 역할 이름에 이 역할의 목적을 설명하는 이름을 입력합니다. 역할 이름은 사용자 내에서 고유해야 합니다 AWS 계정. 다양한 주체가 역할을 참조할 수 있기 때문에 역할을 생성한 후에는 역할 이름을 편집할 수 없습니다.

   Create Role(역할 생성)을 선택합니다.
7. 역할 페이지에서 해당 역할을 선택하여 해당 역할의 세부 정보 페이지를 엽니다.

시작하기 AWS Backup

이 자습서에서는 특징 및 기능을 사용하는 AWS Backup 일반적인 단계를 보여줍니다. 이 기술 설명서의 모든 부분과 마찬가지로 다른 창의 AWS 관리 콘솔을 따라 진행해야 합니다.

다음 자습서를 읽으면 특정 서비스와 AWS Backup 함께 사용하는 방법을 배울 수도 있습니다.

- Amazon 관계형 데이터베이스 서비스 (Amazon RDS) 를 사용한 백업 및 복원 AWS Backup
- 자습서: Amazon EBS 백업 및 복원을 사용한 AWS Backup

주제

필수 조건

시작하기 전에 다음이 있는지 확인하십시오.

- An. AWS 계정자세한 정보는 AWS 처음으로 설정하기을 참조하세요.
- 에서 지원하는 리소스가 하나 이상 있어야 AWS Backup합니다.
- 백업하려는 AWS 서비스와 리소스에 대해 잘 알고 있어야 합니다. 지원되는 AWS 리소스 및 타사 애플리케이션 목록을 참조하세요.

  새 AWS 서비스를 사용할 수 있게 되면 해당 서비스를 사용할 수 AWS Backup 있도록 설정하세요.

에서 사용할 AWS 서비스를 구성하려면 AWS Backup

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 서비스 옵트인 페이지에서 리소스 구성을 선택합니다.
4. 리소스 구성 페이지에서 토글 스위치를 사용하여 함께 AWS Backup사용되는 서비스를 활성화하거나 비활성화할 수 있습니다. 서비스가 구성되면 확인을 선택합니다. 옵트인하려는 AWS 서비스를 내 사이트에서 사용할 수 있는지 확인하세요. AWS 리전

추가 정보는 백업 계획에 리소스 할당 을 참조하십시오. AWS Backup 콘솔을 통해 사용자는 백업 계획에 리소스 유형을 할당할 수 있습니다. 이는 해당 특정 서비스에 옵트인이 활성화되지 않은 경우에도 포함됩니다.

- 백업하려는 리소스가 모두 동일한 AWS 리전에 있는지 확인합니다.

이 자습서를 완료하려면 AWS 계정 루트 사용자를 사용하여 에 로그인하면 됩니다 AWS Management Console. 하지만 AWS Identity and Access Management (IAM) 에서는 AWS 계정 루트 사용자를 사용하지 말 것을 권장합니다. 대신 계정에서 관리자를 생성하고 해당 자격 증명을 사용하여 계정에서 리소스를 관리합니다. 자세한 정보는 AWS 처음으로 설정하기을 참조하세요.

AWS Backup 콘솔은 리소스를 백업하기 위한 다양한 옵션을 제공합니다. 온디맨드 백업을 생성하거나, 리소스 백업 방식을 예약 및 구성하거나, 리소스 생성 시 리소스가 자동으로 백업되도록 구성할 수 있습니다.

시작하기 1: 서비스 옵트인

AWS Backup 콘솔에서는 백업 계획에 리소스 유형을 포함하는 두 가지 방법이 있습니다. 즉, 백업 계획에 리소스 유형을 명시적으로 할당하거나 모든 리소스를 포함하는 것입니다. 이러한 선택 항목이 서비스 옵트인과 어떻게 작동하는지 이해하려면 아래 내용을 참조하세요.

- 태그만 기준으로 하여 리소스를 할당할 경우 서비스 옵트인 설정이 적용됩니다.
- 리소스 유형을 백업 계획에 명시적으로 할당하면 해당 특정 서비스에 대해 옵트인이 활성화되지 않은 경우에도 백업에 포함됩니다. Aurora, Neptune 및 Amazon DocumentDB에는 적용되지 않습니다. 이러한 서비스를 포함하려면 옵트인을 활성화해야 합니다.

- 리소스 배정에 리소스 유형과 태그가 모두 지정된 경우 지정된 리소스 유형이 먼저 필터링된 다음 태그가 해당 리소스를 추가로 필터링합니다.

  서비스 옵트인 설정은 대부분의 리소스 유형에서 무시됩니다. 하지만 Aurora, Neptune 및 Amazon DocumentDB에는 서비스 옵트인이 필요합니다.
- Amazon FSx NetApp for ONTAP의 경우, 태그 기반 리소스 선택을 사용하는 경우 전체 파일 시스템 대신 개별 볼륨에 태그를 적용합니다.

옵트인 선택은 특정 계정 및 에 적용됩니다. AWS 리전계정이 지역에서 사용 AWS Backup (백업 저장소 또는 백업 계획 생성) 하는 경우, 해당 계정은 해당 시점에 해당 지역에서 지원되는 모든 리소스 유형에 자동으로 옵트인됩니다. AWS Backup 나중에 해당 지역에 추가된 지원 서비스는 백업 계획에 자동으로 포함되지 않습니다. 이러한 리소스 유형이 지원되면 해당 유형을 선택하도록 선택할 수 있습니다.

점점 더 많은 AWS 서비스와 타사 애플리케이션을 AWS Backup 지원하므로 새로 지원되는 리소스를 옵트인하려면 이 단계를 다시 검토해야 할 수 있습니다.

AWS Backup 이외의 환경에서 생성된 백업에는 적용되거나 관리되지 않습니다. AWS AWS Backup

지원되는 모든 리소스 유형을 보호하는 AWS Backup 데 사용하도록 옵트인하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 서비스 옵트인 아래에서 리소스 구성을 선택합니다.
4. 모든 토글을 오른쪽으로 이동하여 AWS Backup지원되는 모든 리소스를 옵트인하세요.
5. [Confirm]을 선택합니다.

다음 단계

를 사용하여 AWS Backup온디맨드 백업을 생성하려면 로 진행하십시오. 시작하기 8: 온디맨드 백업 생성

시작하기 8: 온디맨드 백업 생성

AWS Backup 콘솔의 보호된 리소스 페이지에는 한 번 AWS Backup 이상 백업된 리소스가 나열됩니다. 처음 사용하는 AWS Backup 경우 Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스와 같은 리

소스가 이 페이지에 나열되어 있지 않습니다. 백업 계획이 예약된 백업 작업을 한 번 이상 실행하지 않은 경우 이러한 리소스가 해당 백업 계획에 할당되어도 마찬가지입니다.

이 첫 번째 단계에서는 리소스 중 하나에 대한 온디맨드 백업을 생성합니다. 그러면 이 리소스는 보호된 리소스 페이지에 나열됩니다.

온디맨드 백업을 생성하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창을 사용하여, 보호된 리소스를 선택한 다음 온디맨드 백업 생성을 선택합니다.
3. 온디맨드 백업 생성 페이지에서 백업하려는 리소스 유형을 선택합니다. 예를 들어, Amazon DynamoDB용 DynamoDB 테이블을 선택합니다.
4. 보호할 리소스의 이름 또는 ID를 선택합니다. 선택한 리소스가 원하는 리소스인지 확인합니다.

> **Note**
>
> Amazon FSx for Lustre의 경우 Persistent 및 Persistent_2 배포 유형이 지원됩니다.

5. 지금 백업 생성이 선택되었는지 확인합니다. 이를 선택하면 백업이 즉시 시작되고 저장한 리소스를 보호된 리소스 페이지에서 더 빨리 확인할 수 있습니다.
6. 콜드 스토리지 값(해당하는 경우) 및 만료 값으로의 전환을 지정합니다.

> **Note**
>
> - 콜드 스토리지로 전환할 수 있는 리소스 목록을 보려면 리소스별 기능 가용성 표의 "콜드 스토리지로 전환 시 수명 주기" 섹션을 참조하십시오. 다른 모든 리소스 유형은 웜 스토리지에 저장되며, 콜드 스토리지 표현식으로의 전환은 무시됩니다. 만료 값은 모든 리소스 유형에 유효합니다.
> - 백업이 만료되고 수명 주기 정책의 일부로 삭제 대상으로 표시되면 다음 8시간 동안 임의로 선택한 시점에서 백업을 AWS Backup 삭제합니다. 이 창은 일관된 성능을 보장하는 데 도움이 됩니다.

7. 기존 백업 저장소를 선택합니다. 새 백업 저장소 생성을 선택하면 저장소를 생성하는 새 페이지가 열린 후 작업 완료 시 온디맨드 백업 생성 페이지로 돌아갑니다.
8. IAM 역할 아래에서 기본 역할을 선택합니다.

> **Note**
>
> 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 역할이 자동으로 생성됩니다.

9. 온디맨드 백업에 하나 이상의 태그를 할당하려면 키 및 값(선택 사항)을 입력하고 태그 추가를 선택합니다.

> **Note**
>
> - Amazon EC2 리소스의 경우 AWS Backup 백업에 추가한 태그 외에도 기존 그룹 및 개별 리소스 태그를 자동으로 복사합니다. 자세한 내용은 백업에 태그 복사를 참조하세요.
> - 태그 기반 백업 계획을 생성할 때 기본 역할이 아닌 역할을 선택하는 경우 태그가 지정된 모든 리소스를 백업하는 데 필요한 권한이 있는지 확인하십시오. AWS Backup 선택한 태그를 사용하여 모든 리소스를 처리하려고 시도합니다. 액세스 권한이 없는 리소스가 발견되면 백업 계획이 실패합니다.

10. 온디맨드 백업 생성을 선택합니다. 그러면 작업 페이지로 이동합니다. 여기서 작업 목록을 볼 수 있습니다.
11. 리소스 유형이 EC2인 경우 고급 백업 설정 섹션이 나타납니다. EC2 인스턴스에서 Microsoft Windows를 실행 중인 경우 Windows VSS를 선택합니다. 이렇게 하면 애플리케이션에 일관되게 적용되는 Windows VSS 백업을 수행할 수 있습니다.

> **Note**
>
> AWS Backup 현재 Amazon EC2에서 실행되는 애플리케이션 정합성이 보장되는 리소스 백업만 지원합니다. 모든 인스턴스 유형 또는 애플리케이션이 Windows VSS 백업에 대해 지원되는 것은 아닙니다. 자세한 정보는 Windows VSS 백업 생성을 참조하세요.

12. 백업하도록 선택한 리소스의 백업 작업 ID를 선택하여 해당 작업의 세부 정보를 확인합니다.

다음 단계

백업 작업을 자동화하려면 시작하기 3: 예약 백업 생성을 진행하세요.

시작하기 3: 예약 백업 생성

AWS Backup 자습서의 이 단계에서는 백업 계획을 생성하고, 여기에 리소스를 할당한 다음, 백업 저장소를 생성합니다.

시작하기 전에 사전 조건을 충족했는지 확인하십시오. 자세한 정보는 시작하기 AWS Backup을 참조하세요.

주제

1단계: 기존 백업 계획을 기준으로 백업 계획 생성

백업 계획은 Amazon DynamoDB 테이블 또는 Amazon Elastic File System(Amazon EFS) 파일 시스템과 같은 AWS 리소스를 백업할 시기와 방법을 정의하는 정책 표현식입니다. 백업 계획에 리소스를 AWS Backup 할당한 다음 백업 계획에 따라 해당 리소스에 대한 백업을 자동으로 백업하고 보존합니다. 자세한 정보는 백업 계획을 사용하여 백업 관리을 참조하세요.

새 백업 계획을 생성하는 방법에는 두 가지가 있습니다. 처음부터 빌드하거나 기존 백업 계획을 기반으로 빌드하면 됩니다. 이 예에서는 AWS Backup 콘솔을 사용하여 기존 백업 계획을 수정하여 백업 계획을 생성합니다.

기존 백업 계획에서 백업 계획을 생성하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 대시보드에서 백업 계획 관리를 선택합니다. 또는 탐색 창을 사용하여 백업 계획을 선택하고 백업 계획 생성을 선택합니다.
3. 템플릿으로 시작을 선택하고, 목록에서 계획(예: `Daily-Monthly-1yr-Retention`)을 선택한 후 백업 계획 이름 상자에 이름을 입력합니다.

> **Note**
>
> 기존 계획과 동일한 백업 계획을 생성하려고 하면 `AlreadyExistsException` 오류가 발생합니다.

4. 계획 요약 페이지에서 원하는 백업 규칙을 선택한 다음 편집을 선택합니다.
5. 규칙에 대해 원하는 값을 검토하고 선택합니다(규칙 옵션은 백업 계획 옵션 및 구성 참조).
6. 백업 저장소의 경우 기본값을 선택하거나 새 백업 저장소 생성을 선택하여 새 저장소를 생성합니다.
7. (선택 사항) - 대상 지역의 목록에서 백업을 다른 지역으로 복사할 항목을 AWS 리전 선택합니다. 리전을 더 추가하려면 복사 추가를 선택합니다.
8. 규칙 편집을 완료했으면 백업 규칙 저장을 선택합니다.

요약 페이지에서 리소스 할당을 선택하여 다음 섹션을 준비합니다.

2단계: 백업 계획에 리소스 할당

백업 계획을 생성한 후에는 해당 백업 계획에 AWS 리소스를 할당해야 합니다. 리소스 할당에 대한 자세한 내용은 백업 계획에 리소스 할당 섹션을 참조하세요.

백업 계획에 할당할 기존 AWS 리소스가 아직 없는 경우 이 연습에 사용할 새 리소스를 몇 개 생성하세요. 지원되는 AWS 리소스 및 타사 애플리케이션을 사용하여 하나 또는 두 개의 리소스를 생성합니다.

백업 계획에 리소스를 할당하려면

1. 이전 단계를 수행하면 리소스 할당 페이지로 이동합니다.
2. 리소스 할당 이름을 입력합니다.
3. IAM 역할의 경우 기본 역할을 선택합니다. 다른 역할을 선택할 경우, 할당하려는 모든 리소스를 백업할 권한이 있어야 합니다.
4. 리소스 할당 섹션에서 모든 리소스 유형 포함을 선택합니다. 리소스 유형은 AWS Backup지원되는 AWS 서비스 또는 타사 애플리케이션입니다. 이제 이 백업 플랜은 사용자가 사용을 사용하여 보호하기로 선택한 모든 리소스 유형을 보호합니다. AWS Backup
5. 리소스 할당을 선택합니다.

백업 계획 요약 페이지로 돌아갑니다. 백업 계획 생성을 선택하여 첫 번째 백업 계획을 배포하세요.

3단계: 백업 저장소 생성

AWS Backup 콘솔에서 자동으로 생성되는 기본 백업 저장소를 사용하는 대신 백업 그룹을 동일한 저장소에 저장하고 구성하는 특정 백업 저장소를 생성할 수 있습니다.

백업 저장소에 대한 자세한 내용은 백업 저장소 단원을 참조하십시오.

백업 저장소를 생성하려면

1. AWS Backup 콘솔의 탐색 창에서 Backup 볼트를 선택합니다.

   > **Note**
   >
   > 왼쪽에 탐색 창이 보이지 않는 경우 콘솔의 왼쪽 상단에 있는 메뉴 아이콘을 선택하여 열 수 있습니다. AWS Backup

2. 백업 저장소 생성를 선택합니다.
3. 백업 저장소의 이름을 입력합니다. 저장소에 저장할 내용이 잘 반영되도록 저장소의 이름을 지정하거나 필요한 백업을 보다 쉽게 검색할 수 있도록 만들 수 있습니다. 예를 들어, 이름을 **`FinancialBackups`**로 지정할 수 있습니다.
4. AWS Key Management Service (AWS KMS) 키를 선택합니다. 이미 만든 키를 사용하거나 기본 AWS Backup KMS 키를 선택할 수 있습니다.

   > **Note**
   >
   > 여기에 지정된 AWS KMS 키는 AWS Backup 독립 암호화를 지원하는 서비스의 백업에만 적용됩니다. AWS Backup 독립 암호화를 지원하는 리소스 유형 목록을 보려면 리소스별 기능 가용성 표의 “전체 AWS Backup 관리” 섹션을 참조하십시오.

5. 필요에 따라 백업 저장소의 검색 및 식별에 유용한 태그를 추가합니다. 예를 들어, **`BackupType:Financial`** 태그를 추가할 수 있습니다.
6. 백업 저장소 생성을 선택합니다.
7. 탐색 창에서 백업 저장소를 선택하고 백업 저장소가 추가되었는지 확인합니다.

> **Note**
>
> 이제 백업 계획 중 하나에서 백업 규칙을 편집하여 방금 생성한 백업 저장소에 해당 규칙으로 생성된 백업을 저장할 수 있습니다.

다음 단계

Amazon EFS 파일 시스템을 구체적으로 백업하려면 시작하기 4: Amazon EFS 자동 백업 생성을 진행합니다.

시작하기 4: Amazon EFS 자동 백업 생성

Amazon EFS 콘솔을 사용하여 Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성하면 자동 백업이 기본적으로 켜집니다. 기존 Amazon EFS 파일 시스템을 자동으로 백업하려는 경우, Amazon EFS 콘솔, API 또는 CLI를 사용하여 백업할 수 있습니다.

콘솔을 사용하여 기존 Amazon EFS 파일 시스템을 자동으로 백업하려면

1. https://console.aws.amazon.com/efs에서 Amazon EFS 콘솔을 엽니다.
2. 파일 시스템 페이지에서 자동 백업을 활성화할 파일 시스템을 선택합니다.
3. 일반 설정 패널에서 편집을 선택합니다.
4. 자동 백업을 켜려면 자동 백업 사용을 선택합니다.

기본 백업 계획 설정은 `daily backups, 35-day retention`입니다. 기본 백업 기간(백업이 실행될 기간)은 오전 5시 UTC(협정 세계시)에 시작하도록 설정되어 있으며 8시간 동안 지속됩니다.

> **Note**
>
> Amazon EFS 자동 백업 저장소 `aws/efs/automatic-backup-vault`는 이러한 자동 백업용으로만 예약됩니다.
> 이 저장소를 계정 간 복사본을 만드는 데 사용하거나 자동화되지 않은 다른 백업 계획에서 만든 백업의 대상으로 사용해서는 안 됩니다. 다른 백업 계획의 대상으로 사용할 경우 "권한 부족" 오류가 발생합니다.

AWS Backup 계정에서 사용자를 대신하여 서비스 연결 역할을 생성합니다. 이 역할에는 Amazon EFS 백업을 수행하는 데 필요한 권한이 있습니다. 서비스 연결 역할에 대한 자세한 내용은 AWS Backup에 서비스 연결 역할 사용 섹션을 참조하세요.

Amazon EFS 콘솔, API 또는 CLI를 사용하여 자동 백업을 켜거나 끄는 방법에 대한 step-by-step 지침은 Amazon Elastic File System 사용 설명서의 자동 백업을 참조하십시오.

다음 단계

생성한 백업을 보려면 시작하기 5: 백업 작업 및 복구 시점 보기를 진행합니다.

시작하기 5: 백업 작업 및 복구 시점 보기

를 사용하면 사용 중인 AWS 서비스 전반의 백업 및 복원 활동 상태 및 기타 세부 정보를 볼 수 있습니다. AWS Backup

AWS Backup 대시보드에서 백업 계획을 관리하고, 온디맨드 백업을 생성하고, 백업을 복원하고, 백업 및 복원 작업의 상태를 볼 수 있습니다.

주제

백업 작업의 상태 보기

AWS Backup 대시보드를 사용하여 백업 및 복원 작업의 상태를 빠르게 볼 수 있습니다.

백업 작업 상태를 보려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 대시보드를 선택합니다.
3. 백업 작업의 상태를 보려면 백업 작업 세부 정보를 선택합니다. 그러면 백업 작업 페이지로 이동합니다. 여기서 백업 작업 및 복원 작업을 포함하는 테이블을 볼 수 있습니다.
4. 시간별로 표시되는 작업을 필터링할 수 있습니다. 예를 들어, 지난 24시간, 지난 주 또는 지난 30일 동안 생성된 작업이 있습니다. 또한 기어 모양 아이콘을 선택하여 페이지별로 표시할 작업 수를 설정할 수 있습니다.

저장소에서 모든 백업 보기

다음 단계에 따라 AWS Backup의 지정된 저장소에서 생성된 백업을 봅니다.

저장소에서 모든 백업을 보려면

1. AWS Backup 콘솔의 탐색 창에서 Backup 볼트를 선택합니다.
2. 온디맨드 백업 또는 예약된 백업을 생성할 때 사용한 저장소를 선택하고 이 저장소에서 생성된 모든 백업을 봅니다.

> **Note**
>
> 각 백업에는 상태가 있으며, 이는 보통 완료됨으로 표시됩니다. 어떤 이유로든 수명 주기 구성에 따라 백업을 삭제할 AWS Backup 수 없는 경우 이 백업은 만료된 것으로 표시됩니다. 만료됨 상태의 백업이 사용하는 스토리지에 대해 요금이 청구되므로 이러한 백업은 삭제해야 합니다.

보호된 리소스의 세부 정보 보기

보호된 리소스 페이지에서는 AWS Backup에서 백업된 리소스의 세부 정보를 탐색할 수 있습니다.

보호된 리소스를 보려면

1. AWS Backup 콘솔의 탐색 창에서 보호된 리소스를 선택합니다.
2. 백업 중인 AWS 리소스를 볼 수 있습니다. 목록에서 리소스를 선택하여 해당 리소스에 대한 백업을 탐색합니다.

다음 단계

확인한 복구 시점을 복원하려면 시작하기 6: 백업 복원을 진행합니다.

시작하기 6: 백업 복원

리소스가 한 번 이상 백업되면 보호된 것으로 간주되며 를 사용하여 복원할 수 AWS Backup있습니다. 다음 단계에 따라 AWS Backup 콘솔을 사용하여 리소스를 복원합니다.

특정 서비스의 복원 매개 변수 또는 AWS Backup API를 사용한 백업 복원에 대한 자세한 내용은 백업 복원을 참조하십시오. AWS CLI

리소스를 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 복원하려는 보호된 리소스 및 리소스 ID를 선택합니다.
3. 리소스 유형을 포함한 복구 시점 목록이 리소스 ID별로 표시됩니다. 리소스를 선택하여 리소스 세부 정보 페이지를 엽니다.
4. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
5. 복원 파라미터를 지정합니다. 표시된 복원 파라미터는 선택한 리소스 유형과 관련된 파라미터입니다.

   > **Note**
   >
   > 백업을 하나만 보관한 경우 해당 백업을 수행한 시점의 파일 시스템 상태로만 복원할 수 있습니다. 이전 증분 백업으로 복원할 수는 없습니다.

   특정 리소스를 복원하는 방법에 대한 지침은 Restoring a backup을 참조하세요.
6. 역할 복원에서 기본 역할을 선택합니다.

   > **Note**
   >
   > 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 역할이 자동으로 생성됩니다.
7. 백업 복원을 선택합니다.

   복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

> **Note**
>
> Amazon EFS 인스턴스 내에서 특정 항목을 복원하기 위해 복원을 수행하면 해당 항목을 새 파일 시스템 또는 기존 파일 시스템으로 복원할 수 있습니다. 항목을 기존 파일 시스템에 복원하

는 경우 루트 디렉터리에서 항목을 포함할 새 Amazon EFS 디렉터리를 AWS Backup 생성합니다. 지정된 항목의 전체 계층 구조는 복구 디렉터리에 보존됩니다. 예를 들어, 디렉터리 A에 하위 디렉터리 B, C, D가 포함된 경우 A, B, C, D가 복구될 때 계층 구조가 AWS Backup 유지됩니다.
기존 파일 시스템이나 새 파일 시스템으로 Amazon EFS 부분 복원을 수행하는지 여부에 관계없이 각 복원 시도는 루트 디렉터리 외부에 복원된 파일을 포함할 새 복구 디렉터리를 생성합니다. 동일한 경로에 대해 복원을 여러 번 시도하면 복원된 항목이 포함된 여러 디렉터리가 존재할 수 있습니다.

Amazon EFS 인스턴스를 복원하려면

Amazon EFS 인스턴스를 복원하는 경우 전체 파일 시스템을 복원하는 전체 복원을 수행할 수 있습니다. 또는 항목 수준 복원을 사용하여 특정 파일 및 디렉터리를 복원할 수 있습니다(항목 수준 복원에는 제한이 있습니다. 자세한 내용은 Restoring an EFS file system 섹션을 참조하세요). 다른 유형의 리소스를 복원하는 방법에 대한 자세한 내용은 Restoring a backup을 참조하세요.

> **Note**
>
> Amazon EFS 인스턴스를 복원하려면 `backup:startrestorejob`을 "허용"해야 합니다.

백업 복원에 대한 자세한 내용은 백업 복원 섹션을 참조하세요.

다음 단계

AWS Backup Audit Manager를 사용하면 백업 활동 및 리소스를 감사할 수 있습니다. 백업, 복원, 복사 작업의 증거로 사용할 수 있는 보고서를 생성할 수도 있습니다. 보고서를 생성하려면 시작하기 7: 감사 보고서 생성을 참조하세요.

시작하기 7: 감사 보고서 생성

에서는 AWS Backup 대시보드 시작하기 5: 백업 작업 및 복구 시점 보기, 백업 저장소 및 보호된 리소스 보기에서 백업 활동을 관찰했습니다. 하지만 이러한 보기는 동적이며 참조하는 시기에 따라 업데이트됩니다. 이러한 보기가 조직의 데이터 보호 요구 사항 및 컨트롤을 장기간 지속적으로 준수하고 있다는 것을 입증하는 가장 좋은 증거는 아닙니다.

이 단계에서는 AWS Backup Audit Manager를 사용하여 온디맨드 백업 작업 보고서를 생성합니다.

AWS Backup Audit Manager는 CSV, JSON 또는 두 형식의 다양한 감사 보고서를 매일 또는 필요에 따라 Amazon S3 버킷에 제공합니다. 사용자 지정 가능한 여러 컨트롤을 기준으로 백업 작업 및 리소스의 규정 준수를 감사할 수 있습니다. 백업, 복사, 복원 작업에 대한 보고서를 수신할 수 있습니다. 백업 작업 보고서는 백업 작업이 이루어졌다는 증거입니다.

다음은 백업 파일의 예제입니다.


```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```


백업 보고서(온디맨드 백업 보고서 포함)를 생성하려면 우선 보고서를 자동화하고, Amazon S3 버킷으로 보고서를 전송하기 위한 보고서 계획을 생성해야 합니다.

보고서 계획에는 보고서를 수신할 Amazon S3 버킷이 있어야 합니다. 새 S3 버킷 설정에 대한 지침은 Amazon Simple Storage Service 사용 설명서의 1단계: 첫 번째 S3 버킷 생성을 참조하세요.

보고서 계획 생성

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 생성을 선택합니다.
4. 드롭다운 목록에서 작업 보고서 백업을 선택합니다.
5. 보고서 계획 이름에 **`TestBackupJobReport`**를 입력합니다.
6. 파일 형식은 CSV와 JSON을 모두 선택합니다.
7. S3 버킷 이름의 경우 드롭다운 목록에서 보고서의 대상을 선택합니다.
8. 보고서 계획 생성을 선택합니다.

다음으로, S3 버킷이 보고서를 수신하도록 허용해야 AWS Backup합니다. AWS Backup Audit Manager는 사용자를 위해 S3 액세스 정책을 자동으로 생성합니다.

이 액세스 정책을 보고 적용하려면

1. 왼쪽 탐색 창에서 보고서를 선택합니다.
2. 보고서 계획 이름 아래에서 보고서 계획의 이름(`TestBackupJobReport`)을 선택합니다.
3. 편집을 선택합니다.
4. S3 버킷에 대한 액세스 정책 보기를 선택합니다.
5. 권한 복사를 선택합니다.
6. 버킷 정책 편집을 선택해 대상 S3 버킷의 정책을 편집하여 백업 작업 보고서를 수신할 수 있도록 합니다.
7. 대상 S3 버킷 정책에 권한을 복사하거나 추가합니다.

다음 단계에서는 첫 번째 백업 작업 보고서를 생성합니다.

온디맨드 백업 보고서를 생성하려면

1. 왼쪽 탐색 창에서 보고서를 선택합니다.
2. 보고서 계획 이름 아래에서 보고서 계획의 이름(`TestBackupJobReport`)을 선택합니다.
3. 온디맨드 백업 보고서 생성을 선택합니다.

마지막으로, 보고서를 확인합니다.

보고서를 보려면

1. 왼쪽 탐색 창에서 보고서를 선택합니다.
2. 보고서 계획 이름 아래에서 보고서 계획의 이름(`TestBackupJobReport`)을 선택합니다.
3. 보고서 작업 섹션에서 S3 링크를 선택합니다. 이렇게 하면 대상 S3 버킷으로 이동합니다.
4. 다운로드를 선택합니다.
5. CSV 또는 JSON 파일 작업에 사용하는 프로그램을 사용하여 보고서를 엽니다.

다음 단계

시작하기 리소스를 정리하고 원치 않는 요금이 부과되지 않도록 하려면 시작하기 8: 리소스 정리를 진행합니다.

시작하기 8: 리소스 정리

시작하기 AWS Backup에서 모든 작업을 수행한 후에 불필요한 요금이 발생하지 않도록 이전에 생성했던 결과물을 정리할 수도 있습니다.

주제

- 1단계: 복원된 AWS 리소스 삭제
- 2단계: 백업 계획 삭제
- 3단계: 복구 시점 삭제
- 4단계: 백업 저장소 삭제
- 2단계: 보고서 계획 삭제
- 6단계: 보고서 삭제

1단계: 복원된 AWS 리소스 삭제

Amazon Elastic Block Store (Amazon Elastic Block Store) 볼륨 또는 Amazon DynamoDB 테이블과 같이 복구 지점에서 복원한 AWS 리소스를 삭제하려면 해당 서비스의 콘솔을 사용합니다. 예를 들어 Amazon EFS 콘솔을 사용하여 Amazon Elastic File System(Amazon EFS) 파일 시스템을 삭제합니다.

> **Note**
>
> 이 정보는 백업 저장소에 저장된 복구 시점이 아니라 복원된 리소스를 의미합니다.

2단계: 백업 계획 삭제

예약된 백업을 생성하지 않으려면 백업 계획을 삭제해야 합니다. 백업 계획을 삭제하려면 우선 해당 백업 계획에 대한 모든 리소스 할당을 삭제해야 합니다.

다음 단계에 따라 백업 계획을 삭제합니다.

백업 계획을 삭제하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택합니다.
3. 백업 계획 페이지에서 삭제할 백업 계획을 선택합니다. 그러면 해당 백업에 대한 세부 정보 페이지로 이동합니다.
4. 계획에 대한 리소스 할당을 삭제하려면 할당 이름 옆에 있는 라디오 버튼을 선택한 다음 삭제를 선택합니다.
5. 백업 계획을 삭제하려면 페이지 오른쪽 상단 모서리에 있는 삭제를 선택합니다.
6. 확인 페이지에 계획 이름을 입력하고 계획 삭제를 선택합니다.

3단계: 복구 시점 삭제

그런 다음 백업 저장소에 있는 백업 복구 시점을 삭제할 수 있습니다.

복구 시점을 삭제하려면

1. AWS Backup 콘솔의 탐색 창에서 Backup 볼트를 선택합니다.
2. 백업 저장소 페이지에서 백업을 저장한 백업 저장소를 선택합니다.
3. 복구 시점을 확인하고 삭제를 선택합니다.
4. 두 개 이상의 복구 시점을 삭제하려는 경우, 다음 단계를 따릅니다.
   a. 목록에 연속 백업이 포함된 경우 연속 백업 데이터를 유지하거나 삭제할지 선택합니다.
   b. 나열된 복구 시점을 모두 삭제하려면 **delete**를 입력한 다음, 복구 시점 삭제를 선택합니다.

페이지의 상단에 녹색 성공 배너가 표시될 때까지 브라우저 탭을 계속 열어 놓습니다. 이 탭을 너무 일찍 닫으면 삭제 프로세스가 종료되며 삭제하려 했던 복구 시점의 일부가 남을 수 있습니다. 자세한 내용은 Deleting backups 섹션을 참조하세요.

4단계: 백업 저장소 삭제

기본 백업 저장소는 일반적으로 삭제할 수 없습니다. 그러나 리전에 다른 저장소가 하나 이상 있는 경우, AWS CLI를 사용하여 해당 리전의 기본 백업 저장소를 삭제할 수 있습니다.

내부의 모든 백업(복구 시점)이 삭제되면 기본값 이외의 다른 저장소도 삭제할 수 있습니다. 이렇게 하려면 빈 저장소에서 삭제를 선택합니다.

2단계: 보고서 계획 삭제

보고서 계획은 매일 새 보고서를 자동으로 전송합니다. 이를 방지하려면 보고서 계획을 삭제합니다.

보고서 계획을 삭제하려면

1. AWS Backup 콘솔의 탐색 창에서 [Reports] 를 선택합니다.
2. 보고서 계획 이름 아래에서 보고서 계획의 이름을 선택합니다.
3. 삭제를 선택합니다.
4. 보고서 계획의 이름을 입력하고 보고서 계획 삭제를 선택합니다.

6단계: 보고서 삭제

각 보고서의 단일 객체 삭제 지침에 따라 보고서를 삭제할 수 있습니다. 대상 S3 버킷이 더 이상 필요하지 않은 경우, 해당 버킷에서 모든 객체를 삭제한 후에 버킷 삭제 지침에 따라 버킷을 삭제할 수 있습니다.

백업 계획을 사용하여 백업 관리

에서 AWS Backup백업 계획은 Amazon DynamoDB 테이블 또는 Amazon Elastic File System (Amazon EFS) 파일 시스템과 같은 AWS 리소스를 백업할 시기와 방법을 정의하는 정책 표현식입니다. 백업 계획에 리소스를 할당하고 백업 계획에 따라 해당 리소스에 대한 백업을 AWS Backup 자동으로 백업하고 유지할 수 있습니다. 백업 요구 사항이 다른 워크로드가 있는 경우 여러 백업 계획을 만들 수 있습니다. 기본적으로 백업 기간은 AWS Backup에 의해 최적화됩니다. 콘솔에서 또는 프로그래밍 방식으로 백업 기간을 사용자 지정할 수 있습니다.

AWS Backup 주기적인 백업을 점진적으로 효율적으로 저장합니다. AWS 리소스의 첫 번째 백업은 데이터의 전체 복사본을 백업합니다. 연속되는 각 증분 백업의 경우 AWS 리소스의 변경 사항만 백업됩니다. 증분 백업을 사용하면 스토리지 비용을 최소화하면서 백업을 자주 실행하여 데이터를 보호하는 이점을 누릴 수 있습니다.

AWS Backup 또한 보존 설정에 따라 백업 계획의 라이프사이클을 원활하게 관리하므로 필요할 때 복원할 수 있습니다.

다음 섹션에서는 에서 백업 전략을 관리하는 데 필요한 기본 사항을 제공합니다. AWS Backup

주제

- 백업 계획 생성
- 백업 계획에 리소스 할당
- 백업 계획 삭제
- 백업 계획 업데이트

백업 계획 생성

AWS Backup 콘솔, API, CLI, SDK 또는 템플릿을 사용하여 백업 계획을 생성할 수 있습니다. AWS CloudFormation

주제

- AWS Backup 콘솔을 사용하여 백업 계획 생성
- 를 사용하여 백업 계획 생성 AWS CLI
- 백업 계획 옵션 및 구성
- AWS CloudFormation 백업 계획을 위한 템플릿

AWS Backup 콘솔을 사용하여 백업 계획 생성

https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다. 대시보드에서 백업 계획 관리를 선택합니다. 또는 탐색 창을 사용하여 백업 계획을 선택하고 백업 계획 생성을 선택합니다.

시작 옵션

새 백업 계획에는 세 가지 선택 사항이 있습니다.

- 1단계: 기존 백업 계획을 기준으로 백업 계획 생성
- 새 계획 수립
- 를 사용하여 백업 계획 생성 AWS CLI

이 자습서에서는 새 계획 수립을 선택합니다. 구성의 각 부분에는 자세한 내용을 탐색할 수 있는 페이지의 확장된 섹션으로 연결되는 링크가 있습니다.

1. 플랜 이름을 입력합니다 백업 계획 이름. 계획을 만든 후에는 이름을 변경할 수 없습니다.

   기존 계획과 동일한 백업 계획을 만들려고 하면 `AlreadyExistsException` 오류가 발생합니다.
2. 선택적으로, 백업 계획에 태그를 추가할 수 있습니다.
3. 백업 규칙 구성: 백업 규칙 구성 섹션에서 백업 일정, 기간 및 수명 주기를 설정합니다.
4. 일정:

   a. 텍스트 필드에 백업 규칙 이름을 입력합니다.

   b. 백업 볼트 드롭다운 메뉴에서 기본값을 선택하거나 새 백업 볼트 생성을 선택하여 새 볼트를 생성합니다.

   c. 백업 빈도 드롭다운 메뉴에서 이 계획에서 백업을 생성할 빈도를 선택합니다.
5. 백업 기간:

   a. 시작 시간은 시스템의 현지 시간대를 기준으로 오전 12시 30분 (24시간 기준 00:30) 으로 기본 설정됩니다.

   b. 다음 시간 내에 시작의 기본값은 8시간입니다. 이 값을 변경하여 백업 시작 시간을 지정할 수 있습니다.

   c. 다음 시간 내에 완료의 기본값은 7일입니다.
6. 연속 백업 및 point-in-time 복원 (PITR): 복구를 위한 point-in-time 연속 백업 활성화 (PITR) 를 선택할 수 있습니다. 이 유형의 백업에 지원되는 리소스를 확인하려면 리소스별 기능 가용성 매트릭스를 참조하세요.

7. 수명 주기

   a. 콜드 스토리지: 이 상자를 선택하면 총 보존 기간에 지정한 시간표에 따라 적합한 리소스 유형을 콜드 스토리지로 전환할 수 있습니다. 콜드 스토리지를 사용하려면 총 보존 기간이 90일 이상이어야 합니다.

   b. Amazon EBS용 콜드 스토리지는 Amazon EBS 스냅샷 아카이브입니다. 아카이브 스토리지 계층으로 전환된 스냅샷은 콘솔에 콜드 계층으로 표시됩니다. 콜드 스토리지가 활성화되어 있고 백업 빈도가 매월 또는 그보다 짧으면 백업 계획을 EBS 스냅샷으로 전환할 수 있습니다.

   c. 총 보존 기간은 AWS Backup에 리소스를 저장하는 기간(일)입니다. 웜 스토리지에 콜드 스토리지를 더한 총 일수입니다.

8. (선택 사항) 백업 사본을 다른 AWS 리전에 저장하려는 경우 대상으로 복사를 사용하여 적합한 리소스의 리전 간 사본을 생성합니다.

9. (선택 사항) 복구 시점에 추가되는 태그

10. 모든 섹션이 사양에 맞게 설정되면 백업 규칙 저장을 선택합니다.

를 사용하여 백업 계획 생성 AWS CLI

JSON 문서에서 백업 계획을 정의하고 AWS Backup 콘솔 또는 AWS CLI를 사용하여 백업 계획을 제공할 수도 있습니다. 다음 JSON 문서에는 태평양 표준시 1:00 에 일일 백업을 생성하는 샘플 백업 계획이 포함되어 있습니다 (현지 시간은 해당하는 경우 일광, 표준시 또는 서머타임 조건에 맞게 조정됨). 1년 후 백업이 자동으로 삭제됩니다.

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules":[
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone":"America/Los_Angeles",
        "StartWindowMinutes":integer, // Value is in minutes
        "CompletionWindowMinutes":integer, // Value is in minutes
        "Lifecycle":{
          "DeleteAfterDays":integer, // Value is in days
        }
      }
    ]
  }
```

```
}
```

선택한 이름으로 JSON 문서를 저장할 수 있습니다. 아래의 CLI 명령은 이름이 `test-backup-plan.json`인 JSON과 함께 `create-backup-plan`을 표시합니다.

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

참고로 일부 시스템에서는 요일 번호를 0에서 6까지 매기지만, 저희는 1에서 7까지 번호를 매깁니다. 자세한 내용은 Cron 표현식을 참조하십시오. 시간대에 대한 자세한 내용은 Amazon Location Service API 참조를 참조하십시오 TimeZone.

백업 계획 옵션 및 구성

AWS Backup 콘솔에서 백업 계획을 정의할 때 다음 옵션을 구성합니다.

백업 계획 이름

고유한 백업 계획 이름을 제공해야 합니다.

기존 계획의 이름과 동일한 이름을 선택하면 오류 메시지가 표시됩니다.

백업 규칙

백업 계획은 하나 이상의 백업 규칙으로 구성됩니다. 백업 계획에 백업 규칙을 추가하거나 백업 계획의 기존 규칙을 편집하려면

1. AWS Backup 콘솔의 왼쪽 탐색 창에서 Backup plans를 선택합니다.
2. 백업 계획 이름 아래에서 백업 계획을 선택합니다.
3. 백업 규칙 섹션 아래에서

   - 백업 규칙을 추가하려면 백업 규칙 추가를 선택합니다.
   - 기존 백업 규칙을 편집하려면 규칙을 선택한 다음 편집을 선택합니다.

> **Note**
>
> 여러 규칙이 포함된 백업 계획이 있고 두 규칙의 기간이 겹치는 경우 백업을 AWS Backup 최적화하고 보존 기간이 더 긴 규칙에 대한 백업을 생성합니다. 최적화 작업은 일일 백업을 수행하는 시점뿐만 아니라, 전체 시작 기간을 고려합니다.

각 백업 규칙은 다음과 같은 요소로 이루어집니다.

백업 규칙 이름

백업 규칙 이름은 대/소문자를 구분합니다. 1~50자의 영숫자 문자 또는 하이픈으로 구성되어야 합니다.

백업 빈도

백업 빈도에 따라 스냅샷 백업이 AWS Backup 생성되는 빈도가 결정됩니다. 콘솔을 사용하여 1시간마다, 12시간마다, 매일, 매주 또는 매월 중에서 빈도를 선택할 수 있습니다. 시간당 스냅샷 백업을 생성하는 cron 표현식을 생성할 수도 있습니다. AWS Backup CLI를 사용하면 1시간마다 스냅샷 백업을 스케줄링할 수 있습니다.

매주를 선택하면 백업을 수행할 요일을 지정할 수 있습니다. 매월을 선택하면 한 달 중에서 특정 일을 선택할 수 있습니다.

지원되는 리소스에 대한 연속 백업 활성화 확인란을 선택하여 point-in-time 복원 (PITR) 지원 연속 백업 규칙을 생성할 수도 있습니다. 스냅샷 백업과 달리 연속 백업을 사용하면 복원을 수행할 수 있습니다. point-in-time 연속 백업에 대한 자세한 내용은 시점 복구를 참조하세요.

백업 기간

백업 기간은 해당 백업 기간이 시작되는 시간 및 기간의 지속 시간으로 구성됩니다. 백업 작업은 이 기간 내에서 시작됩니다. 콘솔의 기본 설정은 다음과 같습니다.

- 현지 시스템 시간대 기준 오전 12시 30분 (24시간 시스템의 경우 0:30)
- 8시간 이내에 시작
- 7일 이내에 완료

  (다음 시간 내에 완료 파라미터는 Amazon FSx 리소스에는 적용되지 않음)

Cron 식을 사용하여 백업 빈도 및 백업 기간 시작 시간을 사용자 지정할 수 있습니다. AWS 크론 표현식의 6개 필드를 보려면 Amazon CloudWatch Events 사용 설명서의 Cron 표현식을 참조하십시오. AWS 크론 표현식의 두 가지 예로는 `15 * ? * * *` (1시간 이후 15분에 1시간마다 백업 생성) 과 `0 12 * * ? *` (매일 정오 12시 (UTC 기준) 백업) 이 있습니다. 예시 표를 보려면 이전 링크를 클릭하고 페이지를 아래로 스크롤하세요.

AWS Backup 00:00 에서 23:59 사이의 크론 표현식을 평가합니다. '12시간마다'에 대한 백업 규칙을 만들되, 시작 시간을 11:59 이후로 설정하면 백업이 하루에 한 번만 실행됩니다.

연속 백업 및 point-in-time 복원 (PITR) 은 일정 기간 동안 기록된 변경 내용을 참조하므로 시간 또는 cron 표현식을 사용하여 일정을 예약할 수 없습니다.

> **Note**
>
> 일반적으로 AWS 데이터베이스 서비스는 유지 관리 기간 1시간 전 또는 도중에 백업을 시작할 수 없으며 Amazon FSx는 유지 관리 기간 또는 자동 백업 기간 4시간 이전 또는 도중에 백업을 시작할 수 없습니다 (Amazon Aurora는 이 유지 관리 기간 제한에서 제외됨). 이 기간에 예약된 스냅샷 백업은 오류가 발생합니다.
> 지원되는 서비스에 대해 스냅샷 백업과 연속 백업 두 가지 모두에 AWS Backup 을 사용하도록 선택하면 예외가 발생합니다. AWS Backup 은 충돌을 방지하기 위해 백업 기간을 자동으로 예약합니다. 지원되는 서비스 목록과 연속 백업을 수행하는 데 사용하는 방법에 대한 지침은 지정 시간 복구를 참조하십시오. AWS Backup

중복 백업 규칙

경우에 따라 백업 계획에 중복 규칙이 여러 개 포함될 수 있습니다. 서로 다른 규칙의 시작 기간이 겹치는 경우 규칙에 따라 백업을 AWS Backup 보존하고 보존 기간을 연장합니다. 예를 들어, 다음과 같은 두 가지 규칙이 있는 백업 계획을 가정해 보겠습니다.

1. 시간당 백업 - 1시간 시작 기간, 1일 동안 보존.
2. 12시간마다 백업 - 8시간 시작 기간, 1주일 동안 보존.

24시간이 지나면 두 번째 규칙에 따라 두 개의 백업이 생성됩니다. 두 번째 규칙의 보존 기간이 더 길기 때문입니다. 첫 번째 규칙은 백업을 8개 생성합니다. 두 번째 규칙의 8시간 시작 기간으로 인해 시간당 백업을 그 이상 실행할 수 없기 때문입니다. 구체적으로 설명하면 다음과 같습니다.

이 시작 기간 동안	이 규칙은 백업을 1개 생성함
자정부터 오전 8시까지	12시간
8~9	시간당
9~10	시간당
10~11	시간당

이 시작 기간 동안	이 규칙은 백업을 1개 생성함
11시부터 정오까지	시간당
정오부터 오후 8시까지	12시간
8~9	시간당
9~10	시간당
10~11	시간당
11시부터 자정까지	시간당

시작 기간 동안에는 백업 작업이 성공적으로 시작되거나 시작 기간이 만료될 때까지 백업 작업 상태가 CREATED 상태로 유지됩니다. 시작 시간 AWS Backup 내에 작업을 다시 시도할 수 있는 오류가 발생하는 경우 는 백업이 성공적으로 시작 (작업 상태가 로 변경RUNNING) 되거나 작업 상태가 로 변경될 때까지 (시작 창 시간이 끝나면 발생할 것으로 예상됨) 최소 10분마다 작업을 AWS Backup 자동으로 다시 시도합니다. EXPIRED

수명 주기 및 스토리지 계층

백업은 지정한 기간(일) 동안 저장되며, 이것을 백업 수명 주기라고 합니다. 백업은 수명 주기가 끝날 때까지 복원할 수 있습니다.

이 기간은 콘솔의 백업 규칙 구성의 수명 주기 섹션에서 총 보존 기간으로 설정됩니다. AWS Backup

를 사용하는 AWS CLI경우 파라미터를 사용하여 설정됩니다 `DeleteAfterDays`. 스냅샷의 보존 기간은 1일~100년(또는 입력하지 않을 경우 무기한)이며, 연속 백업의 보존 기간은 1일~35일입니다. 백업 작성 날짜는 백업 작업이 완료된 날짜가 아니라 시작된 날짜입니다. 백업 작업이 시작된 날짜와 같은 날짜에 완료되지 않는 경우 보존 기간을 계산하는 데 도움이 되도록 시작 날짜를 사용하십시오.

백업은 스토리지 계층에서 유지 관리됩니다. AWS Backup 요금에 명시된 바와 같이 각 계층마다 스토리지 및 복원 비용이 다릅니다. 모든 백업은 생성되어 웜 스토리지에 저장됩니다. 백업 저장 기간에 따라 백업을 콜드 스토리지라는 저렴한 계층으로 전환해야 할 수 있습니다. 이 선택적 기능이 있는 리소스가 리소스별 기능 가용성에 표시됩니다.

Console

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 백업 계획을 만들거나 편집합니다.
3. 백업 규칙 구성의 수명 주기 섹션에서 백업을 웜 스토리지에서 콜드 스토리지로 이동 확인란을 선택합니다.
4. (선택 사항) Amazon EBS가 백업하는 리소스 중 하나이고 백업 빈도가 매월 또는 그보다 짧으면 EBS 스냅샷 아카이브를 사용하여 콜드 계층으로 전환할 수 있습니다.
5. 백업을 웜 스토리지에 보관할 값 (일) 을 입력합니다. AWS Backup 최소 8일을 권장합니다.
6. 총 보존 기간의 값(일)을 입력합니다. 총 보존 기간과 웜 스토리지 기간 간의 차이는 백업이 콜드 스토리지에 보관되는 일수입니다.

AWS CLI

1. `create-backup-plan` 또는 `update-backup-plan`를 사용합니다.
2.
3. EBS 리소스의 경우 `OptInToArchiveForSupportedResources` 부울 파라미터를 포함합니다.
4. `MoveToColdStorageAfterdays` 파라미터를 포함합니다.
5. `DeleteAfterDays` 파라미터를 사용합니다. 이 값은 90(일)과 `MoveToColdStorageAfterDays`에 입력한 값을 더한 값이어야 합니다.

현재 콜드 스토리지는 다음 리소스 유형에 사용할 수 있습니다.

리소스 유형	콜드 스토리지의 증분 또는 전체 백업
AWS CloudFormation	증분
고급 기능이 있는 DynamoDB	전체. 증분 백업을 사용하는 계층 없음
Amazon EBS(EBS 스냅샷 아카이브 사용)	전체. 전환 후 증분 백업은 전체 백업이 됩니다.
Amazon EFS	증분
Amazon EC2 인스턴스에서 실행되는 SAP HANA 데이터베이스	증분
Amazon Timestream	증분

리소스 유형	콜드 스토리지의 증분 또는 전체 백업
VMware 가상 머신	증분

콘솔 또는 명령줄을 통해 콜드 스토리지로 전환되도록 설정한 후에는 콜드 스토리지(또는 아카이브)의 백업에 다음 조건이 적용됩니다.

- 전환된 백업은 웜 스토리지에 보관 기간 외에도 최소 90일 동안 콜드 스토리지에 보관해야 합니다. AWS Backup 보존 기간을 “며칠 후 콜드 모드로 전환” 설정보다 90일 더 길게 설정해야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.
- 일부 서비스는 증분 백업을 지원합니다. 증분 백업의 경우 웜 전체 백업이 하나 이상 있어야 합니다. AWS Backup 최소 8일이 지나야 백업을 콜드 스토리지로 옮기지 않도록 수명 주기 설정을 지정하는 것이 좋습니다. 전체 백업을 콜드 스토리지로 너무 빨리 전환하면 (예: 1일 후 콜드 스토리지로 전환) 웜 전체 AWS Backup 백업이 하나 더 생성됩니다.
- 증분 백업을 지원하는 리소스 유형의 경우 웜 백업에서 AWS Backup 전환된 데이터를 더 이상 참조하지 않는 경우 웜 스토리지에서 콜드 스토리지로 데이터를 전환합니다. 콜드 스토리지에 보존되며 다른 콜드 백업에서만 참조하는 백업의 데이터에는 콜드 스토리지 계층 요금이 부과됩니다. 다른 백업은 웜 스토리지 계층 요금이 계속 적용됩니다.

백업 저장소

백업 저장소는 백업을 정렬하는 컨테이너입니다. 백업 규칙으로 생성된 백업은 사용자가 백업 규칙에 지정한 백업 저장소에서 구성됩니다. 백업 저장소를 사용하여 백업 저장소의 백업을 암호화하고 백업 저장소의 백업에 대한 액세스를 제어하는 데 사용되는 AWS Key Management Service (AWS KMS) 암호화 키를 설정할 수 있습니다. 또한 백업 저장소에 태그를 추가하여 정리할 수 있습니다. 기본 저장소를 사용하지 않으려면 직접 생성할 수 있습니다. 백업 저장소를 만드는 step-by-step 방법에 대한 지침은 을 참조하십시오. 3단계: 백업 저장소 생성

리전에 복사

백업 계획 중 선택적으로 다른 AWS 리전에서 백업 복사본을 생성할 수 있습니다. 백업 복사본에 대한 자세한 내용은 AWS 리전간 백업 복사본 생성 섹션을 참조하세요.

백업 복사본을 정의할 때 다음 옵션을 구성합니다.

대상 리전

백업 복사본의 대상 리전입니다.

(고급 설정) 백업 저장소

복사본의 대상 백업 저장소입니다.

(고급 설정) IAM 역할

복사본을 생성할 때 AWS Backup 사용하는 IAM 역할. 또한 역할은 역할을 수임할 수 있는 신뢰할 수 있는 개체로 AWS Backup 등록되어 있어야 합니다. AWS Backup 기본값을 선택했는데 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 역할이 자동으로 생성됩니다.

(고급 설정) 수명 주기

백업 복사본을 콜드 스토리지로 전환할 시기와 복사본의 만료(삭제) 시기를 지정합니다. 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 복사본이 콜드 스토리지로 전환된 후에는 이 값을 변경할 수 없습니다.

만료는 복사본 생성 후 삭제될 때까지의 일 수를 지정합니다. 이 값은 콜드 스토리지로 전환 값보다 90일 이상이 커야 합니다.

복구 시점에 추가되는 태그

여기에 나열된 태그는 백업 생성 시 백업에 자동으로 추가됩니다.

백업 계획에 추가된 태그

이러한 태그는 백업 계획을 쉽게 구성하고 추적할 수 있도록 백업 계획 자체와 연결됩니다.

고급 백업 설정

Amazon EC2 인스턴스에서 실행 중인 타사 애플리케이션에 대해 애플리케이션 일치 백업을 수행할 수 있습니다. 현재 Windows VSS 백업을 AWS Backup 지원합니다. AWS Backup Windows VSS 백업에서 특정 Amazon EC2 인스턴스 유형을 제외합니다. 자세한 정보는 Windows VSS 백업 생성을 참조하세요.

AWS CloudFormation 백업 계획을 위한 템플릿

참조용으로 두 개의 샘플 AWS CloudFormation 템플릿을 제공합니다. 첫 번째 템플릿은 간단한 백업 계획을 생성합니다. 두 번째 템플릿을 사용하면 백업 계획에서 VSS 백업을 실행할 수 있습니다.

> **Note**
>
> 기본 서비스 역할을 사용하는 경우 *service-role*을 AWSBackupServiceRolePolicyForBackup으로 바꿉니다.

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"
    DependsOn: BackupVaultWithDailyBackups
```

```
DDBTableWithDailyBackupTag:
  Type: "AWS::DynamoDB::Table"
  Properties:
    TableName: "TestTable"
    AttributeDefinitions:
      - AttributeName: "Album"
        AttributeType: "S"
    KeySchema:
      - AttributeName: "Album"
        KeyType: "HASH"
    ProvisionedThroughput:
      ReadCapacityUnits: "5"
      WriteCapacityUnits: "5"
    Tags:
      - Key: "backup"
        Value: "daily"

BackupRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    ManagedPolicyArns:
      - "arn:aws:iam::aws:policy/service-role/service-role"

TagBasedBackupSelection:
  Type: "AWS::Backup::BackupSelection"
  Properties:
    BackupSelection:
      SelectionName: "TagBasedBackupSelection"
      IamRoleArn: !GetAtt BackupRole.Arn
      ListOfTags:
        - ConditionType: "STRINGEQUALS"
          ConditionKey: "backup"
          ConditionValue: "daily"
    BackupPlanId: !Ref BackupPlanWithDailyBackups
```

```
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
```

백업 계획에 리소스 할당

리소스 AWS Backup 할당은 백업 계획을 사용하여 보호할 리소스를 지정합니다. AWS Backup 간단한 기본 설정과 백업 계획에 리소스를 할당할 수 있는 세밀한 제어 기능을 모두 제공합니다. 백업 계획이 실행될 때마다 리소스 할당 기준과 일치하는 모든 리소스를 AWS 계정 스캔합니다. 이 수준의 자동화를 통해 백업 계획과 리소스 할당을 정확히 한 번만 정의할 수 있습니다. AWS Backup 이전에 정의한 리소스 할당에 맞는 새 리소스를 찾고 백업하는 작업을 추상화합니다.

관리하기로 선택한 모든 AWS Backup지원 리소스 유형을 할당할 수 있습니다. AWS Backup AWS Backup지원되는 추가 리소스 유형을 옵트인하는 방법에 대한 지침은 시작하기 1: 서비스 옵트인을 참조하십시오.

AWS Backup 콘솔에서는 백업 계획에 리소스 유형을 포함하는 두 가지 방법이 있습니다. 즉, 백업 계획에 리소스 유형을 명시적으로 할당하거나 모든 리소스를 포함하는 것입니다. 이러한 선택 항목이 서비스 옵트인과 어떻게 작동하는지 이해하려면 아래 내용을 참조하세요.

- 태그만 기준으로 하여 리소스를 할당할 경우 서비스 옵트인 설정이 적용됩니다.
- 리소스 유형을 백업 계획에 명시적으로 할당하면 해당 특정 서비스에 대해 옵트인이 활성화되지 않은 경우에도 백업에 포함됩니다. Aurora, Neptune 및 Amazon DocumentDB에는 적용되지 않습니다. 이러한 서비스를 포함하려면 옵트인을 활성화해야 합니다.
- 리소스 배정에 리소스 유형과 태그가 모두 지정된 경우 지정된 리소스 유형이 먼저 필터링된 다음 태그가 해당 리소스를 추가로 필터링합니다.

  서비스 옵트인 설정은 대부분의 리소스 유형에서 무시됩니다. 하지만 Aurora, Neptune 및 Amazon DocumentDB에는 서비스 옵트인이 필요합니다.
- 계정이 특정 지역의 백업 저장소 또는 백업 계획을 사용 AWS Backup (백업 저장소 또는 백업 계획 생성) 하는 경우, 해당 계정은 해당 시점에 해당 지역에서 지원되는 모든 리소스 유형에 자동으로 옵트인됩니다. AWS Backup 나중에 해당 지역에 추가된 지원 서비스는 백업 계획에 자동으로 포함되지 않습니다. 이러한 리소스 유형이 지원되면 해당 유형을 선택하도록 선택할 수 있습니다.
- Amazon FSx NetApp for ONTAP의 경우, 태그 기반 리소스 선택을 사용하는 경우 전체 파일 시스템 대신 개별 볼륨에 태그를 적용합니다.

리소스 할당에는 리소스 유형 및 리소스가 포함되거나 제외될 수 있습니다.

- 리소스 유형에는 AWS Backup지원되는 AWS 서비스 또는 타사 애플리케이션의 모든 인스턴스 또는 리소스가 포함됩니다. 예를 들어, DynamoDB 리소스 유형은 모든 DynamoDB 테이블을 참조합니다.

- 리소스는 DynamoDB 테이블 같은 리소스 유형의 단일 인스턴스입니다. 고유한 리소스 ID를 사용하여 리소스를 지정할 수 있습니다.

태그와 조건 연산자를 사용하여 리소스 할당을 더욱 세분화할 수 있습니다.

주제

- 콘솔을 이용하여 리소스 할당
- 프로그래밍 방식으로 리소스 할당
- 를 사용하여 리소스를 할당합니다. AWS CloudFormation
- 리소스 할당에 대한 할당량

콘솔을 이용하여 리소스 할당

리소스 할당 페이지로 이동하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 계획을 선택합니다.
3. 백업 계획 생성을 선택합니다.
4. 템플릿 선택 드롭다운 목록에서 템플릿을 선택한 다음 계획 생성을 선택합니다.
5. 백업 계획 이름을 입력합니다.
6. 계획 생성을 선택합니다.
7. 리소스 할당을 선택합니다.

리소스 할당을 시작하려면 일반 섹션에서

1. 리소스 할당 이름을 입력합니다.
2. 기본 역할을 선택하거나 IAM 역할을 선택합니다.

> **Note**
>
> IAM 역할을 선택할 경우, 할당하려는 모든 리소스를 백업할 권한이 있는지 확인하세요. 역할에서 백업 권한이 없는 리소스가 발견되면 백업 계획이 실패합니다.

리소스를 할당하려면 리소스 할당 섹션에서 리소스 선택 정의에 있는 두 가지 옵션 중 하나를 선택합니다.

- 모든 리소스 유형 포함. 이 옵션은 백업 계획에 할당된 현재 및 향후 AWS Backup지원되는 모든 리소스를 보호하도록 백업 계획을 구성합니다. 이 옵션을 사용하면 데이터 자산을 쉽고 빠르게 보호할 수 있습니다.

  이 옵션을 선택하면 선택에 따라 다음 단계에서 태그를 사용하여 선택 영역 구체화를 수행할 수 있습니다.
- 특정 리소스 유형 포함. 이 옵션을 선택할 경우, 아래의 단계에 따라 특정 리소스 유형 선택을 수행해야 합니다.

  1. 리소스 유형 선택 드롭다운 메뉴를 사용하여 하나 이상의 리소스 유형을 할당합니다.

     > **Important**
     >
     > RDS, Aurora, Nepune, DocumentDB는 동일한 Amazon 리소스 이름(ARN)을 공유합니다. AWS Backup 는 사용하여 이러한 리소스 유형 중 하나를 관리하도록 옵트인하면 백업 계획에 리소스를 할당할 경우 모든 리소스 유형을 옵트인합니다. 선택 범위를 좁히려면 태그와 조건 연산자를 사용하세요.

     작업을 마치면 AWS Backup 선택한 리소스 유형 목록과 선택한 각 리소스 유형의 모든 리소스를 보호하는 기본 설정이 표시됩니다.
  2. 선택한 리소스 유형에서 특정 리소스를 제외하려는 경우, 선택에 따라 다음 작업을 수행할 수 있습니다.

     1. 리소스 선택 드롭다운 메뉴를 사용하여 기본 옵션을 선택 취소합니다.
     2. 백업 계획에 할당할 특정 리소스를 선택합니다.
  3. 선택한 리소스 유형에서 특정 리소스 ID 제외를 선택할 수도 있습니다. 여러 리소스 중에서 하나 또는 몇 개의 리소스를 제외하려는 경우 이 옵션을 사용하세요. 이렇게 하면 이전 단계에서 많은 리소스를 선택하는 것보다 작업 속도가 빠를 수 있기 때문입니다. 먼저 리소스 유형을 포함해야 해당 리소스 유형에서 리소스를 제외할 수 있습니다. 다음 단계를 사용하여 리소스 ID를 제외하십시오.

     1. 선택한 리소스 유형에서 특정 리소스 ID 제외 아래에서 리소스 유형 선택을 사용하여 포함한 리소스 유형 중에서 하나 이상의 리소스 유형을 선택합니다.
     2. 각 리소스 유형에 대해 리소스 선택 메뉴를 사용하여 제외할 리소스를 하나 이상 선택합니다.

이전에 선택한 항목 외에도, 선택에 따라 태그를 사용하여 선택 영역 구체화 기능을 사용하여 훨씬 더 세분화된 선택을 할 수 있습니다. 이 기능을 사용하면 태그를 사용하여 리소스의 하위 집합을 포함하도록 현재 선택 영역을 구체화할 수 있습니다.

태그는 특정 리소스에 할당할 수 있는 키-값 페어로, 리소스를 식별, 구성, 필터링하는 데 도움이 됩니다. 태그는 대/소문자를 구분합니다. 자세한 내용은 AWS 일반 참조에서 AWS 리소스 태그 지정을 참조하세요.

두 개 이상의 태그를 사용하여 선택 영역을 좁히면 AND 조건이 됩니다. 예를 들어, `env: prod` 및 `role: application`이라는 두 가지 태그를 사용하여 선택 영역을 구체화할 경우 두 가지 태그가 모두 포함된 리소스만 백업 계획에 할당됩니다.

태그를 사용하여 선택 영역을 구체화하려면

1. 태그를 사용하여 선택 영역 구체화 드롭다운 목록에서 키를 선택합니다.
2. 드롭다운 목록에서 값의 조건을 선택합니다.
   - 값은 다음 입력, 즉 키-값 페어의 값을 나타냅니다.
   - 조건은 `Equals`, `Contains`, `Begins with`, `Ends with` 또는 이러한 조건의 역인 `Does not equal`, `Does not contain`, `Does not begin with`, `Does not end with`일 수 있습니다.
3. 드롭다운 목록에서 값을 선택합니다.
4. 다른 태그를 사용하여 더 구체화하려면 태그 추가를 선택합니다.

프로그래밍 방식으로 리소스 할당

JSON 문서에서 리소스 배정을 정의할 수 있습니다. 이 리소스 할당 샘플은 모든 Amazon EC2 인스턴스를 백업 계획 *BACKUP-PLAN-ID*에 할당합니다.

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

이 JSON이 backup-selection.json으로 저장되어 있다고 가정한다면, 아래의 CLI 명령을 사용하여 이러한 리소스를 백업 계획에 할당할 수 있습니다.

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

다음은 해당 JSON 문서와 함께 제공되는 리소스 배정의 예시입니다. 이 표를 더 쉽게 읽을 수 있도록 예제에서는 "BackupPlanId", "SelectionName", "IamRoleArn" 필드를 생략했습니다. 와일드카드 *는 공백이 아닌 0개 이상의 문자를 나타냅니다.

Example 예: 내 계정의 모든 리소스 선택

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ]
  }
}
```

Example 예: 내 계정의 모든 리소스를 선택하고 EBS 볼륨은 제외

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example 예: 태그가 지정된 모든 리소스를 선택하고 EBS "backup":"true" 볼륨은 제외

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
```

```
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example 예: 모두 및 로 태그가 지정된 모든 EBS 볼륨 및 RDS DB 인스턴스를 선택합니다. "backup":"true""stage":"prod"

부울 산술은 IAM 정책의 산술과 비슷합니다. 여기에는 부울 OR을 사용하여 결합된 "Resources"의 리소스 및 부울 AND를 사용하여 결합된 "Conditions"의 리소스가 포함됩니다.

해당하는 Aurora, Neptune 또는 DocumentDB 리소스가 없으므로 "Resources" 표현식 "arn:aws:rds:*:*:db:*"는 RDS DB 인스턴스만 선택합니다.

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Example 예: 태그가 있지만 태그는 지정되지 않은 모든 EBS 볼륨 및 RDS 인스턴스 선택
"backup":"true""stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 예: 태그가 지정된 모든 리소스와 해당 단어로 "key1""include" 시작하지만 이 단어로 시작하지는 않는 값 "key2" 및 해당 단어가 포함된 값을 선택합니다. "exclude"

문자열의 시작, 끝, 중간에 와일드카드 문자를 사용할 수 있습니다. 위 예제에서는 `include*` 및 `*exclude*`에 와일드카드 문자(*)를 사용한다는 점에 유의하세요. 이전 예제 `arn:aws:rds:*:*:db:*`처럼, 문자열 중간에 와일드카드 문자를 사용할 수도 있습니다.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/key1",
```

```
          "ConditionValue":"include*"
        }
      ],
      "StringNotLike":[
        {
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
  }
}
```

Example 예: FSx 파일 시스템과 RDS, Aurora, Neptune 및 DocumentDB 리소스를 "backup":"true" 제외하고 태그가 지정된 모든 리소스 선택

NotResources의 항목은 부울 OR을 사용하여 결합됩니다.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example 예: 태그와 임의의 값으로 태그가 지정된 모든 리소스 선택 "backup"

```
{
  "BackupSelection":{
```

```
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Example 예: 모든 FSx 파일 시스템, Aurora "my-aurora-cluster" 클러스터 및 태그가 지정된 모든 리소스 (태그가 지정된 "backup":"true" 리소스 제외) 선택 "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 예: 태그가 지정된 EBS 볼륨을 제외하고 **"backup":"true"** 태그로 태그가 지정된 모든 리소스 선택 **"stage":"test"**

두 개의 CLI 명령을 사용하여 이 리소스 그룹을 선택하기 위한 두 가지 선택 항목을 생성합니다. 첫 번째 선택 항목은 EBS 볼륨을 제외한 모든 리소스에 적용됩니다. 두 번째 선택 항목은 EBS 볼륨에 적용됩니다.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
```

```
        }
      ]
    }
  }
}
```

를 사용하여 리소스를 할당합니다. AWS CloudFormation

이 end-to-end AWS CloudFormation 템플릿은 리소스 배정, 백업 계획 및 대상 백업 보관소를 생성합니다.

- 이름이 *CloudFormationTestBackupVault*지정된 백업 저장소
- 이름이 *CloudFormationTestBackupPlan*지정된 백업 계획 이 계획은 두 가지 백업 규칙이 포함된 두 가지 백업 규칙을 실행합니다. 두 가지 규칙 모두 매일 정오 12시(UTC)에 백업을 수행하고 210일 동안 백업을 보존합니다.
- 이름이 *BackupSelectionName*지정된 리소스 선택
- • 리소스 할당은 다음 리소스를 백업합니다.
  - 키-값 페어 `backupplan:dsi-sandbox-daily`로 태그가 지정된 리소스.
  - `prod`로 태그가 지정된 리소스 또는 `prod/`로 시작하는 값.
- 리소스 할당은 다음 리소스를 백업하지 않습니다.
  - RDS, Aurora, Neptune 또는 DocumentDB 클러스터.
  - `test`로 태그가 지정된 리소스 또는 `test/`로 시작하는 값.

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
```

```
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
```

```
          - RuleName: !Ref RuleName2
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
```

```
        - ConditionKey: 'aws:ResourceTag/path'
          ConditionValue: prod
      StringNotEquals:
        - ConditionKey: 'aws:ResourceTag/path'
          ConditionValue: test
      StringLike:
        - ConditionKey: 'aws:ResourceTag/path'
          ConditionValue: prod/*
      StringNotLike:
        - ConditionKey: 'aws:ResourceTag/path'
          ConditionValue: test/*
```

리소스 할당에 대한 할당량

단일 리소스 할당에는 다음 할당량이 적용됩니다.

- 와일드카드가 포함되지 않은 Amazon 리소스 이름(ARN) 500개
- 와일드카드 표현식이 포함된 ARN 30개
- 조건 30개
- 리소스 할당당 태그 30개(및 태그당 무제한 리소스)

백업 계획 삭제

리소스의 모든 연결된 선택 사항이 삭제된 후에만 백업 계획을 삭제할 수 있습니다. 이러한 선택을 리소스 할당이라고도 합니다. 백업 계획을 삭제하기 전에 이러한 항목을 삭제하지 않은 경우 콘솔에 “백업 계획을 삭제하기 전에 관련 백업 계획 선택을 삭제해야 합니다.” 라는 오류 메시지가 표시됩니다. 콘솔을 사용하거나 사용하십시오 `DeleteBackupSelection`.

백업 계획을 삭제하면 계획의 현재 버전이 삭제됩니다. 현재 및 이전 버전(있는 경우)은 유지되지만 콘솔의 백업 계획 아래에는 더 이상 나열되지 않습니다.

> **Note**
>
> 백업 계획이 삭제되어도 기존 백업은 삭제되지 않습니다. 기존 백업을 제거하려면 백업 삭제의 단계를 사용하여 백업 저장소에서 기존 백업을 삭제하세요.

AWS Backup 콘솔을 사용하여 백업 계획을 삭제하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 백업 계획을 선택합니다.
3. 목록에서 백업 계획을 선택합니다.
4. 백업 계획과 연결된 리소스 할당을 선택합니다.
5. 삭제를 선택합니다.

백업 계획 업데이트

백업 계획을 생성한 후 계획을 편집할 수 있습니다. 예를 들어 태그를 추가, 편집 또는 삭제할 수 있으며 백업 규칙을 추가, 편집 또는 삭제할 수 있습니다. 백업 계획에 대한 모든 변경 사항은 백업 계획으로 생성된 기존 백업에는 아무런 영향을 주지 않습니다. 앞으로 생성되는 백업에만 변경 사항이 적용됩니다.

예를 들어, 백업 규칙의 보존 기간을 업데이트한 경우 업데이트 전에 생성된 백업의 보존 기간은 동일하게 유지됩니다. 이후 해당 규칙으로 생성되는 모든 백업에는 업데이트된 보존 기간이 반영됩니다.

계획을 만든 후에는 계획의 이름을 변경할 수 없습니다.

AWS Backup 콘솔을 사용하여 백업 계획을 편집하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택합니다.
3. 두 번째 창인 Backup plans에는 기존 백 플랜이 표시됩니다. 선택한 백업 계획의 세부 정보를 보려면 백업 계획 이름 열에서 밑줄이 그어진 링크를 선택합니다.
4. 백업 규칙을 편집하거나, 리소스 할당을 보거나, 백업 작업을 보거나, 태그를 관리하거나, Windows VSS 설정을 변경할 수 있습니다.
5. 백업 규칙을 업데이트하려면 백업 규칙의 이름을 선택합니다.

   태그 관리를 선택하여 태그를 추가하거나 삭제합니다.

   고급 백업 설정 옆의 편집을 선택하여 Windows VSS를 켜거나 끕니다.
6. 원하는 설정을 변경한 다음 저장을 선택합니다.

백업 저장소

> **Note**
>
> 2023년 8월 9일부터 논리적으로 AWS Backup 간격이 있는 저장소를 사용할 수 있는 미리 보기를 제공합니다.
> <# #### ##### aws-backup-vault-preview #### ## @amazon .com## ### #####.>
> 평가판 기간 도중 및 이후에 기능이 변경되거나 조정될 수 있습니다. 서비스가 GA(정식 출시)되면 평가판 중에 제공된 데이터 및 구성은 더 이상 사용할 수 없게 됩니다. AWS 는 평가판에서는 프로덕션 데이터 대신 테스트 데이터를 사용할 것을 권장합니다.

에서 AWS Backup백업 저장소는 백업을 저장하고 구성하는 컨테이너입니다.

백업 저장소를 만들 때는 이 저장소에 있는 일부 백업을 암호화하는 AWS Key Management Service (AWS KMS) 암호화 키를 지정해야 합니다. 다른 백업의 암호화는 해당 소스 AWS 서비스에서 관리합니다. 암호화에 대한 자세한 내용은 AWS의 백업 암호화 차트를 참조하세요.

계정에는 항상 기본 백업 저장소가 있습니다. 여러 백업 그룹에 대해 서로 다른 암호화 키 또는 액세스 정책이 필요한 경우 여러 개의 백업 저장소를 생성할 수 있습니다.

이 단원에서는 AWS Backup에서 백업 저장소를 관리하는 방법에 대한 개요를 제공합니다.

주제

- 논리적 에어 갭 처리 저장소(평가판)
- 백업 저장소 생성
- 백업 저장소에 대한 액세스 정책 설정
- AWS Backup 볼트 락
- 백업 저장소 삭제

논리적 에어 갭 처리 저장소(평가판)

> **Note**
>
> 2023년 8월 9일부터 논리적으로 에어 AWS Backup 갭이 있는 저장소를 사용할 수 있는 미리 보기를 제공합니다.
> <# #### ##### aws-backup-vault-preview #### ## @amazon .com## ### #####.>
> 평가판 기간 도중 및 이후에 기능이 변경되거나 조정될 수 있습니다. 서비스가 GA(정식 출시)되면 평가판 중에 제공된 데이터 및 구성은 더 이상 사용할 수 없게 됩니다. AWS 는 평가판에서는 프로덕션 데이터 대신 테스트 데이터를 사용할 것을 권장합니다.

개요

AWS Backup 백업 사본을 다른 저장소에 저장할 수 있는 보조 유형의 저장소를 미리 보는 중입니다. 논리적 에어 갭 처리 저장소는 백업 저장소의 보안 기능을 강화하는 것 외에도 다른 계정 및 조직에 대한 저장소 액세스를 공유할 수 있는 기능을 제공하는 특수 저장소입니다. 이를 통해 리소스의 신속한 복원이 필요한 사고 발생 시 복구 시간(RTO)을 더 빠르고 유연하게 조정할 수 있습니다.

논리적으로 에어 갭 저장소에는 추가 보호 기능이 탑재되어 있습니다. 각 저장소는 AWS 소유 키로 암호화되며 각 저장소에는 규정 준수 모드로 설정된 저장소 잠금이 있습니다.

필요한 경우, 조직 및 계정 간에 논리적 에어 갭 처리 저장소를 공유하도록 선택하여 저장소를 공유하는 계정에서 저장소에 저장된 백업을 복원하도록 할 수 있습니다.

평가판 기간에는 논리적 에어 갭 처리 저장소에 저장해도 추가 요금이 부과되지 않습니다. 논리적 에어 갭 처리 저장소에 있는 백업 복사본에는 요금이 청구되지 않더라도, 표준 백업 저장소 및 교차 리전 복사본의 백업에는 여전히 게시된 요금(가격 참조)으로 요금이 청구됩니다.

사용 사례

논리적 에어 갭 처리 저장소는 데이터 보호 전략의 일환으로 사용되는 보조 저장소입니다. 이 저장소는 다음과 같은 백업용 저장소가 필요한 경우, 조직의 보존 및 복구 기능을 향상하는 데 도움이 될 수 있습니다.

- 규정 준수 모드에서 저장소 잠금으로 자동 설정됨
- 백업을 생성한 계정이 아닌 다른 계정에서 공유하고 복원할 수 있는 백업이 포함됨
- 소유 키로 암호화된 상태로 제공됩니다. AWS

논리적 에어 갭 처리 저장소에서 지원되는 리소스는 다음과 같습니다.

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

논리적 에어 갭 처리 저장소의 평가판은 미국 동부(버지니아 북부) 리전에서만 사용할 수 있습니다. 이 기능은 현재 한 리전에서만 제공되므로, 이 평가판 기간에는 교차 리전 복사가 지원되지 않습니다.

표준 백업 저장소와 비교 및 대조

백업 저장소는 에서 사용되는 기본 및 표준 유형의 AWS Backup저장소입니다. 백업이 생성될 때 각 백업은 백업 저장소에 저장됩니다. 리소스 기반 정책을 할당하여 저장소에 저장된 백업을 관리(예: 저장소 내에 저장된 백업의 수명 주기)할 수 있습니다.

논리적 에어 갭 처리 저장소는 복구 시간(RTO) 단축을 위한 추가적인 보안 및 유연한 공유 기능을 갖춘 특수 저장소입니다. 이 저장소에는 표준 백업 저장소 내에 최초로 생성 및 저장되었던 백업 복사본이 저장됩니다.

백업 저장소는 의도한 사용자의 액세스를 제한하는 보안 메커니즘인 키로 암호화할 수 있습니다. 이러한 키는 고객이 AWS 관리하거나 관리할 수 있습니다. 또한 백업 저장소는 저장소 잠금을 통해 훨씬 더 안전하게 보호할 수 있습니다. 논리적 에어 갭 처리 저장소는 규정 준수 모드의 저장소 잠금이 탑재되어 있습니다.

초기 리소스를 생성할 때 AWS KMS 키를 수동으로 변경하거나 고객 관리 키 (CMK) 로 설정하지 않은 경우 백업을 논리적으로 간격이 있는 저장소에 복사할 수 없습니다.

기능	백업 저장소	논리적 에어 갭 처리 저장소(평가판)
백업 생성	백업이 생성되면 복구 시점으로 저장됨	백업은 생성 시 이 저장소에 저장되지 않음
백업 스토리지	리소스의 최초 백업 및 백업 복사본을 저장할 수 있음	다른 저장소의 백업 복사본을 저장할 수 있음

기능	백업 저장소	논리적 에어 갭 처리 저장소(평가판)
보안	선택적으로 키로 암호화할 수 있음 (고객 관리 또는 관리) AWS 선택에 따라 저장소 잠금을 사용하여 잠그기 가능	AWS 소유한 키로 암호화됩니다. 규정 준수 모드에서는 항상 저장소 잠금을 사용하여 잠김
공유 기능	정책 및 AWS Organizations를 통해 액세스를 관리할 수 있음 다음과 호환되지 않음 AWS Resource Access Manager	선택에 따라 AWS RAM을 사용하여 계정 간에 공유할 수 있음
복원	저장소를 소유한 동일한 계정으로 백업을 복원할 수 있음	저장소를 별도의 계정과 공유할 경우, 백업을 소유한 계정과는 다른 계정으로 백업을 복원할 수 있음
리전 구분	AWS Backup 운영 중인 모든 지역에서 사용 가능	평가판 기간에는 미국 동부(버지니아 북부) 리전에서만 사용 가능
리소스	AWS Backup 지원되는 모든 리소스가 포함된 백업을 저장할 수 있습니다.	Amazon EC2, Amazon EBS, Amazon EFS, Amazon S3 또는 Amazon RDS 데이터가 포함된 백업을 저장할 수 있음

콘솔에서 논리적 에어 갭 처리 저장소 생성

Important

저장소를 생성한 후에는 저장소 이름, 저장소 유형, 최소 및 최대 보존 기간을 변경할 수 없으며 저장소 잠금도 제거할 수 없습니다.

서비스가 일반 사용 가능 상태가 되면 미리 보기 중에 제공된 데이터 및 구성을 더 이상 사용할 수 없게 됩니다. AWS 미리 보기에서는 프로덕션 데이터 대신 테스트 데이터를 사용할 것을 권장합니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 저장소를 선택합니다.
3. 두 가지 유형의 저장소가 모두 표시됩니다. 새 저장소 생성을 선택합니다.
4. 백업 저장소의 이름을 입력합니다. 저장소에 저장할 내용이 잘 반영되도록 저장소의 이름을 지정하거나 필요한 백업을 보다 쉽게 검색할 수 있도록 만들 수 있습니다. 예를 들어, 이름을 `FinancialBackups`로 지정할 수 있습니다.
5. 논리적 에어 갭 처리 저장소의 라디오 버튼을 선택합니다.
6. 최소 보존 기간을 설정합니다.

   이 값(일, 월 또는 년)은 이 저장소에 백업을 보존할 수 있는 가장 짧은 기간입니다. 보존 기간이 이 값보다 짧은 백업은 이 저장소에 복사할 수 없습니다.
7. 최대 보존 기간을 설정합니다.

   이 값(일, 월 또는 년)은 이 저장소에 백업을 보존할 수 있는 가장 긴 기간입니다. 보존 기간이 이 값보다 큰 백업은 이 저장소에 복사할 수 없습니다.
8. (선택 사항) 논리적 에어 갭 처리 저장소를 검색하고 식별하는 데 도움이 되는 태그를 추가합니다. 예를 들어, `BackupType:Financial` 태그를 추가할 수 있습니다.
9. 저장소 생성을 선택합니다.
10. 설정을 검토합니다. 모든 설정이 의도한 대로 표시되면 논리적 에어 갭 처리 저장소 생성을 선택합니다.
11. 콘솔에서 새 저장소의 세부 정보 페이지로 이동합니다. 저장소 세부 정보가 예상과 같은지 확인합니다.

콘솔에서 논리적 에어 갭 처리 저장소의 세부 정보 보기

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 저장소를 선택합니다.
3. 저장소의 설명 아래에는 이 계정이 소유한 저장소와 이 계정으로 공유하는 저장소라는 두 가지 목록이 있습니다. 저장소를 보려면 원하는 탭을 선택합니다.

4. 저장소 이름 아래에서 저장소 이름을 클릭하여 세부 정보 페이지를 엽니다. 요약, 복구 시점, 보호된 리소스, 계정 공유, 액세스 정책, 태그 세부 정보를 볼 수 있습니다.

콘솔의 표준 백업 저장소에서 논리적 에어 갭 처리 저장소로 복사

논리적 에어 갭 처리 저장소는 백업 계획의 복사 작업 대상 또는 온디맨드 복사 작업의 대상만 될 수 있습니다.

복사 작업을 시작하려면 다음과 같은 요소가 있어야 합니다.

- 백업 저장소
- 논리적 에어 갭 처리 저장소
- Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3 또는 Amazon EFS 데이터가 포함된 백업
- 복사본을 생성하는 데 사용되는 역할을 위한 `kms:CreateGrant` 권한
- 논리적으로 빈틈이 있는 저장소에 복사 작업의 일환으로 AWS 관리 키로 암호화된 백업은 없습니다.

위 내용을 확인한 후

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 저장소를 선택합니다.
3. 저장소 세부 정보 페이지에는 해당 저장소 내의 모든 복구 시점이 표시됩니다. 복사하려는 복구 시점 옆에 체크 표시를 합니다.
4. 작업을 선택한 다음, 드롭다운 메뉴에서 복사를 선택합니다.
5. 다음 화면에서 대상의 세부 정보를 입력합니다.
    a. 리전을 미국 동부(버지니아 북부)로 설정해야 합니다.
    b. 대상 백업 저장소 드롭다운 메뉴에 적합한 대상 저장소가 표시됩니다. 유형이 `logically air-gapped vault`인 항목을 선택합니다.
6. 모든 세부 정보가 기본 설정으로 설정되면 복사를 선택합니다.

콘솔의 작업 페이지에서 복사 작업을 선택하여 현재의 복사 작업을 볼 수 있습니다.

자세한 내용은 백업 복사, 교차 리전 백업, 교차 계정 백업을 참조하세요.

콘솔에서 논리적 에어 갭 처리 저장소 공유

> **Note**
>
> 특정 IAM 권한이 있는 계정만 계정 공유를 공유하고 관리할 수 있습니다.

논리적으로 공백이 있는 저장소를 사용자가 지정한 다른 계정과 공유하는 AWS RAM 데 사용할 수 있습니다. 을 (를) 사용하여 AWS RAM공유하려면 다음 사항을 갖추어야 합니다.

- 액세스할 수 있는 두 개 이상의 계정 AWS Backup
- 공유하려는 계정에 필요한 RAM 권한이 있습니다. 이 절차를 수행하려면 `ram:CreateResourceShare` 권한이 필요합니다. `AWSResourceAccessManagerFullAccess` 정책에는 모든 필요한 RAM 관련 권한이 포함되어 있습니다.
- 논리적 에어 갭 처리 저장소 1개 이상

논리적 에어 갭 처리 저장소를 공유하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 저장소를 선택합니다.
3. 저장소의 설명 아래에는 이 계정이 소유한 저장소와 이 계정으로 공유하는 저장소라는 두 가지 목록이 있습니다. 저장소를 보려면 원하는 목록을 선택합니다.
4. 저장소 이름 아래에서 논리적 에어 갭 처리 저장소의 이름을 클릭하여 세부 정보 페이지를 엽니다.
5. 계정 공유 창에 저장소를 공유 중인 계정이 표시됩니다.
6. 다른 계정과 공유를 시작하거나 이미 공유 중인 계정을 편집하려면 공유 관리를 선택합니다.

AWS RAM 공유 관리를 선택하면 콘솔이 열립니다. RAM을 사용하여 리소스를 공유하는 단계는 AWS AWS RAM에 리소스 공유 만들기를 참조하십시오.

적절한 권한이 있는지 확인합니다. 백업 관리자 IAM 정책 [AWSBackupFullAccess] 및 Backup Operator IAM 정책 [AWSBackupOperatorAccess] 에는 공유 계정을 보는 데 필요한 권한이 포함되어 있지만 공유하는 데 사용하는 역할에는 RAM에서 계정을 공유하기 위한 Resource Access Manager 쓰기 권한 (예:) 이 필요합니다. `ram:CreateResourceShare`

공유를 수신하기 위한 초대를 수락하도록 초대된 계정은 12시간 이내에 초대를 수락해야 합니다. AWS RAM 사용 설명서의 리소스 공유 초대 수락 및 거부를 참조하세요.

공유 단계가 완료되고 수락되면 계정 공유 = "공유함 - 아래 계정 공유 표 참조" 아래에 저장소 요약 페이지가 표시됩니다.

콘솔을 사용하여 논리적 에어 갭 처리 저장소에서 백업 복원

논리적 에어 갭 처리 저장소에 저장된 백업을 저장소를 소유한 계정이나 저장소를 공유한 계정으로 복원할 수 있습니다.

복구 시점을 복원하는 방법에 대한 자세한 내용은 백업 복원을 참조하세요.

콘솔을 사용하여 논리적 에어 갭 처리 저장소 삭제

> **Important**
>
> 서비스가 일반 사용 가능 상태가 되면 미리 보기 중에 제공된 데이터 및 구성을 더 이상 사용할 수 없게 됩니다. AWS 미리 보기에서는 프로덕션 데이터 대신 테스트 데이터를 사용할 것을 권장합니다.

저장소를 삭제하려면 백업 저장소 삭제를 참조하세요. 저장소에 백업(복구 시점)이 아직 포함되어 있는 경우 저장소를 삭제할 수 없습니다. 삭제 작업을 시작하기 전에 저장소에 백업이 남아 있지 않은지 확인하세요.

CLI/API를 통한 논리적 에어 갭 처리 저장소

를 AWS CLI 사용하여 논리적으로 에어 갭이 있는 저장소의 작업을 프로그래밍 방식으로 수행할 수 있습니다. 각 CLI는 해당 CLI가 시작된 AWS 서비스에 따라 다릅니다. 공유와 관련된 명령은 앞에 `aws ram`이 추가되고, 다른 모든 명령은 앞에 `aws backup`이 추가됩니다.

생성

아래의 CLI 명령 샘플 `CreateLogicallyAirGappedBackupVault`를 수정하여 논리적 에어 갭 처리 백업 저장소를 생성할 수 있습니다.

```
aws backup create-logically-air-gapped-backup-vault \
--region us-east-1 \
--backup-vault-name sampleName \
--min-retention-days 7 \
--max-retention-days 35 \
--creator-request-id 123456789012-34567-8901 // optional
```

세부 정보 보기

아래의 CLI 명령 샘플 `DescribeBackupVault`를 수정하여 저장소에 대한 세부 정보를 얻을 수 있습니다.

```
aws backup describe-backup-vault \
--region us-east-1  \
--backup-vault-name testvaultname
```

공유

> **Note**
>
> 충분한 IAM 권한이 있는 계정만 계정 공유를 공유하고 관리할 수 있습니다.

사용자가 리소스를 공유하는 데 도움이 되는 서비스인 AWS Resource Access Manager(RAM)을 통해 논리적 에어 갭 처리 저장소를 공유할 수 있습니다.

AWS RAM CLI 명령을 사용합니다. `create-resource-share` 이 명령에 대한 액세스는 충분한 권한이 있는 관리자 계정에만 제공됩니다. CLI 단계는 Creating a resource share in AWS RAM을 참조하세요.

1~4단계는 논리적 에어 갭 처리 저장소를 소유한 계정을 사용하여 수행됩니다. 5~8단계는 논리적 에어 갭 처리 저장소를 공유할 계정을 사용하여 수행됩니다.

1. 소유한 계정으로 로그인하거나, 소스 계정에 액세스할 수 있는 충분한 보안 인증을 가진 조직의 사용자에게 이 단계를 완료해 달라고 요청합니다.
   - 이전에 리소스 공유를 생성했고 추가적인 리소스를 추가하려는 경우, 새 저장소의 ARN과 함께 CLI `associate-resource-share`를 대신 사용하세요.
2. RAM을 통해 공유할 수 있는 충분한 권한이 있는 역할의 보안 인증을 가져옵니다. 이를 CLI에 입력합니다.
   - 이 절차를 수행하려면 `ram:CreateResourceShare` 권한이 필요합니다. AWSResourceAccessManagerFullAccess정책에는 모든 RAM 관련 권한이 포함됩니다.
3. 사용. create-resource-share
   a. 논리적 에어 갭 처리 저장소의 ARN을 포함합니다.

b. 입력 예

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

출력 예:

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. 출력에 리소스 공유 ARN을 복사합니다(이후 단계에 필요). 공유를 수신하기 위해 초대하는 계정의 운영자에게 ARN을 제공합니다.
5. 리소스 공유 ARN 받기

   a. 1~4단계를 수행하지 않았다면 수행한 resourceShareArn 사람으로부터 구하십시오.

   b. 예제: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`

6. CLI에서는 수신자 계정의 보안 인증을 수임합니다.
7. get-resource-share-invitations를 사용하여 리소스 공유 초대를 받습니다. 자세한 내용은 AWS RAM 사용 설명서의 Accepting and rejecting invitations를 참조하세요.
8. 대상(복구) 계정의 초대를 수락합니다.

   - accept-resource-share-invitation을 사용합니다(reject-resource-share-invitation도 사용 가능).

나열

CLI 명령 ListBackupVaults를 수정하여 계정이 소유하고 있고 계정에 존재하는 모든 저장소를 나열할 수 있습니다.

```
aws backup list-backup-vaults \
--region us-east-1
```

논리적 에어 갭 처리 저장소만 나열하려면 파라미터를 추가합니다.

```

--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

계정과 공유된 저장소를 나열하려면 다음을 사용합니다.

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

Copy

논리적 에어 갭 처리 저장소는 백업의 복사 작업을 위한 대상만 될 수 있으며, 최초 백업 작업의 대상이 될 수 없습니다. StartCopyJob을 사용하여 백업 저장소의 기존 백업을 논리적 에어 갭 처리 저장소에 복사할 수 있습니다.

논리적 에어 갭 처리 저장소에 대한 복사 작업을 생성하는 데 사용되는 역할에는 `kms:CreateGrant` 권한이 포함되어야 합니다.

CLI 입력 샘플:

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

복원

논리적 에어 갭 처리 저장소에서 백업이 사용자 계정으로 공유되면 StartRestoreJob을 사용하여 해당 백업을 복원할 수 있습니다. CLI 입력 샘플:

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

삭제

아래의 CLI 명령 샘플 DeleteBackupVault를 사용하여 저장소를 삭제할 수 있습니다. 저장소는 저장소 내에 백업(복구 시점)이 없는 경우에만 삭제할 수 있습니다.

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

사용 가능한 기타 프로그래밍 옵션은 다음과 같습니다.

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

백업 저장소 생성

백업 계획을 생성하거나 백업 작업을 시작하기 전에 저장소를 최소 한 개 이상 생성해야 합니다.

에서 AWS Backup 콘솔을 처음 사용하면 콘솔이 자동으로 기본 보관소를 생성합니다. AWS 리전

하지만 AWS CLI, AWS SDK 또는 AWS CloudFormation를 AWS Backup 통해 사용하는 경우에는 기본 보관소가 생성되지 않습니다. 저장소를 직접 생성해야 합니다.

필요한 권한

를 사용하여 AWS Backup백업 저장소를 만들려면 다음 권한이 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource":
 "arn:aws:kms:region:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:region:444455556666:backup-vault:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

백업 저장소 생성(콘솔)

AWS Backup 콘솔을 사용하여 백업 저장소를 만드는 step-by-step 방법에 대한 지침은 시작하기 안내서를 참조하십시오3단계: 백업 저장소 생성.

백업 저장소 생성(프로그래밍 방식)

다음 AWS Command Line Interface 명령은 백업 저장소를 생성합니다.

```
aws backup create-backup-vault --backup-vault-name test-vault
```

백업 저장소에 다음과 같은 구성을 지정할 수도 있습니다.

백업 저장소 이름

백업 저장소 이름은 대/소문자를 구분합니다. 2~50자의 영숫자 문자, 하이픈 또는 밑줄로 구성되어야 합니다.

AWS KMS 암호화 키

AWS KMS 암호화 키는 이 백업 저장소의 백업을 보호합니다. 기본적으로 AWS Backup 은 aws/backup 별칭으로 마스터 키를 생성합니다. 해당 키를 선택하거나 계정의 다른 키를 선택할 수 있습니다(CLI를 통해 교차 계정 KMS 키를 사용할 수 있음).

AWS Key Management Service 개발자 안내서의 키 생성 절차에 따라 새 암호화 키를 생성할 수 있습니다.

백업 저장소를 생성하고 AWS KMS 암호화 키를 설정한 후에는 더 이상 해당 백업 저장소의 키를 편집할 수 없습니다.

AWS Backup 저장소에 지정된 암호화 키는 특정 리소스 유형의 백업에 적용됩니다. 백업 암호화에 대한 자세한 내용은 보안의 내 백업을 위한 암호화 AWS Backup 단원을 참조하십시오. 다른 모든 리소스 유형의 백업은 소스 리소스를 암호화하는 데 사용되는 키를 사용하여 백업됩니다.

백업 저장소 태그

이러한 태그는 백업 저장소를 쉽게 구성하고 추적할 수 있도록 백업 저장소 자체와 연결됩니다.

백업 저장소에 대한 액세스 정책 설정

를 사용하면 백업 저장소 및 백업 저장소에 포함된 AWS Backup리소스에 정책을 할당할 수 있습니다. 정책을 할당하면 사용자에게 백업 계획 및 온디맨드 백업을 생성할 수 있는 액세스 권한을 부여하는 등의 작업을 수행할 수 있지만 복구 시점이 생성된 후에는 삭제할 수 있는 기능을 제한할 수 있습니다.

정책 사용에 대한 자세한 내용을 알아보려면 IAM 사용 설명서의 자격 증명 기반 정책 및 리소스 기반 정책을 참조하세요. 태그를 사용하여 액세스를 제어할 수도 있습니다.

AWS Backup Vault로 작업할 때 다음 예제 정책을 지침으로 사용하여 리소스에 대한 액세스를 제한할 수 있습니다. 다른 IAM 기반 정책과 달리 AWS Backup 액세스 정책은 키에 와일드카드를 지원하지 않습니다. `Action`

다양한 리소스 유형에 대한 복구 시점을 식별하는 데 사용할 수 있는 Amazon 리소스 이름(ARN) 목록은 AWS Backup 리소스 ARN에서 리소스별 복구 시점 ARN을 참조하십시오.

저장소 액세스 정책은 API에 대한 사용자 액세스만 제어합니다. AWS Backup Amazon Elastic Block Store(Amazon EBS) 및 Amazon Relational Dabase Service(Amazon RDS) 스냅샷과 같은 일부 백업 유형도 해당 서비스의 API를 사용하여 액세스할 수 있습니다. API에 대한 액세스를 제어하는 별도의 액세스 정책을 IAM에 생성하면 이러한 백업 유형에 대한 액세스를 완전히 제어할 수 있습니다.

AWS Backup Vault의 액세스 정책에 관계없이 이외의 작업에 대한 교차 계정 액세스는 `backup:CopyIntoBackupVault` 거부됩니다. 즉, AWS Backup 참조되는 리소스의 계정과 다른 계정의 다른 요청은 거부됩니다.

주제

- 백업 저장소에서 리소스 유형에 대한 액세스 거부
- 백업 저장소에 대한 액세스 거부
- 백업 저장소에서 복구 시점 삭제에 대한 액세스 거부

백업 저장소에서 리소스 유형에 대한 액세스 거부

이 정책은 백업 저장소의 모든 Amazon EBS 스냅샷에 대해 지정된 API 작업에 대한 액세스를 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
```

```
                "backup:StartRestoreJob"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

백업 저장소에 대한 액세스 거부

이 정책은 백업 저장소를 대상으로 지정된 API 작업에 대한 액세스를 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

백업 저장소에서 복구 시점 삭제에 대한 액세스 거부

저장소에 대한 액세스 및 저장소에 저장된 복구 시점 삭제 기능은 사용자에게 부여된 액세스 권한에 따라 결정됩니다.

다음 단계에 따라 백업 저장소에서 백업을 삭제하지 못하도록 해당 백업 저장소에 리소스 기반 액세스 정책을 생성합니다.

백업 저장소에 리소스 기반 액세스 정책을 생성하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 백업 저장소를 선택합니다.
3. 목록에서 백업 저장소를 선택합니다.
4. 액세스 정책 섹션에 다음 JSON 예를 붙여 넣습니다. 이 정책을 사용하면 보안 주체가 아닌 사용자가 대상 백업 저장소에서 복구 시점을 삭제할 수 없습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:userId": [
                       "AAAAAAAAAAAAAAAAAAAAA:",
                       "BBBBBBBBBBBBBBBBBBBBB",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

ARN을 사용하여 목록 IAM ID를 허용하려면 다음 예제의 `aws:PrincipalArn` 전역 조건 키를 사용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
```

```
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                       "arn:aws:iam::112233445566:role/mys3role",
                       "arn:aws:iam::112233445566:user/shaheer",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

IAM 엔터티의 고유 ID 가져오기에 대한 자세한 내용은 IAM 사용 설명서의 고유 식별자 가져오기를 참조하세요.

이를 특정 리소스 유형으로 제한하려는 경우, `"Resource": "*"` 대신 거부할 복구 시점 유형을 명시적으로 포함하면 됩니다. 예를 들어 Amazon EBS 스냅샷의 경우 리소스 유형을 다음으로 변경합니다.

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. 정책 연결을 선택합니다.

AWS Backup 볼트 락

> **Note**
>
> AWS Backup 코하셋 어소시에이츠는 SEC 17a-4, CFTC 및 FINRA 규정이 적용되는 환경에서 볼트 락을 사용할 수 있는지 평가했습니다. AWS Backup Vault Lock이 이러한 규정과 어떤 관련이 있는지에 대한 자세한 내용은 코하셋 어소시에이츠 규정 준수 평가를 참조하십시오.

AWS Backup 저장소 잠금은 백업 저장소의 선택적 기능으로, 백업 저장소에 대한 추가 보안 및 제어 기능을 제공하는 데 유용할 수 있습니다. 규정 준수 모드에서 잠금이 활성화되어 있고 유예 시간이 끝

나면 고객, 계정/데이터 소유자 또는 AWS가 저장소 구성을 변경하거나 삭제할 수 없습니다. 각 저장소에는 저장소 잠금이 하나씩 준비된 상태일 수 있습니다.

AWS Backup 보존 기간이 만료될 때까지 백업을 사용할 수 있도록 합니다. 모든 사용자 (루트 사용자 포함) 가 백업을 삭제하거나 잠긴 저장소의 수명 주기 속성을 변경하려고 AWS Backup 하면 작업이 거부됩니다.

- 거버넌스 모드에서 잠긴 저장소는 충분한 IAM 권한을 가진 사용자가 잠금을 제거할 수 있습니다.
- 규정 준수 모드에서 잠긴 저장소는 쿨링 오프 기간("유예 시간") 이 만료되면 삭제할 수 없습니다. 유예 시간 동안에도 저장소 잠금을 제거하고 잠금 구성을 변경할 수 있습니다.

저장소 잠금 모드

저장소 잠금을 생성할 경우, 거버넌스 모드 또는 규정 준수 모드라는 두 가지 모드 중에서 하나를 선택할 수 있습니다. 거버넌스 모드는 충분한 IAM 권한을 가진 사용자만 저장소를 관리할 수 있도록 하기 위한 모드입니다. 거버넌스 모드는 지정된 담당자만 백업 저장소를 변경할 수 있도록 보장하므로, 조직이 거버넌스 요구 사항을 충족하는 데 도움이 됩니다. 규정 준수 모드는 데이터 보존 기간이 완료될 때까지 저장소(및 더 나아가 저장소의 콘텐츠)가 삭제되거나 변경되지 않아야 하는 백업 저장소를 위한 모드입니다. 규정 준수 모드의 저장소가 잠기면 변경이 불가능합니다. 즉, 잠금을 제거할 수 없습니다.

거버넌스 모드에서 잠긴 저장소는 적절한 IAM 권한이 있는 사용자가 관리하거나 삭제할 수 있습니다.

규정 준수 모드의 저장소 잠금은 다른 사용자 또는 AWS가 변경하거나 삭제할 수 없습니다. 규정 준수 모드의 저장소 잠금에는 저장소가 잠겨서 변경 불가능해지기 전까지 설정한 유예 시간이 있습니다.

저장소 잠금의 이점

AWS Backup Vault Lock은 다음과 같은 여러 가지 이점을 제공합니다.

- 백업 저장소에 저장하고 생성하는 모든 백업을 위한 WORM(write-once, read-many) 구성.
- 백업 저장소의 백업(복구 시점)이 실수로 또는 악의적으로 삭제되지 않도록 보호하는 추가적인 방어 계층입니다.
- 보존 기간 적용: 권한이 있는 사용자 (AWS 계정 루트 사용자 포함) 의 조기 삭제를 방지하고 조직의 데이터 보호 정책 및 절차를 준수합니다.

콘솔을 사용하여 백업 저장소 잠그기

Backup 콘솔을 사용하여 AWS Backup Vault에 저장소 잠금을 추가할 수 있습니다.

백업 저장소에 저장소 잠금을 추가하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 저장소를 선택합니다. 백업 저장소 아래에 중첩된 저장소 잠금이라는 링크를 클릭합니다.
3. 저장소 잠금 작동 방식 또는 저장소 잠금 아래에서 + 저장소 잠금 생성을 클릭합니다.
4. 저장소 잠금 세부 정보 창에서 잠금을 적용할 저장소를 선택합니다.
5. 저장소 잠금 모드에서 저장소를 잠글 모드를 선택합니다. 모드 선택에 대한 자세한 내용은 이 페이지 앞 부분의 저장소 잠금 모드를 참조하세요.
6. 보존 기간의 경우 최소 및 최대 보존 기간을 선택합니다(보존 기간은 선택 사항). 저장소에 생성된 새로운 백업 및 복사 작업이 사용자가 설정한 보존 기간에 맞지 않으면 해당 작업은 실패합니다. 이러한 기간은 저장소에 이미 있는 복구 시점에는 적용되지 않습니다.
7. 규정 준수 모드를 선택한 경우 저장소 잠금 시작 날짜라는 섹션이 표시됩니다. 거버넌스 모드를 선택한 경우 이 섹션은 표시되지 않으며 이 단계를 건너뛸 수 있습니다.

   규정 준수 모드의 저장소 잠금에는 저장소 잠금이 생성된 시점부터 저장소 및 저장소의 잠금을 변경 불가능할 수 없게 될 때까지 쿨링 오프 기간이 있습니다. 이 기간(유예 시간이라고 함)을 선택하되, 최소 3일(72시간)이어야 합니다.

   > **Important**
   >
   > 유예 시간이 만료되면 저장소와 저장소의 잠금은 변경 불가능합니다. 다른 사용자나 AWS가 이를 변경하거나 삭제할 수 없습니다.

8. 구성 선택에 만족하면 저장소 잠금 생성을 클릭합니다.
9. 선택한 모드에서 이 잠금을 생성하도록 확인하려면 텍스트 상자에 `confirm`을 입력한 다음, 구성이 의도한 대로인지 확인하는 상자를 선택합니다.

단계를 성공적으로 완료하면 콘솔 상단에 "성공" 배너가 나타납니다.

프로그래밍 방식으로 백업 저장소 잠그기

AWS Backup 저장소 잠금을 구성하려면 API를 사용하십시오`PutBackupVaultLockConfiguration`. 포함할 파라미터는 사용하려는 저장소 잠금 모드에 따라

달라집니다. 거버넌스 모드에서 저장소 잠금을 생성하려는 경우에는 ChangeableForDays를 포함하지 마세요. 이 파라미터를 포함하면 규정 준수 모드에서 저장소 잠금이 생성됩니다.

다음은 규정 준수 모드 저장소 잠금 생성의 CLI 예제입니다.

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

다음은 거버넌스 모드 저장소 잠금 생성의 CLI 예제입니다.

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

네 가지 옵션을 구성할 수 있습니다.

1. **BackupVaultName**

   잠그려는 저장소의 이름입니다.

2. **ChangeableForDays**(규정 준수 모드에만 포함)

   이 매개변수는 규정 준수 모드에서 금고 잠금을 AWS Backup 생성하도록 지시합니다. 거버넌스 모드에서 잠금을 생성하려면 이 파라미터를 생략하세요.

   이 값은 일 단위로 표시됩니다. 3보다 크고 36,500보다 작은 숫자여야 합니다. 그렇지 않으면 오류가 반환됩니다.

   이 저장소 잠금을 생성한 후 지정된 날짜가 만료될 때까지는 DeleteBackupVaultLockConfiguration을 사용하여 저장소에서 저장소 잠금을 제거할 수 있습니다. 또는 이 기간 동안 PutBackupVaultLockConfiguration을 사용하여 구성을 변경할 수도 있습니다.

   이 파라미터에 의해 정해진 지정된 날짜 이후에는 백업 저장소를 변경할 수 없으며 삭제할 수 없습니다.

3. **MaxRetentionDays**(선택 사항)

이 값은 일 단위로 표시되는 숫자 값입니다. 이는 저장소가 복구 시점을 유지하는 최대 보존 기간입니다.

사용자가 선택하는 최대 보존 기간은 조직의 데이터 보존 정책과 일치해야 합니다. 조직에서 데이터를 일정 기간 동안 보존하도록 지시할 경우, 이 값을 해당 기간(일 단위)으로 설정할 수 있습니다. 예를 들어, 금융 또는 은행 데이터를 7년(윤년에 따라 약 2,557일) 동안 보관해야 할 수 있습니다.

지정하지 않으면 AWS Backup 저장소 잠금은 최대 보존 기간을 적용하지 않습니다. 지정된 경우, 수명 주기 보존 기간이 최대 보존 기간보다 긴 이 저장소로 백업 및 복사하는 작업은 실패합니다. 저장소 잠금의 생성 이전에 저장소에 이미 저장된 복구 시점은 영향을 받지 않습니다. 지정할 수 있는 최대 보존 기간은 36,500일(약 100년)입니다.

4. **`MinRetentionDays`**(선택 사항, 필수) CloudFormation

   이 값은 일 단위로 표시되는 숫자 값입니다. 이는 저장소가 복구 시점을 유지하는 최소 보존 기간입니다. 이 설정은 조직에서 데이터를 유지하는 데 필요한 시간으로 설정해야 합니다. 예를 들어, 규정이나 법률에 따라 데이터를 최소 7년 동안 보존해야 할 경우 일 단위의 값은 윤년에 따라 약 2,557일이 됩니다.

   지정하지 않을 경우 AWS Backup Vault Lock은 최소 보존 기간을 적용하지 않습니다. 지정된 경우, 수명 주기 보존 기간이 최소 보존 기간보다 짧은 이 저장소로 백업 및 복사하는 작업은 실패합니다. AWS Backup 저장소 잠금 이전에 저장소에 이미 저장된 복구 지점은 영향을 받지 않습니다. 지정할 수 있는 가장 짧은 최소 보존 기간은 1일입니다.

백업 저장소의 AWS Backup 저장소 잠금 구성을 검토하십시오.

전화 `DescribeBackupVault` 또는 `ListBackupVaults` API를 통해 언제든지 저장소의 AWS Backup 저장소 잠금 세부 정보를 검토할 수 있습니다.

백업 저장소에 저장소 잠금을 적용했는지 확인하려면 `DescribeBackupVault`를 호출하고 `Locked` 속성을 확인합니다. 다음 예와 같이 백업 AWS Backup 저장소에 저장소 잠금을 적용한 경우 `"Locked": true`

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
```

```
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

앞의 출력은 다음 옵션을 확인합니다.

1. Locked이 백업 AWS Backup 저장소에 저장소 잠금을 적용했는지 여부를 나타내는 불리언입니다. True AWS Backup 저장소 잠금으로 인해 저장소에 저장된 복구 지점에 대한 삭제 또는 업데이트 작업이 실패한다는 의미입니다 (아직 보존 유예 기간 내에 있는지 여부와 관계 없음).
2. LockDate는 쿨링 오프 유예 기간이 종료되는 날짜 및 시간(UTC)입니다. 이 기간이 지나면 이 저장소의 잠금을 삭제하거나 변경할 수 없습니다. 일반적으로 제공되는 시간 변환기를 사용하여 이 문자열을 현지 시간으로 변환합니다.

아래의 예제처럼 "Locked":false인 경우, 저장소 잠금을 적용하지 않았거나 이전 저장소 잠금이 삭제된 것입니다.

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

유예 시간 중에 저장소 잠금 제거(규정 준수 모드)

콘솔을 사용하여 유예 기간 (저장소를 잠근 후 남은 시간LockDate) 에 저장소 잠금을 삭제하려면 AWS Backup

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 왼쪽 탐색 메뉴의 내 계정에서 백업 저장소를 클릭한 다음, 백업 저장소 잠금을 클릭합니다.
3. 제거하려는 저장소 잠금을 클릭한 다음 저장소 잠금 관리를 클릭합니다.
4. 저장소 잠금 삭제를 클릭합니다.
5. 저장소 잠금을 삭제할 것인지 확인하라고 묻는 경고 상자가 나타납니다. 텍스트 상자에 `confirm`을 입력한 다음 확인을 클릭합니다.

단계를 성공적으로 모두 완료하면 콘솔 화면의 상단에 성공 배너가 나타납니다.

CLI 명령을 사용하여 유예 시간 중에 저장소 잠금을 삭제하려면 아래의 CLI 예제처럼 `DeleteBackupVaultLockConfiguration`을 사용하세요.

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

AWS 계정 잠긴 금고로 닫기

백업 저장소가 들어 AWS 계정 있는 계정을 AWS 폐쇄하고 백업을 그대로 유지한 상태로 90일 동안 계정을 AWS Backup 정지하는 경우 90일 동안 계정을 다시 열지 않으면 Vault Lock이 설치되어 있더라도 AWS Backup 백업 저장소의 콘텐츠가 AWS 삭제됩니다.

추가 보안 고려 사항

AWS Backup Vault Lock은 심층적인 데이터 보호 방어에 보안을 한층 더 강화합니다. 저장소 잠금은 다음과 같은 다른 보안 기능과 결합할 수 있습니다.

- 복구 시점의 암호화
- AWS Backup 저장소 및 복구 지점 액세스 정책을 통해 저장소 수준에서 권한을 부여하거나 거부할 수 있습니다.
- AWS Backup AWS 지원되는 서비스별로 백업 및 복원 권한을 부여하거나 거부할 수 있는 고객 관리형 정책 라이브러리를 포함한 보안 모범 사례
- AWS Backup Audit Manager를 사용하면 정의한 제어 목록을 기준으로 백업에 대한 규정 준수 검사를 자동화할 수 있습니다.

  의도한 리소스가 볼트 잠금으로 보호되도록 AWS Backup Audit Manager의 백업은 AWS Backup Vault Lock으로 보호됩니다. 컨트롤에 대해 API를 사용하여 프레임워크 만들기 AWS Backup의 내용을 참조할 수 있습니다.

- 리소스를 비활성화하는 메커니즘은 리소스를 복원하는 기능에 영향을 미칠 수 있습니다. 잠긴 저장소에서는 여전히 삭제할 수 없지만 활성 상태가 아닌 다른 상태일 수 있습니다. 예를 들어 AMI를 비활성화할 수 있는 Amazon Elastic Compute Cloud 설정은 EC2 인스턴스의 백업을 복원하는 기능을 일시적으로 차단할 수 있습니다. 이는 저장소 잠금이나 법적 보류의 영향을 받는 백업을 포함하여 모든 EC2 복구 지점에 영향을 미칩니다.

  EC2 백업이 비활성화된 경우 비활성화된 AMI를 다시 활성화할 수 있습니다. 다시 활성화되면 복원할 수 있습니다. AMI 비활성화 기능을 차단하려면 IAM 정책을 사용하여 허용하지 `ec2:DisableImage` 않도록 설정할 수 있습니다.

> **Note**
>
> AWS Backup 저장소 잠금은 S3 빙하와만 호환되는 Amazon S3 빙하 저장소 잠금과는 기능이 다릅니다.

백업 저장소 삭제

우발적이거나 악의적인 대량 삭제를 방지하기 위해, 백업 저장소의 모든 복구 시점을 삭제한 후에만(또는 백업 계획 수명 주기 이후에만) AWS Backup 의 백업 저장소를 삭제할 수 있습니다. 복구 지점을 수동으로 삭제하려면 리소스 정리를 참조하십시오.

백업 저장소를 삭제했으면 새 백업 저장소를 가리키도록 백업 계획을 업데이트합니다. 백업 계획이 삭제된 백업 저장소를 가리킬 경우 백업 생성이 실패합니다.

> **Note**
>
> 두 개의 백업 저장소, 즉 AWS Backup 기본 백업 저장소와 Amazon EFS 자동 백업 저장소는 삭제할 수 없습니다.

콘솔을 사용하여 백업 저장소를 삭제하려면 AWS Backup

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 백업 저장소의 이름을 선택하여 세부 정보 페이지를 엽니다.

4. 백업 저장소와 연결된 백업을 선택하고 삭제합니다.
5. [저장소 삭제] 를 선택합니다. 확인 메시지가 표시되면 저장소 이름을 입력한 다음 [백업 저장소 삭제] 를 선택합니다.

백업 작업

백업 또는 복구 시점은 지정된 시간에 있는 리소스(예: Amazon Elastic Block Store(Amazon EBS) 볼륨 또는 Amazon DynamoDB 테이블) 콘텐츠를 나타냅니다. 복구 지점은 일반적으로 Amazon EBS 스냅샷 및 DynamoDB 백업과 같은 AWS 서비스의 다양한 백업을 가리키는 용어입니다. 복구 시점과 백업은 서로 통용되는 용어입니다.

AWS Backup 복구 지점을 백업 저장소에 저장하여 비즈니스 요구 사항에 따라 구성할 수 있습니다. 예를 들어, 회계 연도 2020년의 재무 정보가 포함된 일련의 리소스를 저장할 수 있습니다. 리소스를 복구해야 하는 경우 AWS Backup 콘솔이나 AWS Command Line Interface (AWS CLI) 를 사용하여 필요한 리소스를 찾아 복구할 수 있습니다.

각 복구 시점에는 고유 ID가 있습니다. 고유 ID는 복구 시점의 Amazon 리소스 이름(ARN) 끝에 있습니다. 복구 시점 ARN 및 고유 ID의 예는 리소스 및 작업의 표를 참조하세요.

> **Important**
>
> 추가 요금이 부과되지 않도록 하려면 웜 스토리지 기간을 1주 이상으로 설정하도록 보존 정책을 구성하세요. 자세한 정보는 측정, 비용 및 청구을 참조하세요.

다음 단원에서는 AWS Backup의 기본 백업 관리 작업에 대한 개요를 제공합니다.

주제

- 백업 생성
- 백업 복사
- 백업 삭제
- 백업 편집
- 백업 복원
- 복원 테스트
- 백업 목록 보기

백업 생성

를 사용하면 백업 계획을 사용하여 자동으로 백업을 생성하거나 온디맨드 백업을 시작하여 수동으로 백업을 생성할 수 있습니다. AWS Backup

자동 백업 생성

백업 계획으로 백업이 자동으로 생성되면 해당 백업은 백업 계획에 정의된 수명 주기 설정으로 구성됩니다. 백업 계획에 지정된 백업 볼트에 구성됩니다. 또한 백업 계획에 나열된 태그가 할당됩니다. 백업 계획에 대한 자세한 내용은 백업 계획을 사용하여 백업 관리 단원을 참조하세요.

온디맨드 백업 생성

온디맨드 백업을 생성할 때 생성 중인 백업에 대해 이러한 설정을 구성할 수 있습니다. 백업이 자동으로 또는 수동으로 생성되면 백업 작업이 시작됩니다. 온디맨드 백업을 생성하는 방법은 를 사용하여 온디맨드 백업을 생성합니다. AWS Backup 단원을 참조하세요.

참고: 온디맨드 백업은 백업 작업을 생성합니다. 백업 작업은 1시간 이내 (또는 지정된 시점)에 Running 상태로 전환됩니다. 백업 계획에 정의된 예약 시간이 아닌 다른 시간에 백업을 생성하려는 경우 온디맨드 백업을 선택할 수 있습니다. 예를 들어 언제든지 온디맨드 백업을 사용하여 백업 및 기능을 테스트할 수 있습니다.

온디맨드 백업은 리소스를 백업 당시의 상태로 보존하는 반면, PITR은 일정 기간 동안의 변경 사항을 기록하는 연속 백업을 사용하기 때문에 온디맨드 백업은 point-in-time 복원 (PITR) 과 함께 사용할 수 없습니다.

백업 작업 상태

각 백업 작업에는 고유 ID가 있습니다. 예를 들어 D48D8717-0C9D-72DF-1F56-14E703BF2345입니다.

AWS Backup 콘솔의 작업 페이지에서 백업 작업의 상태를 볼 수 있습니다. 백업 작업 상태에는CREATED,,PENDING,,RUNNING,ABORTING, ABORTED COMPLETED FAILEDEXPIRED, 및 PARTIAL 등이 포함됩니다.

증분 백업 작동 방식

를 사용한 증분 백업을 지원하는 리소스가 많습니다. AWS Backup전체 목록은 리소스별 기능 가용성 표의 증분 백업 섹션에서 확인할 수 있습니다.

첫 번째 백업 이후의 각 백업은 증분 백업이지만 (즉, 이전 백업의 변경 사항만 캡처함) 을 사용하여 만든 모든 백업에는 전체 복원에 필요한 참조 데이터가 AWS Backup 보존됩니다. 이는 원본(전체) 백업이 수명 주기의 끝에 도달하여 삭제된 경우에도 마찬가지입니다.

예를 들어 3일 수명 주기 정책으로 인해 1일차 (전체) 백업이 삭제된 경우에도 2일 차 및 3일 차 백업으로 전체 복원을 수행할 수 있습니다. AWS Backup 은 이를 위해 필요한 참조 데이터를 1일 차부터 유지합니다.

소스 리소스에 대한 액세스

AWS Backup 백업하려면 소스 리소스에 대한 액세스 권한이 필요합니다. 예:

- Amazon EC2 인스턴스를 백업하려면 인스턴스가 `running` 또는 `stopped` 상태일 수 있지만 `terminated` 상태일 수는 없습니다. `running`또는 `stopped` 인스턴스는 통신할 수 있지만 인스턴스는 통신할 수 없기 때문입니다. AWS Backup`terminated`
- 가상 머신을 백업하려면 해당 하이퍼바이저가 Backup 게이트웨이 상태 `ONLINE`이어야 합니다. 자세한 내용은 하이퍼바이저 상태 이해를 참조하세요.
- Amazon RDS 데이터베이스, Amazon Aurora 또는 Amazon DocumentDB 클러스터를 백업하려면 해당 리소스가 `AVAILABLE` 상태여야 합니다.
- Amazon Elastic File System(Amazon EFS)을 백업하려면 상태가 `AVAILABLE`이어야 합니다.
- Amazon FSx 파일 시스템을 백업하려면 상태가 `AVAILABLE`이어야 합니다. `UPDATING` 상태인 경우, 백업 요청은 파일 시스템이 `AVAILABLE` 상태가 될 때까지 대기열에 남아 있습니다.

  FSx for ONTAP는 DP(데이터 보호) 볼륨, LS(로드 공유) 볼륨, 전체 볼륨 또는 꽉 찬 파일 시스템의 볼륨을 비롯한 특정 볼륨 유형의 백업을 지원하지 않습니다. 자세한 내용은 FSx for ONTAP 백업 작업을 참조하세요.

AWS Backup 소스 리소스의 상태에 관계없이 이전에 생성된 백업을 수명 주기 정책에 따라 보존합니다.

주제

- 를 사용하여 온디맨드 백업을 생성합니다. AWS Backup
- 연속 백업 및 point-in-time 복원 (PITR)
- Amazon S3 버킷
- 가상 머신 백업
- 고급 DynamoDB 백업
- Amazon Timestream 백업
- Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업
- Amazon Redshift 백업

- Amazon 관계형 데이터베이스 서비스 백업
- AWS CloudFormation 스택 백업
- Windows VSS 백업 생성
- 아마존 EBS 및 AWS Backup
- 백업에 태그 복사
- 백업 작업 중지

를 사용하여 온디맨드 백업을 생성합니다. AWS Backup

AWS Backup 콘솔의 보호된 리소스 페이지에는 한 번 AWS Backup 이상 백업된 리소스가 나열됩니다. 를 처음 사용하는 AWS Backup 경우 이 페이지에 나열된 리소스 (예: Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스) 가 없습니다. 리소스가 백업 계획에 할당되어 있고 해당 백업 계획이 예약된 백업 작업을 한 번 이상 실행하지 않은 경우에도 마찬가지입니다.

참고: 온디맨드 백업은 리소스를 즉시 백업하기 시작합니다. 백업 계획에 정의된 예약 시간이 아닌 다른 시간에 백업을 생성하려는 경우 온디맨드 백업을 선택할 수 있습니다. 예를 들어 언제든지 온디맨드 백업을 사용하여 백업 및 기능을 테스트할 수 있습니다.

온디맨드 백업은 리소스를 백업 당시의 상태로 보존하는 반면, PITR은 일정 기간 동안의 변경 사항을 기록하는 연속 백업을 사용하기 때문에 point-in-time 복원 (PITR) 과 함께 온디맨드 백업을 사용할 수 없습니다.

고려 사항

- 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 기본 역할이 자동으로 생성됩니다.
- 백업이 만료되고 수명 주기 정책에 따라 삭제 대상으로 표시되면 AWS Backup 은 이후 8시간까지 임의로 선택한 시점에서 백업을 삭제합니다. 이 창은 일관된 성능을 보장하는 데 도움이 됩니다.
- Amazon EC2 리소스의 경우, 이 단계에서 추가한 태그 외에도 기존 그룹 및 개별 리소스 태그를 AWS Backup 자동으로 복사합니다.
- AWS Backup 기본 동작으로 “재부팅 없음”을 사용하여 EC2 백업을 수행합니다. AWS Backup 현재 Amazon EC2에서 실행되는 리소스를 지원하지만 특정 인스턴스 유형은 지원되지 않습니다. 자세한 정보는 Windows VSS 백업 생성을 참조하세요.

온디맨드 백업을 생성하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 대시보드에서 온디맨드 백업 생성을 선택합니다. 또는 탐색 창에서 보호된 리소스를 선택한 다음 온디맨드 백업 생성을 선택합니다.
3. 리소스 유형 페이지에서 백업하려는 리소스 유형을 선택합니다. 예를 들어, Amazon DynamoDB 테이블용 DynamoDB를 선택합니다.
4. 보호할 리소스의 이름 또는 ID를 선택합니다. 예를 들어, Amazon DynamoDB의 DynamoDB 테이블 이름을 선택합니다.
5. 지금 백업 생성이 선택되었는지 확인합니다.
6. 리소스 유형이 콜드 스토리지로의 전환을 지원하는 경우 콜드 스토리지가 제공됩니다. 자세한 내용은 리소스별 기능 가용성 표의 콜드 스토리지로의 라이프사이클 열을 참조하십시오.

   이 백업을 콜드 스토리지로 이동하는 시기를 지정하려면 웜 스토리지에서 콜드 스토리지로 백업 이동을 선택한 다음 웜 스토리지에 보관하는 시간을 지정합니다.
7. 총 보존 기간에는 기간 (일) 을 지정합니다. 콜드 스토리지 기간을 지정한 경우 보존 기간은 보온 스토리지와 콜드 스토리지로 구분됩니다.
8. 기존 백업 볼트를 선택하거나 새 볼트를 생성합니다. 새 백업 볼트 생성을 선택하면 볼트를 생성하는 새 페이지가 열린 후 작업 완료 시 온디맨드 백업 생성 페이지로 돌아갑니다.
9. IAM 역할의 경우 기본 역할 또는 생성한 역할을 선택합니다.
10. 온디맨드 백업에 태그를 할당하려면 복구 지점에 추가된 태그를 확장하고 새 태그 추가를 선택한 다음 태그 키와 태그 값을 입력합니다.
11. 리소스 유형이 EC2인 경우 고급 백업 설정이 표시됩니다. Windows 볼륨 섀도 복사본 서비스 (VSS) 를 사용하여 애플리케이션 정합성이 보장되는 스냅샷을 만들려면 Windows VSS를 선택합니다.
12. 온디맨드 백업 생성을 선택합니다. 그러면 작업 목록이 표시되고 작업 상태를 볼 수 있는 작업 페이지가 열립니다.

연속 백업 및 point-in-time 복원 (PITR)

주제

- 연속 백업/PITR (특정 시점 복원) 지원 서비스
- 연속 백업 찾기
- 연속 백업 복원
- 연속 백업 중지 또는 삭제
- 연속 백업 복사

- 보존 기간 변경
- 백업 계획에서 유일한 연속 백업 규칙 제거
- 동일한 리소스에 대한 중복되는 연속 백업
- IP 복구 고려 사항 oint-in-time

일부 리소스의 경우 스냅샷 백업 외에도 연속 백업 및 point-in-time 복구 (PITR) 를 AWS Backup 지원합니다.

연속 백업을 사용하면 선택한 특정 시간으로 되감아 1초 이내 (최대 35일 이전) 로 AWS Backup지원되는 리소스를 복원할 수 있습니다. 연속 백업은 먼저 리소스의 전체 백업을 생성한 다음 리소스의 트랜잭션 로그를 지속적으로 백업하는 방식으로 작동합니다. PITR 복원은 전체 백업에 액세스하여 복구하라고 지시한 시간까지 트랜잭션 로그를 재생하는 방식으로 작동합니다. AWS Backup

또는 스냅샷 백업을 자주(최대 1시간마다) 생성할 수도 있습니다. 스냅샷 백업은 최대 100년까지 저장할 수 있습니다. 전체 또는 증분 백업을 위해 스냅샷을 복사할 수 있습니다.

연속 백업과 스냅샷 백업은 서로 다른 이점을 제공하므로 연속 백업 규칙과 스냅샷 백업 규칙을 모두 사용하여 리소스를 보호하는 것이 좋습니다.

참고: 온디맨드 백업은 리소스를 즉시 백업하기 시작합니다. 백업 계획에 정의된 예약 시간이 아닌 다른 시간에 백업을 생성하려는 경우 온디맨드 백업을 선택할 수 있습니다. 예를 들어 언제든지 온디맨드 백업을 사용하여 백업 및 기능을 테스트할 수 있습니다.

온디맨드 백업은 리소스를 백업 당시의 상태로 보존하는 반면, PITR은 일정 기간 동안의 변경 사항을 기록하는 연속 백업을 사용하기 때문에 온디맨드 백업은 point-in-time 복원 (PITR) 과 함께 사용할 수 없습니다.

콘솔 또는 API를 AWS Backup 사용하여 백업 계획을 만들 때 지원되는 리소스의 연속 백업을 선택할 수 있습니다. AWS Backup

콘솔을 사용하여 연속 백업을 활성화하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택한 후 백업 계획 생성을 선택합니다.
3. 백업 규칙에서 백업 규칙 추가를 선택합니다.
4. 백업 규칙 구성 섹션에서 지원되는 리소스에 대해 지속적 백업 활성화를 선택합니다.

연속 백업/PITR (특정 시점 복원) 지원 서비스

AWS Backup 다음 서비스 및 애플리케이션에 대한 연속 백업 및 point-in-time 복구를 지원합니다.

Amazon S3

S3 백업에서 PITR을 활성화하려면 연속 백업이 백업 계획의 일부가 되어야 합니다.

소스 버킷의 이 원본 백업에는 PITR이 활성화되어 있을 수 있지만 교차 리전 또는 교차 계정 대상 복사본에는 PITR이 포함되지 않으므로 이러한 복사본에서 복원하면 지정된 시점으로 복원하는 대신 생성된 시점(복사본은 스냅샷 복사본)으로 복원됩니다.

RDS

백업 일정: AWS Backup 계획에서 Amazon RDS 스냅샷과 연속 백업을 모두 AWS Backup 생성하면 Amazon RDS 유지 관리 기간에 맞춰 지능적으로 백업 기간을 예약하여 충돌을 방지합니다. 충돌을 추가로 방지하기 위해 Amazon RDS 자동 백업 창을 수동으로 구성할 수 없습니다. RDS는 백업 계획의 스냅샷 백업 빈도가 하루에 한 번이 아니더라도 하루에 한 번 스냅샷을 생성합니다.

설정: Amazon RDS 인스턴스에 AWS Backup 연속 백업 규칙을 적용한 후에는 Amazon RDS에서 해당 인스턴스에 대한 연속 백업 설정을 생성하거나 수정할 수 없습니다. 수정은 AWS Backup 콘솔 또는 AWS Backup CLI를 통해 수행해야 합니다.

Amazon RDS 인스턴스의 연속 백업 제어를 Amazon RDS로 다시 이전합니다.

Console

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택합니다.
3. 해당 리소스를 보호하는 연속 백업이 포함된 모든 Amazon RDS 백업 계획을 삭제합니다.
4. 백업 볼트를 선택합니다. 백업 볼트에서 연속 백업 복구 시점을 삭제합니다. 또는 보존 기간이 경과할 때까지 기다리면 복구 지점이 AWS Backup 자동으로 삭제됩니다.

이 단계를 완료하면 리소스의 지속적 백업 제어를 Amazon RDS로 다시 전환합니다. AWS Backup

AWS CLI

`DisassociateRecoveryPoint` API 작업을 호출합니다.

자세한 내용은 DisassociateRecoveryPoint 섹션을 참조하세요.

Amazon RDS 연속 백업에 필요한 IAM 권한

- Amazon RDS 데이터베이스의 연속 백업을 구성하는 AWS Backup 데 사용하려면 백업 계획 구성에서 정의한 IAM 역할에 API 권한이 `rds:ModifyDBInstance` 있는지 확인하십시오. Amazon RDS 연속 백업을 복원하려면 복원 작업을 위해 제출한 IAM 역할에 `rds:RestoreDBInstanceToPointInTime` 권한을 추가해야 합니다. `AWS Backup default service role`을 사용하여 백업 및 복원을 수행할 수 있습니다.
- point-in-time 복구에 사용할 수 있는 시간 범위를 설명하려면 를 호출하십시오. AWS Backup `rds:DescribeDBInstanceAutomatedBackupsAPI` AWS Backup 콘솔의 경우 AWS Identity and Access Management (IAM) 관리형 정책의 `rds:DescribeDBInstanceAutomatedBackups` API 권한이 있어야 합니다. `AWSBackupFullAccess` 또는 `AWSBackupOperatorAccess` 관리형 정책을 사용할 수 있습니다. 두 정책 모두 필요한 권한이 모두 있습니다. 자세한 내용은 관리형 정책을 참조하세요.

보존 기간: PITR 보존 기간을 변경하면 변경 사항을 AWS Backup 즉시 `ModifyDBInstance` 호출하고 적용합니다. 다음 유지 관리 기간에 보류 중인 다른 구성 업데이트가 있는 경우 PITR 보존 기간을 변경하면 해당 구성 업데이트도 즉시 적용됩니다. 자세한 내용은 Amazon Relational Database Service API 참조의 `ModifyDBInstance`를 참조하세요.

Amazon RDS 연속 백업의 사본:

- 증분 스냅샷 복사 작업은 전체 스냅샷 복사 작업보다 처리 속도가 빠릅니다. 새 복사 작업이 완료될 때까지 이전 스냅샷 복사본을 보관하면 복사 작업 기간을 줄일 수 있습니다. RDS 데이터베이스 인스턴스에서 스냅샷을 복사하기로 선택한 경우 이전 복사본을 먼저 삭제하면 증분 대신 전체 스냅샷 복사본이 생성된다는 점에 유의해야 합니다. 복사 최적화에 대한 자세한 내용은 Amazon RDS 사용 설명서의 증분 스냅샷 복사를 참조하세요.
- Amazon RDS 연속 백업의 복사본 생성 — Amazon RDS의 경우 트랜잭션 로그의 복사를 허용하지 않으므로 AWS Backup Amazon RDS 연속 백업의 복사본을 생성할 수 없습니다. 대신 스냅샷을 AWS Backup 생성하여 백업 계획에 지정된 빈도에 따라 복사합니다.

point-in-time 복원: 둘 중 하나 AWS Backup 또는 Amazon RDS를 사용하여 복원을 수행할 수 있습니다. AWS Backup 콘솔 지침은 Amazon RDS 데이터베이스 복원을 참조하십시오. Amazon RDS 지침은 Amazon RDS 사용 설명서의 DB 인스턴스를 지정된 시간으로 복원을 참조하세요.

> **Tip**
>
> 로 설정된 다중 AZ (가용 영역) 데이터베이스 인스턴스는 백업 보존이 0으로 `Always On` 설정되어서는 안 됩니다. 오류가 발생하면 `disassociate-recovery-point` 대신 AWS CLI `delete-recovery-point` 명령을 사용하고 Amazon RDS 설정에서 보존 설정을 1로 변경하십시오.

Amazon RDS 작업에 대한 자세한 내용은 Amazon RDS 사용 설명서를 참조하세요.

Aurora

Aurora 리소스의 연속 백업을 활성화하려면 이 페이지의 첫 번째 섹션에 있는 단계를 참조하세요.

Aurora 클러스터를 시점 복원하는 절차는 Aurora 클러스터의 스냅샷을 복원하는 단계를 변형한 것입니다.

시점 복원을 수행하면 콘솔에 복원 시간 섹션이 표시됩니다. 이 페이지 아래에 있는 연속 백업 작업에서 연속 백업 복원을 참조하세요.

SAP HANA on Amazon EC2 인스턴스

point-in-time 복원 (PITR) 과 함께 사용할 수 있는 연속 백업을 만들 수 있습니다. 단, 온디맨드 백업은 리소스를 가져온 상태로 보존하는 반면 PITR은 일정 기간 동안의 변경 사항을 기록하는 연속 백업을 사용합니다.

연속 백업을 사용하면 EC2 인스턴스의 SAP HANA 데이터베이스를 선택한 특정 시점으로 되돌릴 수 있습니다(최대 35일 전까지 1초 단위로). 연속 백업은 먼저 리소스의 전체 백업을 생성한 다음 리소스의 트랜잭션 로그를 지속적으로 백업하는 방식으로 작동합니다. PITR 복원은 전체 백업에 액세스하여 복구하라고 지정한 시간까지 트랜잭션 로그를 재생하는 방식으로 작동합니다. AWS Backup

AWS Backup 콘솔 또는 API를 AWS Backup 사용하여 백업 계획을 생성할 때 연속 백업을 선택할 수 있습니다.

콘솔을 사용하여 연속 백업을 활성화하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택한 후 백업 계획 생성을 선택합니다.

3. 백업 규칙에서 백업 규칙 추가를 선택합니다.
4. 백업 규칙 구성 섹션에서 지원되는 리소스에 대해 지속적 백업 활성화를 선택합니다.

SAP HANA 데이터베이스 백업의 PITR (point-in-time복원) 을 비활성화하면 복구 지점이 만료될 AWS Backup 때까지 (상태가 같음) 로그가 계속 전송됩니다. EXPIRED) SAP HANA의 대체 로그 백업 위치로 변경하여 AWS Backup으로 로그 전송을 중지할 수 있습니다.

상태가 인 연속 복구 지점은 연속 복구 지점이 STOPPED 중단되었음을 나타냅니다. 즉, SAP HANA에서 데이터베이스의 증분 변경을 보여주는 로그에 간격이 있습니다. AWS Backup 이 기간 간격 내에 발생하는 복구 시점은 상태가 STOPPED. 입니다.

연속 백업(복구 시점)의 복원 작업 중에 발생할 수 있는 문제에 대해서는 이 설명서의 SAP HANA 복원 문제 해결 단원을 참조하세요.

연속 백업 찾기

AWS Backup 콘솔을 사용하여 연속 백업을 찾을 수 있습니다.

AWS Backup 콘솔을 사용하여 연속 백업을 찾으려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택한 다음 목록에서 백업 볼트를 선택합니다.
3. 백업 섹션에서 백업 유형 열을 연속 복구 시점으로 정렬합니다. 복구 시점 ID를 연속 접두사 기준으로 정렬할 수도 있습니다.

연속 백업 복원

AWS Backup 콘솔을 사용하여 연속 백업을 복원하려면

- PITR 복원 프로세스 중에 AWS Backup 콘솔에 복원 시간 섹션이 표시됩니다. 이 섹션에서는 다음 작업 중 하나를 수행합니다.
  - 복원 가능한 최근 시간으로 복원하려면 선택합니다.
  - 보존 기간 내의 날짜 및 시간을 직접 입력하려면 날짜 및 시간 지정을 선택합니다.

API를 사용하여 연속 백업을 복원하려면 AWS Backup

1. Amazon S3의 경우 AWS Backup API, CLI 또는 SDK를 사용하여 S3 복구 지점 복원을 참조하십시오.

2. Amazon RDS의 경우 AWS Backup API, CLI 또는 SDK를 사용하여 Amazon RDS 복구 지점 복원을 참조하십시오.

연속 백업 중지 또는 삭제

연속 백업 생성을 중단하거나 특정 백업 (point-in-time-recovery 또는 PITR 지점) 을 삭제할 수 있습니다.

연속 백업을 중지하려면 백업 계획에서 연속 백업 규칙을 삭제해야 합니다. 모든 리소스가 아닌 하나 이상의 리소스에 대한 연속 백업을 중지하려면 계속 백업하려는 리소스에 대한 연속 백업 규칙이 포함된 새 백업 계획을 생성하세요. 백업 볼트에서 연속 백업 복구 시점만 삭제하는 경우 백업 계획은 연속 백업 규칙을 계속 실행하여 새 복구 시점을 생성합니다.

하지만 연속 백업 규칙을 삭제한 후에도 현재 삭제된 백업 규칙의 보존 기간은 AWS Backup 기억됩니다. 지정된 보존 기간에 따라 백업 볼트에서 연속 백업 복구 시점을 자동으로 삭제합니다.

Amazon RDS 복구 지점을 삭제할 때는 다음 사항을 고려하십시오.

- 로 설정된 다중 AZ (가용 영역) 데이터베이스 인스턴스는 백업 보존이 0으로 `Always On` 설정되어서는 안 됩니다. 오류가 발생하면 `disassociate-recovery-point` 대신 AWS CLI `delete-recovery-point` 명령을 사용하고 Amazon RDS 설정에서 보존 설정을 1로 변경하십시오.
- Amazon RDS의 point-in-time 복구 지점 (연속 백업으로 생성된 백업) 이 삭제되면 데이터베이스 재부팅이 트리거되고 바이너리 로그는 비활성화됩니다. 자세한 내용은 Amazon RDS 사용 설명서의 백업 보존 기간을 참조하세요.

Aurora 복구 지점을 삭제할 때는 다음 사항을 고려하십시오.

Amazon Aurora 복구 지점으로 선택한 경우 보존 기간을 1일로 AWS Backup 설정합니다. 소스 클러스터도 삭제해야 Aurora 백업을 완전히 삭제할 수 있습니다.

연속 백업 복사

연속 백업 규칙에 교차 계정 또는 교차 리전 복사도 지정하는 경우 AWS Backup 은 연속 백업의 스냅샷을 생성하여 대상 볼트에 복사합니다. 계정 및 리전 간 복구 시점 복사에 대한 자세한 내용은 백업 복사를 참조하세요.

연속 백업은 대상 계정 및/또는 지역의 백업 계획 규칙에 설정된 빈도에 따라 정기 백업을 생성합니다.

AWS Backup 연속 백업의 온디맨드 복사본을 지원하지 않습니다.

보존 기간 변경

를 AWS Backup 사용하여 기존 연속 백업 규칙의 보존 기간을 늘리거나 줄일 수 있습니다. 최소 보존 기간은 1일입니다. 최대 보존 기간은 35일입니다.

보존 기간을 늘리는 경우 변경 사항이 즉시 적용됩니다 보존 기간을 줄이면 데이터 손실을 방지하기 위해 변경 사항을 적용하기 전에 충분한 시간이 경과할 때까지 기다립니다. AWS Backup 예를 들어 보존 기간을 35일에서 20일로 줄이면 15일이 경과할 때까지 35일간의 연속 백업이 계속 보존됩니다. AWS Backup 이 설계는 변경 시점으로부터 마지막 15일간의 백업을 보호합니다.

백업 계획에서 유일한 연속 백업 규칙 제거

연속 백업 규칙이 포함된 백업 계획을 만든 다음 해당 규칙을 제거하면 현재 삭제된 규칙의 보존 기간이 AWS Backup 기억됩니다. 보존 기간이 경과하면 백업 볼트에서 연속 백업을 삭제합니다.

동일한 리소스에 대한 중복되는 연속 백업

일반적으로 연속 백업 규칙을 하나만 사용하여 각 리소스를 보호해야 합니다. 추가 연속 백업은 중복이기 때문입니다. 그러나 백업 영역을 확장하면 단일 리소스에서 여러 백업 계획, 규칙 및 저장소가 겹칠 수 있습니다. AWS Backup 이러한 중복을 다음과 같이 처리합니다.

연속 백업 규칙이 있는 둘 이상의 백업 계획에 동일한 리소스를 포함하는 경우 AWS Backup 는 평가하는 첫 번째 백업 계획에 대해서만 연속 백업을 생성합니다. 다른 모든 백업 계획에 대한 스냅샷 백업을 생성합니다.

단일 백업 계획에 여러 연속 백업 규칙을 포함하는 경우

- 규칙이 동일한 백업 저장소를 가리키는 경우 보존 기간이 가장 긴 규칙에 AWS Backup 대해서만 연속 백업을 생성합니다. 다른 모든 규칙은 무시됩니다.
- 규칙이 다른 백업 저장소를 가리키는 경우 해당 계획을 유효하지 않은 것으로 간주하여 AWS Backup 거부합니다.

IP 복구 고려 사항 oint-in-time

point-in-time 복구에 대한 다음 고려 사항에 유의하십시오.

- 스냅샷으로 자동 폴백 - AWS Backup 이 연속 백업을 수행할 수 없는 경우 대신 스냅샷 백업을 시도합니다.
- 온디맨드 연속 백업이 지원되지 AWS Backup 않음 - 온디맨드 백업은 특정 시점을 기록하는 반면, 연속 백업 레코드는 일정 기간 동안 변경되므로 온디맨드 연속 백업을 지원하지 않습니다.

- 콜드 스토리지로의 전환을 지원하지 않음 - 콜드 스토리지로 전환하려면 최소 90일의 전환 기간이 필요하지만 연속 백업은 최대 보존 기간이 35일이기 때문에 콜드 스토리지로의 전환을 지원하지 않습니다.
- 최근 활동 복원 - Amazon RDS 활동은 최근 5분의 활동까지 복원할 수 있고, Amazon S3에서는 최근 15분의 활동까지 복원할 수 있습니다.

Amazon S3 버킷

AWS Backup S3에 데이터를 단독으로 저장하거나 데이터베이스, 스토리지, 컴퓨팅을 위한 다른 AWS 서비스와 함께 저장하는 애플리케이션의 중앙 집중식 백업 및 복원을 지원합니다. S3 백업에는 Backup Audit Manager를 비롯한 다양한 기능을 사용할 수 있습니다.

에서 단일 백업 정책을 사용하여 애플리케이션 데이터의 백업 생성을 중앙에서 AWS Backup 자동화할 수 있습니다. AWS Backup 여러 AWS 서비스 및 타사 애플리케이션의 백업을 암호화된 중앙 집중식 위치 (백업 저장소라고 함) 에 자동으로 정리하므로 중앙 집중식 환경을 통해 전체 애플리케이션의 백업을 관리할 수 있습니다. S3의 경우 클릭 한 point-in-time 번으로 연속 백업을 생성하고 S3에 저장된 애플리케이션 데이터를 복원한 다음 백업을 복원할 수 있습니다.

를 사용하면 객체 데이터 AWS Backup, 태그, 액세스 제어 목록 (ACL), 사용자 정의 메타데이터를 포함하여 다음과 같은 유형의 S3 버킷 백업을 생성할 수 있습니다.

- 연속 백업을 사용하면 최근 35일 중 원하는 시점으로 복원할 수 있습니다. S3 버킷의 연속 백업은 하나의 백업 계획으로만 구성해야 합니다.

  지원되는 서비스 목록 및 AWS Backup 을 사용하여 연속 백업을 수행하는 방법에 대한 지침은 시점 복구를 참조하세요.
- 정기 백업에서는 데이터의 스냅샷을 사용하여 최대 99년까지 지정된 기간 동안 데이터를 유지할 수 있습니다. 정기 백업을 1시간, 12시간, 1일, 1주, 1개월과 같은 빈도로 예약할 수 있습니다. AWS Backup 은 백업 계획에서 정의한 백업 기간 동안 정기적으로 백업을 수행합니다.

  백업 계획을 리소스에 AWS Backup 적용하는 방법을 이해하려면 백업 계획 생성을 참조하십시오.

S3 백업에는 계정 간 및 지역 간 복사본을 사용할 수 있지만 연속 백업의 사본에는 point-in-time 복원 기능이 없습니다.

S3 버킷의 연속 및 정기 백업은 모두 동일한 백업 볼트에 있어야 합니다.

두 백업 유형 모두 첫 번째 백업은 전체 백업이고 후속 백업은 객체 수준에서의 증분 백업입니다.

> **Note**
>
> Amazon S3에 사용하려면 S3 버킷에서 S3 버전 관리를 활성화해야 합니다. AWS Backup 데이터 보호를 위한 모범 사례로 S3 버전 관리를 권장하기 때문에 AWS 에서 이 전제 조건을 유지했습니다.
> S3 버전 관리에 수명 주기 만료 기간을 설정하는 것이 좋습니다. 수명 주기 만료 기간을 설정하지 않으면 만료되지 않은 S3 데이터 버전을 모두 AWS Backup 백업하고 저장하므로 S3 비용이 증가할 수 있습니다. S3 수명 주기 정책 설정에 대해 자세히 알아보려면 이 페이지의 지침을 따르세요.

S3 백업 유형 비교

S3 리소스에 대한 백업 전략에는 연속 백업만 포함하거나, 정기(스냅샷) 백업만 포함하거나, 이 둘을 조합하여 사용할 수 있습니다. 아래 정보는 조직에 가장 적합한 전략을 선택하는 데 도움이 될 수 있습니다.

연속 백업만:

- 기존 데이터의 첫 번째 전체 백업이 완료된 후에는 S3 버킷 데이터의 변경 사항이 발생하는 즉시 추적됩니다.
- 추적된 변경 내용을 통해 연속 백업의 보존 기간 동안 PITR (point-in-time 복원) 을 사용할 수 있습니다. 복원 작업을 수행하려면 복원하려는 시점을 선택합니다.
- 각 연속 백업의 보존 기간은 최대 35일입니다.

정기(스냅샷) 백업만, 예약 또는 온디맨드 백업:

- AWS Backup 전체 S3 버킷을 스캔하고, 각 객체의 ACL과 태그를 검색하고, 이전 스냅샷에는 있었지만 생성 중인 스냅샷에서는 발견되지 않은 모든 객체에 대해 Head 요청을 시작합니다.
- 백업은 일관적입니다. point-in-time
- 기록되는 백업 날짜 및 시간은 백업 작업이 생성된 시간이 아니라 버킷 순회가 AWS Backup 완료되는 시간입니다.
- 버킷의 첫 번째 백업은 전체 백업입니다. 이후의 각 백업은 증분 백업이며, 이는 마지막 스냅샷 이후의 데이터 변경을 나타냅니다.
- 정기 백업에 의한 스냅샷의 보존 기간은 최대 99년입니다.

정기/스냅샷 백업과 결합된 연속 백업:

- 기존 데이터(각 버킷)의 첫 번째 전체 백업이 완료되면 버킷의 변경 사항이 발생하는 대로 추적됩니다.
- 연속 point-in-time 복구 지점에서 복원을 수행할 수 있습니다.
- 스냅샷은 point-in-time 일관성이 있습니다.
- 스냅샷은 연속 복구 시점에서 직접 생성되므로 버킷을 다시 스캔할 필요가 없어 프로세스가 더 빠릅니다.
- 스냅샷과 연속 복구 시점은 데이터 계보를 공유하므로 스냅샷과 연속 복구 시점 간의 데이터 스토리지는 중복되지 않습니다.

지원되는 S3 스토리지 클래스

AWS Backup 다음 S3 스토리지 클래스에 저장된 S3 데이터를 백업할 수 있습니다.

- S3 Standard
- S3 스탠다드 - 간헐적 액세스 (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering(S3 INT)

스토리지 클래스 S3 지능형 계층화 (INT) 의 객체 백업은 해당 객체에 액세스합니다. 이 액세스는 S3 Intelligent-Tiering을 트리거하여 해당 객체를 자동으로 빈번한 액세스로 이동합니다.

S3 Standard - IA (간헐적 액세스) 및 S3 One Zone-IA 클래스를 포함하여 자주 액세스하지 않는 계층에 액세스하는 백업은 빈번한 액세스의 S3 스토리지 요금 (간헐적 액세스 또는 아카이브 인스턴트 액세스 계층에 적용) 을 따릅니다.

Glacier 인스턴트 검색을 제외하고 보관된 스토리지 클래스는 지원되지 않습니다.

Amazon S3의 스토리지 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하십시오.

Amazon AWS Backup S3에 대한 고려 사항

S3 리소스를 백업할 때는 다음 사항을 고려해야 합니다.

- 집중 객체 메타데이터 지원: 태그, 액세스 제어 목록 (ACL), 사용자 정의 메타데이터, 원본 생성 날짜 및 버전 ID와 같은 메타데이터를 AWS Backup 지원합니다. 또한 원본 생성 날짜, 버전 ID, 스토리지 클래스, e-태그를 제외한 모든 백업 데이터 및 메타데이터를 복원할 수 있습니다.
- S3 객체 키 이름은 대부분의 UTF-8 인코딩 가능 문자열로 구성될 수 있습니다. 다음 유니코드 문자가 허용됩니다. `#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF`.

  이 목록에 없는 문자가 포함된 객체 키 이름은 백업에서 제외될 수 있습니다. 자세한 내용은 문자에 대한 W3C 사양을 참조하세요.
- 콜드 스토리지 전환: AWS Backup의 수명 주기 관리 정책을 통해 백업 만료 일정을 정의할 수 있지만 S3 백업의 콜드 스토리지 전환은 현재 지원되지 않습니다.
- 동일한 시점에 생성된 동일한 객체의 여러 버전이 포함된 S3 버킷의 백업은 현재 지원되지 않습니다.
- 정기 백업의 경우 AWS Backup 객체 메타데이터의 모든 변경 사항을 추적하기 위해 최선을 다하십시오. 그러나 태그 또는 ACL을 1분 이내에 여러 번 업데이트하면 AWS Backup 이 중간 상태를 모두 캡처하지 못할 수 있습니다.
- AWS Backup 현재 SSE-C로 암호화된 객체의 백업은 지원하지 않습니다. AWS Backup 또한 현재 버킷 정책, 설정, 이름 또는 액세스 포인트를 포함한 버킷 구성 백업도 지원하지 않습니다.
- AWS Backup 현재 S3 on의 백업은 지원하지 않습니다 AWS Outposts.

> **Important**
>
> 데이터 읽기 이벤트를 로깅하는 계정에서 CloudTrail 로그가 활성화된 S3 버킷은 액세스 로그를 다른 대상 버킷에 저장해야 합니다. CloudTrail 로그를 기록하는 동일한 버킷에 저장하면 무한 루프가 형성됩니다. 이 루프로 인해 예상치 못하게 원치 않는 요금이 부과될 수 있습니다. 자세한 내용은 CloudTrail 사용 설명서의 데이터 이벤트를 참조하십시오.

S3 백업 완료 기간

아래 표에는 S3 버킷의 초기 전체 백업 완료 시간을 추정하는 데 도움이 되는 다양한 크기의 샘플 버킷이 나와 있습니다. 백업 시간은 각 버킷의 크기, 콘텐츠, 구성 및 설정에 따라 달라집니다.

버킷 크기	객체 수	초기 백업을 완료하는 데 걸리는 예상 시간
425GB(기가바이트)	1억 3,500만 개	31시간
800TB(테라바이트)	6억 7,000만 개	38시간
6PB(페타바이트)	50억 개	100시간
370TB(테라바이트)	75억 개	180시간

Amazon S3 백업 및 복원에 대한 권한 및 정책

S3 리소스를 백업, 복사, 복원하려면 역할에 올바른 정책이 있어야 합니다. 이러한 정책을 추가하려면 AWS 관리형 정책으로 이동하세요. S3 버킷을 백업 AWSBackupServiceRolePolicyForS3Backup및 AWSBackupServiceRolePolicyForS3Restore복원하는 데 사용할 역할에 및 를 추가합니다.

충분한 권한이 없는 경우 조직의 관리(관리자) 계정 관리자에게 의도한 역할에 정책을 추가해 달라고 요청하세요.

자세한 내용은 IAM 사용 설명서의 관리형 정책과 인라인 정책을 참조하세요.

AWS Backup for S3는 EventBridge Amazon을 통한 S3 이벤트 수신에 의존합니다. S3 버킷 알림 설정에서 이 설정을 비활성화하면 해당 설정이 비활성화된 버킷에 대해서는 연속 백업이 중지됩니다. 자세한 내용은 사용을 EventBridge 참조하십시오.

S3 백업의 모범 사례 및 비용 고려 사항

모범 사례

객체를 3억 개 이상 포함하는 버킷의 경우:

- 객체를 3억 개 이상 포함하는 버킷의 경우 버킷의 초기 전체 백업 시 백업 속도는 초당 최대 17,000개까지 도달할 수 있으며(증분 백업은 속도가 달라짐), 3억 개 미만의 객체를 포함하는 버킷은 초당 1,000개 객체에 가까운 속도로 백업됩니다.
- 연속 백업을 권장합니다.
- 백업 수명 주기가 35일을 초과하도록 계획된 경우 연속 백업이 저장된 동일한 볼트에서 버킷의 스냅샷 백업을 활성화할 수도 있습니다.

비용 고려 사항

- S3 수명 주기 정책에는 만료된 객체 삭제 마커 삭제라는 선택적 기능이 있습니다. 이 기능을 사용하지 않으면 삭제 마커(때로는 수백만 개가 있음)가 정리 계획 없이 만료됩니다. 이 기능이 없는 버킷을 백업하면 시간과 비용에 영향을 미치는 두 가지 문제가 발생합니다.
  - 삭제 마커는 객체와 마찬가지로 백업됩니다. 백업 시간 및 복원 시간은 삭제 마커 대비 객체의 비율에 따라 영향을 받을 수 있습니다.
  - 백업되는 각 객체 및 마커에는 최소 요금이 부과됩니다. 각 삭제 마커에는 128KiB 객체와 동일한 요금이 부과됩니다.
- 적어도 매일 또는 그 이상 자주 백업하는 계정의 경우 백업 간에 백업 내 데이터에 변화가 거의 없는 경우 연속 백업을 사용하면 비용을 절감할 수 있습니다.
- 자주 변경되지 않는 대용량 버킷은 연속 백업의 이점을 누릴 수 있습니다. 기존 객체(이전 백업 이후 변경되지 않은 객체)에 대해 객체당 여러 요청과 함께 전체 버킷을 스캔할 필요가 없으므로 비용이 절감될 수 있기 때문입니다.
- 1억 개 이상의 객체를 포함하고 전체 백업 크기에 비해 삭제율이 작은 버킷의 경우 보존 기간이 2일인 연속 백업과 보존 기간이 더 긴 스냅샷을 모두 포함하는 백업 계획을 사용하면 비용을 절감할 수 있습니다.
- 정기(스냅샷) 백업 시간은 버킷 스캔이 필요하지 않은 백업 프로세스의 시작 시간과 일치합니다. 연속 백업과 스냅샷이 모두 있는 버킷에서는 스캔이 필요하지 않습니다. 이러한 경우 스냅샷은 연속 복구 시점에서 생성되기 때문입니다.
- 단일 S3-GIR (Amazon S3 Glacier 인스턴트 검색) 의 각 객체에 대해 여러 번의 호출을 AWS Backup 수행하므로 백업 수행 시 검색 요금이 발생합니다.

  S3-IA 및 S3 One Zone-IA 스토리지 클래스의 객체가 있는 버킷에도 비슷한 검색 비용이 적용됩니다.
- AWS KMS CloudTrail, 및 백업 전략의 일부인 Amazon CloudWatch 기능으로 인해 S3 버킷 데이터 스토리지 외에 추가 비용이 발생할 수 있습니다. 이러한 기능에 대한 자세한 내용은 다음을 참조하세요.
  - Amazon S3 사용 설명서의 Amazon S3 버킷 키를 사용하여 SSE-KMS 비용 절감.
  - AWS KMS 이벤트를 제외하고 S3 데이터 이벤트를 비활성화하여 CloudTrail 비용을 절감할 수 있습니다.
    - AWS KMS 이벤트 제외: CloudTrail 사용 설명서에서 콘솔에서 트레일을 생성하면 (기본 이벤트 선택기) 이벤트를 제외하여 트레일에서 해당 AWS KMS 이벤트를 필터링할 수 있습니다 (기본 설정에는 모든 KMS 이벤트가 포함됨).

- KMS 이벤트를 로그하거나 제외하는 옵션은 추적에서 관리 이벤트를 로그하는 경우에만 사용할 수 있습니다. 관리 이벤트를 로그하지 않도록 선택하는 경우 KMS 이벤트가 로그되지 않으며, KMS 이벤트 로깅 설정을 변경할 수 없습니다.
- AWS KMS `EncryptDecrypt`, 와 같은 작업은 `GenerateDataKey` 일반적으로 대규모 (99% 이상) 의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. `Disable`, `Delete` 및 `ScheduleKey`와 같은 저용량의 관련 KMS 작업(일반적으로 KMS 이벤트 볼륨의 0.5% 미만을 차지함)은 쓰기 이벤트로 로그됩니다.
- `Encrypt`, `Decrypt` 및 `GenerateDataKey`와 같은 대량의 이벤트를 제외하지만 `Disable`, `Delete` 및 `ScheduleKey`와 같은 관련 이벤트를 계속 로그하려면 쓰기 관리 이벤트를 로그하도록 선택하고 AWS KMS 이벤트 제외 확인란의 선택을 취소합니다.
- S3 데이터 이벤트 비활성화: 기본적으로 추적 및 이벤트 데이터 스토어는 데이터 이벤트를 로그하지 않습니다. 초기 백업 전에 S3 데이터 이벤트를 비활성화하여 비용을 줄이세요.

- CloudWatch 비용을 줄이려면 CloudWatch CloudWatch 로그 설정을 비활성화하도록 트레일을 업데이트할 때 Logs에 CloudTrail 이벤트 전송을 중지할 수 있습니다.

S3 백업 복원

사용하여 백업한 S3 데이터를 S3 표준 스토리지 클래스로 AWS Backup 복원할 수 있습니다. S3 데이터를 원본 버킷을 포함한 기존 버킷에 복원할 수 있습니다. 복원 중에 새 S3 버킷을 복원 대상으로 생성할 수도 있습니다. S3 백업은 백업이 AWS 리전 있는 위치에만 복원할 수 있습니다.

전체 S3 버킷 또는 버킷 내 폴더 또는 객체를 복원할 수 있습니다. AWS Backup 은 해당 객체의 현재 버전을 복원합니다.

를 사용하여 AWS Backup S3 데이터를 복원하려면 을 참조하십시오S3 데이터 복원.

가상 머신 백업

AWS Backup VMware Cloud™ (VMC) 가 켜져 있고 VMware Cloud™ (VMC) 가 켜져 있는 VM에 있는 VM과 함께 온프레미스 VMware 가상 머신 (VM) 에 대한 중앙 집중식 AWS 및 자동 데이터 보호를 지원합니다. AWS Outposts온-프레미스 및 VMC 가상 시스템에서 로 백업할 수 있습니다. AWS Backup 그런 다음, AWS Backup 에서 온-프레미스 VM, VMC의 VM 또는 VMC on AWS Outposts로 복원할 수 있습니다.

AWS Backup 또한 VM 검색, 백업 예약, 보존 관리, 저렴한 스토리지 계층, 지역 간 및 계정 간 복사, Vault Lock AWS Backup 및 AWS Backup Audit Manager 지원, 소스 데이터와 독립된 암호화, 백업 액

세스 정책 등 완벽하게 관리되는 AWS기본 VM 백업 관리 기능을 제공합니다. 기능 및 세부 정보의 전체 목록은 리소스별 기능 가용성 표를 참조하세요.

VMware Cloud™ on에서 가상 시스템을 보호하는 AWS Backup 데 사용할 수 있습니다. AWS Outposts AWS Backup VMware Cloud™ 가 연결된 곳에 VM 백업을 저장합니다. AWS 리전 AWS Outposts VMware Cloud™ AWS Backup AWS Backup on을 사용할 때 VMware Cloud™ 를 VM에서 보호하는 AWS Outposts 데 사용하면 애플리케이션 데이터에 대한 지연 시간이 짧고 로컬 데이터 처리 요구 사항을 충족할 수 있습니다. 데이터 상주 요구 사항에 따라 애플리케이션 데이터의 백업을 연결된 AWS Backup 상위 위치에 저장하도록 선택할 수 있습니다. AWS 리전 AWS Outposts

지원되는 VM

AWS Backup VMware vCenter에서 관리하는 가상 시스템을 백업하고 복원할 수 있습니다.

현재 지원되는 항목은 다음과 같습니다.

- vSphere 8, 7.0, 6.7
- 1KiB의 배수인 가상 디스크 크기
- 온프레미스와 VMC 온프레미스에 있는 NFS, VMFS 및 VSAN 데이터스토어 AWS
- 소스 VM의 데이터를 온프레미스 VMware용으로 복제하기 위한 SCSI 핫 애드 및 네트워크 블록 디바이스 보안 소켓 레이어 (NBDSSL) 전송 모드 AWS
- VMware Cloud에서 VM을 보호하기 위한 핫 애드 모드 AWS

현재 지원되지 않음:

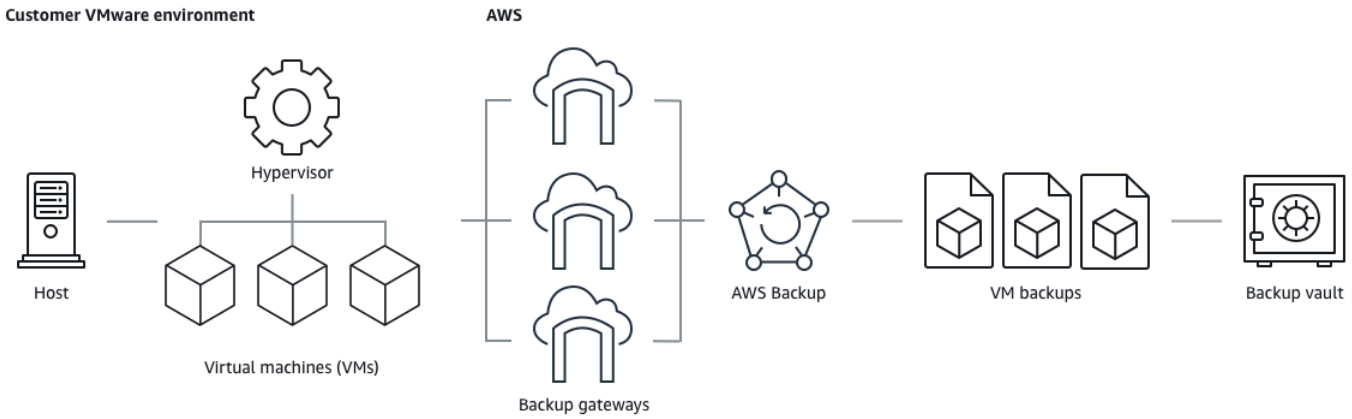
- RDM (원시 디스크 매핑) 디스크 또는 NVMe 컨트롤러 및 해당 디스크
- 독립-영구 및 독립-비영구 디스크 모드

백업 일관성

AWS Backup은 기본적으로 VM의 VMware Tools 일시 중지 설정을 사용하여 VM의 애플리케이션 일관성 백업을 캡처합니다. 애플리케이션이 VMware Tools와 호환되는 경우 백업은 애플리케이션 일관성입니다. 중지 기능을 사용할 수 없는 경우 장애 발생 시에도 정합성이 보장되는 백업을 캡처합니다. AWS Backup 복원을 테스트하여 백업이 조직의 요구 사항을 충족하는지 확인하세요.

Backup 게이트웨이

백업 게이트웨이는 VMware VM을 연결하기 위해 VMware 인프라에 배포하는 다운로드 가능한 AWS Backup 소프트웨어입니다. AWS Backup이 게이트웨이는 VM을 검색하기 위해 VM 관리 서버에 연결하고, VM을 검색하고, 데이터를 암호화하고, 데이터를 AWS Backup에 효율적으로 전송합니다. 다음 다이어그램에서는 Backup 게이트웨이가 VM에 연결되는 방식을 보여 줍니다.



Backup 게이트웨이 소프트웨어를 다운로드하려면 NAT 게이트웨이 작업의 절차를 따르세요.

VPC (가상 사설 클라우드) 엔드포인트에 대한 자세한 내용은 및 연결을 참조하십시오AWS Backup . AWS PrivateLink

Backup 게이트웨이는 AWS Backup API와 별도로 유지 관리되는 자체 API와 함께 제공됩니다. Backup 게이트웨이 API 작업 목록을 보려면 Backup 게이트웨이 작업을 참조하세요. Backup 게이트웨이 API 데이터 형식 목록을 보려면 Backup 게이트웨이 데이터 형식을 참조하세요.

엔드포인트

현재 퍼블릭 엔드포인트를 사용하고 있는 기존 사용자 중 VPC(Virtual Private Cloud) 엔드포인트로 전환하고자 하는 사용자는 AWS PrivateLink을 사용하여 VPC 엔드포인트가 있는 새 게이트웨이를 생성하고 기존 하이퍼바이저를 게이트웨이에 연결한 다음 퍼블릭 엔드포인트가 포함된 게이트웨이를 삭제할 수 있습니다.

Backup 게이트웨이를 사용하도록 인프라 구성

Backup 게이트웨이에서 가상 머신을 백업하고 복원하려면 다음과 같은 네트워크, 방화벽 및 하드웨어 구성이 필요합니다.

네트워크 구성

Backup 게이트웨이가 작동하려면 특정 포트가 필요합니다. 다음 포트를 허용하세요.

1. TCP 443 아웃바운드
   - 소스: Backup 게이트웨이
   - 목적지: AWS
   - 사용: Backup 게이트웨이가 통신할 수 있도록 AWS합니다.
2. TCP 80 인바운드
   - 소스: 연결할 때 사용하는 호스트 AWS Management Console
   - 대상: Backup 게이트웨이
   - 용도: Backup 게이트웨이 활성화 키를 가져올 때 로컬 시스템이 사용합니다. 포트 80은 Backup 게이트웨이를 활성화하는 동안에만 사용됩니다. AWS Backup 공개적으로 액세스할 수 있는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. 에서 게이트웨이를 활성화하는 경우 콘솔에 연결하는 호스트는 게이트웨이의 포트 80에 액세스할 수 있어야 합니다. AWS Management Console
3. UDP 53 아웃바운드
   - 소스: Backup 게이트웨이
   - 대상: DNS(Domain Name Service) 서버
   - 용도: Backup 게이트웨이가 DNS와 통신할 수 있도록 합니다.
4. TCP 22 아웃바운드
   - 소스: Backup 게이트웨이
   - 목적지: AWS Support
   - 사용: 게이트웨이에 AWS Support 액세스하여 문제 해결에 도움을 줄 수 있습니다. 게이트웨이의 정상 작동 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결을 위해서는 열어두어야 합니다.
5. UDP 123 아웃바운드
   - 소스: NTP 클라이언트
   - 대상: NTP 서버
   - 용도: 로컬 시스템이 가상 머신 시간을 호스트 시간과 동기화하는 데 사용됩니다.
6. TCP 443 아웃바운드
   - 소스: Backup 게이트웨이
   - 대상: VMware vCenter
   - 용도: Backup 게이트웨이가 VMware vCenter와 통신할 수 있도록 합니다.

7. TCP 443 아웃바운드
   - 소스: Backup 게이트웨이
   - 대상: ESXi 호스트
   - 용도: Backup 게이트웨이가 ESXi 호스트와 통신할 수 있도록 합니다.
8. TCP 902 아웃바운드
   - 소스: Backup 게이트웨이
   - 대상: VMware ESXi 호스트
   - 용도: Backup 게이트웨이를 통한 데이터 전송에 사용됩니다.

위의 포트는 Backup 게이트웨이에 필요합니다. Amazon VPC 엔드포인트를 구성하는 방법에 AWS Backup VPC 엔드포인트 생성 대한 자세한 내용은 을 참조하십시오. AWS Backup

방화벽 구성

Backup Gateway와 Amazon Web Services통신하려면 다음 서비스 엔드포인트에 대한 액세스 권한이 필요합니다. 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. Backup 게이트웨이와 서비스 지점 간의 HTTP 프록시 사용은 지원되지 않습니다.

```
proxy-app.backup-gateway.region.amazonaws.com:443
dp-1.backup-gateway.region.amazonaws.com:443
anon-cp.backup-gateway.region.amazonaws.com:443
client-cp.backup-gateway.region.amazonaws.com:443
```

VMware에서 여러 NIC에 대한 게이트웨이 구성

게이트웨이에 여러 가상 네트워크 인터페이스 연결 (NIC) 을 연결한 다음 내부 트래픽 (게이트웨이에서 하이퍼바이저로) 과 외부 트래픽 (게이트웨이로) 을 개별적으로 전달하여 내부 트래픽과 외부 트래픽을 위한 별도의 네트워크를 유지할 수 있습니다. AWS

기본적으로 AWS Backup 게이트웨이에 연결된 가상 컴퓨터에는 네트워크 어댑터 () 가 하나 있습니다. `eth0` 이 네트워크에는 하이퍼바이저, 가상 머신, 광범위한 인터넷과 통신하는 네트워크 게이트웨이 (Backup gateway) 가 포함됩니다.

다음은 여러 가상 네트워크 인터페이스를 사용하는 설정의 예입니다.

```
eth0:
- IP: 10.0.3.83
- routes: 10.0.3.0/24

eth1:
- IP: 10.0.0.241
- routes: 10.0.0.0/24
- default gateway: 10.0.0.1
```

- 이 예시에서는 게이트웨이는 IP가 `10.0.3.123`인 하이퍼바이저에 연결하기 위해 `eth0`를 사용합니다(하이퍼바이저 IP가 `10.0.3.0/24` 블록의 일부이기 때문).
- IP가 `10.0.0.234`인 하이퍼바이저에 연결하려면 게이트웨이는 `eth1`을 사용합니다.
- 로컬 네트워크 외부의 IP(예: `34.193.121.211`)에 연결하려면 게이트웨이는 기본 게이트웨이인 `10.0.0.1`로 폴백합니다. 이 IP는 `10.0.0.0/24` 블록의 일부이며 따라서 `eth1`를 통과합니다.

네트워크 어댑터를 추가하는 첫 번째 순서는 vSphere Client에서 수행됩니다.

1. VMware vSphere Client에서 게이트웨이 가상 머신을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.
2. 가상 머신 속성 대화 상자의 가상 하드웨어 탭에서 새 디바이스 추가 메뉴를 열고 네트워크 어댑터를 선택하여 새 네트워크 어댑터를 추가합니다.
3.
   a. 새 네트워크 세부 정보를 확장하여 새 어댑터를 구성합니다.
   b. 전원이 켜질 때 연결이 선택되어 있는지 확인합니다.
   c. 어댑터 유형에 대해서는 ESXi 및 vCenter Server 설명서의 네트워크 어댑터 유형을 참조하세요.
4. 확인을 클릭하여 새 네트워크 어댑터 설정을 저장합니다.

추가 어댑터를 구성하는 다음 단계는 AWS Backup 게이트웨이 콘솔에서 수행됩니다. 단, 이 인터페이스는 백업 및 기타 서비스를 AWS 관리하는 관리 콘솔과 동일하지 않습니다.

새 NIC를 게이트웨이 VM에 추가한 후에는 다음을 수행해야 합니다.

- `Command Prompt`로 이동하여 새 어댑터의 전원을 켭니다.
- 새 NIC마다 고정 IP를 구성합니다.
- 기본 NIC를 기본값으로 설정합니다.

방법:

1. VMware vSphere 클라이언트에서 게이트웨이 가상 시스템을 선택하고 웹 콘솔을 실행하여 Backup 게이트웨이 로컬 콘솔에 액세스합니다.

   - 로컬 콘솔에 액세스하는 방법에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔 액세스를 참조하세요.

2. 명령 프롬프트를 종료하고 네트워크 구성 > 고정 IP 구성으로 이동한 다음 설정 지침에 따라 라우팅 테이블을 업데이트합니다.

   a. 네트워크 어댑터의 서브넷 내의 고정 IP를 할당합니다.

   b. 네트워크 마스크를 설정합니다.

   c. 기본 게이트웨이의 IP 주소를 입력합니다. 이 네트워크 게이트웨이는 로컬 네트워크 외부의 모든 트래픽에 연결합니다.

3. 기본 어댑터 설정을 선택하여 클라우드에 연결할 어댑터를 기본 디바이스로 지정합니다.

4. 게이트웨이의 모든 IP 주소는 로컬 콘솔과 VMware vSphere의 VM 요약 페이지에 모두 표시할 수 있습니다.

하드웨어 요구 사항

다음과 같은 최소 리소스를 Backup 게이트웨이용 가상 머신 호스트에서 전용으로 사용할 수 있어야 합니다.

- 가상 프로세서 4개
- 예약된 RAM 8GiB

VMware 권한

이 섹션에는 사용하는 데 필요한 최소 VMware 권한이 나열되어 있습니다. AWS Backup gateway이러한 권한은 Backup 게이트웨이가 가상 머신을 검색, 백업, 복원하는 데 필요합니다.

VMware Cloud™ 가 켜져 AWS 있거나 VMware Cloud™ 가 AWS Outposts켜진 상태에서 백업 게이트웨이를 사용하려면 기본 관리자 사용자를 `cloudadmin@vmc.local` 사용하거나 전용 사용자에게 CloudAdmin 역할을 할당해야 합니다.

Backup Gateway를 VMware 온프레미스 가상 머신과 함께 사용하려면 아래 나열된 권한을 가진 전용 사용자를 생성하십시오.

전 세계

- 메서드 비활성화
- 메서드 활성화
- 라이선스
- 로그 이벤트
- 사용자 지정 속성 관리
- 사용자 지정 속성 설정

vSphere 태깅

- vSphere 태그 할당 또는 할당 취소

DataStore

- 공간 할당
- 데이터 스토어 찾아보기
- 데이터 스토어 구성(vSAN 데이터 스토어용)
- 하위 수준 파일 작업
- 가상 머신 파일 업데이트

Host

- 구성
  - 고급 설정
  - 스토리지 파티션 구성

폴더

- 폴더 생성

네트워크

- 네트워크 할당

dvPort 그룹

- 생성
- 삭제

Resource

- 리소스 풀에 가상 머신 할당

가상 머신

- 구성 변경
  - 디스크 리스 획득
  - 기존 디스크 추가
  - 새 디스크 추가
  - 고급 구성
  - 설정 변경
  - 원시 디바이스 구성
  - 디바이스 설정 수정
  - 디스크 제거
  - 주석 설정
  - 디스크 변경 사항 추적 전환
- 인벤토리 편집
  - 기존 항목에서 생성
  - 새로 생성
  - 등록
  - Remove
  - 등록 취소
- 상호 작용
  - 전원 끄기
  - 전원 켜기
  - 포 로 비저닝

  - 디스크 액세스 허용
  - 읽기 전용 디스크 액세스 허용
  - 가상 머신 다운로드 허용
- 스냅샷 관리
  - 스냅샷 생성
  - 스냅샷 제거
  - 스냅샷으로 되돌리기

NAT 게이트웨이 작업

를 사용하여 AWS Backup가상 머신 (VM) 을 백업 및 복원하려면 먼저 백업 게이트웨이를 설치해야 합니다. 게이트웨이는 Backup을 하이퍼바이저에 연결하는 OVF (Open Virtualization Format) 템플릿 형태의 소프트웨어로서, 가상 머신을 자동으로 탐지하고 사용자가 가상 머신을 Amazon Web Services 백업 및 복원할 수 있도록 합니다.

단일 게이트웨이에서 한 번에 최대 4개의 백업 또는 복원 작업을 실행할 수 있습니다. 한 번에 5개 이상의 작업을 실행하려면 게이트웨이를 추가로 생성하여 하이퍼바이저에 연결하세요.

게이트웨이 생성

게이트웨이를 생성하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창의 외부 리소스 섹션에서 게이트웨이를 선택합니다.
3. 게이트웨이 생성을 선택합니다.
4. 게이트웨이 설정 섹션에서 다음 지침에 따라 OVF 템플릿을 다운로드하고 배포합니다.

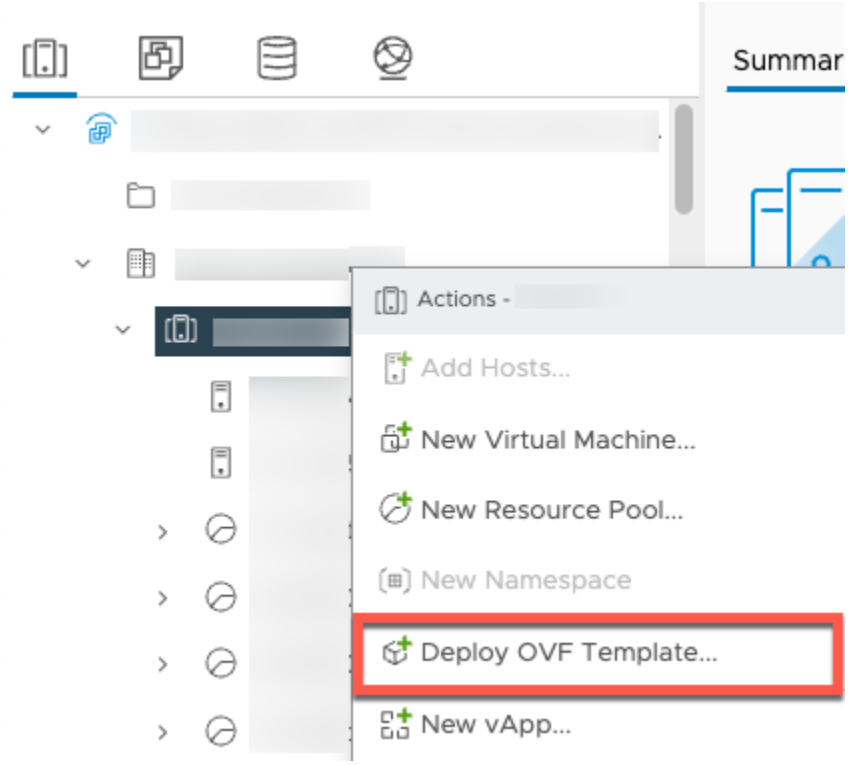
VMware 소프트웨어 다운로드

하이퍼바이저 연결

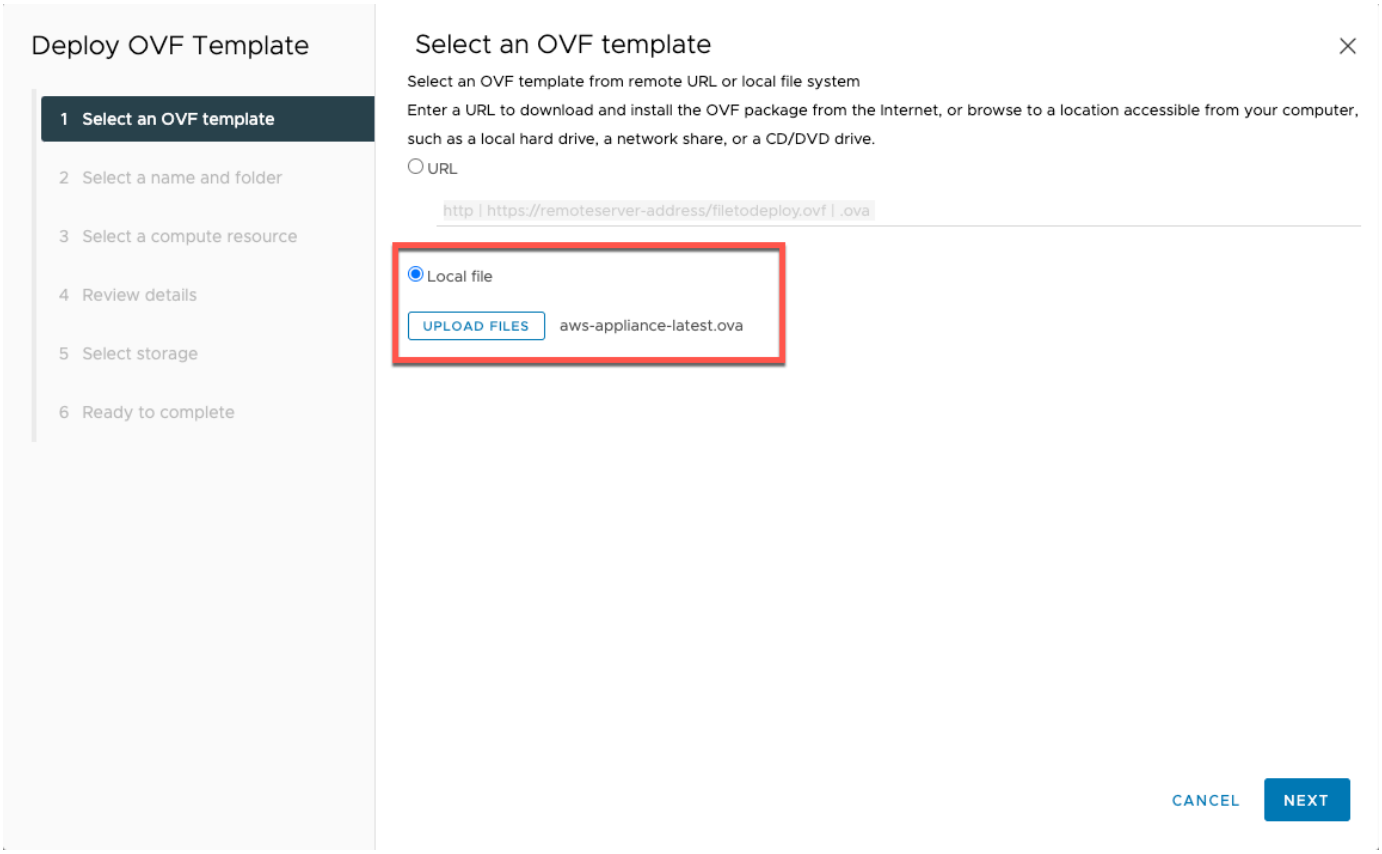
게이트웨이는 AWS Backup 하이퍼바이저에 연결되므로 가상 머신의 백업을 생성하고 저장할 수 있습니다. VMware ESXi에 게이트웨이를 설정하려면 OVF 템플릿을 다운로드하세요. 다운로드는 10분 정도 걸릴 수 있습니다.

작업이 완료되면 다음 단계를 진행합니다.

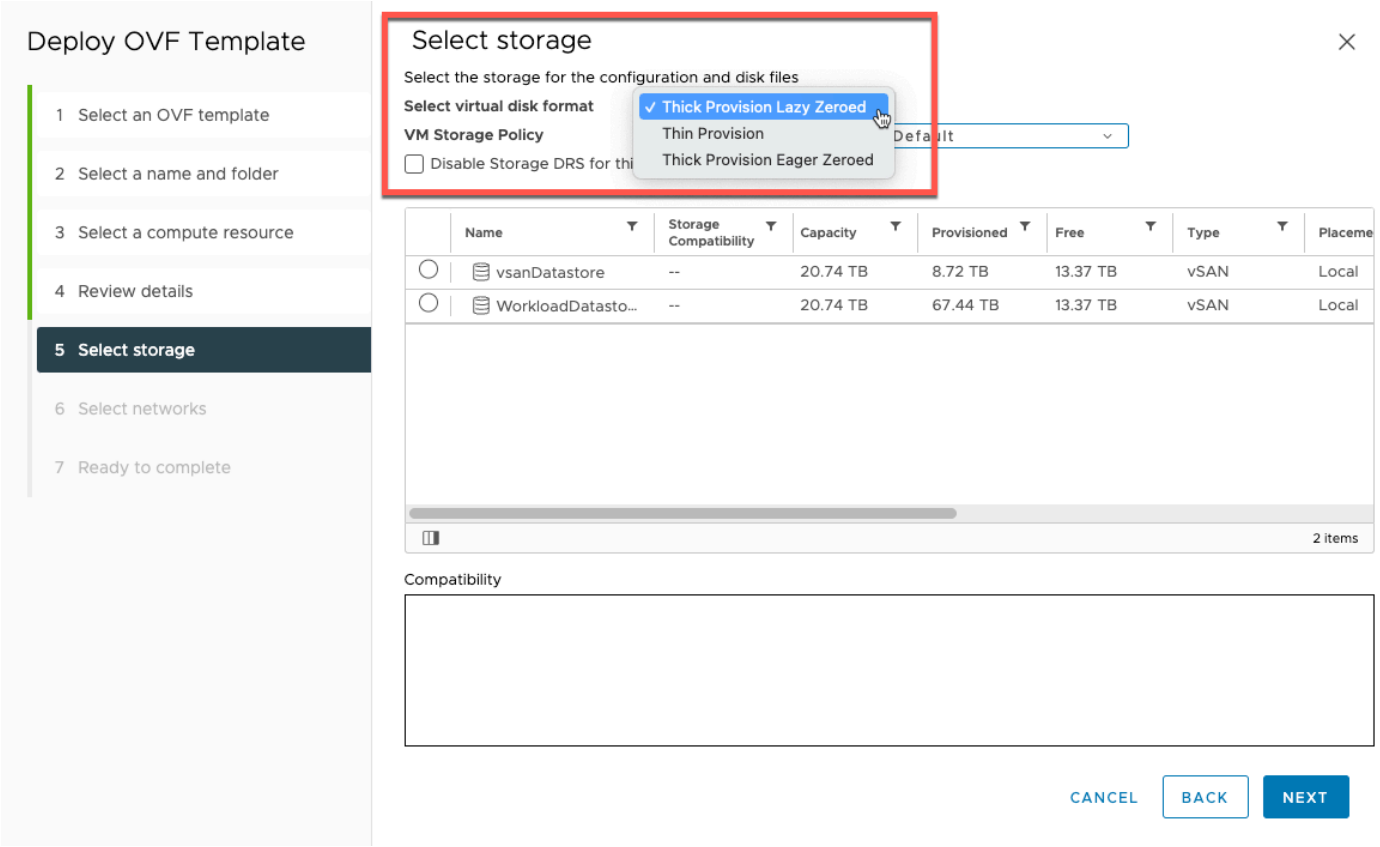
1. VMware vSphere를 사용하여 가상 머신 하이퍼바이저에 연결합니다.
2. 가상 머신의 상위 객체를 마우스 오른쪽 단추로 클릭하고 OVF 템플릿 배포를 선택합니다.



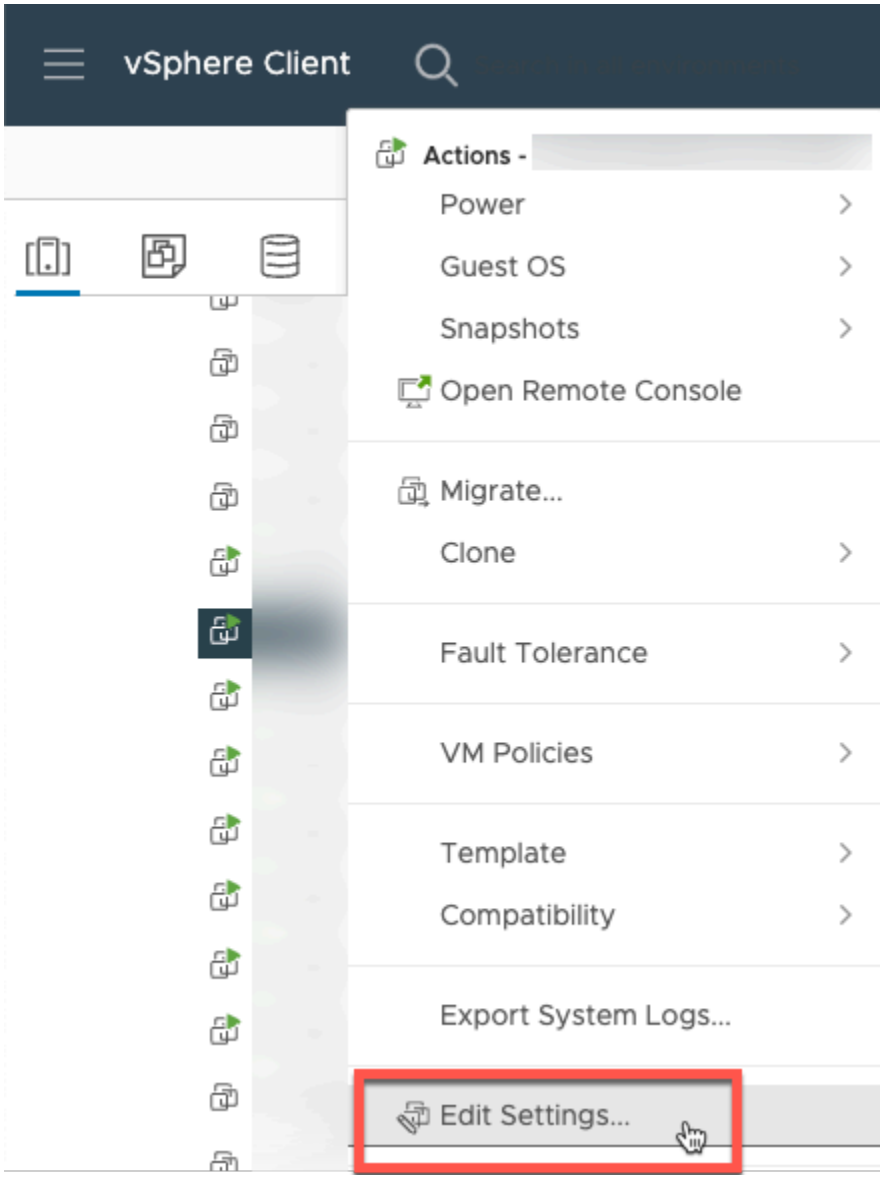
3. 로컬 파일을 선택하고 aws-appliance-latest다운로드한.ova 파일을 업로드합니다.



4. 배포 마법사 단계에 따라 배포합니다. 스토리지 선택 페이지에서 가상 디스크 형식 Thick Provision Lazy Zeroed를 선택합니다.

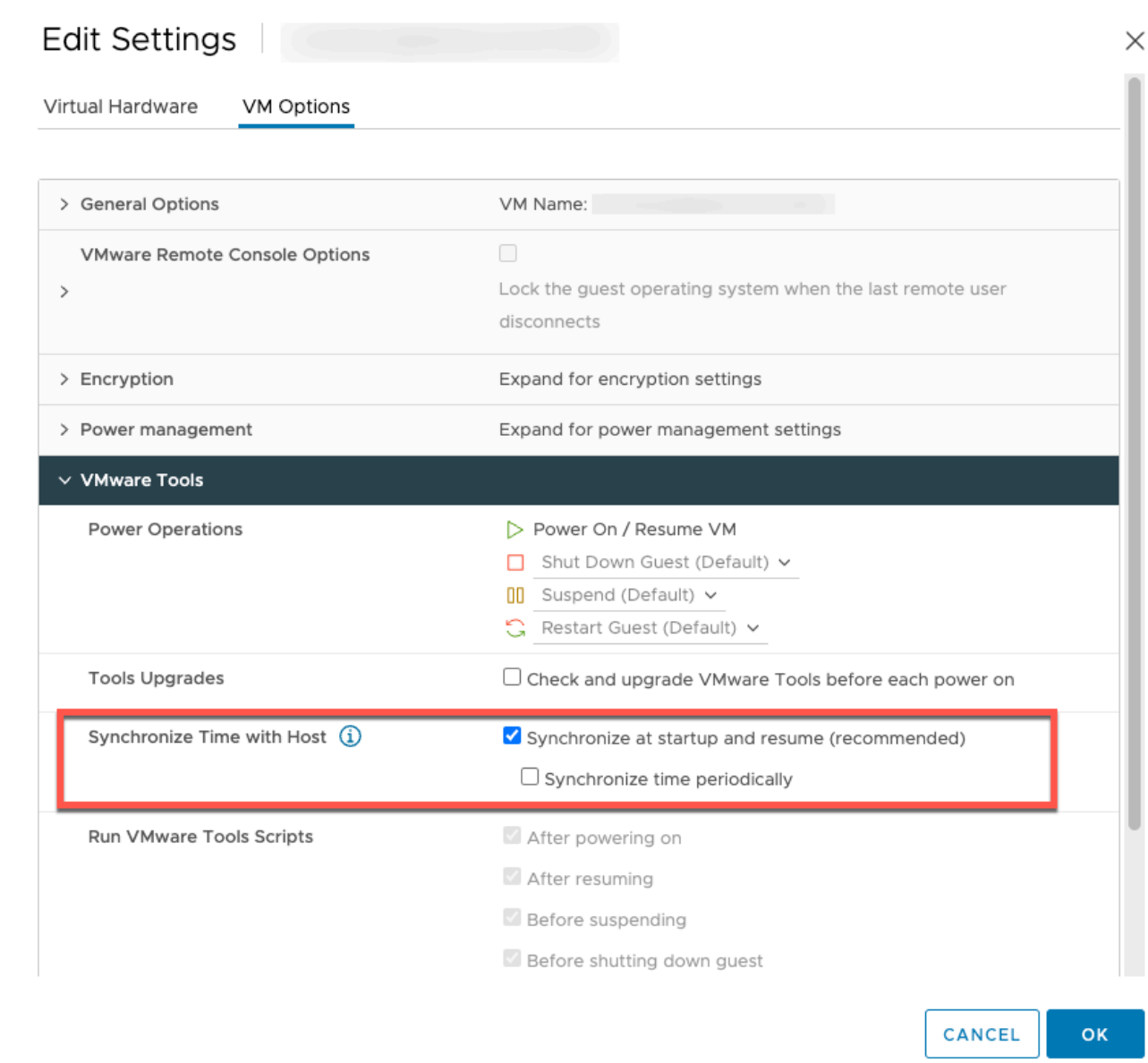


5. OVF를 배포한 후 게이트웨이를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다.

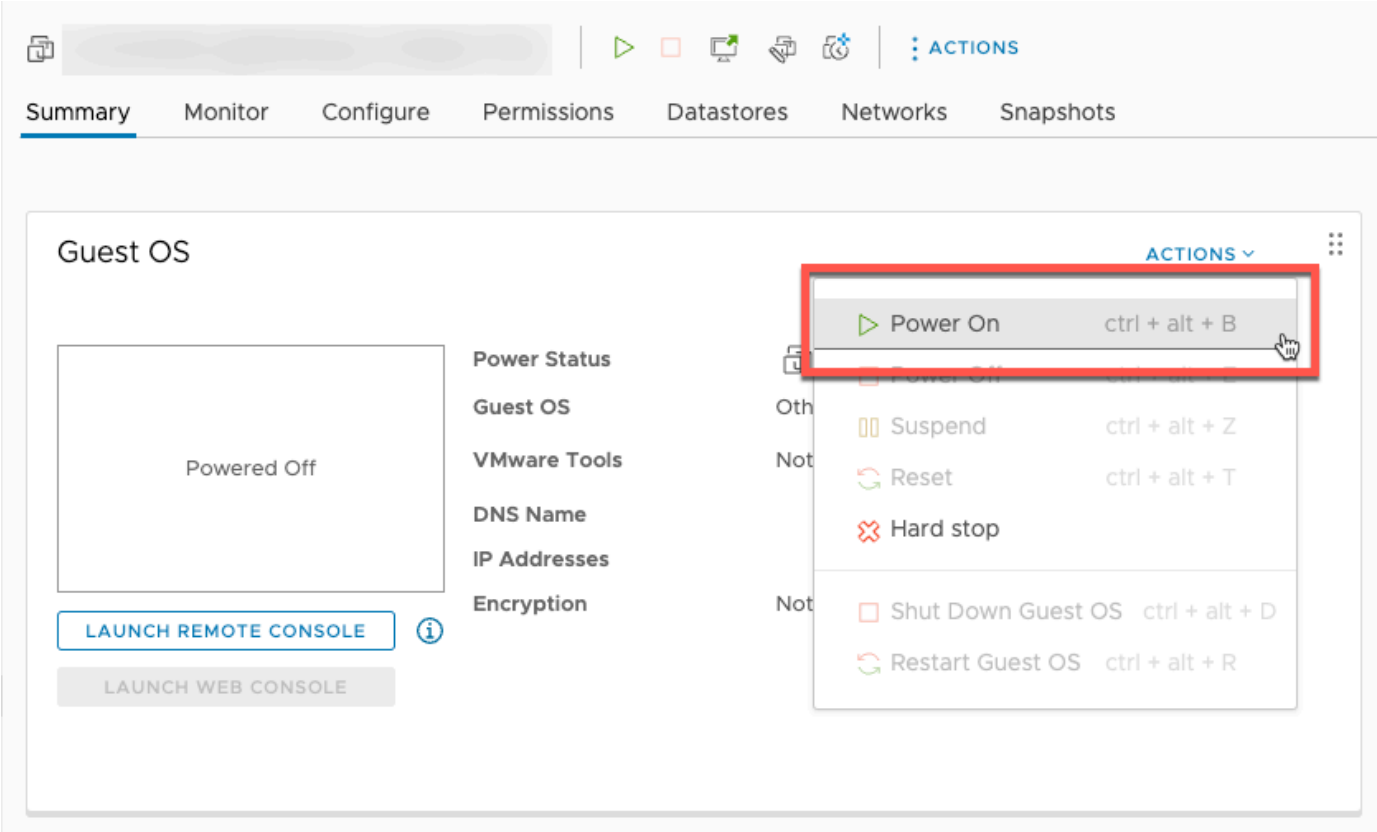


a. VM 옵션에서 VM 도구로 이동합니다.

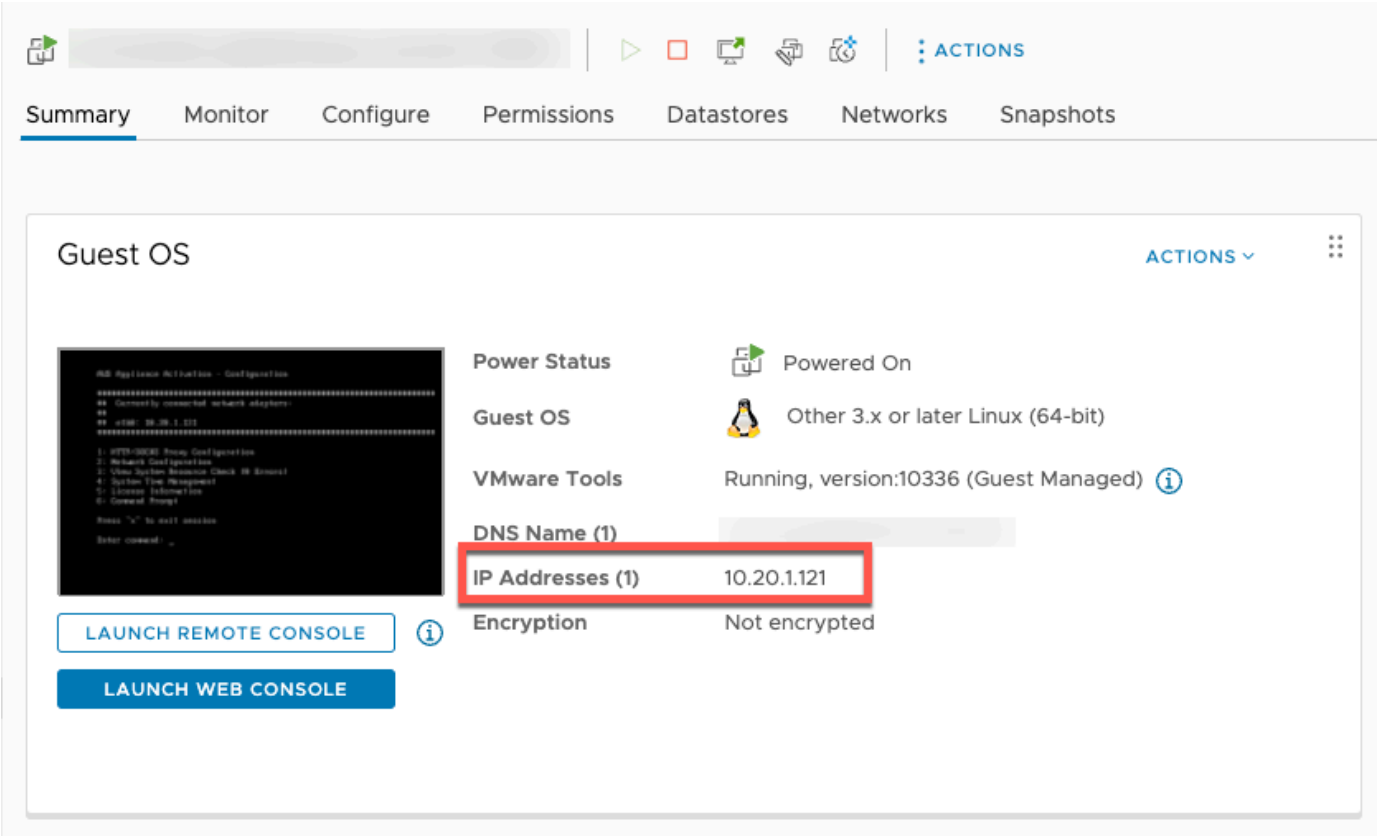
b. 시간을 호스트와 동기화에 시작 및 재개 시 동기화가 선택되어 있는지 확인합니다.



6. 작업 메뉴에서 '전원 켜기'를 선택하여 가상 머신을 켭니다.



7. VM 요약에서 IP 주소를 복사하여 아래에 입력합니다.



VMware 소프트웨어를 다운로드한 후 다음 단계를 수행합니다.

1. 게이트웨이 연결 섹션에 게이트웨이의 IP 주소를 입력합니다.

   a. 이 IP 주소를 찾으려면 vSphere Client로 이동합니다.

   b. 요약 탭에서 게이트웨이를 선택합니다.

   c. IP 주소를 복사하여 AWS Backup 콘솔 텍스트 표시줄에 붙여넣습니다.

2. 게이트웨이 설정 섹션에서

   a. 게이트웨이 이름을 입력합니다.

   b. AWS 지역을 확인하세요.

   c. 엔드포인트가 공개적으로 액세스할 수 있는지 또는 Virtual Private Cloud(VPC)에서 호스팅할지 선택합니다.

   d. 선택한 엔드포인트에 따라 VPC 엔드포인트 DNS 이름을 입력합니다.

      자세한 내용은 VPC 엔드포인트 생성을 참조하세요.

3. [선택 사항] 게이트웨이 태그 섹션에서 키 및 선택적 값을 입력하여 태그를 할당할 수 있습니다. 2개 이상의 태그를 추가하려면 다른 태그 추가를 클릭합니다.

4. 프로세스를 완료하려면 게이트웨이 생성을 클릭합니다. 그러면 게이트웨이 세부 정보 페이지로 이동합니다.

게이트웨이 편집 또는 삭제

게이트웨이를 편집 또는 삭제하려면

1. 왼쪽 탐색 창의 외부 리소스 섹션에서 게이트웨이를 선택합니다.

2. 게이트웨이 섹션에서 게이트웨이 이름을 기준으로 게이트웨이를 선택합니다.

3. 게이트웨이 이름을 편집하려면 편집을 선택합니다.

4. 게이트웨이를 삭제하려면 삭제를 선택한 다음 게이트웨이 삭제를 선택합니다.

   삭제한 게이트웨이는 다시 활성화할 수 없습니다. 하이퍼바이저에 다시 연결하려면 게이트웨이 생성의 절차를 따르세요.

5. 하이퍼바이저에 연결하려면 연결된 하이퍼바이저 섹션에서 연결을 선택합니다.

   각 게이트웨이는 단일 하이퍼바이저에 연결됩니다. 그러나 여러 게이트웨이를 동일한 하이퍼바이저에 연결하여 게이트웨이 간의 대역폭을 첫 번째 게이트웨이 이상으로 늘릴 수 있습니다.

6. 태그를 할당, 편집 또는 관리하려면 태그 섹션에서 태그 관리를 선택합니다.

백업 게이트웨이 대역폭 조절

> **Note**
>
> 이 기능은 2022년 12월 15일 이후 배포된 새 게이트웨이에서 사용할 수 있습니다. 기존 게이트웨이의 경우 2023년 1월 30일 또는 그 이전에 자동 소프트웨어 업데이트를 통해 이 새로운 기능을 사용할 수 있습니다. 게이트웨이를 최신 버전으로 수동으로 업데이트하려면 명령을 사용합니다 AWS CLI . `UpdateGatewaySoftwareNow`

게이트웨이의 업로드 처리량을 AWS Backup 제한하여 게이트웨이가 사용하는 네트워크 대역폭의 양을 제어할 수 있습니다. 기본적으로 활성화된 게이트웨이는 속도 제한이 없습니다.

AWS Backup 콘솔을 사용하거나 AWS CLI () `PutBandwidthRateLimitSchedule`를 통한 API를 사용하여 대역폭 속도 제한 일정을 구성할 수 있습니다. 대역폭 속도 제한 일정을 사용하는 경우 하루 또는 일주일 내내 제한이 자동으로 변경되도록 구성할 수 있습니다.

대역폭 속도 제한은 업로드되는 모든 데이터의 초당 평균 처리량을 밸런싱하는 방식으로 작동합니다. 업로드가 특정 마이크로초 또는 밀리초 동안 대역폭 속도 제한을 잠시 초과할 수는 있지만, 장기간에 걸쳐 큰 폭의 스파이크가 발생하지는 않습니다.

최대 20개의 간격을 추가할 수 있습니다. 업로드 속도의 최대값은 8,000,000Mbps(초당 메가바이트)입니다.

콘솔을 사용하여 게이트웨이의 대역폭 속도 제한 일정을 보고 편집할 수 있습니다. AWS Backup

이 섹션에서는 게이트웨이의 대역폭 속도 제한 일정을 보고 편집하는 방법을 설명합니다.

대역폭 속도 제한 일정을 보고 편집하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 게이트웨이를 선택합니다. 게이트웨이 창에는 게이트웨이가 이름별로 표시됩니다. 관리하려는 게이트웨이 이름 옆의 라디오 버튼을 클릭합니다.
3. 라디오 버튼을 선택하면 드롭다운 메뉴 작업을 클릭할 수 있습니다. 작업을 클릭한 다음 대역폭 속도 제한 일정 편집을 클릭합니다. 현재 일정이 표시됩니다. 기본적으로 새 게이트웨이 또는 편집되지 않은 게이트웨이에는 정의된 대역폭 속도 제한이 없습니다.

> **Note**
>
> 게이트웨이 세부 정보 페이지에서 일정 관리를 클릭하여 대역폭 편집 페이지로 이동할 수도 있습니다.

4. (선택 사항) 간격 추가를 선택하여 구성 가능한 새 간격을 일정에 추가합니다. 각 간격에 대해 다음 정보를 입력합니다.

   a. 요일 - 간격을 적용할 반복되는 요일을 선택합니다. 요일을 선택하면 드롭다운 메뉴 아래에 해당 요일이 표시됩니다. 요일 옆에 있는 X를 클릭하면 요일을 삭제할 수 있습니다.

   b. 시작 시간 - HH:MM 24시간 형식을 사용하여 대역폭 간격의 시작 시간을 입력합니다. 시간은 협정 세계시(UTC)로 표시됩니다.

      참고: bandwidth-rate-limit 인터벌은 지정된 분이 시작될 때 시작됩니다.

   c. 종료 시간 - HH:MM 24시간 형식을 사용하여 대역폭 간격의 종료 시간을 입력합니다. 시간은 협정 세계시(UTC)로 표시됩니다.

      > **Important**
      >
      > bandwidth-rate-limit 간격은 지정된 분이 끝날 때 종료됩니다. 한 시간이 지나면 종료되는 간격을 예약하려면 59를 입력합니다. 간격 사이에 중단 없이 시간 시작 시점에 전환되는 연속적인 간격을 예약하려면 첫 번째 간격의 종료 분에 59를 입력합니다. 후속 간격의 시작 분에 00을 입력합니다.

   d. 업로드 속도 - 업로드 속도 제한을 초당 메가비트(Mbps) 단위로 입력합니다. 최소값은 102Mbps(초당 메가바이트)입니다.

5. (선택 사항) 대역폭 속도 제한 일정이 완료될 때까지 원하는 대로 이전 단계를 반복합니다. 일정에서 일정 간격을 삭제해야 하는 경우 제거를 선택합니다.

> **Important**
>
> 대역폭 속도 제한 간격은 겹칠 수 없습니다. 간격의 시작 시간은 이전 간격의 종료 시간 이후이고 다음 간격의 시작 시간 이전이어야 합니다. 종료 시간은 다음 간격의 시작 시간 이전이어야 합니다.

6. 작업을 마쳤으면 변경 사항 저장 버튼을 클릭합니다.

AWS CLI를 사용하여 게이트웨이의 대역폭 속도 제한 일정을 보고 편집합니다.

GetBandwidthRateLimitSchedule 작업을 사용하여 지정된 게이트웨이의 대역폭 제한 일정을 볼 수 있습니다. 일정이 설정되지 않은 경우 일정은 빈 간격 목록이 됩니다. 다음은 를 사용하여 게이트웨이의 대역폭 스케줄을 가져오는 예입니다. AWS CLI

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

게이트웨이의 대역폭 제한 일정을 편집하려면 PutBandwidthRateLimitSchedule 작업을 사용할 수 있습니다. 개별 간격을 수정, 추가 또는 제거하는 대신 게이트웨이 일정 전체만 업데이트할 수 있다는 점에 유의하세요. 이 작업을 호출하면 게이트웨이의 이전 대역폭 제한 일정을 덮어씁니다.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

하이퍼바이저 작업

작업을 마친 게이트웨이 생성 후에는 하이퍼바이저에 연결하여 해당 하이퍼바이저에서 관리하는 가상 컴퓨터와 작업할 수 AWS Backup 있습니다. 예를 들어 VMware VM용 하이퍼바이저는 VMware vCenter Server입니다. 하이퍼바이저가 AWS Backup에 필요한 권한을 갖도록 구성되어 있는지 확인하세요.

하이퍼바이저 추가

하이퍼바이저를 추가하려면

1. 왼쪽 탐색 창의 외부 리소스 섹션에서 하이퍼바이저를 선택합니다.
2. 하이퍼바이저 추가를 선택합니다.
3. 하이퍼바이저 설정 섹션의 하이퍼바이저 이름에 이름을 입력합니다.
4. vCenter Server 호스트에서 드롭다운 메뉴를 사용하여 IP 주소 또는 FQDN(정규화된 도메인 이름)을 선택합니다. 해당 값을 입력합니다.
5. 하이퍼바이저에서 가상 컴퓨터를 검색할 수 있게 AWS Backup 하려면 하이퍼바이저의 사용자 이름과 암호를 입력합니다.
6. 암호를 암호화합니다. 드롭다운 메뉴를 사용하여 특정 서비스 관리형 KMS 키 또는 고객 관리형 KMS 키를 선택하거나 KMS 키 생성을 선택하여 이 암호화를 지정할 수 있습니다. 특정 키를 선택하지 않는 경우 AWS Backup 은 서비스 소유 키를 사용하여 암호를 암호화합니다.

7. 연결 게이트웨이 섹션에서 드롭다운 목록을 사용하여 하이퍼바이저에 연결할 게이트웨이를 지정합니다.
8. 게이트웨이 연결 테스트를 선택하여 이전 입력을 확인합니다.
9. 선택적으로 하이퍼바이저 태그 섹션에서 새 태그 추가를 선택하여 하이퍼바이저에 태그를 할당할 수 있습니다.
10. 선택적 VMware 태그 매핑: 현재 가상 시스템에서 사용하고 있는 VMware 태그를 최대 10개까지 추가하여 태그를 생성할 수 있습니다. AWS
11. 로그 그룹 설정 패널에서 Amazon CloudWatch Logs와 통합하여 하이퍼바이저의 로그를 관리할 수 있습니다 (사용량에 따라 표준 CloudWatch 로그 요금이 적용됨). 각 하이퍼바이저는 하나의 로그 그룹에 속할 수 있습니다.

    a. 아직 로그 그룹을 생성하지 않은 경우 새 로그 그룹 생성 라디오 버튼을 선택합니다. 편집 중인 하이퍼바이저는 이 로그 그룹과 연결됩니다.

    b. 이전에 다른 하이퍼바이저에 대한 로그 그룹을 생성한 경우 해당 로그 그룹을 이 하이퍼바이저에 사용할 수 있습니다. 기존 로그 그룹 사용을 선택합니다.

    c. 로깅을 원하지 않는 경우 CloudWatch 로깅 비활성화를 선택합니다.
12. 하이퍼바이저 추가를 선택하면 해당 세부 정보 페이지로 이동합니다.

> **Tip**
>
> Amazon CloudWatch Logs (위의 11단계 참조) 를 사용하여 오류 모니터링, 게이트웨이와 하이퍼바이저 간 네트워크 연결, 네트워크 구성 정보 등 하이퍼바이저에 대한 정보를 얻을 수 있습니다. CloudWatch 로그 그룹에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 로그 그룹 및 로그 스트림 작업을 참조하십시오.

하이퍼바이저로 관리되는 가상 머신 보기

하이퍼바이저에서 가상 머신을 보려면

1. 왼쪽 탐색 창의 외부 리소스 섹션에서 하이퍼바이저를 선택합니다.
2. 하이퍼바이저 섹션에서 하이퍼바이저 이름을 기준으로 하이퍼바이저를 선택하면 해당 세부 정보 페이지로 이동합니다.
3. 하이퍼바이저 요약 아래의 섹션에서 가상 머신 탭을 선택합니다.
4. 연결된 가상 머신 섹션에는 가상 머신 목록이 자동으로 채워집니다.

하이퍼바이저에 연결된 게이트웨이 보기

하이퍼바이저에 연결된 게이트웨이를 보려면

1. 게이트웨이 탭을 선택합니다.
2. 연결된 게이트웨이 섹션에는 게이트웨이 목록이 자동으로 채워집니다.

하이퍼바이저를 추가 게이트웨이에 연결

백업 및 복원 속도는 게이트웨이와 하이퍼바이저 간 연결 대역폭에 의해 제한될 수 있습니다. 하나 이상의 추가 게이트웨이를 하이퍼바이저에 연결하여 속도를 높일 수 있습니다. 연결된 게이트웨이 섹션에서 다음과 같이 이 작업을 수행할 수 있습니다.

1. 연결을 선택합니다.
2. 드롭다운 메뉴를 사용하여 다른 게이트웨이를 선택합니다. 또는 게이트웨이 생성을 선택하여 새 게이트웨이를 생성합니다.
3. 연결을 선택합니다.

하이퍼바이저 구성 편집

게이트웨이 연결 테스트 기능을 사용하지 않는 경우 잘못된 사용자 이름 또는 암호로 하이퍼바이저를 추가할 수 있습니다. 이 경우 하이퍼바이저의 연결 상태는 항상 `Pending`입니다. 또는 사용자 이름 또는 암호를 교체하여 하이퍼바이저에 액세스할 수도 있습니다. 이 절차를 사용하여 다음 정보를 업데이트합니다.

이미 추가된 하이퍼바이저를 편집하려면

1. 왼쪽 탐색 창의 외부 리소스 섹션에서 하이퍼바이저를 선택합니다.
2. 하이퍼바이저 섹션에서 하이퍼바이저 이름을 기준으로 하이퍼바이저를 선택하면 해당 세부 정보 페이지로 이동합니다.
3. 편집을 선택합니다.
4. 상단 패널의 이름은 하이퍼바이저 설정입니다.
    a. vCenter Server 호스트에서 FQDN(정규화된 도메인 이름) 또는 IP 주소를 편집할 수도 있습니다.
    b. 선택적으로 하이퍼바이저의 사용자 이름 및 암호를 입력합니다.

5. 로그 그룹 설정 패널에서 CloudWatchAmazon과 통합하여 하이퍼바이저의 로그를 관리할 수 있습니다 (사용량에 따라 표준 CloudWatch 요금이 적용됨). 각 하이퍼바이저는 하나의 로그 그룹에 속할 수 있습니다.

   a. 아직 로그 그룹을 생성하지 않은 경우 새 로그 그룹 생성 라디오 버튼을 선택합니다. 편집 중인 하이퍼바이저는 이 로그 그룹과 연결됩니다.

   b. 이전에 다른 하이퍼바이저에 대한 로그 그룹을 생성한 경우 해당 로그 그룹을 이 하이퍼바이저에 사용할 수 있습니다. 기존 로그 그룹 사용을 선택합니다.

   c. 로깅을 원하지 않는 경우 CloudWatch 로깅 비활성화를 선택합니다.

> **Tip**
>
> Amazon CloudWatch Logs (위의 5단계 참조) 를 사용하여 오류 모니터링, 게이트웨이와 하이퍼바이저 간 네트워크 연결, 네트워크 구성 정보 등 하이퍼바이저에 대한 정보를 얻을 수 있습니다. CloudWatch 로그 그룹에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 로그 그룹 및 로그 스트림 작업을 참조하십시오.

하이퍼바이저를 프로그래밍 방식으로 업데이트하려면 CLI 명령 update-하이퍼바이저 및 API 호출을 사용합니다. UpdateHypervisor

하이퍼바이저 구성 삭제

이미 추가된 하이퍼바이저를 제거해야 하는 경우 하이퍼바이저 구성을 제거하고 다른 구성을 추가하세요. 이 제거 작업은 하이퍼바이저에 연결하기 위한 구성에 적용됩니다. 하이퍼바이저는 삭제되지 않습니다.

이미 추가된 하이퍼바이저에 연결하기 위한 구성을 삭제하려면

1. 왼쪽 탐색 창의 외부 리소스 섹션에서 하이퍼바이저를 선택합니다.
2. 하이퍼바이저 섹션에서 하이퍼바이저 이름을 기준으로 하이퍼바이저를 선택하면 해당 세부 정보 페이지로 이동합니다.
3. 제거를 선택한 다음 하이퍼바이저 제거를 선택합니다.
4. 선택 사항: 하이퍼바이저 추가의 절차를 사용하여 제거된 하이퍼바이저 구성을 교체합니다.

하이퍼바이저 상태 이해

다음은 가능한 각 하이퍼바이저 상태 및 문제 해결 단계(해당하는 경우)를 설명합니다. ONLINE 상태는 하이퍼바이저의 정상 상태입니다. 하이퍼바이저는 하이퍼바이저에서 관리하는 VM의 백업 및 복구에 사용되는 전체 또는 대부분의 시간 동안 이 상태를 유지해야 합니다.

하이퍼바이저 상태

상태 표시기	의미 및 문제 해결
ONLINE	하이퍼바이저를 추가하고 게이트웨이에 연결했으며 네트워크를 통해 해당 게이트웨이에 연결하여 하이퍼바이저로 관리되는 가상 머신의 백업 및 복구를 수행할 수 있습니다. AWS Backup 언제든지 이러한 가상 머신의 온디맨드 백업 및 예약 백업을 수행할 수 있습니다.
PENDING	하이퍼바이저를 추가했지만: AWS Backup • 어떤 게이트웨이와도 연결되지 않았습니다. 또는 • 하나 이상의 게이트웨이와 연결되어 있지만 해당 게이트웨이가 모두 삭제되었거나 활성화되지 않았습니다. 하이퍼바이저 상태를 PENDING에서 ONLINE으로 변경하려면 게이트웨이를 생성하고 하이퍼바이저를 해당 게이트웨이에 연결합니다.
OFFLINE	하이퍼바이저를 게이트웨이에 추가하고 게이트웨이에 연결했지만 게이트웨이는 네트워크를 통해 하이퍼바이저에 연결할 수 없습니다. AWS Backup 하이퍼바이저 상태를 OFFLINE에서 ONLINE으로 변경하려면 네트워크 구성이 정확한지 확인합니다.

상태 표시기	의미 및 문제 해결
	문제가 지속되면 하이퍼바이저의 IP 주소 또는 정규화된 도메인 이름이 올바른지 확인합니다. 해당 정보가 잘못된 경우 올바른 정보를 사용하여 하이퍼바이저를 다시 추가하고 게이트웨이 연결을 테스트합니다.
ERROR	하이퍼바이저를 추가하고 게이트웨이에 연결했지만 게이트웨이는 하이퍼바이저와 통신할 AWS Backup 수 없습니다. 하이퍼바이저 상태를 ERROR에서 ONLINE으로 변경하려면 하이퍼바이저의 사용자 이름 및 암호가 올바른지 확인합니다. 해당 정보가 잘못된 경우 하이퍼바이저 구성을 편집합니다.

다음 단계

하이퍼바이저의 가상 머신을 백업하려면 가상 머신 백업을 참조하세요.

가상 머신 백업

하이퍼바이저 추가 이후, Backup 게이트웨이는 사용자의 가상 머신을 자동으로 나열합니다. 왼쪽 탐색 창에서 하이퍼바이저 또는 가상 머신을 선택하여 가상 머신을 볼 수 있습니다.

- 특정 하이퍼바이저에서 관리하는 가상 머신만 보려면 하이퍼바이저를 선택합니다. 이 보기를 사용하면 한 번에 하나의 가상 머신에 대해서만 작업할 수 있습니다.
- 가상 머신을 선택하면 추가한 모든 하이퍼바이저의 모든 가상 머신을 볼 수 있습니다. AWS 계정이 보기를 사용하면 여러 하이퍼바이저의 일부 또는 모든 가상 머신에 대해 작업할 수 있습니다.

어떤 보기를 선택하든 특정 가상 머신에서 백업 작업을 수행하려면 해당 VM 이름을 선택하여 세부 정보 페이지를 여세요. VM 세부 정보 페이지는 다음 절차의 시작점입니다.

가상 머신의 온디맨드 백업 생성

온디맨드 백업은 수동으로 시작하는 일회성 전체 백업입니다. 온디맨드 백업을 사용하여 백업 및 복원 기능을 AWS Backup테스트할 수 있습니다.

가상 머신의 온디맨드 백업을 생성하려면

1. 온디맨드 백업 생성을 선택합니다.
2. 온디맨드 백업을 구성합니다
3. 온디맨드 백업 생성을 선택합니다.
4. 백업 작업의 상태가 `Completed`인지 확인합니다. 왼쪽 탐색 창에서 작업을 선택합니다.
5. 백업 작업 ID를 선택하여 백업 크기, 생성 날짜와 완료 날짜 사이에 경과된 시간과 같은 백업 작업 정보를 볼 수 있습니다.

증분 VM 백업

최신 VMware 버전에는 시간이 지남에 따라 변경되는 가상 머신의 스토리지 블록을 추적하는 변경된 블록 추적이라는 기능이 포함되어 있습니다. 를 사용하여 가상 시스템을 AWS Backup 백업할 때 CBT 데이터를 사용할 수 있는 경우 해당 데이터를 AWS Backup 사용하려고 시도합니다. AWS Backup CBT 데이터를 사용하여 백업 프로세스 속도를 높입니다. CBT 데이터가 없으면 백업 작업이 느려지고 하이퍼바이저 리소스가 더 많이 사용되는 경우가 많습니다. CBT 데이터가 유효하지 않거나 사용할 수 없는 경우에도 백업을 성공적으로 완료할 수 있습니다. 예를 들어 가상 머신 또는 ESXi 호스트가 강제 종료되는 경우 CBT 데이터가 유효하지 않거나 사용할 수 없을 수 있습니다.

CBT 데이터가 유효하지 않거나 사용할 수 없는 경우 백업 상태가 메시지와 함께 `Successful`로 표시됩니다. 이러한 경우 CBT 데이터가 없는 경우 VMware의 CBT 데이터 대신 자체 고유 변경 감지 메커니즘을 AWS Backup 사용하여 백업을 완료했다는 메시지가 표시됩니다. 후속 백업에서는 CBT 데이터를 다시 사용하려고 시도하며, 대부분의 경우 CBT 데이터는 유효하고 사용할 수 있게 됩니다. 문제가 지속되면 VMware 문제 해결에서 문제 해결 단계를 참조하세요.

CBT가 제대로 작동하려면 다음 조건이 충족되어야 합니다.

- 호스트가 ESXi 4.0 이상이어야 합니다.
- 디스크를 소유하는 VM에 하드웨어 버전 7 이상이 있어야 합니다.
- 가상 머신에 CBT가 활성화되어야 합니다(기본적으로 활성화됨).

가상 디스크에 CBT가 활성화되어 있는지 확인하려면

1. vSphere Client를 열고 전원이 꺼진 가상 머신을 선택합니다.
2. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 설정 편집 > 옵션 > 고급/일반 > 구성 파라미터로 이동합니다.

3. 옵션 `ctkEnabled`가 `True`여야 합니다.

백업 계획에 리소스를 할당하여 가상 머신 백업 자동화

백업 계획은 여러 AWS 서비스 및 서드 파티 애플리케이션에서 데이터 보호를 자동화하는 사용자 정의 데이터 보호 정책입니다. 먼저 백업 빈도, 보존 기간, 수명 주기 정책 및 기타 여러 옵션을 지정하여 백업 계획을 생성합니다. 백업 계획을 생성하려면 시작하기 자습서를 참조하세요.

백업 계획을 만든 후에는 가상 시스템을 포함하여 AWS Backup지원되는 리소스를 해당 백업 계획에 할당합니다. AWS Backup 는 계정의 모든 리소스를 할당 (특정 리소스 하나만 포함 또는 제외) 하거나 특정 태그가 있는 리소스를 추가하는 등 리소스를 할당하는 다양한 방법을 제공합니다.

기존 리소스 할당 기능 외에도 가상 컴퓨터 AWS Backup 지원에는 백업 계획에 가상 컴퓨터를 신속하게 할당하는 데 도움이 되는 몇 가지 새로운 기능이 도입되었습니다. 가상 머신 페이지에서 여러 가상 머신에 태그를 할당하거나 새로운 계획에 리소스 할당 기능을 사용할 수 있습니다. 이러한 기능을 사용하여 AWS Backup 게이트웨이에서 이미 검색된 가상 컴퓨터를 할당할 수 있습니다.

향후에 추가 가상 머신을 검색하여 할당할 계획이고 향후 가상 머신을 포함하도록 리소스 할당 단계를 자동화하려면 새로운 그룹 할당 생성 기능을 사용하세요.

VMware 태그

태그는 리소스를 관리, 필터링, 검색하는 데 도움이 되는 키-값 페어입니다.

VMware 태그는 범주 및 태그 이름으로 구성됩니다. VMware 태그는 가상 머신을 그룹화하는 데 사용됩니다. 태그 이름은 가상 머신에 할당되는 레이블입니다. 범주는 태그 이름 모음입니다.

AWS 태그에는 UTF-8 문자, 숫자, 공백 및 특수 문자 중 문자를 사용할 수 `+ - = . _ : /` 있습니다.

가상 머신에 태그를 사용하는 경우 구성에 도움이 되도록 AWS Backup 에 일치 태그를 최대 10개까지 추가할 수 있습니다. 최대 10개의 VMware 태그를 태그에 매핑할 AWS 수 있습니다. AWS Backup 콘솔에서 이러한 항목은 내 조직 > 가상 시스템 > AWS 태그 또는 VMware 태그에서 찾을 수 있습니다.

VMware 태그 매핑

가상 머신에 태그를 사용하는 경우 명확성 및 구성에 도움이 되도록 AWS Backup 에 일치 태그를 최대 10개까지 추가할 수 있습니다. 매핑은 하이퍼바이저의 모든 가상 머신에 적용됩니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 콘솔에서 하이퍼바이저 편집으로 이동합니다(외부 리소스, 하이퍼바이저, 하이퍼바이저 이름, 매핑 관리를 차례로 클릭).

3. 마지막 창인 VMware 태그 매핑에는 기존 VMware 태그 정보를 해당 태그에 입력할 수 있는 네 개의 입력란 필드가 있습니다. AWS 네 개의 필드는 VMware 태그 범주, VMware 태그 이름, 태그 키 및AWS AWS 태그 값입니다 (예: 범주 = OS, 태그 이름 = Windows, 태그 키 = OS-Windows, AWS 태그 값 = Windows). AWS
4. 원하는 값을 입력한 후 매핑 추가를 클릭합니다. 잘못 입력한 경우 제거를 클릭하여 입력한 정보를 삭제할 수 있습니다.
5. 매핑을 추가한 후 이러한 AWS 태그를 VMware 가상 머신에 적용하는 데 사용할 IAM 역할을 지정합니다.

   정책 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync에는 필요한 권한이 포함되어 있습니다. 사용 중인 역할에 이 정책을 연결하거나 관리자에게 이 정책을 연결하도록 요청하거나 사용 중인 역할에 대한 사용자 지정 정책을 생성할 수 있습니다.
6. 마지막으로 하이퍼바이저 추가 또는 저장을 클릭합니다.

backup-gateway.amazonaws.com 및 backup.amazonaws.com 서비스를 추가하려면 IAM 역할 신뢰 관계를 수정해야 합니다. 이 서비스가 없으면 태그를 매핑할 때 오류가 발생할 수 있습니다. 기존 역할에서 신뢰 관계를 편집하려면

1. IAM 콘솔에 로그인합니다.
2. 콘솔의 탐색 창에서 역할을 선택합니다.
3. 수정하려는 역할의 이름을 선택한 후 세부 정보 페이지에서 신뢰 관계 탭을 선택합니다.
4. 정책 문서 아래에 다음을 붙여넣습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. 신뢰 정책 업데이트를 선택합니다.

자세한 내용은 AWS Directory Service 관리 안내서의 기존 역할에 대한 신뢰 관계 편집을 참조하세요.

VMware 태그 매핑 보기

AWS Backup 콘솔에서 외부 리소스를 클릭한 다음 하이퍼바이저를 클릭한 다음 하이퍼바이저 이름 링크를 클릭하여 선택한 하이퍼바이저의 속성을 확인합니다. 요약 창 아래에는 네 개의 탭이 있으며, 마지막 탭은 VMware 태그 매핑입니다. 아직 매핑이 아직 없는 경우 'VMware 태그 매핑 없음'이 표시됩니다.

여기에서 하이퍼바이저로 검색된 가상 머신의 메타데이터를 동기화하고, 하이퍼바이저에 매핑을 복사하거나, VMware AWS 태그에 매핑된 태그를 백업 계획의 백업 선택에 추가하거나, 매핑을 관리할 수 있습니다.

콘솔에서 선택한 가상 머신에 적용되는 태그를 확인하려면 가상 머신을 클릭하고 가상 머신 이름을 클릭한 다음 AWS 태그 또는 VMware 태그를 클릭합니다. 이 가상 머신과 연결된 태그를 볼 수 있으며 태그를 관리할 수도 있습니다.

VMware 태그 매핑을 사용하여 계획에 가상 머신 할당

매핑된 태그를 사용하여 백업 계획에 가상 머신을 할당하려면 다음 작업을 수행합니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 콘솔에서 하이퍼바이저 세부 정보 페이지의 VMware 태그 매핑으로 이동합니다(외부 리소스를 클릭하고 하이퍼바이저를 클릭한 다음 하이퍼바이저 이름을 클릭).
3. 매핑된 여러 태그 옆의 확인란을 선택하여 해당 태그를 동일한 백업 계획에 할당합니다.
4. 리소스 할당에 추가를 클릭합니다.
5. 드롭다운 목록에서 기존 백업 계획을 선택합니다. 또는 백업 계획 생성을 선택하여 새 백업 계획을 생성할 수 있습니다.
6. 확인을 클릭합니다. 그러면 태그를 사용하여 선택 영역 구체화 필드에 값이 미리 채워진 리소스 할당 페이지가 열립니다.

VMware 태그는 다음을 사용합니다. AWS CLI

AWS Backup API 호출을 `PutHypervisorPropertyMappings`사용하여 온프레미스의 하이퍼바이저 엔티티 속성을 내부 속성에 매핑합니다. AWS

AWS CLI에서는 다음 작업을 사용합니다. `put-hypervisor-property-mappings`

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

예:

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

GetHypervisorPropertyMappings를 사용하여 속성 매핑 정보를 지원할 수도 있습니다. AWS CLI에서는 작업을 사용합니다`get-hypervisor-property-mappings`. 다음은 예제 템플릿입니다.

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

예:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

API, CLI 또는 SDK를 AWS 사용하여 하이퍼바이저가 검색한 가상 시스템의 메타데이터를 동기화합니다.

가상 머신의 메타데이터를 동기화할 수 있습니다. 이렇게 하면 가상 머신에 있는 매핑의 일부인 VMware 태그가 동기화됩니다. 또한 가상 머신에 있는 VMware 태그에 매핑된 AWS 태그가 AWS 가상 머신 리소스에 적용됩니다.

AWS Backup API 호출을 StartVirtualMachinesMetadataSync사용하여 하이퍼바이저에서 검색된 가상 머신의 메타데이터를 동기화합니다. AWS CLI를 사용하여 하이퍼바이저가 검색한 가상 머신의 메타데이터를 동기화하려면 `start-virtual-machines-metadata-sync` 작업을 사용합니다.

템플릿 예제:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

예제

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

또한 GetHypervisor를 사용하여 호스트, 상태, 최신 메타데이터 동기화 상태와 같은 하이퍼바이저 정보를 지원하고 마지막으로 성공한 메타데이터 동기화 시간을 검색할 수도 있습니다. AWS CLI에서는 작업을 사용합니다. `get-hypervisor`

템플릿 예제:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

예제

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

자세한 내용은 API 설명서 VmwareTag및 을 참조하십시오 VmwareToAwsTagMapping.

이 기능은 2022년 12월 15일 이후 배포된 새 게이트웨이에서 사용할 수 있습니다. 기존 게이트웨이의 경우 2023년 1월 30일 또는 그 이전에 자동 소프트웨어 업데이트를 통해 이 새로운 기능을 사용할 수 있습니다. 게이트웨이를 최신 버전으로 수동으로 업데이트하려면 AWS CLI 명령을 사용하십시오 UpdateGatewaySoftwareNow.

예제

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

태그를 사용하여 가상 머신 할당

기존 백업 계획 중 하나에 이미 할당한 태그를 할당하여 다른 AWS Backup 리소스와 함께 현재 검색된 가상 시스템을 할당할 수 있습니다. AWS Backup새 백업 계획과 새 태그 기반 리소스 할당을 생성할 수도 있습니다. 백업 계획은 백업 작업을 실행할 때마다 새로 할당된 리소스를 확인합니다.

여러 가상 머신에 동일한 태그를 지정하려면

1. 왼쪽 탐색 창에서 가상 머신 을 선택합니다.
2. VM 이름 옆의 확인란을 선택하여 모든 가상 머신을 선택합니다. 또는 태그를 지정하려는 VM 이름 옆의 확인란을 선택합니다.
3. 태그 추가를 선택합니다.
4. 태그 키를 입력합니다.
5. 권장: 태그 값을 입력합니다.
6. 확인을 선택합니다.

계획에 리소스 할당 기능을 사용하여 가상 머신 할당

계획에 리소스 할당 기능을 사용하여 현재 검색된 AWS Backup 가상 시스템을 기존 또는 새 백업 계획에 할당할 수 있습니다.

계획에 리소스 할당 기능을 사용하여 가상 머신을 할당하려면

1. 왼쪽 탐색 창에서 가상 머신 을 선택합니다.
2. VM 이름 옆의 확인란을 선택하여 모든 가상 머신을 선택합니다. 또는 여러 VM 이름 옆의 확인란을 선택하여 동일한 백업 계획에 할당할 수도 있습니다.
3. 할당을 선택한 다음 계획에 리소스 할당을 선택합니다.
4. 리소스 할당 이름을 입력합니다.
5. 리소스 할당 IAM 역할을 선택하여 백업을 생성하고 복구 시점을 관리합니다. 사용할 특정 IAM 역할이 없는 경우 올바른 권한이 있는 기본 역할을 사용하는 것이 좋습니다.
6. 백업 계획 섹션의 드롭다운 목록에서 기존 백업 계획을 선택합니다. 또는 백업 계획 생성을 선택하여 새 백업 계획을 생성합니다.
7. 리소스 할당을 선택합니다.
8. 선택 사항: 백업 계획 보기를 선택하여 가상 머신이 백업 계획에 할당되었는지 확인합니다. 그런 다음 리소스 할당 섹션에서 리소스 할당 이름을 선택합니다.

그룹 할당 생성 기능을 사용하여 가상 머신 할당

위의 두 가상 컴퓨터에 대한 리소스 할당 기능과 달리 그룹 할당 생성 기능은 현재 검색된 가상 컴퓨터뿐만 아니라 사용자가 AWS Backup정의한 폴더 또는 하이퍼바이저에서 미래에 발견될 가상 컴퓨터도 할당합니다.

또한 그룹 할당 생성 기능을 사용하기 위해 확인란을 선택할 필요가 없습니다.

계획에 리소스 할당 기능을 사용하여 가상 머신을 할당하려면

1. 왼쪽 탐색 창에서 가상 머신 을 선택합니다.
2. 할당을 선택한 다음 그룹 할당 생성을 선택합니다.
3. 리소스 할당 이름을 입력합니다.
4. 리소스 할당 IAM 역할을 선택하여 백업을 생성하고 복구 시점을 관리합니다. 사용할 특정 IAM 역할이 없는 경우 올바른 권한이 있는 기본 역할을 사용하는 것이 좋습니다.
5. 리소스 그룹 섹션에서 그룹 유형 드롭다운 메뉴를 선택합니다. 폴더 또는 하이퍼바이저 옵션이 있습니다.

   a. 하이퍼바이저의 폴더에 있는 모든 가상 머신을 할당하려면 폴더를 선택합니다. 드롭다운 메뉴를 사용하여 폴더 그룹 이름(예: `datacenter/vm`)을 선택합니다. 하위 폴더를 포함하도록 선택할 수도 있습니다.

   > **Note**
   >
   > 폴더 기반 할당을 수행하려면 검색 프로세스 중에 가상 시스템이 찾은 폴더로 가상 컴퓨터에 AWS Backup 태그를 지정해야 합니다. 나중에 가상 시스템을 다른 폴더로 이동하는 경우 AWS 태그 지정 모범 사례로 인해 태그를 업데이트할 AWS Backup 수 없습니다. 이 할당 방법을 사용하면 할당된 폴더 밖으로 이동한 가상 머신의 백업을 계속 생성하게 될 수 있습니다.

   b. 하이퍼바이저로 관리되는 모든 가상 머신을 할당하려면 하이퍼바이저를 선택합니다. 드롭다운 메뉴를 사용하여 하이퍼바이저 ID 그룹 이름을 선택합니다.
6. 백업 계획 섹션의 드롭다운 목록에서 기존 백업 계획을 선택합니다. 또는 백업 계획 생성을 선택하여 새 백업 계획을 생성합니다.
7. 그룹 할당 생성을 선택합니다.
8. 선택 사항: 백업 계획 보기를 선택하여 가상 머신이 백업 계획에 할당되었는지 확인합니다. 리소스 할당 섹션에서 리소스 할당 이름을 선택합니다.

다음 단계

가상 머신을 복원하려면 다음을 사용하여 가상 시스템을 복원합니다. AWS Backup을 참조하세요.

Backup 게이트웨이의 서드 파티 소스 구성 요소 관련 정보

이 섹션에서는 Backup 게이트웨이 기능을 제공하는 데 사용하는 서드 파티 도구 및 라이선스에 대한 정보를 제공합니다.

Backup 게이트웨이 소프트웨어에 포함된 특정 서드 파티 소스 소프트웨어 구성 요소의 소스 코드는 다음 위치에서 다운로드할 수 있습니다.

- VMware ESXi에 배포된 게이트웨이의 경우 sources.tgz를 다운로드합니다.

이 제품에는 OpenSSL 툴킷 (https://www.openssl.org/) 에서 사용하기 위해 OpenSSL 프로젝트에서 개발한 소프트웨어가 포함되어 있습니다.

이 제품에는 VMware® vSphere 소프트웨어 개발 키트(https://www.vmware.com)에서 개발한 소프트웨어가 포함되어 있습니다.

모든 종속 서드 파티 도구와 관련된 라이선스는 서드 파티 라이선스를 참조하세요.

AWS 어플라이언스용 오픈 소스 구성 요소

Backup 게이트웨이의 기능을 제공하기 위해 여러 서드 파티 도구 및 라이선스가 사용됩니다.

다음 링크를 사용하여 어플라이언스 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드를 다운로드하십시오. AWS

- VMware ESXi에 배포된 게이트웨이의 경우 sources.tar을 다운로드합니다.

이 제품에는 OpenSSL 툴킷 (https://www.openssl.org/) 에서 사용하기 위해 OpenSSL 프로젝트에서 개발한 소프트웨어가 포함되어 있습니다. 모든 종속 서드 파티 도구와 관련된 라이선스는 서드 파티 라이선스를 참조하세요.

VM 문제 해결

증분 백업/CBT 문제 및 메시지

오류 메시지: **"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."**

이 메시지가 계속되면 VMware의 지시에 따라 CBT를 재설정하세요.

메시지는 CBT가 활성화되지 않았거나 사용할 수 없음을 나타냅니다. “이 가상 머신에는 VMware CBT(변경 블록 추적)를 사용할 수 없었지만 당사의 독점적인 변경 메커니즘을 사용하여 증분 백업이 성공적으로 완료되었습니다.”

CBT가 활성화되어 있는지 확인하세요. 가상 디스크에 CBT가 활성화되어 있는지 확인하려면

1. vSphere Client를 열고 전원이 꺼진 가상 머신을 선택합니다.
2. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 설정 편집 > 옵션 > 고급/일반 > 구성 파라미터로 이동합니다.
3. 옵션 `ctkEnabled`가 `True`여야 합니다.

이 기능이 켜져 있는 경우 VMware 기능을 사용하고 up-to-date 있는지 확인하십시오. 호스트는 ESXi 4.0 이상이어야 하고 추적할 디스크를 소유한 가상 머신은 하드웨어 버전 7 이상이어야 합니다.

CBT가 활성화되어 있고 소프트웨어 및 하드웨어가 최신 버전이면 가상 머신을 껐다가 다시 켭니다. CBT가 활성화되는지 확인합니다. 그런 다음 백업을 다시 수행합니다.

고급 DynamoDB 백업

AWS Backup Amazon DynamoDB 데이터 보호 요구 사항을 위한 추가 고급 기능을 지원합니다. 에서 AWS Backup의 고급 기능을 활성화하면 새로 생성하는 모든 DynamoDB 테이블 백업에 대해 다음 기능을 잠금 해제할 수 있습니다. AWS 리전

- 비용 절감 및 최적화:
  - 백업을 콜드 스토리지로 계층화하여 스토리지 비용 절감
  - Cost Explorer와 함께 사용하기 위한 비용 할당 태깅
- 비즈니스 연속성:
  - 교차 리전 복사
  - 교차 계정 복사
- 보안:
  - 백업은 AWS Backup 볼트 잠금, AWS Backup 정책 및 암호화 키로 보호할 수 있는 암호화된 AWS Backup 볼트에 저장합니다.
  - 백업은 소스 DynamoDB 테이블에서 태그를 상속하므로 이러한 태그를 사용하여 권한 및 서비스 제어 정책 (SCP)을 설정할 수 있습니다.

2021년 11월 AWS Backup 이후에 가입하는 신규 고객에게는 고급 DynamoDB 백업 기능이 기본적으로 활성화되어 있습니다. 특히, 2021년 11월 21일 이전에 백업 볼트를 생성하지 않은 고객에게는 고급 DynamoDB 백업 기능이 기본적으로 활성화됩니다.

모든 기존 AWS Backup 고객이 DynamoDB의 고급 기능을 활성화하는 것이 좋습니다. 고급 기능을 활성화한 후 웜 백업 스토리지 요금에는 차이가 없습니다. 백업을 콜드 스토리지로 계층화하여 비용을 절감하고 비용 할당 태그를 사용하여 비용을 최적화할 수 있습니다. AWS Backup의 비즈니스 연속성 및 보안 기능을 활용할 수도 있습니다.

> **Note**
>
> 기본 서비스 역할 대신 사용자 지정 역할 또는 정책을 사용하는 경우 사용자 지정 역할에 다음 권한 정책을 추가 또는 사용하거나 이에 상응하는 권한을 추가해야 합니다. AWS Backup
>
> - 고급 DynamoDB 백업을 수행하기 위한 `AWSBackupServiceRolePolicyForBackup`
> - 고급 DynamoDB 백업을 복원하기 위한 `AWSBackupServiceRolePolicyForRestores`
>
> AWS-managed 정책에 대해 자세히 알아보고 고객 관리형 정책의 예를 보려면 을 참조하십시오. 관리형 정책 대상 AWS Backup

주제

콘솔을 사용하여 고급 DynamoDB 백업 활성화

AWS Backup 또는 DynamoDB 콘솔 중 하나를 사용하여 DynamoDB 백업의 AWS Backup 고급 기능을 활성화할 수 있습니다.

콘솔에서 고급 DynamoDB 백업 기능을 활성화하려면: AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 메뉴에서 설정을 선택합니다.
3. 지원되는 서비스 섹션에서 DynamoDB가 활성화됨인지 확인합니다.

   그렇지 않은 경우 옵트인을 선택하고 DynamoDB를 AWS Backup 지원 서비스로 활성화합니다.
4. DynamoDB 백업에 대한 고급 기능 섹션에서 활성화를 선택합니다.
5. 기능 활성화를 선택합니다.

DynamoDB 콘솔을 사용하여 AWS Backup 고급 기능을 활성화하는 방법은 Amazon DynamoDB AWS Backup 사용 설명서의 기능 활성화를 참조하십시오.

프로그래밍 방식으로 고급 DynamoDB 백업 활성화

AWS Command Line Interface (CLI) 를 사용하여 DynamoDB 백업의 AWS Backup 고급 기능을 활성화할 수도 있습니다. 다음 값을 모두 `true`로 설정하면 고급 DynamoDB 백업이 활성화됩니다.

프로그래밍 방식으로 DynamoDB 백업의 AWS Backup 고급 기능을 활성화하려면:

1. 다음 명령을 사용하여 DynamoDB의 AWS Backup 고급 기능을 이미 활성화했는지 확인하십시오.

   ```
   $ aws backup describe-region-settings
   ```

   `"ResourceTypeManagementPreference"` 및 `"ResourceTypeOptInPreference"` 모두 `"DynamoDB":true`인 경우 고급 DynamoDB 백업을 이미 활성화한 것입니다.

   다음 출력과 같이 `"DynamoDB":false` 인스턴스가 하나 이상 있는 경우 고급 DynamoDB 백업을 아직 활성화하지 않은 것이므로 다음 단계로 진행하세요.

   ```
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
     "ResourceTypeOptInPreference":{
       "Aurora":true,
       "DocumentDB":false,
       "DynamoDB":false,
       "EBS":true,
       "EC2":true,
       "EFS":true,
       "FSx":true,
   ```

```
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. 다음 UpdateRegionSettings 작업을 사용하여 "ResourceTypeManagementPreference" 및 "ResourceTypeOptInPreference" 둘 다 "DynamoDB":true로 설정합니다.

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

고급 DynamoDB 백업 편집

고급 기능을 AWS Backup 활성화한 후 DynamoDB 백업을 생성하면 다음을 사용할 수 있습니다. AWS Backup

- 리전 간에 백업 복사
- 계정 간에 백업 복사
- 백업을 콜드 스토리지로 AWS Backup 계층화하는 시기 변경
- 백업에 태그 지정

기존 백업에서 이러한 고급 기능을 사용하려면 백업 편집을 참조하세요.

나중에 DynamoDB의 AWS Backup 고급 기능을 비활성화해도 고급 기능을 활성화한 기간 동안 생성한 DynamoDB 백업에 해당 작업을 계속 수행할 수 있습니다.

고급 DynamoDB 백업 복원

고급 기능을 활성화하기 전에 수행한 DynamoDB 백업을 복원하는 것과 동일한 방식으로 고급 기능을 활성화한 AWS Backup 상태에서 수행한 DynamoDB 백업을 복원할 수 있습니다. AWS Backup 둘 중 하나 AWS Backup 또는 DynamoDB를 사용하여 복원을 수행할 수 있습니다.

다음 옵션을 사용하여 새로 복원한 테이블을 암호화하는 방법을 지정할 수 있습니다.

- 원본 테이블과 동일한 리전에 복원하는 경우 복원된 테이블의 암호화 키를 선택적으로 지정할 수 있습니다. 암호화 키를 지정하지 않으면 원래 테이블을 암호화한 것과 동일한 키를 사용하여 복원된 테이블을 자동으로 암호화합니다. AWS Backup

- 원본 테이블과 다른 리전에서 복원하는 경우 암호화 키를 지정해야 합니다.

를 사용하여 AWS Backup복원하려면 을 참조하십시오Amazon DynamoDB 테이블 복원.

DynamoDB를 사용하여 복원하려면 Amazon DynamoDB 사용 설명서의 백업에서 DynamoDB 테이블 복원을 참조하세요.

고급 DynamoDB 백업 삭제

이러한 고급 기능을 사용하여 생성된 백업은 DynamoDB에서 삭제할 수 없습니다. AWS 환경 전체에서 글로벌 일관성을 유지하려면 백업을 삭제하는 데 AWS Backup 을 사용해야 합니다.

DynamoDB 백업을 삭제하려면 백업 삭제 단원을 참조하세요.

고급 DynamoDB 백업을 활성화하는 경우 전체 AWS Backup 관리가 제공하는 기타 이점

DynamoDB의 AWS Backup 고급 기능을 활성화하면 DynamoDB 백업을 완벽하게 관리할 수 있습니다. AWS Backup이렇게 하면 다음과 같은 추가 이점이 제공됩니다.

암호화(Encryption)

AWS Backup 대상 저장소의 KMS 키를 사용하여 백업을 자동으로 암호화합니다. AWS Backup 이전에는 소스 DynamoDB 테이블과 동일한 암호화 방법을 사용하여 암호화되었습니다. 이렇게 하면 데이터를 보호하는 데 사용할 수 있는 방어 수단이 늘어납니다. 자세한 정보는 내 백업을 위한 암호화 AWS Backup을 참조하세요.

Amazon 리소스 이름(ARN)

각 백업 ARN의 서비스 네임스페이스는 awsbackup입니다. 이전에는 서비스 네임스페이스가 dynamodb였습니다. 다시 말해, 각 ARN의 시작 부분이 `arn:aws:dynamodb`에서 `arn:aws:backup`으로 변경됩니다. 서비스 권한 부여 AWS Backup참조의 ARN을 참조하십시오.

이번 변경으로 사용자 또는 사용자의 백업 관리자는 이제 고급 기능을 활성화한 후 생성되는 DynamoDB 백업에 적용되는 awsbackup 서비스 네임스페이스를 사용하여 백업에 대한 액세스 정책을 생성할 수 있습니다. awsbackup 서비스 네임스페이스를 사용하여 AWS Backup에서 생성한 다른 백업에도 정책을 적용할 수 있습니다. 자세한 정보는 액세스 제어을 참조하세요.

청구서 상의 요금 위치

백업 비용 (스토리지, 데이터 전송, 복원 및 조기 삭제 포함) 은 AWS 청구서의 “Backup”에 표시됩니다. 이전에는 청구서의 ‘DynamoDB’ 아래에 요금이 표시되었습니다.

이번 변경으로 AWS Backup 청구를 사용하여 백업 비용을 중앙에서 모니터링할 수 있습니다. 자세한 정보는 측정, 비용 및 청구을 참조하세요.

Amazon Timestream 백업

Amazon Timestream은 매일 최대 1조 개의 시계열 데이터 포인트를 저장 및 분석할 수 있는 확장 가능한 시계열 데이터베이스입니다. Timestream은 최신 데이터를 메모리에 보관하고 정책에 따라 비용 최적화된 스토리지 계층에 과거 데이터를 저장함으로써 비용 및 시간 절감에 최적화되었습니다.

Timestream 데이터베이스에는 테이블이 있습니다. 이 테이블에는 레코드가 포함되어 있으며 각 레코드는 시계열에 있는 단일 데이터 포인트입니다. 시계열은 주가, Amazon EC2 인스턴스의 메모리 사용 수준 또는 온도 측정값과 같이 일정 기간 동안 기록되는 일련의 기록입니다. AWS Backup 타임스트림 테이블을 중앙에서 백업 및 복원할 수 있습니다. 이러한 테이블 백업을 같은 조직 AWS 리전 내의 다른 계정과 다른 여러 계정에 복사할 수 있습니다.

Timestream은 현재 기본 백업 및 복원 서비스를 제공하지 않으므로 Timestream 테이블의 보안 복사본을 만드는 AWS Backup 데 사용하면 리소스에 보안 및 복원력을 한 층 더 강화할 수 있습니다.

Timestream 테이블 백업

AWS Backup 콘솔이나 를 사용하여 Timestream 테이블을 백업할 수 있습니다. AWS CLI

AWS Backup 콘솔을 사용하여 Timestream 테이블을 백업하는 방법에는 필요에 따라 백업하는 방법과 백업 계획의 일부로 백업하는 두 가지 방법이 있습니다.

온디맨드 Timestream 백업 생성

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창을 사용하여, 보호된 리소스를 선택한 다음 온디맨드 백업 생성을 선택합니다.
3. 온디맨드 백업 생성 페이지에서 Amazon Timestream을 선택합니다.
4. 리소스 유형 Timestream을 선택한 다음 백업하려는 테이블 이름을 선택합니다.
5. 백업 창에서 지금 백업 생성이 선택되었는지 확인합니다. 이를 선택하면 백업이 즉시 시작되고 클러스터를 보호된 리소스 페이지에서 더 빨리 확인할 수 있습니다.
6. 콜드 스토리지로 전환 드롭다운 메뉴에서 전환 설정을 지정할 수 있습니다.
7. 보존 기간에서 백업을 유지할 기간을 선택할 수 있습니다.

8. 기존 백업 볼트를 선택하거나 새 백업 볼트를 생성합니다. 새 백업 볼트 생성을 선택하면 볼트를 생성하는 새 페이지가 열린 후 작업 완료 시 온디맨드 백업 생성 페이지로 돌아갑니다.
9. IAM 역할에서 기본 역할을 선택합니다. 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 사용하여 자동으로 생성됩니다.
10. 선택적으로 복구 시점에 태그를 추가할 수 있습니다. 온디맨드 백업에 하나 이상의 태그를 할당하려면 키 및 값(선택 사항)을 입력하고 태그 추가를 선택합니다.
11. 온디맨드 백업 생성을 선택합니다. 그러면 작업 페이지로 이동합니다. 여기서 작업 목록을 볼 수 있습니다.
12. 해당 작업의 세부 정보를 보려면 클러스터의 백업 작업 ID를 선택합니다. 상태가 `Completed`, `In Progress` 또는 `Failed`로 표시됩니다. 새로 고침 버튼을 클릭하여 표시된 상태를 업데이트할 수 있습니다.

백업 계획에서 예약된 Timestream 백업을 생성합니다.

Timestream 테이블이 보호된 리소스인 경우 예약 백업에 포함할 수 있습니다. Amazon Timestream 테이블을 보호하도록 선택하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택합니다.
3. Amazon Timestream을 켜기로 전환합니다.
4. 기존 계획 또는 새 계획에 Timestream 테이블을 포함하려면 콘솔에 리소스 할당을 참조하세요.

백업 계획 관리에서 백업 계획을 생성하고 Timestream 테이블을 포함하도록 선택하거나 Timestream 테이블을 포함하도록 기존 계획을 업데이트할 수 있습니다. 리소스 유형 Timestream을 추가할 때 모든 Timestream 테이블을 추가하거나 특정 리소스 유형 선택에서 추가하려는 테이블 옆의 확인란을 선택할 수 있습니다.

Timestream 테이블로 구성된 첫 번째 백업은 전체 백업입니다. 후속 백업은 증분 백업입니다.

백업 계획을 생성하거나 수정한 후에는 왼쪽 탐색 메뉴에서 백업 계획으로 이동합니다. 지정한 백업 계획은 리소스 할당 아래에 클러스터를 표시해야 합니다.

프로그래밍 방식 백업

`start-backup-job` 작업을 사용할 수 있습니다. 다음 파라미터를 포함합니다.

```
aws backup start-backup-job \
```

```
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region AWS ## \
--endpoint-url URL
```

Timestream 테이블 백업 보기

콘솔에서 Timestream 테이블 백업을 보고 수정하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 볼트를 선택합니다. 그런 다음 Timestream 테이블이 들어 있는 백업 볼트 이름을 클릭합니다.
3. 백업 볼트에는 요약 및 백업 목록이 표시됩니다.

    a. 복구 시점 ID 열에서 링크를 클릭하거나

    b. 복구 시점 ID 왼쪽의 확인란을 선택하고 작업을 클릭하여 더 이상 필요하지 않은 복구 시점을 삭제할 수 있습니다.

Timestream 테이블 복원

Timestream 테이블을 복원하는 방법을 참조하세요.

Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업

> **Note**
>
> 지원되는 서비스는 다음과 같습니다. AWS 리전Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업을 사용할 수 있는 현재 지원되는 지역을 포함합니다.

AWS Backup Amazon EC2 인스턴스에서 SAP HANA 데이터베이스의 백업 및 복원을 지원합니다.

주제

- 다음을 포함하는 SAP HANA 데이터베이스의 개요 AWS Backup
- 를 통해 SAP HANA 데이터베이스를 백업하기 위한 사전 요구 사항 AWS Backup
- 콘솔에서의 SAP HANA 백업 작업 AWS Backup

- SAP HANA 데이터베이스 백업 보기
- 다음과 AWS CLI 같은 SAP HANA 데이터베이스에 사용하십시오. AWS Backup
- SAP HANA 데이터베이스 백업 문제 해결
- 사용 시 SAP HANA 용어에 대한 용어집 AWS Backup
- AWS Backup EC2 인스턴스의 SAP HANA 데이터베이스 지원 릴리스 노트

다음을 포함하는 SAP HANA 데이터베이스의 개요 AWS Backup

백업을 생성하고 데이터베이스를 복원하는 기능 외에도 Amazon EC2 Systems Manager for SAP와의 AWS Backup 통합을 통해 고객은 SAP HANA 데이터베이스를 식별하고 태그를 지정할 수 있습니다.

AWS Backup AWS Backint Agent와 통합되어 SAP HANA 백업 및 복원을 수행합니다. 자세한 내용은 AWS Backint를 참조하세요.

를 통해 SAP HANA 데이터베이스를 백업하기 위한 사전 요구 사항 AWS Backup

백업 및 복원 작업을 수행하려면 몇 가지 사전 요구 사항을 완료해야 합니다. 참고: 이러한 단계를 수행하려면 SAP HANA 데이터베이스에 대한 관리 액세스 권한과 AWS 계정에 새 IAM 역할 및 정책을 생성할 수 있는 권한이 필요합니다.

Amazon EC2 Systems Manager에서 이러한 사전 요구 사항을 완료하세요.

1. SAP HANA 데이터베이스를 실행하는 Amazon EC2 인스턴스에 필요한 권한을 설정
2. 에 자격 증명을 등록하십시오. AWS Secrets Manager
3. AWS Backint 및 SAP AWS Systems Manager 에이전트용 설치
4. SSM 에이전트를 확인
5. 파라미터를 확인
6. SAP HANA 데이터베이스를 등록

각 HANA 인스턴스를 한 번만 등록하는 것이 가장 좋습니다. 여러 번 등록하면 동일한 데이터베이스에 대해 여러 ARN이 생성될 수 있습니다. 단일 ARN 및 등록을 유지하면 백업 계획 생성 및 유지 관리가 단순화되고 계획되지 않은 백업 중복을 줄일 수 있습니다.

콘솔에서의 SAP HANA 백업 작업 AWS Backup

사전 요구 사항 및 SAP용 SSM 설정이 완료되면 SAP HANA on EC2 데이터베이스를 백업하고 복원할 수 있습니다.

SAP HANA 리소스를 보호하도록 선택

SAP HANA 데이터베이스를 보호하는 AWS Backup 데 사용하려면 SAP HANA를 보호 리소스 중 하나로 설정해야 합니다. 옵트인하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 서비스 옵트인에서 리소스 구성을 선택합니다.
4. SAP HANA on Amazon EC2를 옵트인합니다.
5. 확인을 클릭합니다.

SAP HANA on Amazon EC2에 대한 서비스 옵트인이 이제 활성화됩니다.

SAP HANA 데이터베이스의 스케줄 지정 백업을 생성합니다.

기존 백업 계획을 편집하여 SAP HANA 리소스를 추가하거나 SAP HANA 리소스만을 위한 새 백업 계획을 생성할 수 있습니다.

새 백업 계획을 생성하기로 선택한 경우 다음과 같은 세 가지 옵션이 있습니다.

1. 옵션 1: 템플릿을 사용하여 시작
    1. 백업 계획 템플릿을 선택합니다.
    2. 백업 계획 이름을 지정합니다.
    3. 계획 생성을 클릭합니다.
2. 옵션 2: 새 계획 작성
    1. 백업 계획 이름을 지정합니다.
    2. 선택적으로 백업 계획에 추가할 태그를 지정합니다.
    3. 백업 규칙 구성을 지정합니다.
        a. 백업 규칙 이름을 지정합니다.
        b. 기존 볼트를 선택하거나 새 백업 볼트를 생성합니다. 여기에 백업이 저장됩니다.
        c. 백업 빈도를 지정합니다.
        d. 백업 기간을 지정합니다.

            콜드 스토리지로 전환은 현재 지원되지 않습니다.

e. 보존 기간을 지정합니다.

대상으로 복사는 현재 지원되지 않습니다.

f. (선택 사항) 복구 시점에 추가할 태그를 지정합니다.

4. 계획 생성을 클릭합니다.

3. 옵션 3: JSON을 사용하여 계획 정의

1. 기존 백업 계획의 JSON 표현식을 수정하거나 새 표현식을 생성하여 백업 계획의 JSON을 지정합니다.
2. 백업 계획 이름을 지정합니다.
3. JSON 검증을 클릭합니다.

백업 계획이 성공적으로 생성되면 다음 단계에서 백업 계획에 리소스를 할당할 수 있습니다.

어떤 계획을 사용하든 반드시 리소스를 할당해야 합니다. 시스템 및 테넌트 데이터베이스를 포함하여 할당할 SAP HANA 데이터베이스를 선택할 수 있습니다. 특정 리소스 ID를 제외하는 옵션도 있습니다.

SAP HANA 데이터베이스의 온디맨드 백업을 생성합니다.

생성 후 즉시 실행되는 전체 온디맨드 백업을 생성할 수 있습니다. Amazon EC2 인스턴스의 SAP HANA 데이터베이스의 온디맨드 백업은 전체 백업이며 증분 백업은 지원되지 않습니다.

이제 온디맨드 백업이 생성됩니다. 그러면 지정된 리소스의 백업이 시작됩니다. 콘솔은 작업 진행 상황을 볼 수 있는 백업 작업 페이지로 이동합니다. 백업 작업의 상태를 쉽게 찾는 데 필요하므로 화면 상단의 파란색 배너에 있는 백업 작업 ID를 기록해 두세요. 백업이 완료되면 상태가 `Completed`로 전환됩니다. 백업에는 최대 몇 시간이 소요될 수 있습니다.

상태 변경을 확인하려면 백업 작업 목록을 새로 고칩니다. 백업 작업 ID를 검색하고 클릭하여 자세한 작업 상태를 볼 수도 있습니다.

SAP HANA 데이터베이스의 연속 백업

point-in-time 복원 (PITR) 과 함께 사용할 수 있는 연속 백업을 만들 수 있습니다. 단, 온디맨드 백업은 리소스를 가져온 상태로 보존하는 반면 PITR은 일정 기간 동안의 변경 사항을 기록하는 연속 백업을 사용합니다.

연속 백업을 사용하면 EC2 인스턴스의 SAP HANA 데이터베이스를 선택한 특정 시점으로 되돌릴 수 있습니다(최대 35일 전까지 1초 단위로). 연속 백업은 먼저 리소스의 전체 백업을 생성한 다음 리소스

의 트랜잭션 로그를 지속적으로 백업하는 방식으로 작동합니다. PITR 복원은 전체 백업에 액세스하여 복구하라고 지정한 시간까지 트랜잭션 로그를 재생하는 방식으로 작동합니다. AWS Backup

AWS Backup 콘솔 또는 API를 AWS Backup 사용하여 백업 계획을 생성할 때 연속 백업을 선택할 수 있습니다.

콘솔을 사용하여 연속 백업을 활성화하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 계획을 선택한 후 백업 계획 생성을 선택합니다.
3. 백업 규칙에서 백업 규칙 추가를 선택합니다.
4. 백업 규칙 구성 섹션에서 지원되는 리소스에 대해 지속적 백업 활성화를 선택합니다.

SAP HANA 데이터베이스 백업의 PITR (point-in-time복원) 을 비활성화하면 복구 지점이 만료될 AWS Backup 때까지 (상태가 같음) 로그가 계속 전송됩니다. EXPIRED) SAP HANA의 대체 로그 백업 위치로 변경하여 AWS Backup으로 로그 전송을 중지할 수 있습니다.

상태가 인 연속 복구 지점은 연속 복구 지점이 STOPPED 중단되었음을 나타냅니다. 즉, SAP HANA에서 데이터베이스의 증분 변경을 보여주는 로그에 간격이 있습니다. AWS Backup 이 기간 간격 내에 발생하는 복구 시점은 상태가 STOPPED. 입니다.

연속 백업(복구 시점)의 복원 작업 중에 발생할 수 있는 문제에 대해서는 이 설명서의 SAP HANA 복원 문제 해결 단원을 참조하세요.

SAP HANA 데이터베이스 백업 보기

백업 및 복원 작업 상태 보기:

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 백업 작업, 복원 작업 또는 복사 작업을 선택하여 작업 목록을 확인합니다.
4. 작업 ID를 검색하고 클릭하면 자세한 작업 상태를 볼 수 있습니다.

볼트의 모든 복구 시점 보기:

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.

3. 백업 볼트를 검색하고 클릭하면 볼트 내의 모든 복구 시점을 볼 수 있습니다.

보호된 리소스의 세부 정보 보기:

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택합니다.
3. 리소스 유형을 기준으로 필터링하여 해당 리소스 유형의 모든 백업을 볼 수도 있습니다.

다음과 AWS CLI 같은 SAP HANA 데이터베이스에 사용하십시오. AWS Backup

Backup 콘솔 내의 각 작업에는 해당하는 API 호출이 있습니다.

프로그래밍 방식으로 리소스를 구성 AWS Backup 및 관리하려면 API 호출을 `StartBackupJob`사용하여 EC2 인스턴스에 SAP HANA 데이터베이스를 백업하십시오.

`start-backup-job`을 CLI 명령으로 사용합니다.

SAP HANA 데이터베이스 백업 문제 해결

워크플로우 중에 오류가 발생하는 경우 다음 오류 예시와 제안된 해결 방법을 참조하십시오.

Python 전제 조건

- 오류: SAP용 SSM 이후 Python 버전과 관련된 Zypper 오류가 발생했으며 AWS Backup Python 3.6이 필요하지만 SUSE 12 SP5는 기본적으로 Python 3.4를 지원합니다.

  해결 방법: 다음 단계를 수행하여 SUSE12 SP5에 여러 버전의 Python을 설치합니다.

  1. '/usr/bin/python3'을 직접 사용하는 대신 '/usr/local/bin/'에서 파이썬 3에 대한 심볼릭 링크를 생성하려면 업데이트 대안 명령을 실행하십시오. 이 명령은 Python 3.4를 기본 버전으로 설정합니다. 명령은 다음과 같습니다. `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. 다음 명령을 실행하여 Python 3.6을 대체 구성에 추가합니다. `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. 다음 명령을 실행하여 대체 구성을 Python 3.6으로 변경합니다. `# sudo update-alternatives –config python3`

     다음과 같은 출력이 표시되어야 합니다.

     ```
     There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
     ```

```
 Selection Path Priority Status
* 0 /usr/bin/python3.4 5 auto mode
 1 /usr/bin/python3.4 5 manual mode
 2 /usr/bin/python3.6 2 manual mode
Press enter to keep the current choice[*], or type selection number:
```

4. Python 3.6에 해당하는 숫자를 입력합니다.
5. Python 버전을 확인하고 Python 3.6이 사용되고 있는지 확인합니다.
6. (선택 사항이지만 권장됨) Zypper 명령이 예상대로 작동하는지 확인하십시오.

SAP용 아마존 EC2 Systems Manager 검색 및 등록

- 오류: SSM for SAP는 AWS Secrets Manager 및 SSM용 퍼블릭 엔드포인트에 대한 액세스가 차단되어 워크로드를 발견하지 못했습니다.

  해결 방법: SAP HANA 데이터베이스에서 엔드포인트에 연결할 수 있는지 테스트하십시오. 연결할 수 없는 경우 SAP용 Amazon VPC 엔드포인트와 SAP용 AWS Secrets Manager SSM을 생성할 수 있습니다.

  1. 다음 명령을 실행하여 HANA DB용 Amazon EC2 호스트에서 Secrets Manager에 대한 액세스를 테스트하십시오. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` 명령이 값을 반환하지 못하면 방화벽이 Secrets Manager 서비스 엔드포인트에 대한 액세스를 차단합니다. 로그는 “Secrets Manager에서 비밀 정보 검색” 단계에서 중지됩니다.
  2. 명령을 실행하여 SSM for SAP 엔드포인트에 대한 연결을 테스트합니다. `aws ssm-sap list-registration` 명령이 값을 반환하지 못하면 방화벽이 SSM for SAP 엔드포인트에 대한 액세스를 차단합니다.

     예제 오류:. `Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`

  엔드포인트에 연결할 수 없는 경우 다음 두 가지 방법으로 진행할 수 있습니다.

  - 방화벽 포트를 열어 Secrets Manager의 공용 서비스 엔드포인트 및 SAP용 SSM에 대한 액세스를 허용하거나,
  - Secrets Manager용 VPC 엔드포인트와 SAP용 SSM을 생성한 다음,
    - Amazon VPC가 DNS 지원 및 DNS 호스트 이름을 사용할 수 있도록 활성화되어 있는지 확인하십시오.

  - VPC 엔드포인트에서 프라이빗 DNS 이름 허용을 활성화했는지 확인하십시오.
  - SSM for SAP의 검색이 성공적으로 완료되면 로그에 호스트가 검색된 것으로 표시됩니다.
- 오류: AWS Backup 서비스 퍼블릭 엔드포인트에 대한 액세스가 AWS Backup 차단되어 Backint 연결이 실패했습니다. `aws-backint-agent.log`또는 와 유사한 오류가 표시될 수 있습니다. `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id" level=fatal msg="Error performing backup missing backup data plane Id` 또한 AWS Backup 콘솔에 다음과 같은 내용이 표시될 수 있습니다. `Fatal Error: An internal error occured.`

  해결 방법: 엔드포인트에 연결할 수 없는 경우 다음 두 가지 방법으로 진행할 수 있습니다.

  - 방화벽 포트를 열어 공용 서비스 엔드포인트 (HTTPS) 에 대한 액세스를 허용하십시오. 이 옵션을 사용하면 DNS가 퍼블릭 IP 주소를 통해 AWS 서비스에 대한 요청을 해결합니다.
  - 필요한 서비스를 오가는 트래픽을 비공개로 라우팅하는 VPC 엔드포인트를 생성합니다. AWS AWS Backup이 옵션을 사용하면 DNS가 사설 IP 주소를 통해 해당 서비스에 대한 요청을 해결합니다. 이 옵션을 사용하려면 요청을 프라이빗 엔드포인트로 전달하는 규칙을 추가하기 위해 DNS 서버를 업데이트해야 할 수 있습니다.
- 오류: 특수 문자가 포함된 HANA 암호로 인해 SSM for SAP를 등록하지 못했습니다. 예제 오류에는 HANA 데이터베이스 Amazon EC2 인스턴스에서 `Error connecting to database HBX/HBX when validating its credentials.` 테스트하거나 `systemdb` for를 사용하여 `hdbsql` 연결을 `tenantdb` 테스트한 `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` 후 오류가 포함될 수 있습니다.

  AWS Backup콘솔의 작업 페이지에서 백업 작업 세부 정보에 오류가 발생한 `Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’` 상태가 표시될 수 있습니다. `FAILED`

  해결 방법: 암호에 $와 같은 특수 문자가 없어야 합니다.
- 오류: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  해결 방법: SAP AWS BackInt HANA용 에이전트 설치가 성공적으로 완료되지 않았을 수 있습니다. SAP 애플리케이션 서버에 AWS Backint 에이전트와 Amazon EC2 Systems Manager 에이전트를 배포하는 프로세스를 다시 시도하십시오.
- 오류: 등록 후 콘솔이 로그 파일과 일치하지 않습니다.

특수 문자가 포함된 암호로 인해 HANA DB에 연결하려고 할 때 등록 실패로 표시되지만 SSM for SAP Application Manager for SAP 콘솔에 등록이 성공적으로 표시되지만 등록 성공 여부는 확인되지 않습니다. 콘솔에는 등록 성공이 표시되지만 로그에는 표시되지 않으면 백업이 실패합니다.

등록 상태 확인:

1. SSM 콘솔에 로그인
2. 왼쪽 탐색 메뉴에서 명령 실행을 선택합니다.
3. 텍스트 필드에 명령 기록을 입력하고 `Instance ID:Equal:` 등록에 사용한 인스턴스와 동일한 값을 입력합니다. 그러면 명령 기록이 필터링됩니다.
4. 명령 ID 열을 사용하여 상태가 있는 명령을 찾을 수 `Failed` 있습니다. 그런 다음 AWSSystemsManagerSAP-Discovery라는 문서 이름을 찾으십시오.
5. 에서 AWS CLI명령을 `aws ssm-sap register-application status` 실행합니다. 반환된 값이 `Error` 표시되면 등록에 실패한 것입니다.

해결 방법: HANA 비밀번호에 특수 문자 (예: '$') 가 없는지 확인하십시오.

SAP HANA 데이터베이스의 백업 생성

- 오류: SystemDB 또는 TenantDB에 대한 온디맨드 백업이 생성되면 AWS Backup 콘솔에 “치명적 오류”라는 메시지가 표시됩니다. 이는 퍼블릭 엔드포인트 셀-1.prod.us-west-2.storage.cryo.aws.a2z.com에 액세스할 수 없기 때문에 발생합니다. 이는 이 엔드포인트에 대한 액세스를 차단하는 클라이언트 측 방화벽 때문입니다.

  `aws-backint-agent.loglevel=error msg="Storage configuration validation failed: missing backup data plane Id"`또는 다음과 같은 오류가 표시될 수 있습니다. `level=fatal msg="Error performing backup missing backup data plane Id."`

  해결 방법: 공개 엔드포인트 셀-1.prod.us-west-2.storage.cryo.aws.a2z.com에 대한 개방형 방화벽 액세스.

- **`Database cannot be backed up while it is stopped`**오류:.

  해결 방법: 백업할 데이터베이스가 활성 상태인지 확인합니다. 데이터베이스 데이터 및 로그는 데이터베이스가 온라인 상태일 때 백업할 수 있습니다.

- 오류: `Getting backup metadata failed. Check the SSM document execution for more details.`

해결 방법: 백업할 데이터베이스가 활성 상태인지 확인합니다. 데이터베이스 데이터 및 로그는 데이터베이스가 온라인 상태일 때 백업할 수 있습니다.

백업 로그 모니터링

- 오류: `Encountered an issue with log backups, please check SAP HANA for details.`

  해결 방법: SAP AWS Backup HANA에서 로그 백업이 SAP HANA로 전송되고 있는지 확인하십시오.
- 오류: `One or more log backup attempts failed for recovery point.`

  해결 방법: 자세한 내용은 SAP HANA를 확인하세요. SAP AWS Backup HANA에서 로그 백업이 전송되고 있는지 확인하십시오.
- 오류: `Unable to determine the status of log backups for recovery point.`

  해결 방법: 자세한 내용은 SAP HANA를 확인하세요. SAP AWS Backup HANA에서 로그 백업이 전송되고 있는지 확인하십시오.
- 오류: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  해결 방법: 복원 작업이 완료될 때까지 기다립니다. 로그 백업이 재개되어야 합니다.

사용 시 SAP HANA 용어에 대한 용어집 AWS Backup

데이터 백업 유형: SAP HANA는 전체 백업과 INC (증분) 의 두 가지 데이터 백업 유형을 지원합니다. AWS Backup 각 백업 작업 중에 사용되는 유형을 최적화합니다.

카탈로그 백업: SAP HANA는 카탈로그라는 자체 매니페스트를 유지 관리합니다. AWS Backup 이 카탈로그와 상호 작용합니다. 새로 백업할 때마다 카탈로그에 항목이 하나씩 생성됩니다.

연속 로그 백업(트랜잭션 로그): 시점 복구(PITR) 기능의 경우 SAP HANA는 가장 최근 백업 이후의 모든 트랜잭션을 추적합니다.

시스템 복사: 복원 대상 데이터베이스가 복구 시점이 생성된 소스 데이터베이스와 다른 복원 작업입니다.

파괴 복원: 파괴 복원은 복원된 데이터베이스에서 원본 또는 기존 데이터베이스를 삭제하거나 덮어쓰는 복원 작업입니다.

FULL: 전체 백업은 전체 데이터베이스의 백업입니다.

INC: 증분 백업은 SAP HANA 데이터베이스에서 이전 백업 이후의 모든 변경 사항을 백업하는 것입니다.

자세한 내용은 AWS 용어집을 참조하세요.

AWS Backup EC2 인스턴스의 SAP HANA 데이터베이스 지원 릴리스 노트

현재 일부 기능은 지원되지 않습니다.

- 교차 계정 및 교차 리전 복사는 현재 지원되지 않습니다.
- Backup Audit Manager 및 보고 기능은 현재 지원되지 않습니다.
- 지원되는 서비스는 다음과 같습니다. AWS 리전Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업을 위해 현재 지원되는 지역을 포함합니다.

Amazon Redshift 백업

Amazon Redshift는 확장 가능한 완전관리형 클라우드 데이터 웨어하우스로, 빠르고 쉽고 안전한 분석을 통해 인사이트를 얻는 시간을 단축합니다. 변경할 수 없는 백업, 별도의 액세스 정책, 백업 및 복원 작업에 대한 중앙 집중식 조직 거버넌스를 통해 데이터 웨어하우스를 보호하는 데 사용할 AWS Backup 수 있습니다.

Amazon Redshift 데이터 웨어하우스는 노드라고 하는 컴퓨팅 리소스 모음으로, 클러스터라는 그룹으로 구성되어 있습니다. AWS Backup 이러한 클러스터를 백업할 수 있습니다.

Amazon Redshift에 대한 자세한 내용은 Amazon Redshift 시작 가이드, Amazon Redshift 데이터베이스 개발자 안내서 및 Amazon Redshift 클러스터 관리 안내서를 참조하세요.

Amazon Redshift 프로비저닝 클러스터 백업

AWS Backup 콘솔을 사용하거나 API 또는 CLI를 사용하여 프로그래밍 방식으로 Amazon Redshift 클러스터를 보호할 수 있습니다. 이러한 클러스터는 백업 계획의 일부로 정기적으로 백업하거나 온디맨드 백업을 통해 필요에 따라 백업할 수 있습니다.

단일 테이블(항목 수준 복원이라고도 함) 또는 전체 클러스터를 복원할 수 있습니다. 테이블은 단독으로 백업할 수 없으며 클러스터를 백업할 때 클러스터의 일부로 백업됩니다.

를 AWS Backup 사용하면 리소스를 중앙 집중식으로 볼 수 있지만 Amazon Redshift만 사용하는 경우 Amazon Redshift의 자동 스냅샷 스케줄러를 계속 사용할 수 있습니다. 단, Amazon Redshift를 통해 수동 스냅샷 설정을 관리하기로 선택한 경우에는 Amazon Redshift를 사용하여 수동 스냅샷 설정을 계속 관리할 수 없습니다. AWS Backup

Amazon Redshift 클러스터는 AWS Backup 콘솔을 통해 또는 를 사용하여 백업할 수 있습니다. AWS CLI

AWS Backup 콘솔을 사용하여 Amazon Redshift 클러스터를 백업하는 방법에는 온디맨드 백업과 백업 계획의 일부로 백업하는 방법이 있습니다.

온디맨드 Amazon Redshift 백업 생성

자세한 내용은 온디맨드 백업 유형 생성 페이지를 참조하세요.

수동 스냅샷을 생성하려면 Amazon Redshift 리소스가 포함된 백업 계획을 생성할 때 연속 백업 확인란을 선택하지 마세요.

백업 계획에서 예약된 Amazon Redshift 백업 생성

Amazon Redshift 클러스터가 보호된 리소스인 경우 예약 백업에 포함할 수 있습니다. Amazon Redshift 테이블을 보호하도록 선택하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택합니다.
3. Amazon Redshift를 켜기로 전환합니다.
4. 기존 계획 또는 새 계획에 Amazon Redshift 클러스터를 포함하려면 콘솔에 리소스 할당을 참조하세요.

백업 계획 관리에서 백업 계획을 생성하고 Amazon Redshift 클러스터를 포함하도록 선택하거나 Amazon Redshift 클러스터를 포함하도록 기존 계획을 업데이트할 수 있습니다. 리소스 유형 Amazon Redshift를 추가할 때 모든 Amazon Redshift 클러스터를 추가하거나 클러스터 옆의 확인란을 선택할 수 있습니다.

프로그래밍 방식 백업

또한 JSON 문서에서 백업 계획을 정의하고 AWS Backup 콘솔을 사용하여 제공할 수도 있습니다. AWS CLI프로그래밍 방식으로 백업 계획을 생성하는 방법에 대한 자세한 내용은 JSON 문서 및 AWS Backup CLI를 사용하여 백업 계획 만들기를 참조하십시오.

API를 다음 작업을 수행할 수 있습니다.

- 백업 작업 중지
- 백업 작업 설명
- 복구 시점 메타데이터 가져오기
- 리소스별 복구 시점 나열
- 복구 시점 태그 나열

Amazon Redshift 클러스터 백업 보기

콘솔 내에서 Amazon Redshift 테이블 백업을 보고 수정하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 볼트를 선택합니다. 그런 다음 Amazon Redshift 클러스터가 포함된 백업 볼트 이름을 클릭합니다.
3. 백업 볼트에는 요약 및 백업 목록이 표시됩니다. 복구 시점 ID 열의 링크를 클릭할 수 있습니다.
4. 하나 이상의 복구 시점을 삭제하려면 삭제하려는 항목의 확인란을 선택합니다. 작업 버튼 아래에서 삭제를 선택할 수 있습니다.

Amazon Redshift 클러스터 복원

자세한 내용은 Amazon Redshift 클러스터 복원을 참조하세요.

Amazon 관계형 데이터베이스 서비스 백업

아마존 RDS 및 AWS Backup

Amazon RDS 인스턴스 및 클러스터를 백업하는 옵션을 고려할 때는 어떤 종류의 백업을 생성하여 사용할지 명확히 하는 것이 중요합니다. Amazon RDS를 비롯한 여러 AWS 리소스는 자체 기본 백업 솔루션을 제공합니다.

Amazon RDS는 자동 백업 및 수동 백업 옵션을 제공합니다. Amazon RDS 용어에 따르면 백업 계획에 있는 복구 지점을 포함하여 에서 생성한 AWS Backup모든 복구 지점은 수동 백업을 고려합니다.

를 AWS Backup 사용하여 Amazon RDS 인스턴스의 백업 (복구 지점) 을 생성할 때는 이전에 Amazon RDS를 사용하여 자동 백업을 생성한 적이 AWS Backup 있는지 확인합니다. 자동 백업이 있는 경우,

이 스냅샷 (`copy-db-snapshot`작업) 의 사본을 AWS Backup 생성합니다. 기존 백업이 없는 경우 복사본 (`create-db-snapshot`작업) 대신 지정한 인스턴스의 스냅샷을 AWS Backup 생성합니다.

에서 만든 AWS Backup첫 번째 스냅샷을 두 작업 중 하나로 생성하면 전체 스냅샷 1개가 됩니다. 전체 백업이 존재하는 한, 이 스냅샷의 모든 후속 사본은 증분 백업이 됩니다.

> **Important**
>
> Amazon RDS 인스턴스의 스냅샷을 매일 여러 개 생성하도록 AWS Backup 백업 계획이 예약되어 있고 예약된 AWS Backup 백업 시작 기간 중 하나가 Amazon RDS 백업 창과 일치하면 백업의 데이터 계보가 동일하지 않은 백업으로 분기되어 예상치 못한 백업이 생성되고 충돌이 발생할 수 있습니다. 이를 방지하려면 AWS Backup 백업 계획 또는 Amazon RDS 기간이 서로 일치하지 않도록 하십시오.

Amazon RDS 연속 백업 및 특정 시점 복원

연속 백업에는 를 AWS Backup 사용하여 Amazon RDS 리소스의 전체 백업을 생성한 다음 트랜잭션 로그를 통해 모든 변경 사항을 캡처하는 작업이 포함됩니다. 고정된 시간 간격으로 촬영한 이전 스냅샷을 선택하는 대신 복원하려는 시점으로 되감으면 세분성을 높일 수 있습니다.

자세한 내용은 연속 백업 및 PITR 지원 서비스 및 연속 백업 설정 관리를 참조하십시오.

Amazon RDS 다중 가용 영역 백업

AWS Backup 기본 데이터베이스 인스턴스 하나와 읽기 가능한 대기 데이터베이스 인스턴스 두 개를 포함하는, MySQL용 Amazon RDS 및 PostgreSQL 다중 AZ (가용 영역) 배포 옵션을 백업하고 지원합니다.

다중 가용 영역 백업은 다음 리전에서 사용할 수 있습니다. 아시아 태평양(시드니) 리전, 아시아 태평양(도쿄) 리전, 유럽(아일랜드) 리전, 미국 동부(오하이오) 리전, 미국 서부(오레곤) 리전, 유럽(스톡홀름) 리전, 아시아 태평양(싱가포르) 리전, 미국 동부(버지니아 북부) 리전, 유럽(프랑크푸르트) 리전.

다중 AZ 배포 옵션은 쓰기 트랜잭션을 최적화하며, 워크로드에 추가 읽기 용량, 쓰기 트랜잭션 지연 시간 감소, 쓰기 트랜잭션 지연 시간의 일관성에 영향을 미치는 네트워크 지터로부터의 복원력 향상, 고가용성 및 내구성이 필요한 경우에 적합합니다.

다중 AZ 클러스터를 생성하려면 MySQL 또는 PostgreSQL을 엔진 유형으로 선택하면 됩니다.

AWS Backup 콘솔에는 다음과 같은 세 가지 배포 옵션이 있습니다.

- 다중 AZ DB 클러스터: 프라이머리 DB 인스턴스 1개와 읽기 가능한 스탠바이 DB 인스턴스 2개를 포함하는 DB 클러스터를 생성합니다. 각 DB 인스턴스는 서로 다른 가용 영역에 있습니다. 고가용성 및 데이터 중복성을 제공하고 서버용 워크로드의 용량을 늘립니다.
- 다중 AZ DB 인스턴스: 프라이머리 DB 인스턴스 1개와 스탠바이 DB 인스턴스 1개를 서로 다른 가용 영역에 생성합니다. 이렇게 하면 고가용성 및 데이터 중복성이 제공되지만, 스탠바이 DB 인스턴스는 읽기 워크로드를 위한 연결을 지원하지 않습니다.
- 단일 DB 인스턴스: 스탠바이 DB 인스턴스 없이 단일 DB 인스턴스를 생성합니다.

Amazon RDS용 백업을 생성하려면 백업 계획의 일부로 백업을 예약하기 위한 백업 생성 또는 온디맨드 백업 생성을 참조하세요.

> **Note**
>
> 시점 복구(PITR)는 인스턴스를 지원할 수 있지만 클러스터는 지원할 수 없습니다.
> 다중 AZ DB 클러스터 스냅샷 복사는 지원되지 않습니다.

다중 AZ 클러스터와 RDS 인스턴스 간의 차이점

단일 가용 영역 또는 2개 가용 영역에서의 백업은 RDS 인스턴스이고, 3개 이상의 인스턴스가 포함된 배포 및 백업은 Amazon Aurora, Amazon Neptune 및 Amazon DocumentDB 클러스터와 유사한 클러스터입니다.

ARN(Amazon 리소스 이름)은 인스턴스 또는 클러스터 중 무엇을 사용하는지에 따라 다르게 렌더링됩니다.

RDS 인스턴스 ARN: `arn:aws:rds:`*`region`*`:` *`account`*`:db:`*`name`*

RDS 다중 가용성 클러스터: `arn:aws:rds:`*`region`*`:`*`account`* `:cluster:`*`name`*

자세한 내용은 Amazon RDS 사용 설명서의 다중 AZ DB 클러스터 배포를 참조하세요.

자세한 내용은 다중 AZ DB 클러스터 스냅샷 생성에 대한 자세한 내용은 Amazon RDS 사용 설명서를 참조하세요.

AWS CloudFormation 스택 백업

CloudFormation 스택은 단일 단위로 백업할 수 있는 여러 개의 상태 저장 및 상태 비저장 리소스로 구성됩니다. 즉, 스택을 백업하고 그 안에 포함된 리소스를 복원하여 여러 리소스가 포함된 애플리케이션

을 백업 및 복원할 수 있습니다. 스택의 모든 리소스는 스택의 AWS CloudFormation 템플릿으로 정의합니다.

CloudFormation 스택이 백업되면 CloudFormation 템플릿과 AWS Backup 스택에서 지원하는 각 추가 리소스에 대한 복구 지점이 생성됩니다. 이러한 복구 시점은 복합이라는 중요한 복구 시점 내에 그룹화됩니다.

이 복합 복구 시점은 복원할 수 없지만 중첩 복구 시점은 복원할 수 있습니다. 콘솔 또는 AWS CLI를 사용하여 복합 백업 내의 한 백업에서 모든 중첩 백업까지 원하는 대로 복원할 수 있습니다.

CloudFormation 애플리케이션 스택 용어

- 복합 복구 시점: 중첩 복구 시점과 기타 메타데이터를 함께 그룹화하는 데 사용되는 복구 시점입니다.
- 중첩된 복구 지점: CloudFormation 스택의 일부이며 복합 복구 지점의 일부로 백업되는 리소스의 복구 지점입니다. 각 중첩 복구 시점은 하나의 복합 복구 시점의 스택에 속합니다.
- 복합 작업: 스택 내 개별 리소스에 대해 다른 백업 작업을 트리거할 수 있는 CloudFormation 스택의 백업, 복사 또는 복원 작업입니다.
- 중첩 작업: AWS CloudFormation 스택 내 리소스에 대한 백업, 복사 또는 복원 작업입니다.

CloudFormation 스택 백업 작업

백업 생성 프로세스를 백업 작업이라고 합니다. CloudFormation 스택 백업 작업에는 상태가 있습니다. 백업 작업이 완료되면 상태는 `Completed`입니다. 이는 AWS CloudFormation 복구 지점(백업)이 생성되었음을 의미합니다.

CloudFormation 스택은 콘솔을 사용하여 백업하거나 프로그래밍 방식으로 백업할 수 있습니다. CloudFormation 스택을 비롯한 모든 리소스를 백업하려면 이AWS Backup 개발자 안내서의 다른 위치에 백업 만들기를 참조하세요.

CloudFormation API 명령을 사용하여 스택을 백업할 수 있습니다. `StartBackupJob` 설명서 및 콘솔에서는 복합 및 중첩 복구 시점이 사용되고, API 언어는 동일한 맥락 관계에서 '상위 및 하위 복구 시점'이라는 용어를 사용한다는 점에 유의하세요.

CloudFormation 스택에는 템플릿에 표시된 모든 AWS 리소스가 포함됩니다. CloudFormation 템플릿에는 AWS Backup이 아직 지원하지 않는 리소스가 포함되어 있을 수 있습니다. 템플릿에 AWS 지원되는 리소스와 지원되지 않는 리소스가 조합되어 있는 경우 AWS Backup 는 여전히 템플릿을 복합 스택에 백업하지만 Backup은 백업 지원 서비스의 복구 지점만 생성합니다. 특정 서비스를 선택하지 않았더

라도 (콘솔 설정에서 서비스를 “사용 가능”으로 전환) CloudFormation 템플릿에 포함된 모든 리소스 유형이 백업에 포함됩니다. AWS Backup 이 지원하는 중첩 백업(복구 시점)은 복원할 수 있지만 중첩 스택은 백업 또는 복원할 수 없습니다.

AWS CloudFormation 복구 지점

복구 시점 상태

스택의 백업 작업이 완료되면(작업 상태가 `Completed`) 스택의 백업이 생성된 것입니다. 이 백업을 복합 복구 시점이라고도 합니다. 복합 복구 시점은 `Completed`, `Failed` 또는 `Partial` 상태 중 하나일 수 있습니다. 백업 작업에는 상태가 있고 복구 시점(백업이라고도 함)도 별도의 상태가 있다는 점에 유의하세요.

백업 작업이 완료되면 전체 스택과 내부 리소스가 보호됩니다 AWS Backup. 실패 상태는 백업 작업이 실패했음을 나타냅니다. 실패를 초래한 문제가 해결되면 백업을 다시 생성해야 합니다.

`Partial` 상태는 스택의 모든 리소스가 백업되지 않았음을 의미합니다. 이 문제는 CloudFormation 템플릿에 현재 지원되지 않는 리소스가 포함된 경우 또는 스택 내 리소스 (중첩된 리소스) 에 속하는 하나 이상의 백업 작업이 다음 상태가 아닌 경우 발생할 수 있습니다. AWS Backup`Completed` 온디맨드 백업을 수동으로 생성하여 `Completed` 상태가 아닌 리소스를 다시 실행할 수 있습니다. 스택의 상태가 `Completed`일 것으로 예상했지만 대신 `Partial`로 표시되는 경우 스택에서 위의 조건을 확인하세요.

복합 복구 시점 내의 각 중첩된 리소스에는 각각 고유한 상태(`Completed` 또는 `Failed`)를 갖는 고유한 개별 복구 시점이 있습니다. 상태가 `Completed`인 중첩 복구 시점은 복원할 수 있습니다.

복구 시점 관리

복합 복구 시점(백업)은 복사할 수 있고, 중첩 복구 시점은 복사, 삭제, 연결 해제 또는 복원할 수 있습니다. 중첩 백업이 포함된 복합 복구 시점은 삭제할 수 없습니다. 복합 복구 시점 내의 중첩 복구 시점이 삭제되거나 연결이 해제된 후에는 복합 복구 시점을 수동으로 삭제하거나 백업 계획 수명 주기에서 해당 복구 시점을 삭제할 때까지 그대로 둘 수 있습니다.

복구 시점 삭제

AWS Backup 콘솔이나 를 사용하여 복구 지점을 삭제할 수 있습니다. AWS CLI

AWS Backup 콘솔을 사용하여 복구 지점을 삭제하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보호된 리소스를 클릭합니다. 텍스트 상자에 입력하여 CloudFormation 스택만 표시합니다. `CloudFormation`

3. 복합 복구 시점이 복구 시점 창에 표시됩니다. 각 복구 시점 ID의 왼쪽에 있는 더하기 기호(+)를 클릭하여 각 복합 복구 시점을 확장하면 복합에 포함된 모든 중첩 복구 시점이 표시됩니다. 복구 시점의 왼쪽에 있는 확인란을 선택하여 삭제하려는 복구 시점 선택 항목에 해당 복구 시점을 포함시킬 수 있습니다.
4. 삭제 버튼을 클릭합니다.

콘솔을 사용하여 하나 이상의 복합 복구 시점을 삭제하면 경고 상자가 나타납니다. 이 경고 상자에서 복합 스택 내의 중첩 복구 시점을 포함하여 복합 복구 시점을 삭제할 의도를 확인해야 합니다.

API를 사용하여 복구 시점을 삭제하려면 `DeleteRecoveryPoint` 명령을 사용합니다.

와 함께 API를 사용하는 AWS Command Line Interface 경우 복합 지점을 삭제하기 전에 중첩된 복구 지점을 모두 삭제해야 합니다. 여전히 중첩 복구 시점이 포함되어 있는 복합 스택 백업(복구 시점)을 삭제하라는 API 요청을 전송하면 요청이 오류를 반환합니다.

복합 복구 시점에서 중첩 복구 시점 연결 해제

복합 복구 시점에서 중첩 복구 시점의 연결을 해제할 수 있습니다(예: 중첩 복구 시점은 유지하되 복합 복구 시점은 삭제하려는 경우). 두 복구 시점은 모두 유지되지만 더 이상 연결되지 않습니다. 즉, 연결 해제 후에는 복합 복구 시점에서 발생한 작업이 더 이상 중첩 복구 시점에 적용되지 않습니다.

콘솔을 사용하여 복구 시점의 연결을 해제하거나 API `DisassociateRecoveryPointFromParent`를 호출할 수 있습니다. [API 호출은 복합 복구 시점을 지칭할 때 '상위'라는 용어를 사용합니다.]

복구 시점 복사

복합 복구 지점을 복사하거나, 리소스가 계정 간 및 지역 간 복사를 지원하는 경우 중첩된 복구 지점을 복사할 수 있습니다.

콘솔을 사용하여 복구 지점을 복사하려면: AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보호된 리소스를 클릭합니다. 텍스트 상자에 입력하여 CloudFormation 스택만 표시합니다. `CloudFormation`
3. 복합 복구 시점이 복구 시점 창에 표시됩니다. 각 복구 시점 ID의 왼쪽에 있는 더하기 기호(+)를 클릭하여 각 복합 복구 시점을 확장하면 복합에 포함된 모든 중첩 복구 시점이 표시됩니다. 복구 시점의 왼쪽에 있는 원형 라디오 버튼을 클릭하여 복구 시점을 복사할 수 있습니다.

4. 복구 시점을 선택한 후 창의 오른쪽 상단에 있는 복사 버튼을 클릭합니다.

복합 복구 시점을 복사할 때 복사 기능을 지원하지 않는 중첩 복구 시점은 복사된 스택에 포함되지 않습니다. 복합 복구 시점은 `Partial` 상태가 됩니다.

FAQ

1. “애플리케이션 백업에는 무엇이 포함되나요?”

   를 사용하여 정의된 애플리케이션의 각 백업의 일부로 템플릿 CloudFormation, 템플릿에 있는 각 매개 변수의 처리된 값 및 에서 지원하는 중첩된 리소스가 AWS Backup 백업됩니다. 중첩된 리소스는 CloudFormation 스택에 포함되지 않은 개별 리소스를 백업하는 것과 같은 방식으로 백업됩니다. `no-echo`로 표시된 파라미터의 값은 백업되지 않습니다.

2. “스택이 중첩된 AWS CloudFormation 스택을 백업할 수 있나요?”

   예. 중첩된 CloudFormation 스택이 포함된 스택은 백업에 포함될 수 있습니다.

3. “*`Partial`* 상태란 백업 생성이 실패했다는 뜻인가요?”

   아니요. 부분 상태는 복구 시점이 일부는 백업되었지만 일부는 백업되지 않았음을 나타냅니다. `Completed` 백업 결과를 예상했다면 다음 세 가지 조건을 확인할 수 있습니다.

   a. CloudFormation 스택에 현재 지원되지 않는 리소스가 포함되어 있나요? AWS Backup지원되는 리소스 목록은 개발자 안내서의 지원되는 AWS 리소스 및 타사 애플리케이션을 참조하십시오.

   b. 스택 내 리소스에 속하는 백업 작업이 하나 이상 성공하지 못했으므로 작업을 다시 실행해야 합니다.

   c. 중첩 복구 시점이 삭제되었거나 복합 복구 시점과의 연결이 해제되었습니다.

4. “ CloudFormation 스택 백업에서 리소스를 제외하려면 어떻게 해야 하나요?”

   CloudFormation 스택을 백업할 때 백업의 일부에서 리소스를 제외할 수 있습니다. 콘솔에서 백업 계획 생성 및 백업 계획 업데이트 프로세스 도중 리소스 할당 단계가 있습니다. 이 단계에는 리소스 선택 섹션이 있습니다. 특정 리소스 유형을 포함하도록 선택하고 백업할 CloudFormation 리소스로 포함시킨 경우 선택한 리소스 유형에서 특정 리소스 ID를 제외할 수 있습니다. 태그를 사용하여 스택 내의 리소스를 제외할 수도 있습니다.

   CLI를 사용하면

   - `NotResources`백업 계획에서 CloudFormation 스택에서 특정 리소스를 제외할 수 있습니다.

- `StringNotLike`를 사용하여 태그를 통해 항목을 제외할 수 있습니다.

5. “중첩된 리소스에는 어떤 유형의 백업이 지원되나요?”

   중첩된 리소스의 백업은 해당 리소스에 지원되는 백업 종류에 따라 전체 백업일 수도 있고 증분 백업일 수도 있습니다. AWS Backup 자세한 내용은 증분 백업 작동 방법을 참조하세요. 하지만 Amazon S3 및 Amazon RDS 중첩 리소스에서는 PITR (point-in-time 복원) 이 지원되지 않는다는 점에 유의하십시오.

6. “ CloudFormation 스택의 일부인 변경 세트는 백업됩니까?”

   아니요. 변경 세트는 CloudFormation 스택 백업의 일부로 백업되지 않습니다.

7. “ AWS CloudFormation 스택 상태가 백업에 어떤 영향을 미칩니까?”

   CloudFormation 스택 상태가 백업에 영향을 미칠 수 있습니다. `COMPLETE`를 포함하는 상태의 스택은 백업할 수 있습니다(예: `CREATE_COMPLETE`, `ROLLBACK_COMPLETE` `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` 또는 `IMPORT_ROLLBACK_COMPLETE`).

   새 템플릿 업로드가 실패하고 스택이 `ROLLBACK_COMPLETE` 상태로 이동하는 경우 새 템플릿은 백업되지만 중첩된 리소스의 백업은 롤백된 리소스를 기반으로 합니다.

8. “애플리케이션 스택 수명 주기는 다른 복구 시점 수명 주기와 어떻게 다른가요?”

   중첩 복구 시점 수명 주기는 해당 주기가 속한 백업 계획에 따라 결정됩니다. 복합 복구 시점은 모든 중첩 복구 시점 중 가장 긴 수명 주기에 의해 결정됩니다. 복합 복구 시점 내에 마지막으로 남아 있는 중첩 복구 시점이 삭제되거나 연결 해제되면 복합 복구 시점도 삭제됩니다.

9. “태그는 복구 지점에 어떻게 CloudFormation 복사됩니까?”

   예. 해당 태그는 각 중첩 복구 시점에 복사됩니다.

10. “복합 및 중첩 복구 시점(백업)을 삭제하는 순서가 있나요?”

    예. 일부 백업은 먼저 삭제해야 다른 백업을 삭제할 수 있습니다. 중첩 복구 시점이 포함된 복합 백업은 복합 내의 모든 복구 시점이 삭제될 때까지 삭제할 수 없습니다. 복합 복구 시점에 더 이상 중첩 복구 시점이 없으면 수동으로 삭제할 수 있습니다. 그렇지 않으면 백업 계획 수명 주기에 따라 삭제됩니다.

스택 내 애플리케이션 복원

중첩 복구 시점 복원에 대한 자세한 내용은 애플리케이션 스택 백업을 복원하는 방법을 참조하세요.

Windows VSS 백업 생성

를 사용하면 Amazon EC2 인스턴스에서 실행되는 VSS (볼륨 섀도 복사본 서비스) 지원 Windows 애플리케이션을 백업 및 복원할 수 있습니다. AWS Backup애플리케이션에 Windows VSS에 등록된 VSS 작성기가 있는 경우 해당 애플리케이션에 대해 AWS Backup 일관성을 유지하는 스냅샷을 생성합니다.

다른 리소스를 보호하는 데 사용되는 것과 동일한 관리형 백업 서비스를 사용하면서 일관된 복원을 수행할 수 있습니다. AWS EC2에서 애플리케이션 일관성 Windows 백업을 사용하면 기존 백업 도구와 동일한 일관성 설정 및 애플리케이션 인식을 얻을 수 있습니다.

> **Note**
>
> AWS Backup 현재는 Amazon EC2에서 실행되는 리소스의 애플리케이션 정합성이 보장되는 백업, 특히 기존 인스턴스를 백업에서 생성된 새 인스턴스로 교체하여 애플리케이션 데이터를 복원할 수 있는 백업 시나리오만 지원합니다. 모든 인스턴스 유형 또는 애플리케이션이 Windows VSS 백업에 대해 지원되는 것은 아닙니다.

자세한 내용은 Amazon EC2 사용 설명서의 VSS 애플리케이션 정합성이 보장되는 스냅샷 생성을 참조하십시오.

Amazon EC2를 실행하는 VSS 지원 Windows 리소스를 백업 및 복원하려면 다음 단계에 따라 필수 사전 작업을 완료하세요. 지침은 Windows 인스턴스용 Amazon EC2 사용 설명서의 시작하기 전을 참조하세요.

1. 에서 SSM 에이전트를 다운로드, 설치 및 구성합니다. AWS Systems Manager이 단계는 필수입니다. 지침은 Systems AWS Manager 사용 설명서의 Windows Server용 Amazon EC2 인스턴스에서 SSM 에이전트 사용을 참조하십시오.
2. Windows VSS(Volume Shadow Copy Service) 백업을 수행하기 전에 IAM 역할에 IAM 정책을 추가하고 해당 역할을 Amazon EC2 인스턴스에 연결합니다. 지침은 Amazon EC2 사용 설명서의 VSS 지원 스냅샷용 IAM 역할 생성을 참조하십시오. IAM 정책 예제는 관리형 정책 대상 AWS Backup 단원을 참조하세요.
3. Amazon EC2 인스턴스의 Windows에 VSS 구성 요소를 다운로드하여 설치합니다.
4. AWS Backup다음에서 VSS를 활성화합니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 대시보드에서 생성하려는 백업 유형(온디맨드 백업 생성 또는 백업 계획 관리)을 선택합니다. 백업 유형에 필요한 정보를 제공합니다.
3. 리소스를 할당할 때 EC2를 선택합니다. Windows VSS 백업은 현재 EC2 인스턴스에서만 지원됩니다.
4. 고급 설정 섹션에서 Windows VSS를 선택합니다. 이렇게 하면 애플리케이션 일관성 Windows VSS 백업을 수행할 수 있습니다.
5. 백업을 생성합니다.

`Completed` 상태 백업 작업이 VSS 부분의 성공을 보장하지는 않습니다. VSS 포함은 최선의 노력 기준입니다. 다음 단계를 따라 백업이 애플리케이션 일관성, 중단 일관성 또는 실패인지 확인하세요.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창의 내 계정에서 작업을 클릭합니다.
3. `Completed` 상태는 애플리케이션 일관성(VSS) 작업이 성공적으로 수행되었음을 나타냅니다.

   `Completed with issues` 상태는 VSS 작업이 실패하여 중단 일관성 백업만 성공했음을 나타냅니다. 이 상태에는 팝오버 메시지 `"Windows VSS Backup Job Error encountered, trying for regular backup"`도 표시됩니다.

   백업이 실패한 경우 상태는 `Failed`입니다.
4. 백업 작업의 추가 세부 정보를 보려면 개별 작업을 클릭합니다. 예를 들어 세부 정보가 `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`로 표시될 수 있습니다.

Windows가 아니거나 VSS가 아닌 구성 요소를 대상으로 하는 VSS 지원 백업의 경우 작업이 성공적으로 완료된 Windows는 VSS를 사용하지 않아도 충돌 시 정합성이 보장됩니다.

지원되지 않는 Amazon EC2 인스턴스

다음 Amazon EC2 인스턴스 유형은 소형 인스턴스이고 백업을 제대로 생성하지 못할 수 있으므로 VSS 지원 Windows 백업이 지원되지 않습니다.

- t3.nano
- t3.micro

- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

아마존 EBS 및 AWS Backup

Amazon EBS 리소스의 백업 프로세스는 다른 리소스 유형을 백업하는 데 사용되는 단계와 비슷합니다.

- 온디맨드 백업 생성
- 예약 백업 생성

리소스별 정보는 다음 섹션에 설명되어 있습니다.

콜드 스토리지용 Amazon EBS 아카이브 계층

EBS는 백업을 콜드 스토리지로 전환할 수 있도록 지원하는 리소스 중 하나입니다. 자세한 정보는 수명 주기 및 스토리지 계층을 참조하세요.

> **Note**
>
> 이 기능은 중국 (베이징), 중국 (닝샤), (미국 동부) 및 AWS GovCloud AWS GovCloud (미국 서부) 지역에서는 사용할 수 없습니다.

Amazon EBS 다중 볼륨 중단 일관성 백업

기본적으로 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨의 충돌 시에도 정합성이 보장되는 백업을 AWS Backup 생성합니다. 중단 일관성이란 동일한 Amazon EC2 인스턴스에 연결된 모든 Amazon EBS 볼륨의 스냅샷이 정확히 같은 순간에 생성된다는 것을 의미합니다. 애플리케이션 상태의 중단 일관성을 보장하기 위해 더 이상 인스턴스를 중지하거나 여러 Amazon EBS 볼륨 간에 조정하지 않아도 됩니다.

여러 볼륨의 충돌 정합성이 보장되는 스냅샷은 기본 AWS Backup 기능이므로 이 기능을 사용하기 위해 별도의 조치를 취하지 않아도 됩니다. 다음 절차 중 하나를 사용하여 Amazon EBS 볼륨을 백업할 수 있습니다.

EBS 스냅샷 복구 지점을 생성하는 데 사용되는 역할은 해당 스냅샷과 연결됩니다. 이 역할과 동일한 역할을 사용하여 생성된 복구 지점을 삭제하거나 복구 지점을 아카이브 계층으로 전환해야 합니다.

Amazon EBS 스냅샷 잠금 및 AWS Backup

AWS Backup Amazon EBS 스냅샷 잠금이 적용된 관리형 Amazon EBS 스냅샷 및 관리형 AWS Backup Amazon EC2 AMI와 연결된 스냅샷은 스냅샷 잠금 기간이 백업 수명 주기를 초과하는 경우 복구 지점 수명 주기의 일부로 삭제되지 않을 수 있습니다. 대신 이 복구 시점의 상태는 `EXPIRED`가 됩니다. Amazon EBS 스냅샷 잠금을 먼저 제거하면 이러한 복구 시점을 수동으로 삭제할 수 있습니다.

Amazon EBS 리소스 복원

Amazon EBS 볼륨을 복원하려면 Amazon EBS 볼륨 복원의 단계를 따릅니다.

백업에 태그 복사

일반적으로 보호하는 리소스의 태그를 복구 지점으로 AWS Backup 복사합니다. 복원 중에 태그를 복사하는 방법에 대한 자세한 내용은 복원 중 태그 복사를 참조하세요.

예를 들어, Amazon EC2 볼륨을 백업할 때 다음 조건에 따라 그룹 및 개별 리소스 태그를 결과 스냅샷에 AWS Backup 복사합니다.

- 백업에 메타데이터 태그를 저장하는 데 필요한 리소스별 권한 목록은 백업에 태그를 할당하는 데 필요한 권한을 참조하세요.
- 원래 리소스와 연결된 태그와 백업 중에 할당된 태그는 백업 저장소에 저장된 복구 지점에 최대 50개까지 할당됩니다 (AWS 제한 사항). 백업 중에 할당되는 태그의 우선 순위가 높으며 두 태그 세트는 모두 알파벳 순서로 복사됩니다.
- DynamoDB는 먼저 고급 DynamoDB 백업을 활성화하지 않는 한 백업에 태그 할당을 지원하지 않습니다.
- Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨은 중첩된 리소스입니다. Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨의 태그는 중첩된 태그입니다. AWS Backup 중첩된 태그를 복사하기 위해 최선을 다하지만 실패하면 중첩된 태그 없이 백업을 생성하고 상태 완료됨을 보고합니다.
- Amazon EC2 백업이 이미지 복구 지점과 스냅샷 세트를 생성하면 태그를 결과 AMI에 AWS Backup 복사합니다. AWS Backup 또한 Amazon EC2 인스턴스와 연결된 볼륨의 태그를 결과 스냅샷으로 복사하기 위해 최선을 다합니다.

백업을 다른 AWS 리전백업에 복사하는 경우 원본 백업의 모든 태그를 대상에 AWS Backup 복사합니다. AWS 리전

백업 작업 중지

백업 작업이 시작된 AWS Backup 후에 중지할 수 있습니다. 중지하면 백업이 생성되지 않고 백업 작업 기록이 중단됨 상태로 유지됩니다.

콘솔을 AWS Backup 사용하여 백업 작업을 중지하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 작업을 선택합니다.
3. 중지할 백업 작업을 선택합니다.
4. 백업 작업 세부 정보 창에서 중지를 선택합니다.

백업 복사

대부분의 리소스 유형에 대해 예약된 백업 계획의 일부로 백업을 여러 개 AWS 계정 또는 필요에 AWS 리전 따라 복사하거나 자동으로 복사할 수 있습니다. 자세한 내용은 을 참조하십시오the section called “리소스별 기능 가용성”.

Amazon RDS 및 Aurora를 제외하고 지원되는 대부분의 리소스에 대해 교차 계정 복사 및 교차 리전 복사의 시퀀스를 자동화할 수도 있습니다. Amazon RDS 및 Aurora 스냅샷의 경우 AWS Backup , 서비스에서 암호화 키를 생성하는 방식 때문에 계정 간 또는 지역 간 복사 자동화만 지원합니다 (다중 AZ DB 클러스터 스냅샷 복사는 지원되지 않음).

일부 리소스 유형에는 연속 백업 기능과 교차 리전 복사 및 교차 계정 복사를 모두 사용할 수 있습니다. 연속 백업의 교차 리전 또는 교차 계정 복사본을 생성하면 복사된 복구 시점(백업)은 스냅샷(정기) 백업이 됩니다. 리소스 유형에 따라 스냅샷은 증분 복사본일 수도 있고 전체 복사본일 수도 있습니다. 이러한 복사본에는 PITR(시점 복원)을 사용할 수 없습니다.

사본에는 생성 날짜 및 보존 기간을 포함한 소스 구성이 그대로 유지됩니다. 생성일은 사본이 생성된 날짜가 아니라 원본이 생성된 날짜를 나타냅니다.

참고: 복사본이 만료되지 않도록 설정된 경우에도 소스 구성은 복사본의 만료 설정을 재정의합니다. 만료되지 않도록 설정된 복사본은 여전히 소스의 만료 날짜를 유지합니다.

백업 복사본이 만료되지 않도록 하려면 소스 백업이 만료되지 않도록 설정하거나 새 복사본을 생성한 후 100년 후에 만료되도록 지정하세요.

내용

전체에 백업 복사본 생성 AWS 리전

를 사용하면 AWS Backup필요에 AWS 리전 따라 백업을 여러 개에 복사하거나 예약된 백업 계획의 일부로 자동으로 복사할 수 있습니다. 교차 리전 복제는 프로덕션 데이터로부터 최소 거리에 백업을 저장해야 하는 비즈니스 연속성 또는 규정 준수 요구 사항이 있는 경우 특히 유용합니다. 동영상 자습서는 백업의 교차 리전 복사본 관리를 참조하세요.

백업을 새 백업에 AWS 리전 처음으로 복사하는 경우 백업 전체를 AWS Backup 복사합니다. 일반적으로 서비스가 증분 백업을 지원하는 경우 동일한 백업의 후속 사본은 증분 AWS 리전 백업이 됩니다. AWS Backup 대상 저장소의 고객 관리 키를 사용하여 사본을 다시 암호화합니다.

Amazon EBS는 예외로, 복사 작업 중에 스냅샷의 암호화 상태를 변경하면 증분 복사가 아닌 전체 복사가 발생합니다.

요구 사항

- AWS Backup지원되는 대부분의 리소스는 지역 간 백업을 지원합니다. 구체적인 내용은 리소스별 기능 가용성 섹션을 참조하세요.
- 대부분의 AWS 지역은 지역 간 백업을 지원합니다. 구체적인 내용은 기능 가용성은 다음과 같습니다. AWS 리전 섹션을 참조하세요.
- AWS Backup 콜드 티어 스토리지용 교차 리전 복사본은 지원하지 않습니다.

특정 리소스를 사용한 지역 간 복사 고려 사항

Amazon RDS

옵션 그룹을 다른 AWS 리전그룹에 복사할 수 없습니다. 이렇게 시도하면 “스냅샷에는 다음 옵션이 있는 대상 옵션 그룹이 필요합니다.” 와 같은 오류가 발생할 수 있습니다.

Amazon RDS 스냅샷의 리전 간 사본을 새로 생성할 AWS 리전 때 대상에 동일한 옵션 그룹을 입력해야 합니다.

온디맨드 교차 리전 백업 수행

요청 시 기존 백업을 복사하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 볼트를 선택합니다.
3. 복사하려는 복구 시점이 포함된 볼트를 선택합니다.
4. 백업 섹션에서 복사할 복구 시점을 선택합니다.
5. 작업 드롭다운 버튼을 사용하여 복사를 선택합니다.
6. 다음 값을 입력합니다.

대상에 복사

복사할 AWS 리전 대상을 선택합니다. 복사할 때마다 새 복사 규칙을 새 대상에 추가할 수 있습니다.

대상 백업 볼트

복사본의 대상 백업 볼트를 선택합니다.

콜드 스토리지로 전환

백업 복사본을 콜드 스토리지로 전환할 시기를 선택합니다. 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 복사본이 콜드 스토리지로 전환된 후에는 이 값을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 목록을 보려면 리소스별 기능 가용성 표의 '콜드 스토리지로 전환 시 수명 주기'를 참조하세요. 다른 리소스에서는 콜드 스토리지 표현식이 무시됩니다.

보존 기간

복사본 생성 후 삭제될 때까지의 일 수를 지정합니다. 이 값은 콜드 스토리지로 전환 값보다 90일 이상이 커야 합니다. 상시 보존 기간은 복사본을 무기한 유지합니다.

IAM 역할

사본을 생성할 때 사용할 IAM 역할을 선택합니다. AWS Backup 또한 역할은 역할을 수임할 수 있는 신뢰할 수 있는 개체로 AWS Backup 등록되어 있어야 합니다. AWS Backup 기본값을 선택했는데 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 역할이 자동으로 생성됩니다.

7. 복사를 선택합니다.

교차 리전 백업 예약

예약 백업 계획을 사용하여 AWS 리전간에 백업을 복사할 수 있습니다.

예약 백업 계획을 사용하여 백업을 복사하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 내 계정에서 백업 계획을 선택한 다음 백업 계획 생성을 선택합니다.
3. 백업 계획 생성 페이지에서 새 계획 수립을 선택합니다.
4. 백업 계획 이름에 백업 계획의 이름을 입력합니다.
5. 백업 규칙 구성 섹션에서 백업 일정, 백업 기간, 수명 주기 규칙을 정의하는 백업 규칙을 추가합니다. 나중에 백업 규칙을 더 추가할 수 있습니다.

   a. 백업 규칙 이름에 규칙의 이름을 입력합니다.

   b. 백업 볼트의 경우 목록에서 볼트를 선택합니다. 이 백업의 복구 시점은 이 볼트에 저장됩니다. 새 백업 볼트를 생성할 수 있습니다.

   c. 백업 빈도에서 백업을 생성할 빈도를 선택합니다.

   d. PITR을 지원하는 서비스의 경우 이 기능을 사용하려면 point-in-time 복구를 위한 연속 백업 활성화 (PITR) 를 선택합니다. PITR을 지원하는 서비스의 목록은 리소스별 기능 가용성 표의 해당 섹션을 참조하세요.

   e. 백업 기간에서 백업 기간 기본값 사용 - 권장을 선택합니다. 백업 기간을 사용자 지정할 수 있습니다.

   f. 대상으로 복사에서 백업 복사본의 대상 AWS 리전 을 선택합니다. 백업이 이 리전에 복사됩니다. 복사할 때마다 새 복사 규칙을 새 대상에 추가할 수 있습니다. 다음 값을 입력합니다.

      다른 계정의 볼트로 복사

      이 옵션은 켜지 마세요. 계정 간 복사에 대해 자세히 알아보려면 계정 간 백업 사본 만들기를 참조하십시오. AWS 계정

      대상 백업 볼트

      백업을 AWS Backup 복사할 대상 지역의 백업 저장소를 선택하십시오.

      교차 리전 복사를 위한 새 백업 볼트를 생성하려면 새 백업 볼트 생성을 선택합니다. 마법사에 정보를 입력합니다. 그런 다음 백업 볼트 생성을 선택합니다.

6. 계획 생성을 선택합니다.

전체에 백업 복사본 생성 AWS 계정

를 사용하면 AWS Backup필요에 AWS 계정 따라 여러 개에 백업하거나 예약된 백업 계획의 일부로 자동으로 백업할 수 있습니다. 운영상 또는 보안상의 이유로 조직 내 하나 AWS 계정 이상에 백업을 안전하게 복사하려면 계정 간 백업을 사용하세요. 원본 백업이 실수로 삭제된 경우 대상 계정에서 소스 계정으로 백업을 복사한 다음 복원을 시작할 수 있습니다. 이렇게 하려면 먼저 AWS Organizations 서비스에서 동일한 조직에 속하는 2개의 계정이 있어야 합니다. 자세한 내용은 Organizations 사용 설명서의 자습서: 조직 생성 및 구성을 참조하세요.

대상 계정에서 백업 볼트를 생성해야 합니다. 그런 다음 대상 계정의 백업을 암호화하는 고객 관리 키와 복사하려는 리소스에 대한 액세스를 허용하는 AWS Backup 리소스 기반 액세스 정책을 할당합니다. 소스 계정에서 리소스가 고객 관리형 키로 암호화되는 경우 이 고객 관리형 키를 대상 계정과 공유해야 합니다. 그런 다음 백업 계획을 생성하고 AWS Organizations의 조직 단위에 속하는 대상 계정을 선택할 수 있습니다.

크로스 어카운트에 백업을 처음으로 복사하는 경우 백업 전체가 AWS Backup 복사됩니다. 일반적으로 서비스가 증분 백업을 지원하는 경우 동일한 계정에 있는 해당 백업의 후속 복사본은 증분 백업입니다. AWS Backup 대상 저장소의 고객 관리 키를 사용하여 사본을 다시 암호화합니다.

요구 사항

- 여러 AWS 계정 핀의 AWS Backup리소스를 관리하려면 먼저 계정이 서비스의 동일한 조직에 속해야 합니다. AWS Organizations
- 에서 AWS Backup 지원하는 대부분의 리소스는 계정 간 백업을 지원합니다. 구체적인 내용은 리소스별 기능 가용성 섹션을 참조하세요.
- 대부분의 AWS 지역에서는 계정 간 백업을 지원합니다. 구체적인 내용은 기능 가용성은 다음과 같습니다. AWS 리전 섹션을 참조하세요.
- AWS Backup 콜드 티어의 스토리지에는 계정 간 복사본을 지원하지 않습니다.

교차 계정 백업 설정

교차 계정 백업을 생성하려면 무엇이 필요한가요?

- 소스 계정

  소스 계정은 프로덕션 AWS 리소스와 기본 백업이 있는 계정입니다.

소스 계정 사용자가 교차 계정 백업 작업을 시작합니다. 소스 계정 사용자 또는 역할에 적절한 API 권한이 있어야 작업을 시작할 수 있습니다. 적절한 권한은 작업에 대한 전체 액세스를 허용하는 AWS 관리형 `AWSBackupFullAccess` 정책이나 다음과 같은 AWS Backup `ec2:ModifySnapshotAttribute` 작업을 허용하는 고객 관리형 정책일 수 있습니다. 정책 유형에 대한 자세한 내용은 AWS Backup 관리형 정책을 참조하세요.

- 대상 계정

  대상 계정은 백업 복사본을 보관하려는 계정입니다. 대상 계정을 두 개 이상 선택할 수 있습니다. 대상 계정은 AWS Organizations의 소스 계정과 동일한 조직에 있어야 합니다.

  대상 백업 볼트에 대한 액세스 정책 `backup:CopyIntoBackupVault`를 '허용'해야 합니다. 이 정책이 없으면 대상 계정으로의 복사 시도가 거부됩니다.

- 의 관리 계정 AWS Organizations

  관리 계정은 AWS Organizations에서 정의한 대로 AWS 계정간에 교차 계정 백업을 관리하는 데 사용하는 조직의 기본 계정입니다. 교차 계정 백업을 사용하려면 서비스 신뢰도 활성화해야 합니다. 서비스 신뢰를 활성화한 후에는 조직의 모든 계정을 대상 계정으로 사용할 수 있습니다. 대상 계정에서 교차 계정 백업에 사용할 볼트를 선택할 수 있습니다.

- AWS Backup 콘솔에서 교차 계정 백업 활성화

보안에 대한 자세한 내용은 교차 계정 백업을 위한 보안 고려 사항 단원을 참조하세요.

교차 계정 백업을 사용하려면 교차 계정 백업 기능을 활성화해야 합니다. 그런 다음 대상 백업 볼트에 대한 액세스 정책 `backup:CopyIntoBackupVault`를 '허용'해야 합니다.

계정 간 백업 활성화

1. AWS Organizations 관리 계정 자격 증명을 사용하여 로그인합니다. 교차 계정 백업은 이러한 보안 인증 정보를 사용해서만 활성화 또는 비활성화할 수 있습니다.
2. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
3. 내 계정에서 설정을 선택합니다.
4. 교차 계정 백업에 활성화를 선택합니다.
5. 백업 볼트에서 대상 볼트를 선택합니다.

   계정 간 복사의 경우 원본 보관소와 대상 저장소는 서로 다른 계정에 있습니다. 필요에 따라 대상 계정을 소유한 계정으로 전환하십시오.

6. 액세스 정책 섹션에서 backup:CopyIntoBackupVault를 '허용'합니다. 예를 들어 권한 추가를 선택한 다음 조직의 백업 볼트에 대한 액세스 허용을 선택합니다. 이외의 모든 계정 간 활동은 backup:CopyIntoBackupVault 거부됩니다.
7. 이제 조직의 모든 계정이 조직의 다른 모든 계정과 백업 볼트의 콘텐츠를 공유할 수 있습니다. 자세한 정보는 백업 볼트를 다른 AWS 계정과 공유을 참조하세요. 다른 계정의 백업 볼트의 콘텐츠를 수신할 수 있는 계정을 제한하려면 계정을 대상 계정으로 구성 단원을 참조하세요.

교차 계정 백업 예약

예약 백업 계획을 사용하여 AWS 계정간에 백업을 복사할 수 있습니다.

예약 백업 계획을 사용하여 백업을 복사하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 내 계정에서 백업 계획을 선택한 다음 백업 계획 생성을 선택합니다.
3. 백업 계획 생성 페이지에서 새 계획 수립을 선택합니다.
4. 백업 계획 이름에 백업 계획의 이름을 입력합니다.
5. 백업 규칙 구성 섹션에서 백업 일정, 백업 기간, 수명 주기 규칙을 정의하는 백업 규칙을 추가합니다. 나중에 백업 규칙을 더 추가할 수 있습니다.

   규칙 이름에 규칙의 이름을 입력합니다.
6. 예약 섹션의 빈도에서 백업을 수행할 빈도를 선택합니다.
7. 백업 기간에서 백업 기간 기본값 사용(권장)을 선택합니다. 백업 기간을 사용자 지정할 수 있습니다.
8. 백업 볼트의 경우 목록에서 볼트를 선택합니다. 이 백업의 복구 시점은 이 볼트에 저장됩니다. 새 백업 볼트를 생성할 수 있습니다.
9. 사본 생성 - 선택 사항 섹션에 다음 값을 입력합니다.

   대상 리전

   백업 복사본을 저장할 대상을 AWS 리전 선택합니다. 백업이 이 리전에 복사됩니다. 복사할 때마다 새 복사 규칙을 새 대상에 추가할 수 있습니다.

   다른 계정의 볼트로 복사

   토글하여 이 옵션을 선택합니다. 선택하면 옵션이 파란색으로 바뀝니다. 외부 볼트 ARN 옵션이 나타납니다.

외부 볼트 ARN

대상 계정의 Amazon 리소스 이름(ARN)을 입력합니다. ARN은 계정 ID와 계정 ID가 포함된 문자열입니다. AWS 리전 AWS Backup 백업을 대상 계정의 저장소에 복사합니다. 대상 리전 목록은 외부 볼트 ARN의 리전으로 자동 업데이트됩니다.

백업 볼트 액세스 허용에서 허용을 선택합니다. 그런 다음 열리는 마법사에서 허용을 선택합니다.

AWS Backup 백업을 지정된 값으로 복사하려면 외부 계정에 액세스할 수 있는 권한이 필요합니다. 마법사는 이러한 액세스를 제공하는 다음과 같은 예제 정책을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

콜드 스토리지로 전환

백업 복사본을 콜드 스토리지로 전환할 시기와 복사본의 만료(삭제) 시기를 선택합니다. 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 복사본이 콜드 스토리지로 전환된 후에는 이 값을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 목록을 보려면 리소스별 기능 가용성 표의 '콜드 스토리지로 전환 시 수명 주기'를 참조하세요. 다른 리소스에서는 콜드 스토리지 표현식이 무시됩니다.

만료는 복사본 생성 후 삭제될 때까지의 일 수를 지정합니다. 이 값은 콜드 스토리지로 전환 값보다 90일 이상이 커야 합니다.

> **Note**
>
> 백업이 만료되고 수명 주기 정책의 일부로 삭제 대상으로 표시되면 다음 8시간 동안 임의로 선택한 시점에서 백업을 AWS Backup 삭제합니다. 이 창은 일관된 성능을 보장하는 데 도움이 됩니다.

10. 복구 시점에 태그를 추가하려면 복구 시점에 추가되는 태그를 선택합니다.
11. 고급 백업 설정에서 Windows VSS를 선택하여 EC2에서 실행되는 선택된 서드 파티 소프트웨어에 대해 애플리케이션 인식 스냅샷을 활성화합니다.
12. 계획 생성을 선택합니다.

온디맨드 교차 계정 백업 수행

필요에 따라 백업을 다른 백업에 복사할 수 있습니다. AWS 계정

온디맨드로 백업을 복사하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 내 계정에서 백업 볼트를 선택하여 모든 백업 볼트를 나열합니다. 백업 볼트 이름 또는 태그를 기준으로 필터링할 수 있습니다.
3. 복사하려는 백업의 복구 시점 ID를 선택합니다.
4. 복사를 선택합니다.
5. 백업 세부 정보를 확장하여 복사 중인 복구 시점에 대한 정보를 확인합니다.
6. 복사 구성 섹션의 대상 리전 목록에서 옵션을 선택합니다.
7. 다른 계정의 볼트로 복사를 선택합니다. 선택하면 옵션이 파란색으로 바뀝니다.
8. 대상 계정의 Amazon 리소스 이름(ARN)을 입력합니다. ARN은 계정 ID와 계정 ID가 포함된 문자열입니다. AWS 리전 AWS Backup 백업을 대상 계정의 저장소에 복사합니다. 대상 리전 목록은 외부 볼트 ARN의 리전으로 자동 업데이트됩니다.
9. 백업 볼트 액세스 허용에서 허용을 선택합니다. 그런 다음 열리는 마법사에서 허용을 선택합니다.

   사본을 만들려면 원본 계정에 액세스할 수 있는 권한이 AWS Backup 필요합니다. 마법사는 이러한 액세스를 제공하는 예제 정책을 보여줍니다. 이 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

10. 콜드 스토리지로 전환에서 백업 복사본을 콜드 스토리지로 전환할 시기와 복사본의 만료(삭제) 시기를 선택합니다. 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 복사본이 콜드 스토리지로 전환된 후에는 이 값을 변경할 수 없습니다.

    콜드 스토리지로 전환할 수 있는 리소스 목록을 보려면 리소스별 기능 가용성 표의 '콜드 스토리지로 전환 시 수명 주기'를 참조하세요. 다른 리소스에서는 콜드 스토리지 표현식이 무시됩니다.

    만료는 복사본 생성 후 삭제될 때까지의 일 수를 지정합니다. 이 값은 콜드 스토리지로 전환 값보다 90일 이상이 커야 합니다.

11. IAM 역할에서 백업을 복사에 사용할 수 있는 권한이 있는 IAM 역할(예: 기본 역할)을 지정합니다. 복사 작업은 대상 계정의 서비스 연결 역할에 의해 수행됩니다.
12. 복사를 선택합니다. 복사하는 리소스의 크기에 따라 이 프로세스를 완료하는 데 몇 시간이 걸릴 수 있습니다. 복사 작업이 완료되면 작업 메뉴의 복사 작업 탭에 복사가 표시됩니다.

암호화 키 및 계정 간 사본

계정 간 복사 암호화 키는 리소스 유형에 따라 달라집니다. 소스 백업 저장소의 암호화 키를 전체 관리 AWS Backup 사용한 리소스 고객 관리형 KMS 키는 이러한 리소스 유형의 계정 간 복사 암호화에 사용할 수 있습니다.

에서 완전히 관리되지 않는 리소스 유형은 소스 KMS 키와 리소스 KMS 키가 동일합니다. AWS Backup 에서 완전히 AWS 관리되지 않는 이러한 유형의 리소스에는 관리형 KMS 키를 사용한 계정 간 복사가 지원되지 않습니다. AWS Backup

계정 간 복사 실패 문제를 해결하는 데 도움이 더 필요하면 지식 센터를 참조하십시오.AWS

계정 간 복사 시 소스 계정 KMS 키 정책은 KMS 키 정책에서 대상 계정을 허용해야 합니다.

한 백업에서 다른 백업으로 복원 AWS 계정

AWS Backup 한 리소스에서 다른 AWS 계정 리소스로의 리소스 복구를 지원하지 않습니다. 하지만 한 계정의 백업을 다른 계정으로 복사한 다음 해당 계정에서 복원할 수 있습니다. 예를 들어 백업을 계정 A에서 계정 B로 복원할 수는 없지만 백업을 계정 A에서 계정 B로 복사한 다음 계정 B에서 복원할 수 있습니다.

백업을 한 계정에서 다른 계정으로 복원하는 절차는 2단계 프로세스입니다.

백업을 한 계정에서 다른 계정으로 복원하려면

1. AWS 계정 원본의 백업을 복원하려는 계정에 복사합니다. 지침은 교차 계정 백업 설정을 참조하세요.
2. 리소스에 적절한 지침을 사용하여 백업을 복원합니다.

백업 볼트를 다른 AWS 계정과 공유

AWS Backup 백업 저장소를 하나 이상의 계정과 공유하거나 조직 전체와 공유할 수 AWS Organizations있습니다. 대상 백업 볼트를 소스 AWS 계정, 사용자 또는 IAM 역할과 공유할 수 있습니다.

대상 백업 볼트를 공유하려면

1. AWS Backup을 선택한 다음 백업 볼트를 선택합니다.
2. 공유할 백업 볼트의 이름을 선택합니다.
3. 액세스 정책 창에서 권한 추가 드롭다운을 선택합니다.
4. 백업 볼트에 계정 수준 액세스 허용을 선택합니다. 또는, 조직 수준 또는 역할 수준 액세스를 허용하도록 선택할 수 있습니다.
5. 이 대상 백업 볼트와 공유하려는 계정의 AccountID를 입력합니다.
6. 정책 저장을 선택합니다.

IAM 정책을 사용하여 백업 볼트를 공유할 수 있습니다.

대상 백업 볼트를 AWS 계정 또는 IAM 역할과 공유

다음 정책은 백업 볼트를 계정 번호 4444555566666 및 계정 번호 111122223333의 IAM 역할 SomeRole과 공유합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

대상 백업 저장소 (조직 구성 단위) 를 공유합니다. AWS Organizations

다음 정책은 해당 `PrincipalOrgPaths` 사용하여 조직 단위와 백업 볼트를 공유합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

대상 백업 저장소를 다음 조직과 공유하십시오. AWS Organizations

다음 정책은 백업 볼트를 PrincipalOrgID 'o-a1b2c3d4e5'의 조직과 공유합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

계정을 대상 계정으로 구성

AWS Organizations 관리 계정을 사용하여 처음으로 계정 간 백업을 활성화하면 멤버 계정의 모든 사용자가 자신의 계정을 대상 계정으로 구성할 수 있습니다. 대상 계정을 제한하려면 AWS Organizations 에서 다음 서비스 제어 정책(SCP)을 하나 이상 설정하는 것이 좋습니다. AWS Organizations 노드에 서비스 제어 정책을 연결하는 방법에 대한 자세한 내용은 서비스 제어 정책 연결 및 분리를 참조하십시오.

태그를 사용하여 대상 계정 제한

이 정책은 AWS Organizations 루트, OU 또는 개인 계정에 연결하는 경우 해당 루트, OU 또는 계정의 복사 대상을 사용자가 태깅한 백업 저장소가 있는 계정으로만 제한합니다. DestinationBackupVault 권한 "backup:CopyIntoBackupVault"는 백업 볼트가 작동하는 방식, 그리고 이 경우에는 유효한 대상 백업 볼트를 제어합니다. 이 정책을 승인된 대상 볼트에 적용되는 해당 태그와 함께 사용하여 교차 계정 복사의 대상을 승인된 계정 및 백업 볼트로만 제어할 수 있습니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

계정 번호 및 볼트 이름을 사용하여 대상 계정 제한

이 정책은 AWS Organizations 루트, OU 또는 개별 계정에 연결하는 경우 해당 루트, OU 또는 계정에서 생성되는 복사본을 두 개의 대상 계정으로만 제한합니다. 권한 `"backup:CopyFromBackupVault"`는 백업 볼트에서 복구 시점이 작동하는 방식, 그리고 이 경우에는 해당 복구 시점을 복사할 수 있는 대상을 제어합니다. 하나 이상의 대상 백업 볼트 이름이 `cab-`으로 시작하는 경우 소스 볼트가 첫 번째 대상 계정(112233445566)으로의 복사만 허용합니다. 대상이 `fort-knox`로 이름이 지정된 단일 백업 볼트인 경우 소스 볼트가 두 번째 대상 계정(123456789012)으로의 복사만 허용합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
      }
    }
  ]
}
```

다음 조직 단위를 사용하여 대상 계정을 제한합니다. AWS Organizations

원본 계정이 포함된 AWS Organizations 루트 또는 OU에 연결하거나 원본 계정에 연결할 경우 다음 정책에 따라 대상 계정이 지정된 두 OU 내의 해당 계정으로 제한됩니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

교차 계정 백업을 위한 보안 고려 사항

AWS Backup에서 교차 계정 백업을 수행할 때는 다음 사항에 유의해야 합니다.

- 대상 볼트는 기본 볼트가 될 수 없습니다. 이는 기본 볼트가 다른 계정과 공유할 수 없는 키로 암호화되어 있기 때문입니다.
- 교차 계정 백업을 비활성화한 후에도 최대 15분 동안 교차 계정 백업이 계속 실행될 수 있습니다. 이는 최종 일관성 때문이며, 교차 계정 백업을 비활성화한 후에도 일부 교차 계정 작업이 시작되거나 완료될 수 있습니다.
- 대상 계정이 나중에 조직을 벗어나는 경우 해당 계정에 백업이 유지됩니다. 잠재적 데이터 유출을 방지하려면 대상 계정에 연결된 서비스 제어 정책(SCP)에서 `organizations:LeaveOrganization` 권한에 거부 권한을 부여하세요. SCP에 대한 자세한 내용은 Organizations 사용 설명서의 조직에서 멤버 계정 제거를 참조하세요.
- 계정 간 복사 중에 복사 작업 역할을 삭제하면 복사 작업이 완료될 때 소스 계정에서 스냅샷을 공유 해제할 AWS Backup 수 없습니다. 이 경우 백업 작업은 완료되지만 복사 작업 상태는 스냅샷 공유 취소 실패로 표시됩니다.

백업 삭제

백업 계획을 생성할 때 수명 주기를 구성하여 더 이상 필요하지 않은 백업을 자동으로 삭제하는 데 사용하는 AWS Backup 것이 좋습니다. 예를 들어 복구 지점을 1년 동안 보존하도록 백업 계획의 수명 주기를 설정한 경우, AWS Backup 2021년 1월 1일 또는 몇 시간 이내에 생성한 복구 지점이 2022년 1월 1일에 자동으로 삭제됩니다. (AWS Backup 성능 유지를 위해 복구 지점 만료 후 8시간 이내에 데이터를 임의로 삭제합니다.) 수명 주기 보존 정책을 구성하는 방법에 대한 자세한 내용은 백업 계획 생성을 참조하세요.

그러나 하나 이상의 복구 시점을 수동으로 삭제해야 할 수 있습니다. 예:

- EXPIRED 복구 시점이 있습니다. 백업 계획을 만들 때 사용한 원래 IAM 정책을 삭제하거나 수정했기 때문에 복구 지점이 자동으로 삭제되지 AWS Backup 않았습니다. 삭제하려고 AWS Backup 시도했지만 삭제할 권한이 없었습니다.

  AWS 관리형 Amazon EBS 또는 Amazon EC2 복구 지점에 Amazon EBS 스냅샷 잠금이 적용되어 AWS Backup 있고 일반적으로 복구 지점이 삭제되는 수명 주기 프로세스를 완료할 수 없는 경우에도 만료된 복구 지점이 생성될 수 있습니다. 참고로 이러한 만료된 복구 시점은 Amazon EC2 콘솔 및 API 또는 Amazon EBS 콘솔 및 API에서 복원할 수 있습니다.

  > **Warning**
  >
  > 만료된 복구 시점은 계정에 계속 보관됩니다. 이로 인해 스토리지 비용이 증가할 수 있습니다.

  2021년 8월 6일 이후에는 백업 저장소에 대상 복구 지점이 만료됨으로 AWS Backup 표시됩니다. 빨간색 만료됨 상태에 마우스를 갖다 대면 백업을 삭제할 수 없는 이유를 설명하는 팝오버 상태 메시지가 표시됩니다. 새로 고침을 선택하여 최신 정보를 받을 수도 있습니다.
- 백업 계획을 이전에 구성한 방식으로 더 이상 운영하지 않으려고 합니다. 백업 계획을 업데이트하면 이후에 생성될 복구 시점에는 영향을 주지만 이미 생성한 복구 시점에는 영향을 주지 않습니다. 자세한 내용은 백업 계획 업데이트을 참조하세요.
- 테스트 또는 자습서를 마친 후에 정리해야 합니다.

수동으로 백업 삭제

수동으로 복구 시점을 삭제하려면

1. AWS Backup 콘솔의 탐색 창에서 Backup 볼트를 선택합니다.
2. 백업 볼트 페이지에서 백업을 저장한 백업 볼트를 선택합니다.
3. 복구 시점을 선택하고 작업 드롭다운을 선택한 다음 삭제를 선택합니다.
4. 1. 목록에 연속 백업이 포함된 경우 다음 옵션 중 하나를 선택합니다. 각 연속 백업에는 단일 복구 시점이 있습니다.
   - 내 백업 데이터를 영구적으로 삭제 또는 복구 시점 삭제. 이러한 옵션 중 하나를 선택하면 향후 연속 백업이 중지되고 기존의 연속 백업 데이터도 삭제됩니다.

     > **Note**
     >
     > Amazon S3, Amazon RDS 및 Aurora 연속 백업 고려 사항은 을 참조하십시오연속 백업 및 point-in-time 복원 (PITR).

   - 연속 백업 데이터를 보관하거나 복구 지점 연결을 끊으십시오. 이러한 옵션 중 하나를 선택하면 향후 연속 백업이 중지되지만 보존 기간에 정의된 대로 만료될 때까지 기존의 연속 백업 데이터를 유지할 수 있습니다.

     연결이 끊긴 Amazon S3 연속 복구 지점 (백업) 은 백업 저장소에 남아 있지만 상태는 로 STOPPED 전환됩니다.

   2. 나열된 복구 시점을 모두 삭제하려면 삭제를 입력한 다음, 복구 시점 삭제를 선택합니다.
   3. AWS Backup 삭제를 위해 복구 지점을 제출하기 시작하고 진행률 표시줄을 표시합니다. 브라우저 탭을 열어 두고 제출 과정에서 이 페이지를 벗어나지 마세요.
   4. 제출 프로세스가 끝나면 AWS Backup 배너에 상태가 표시됩니다. 가능한 상태는 다음과 같습니다.
      - 성공적으로 제출함. 각 복구 시점의 삭제 상태에 대한 진행률 보기를 선택할 수 있습니다.
      - 제출하지 못함. 각 복구 시점의 삭제 상태에 대한 진행률 보기를 선택하거나 제출을 다시 시도할 수 있습니다.
      - 일부 복구 시점은 성공적으로 제출되었지만 다른 복구 시점은 제출하지 못한 혼합된 결과.
   5. 진행률 보기를 선택하면 각 백업의 삭제 상태를 검토할 수 있습니다. 삭제 상태가 실패 또는 만료됨인 경우 해당 상태를 클릭하여 이유를 확인할 수 있습니다. 실패한 삭제 재시도를 선택할 수도 있습니다.

수동 삭제 문제 해결

드문 경우이긴 하지만 삭제 요청을 완료하지 AWS Backup 못할 수도 있습니다. AWS Backup 서비스 연결 역할을 `AWSServiceRoleForBackup` 사용하여 삭제를 수행합니다.

삭제 요청이 실패할 경우 IAM 역할에 서비스 연결 역할을 생성할 수 있는 권한이 있는지 확인합니다. 특히, IAM 역할이 `iam:CreateServiceLinkedRole` 작업을 포함하는지 확인해야 합니다. 그렇지 않은 경우 백업을 생성하는 데 사용된 역할에 이 권한을 추가합니다. 이 권한을 추가하면 수동 AWS Backup 삭제를 수행할 수 있습니다.

IAM 역할이 `iam:CreateServiceLinkedRole` 작업을 포함함을 확인한 후에도 복구 시점이 여전히 해당 `DELETING` 상태로 유지되는 경우 AWS에서 해당 문제를 조사 중일 수 있습니다. 다음 단계에 따라 수동 삭제를 완료합니다.

1. 2~3일 후에 다시 확인하도록 알림을 설정합니다.
2. 2~3일 후, 첫 번째 수동 삭제 작업의 결과인 최근 `EXPIRED` 삭제 지점이 있는지 확인합니다.
3. 해당 `EXPIRED` 복구 시점을 수동으로 삭제합니다.

역할에 대한 자세한 내용은 서비스 연결 역할 사용 및 IAM 자격 증명 권한 추가 및 제거를 참조하세요.

백업 편집

를 사용하여 AWS Backup백업을 만든 후 백업의 수명 주기 또는 태그를 변경할 수 있습니다. 수명 주기는 백업이 콜드 스토리지로 전환되는 시기와 만료되는 시점을 정의합니다. AWS Backup 은 사용자가 정의한 수명 주기에 따라 백업을 자동으로 전환하고 만료합니다.

콜드 스토리지로 전환할 수 있는 리소스 목록을 보려면 리소스별 기능 가용성 표의 '콜드 스토리지로 전환 시 수명 주기'를 참조하세요. 다른 리소스에서는 콜드 스토리지 표현식이 무시됩니다.

> **Note**
>
> AWS Backup 콘솔을 사용한 백업 태그 편집은 Amazon Elastic File System (Amazon EFS) 파일 시스템 및 고급 Amazon DynamoDB의 백업에만 지원됩니다.
> 다른 리소스를 생성할 때 복구 시점에 추가된 태그는 계속 표시되지만 회색으로 표시되고 편집할 수 없습니다. 이러한 태그는 콘솔에서 편집할 수 없지만 서비스의 AWS Backup 콘솔 또는 API를 사용하여 이러한 다른 서비스 백업의 태그를 편집할 수 있습니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 따라서 "콜드로 전환 전 보관 일수" 설정을 업데이트할 때 값은 최소 백업 기간에 1일을 더해야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

다음은 백업 수명 주기를 업데이트하는 방법을 보여주는 예입니다.

백업 수명 주기를 편집하려면

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 백업 섹션에서 백업을 선택합니다.
4. 백업 세부 정보 페이지에서 편집을 선택합니다.
5. 수명 주기 설정을 구성하고 저장을 선택합니다.

백업 복원

복원 방법

콘솔 복원 지침 및 AWS Backup지원되는 각 리소스 유형에 대한 설명서 링크는 이 페이지 하단에 있는 링크를 참조하십시오.

백업을 프로그래밍 방식으로 복원하려면 StartRestoreJob API 작업을 사용합니다.

리소스를 복원하는 데 필요한 구성 값('복원 메타데이터')은 복원하려는 리소스에 따라 다릅니다. 백업을 생성할 때 사용한 구성 메타데이터를 가져오려면 GetRecoveryPointRestoreMetadata를 호출할 수 있습니다. 이 페이지 하단의 링크에서 메타데이터 복원 예제도 확인할 수 있습니다.

콜드 스토리지로부터 복원은 웜 스토리지로부터 복원보다 일반적으로 4시간이 더 걸립니다.

각 복원마다 고유한 작업 ID(예: `1323657E-2AA4-1D94-2C48-5D7A423E7394`)를 사용하여 복원 작업이 생성됩니다.

> **Note**
>
> AWS Backup 복원 시간에 대한 서비스 수준 계약 (SLA) 을 제공하지 않습니다. 복원 시간은 시스템 로드 및 용량에 따라 달라질 수 있으며, 동일한 리소스를 포함하는 복원의 경우에도 마찬가지입니다.

비파괴 복원

를 AWS Backup 사용하여 백업을 복원하면 복원 중인 백업과 함께 새 리소스가 생성됩니다. 이는 복원 활동으로 인해 기존 리소스가 손상되지 않도록 보호하기 위한 것입니다.

복원 테스트

리소스에 대한 테스트를 수행하여 복원 경험을 시뮬레이션할 수 있습니다. 이를 통해 조직의 복원 시점 목표(RTO)를 충족하는지 판단하고 향후 복원 요구 사항에 대비할 수 있습니다.

자세한 내용은 복원 테스트 섹션을 참조하세요.

복원 중 태그 복사

> **Note**
>
> Amazon DynamoDB, Amazon S3, SAP HANA on Amazon EC2 인스턴스, 가상 머신 및 Amazon Timestream 리소스의 복원에서는 현재 이 기능을 사용할 수 없습니다.

소개

태그가 백업 당시 보호된 리소스에 속해 있었다면 리소스를 복원하면서 태그를 복사할 수 있습니다. 키-값 페어가 포함된 레이블인 태그는 리소스를 식별하고 검색하는 데 도움이 될 수 있습니다. 복원 작업을 시작할 때 원래 백업된 리소스에 속한 태그를 복원 중인 리소스에 추가할 수 있습니다.

복원 작업 중에 태그를 포함하도록 선택하면 이 단계를 통해 복원 작업이 완료된 후 리소스에 태그를 수동으로 적용하는 데 드는 오버헤드와 수고를 대체할 수 있습니다. 단, 이 기능은 복원된 리소스에 새 태그를 추가하는 것과는 다릅니다.

콘솔 흐름에서 백업을 복원하면 기본적으로 소스 태그가 복사됩니다. 복원된 리소스에 태그를 복사하지 않도록 하려면 콘솔에서 확인란을 선택 취소하세요.

API 작업 `StartRestoreJob`에서 `CopySourceTagsToRestoredResource` 파라미터는 기본적으로 `false`로 설정되며, 이렇게 하면 복원 중인 리소스에서 원본 소스 태그가 제외됩니다. 원본 소스의 태그를 포함하려면 이 파라미터를 `True`로 설정합니다.

고려 사항

- 리소스에는 복원된 리소스를 포함하여 최대 50개의 태그가 포함될 수 있습니다. 태그 제한에 대한 자세한 내용은 AWS 리소스 태그 지정을 참조하십시오.
- 복원에 사용되는 역할에 태그를 복사할 수 있는 올바른 권한이 있는지 확인하세요. 복원 기본 역할에는 필요한 권한이 포함되어 있습니다. 사용자 지정 역할에는 리소스에 태그를 지정할 수 있는 추가 권한이 포함되어야 합니다.
- VMware Cloud™ on, VMware Cloud™ on, 온프레미스 시스템, Amazon EC2 기반 SAP HANA 인스턴스 AWS, 타임스트림 AWS Outposts, DynamoDB, 고급 DynamoDB 및 Amazon S3와 같은 리소스는 현재 복원 태그 포함이 지원되지 않습니다.
- 연속 백업의 경우 가장 최근 백업을 기준으로 원본 리소스의 태그가 복원된 리소스에 복사됩니다.
- 항목 수준 복원에서는 태그가 복사되지 않습니다.
- 백업 작업이 완료된 후 백업에 추가되었지만 백업 전에는 원래 리소스에 없던 태그는 복원된 리소스에 복사되지 않습니다. 2023년 5월 22일 이후에 생성된 백업만 복원 시 태그 복사 기능이 적용됩니다.

특정 리소스와의 태그 상호 작용

- Amazon EC2
  - 복원된 Amazon EC2 인스턴스에 적용된 태그는 연결된 복원된 Amazon EBS 볼륨에도 적용됩니다.
  - 원본 인스턴스에 연결된 EBS 볼륨에 적용된 태그는 복원된 인스턴스에 연결된 볼륨에 복사되지 않습니다. 태그를 기반으로 사용자의 EBS 볼륨 액세스를 허용하거나 거부하는 IAM 정책이 있는 경우, 정책이 계속 유효하도록 복원된 볼륨에 필요한 태그를 수동으로 재할당해야 합니다.
- Amazon EFS 리소스는 복원할 때 새 파일 시스템에 복사해야 합니다. 기존 파일 시스템에 복원하는 경우 태그를 기존 파일 시스템에 복사할 수 없습니다.
- Amazon RDS
  - 백업된 RDS 클러스터가 여전히 활성 상태인 경우 이 클러스터의 태그가 복사됩니다.
  - 원래 클러스터가 더 이상 활성 상태가 아닌 경우 대신 클러스터 스냅샷의 태그가 복사됩니다.

- 백업 당시 리소스에 있던 태그는 CopySourceTagsToRestoredResource의 부울 파라미터가 True 또는 False로 설정되었는지 관계없이 복원 중에 복사됩니다. 하지만 스냅샷에 태그가 없는 경우 위의 부울 설정이 사용됩니다.
- Amazon Redshift 클러스터는 기본적으로 복원 작업 중에 항상 태그를 포함합니다.

콘솔을 통해 태그 복사

1. AWS Backup 콘솔을 엽니다
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon S3 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택한 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면

   a. 백업 창에서 리소스의 복구 시점 ID를 선택합니다.

   b. 창의 오른쪽 위에서 복원을 선택합니다. 또는 백업 볼트로 이동하여 복구 시점을 찾은 다음 작업, 복원을 차례로 클릭해도 됩니다.
4. 백업 복원 페이지에서 '태그 포함 복원'이라는 패널을 찾습니다. 원본 리소스의 태그를 모두 포함하려면 확인란을 선택한 상태로 유지합니다(콘솔에서는 이 확인란이 기본적으로 선택되어 있음).
5. 원하는 설정 및 역할을 모두 선택한 후 백업 복원을 클릭합니다.

프로그래밍 방식으로 태그를 포함하려면

API 작업 StartRestoreJob을 사용합니다. 다음 부울 파라미터가 True로 설정되어 있는지 확인합니다.

```
CopySourceTagsToRestoredResource = true
```

부울 파라미터 CopySourceTagsToRestoredResource가 True인 경우 복원 작업은 원본 리소스의 태그를 복원된 자료에 복사합니다.

> **Important**
>
> 지원되지 않는 리소스 (VMware, 온프레미스 시스템, EC2 인스턴스의 SAP HANA, 타임스트림, DynamoDB AWS Outposts, 고급 DynamoDB, Amazon S3) 에 대해 이 파라미터가 포함된 경우 복원 작업이 실패합니다.

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

태그 복원 문제 해결

오류: 권한 부족

해결 방법: 복원 역할에 복원된 리소스에 태그를 포함하는 데 필요한 권한이 있는지 확인합니다. 복원을 위한 기본 AWS 관리형 서비스 역할 정책에는 이 작업에 필요한 권한이 포함되어 있습니다. AWSBackupServiceRolePolicyForRestores

사용자 지정 역할을 사용하는 경우 다음 권한이 있어야 합니다.

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

자세한 내용은 API 권한을 참조하세요.

복원 작업 상태

AWS Backup 콘솔의 작업 페이지에서 복원 작업의 상태를 볼 수 있습니다. 복원 작업 상태에는 대기 중, 실행 중, 완료됨, 중단됨, 실패가 있습니다.

주제

S3 데이터 복원

사용하여 백업한 S3 데이터를 S3 Standard 스토리지 클래스로 AWS Backup 복원할 수 있습니다. 버킷의 모든 객체 또는 특정 객체를 복원할 수 있습니다. 객체를 기존 버킷 또는 새 버킷에 복원할 수 있습니다.

Amazon S3 복원 권한

리소스 복원을 시작하기 전에 사용 중인 역할에 충분한 권한이 있는지 확인하세요.

자세한 내용은 정책에 대한 다음 항목을 참조하십시오.

1. AWSBackupServiceRolePolicyForS3Restore
2. AWSBackupServiceRolePolicyForRestores
3. 관리형 정책 대상 AWS Backup

Amazon S3 복원 고려 사항

- AWS Backup 모든 S3 버전의 백업을 생성하지만 어느 시점에서든 버전 스택에서 최신 버전만 복원합니다.
- 대상 버킷에서 액세스 제어 목록(ACL)을 활성화해야 합니다. 그렇지 않으면 작업이 실패합니다. ACL을 활성화하려면 ACL 구성 페이지의 지침을 따르세요.
- 소스 버킷에 이름 또는 버전 ID가 같은 객체가 있는 경우 해당 객체의 복원은 건너뜁니다.
- 특정 객체를 복원하는 경우 객체의 현재 버전을 복원할 수 있습니다.
- 원본 S3 버킷으로 복원할 때
  - AWS Backup 파괴적 복원을 수행하지 않습니다. 즉 AWS Backup , 버전에 관계없이 이미 존재하는 객체 대신 버킷에 객체를 넣지 않습니다.
  - 현재 버전의 삭제 마커는 존재하지 않는 객체로 취급되므로 복원이 발생할 수 있습니다.
  - AWS Backup 복원 중에 버킷에서 삭제 마커가 없는 객체를 삭제하지 않습니다 (예: 백업 중에는 없었던 현재 버킷에 있는 키는 그대로 유지됨).
- 리전 간 복사본 복원
  - S3 백업은 리전 간에 복사할 수 있지만 복원 작업은 원본 백업 또는 복사본이 있는 동일한 리전에서만 이루어집니다.

    Example

    예: 미국 동부 (버지니아 북부) 지역에서 생성된 S3 버킷을 캐나다 (중부) 지역으로 복사할 수 있습니다. 미국 동부(버지니아 북부) 리전에 있는 원본 버킷을 사용하여 복원 작업을 시작하고 해당 리전으로 복원하거나, 캐나다(중부) 리전에 있는 복사본을 사용하여 복원 작업을 시작하고 해당 리전으로 복원할 수 있습니다.
  - 원래 암호화 방법으로는 다른 지역에서 복사한 복구 지점 (백업) 을 복원할 수 없습니다. Amazon S3 리소스에는 지역 간 복사 AWS KMS 암호화를 사용할 수 없습니다. 대신 복원 작업에 다른 암호화 유형을 사용하십시오.

AWS Backup 콘솔을 사용하여 Amazon S3 복구 지점을 복원하십시오.

AWS Backup 콘솔을 사용하여 Amazon S3 데이터를 복원하려면:

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon S3 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택한 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면

   a. 백업 창에서 리소스의 복구 시점 ID를 선택합니다.

   b. 창의 오른쪽 위에서 복원을 선택합니다.

   (또는 백업 볼트로 이동하여 복구 시점을 찾은 다음 작업, 복원을 차례로 클릭해도 됩니다.)
4. 연속 백업을 복원하는 경우 복원 시간 창에서 다음 옵션 중 하나를 선택합니다.

   a. 기본값을 수락하여 복원 가능한 최근 시간으로 복원합니다.

   b. 복원할 날짜 및 시간을 지정합니다.
5. 설정 창에서 전체 버킷 복원 또는 항목 수준 복원을 지정합니다.

   a. 항목 수준 복원을 선택하면 해당 객체를 고유하게 식별하는 각 항목의 S3 URI를 지정하여 복원 작업당 최대 5개의 항목 (버킷의 객체 또는 폴더) 을 복원할 수 있습니다.

   (S3 버킷 URI에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 액세스 방법을 참조하세요.)

   b. 복원할 다른 항목을 지정하려면 항목 추가를 선택합니다.
6. 복원 대상을 선택합니다. 소스 버킷에 복원, 기존 버킷 사용 또는 새 버킷 생성을 선택할 수 있습니다.

> **Note**
>
> 복원 대상 버킷에 버전 관리가 켜져 있어야 합니다. AWS Backup 선택한 버킷이 이 요구 사항을 충족하지 않는 경우 알려줍니다.

   a. 기존 버킷 사용을 선택한 경우 현재 지역 내의 모든 기존 버킷을 보여주는 드롭다운 메뉴에서 대상 S3 버킷을 선택합니다. AWS

b. 새 버킷 생성을 선택한 경우 새 버킷 이름을 입력합니다. 새 버킷은 기본적으로 S3 버전 관리가 활성화됩니다. 퍼블릭 액세스 차단(BPA) 설정은 기본적으로 비활성화됩니다. S3에 버킷을 생성한 후 이러한 설정을 수정할 수 있습니다.

7. S3 버킷의 객체를 암호화하려면 복원된 객체 암호화를 선택할 수 있습니다. 원본 암호화 키(기본값), Amazon S3 키(SSE-S3) 또는 AWS Key Management Service 키(SSE-KMS)를 사용합니다.

   이러한 설정은 S3 버킷의 객체 암호화에만 적용됩니다. 이는 버킷 자체의 암호화에는 영향을 주지 않습니다.

   a. 원본 암호화 키 사용 (기본값) 은 원본 객체에서 사용한 것과 동일한 암호화 키로 객체를 복원합니다. 원본 객체가 암호화되지 않은 경우 이 메서드는 암호화 없이 객체를 복원합니다.

      이 복원 옵션을 사용하면 원래 키를 사용할 수 없는 경우 복원 객체를 암호화할 대체 암호화 키를 선택적으로 선택할 수 있습니다.

   b. Amazon S3 키(SSE-S3)를 선택하면 다른 옵션을 지정할 필요가 없습니다.

   c. AWS Key Management Service 키 (SSE-KMS) 를 선택하는 경우AWS 관리형 키 (aws/s3), 키에서 선택 또는 AWS KMS 키 ARN 입력을 선택할 수 있습니다. AWS KMS

      i. AWS 관리형 키 (aws/s3)를 선택하면 다른 옵션을 지정할 필요가 없습니다.

      ii. 키에서 키를 선택하는 경우 드롭다운 메뉴에서 AWS KMS 키를 선택합니다. AWS KMS 또는 키 생성을 선택합니다.

      iii. AWS KMS 키 ARN을 입력하는 경우 텍스트 상자에 ARN을 입력합니다. 또는 키 생성을 선택합니다.

8. 복원 역할 창에서 AWS Backup 에서 이 복원 수행을 위임할 IAM 역할을 선택합니다.

9. 백업 복원을 선택합니다. 복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon S3 복구 지점을 복원하십시오.

StartRestoreJob를 사용합니다. Amazon S3를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
```

```
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

복구 시점 상태

복구 시점은 해당 상태를 나타내는 상태가 있습니다.

PARTIAL상태는 백업 창이 닫히기 전에 복구 지점을 생성할 AWS Backup 수 없음을 나타냅니다. API를 사용하여 백업 계획 기간을 늘리려면 을 참조하십시오 UpdateBackupPlan. 콘솔을 사용하여 백업 계획을 선택하고 편집하여 백업 계획 기간을 늘릴 수도 있습니다.

EXPIRED상태는 복구 지점이 보존 기간을 초과했지만 권한이 AWS Backup 없거나 삭제할 수 없는 상태임을 나타냅니다. 이러한 복구 시점을 수동으로 삭제하려면 시작하기의 리소스 정리 섹션에서 3단계: 복구 시점 삭제를 참조하세요.

STOPPED 상태는 연속 백업에서 사용자가 연속 백업을 비활성화하는 작업을 수행한 경우에 발생합니다. 이는 권한 제거, 버전 관리 해제, Amazon으로 전송되는 이벤트 비활성화 또는 EventBridge Amazon에서 설정한 EventBridge 규칙 비활성화 등으로 인해 발생할 수 있습니다. AWS Backup

STOPPED 상태를 해결하려면 요청된 모든 권한이 부여되고 S3 버킷에서 버전 관리가 활성화되어 있는지 확인합니다. 이러한 조건이 충족되면 백업 규칙의 다음 인스턴스를 실행하면 새로운 연속 복구 시점이 생성될 것입니다. 중지됨 상태인 복구 시점은 삭제할 필요가 없습니다.

다음을 사용하여 가상 시스템을 복원합니다. AWS Backup

가상 머신을 VMware, VMware 클라우드 온, VMware 클라우드 온 AWS, Amazon EBS 볼륨 또는 Amazon EC2 AWS Outposts 인스턴스로 복원할 수 있습니다. 가상 머신을 EC2로 복원(또는 마이그레이션)하려면 라이선스가 필요합니다. 기본적으로 AWS 라이선스가 포함됩니다 (요금 적용). 자세한 내용은 VM 가져오기/내보내기 사용 설명서의 라이선스 옵션을 참조하십시오.

AWS Backup 콘솔을 사용하거나 를 통해 VMware 가상 시스템을 복원할 수 있습니다. AWS CLI가상 시스템을 복원할 때 VMware Tools 폴더는 포함되지 않습니다. VMware Tools를 다시 설치하려면 VMware 설명서를 참조하십시오.

AWS Backup 가상 시스템 복원은 비파괴적이므로 복원 중에 기존 가상 시스템을 덮어쓰지 AWS Backup 않습니다. 대신 복원 작업에서는 새 가상 시스템을 배포합니다.

Tasks

- VM을 Amazon EC2 인스턴스로 복원할 때의 고려 사항
- AWS Backup 콘솔을 사용하여 가상 머신 복구 지점을 복원할 수 있습니다.
- 가상 머신 복구 지점을 복원하는 AWS CLI 데 사용합니다.

VM을 Amazon EC2 인스턴스로 복원할 때의 고려 사항

- 가상 머신을 EC2로 복원(또는 마이그레이션)하려면 라이선스가 필요합니다. 기본적으로 AWS 에는 라이선스가 포함되어 있습니다(요금 적용). 자세한 내용은 VM 가져오기/내보내기 사용 설명서의 라이선스 옵션을 참조하십시오.
- 각 가상 머신 디스크의 최대 한도는 5TB(테라바이트)입니다.
- 가상 머신을 인스턴스에 복원할 때는 키 페어를 지정할 수 없습니다. 시작 `authorized_keys` 중 (인스턴스 사용자 데이터를 통해) 또는 시작 후 (Amazon EC2 사용 설명서의 이 문제 해결 섹션에 설명된 대로) 키 페어를 추가할 수 있습니다.
- VM 가져오기/내보내기 사용 설명서에서 운영 체제가 Amazon EC2에서 가져오고 Amazon EC2에서 내보낼 수 있도록 지원되는지 확인하십시오.
- VM 가져오기/내보내기 사용 설명서에서 Amazon EC2로 VM 가져오기와 관련된 제한 사항을 검토하십시오.
- 를 사용하여 AWS CLI Amazon EC2 인스턴스로 복원할 때는 다음을 지정해야 합니다. `"RestoreTo":"EC2Instance"` 다른 모든 속성에는 기본값이 있습니다.

AWS Backup 콘솔을 사용하여 가상 머신 복구 지점을 복원할 수 있습니다.

AWS Backup 콘솔의 왼쪽 탐색 창에서 여러 위치에서 가상 컴퓨터를 복원할 수 있습니다.

- AWS Backup에 연결된 하이퍼바이저로 관리되는 가상 머신의 복구 시점을 보려면 하이퍼바이저를 선택합니다.
- AWS Backup에 연결된 모든 하이퍼바이저에서 가상 머신의 복구 시점을 보려면 가상 머신을 선택합니다.
- 특정 저장소에 저장된 복구 지점을 보려면 Backup AWS Backup Vaults를 선택합니다.
- 보호된 리소스를 선택하면 모든 보호 대상 리소스의 복구 지점을 볼 수 있습니다 AWS Backup .

더 이상 Backup 게이트웨이와 연결되지 않은 가상 머신을 복원해야 하는 경우 백업 볼트 또는 보호된 리소스를 선택하여 복구 시점을 찾습니다.

옵션

- VMware로 복원
- Amazon EBS 볼륨으로 복원
- Amazon EC2 인스턴스로 복원

가상 머신을 VMware, VMware 클라우드 온 및 VMware 클라우드 온으로 AWS복원하려면 AWS Outposts

1. 하이퍼바이저 또는 가상 머신 보기에서 복원할 VM 이름을 선택합니다. 보호된 리소스 보기에서 복원할 가상 머신 리소스 ID를 선택합니다.
2. 복원할 복구 시점 ID 옆의 라디오 버튼을 선택합니다.
3. 복원을 선택합니다.
4. 복원 유형을 선택합니다.

    a. 전체 복원은 모든 가상 머신의 디스크를 복원합니다.

    b. 디스크 수준 복원은 사용자가 선택한 하나 이상의 디스크를 복원합니다. 드롭다운 메뉴를 사용하여 복원할 디스크를 선택합니다.
5. 복원 위치를 선택합니다. 옵션은 VMware, VMware 클라우드 온 AWS, VMware 클라우드 온입니다. AWS Outposts
6. 전체 복원을 수행하는 경우에는 다음 단계로 건너뜁니다. 디스크 수준 복원을 수행하는 경우 VM 디스크 아래에 드롭다운 메뉴가 나타납니다. 복원할 부팅 가능 볼륨을 하나 이상 선택합니다.
7. 드롭다운 메뉴에서 하이퍼바이저를 선택하여 복원된 가상 머신을 관리합니다.
8. 복원된 가상 머신에 대해 조직의 가상 머신 모범 사례를 사용하여 다음을 지정합니다.

    a. 이름

    b. 경로(예: `/datacenter/vm`)

    c. 컴퓨팅 리소스 이름(예: VMHost 또는 클러스터)

    호스트가 클러스터의 일부인 경우 호스트로는 복원할 수 없고 지정된 클러스터로만 복원할 수 있습니다.

    d. 데이터 스토어

9. 복원 역할에서 드롭다운 메뉴를 사용하여 기본 역할(권장) 또는 IAM 역할 선택을 선택합니다.
10. 백업 복원을 선택합니다.
11. 선택 사항: 언제 복원 작업의 상태가 `Completed`인지 확인합니다. 왼쪽 탐색 창에서 작업을 선택합니다.

가상 머신을 Amazon EBS 볼륨으로 복원하려면

1. 하이퍼바이저 또는 가상 머신 보기에서 복원할 VM 이름을 선택합니다. 보호된 리소스 보기에서 복원할 가상 머신 리소스 ID를 선택합니다.
2. 복원할 복구 시점 ID 옆의 라디오 버튼을 선택합니다.
3. 복원을 선택합니다.
4. 복원 유형을 선택합니다.
    - 디스크 복원은 사용자가 선택한 디스크 1개를 복원합니다. 드롭다운 메뉴를 사용하여 복원할 디스크를 선택합니다.
5. 복원 위치를 Amazon EBS로 선택합니다.
6. VM 디스크 드롭다운 메뉴에서 복원할 부팅 가능 볼륨을 선택합니다.
7. EBS 볼륨 유형에서 볼륨 유형을 선택합니다.
8. 가용 영역을 선택합니다.
9. 암호화(선택 사항). EBS 볼륨을 암호화하도록 선택한 경우 확인란을 선택합니다.
10. 메뉴에서 KMS 키를 선택합니다.
11. 복원 역할의 경우 기본 역할 (권장) 또는 IAM 역할 선택을 선택합니다.
12. 백업 복원을 선택합니다.
13. 선택 사항: 언제 복원 작업의 상태가 `Completed`인지 확인합니다. 왼쪽 탐색 창에서 작업을 선택합니다.
14. 선택 사항: 전체 Amazon EBS 볼륨에 LVM 논리 볼륨을 생성하려면 어떻게 합니까?를 참조하여 관리형 볼륨을 탑재하고 복원된 Amazon EBS 볼륨의 데이터에 액세스하는 방법에 대해 자세히 알아보세요.

Amazon EC2 인스턴스로 가상 머신을 복원하려면

1. 하이퍼바이저 또는 가상 머신 보기에서 복원할 VM 이름을 선택합니다. 보호된 리소스 보기에서 복원할 가상 머신 리소스 ID를 선택합니다.
2. 복원할 복구 시점 ID 옆의 라디오 버튼을 선택합니다.
3. 복원을 선택합니다.
4. 복원 유형을 선택합니다.

   - 전체 복원은 루트 수준 폴더 및 파일을 포함하여 파일 시스템을 완전히 복원합니다.
5. 복원 위치를 Amazon EC2로 선택합니다.
6. 인스턴스 유형에서는 새 인스턴스에서 애플리케이션을 실행하는 데 필요한 컴퓨팅과 메모리의 조합을 선택합니다.

   > **Tip**
   >
   > 원래 가상 머신의 사양과 일치하거나 초과하는 인스턴스 유형을 선택하십시오. 자세한 내용은 Amazon EC2 인스턴스 유형 안내서를 참조하세요.
7. VPC (가상 사설 클라우드) 의 경우 인스턴스의 네트워킹 환경을 정의하는 가상 사설 클라우드 (VPC) 를 선택합니다.
8. Subnet의 경우 VPC의 서브넷 중 하나를 선택합니다. 인스턴스는 서브넷 주소 범위의 프라이빗 IP 주소를 받습니다.
9. 보안 그룹의 경우 인스턴스로 향하는 트래픽의 방화벽 역할을 하는 보안 그룹을 선택하십시오.
10. 복원 역할에서 기본 역할 (권장) 또는 IAM 역할 선택을 선택합니다.
11. 선택 사항: 시작 시 인스턴스에서 스크립트를 실행하려면 고급 설정을 확장하고 사용자 데이터에 스크립트를 입력합니다.
12. 백업 복원을 선택합니다.
13. 선택 사항: 언제 복원 작업의 상태가 `Completed`인지 확인합니다. 왼쪽 탐색 창에서 작업을 선택합니다.

가상 머신 복구 지점을 복원하는 AWS CLI 데 사용합니다.

`StartRestoreJob`를 사용합니다.

Amazon EC2 및 Amazon EBS로의 가상 머신 복원에 대해 다음과 같은 메타데이터를 지정할 수 있습니다.

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Outpost에서 VMware, VMware 클라우드 온 AWS및 VMware 클라우드 기반 가상 머신을 복원하기 위해 다음과 같은 메타데이터를 지정할 수 있습니다. AWS

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

이 예제는 VMware에 대한 전체 복원을 수행하는 방법을 보여줍니다.

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

FSX 파일 시스템 복원

Amazon FSx 파일 시스템을 복원하는 AWS Backup 데 사용할 때 사용할 수 있는 복원 옵션은 기본 Amazon FSx 백업을 사용하는 것과 동일합니다. 백업의 복구 지점을 사용하여 새 파일 시스템을 생성하고 다른 파일 시스템의 point-in-time 스냅샷을 복원할 수 있습니다.

Amazon FSx 파일 시스템을 복원할 때 새 파일 시스템을 AWS Backup 생성하고 데이터로 채웁니다(Amazon FSx NetApp for ONTAP에서는 볼륨을 기존 파일 시스템으로 복원할 수 있음). 이는 네이티브 Amazon FSx가 파일 시스템을 백업 및 복원하는 방식과 유사합니다. 백업을 새 파일 시스템으로 복원하는 데는 새 파일 시스템을 생성하는 것과 동일한 시간이 걸립니다. 백업에서 복원된 데이터는 파일 시스템에 지연 로드됩니다. 따라서 프로세스 중에 지연 시간이 약간 더 길어질 수 있습니다.

> **Note**
>
> 기존 Amazon FSx 파일 시스템으로 복원할 수 없으며 개별 파일 또는 폴더를 복원할 수 없습니다.
>
> FSx for ONTAP는 DP(데이터 보호) 볼륨, LS(로드 공유) 볼륨, 전체 볼륨 또는 꽉 찬 파일 시스템의 볼륨을 비롯한 특정 볼륨 유형의 백업을 지원하지 않습니다. 자세한 내용은 FSx for ONTAP 백업 작업을 참조하세요.
>
> AWS Backup Amazon FSx 파일 시스템의 복구 지점이 들어 있는 보관소는 외부에서 볼 수 있습니다. AWS Backup Amazon FSx를 사용하여 복구 시점을 복원할 수 있지만 삭제할 수는 없습니다.

내장된 Amazon FSx 자동 백업 기능으로 생성된 백업을 콘솔에서 확인할 수 있습니다. AWS Backup 를 사용하여 이러한 백업을 복구할 수도 있습니다. AWS Backup하지만 를 사용하여 이러한 백업을 삭제하거나 Amazon FSx 파일 시스템의 자동 백업 일정을 변경할 수는 없습니다. AWS Backup

AWS Backup 콘솔, API 또는 AWS Backup 를 사용하여 생성한 백업을 복원할 수 있습니다. AWS CLI 이 섹션에서는 AWS Backup 콘솔을 사용하여 Amazon FSx 파일 시스템을 복원하는 방법을 보여줍니다.

AWS Backup 콘솔을 사용하여 Amazon FSx 복구 지점을 복원하십시오.

FSx for Windows File Server 파일 시스템 복원

FSx for Windows File Server 파일 시스템을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon FSx 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스의 복구 시점 ID를 선택합니다.
4. 창의 오른쪽 위에서 복원을 선택하여 백업 복원 페이지를 엽니다.
5. 파일 시스템 세부 정보 섹션에서 백업 ID가 백업 ID 아래에 표시되고 파일 시스템 유형이 파일 시스템 유형 아래에 표시됩니다. FSx for Windows File Server 파일 시스템과 FSx for Lustre 파일 시스템 모두 복원할 수 있습니다.
6. 배포 유형에서 기본값을 수락합니다. 복원 도중에는 파일 시스템의 배포 유형을 변경할 수 없습니다.
7. 사용할 스토리지 유형을 선택합니다. 파일 시스템의 스토리지 용량이 2,000GiB 미만인 경우 HDD 스토리지 유형을 사용할 수 없습니다.
8. 처리량 용량에서 권장 처리량 용량을 선택하여 권장 16MBps(초당 메가바이트) 속도를 사용하거나 처리량 용량 지정을 선택하고 새 속도를 입력합니다.
9. 네트워크 및 보안 섹션에서 필수 정보를 제공합니다.
10. FSx for Windows File Server 파일 시스템을 복원하는 경우 파일 시스템에 액세스하는 데 사용되는 Windows 인증 정보를 제공하거나 새 인증 정보를 생성할 수 있습니다.

    > **Note**
    >
    > 백업을 복원할 때는 파일 시스템의 Active Directory 유형을 변경할 수 없습니다.

    Microsoft Active Directory에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서의 Amazon FSx for Windows File Server에서 Active Directory로 작업하기를 참조하세요.
11. (선택 사항) 백업 및 유지 관리 섹션에서 백업 기본 설정을 위한 정보를 제공합니다.
12. 복원 역할 섹션에서 AWS Backup 이 사용자 대신 백업을 생성 및 관리하는 데 사용할 IAM 역할을 선택합니다. 기본 역할을 선택하는 것이 좋습니다. 기본 역할이 없는 경우 올바른 권한을 가진 역할이 생성됩니다. 자체 IAM 역할을 제공할 수도 있습니다.
13. 모든 항목을 확인하고 백업 복원을 선택합니다.

Amazon FSx for Lustre 파일 시스템 복원

AWS Backup 영구 스토리지 배포 유형이 있고 Amazon S3와 같은 데이터 리포지토리에 연결되지 않은 Amazon FSx for Lustre 파일 시스템을 지원합니다.

Amazon FSx for Lustre 파일 시스템을 복원하려면

1. https://console.aws.amazon.com/backup 에서 콘솔을 엽니다. AWS Backup
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon FSx 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스의 복구 시점 ID를 선택합니다.
4. 창의 오른쪽 위에서 복원을 선택하여 백업을 새 파일 시스템으로 복원 페이지를 엽니다.
5. 설정 섹션에서 백업 ID가 백업 ID 아래에 표시되고 파일 시스템 유형이 파일 시스템 유형 아래에 표시됩니다. 파일 시스템 유형은 Lustre여야 합니다.
6. (선택 사항) 파일 시스템의 이름을 입력합니다.
7. 배포 유형을 선택합니다. AWS Backup 영구 배포 유형만 지원합니다. 복원 도중에는 파일 시스템의 배포 유형을 변경할 수 없습니다.

   영구 배포 유형은 장기 스토리지용입니다. FSx for Lustre 배포 옵션에 대한 자세한 내용은 Amazon FSx for Lustre 사용 설명서의 Amazon FSx for Lustre 파일 시스템에서 사용 가능한 배포 옵션 사용을 참조하세요.
8. 사용하려는 스토리지 단위당 처리량을 선택합니다.
9. 사용할 스토리지 용량을 지정합니다. 32GiB~64,436GiB 사이의 용량을 입력합니다.
10. 네트워크 및 보안 섹션에서 필수 정보를 제공합니다.
11. (선택 사항) 백업 및 유지 관리 섹션에서 백업 기본 설정을 위한 정보를 제공합니다.
12. 복원 역할 섹션에서 AWS Backup 이 사용자 대신 백업을 생성 및 관리하는 데 사용할 IAM 역할을 선택합니다. 기본 역할을 선택하는 것이 좋습니다. 기본 역할이 없는 경우 올바른 권한을 가진 역할이 생성됩니다. IAM 역할도 제공할 수 있습니다.
13. 모든 항목을 확인하고 백업 복원을 선택합니다.

ONTAP 볼륨용 Amazon NetApp FSx 복원

ONTAP 볼륨용 Amazon FSx를 NetApp 복원하려면:

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon FSx 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스의 복구 시점 ID를 선택합니다.
4. 창의 오른쪽 위에서 복원을 선택하여 복원 페이지를 엽니다.

첫 번째 섹션인 파일 시스템 세부 정보에는 복구 시점 ID, 파일 시스템 ID 및 파일 시스템 유형이 표시됩니다.

5. 복원 옵션에는 몇 가지 선택 항목이 있습니다. 먼저 드롭다운 메뉴에서 파일 시스템을 선택합니다.
6. 그런 다음 드롭다운 메뉴에서 원하는 스토리지 가상 머신을 선택합니다.
7. 볼륨의 이름을 입력합니다.
8. 파일 시스템 내에서 볼륨이 탑재될 위치인 정션 경로를 지정합니다.
9. 생성 중인 볼륨 크기를 메가바이트(MB) 단위로 지정합니다.
10. (선택 사항) 확인란을 선택하여 스토리지 효율성을 활성화하도록 선택할 수 있습니다. 이렇게 하면 중복 제거, 압축 및 컴팩션이 가능합니다.
11. 용량 풀 계층화 정책 드롭다운 메뉴에서 계층화 기본 설정을 선택합니다.
12. 복원 권한에서 백업을 복원하는 AWS Backup 데 사용할 IAM 역할을 선택합니다.
13. 모든 항목을 확인하고 백업 복원을 선택합니다.

Amazon FSx for OpenZFS 파일 시스템 복원

Amazon FSx for OpenZFS 파일 시스템을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon FSx 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스의 복구 시점 ID를 선택합니다.
4. 창의 오른쪽 위에서 복원을 선택하여 백업 복원 페이지를 엽니다.

   파일 시스템 세부 정보 섹션에서 백업 ID가 백업 ID 아래에 표시되고 파일 시스템 유형이 파일 시스템 유형 아래에 표시됩니다. 파일 시스템 유형은 FSx for OpenZFS여야 합니다.
5. 복원 옵션에서 빠른 복원 또는 표준 복원을 선택할 수 있습니다. 빠른 복원에는 소스 파일 시스템의 기본 설정이 사용됩니다. 빠른 복원을 수행하는 경우에는 7단계로 건너뜁니다.

   표준 복원을 선택한 경우 다음 구성을 추가로 지정합니다.

   a. 프로비저닝된 SSD IOPS: 자동 라디오 버튼을 선택하거나 사용 가능한 경우 사용자 프로비저닝 옵션을 선택할 수 있습니다.
   b. 처리량 용량: 64MB/초의 권장 처리량 용량을 선택하거나 처리량 용량 지정을 선택할 수 있습니다.

c. (선택 사항) VPC 보안 그룹: 파일 시스템의 네트워크 인터페이스와 연결할 VPC 보안 그룹을 지정할 수 있습니다.

d. 암호화 키: 복원된 파일 시스템 데이터를 유휴 상태로 보호할 AWS Key Management Service 키를 지정합니다.

e. (선택 사항) 루트 볼륨 구성: 이 구성은 기본적으로 축소되어 있습니다. 아래쪽을 가리키는 캐럿(화살표)을 클릭하여 확장할 수 있습니다. 백업에서 파일 시스템을 생성하면 새 파일 시스템이 생성되고 볼륨 및 스냅샷은 해당 소스 구성을 유지합니다.

f. (선택 사항) 백업 및 유지 관리: 예약 백업을 설정하려면 아래쪽을 가리키는 캐럿(화살표)을 클릭하여 섹션을 확장합니다. 백업 기간, 시간 및 분, 보존 기간, 주간 유지 관리 기간을 선택할 수 있습니다.

6. (선택 사항) 볼륨의 이름을 입력할 수 있습니다.
7. SSD 스토리지 용량에는 파일 시스템의 스토리지 용량이 표시됩니다.
8. 파일 시스템에 액세스할 수 있는 Virtual Private Cloud(VPC)를 선택합니다.
9. 서브넷 드롭다운 메뉴에서 파일 시스템의 네트워크 인터페이스가 있는 서브넷을 선택합니다.
10. 복원 역할 섹션에서 사용자 대신 백업을 생성하고 관리하는 AWS Backup 데 사용할 IAM 역할을 선택합니다. 기본 역할을 선택하는 것이 좋습니다. 기본 역할이 없는 경우 올바른 권한을 가진 역할이 생성됩니다. IAM 역할을 선택할 수도 있습니다.
11. 모든 항목을 확인하고 백업 복원을 선택합니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon FSx 복구 지점을 복원하십시오.

API 또는 CLI를 사용하여 Amazon FSx를 복원하려면 `StartRestoreJob`을 사용합니다. Amazon FSx를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
```

```
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

FSx for Windows File Server 복원 메타데이터

FSx for Windows File Server를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx for Lustre 복원 메타데이터

FSx for Lustre를 복원할 때 다음 `PerUnitStorageThroughput` 및 `DriveCacheType`을 지정할 수 있습니다.

FSx for ONTAP 복원 메타데이터

FSx for ONTAP를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

- 생성할 볼륨의 이름 #name
- OntapConfiguration: # 온탭 구성
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx for OpenZFS 복원 메타데이터

FSX for OpenZFS를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

- `ThroughputCapacity`
- `DesklopsConfiguration`
- IOPS를 지정하는 경우 0~160,000 사이의 값을 포함해야 하지만 모드는 포함하지 않아야 합니다.

CLI 복원 명령 예:

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

복원 메타데이터 예:

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Amazon EBS 볼륨 복원

Amazon Elastic Block Store (Amazon EBS) 스냅샷을 AWS Backup 복원하면 Amazon EC2 인스턴스에 연결할 수 있는 새 Amazon EBS 볼륨이 생성됩니다.

스냅샷을 EBS 볼륨 또는 AWS Storage Gateway 볼륨으로 복원하도록 선택할 수 있습니다.

AWS Backup 콘솔을 사용하여 Amazon EBS 복구 지점을 복원하십시오.

Amazon EBS 볼륨을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 EBS 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 리소스에 대한 복원 파라미터를 지정합니다. 입력하는 복원 파라미터는 선택한 리소스 유형에 따라 다릅니다.

   리소스 유형에서는 이 백업을 복원할 때 생성할 AWS 리소스를 선택합니다.
5. EBS 볼륨을 선택한 경우 볼륨 유형 및 크기(GiB)에 대한 값을 입력하고 가용 영역을 선택합니다.

- 처리량 다음에는 이 볼륨 암호화 확인란(선택 사항)이 나타납니다. EBS 복구 시점이 암호화된 경우 이 옵션은 활성 상태로 유지됩니다.

  KMS 키를 지정하거나 AWS KMS 키를 생성할 수 있습니다.

Storage Gateway 볼륨을 선택한 경우 연결 가능한 상태의 게이트웨이를 선택합니다. iSCSI 대상 이름도 선택합니다.

- 저장 볼륨 게이트웨이에서 디스크 ID를 선택합니다.
- 캐시 볼륨 게이트웨이에서 보호된 리소스 이상의 용량을 선택합니다.

6. 복원 역할에서 이 복원을 맡을 IAM 역할을 선택합니다. AWS Backup

> **Note**
>
> 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 기본 역할이 자동으로 생성됩니다. 이 기본 역할을 삭제하거나 사용할 수 없게 만들 수 있습니다.

7. 백업 복원을 선택합니다.

   복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

아카이브된 EBS 스냅샷을 복원하면 새 EBS 볼륨을 생성하기 위해 스냅샷이 일시적으로 콜드 스토리지에서 웜 스토리지로 이동합니다. 이러한 유형의 복원에는 일회성 검색 비용이 발생합니다. 이 복원 기간 동안에는 웜 스토리지와 콜드 스토리지의 스토리지 비용이 모두 청구됩니다. 콜드 스토리지의 EBS 볼륨은 Backup 게이트웨이 볼륨으로 복원할 수 없습니다.

AWS Backup 콘솔이나 명령줄을 사용하여 콜드 스토리지에 아카이브된 EBS 스냅샷을 복원할 수 있습니다. 콜드 스토리지에서 복원하려면 최대 72시간이 소요될 수 있습니다. 자세한 내용은 Amazon EBS 사용 설명서의 Archive Amazon EBS snapshots를 참조하세요.

Console

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 볼트 > **##** > 아카이브된 EBS 스냅샷 복원으로 이동합니다.
3. 설정 섹션에서 아카이브된 스냅샷을 임시로 복원할 일수를 지정하는 값을 0에서 180까지 입력합니다.

4. 볼륨 유형, 크기, IOPS, 가용 영역, 처리량 및 암호화와 같은 기타 설정을 입력합니다.
5. 역할 복원을 선택합니다.
6. 백업 복원을 선택합니다. 확인 팝업에서 스냅샷과 복원 유형을 확인합니다. 그런 다음 스냅샷 복원을 선택합니다.

AWS CLI

1. start-restore-job 사용
2. 파라미터를 포함합니다.
3.
4.
5.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon EBS 복구 지점을 복원하십시오.

API 또는 CLI를 사용하여 Amazon EBS를 복원하려면 StartRestoreJob을 사용합니다. Amazon EBS를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
availabilityZone
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

예제

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Amazon EFS 파일 시스템 복원

Amazon Elastic File System(Amazon EFS) 인스턴스를 복원하는 경우 전체 복원 또는 항목 수준 복원을 수행할 수 있습니다.

전체 복원

전체 복원을 수행하면 전체 파일 시스템이 복원됩니다.

AWS Backup Amazon EFS를 사용한 파괴적 복원은 지원하지 않습니다. 파괴적 복원이란 복원된 파일 시스템이 소스 또는 기존 파일 시스템을 삭제하거나 덮어쓰는 것을 말합니다. 대신 AWS Backup 은 파일 시스템을 루트 디렉터리의 복구 디렉터리에 복원합니다.

항목 수준 복원

항목 수준 복원을 수행하면 특정 파일 또는 디렉터리를 복원합니다. AWS Backup 파일 시스템 루트를 기준으로 경로를 지정해야 합니다. 예를 들어, 파일 시스템이 `/user/home/myname/efs`에 탑재되고 파일 경로가 `user/home/myname/efs/file1`인 경우 **`/file1`**을 입력합니다. 경로는 대/소문자를 구분합니다. 와일드카드 문자 및 정규식 문자열은 지원되지 않습니다. 액세스 포인트를 사용하여 파일 시스템을 마운트한 경우 경로가 호스트의 경로와 다를 수 있습니다.

콘솔을 사용하여 EFS 복원을 수행할 때 최대 10개의 항목을 선택할 수 있습니다. CLI를 사용하여 복원하는 경우 항목 제한은 없지만, 전달할 수 있는 복원 메타데이터 길이에는 200KB 제한이 있습니다.

이러한 항목을 새 파일 시스템 또는 기존 파일 시스템으로 복원할 수 있습니다. 어느 쪽이든 AWS Backup 은 루트 디렉터리에서 항목을 포함할 새 Amazon EFS 디렉터리(`aws-backup-restore_`*`datetime`*)를 생성합니다. 지정된 항목의 전체 계층 구조는 복구 디렉터리에 보존됩니다. 예를 들어, 디렉터리 A에 하위 디렉터리 B, C 및 D가 포함되어 있는 경우 AWS Backup 은 A, B, C 및 D가 복구될 때 계층 구조를 유지합니다. 기존 파일 시스템이나 새 파일 시스템으로 Amazon EFS 항목 수준 복원을 수행하는지 여부에 관계없이 각 복원 시도는 루트 디렉터리 외부에 복원된 파일을 포함할 새 복구 디렉터리를 생성합니다. 동일한 경로에 대해 복원을 여러 번 시도하면 복원된 항목이 포함된 여러 디렉터리가 존재할 수 있습니다.

> **Note**
>
> 매주 백업을 하나만 보관하는 경우 해당 백업을 수행한 시점의 파일 시스템 상태로만 복원할 수 있습니다. 이전 증분 백업으로 복원할 수는 없습니다.

AWS Backup 콘솔을 사용하여 Amazon EFS 복구 지점을 복원하십시오.

Amazon EFS 파일 시스템을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. EFS 백업 볼트는 생성 시 액세스 정책 Deny `backup:StartRestoreJob`을 부여받습니다. 백업 볼트를 처음으로 복원하는 경우 액세스 정책을 다음과 같이 변경해야 합니다.

   a. 백업 볼트를 선택합니다.

   b. 복원하려는 복구 시점이 들어 있는 백업 볼트를 선택합니다.

   c. 아래로 스크롤하여 볼트 액세스 정책을 찾습니다.

   d. 있는 경우 `Statement`에서 `backup:StartRestoreJob`을 삭제합니다. 편집을 선택하고 `backup:StartRestoreJob`을 삭제한 다음 정책 저장을 선택하면 됩니다.
3. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 EFS 파일 시스템 ID를 선택합니다.
4. 리소스 세부 정보 페이지에는 선택된 파일 시스템 ID의 복구 시점 목록이 표시됩니다. 파일 시스템을 복원하려면 백업 창에서 파일 시스템의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
5. 파일 시스템에 대한 복원 파라미터를 지정합니다. 입력하는 복원 파라미터는 선택한 리소스 유형에 따라 다릅니다.

   전체 파일 시스템을 복원하는 전체 복원을 수행할 수 있습니다. 또는 항목 수준 복원을 사용하여 특정 파일 및 디렉터리를 복원할 수 있습니다.

   - 모든 루트 수준 폴더 및 파일을 포함하여 파일 시스템 전체를 복원하려면 전체 복원 옵션을 선택합니다.
   - 특정 파일 또는 디렉터리를 복원하려면 항목 수준 복원 옵션을 선택합니다. Amazon EFS 내에서 최대 5개의 항목을 선택하고 복원할 수 있습니다.

     특정 파일 또는 디렉터리를 복원하려면 탑재 지점에 대한 상대 경로를 지정해야 합니다. 예를 들어, 파일 시스템이 `/user/home/myname/efs`에 탑재되고 파일 경로가 `user/home/myname/efs/file1`인 경우 **`/file1`**을 입력합니다. 경로는 대소문자를 구분하며 특수 문자, 와일드카드 문자 및 정규식 문자열을 포함할 수 없습니다.

     1. 항목 경로 텍스트 상자에 파일 또는 폴더의 경로를 입력합니다.
     2. 추가 파일 또는 디렉터리를 추가하려면 항목 추가를 선택합니다. EFS 파일 시스템 내에서 최대 5개의 항목을 선택하고 복원할 수 있습니다.
6. 복원 위치의 경우

- 소스 파일 시스템에 복원하려면 소스 파일 시스템의 디렉터리에 복원을 선택합니다.
- 다른 파일 시스템에 복원하려면 새 파일 시스템에 복원을 선택합니다.

7. 파일 시스템 유형에서

   - (권장) 여러 가용 AWS 영역에 걸쳐 파일 시스템을 복원하려면 [Regional] 을 선택합니다.
   - 파일 시스템을 단일 가용 영역에 복원하려면 One Zone을 선택합니다. 그런 다음 가용 영역 드롭다운에서 복원 대상을 선택합니다.

   자세한 내용은 Amazon EFS 사용 설명서의 Amazon EFS 스토리지 클래스 관리를 참조하세요.

8. 성능에서

   - 리전 복원을 수행하기로 선택한 경우 (권장) 범용 또는 최대 I/O를 선택합니다.
   - One Zone 복원을 수행하기로 선택한 경우 (권장) 범용을 선택해야 합니다. One Zone 복원은 최대 I/O를 지원하지 않습니다.

9. 암호화 활성화에서

   - 파일 시스템을 암호화하려면 암호화 활성화를 선택합니다. KMS 키 ID와 별칭은 AWS Key Management Service (AWS KMS) 콘솔을 사용하여 만든 후 목록에 나타납니다.
   - KMS 키 텍스트 상자의 목록에서 사용할 키를 선택합니다.

10. 복원 역할의 경우 AWS Backup 이 복원을 수행할 IAM 역할을 선택합니다.

    > **Note**
    >
    > 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 기본 역할이 자동으로 생성됩니다. 이 기본 역할을 삭제하거나 사용할 수 없게 만들 수 있습니다.

11. 백업 복원을 선택합니다.

    복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

    > **Note**
    >
    > 매주 백업을 하나만 보관하는 경우 해당 백업을 수행한 시점의 파일 시스템 상태로만 복원할 수 있습니다. 이전 증분 백업으로 복원할 수는 없습니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon EFS 복구 지점을 복원하십시오.

StartRestoreJob를 사용합니다. Amazon EFS 인스턴스를 복원할 때 전체 파일 시스템을 복원하거나 특정 파일 또는 디렉터리를 복원할 수 있습니다. Amazon EFS 리소스를 복원하려면 다음 정보가 필요합니다.

- `file-system-id`— 백업된 Amazon EFS 파일 시스템의 ID입니다 AWS Backup. `GetRecoveryPointRestoreMetadata`로 반환됩니다. 새 파일 시스템을 복원할 때는 필요하지 않습니다. 파라미터가 `newFileSystem` 다음과 같은 경우 이 값은 `True` 무시됩니다.
- `Encrypted` - True인 경우 파일 시스템이 암호화되었음을 나타내는 부울 값입니다. `KmsKeyId`를 지정하면 `Encrypted`는 `true`로 설정되어야 합니다.
- `KmsKeyId`- 복원된 파일 시스템을 암호화하는 데 사용되는 AWS KMS 키를 지정합니다.
- `PerformanceMode` - 파일 시스템의 처리량 모드를 지정합니다.
- `CreationToken` - 요청의 고유성(멱등성)을 보장하는 사용자 제공 값입니다.
- `newFileSystem` - True인 경우 복구 시점이 새 Amazon EFS 파일 시스템에 복원되었음을 나타내는 부울 값입니다.
- `ItemsToRestore` - 각 문자열이 파일 경로인 최대 5개 문자열의 배열입니다. 전체 파일 시스템이 아닌 특정 파일 또는 디렉터리를 복원하려면 `ItemsToRestore`를 사용합니다. 이 파라미터는 선택 사항입니다.

`aws:backup:request-id`를 포함할 수도 있습니다.

다음 매개 변수를 포함하여 One Zone 복원을 수행할 수 있습니다.

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Amazon EFS 구성 값에 대한 자세한 내용은 을 참조하십시오 create-file-system.

Amazon EFS에서 자동 백업 비활성화

기본적으로 Amazon EFS는 데이터 백업을 자동으로 생성합니다. 이러한 백업은 에서 복구 지점으로 표시됩니다 AWS Backup. 복구 시점을 제거하려고 하면 작업을 수행할 권한이 충분하지 않다는 오류 메시지가 표시됩니다.

이 자동 백업을 활성 상태로 유지하는 것이 모범 사례입니다. 특히 실수로 데이터를 삭제한 경우 이 백업을 통해 파일 시스템 콘텐츠를 마지막 복구 시점이 생성된 날짜로 복원할 수 있습니다.

드문 경우이긴 하지만 이 기능을 비활성화하려는 경우에는 액세스 정책을 `"Effect": "Deny"`에서 `"Effect": "Allow"`로 변경해야 합니다. 자동 백업 활성화 또는 비활성화에 대한 자세한 내용은 Amazon EFS 사용 설명서를 참조하세요.

Amazon DynamoDB 테이블 복원

AWS Backup 콘솔을 사용하여 DynamoDB 복구 지점을 복원하십시오.

DynamoDB 테이블을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 DynamoDB 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 설정의 새 테이블 이름 텍스트 필드에 새 테이블 이름을 입력합니다.
5. 복원 역할에서 이 복원을 맡을 AWS Backup IAM 역할을 선택합니다.
6. 암호화 설정에서

   a. DynamoDB에서 백업을 관리하는 경우 (ARN은 `arn:aws:dynamodb` 로 시작) AWS Backup , 소유한 키를 사용하여 복원된 테이블을 암호화합니다. AWS

      복원된 테이블을 암호화할 다른 키를 선택하려면 작업을 사용하거나 DynamoDB AWS Backup StartRestoreJob 콘솔에서 복원을 수행할 수 있습니다.

   b. 백업이 전체 AWS Backup 관리를 지원하는 경우 (ARN은 로 시작`arn:aws:backup`) 다음 암호화 옵션 중 하나를 선택하여 복원된 테이블을 보호할 수 있습니다.

      - (기본값) DynamoDB 소유 KMS 키(암호화 추가 비용 없음)
      - DynamoDB 관리형 KMS 키(KMS 요금 적용)
      - 고객 관리형 KMS 키(KMS 요금 적용)

      'DynamoDB 소유' 및 'DynamoDB 관리형' 키는 각각 'AWS소유' 및 'AWS관리형' 키와 동일합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 유휴 시 암호화: 작동 방식을 참조하세요.

      전체 AWS Backup 관리에 대한 자세한 내용은 을 참조하십시오고급 DynamoDB 백업.

> **Note**
>
> 다음 지침은 복사된 백업을 복원하고 원래 테이블을 암호화하는 데 사용한 것과 동일한 키로 복원된 테이블을 암호화하려는 경우에만 적용됩니다.
> 교차 리전 백업을 복원할 때 원래 테이블을 암호화하는 데 사용한 것과 동일한 키를 사용하여 복원된 테이블을 암호화하려면 키가 다중 지역 키여야 합니다. AWS-소유 키와 AWS-관리 키는 다중 지역 키가 아닙니다. 자세한 내용을 알아보려면 AWS Key Management Service 개발자 안내서의 다중 리전 키를 참조하세요.
> 계정 간 백업을 복원할 때 원래 테이블을 암호화하는 데 사용한 것과 동일한 키를 사용하여 복원된 테이블을 암호화하려면 소스 계정의 키를 대상 계정과 공유해야 합니다. AWS-소유 키와 AWS관리 키는 계정 간에 공유할 수 없습니다. 자세한 내용을 알아보려면 AWS Key Management Service 개발자 안내서의 다른 계정의 사용자가 CMK를 사용하도록 허용을 참조하세요.

7. 백업 복원을 선택합니다.

   복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

AWS Backup API, CLI 또는 SDK를 사용하여 DynamoDB 복구 지점을 복원하십시오.

`StartRestoreJob`를 사용합니다. DynamoDB를 복원할 때 다음 메타데이터를 지정할 수 있습니다. 메타데이터는 대/소문자를 구분하지 않습니다.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

다음은 CLI의 `StartRestoreJob` 작업에 대한 `restoreMetadata` 인수 예제입니다.

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
```

```
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

위 예제에서는 소유한 키를 사용하여 복원된 테이블을 암호화합니다. AWS복원 메타데이터에서 AWS-소유 키를 사용한 암호화를 지정하는 부분은 다음과 같습니다. `\"encryptionType\":\"Default\",\"kmsMasterKeyArn\":\"Not Applicable\"`

AWS-managed 키를 사용하여 복원된 테이블을 암호화하려면 다음 복원 메타데이터를 지정하십시오. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

고객 관리형 키를 사용하여 복원된 테이블을 암호화하려면 다음 복원 메타데이터를 지정합니다. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

RDS 데이터베이스 복원

Amazon RDS 데이터베이스를 복원하려면 여러 복원 옵션을 지정해야 합니다. 이러한 옵션에 대한 자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 백업 및 복원을 참조하세요.

AWS Backup 콘솔을 사용하여 Amazon RDS 복구 지점을 복원하십시오.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon RDS 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 인스턴스 사양 창에서 기본값을 수락하거나 DB 엔진, 라이선스 모델, DB 인스턴스 클래스, 다중 AZ 및 스토리지 유형 설정의 옵션을 지정합니다. 예를 들어, 스탠바디 데이터베이스 인스턴스를 원하는 경우 다중 AZ를 지정합니다.
5. 설정 창에서 현재 지역의 사용자가 소유한 모든 DB 인스턴스 및 AWS 계정 클러스터에 대해 고유한 이름을 지정합니다. DB 인스턴스 식별자는 대소문자를 구분하지 않지만 'mydbinstance'와 같이 모두 소문자로 저장됩니다. 필수 필드입니다.
6. 네트워크 및 보안 창에서 기본값을 그대로 사용하거나 VPC (Virtual Private Cloud), 서브넷 그룹, 공용 접근성 (일반적으로 예) 및 가용 영역 설정에 대한 옵션을 지정합니다.
7. 데이터베이스 옵션 창에서 기본값을 수락하거나 데이터베이스 포트, DB 파라미터 그룹, 옵션 그룹, 스냅샷으로 태그 복사 및 IAM DB 인증 활성화 설정의 옵션을 지정합니다.

8. 암호화 창에서 기본 설정을 사용합니다. 스냅샷의 소스 데이터베이스 인스턴스가 암호화된 경우 복원된 데이터베이스 인스턴스도 암호화됩니다. 이 암호화는 제거할 수 없습니다.
9. 로그 내보내기 창에서 Amazon CloudWatch Logs에 게시할 로그 유형을 선택합니다. IAM 역할이 이미 정의되어 있습니다.
10. 유지 관리 창에서 기본값을 수락하거나 자동 마이너 버전 업그레이드 옵션을 지정합니다.
11. 복원 역할 창에서 AWS Backup 에서 이 복원 수행을 위임할 IAM 역할을 선택합니다.
12. 모든 설정을 지정했으면 백업 복원을 선택합니다.

    복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon RDS 복구 지점을 복원하십시오.

`StartRestoreJob`를 사용합니다. 허용되는 메타데이터 및 값에 대한 자세한 내용은 Amazon RDS API 참조에서 `RestoreDBInstanceFromDBSnapshot` 섹션을 참조하세요. 또한 다음과 같은 정보 AWS Backup 전용 속성을 허용합니다. 하지만 이러한 항목을 포함해도 복원에는 영향을 주지 않습니다.

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Amazon Aurora 클러스터 복원

AWS Backup 콘솔을 사용하여 Aurora 복구 지점 복원

AWS Backup Aurora 클러스터를 복원합니다. Amazon RDS 인스턴스를 생성하거나 클러스터에 연결하지는 않습니다. 다음 단계에서는 CLI를 사용하여 Amazon RDS 인스턴스를 생성하고 복원된 Aurora 클러스터에 연결합니다.

Aurora 클러스터를 복원하려면 여러 복원 옵션을 지정해야 합니다. 이러한 옵션에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Aurora DB 클러스터 백업 및 복원에 대한 개요를 참조하세요. 복원 옵션 사양은 의 API 가이드에서 확인할 수 있습니다. `RestoreDBClusterFromSnapshot`

Amazon Aurora 클러스터를 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Aurora 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 인스턴스 사양 창에서 기본값을 수락하거나 DB 엔진, DB 엔진 버전 및 용량 유형 설정의 옵션을 지정합니다.

   > **Note**
   >
   > 서버리스 용량 유형을 선택하면 용량 설정 창이 나타납니다. 최소 Aurora 용량 단위 및 최대 Aurora 용량 단위 설정의 옵션을 지정하거나 추가 조정 구성 섹션에서 다른 옵션을 선택합니다.

5. 설정 창에서 현재 지역의 사용자가 소유한 모든 DB 클러스터 인스턴스에 대해 고유한 이름을 지정합니다. AWS 계정
6. 네트워크 및 보안 창에서 기본값을 수락하거나 Virtual Private Cloud(VPC), 서브넷 그룹 및 가용 영역 설정의 옵션을 지정합니다.
7. 데이터베이스 옵션 창에서 기본값을 수락하거나 데이터베이스 포트, DB 클러스터 파라미터 그룹 및 IAM DB 인증 활성화 설정의 옵션을 지정합니다.
8. 백업 창에서 기본값을 수락하거나 스냅샷으로 태그 복사 설정의 옵션을 지정합니다.
9. 역추적 창에서 기본값을 수락하거나 역추적 활성화 또는 역추적 비활성화 설정의 옵션을 지정합니다.
10. 암호화 창에서 기본값을 수락하거나 암호화 활성화 또는 암호화 비활성화 설정의 옵션을 지정합니다.
11. 로그 내보내기 창에서 Amazon CloudWatch Logs에 게시할 로그 유형을 선택합니다. IAM 역할이 이미 정의되어 있습니다.
12. 복원 역할 창에서 AWS Backup 에서 이 복원 수행을 위임할 IAM 역할을 선택합니다.
13. 모든 설정을 지정한 후 백업 복원을 선택합니다.

    복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.
14. 복원이 완료되면 복원된 Aurora 클러스터를 Amazon RDS 인스턴스에 연결합니다.

    AWS CLI 사용:

    - Linux, macOS, Unix의 경우:

```
aws rds create-db-instance --db-instance-identifier sample-instance \
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

- Windows의 경우:

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

연속 백업 및 선택한 시점으로의 복원에 대한 자세한 내용은 연속 백업 및 point-in-time 복원 (PITR) 을 참조하십시오.

AWS Backup API, CLI 또는 SDK를 사용하여 Aurora 복구 지점을 복원하십시오.

StartRestoreJob를 사용합니다. Aurora를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

예제

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
```

```
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"
```

Amazon EC2 인스턴스 복원

EC2 인스턴스를 복원하면 Amazon 머신 이미지 (AMI), 인스턴스, Amazon EBS 루트 볼륨, Amazon EBS 데이터 볼륨 (보호된 리소스에 데이터 볼륨이 있는 경우) 및 Amazon EBS 스냅샷이 AWS Backup 생성됩니다. AWS Backup 콘솔을 사용하여 일부 인스턴스 설정을 사용자 지정하거나 또는 SDK를 사용하여 더 많은 설정을 사용자 지정할 수 있습니다. AWS CLI AWS

EC2 인스턴스 복원에는 다음 고려 사항이 적용됩니다.

- AWS Backup 보호된 리소스가 원래 사용한 것과 동일한 키 쌍을 사용하도록 복원된 인스턴스를 구성합니다. 복원 프로세스 중에는 복원된 인스턴스에 다른 키 페어를 지정할 수 없습니다.
- AWS Backup Amazon EC2 인스턴스를 시작하는 동안 사용된 사용자 데이터는 백업 및 복원하지 않습니다.
- 복원된 인스턴스를 구성할 때 보호 리소스가 원래 사용한 것과 동일한 인스턴스 프로필을 사용하거나 인스턴스 프로필 없이 시작하는 방법 중에서 선택할 수 있습니다. 이는 권한 상승 가능성을 방지하기 위한 것입니다. Amazon EC2 콘솔을 사용하여 복원된 인스턴스의 인스턴스 프로필을 업데이트할 수 있습니다.

  원래 인스턴스 프로필을 사용하는 경우 다음 권한을 AWS Backup 부여해야 합니다. 여기서 리소스 ARN은 인스턴스 프로필과 연결된 IAM 역할의 ARN입니다.

  ```
  {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::account-id:role/role-name"
  },
  ```

- 복원 중에 모든 Amazon EC2 할당량 및 구성 제한이 적용됩니다.
- Amazon EC2 복구 지점이 들어 있는 저장소에 저장소 잠금이 있는 경우 자세한 내용은 추가 보안 고려 사항 을 참조하십시오.

AWS Backup 콘솔을 사용하여 Amazon EC2 복구 지점을 복원하십시오.

단일 복구 지점에서 루트 볼륨, 데이터 볼륨, 일부 인스턴스 구성 설정 (예: 인스턴스 유형 및 키 쌍) 을 포함한 전체 Amazon EC2 인스턴스를 복원할 수 있습니다.

콘솔을 사용하여 Amazon EC2 리소스를 복원하려면 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택한 다음 Amazon EC2 리소스의 ID를 선택하여 리소스 세부 정보 페이지를 엽니다.
3. 복구 지점 창에서 복원할 복구 지점의 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. Network settings 창에서는 보호된 인스턴스의 설정을 사용하여 인스턴스 유형, VPC, 서브넷, 보안 그룹, 인스턴스 IAM 역할에 대한 기본값을 선택합니다. 이러한 기본값을 사용하거나 필요에 따라 변경할 수 있습니다.
5. Restore role 창에서 기본 역할을 사용하거나 IAM 역할 선택을 사용하여 백업을 복원할 AWS Backup 권한을 부여하는 IAM 역할을 지정합니다.
6. 보호된 리소스 태그 창에서 기본적으로 보호된 리소스의 태그를 복원된 리소스로 복사를 선택합니다. 이러한 태그를 복사하지 않으려면 확인란의 선택을 취소하십시오.
7. 고급 설정 창에서 인스턴스 설정의 기본값을 그대로 사용하거나 필요에 따라 변경합니다. 이러한 설정에 대한 자세한 내용을 보려면 설정에 대한 정보를 선택하여 도움말 창을 여십시오.
8. 인스턴스 구성을 마치면 백업 복원을 선택합니다.

다음을 사용하여 Amazon EC2를 복원합니다. AWS CLI

명령줄 인터페이스에서 최대 32개의 파라미터 (AWS Backup 콘솔을 통해 사용자 지정할 `start-restore-job`수 없는 일부 파라미터 포함) 를 사용하여 복원할 수 있습니다.

다음은 Amazon EC2 복구 시점을 복원하기 위해 전달할 수 있는 허용되는 메타데이터의 목록입니다.

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
```

```
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
aws:backup:request-id
```

AWS Backup 다음과 같은 정보 전용 속성을 허용합니다. 하지만 이러한 항목을 포함해도 복원에는 영향을 주지 않습니다.

```
vpcId
```

저장된 파라미터를 포함하지 않고 Amazon EC2 인스턴스를 복원할 수도 있습니다. 이 옵션은 AWS Backup 콘솔의 보호된 리소스 탭에서 사용할 수 있습니다.

Storage Gateway 볼륨 복원

AWS Storage Gateway 볼륨 스냅샷을 복원하는 경우 스냅샷을 Storage Gateway 볼륨 또는 Amazon EBS 볼륨으로 복원하도록 선택할 수 있습니다. 이는 두 서비스와 AWS Backup 통합되며 모든 Storage Gateway 스냅샷을 Storage Gateway 볼륨 또는 Amazon EBS 볼륨으로 복원할 수 있기 때문입니다.

AWS Backup 콘솔을 통해 Storage Gateway를 복원합니다

Storage Gateway 볼륨을 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Storage Gateway 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 리소스에 대한 복원 파라미터를 지정합니다. 입력하는 복원 파라미터는 선택한 리소스 유형에 따라 다릅니다.

   리소스 유형에서는 이 백업을 복원할 때 생성할 AWS 리소스를 선택합니다.
5. Storage Gateway 볼륨을 선택한 경우 연결 가능한 상태의 게이트웨이를 선택합니다. iSCSI 대상 이름도 선택합니다.

   1. '저장 볼륨' 게이트웨이에서 디스크 ID를 선택합니다.
   2. '캐시 볼륨' 게이트웨이에서 보호된 리소스 이상의 용량을 선택합니다.

   EBS 볼륨을 선택한 경우 볼륨 유형 및 크기(GiB)에 대한 값을 입력하고 가용 영역을 선택합니다.
6. 복원 역할에서 이 복원을 수행할 IAM 역할을 선택합니다. AWS Backup

   > **Note**
   >
   > 계정에 AWS Backup 기본 역할이 없는 경우 올바른 권한을 가진 기본 역할이 자동으로 생성됩니다. 이 기본 역할을 삭제하거나 사용할 수 없게 만들 수 있습니다.
7. 백업 복원을 선택합니다.

   복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.

Storage Gateway를 사용하여 복원합니다. AWS CLI

명령줄 인터페이스에서 `start-restore-job`을 사용하면 Storage Gateway 볼륨을 복원할 수 있습니다.

허용되는 메타데이터는 다음과 같습니다.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and AWS ##.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
```

```
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Amazon Timestream 테이블 복원

Amazon Timestream 테이블을 복원할 때는 새 테이블 이름, 대상 데이터베이스, 스토리지 할당 기본 설정(메모리 및 마그네틱 스토리지), 복원 작업을 완료하는 데 사용할 역할 등 여러 옵션을 구성할 수 있습니다. 오류 로그를 저장할 Amazon S3 버킷도 선택할 수 있습니다. 마그네틱 스토리지 쓰기는 비동기식이므로 오류를 로그하는 것이 좋습니다.

Timestream 데이터 스토리지에는 두 개의 계층, 즉 메모리 저장소 및 마그네틱 저장소가 있습니다. 메모리 저장소는 필수이지만, 지정된 메모리 기간이 끝난 후 복원된 테이블을 마그네틱 스토리지로 전송할 수도 있습니다. 메모리 저장소는 높은 처리량의 데이터 쓰기 및 빠른 point-in-time 쿼리에 최적화되어 있습니다. 마그네틱 저장소는 처리량이 낮은 지연 도착 데이터 쓰기, 장기 데이터 스토리지, 빠른 분석 쿼리에 최적화되어 있습니다.

Timestream 테이블을 복원할 때는 각 스토리지 계층에 테이블을 보관할 기간을 결정합니다. 콘솔 또는 API를 사용하여 두 가지 모두에 대한 스토리지 기간을 설정할 수 있습니다. 스토리지는 선형적이고 순차적입니다. Timestream은 복원된 테이블을 먼저 메모리 스토리지에 저장한 다음 메모리 스토리지 기간에 도달하면 자동으로 마그네틱 스토리지로 전환합니다.

> **Note**
>
> 마그네틱 저장소 보존 기간은 원래 보존 기간(콘솔 오른쪽 위에 표시됨)과 같거나 더 길어야 합니다. 그렇지 않으면 데이터가 손실됩니다.

예: 메모리 저장소 할당은 데이터를 1주일 동안 보관하도록 설정하고 마그네틱 저장소 할당은 동일한 데이터를 1년 동안 보관하도록 설정합니다. 메모리 저장소의 데이터가 1주일이 되면 자동으로 마그네틱 저장소로 이동됩니다. 그런 다음 마그네틱 저장소에서 1년 동안 유지됩니다. 이 기간이 끝나면 Timestream과 AWS Backup에서 삭제됩니다.

콘솔을 사용하여 Amazon Timestream 테이블을 복원하려면 AWS Backup

에서 생성한 타임스트림 테이블을 AWS Backup 콘솔에서 복원할 수 있습니다. AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon Timestream 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 다음과 같은 새 테이블 구성 설정을 지정합니다.

   a. 2~256자(문자, 숫자, 대시, 마침표, 밑줄)로 구성된 새 테이블 이름.

   b. 드롭다운 메뉴에서 선택한 대상 데이터베이스.
5. 스토리지 할당: 복원된 테이블이 처음에 메모리 스토리지에 보관되는 기간을 설정하고, 그런 다음 복원된 테이블이 마그네틱 스토리지에 보관되는 기간을 설정합니다. 메모리 스토리지는 시간, 일, 주 또는 월 단위로 설정할 수 있습니다. 마그네틱 스토리지는 일, 주, 월 또는 연 단위로 설정할 수 있습니다.
6. (선택 사항) 마그네틱 스토리지 쓰기 활성화: 마그네틱 스토리지 쓰기를 허용하는 옵션이 있습니다. 이 옵션을 선택하면 지연 도착 데이터, 즉 메모리 스토리지 보존 기간을 벗어난 타임스탬프가 있는 데이터가 마그네틱 저장소에 직접 기록됩니다.
7. (선택 사항) Amazon S3 오류 로그 위치: 오류 로그를 저장할 S3 위치를 지정할 수 있습니다. S3 파일을 찾아보거나 S3 파일 경로를 복사하여 붙여넣습니다.

   > **Note**
   >
   > S3 오류 로그 위치를 지정하기로 선택한 경우 이 복원에 사용하는 역할에는 S3 버킷에 쓸 수 있는 권한이 있거나 해당 권한이 있는 정책이 포함되어 있어야 합니다.
8. 복원을 수행하기 위해 전달할 IAM 역할을 선택합니다. 기본 IAM 역할을 사용하거나 다른 역할을 지정할 수 있습니다.
9. 백업 복원을 클릭합니다.

복원 작업은 보호된 리소스 아래에 표시됩니다. 새로 고침 버튼 또는 CTRL-R을 클릭하여 복원 작업의 현재 상태를 볼 수 있습니다.

API, CLI 또는 SDK를 사용하여 Amazon Timestream 테이블을 복원하려면

API를 통해 Timestream 테이블을 복원하려면 `StartRestoreJob`을 사용합니다.

를 사용하여 타임스트림을 복원하려면 작업을 `start-restore-job`. 사용하고 다음 메타데이터를 지정합니다. AWS CLI

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

다음은 예제 템플릿입니다.

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

복원 정보를 위해 DescribeRestoreJob을 사용할 수도 있습니다.

에서는 작업을 describe-restore-job 사용하고 다음 메타데이터를 사용합니다. AWS CLI

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

다음은 예제 템플릿입니다.

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Amazon Redshift 클러스터 복원

AWS Backup 콘솔이나 CLI를 통해 자동 및 수동 스냅샷을 복원할 수 있습니다.

Amazon Redshift 클러스터를 복원하면 기본적으로 원래 클러스터 설정이 콘솔에 입력됩니다. 아래 구성에 대해 다른 설정을 지정할 수 있습니다. 테이블을 복원할 때는 소스 및 대상 데이터베이스를 지정해야 합니다. 이러한 구성에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 스냅샷에서 클러스터 복원을 참조하세요.

- 단일 테이블 또는 클러스터: 전체 클러스터 또는 단일 테이블을 복원하도록 선택할 수 있습니다. 단일 테이블을 복원하도록 선택한 경우 소스 데이터베이스, 소스 스키마 및 소스 테이블 이름과 대상 클러스터, 스키마 및 새 테이블 이름이 필요합니다.
- 노드 유형: 각 Amazon Redshift 클러스터는 하나의 리더 노드와 하나 이상의 컴퓨팅 노드로 구성됩니다. 클러스터를 복원할 때는 CPU, RAM, 스토리지 용량 및 드라이브 유형에 대한 요구 사항을 충족하는 노드 유형을 지정해야 합니다.
- 노드 수: 클러스터를 복원할 때 필요한 노드 수를 지정해야 합니다.
- 구성 요약
- 클러스터 권한

콘솔을 사용하여 Amazon Redshift 클러스터 또는 테이블을 복원하려면 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택하고 복원하려는 Amazon Redshift 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 복원 시점 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 복원 옵션

    a. 스냅샷에서 클러스터를 복원합니다. 또는

    b. 스냅샷 내의 단일 테이블을 새 클러스터로 복원합니다. 이 옵션을 선택하는 경우 다음을 구성해야 합니다.

        i. 대소문자 구분 이름을 켜거나 끕니다.

        ii. 데이터베이스, 스키마, 테이블 등 소스 테이블 값을 입력합니다. 소스 테이블 정보는 Amazon Redshift 콘솔에서 확인할 수 있습니다.

        iii. 데이터베이스, 스키마, 새 테이블 이름 등 대상 테이블 값을 입력합니다.

5. 새 클러스터 구성 설정을 지정합니다.

   a. 클러스터 복원의 경우: 클러스터 식별자, 노드 유형 및 노드 수를 선택합니다.

   b. 가용 영역 및 유지 관리 기간을 지정합니다.

   c. IAM 역할 연결을 클릭하여 추가 역할을 연결할 수 있습니다.

6. 선택 사항: 추가 구성:

   a. 기본값 사용은 기본적으로 활성화됩니다.

   b. 드롭다운 메뉴를 사용하여 네트워킹 및 보안, VPC 보안 그룹, 클러스터 서브넷 그룹, 가용 영역에 대한 설정을 선택합니다.

   c. 향상된 VPC 라우팅을 켜거나 끕니다.

   d. 클러스터 엔드포인트를 퍼블릭 액세스 가능으로 지정할지 여부를 결정합니다. 퍼블릭 액세스 가능일 경우 VPC 외부의 인스턴스 및 디바이스가 클러스터 엔드포인트를 통해 데이터베이스에 연결할 수 있습니다. 이 옵션이 켜져 있으면 탄력적 IP 주소를 입력합니다.

7. 선택 사항: 데이터베이스 구성. 다음을 입력하도록 선택할 수 있습니다.

   a. 데이터베이스 포트(텍스트 필드에 입력)

   b. 파라미터 그룹

8. 유지 관리: 다음을 선택할 수 있습니다.

   a. 유지보수 윈도우

   b. 유지 관리 트랙(현재, 후행 또는 미리 보기 중에서 선택). 이 옵션은 유지 관리 기간 중 적용되는 클러스터 버전을 제어합니다.

9. 자동 스냅샷은 기본값으로 설정되어 있습니다.

   a. 자동 스냅샷 보존 기간. 보존 기간은 0~35일이어야 합니다. 자동 스냅샷을 생성하지 않으려면 0을 선택합니다.

   b. 수동 스냅샷 보존 기간은 1~3,653일입니다.

   c. 클러스터 재배치 확인란(선택 사항)이 있습니다. 이 확인란을 선택하면 클러스터를 다른 가용 영역에 재배치할 수 있습니다. 재배치를 활성화한 후 VPC 엔드포인트를 사용할 수 있습니다.

10. 모니터링: 클러스터가 복원된 후 Amazon Redshift를 통해 모니터링을 CloudWatch 설정할 수 있습니다.

11. 복원을 수행하기 위해 전달할 IAM 역할을 선택합니다. 기본 역할을 사용할 수도 있고 다른 역할을 지정할 수도 있습니다.

복원 작업은 작업 아래에 표시됩니다. 새로 고침 버튼 또는 CTRL-R을 클릭하여 복원 작업의 현재 상태를 볼 수 있습니다.

API, CLI 또는 SDK를 사용하여 Amazon Redshift 클러스터 복원

StartRestoreJob을 사용하여 Amazon Redshift 클러스터를 복원합니다.

를 사용하여 Amazon Redshift를 복원하려면 명령을 start-restore-job 사용하고 다음 메타데이터를 지정하십시오. AWS CLI

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
```

```
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

자세한 내용은 Amazon Redshift API 참조의 RestoreFromClusterSnapshot 섹션 및 AWS CLI 설명서의 restore-from-cluster-snapshot 섹션을 참조하세요.

다음은 예제 템플릿입니다.

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region AWS ##
-\-endpoint-url URL
```

예:

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

복원 정보를 위해 DescribeRestoreJob을 사용할 수도 있습니다.

에서는 작업을 describe-restore-job 사용하고 다음 메타데이터를 사용하십시오. AWS CLI

```
Region
```

다음은 예제 템플릿입니다.

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region AWS ##
```

예:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
```

```
-\-region us-west-2 \
```

Amazon EC2 인스턴스의 SAP HANA 데이터베이스 복원

EC2 인스턴스의 SAP HANA 데이터베이스는 AWS Backup 콘솔, API 또는 를 사용하여 복원할 수 있습니다. AWS CLI

주제

- 콘솔을 사용하여 Amazon EC2 인스턴스 데이터베이스에서 SAP HANA를 복원합니다. AWS Backup
- StartRestoreJob EC2 기반 SAP HANA용 API
- SAP HANA on EC2용 CLI
- 문제 해결

콘솔을 사용하여 Amazon EC2 인스턴스 데이터베이스에서 SAP HANA를 복원합니다. AWS Backup

동일한 데이터베이스를 포함하는 백업 작업과 복원 작업은 동시에 실행될 수 없습니다. SAP HANA 데이터베이스 복원 작업이 실행될 때 동일한 데이터베이스를 백업하려고 하면 '중지된 데이터베이스는 백업할 수 없음'이라는 오류가 발생할 수 있습니다.

1. 사전 요구 사항의 자격 증명을 사용하여 AWS Backup 콘솔에 액세스합니다.
2. 대상 복원 위치 드롭다운 메뉴에서 복원에 사용 중인 복구 시점으로 덮어쓸 데이터베이스를 선택합니다(복원 대상 데이터베이스를 호스팅하는 인스턴스에도 사전 요구 사항의 권한이 있어야 함).

   > **Important**
   >
   > SAP HANA 데이터베이스 복원은 파괴적입니다. 데이터베이스를 복원하면 지정된 대상 복원 위치에 있는 데이터베이스를 덮어씁니다.

3. 이 단계는 시스템 복사 복원을 수행하는 경우에만 완료하고, 그렇지 않으면 4단계로 건너뜁니다.

   시스템 복사 복원은 복구 시점을 생성한 소스 데이터베이스가 아닌 다른 대상 데이터베이스로 복원하는 복원 작업입니다. 시스템 복사 복원의 경우 콘솔에 제공된 `aws ssm-sap put-resource-permission` 명령을 확인하세요. 이 명령은 사전 요구 사항이 완료된 시스템에서 복사, 붙여넣기 및 실행해야 합니다. 이 명령을 실행할 때 애플리케이션 등록에 필요한 권한을 설정하는 사전 요구 사항에 있는 역할의 보안 인증 정보를 사용하세요.

```
// Example command
aws ssm-sap put-resource-permission \
--region us-east-1 \
--action-type RESTORE \
--source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
--resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
```

4. 복원 위치를 선택하면 대상 데이터베이스의 리소스 ID, 애플리케이션 이름, 데이터베이스 유형 및 EC2 인스턴스를 볼 수 있습니다.
5. 선택적으로 고급 복원 설정을 열어 카탈로그 복원 옵션을 변경할 수 있습니다. 기본 선택은 AWS Backup에서 최신 카탈로그를 복원하는 것입니다.
6. 백업 복원을 클릭합니다.
7. 복원 중에 대상 위치를 덮어쓰므로("파괴적 복원") 다음 팝업 대화 상자에서 이를 허용하도록 확인해야 합니다.

   a. 계속하려면 복원 중인 데이터베이스가 기존 데이터베이스를 덮어쓴다는 점을 이해해야 합니다.

   b. 이 점을 이해했으면 기존 데이터를 덮어쓸 것임을 인정해야 합니다. 이를 인정하고 계속하려면 텍스트 입력 필드에 덮어쓰기를 입력합니다.
8. 백업 복원을 클릭합니다.

절차가 성공하면 콘솔 상단에 파란색 배너가 나타납니다. 이는 복원 작업이 진행 중임을 나타냅니다. 자동으로 작업 페이지로 리디렉션됩니다. 이 페이지에서 복원 작업이 복원 작업 목록에 나열됩니다. 가장 최근 작업의 상태는 Pending일 것입니다. 복원 작업 ID를 검색한 다음 클릭하여 각 복원 작업의 세부 정보를 볼 수 있습니다. 새로 고침 버튼을 클릭하여 복원 작업 목록을 새로 고치면 복원 작업의 상태 변화를 확인할 수 있습니다.

StartRestoreJob EC2 기반 SAP HANA용 API

이 작업은 Amazon 리소스 이름(ARN)으로 식별되는 저장된 리소스를 복구합니다.

요청 구문

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
```

```
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 요청 파라미터: 요청은 URI 파라미터를 사용하지 않습니다.

요청 본문: 요청은 JSON 형식의 다음 데이터를 받습니다.

IdempotencyToken고객이 선택한 문자열로, 동일한 호출을 구분하는 데 사용할 수 있습니다. StartRestoreJob 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

Metadata

메타데이터 키-값 페어의 집합입니다. 복구 시점을 복원하는 데 필요한 리소스 이름과 같은 정보가 들어 있습니다. GetRecoveryPointRestoreMetadata를 호출하여 백업했던 당시의 리소스에 대한 구성 메타데이터를 가져올 수 있습니다. 하지만 리소스를 복원하려면 GetRecoveryPointRestoreMetadata에서 제공한 값 외에 다른 값이 필요할 수 있습니다. 예를 들어, 원본이 이미 있는 경우 새 리소스 이름을 제공해야 할 수 있습니다.

SAP HANA on Amazon EC2 인스턴스를 복원하려면 특정 메타데이터를 포함해야 합니다. SAP HANA StartRestoreJob 관련 항목의 메타데이터를 참조하십시오.

관련 메타데이터를 검색하려면 GetRecoveryPointRestoreMetadata 호출을 사용합니다.

표준 SAP HANA 데이터베이스 복구 시점의 예:

```
"RestoreMetadata": {
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
```

```
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

연속 SAP HANA 데이터베이스 복구 시점의 예:

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

SAP HANA on EC2용 CLI

`start-restore-job` 명령은 Amazon 리소스 이름(ARN)으로 식별되는 저장된 리소스를 복구합니다. CLI는 위의 API 지침을 따릅니다.

시놉시스:

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
```

```
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

옵션

`--recovery-point-arn`(문자열)은 복구 시점을 고유하게 식별하는 Amazon 리소스 번호(ARN) 형식의 문자열입니다. 예: `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata`(맵): 메타데이터 키-값 페어의 집합입니다. 복구 시점을 복원하는 데 필요한 리소스 이름과 같은 정보가 들어 있습니다. `GetRecoveryPointRestoreMetadata`를 호출하여 백업했던 당시의 리소스에 대한 구성 메타데이터를 가져올 수 있습니다. 하지만 리소스를 복원하려면 `GetRecoveryPointRestoreMetadata`에서 제공한 값 외에 다른 값이 필요할 수 있습니다. SAP HANA on Amazon EC2 인스턴스를 복원하려면 특정 메타데이터를 지정해야 합니다.

- `aws:backup:request-id`: 멱등성에 사용되는 임의의 UUID 문자열입니다. 복원 환경은 어떤 식으로든 바뀌지 않습니다.
- `aws:backup:TargetDatabaseArn`: 복원하려는 데이터베이스를 지정합니다. SAP HANA on Amazon EC2 데이터베이스 ARN입니다.
- `CatalogRestoreOption`: 카탈로그를 복원할 위치를 지정합니다. `NO_CATALOG` `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH` 중 하나입니다.
- `LocalCatalogPath`: CatalogRestoreOption 메타데이터 값이 `CATALOG_FROM_LOCAL_PATH` 인 경우 EC2 인스턴스의 로컬 카탈로그 경로를 지정하십시오. 이 경로는 EC2 인스턴스의 유효한 파일 경로여야 합니다.
- `RecoveryType`: 현재 `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` 및 `MOST_RECENT_TIME_RECOVERY` 복구 유형이 지원됩니다.

키 = (문자열), 값 = (문자열). 간편 구문:

```
KeyName1=string,KeyName2=string
```

JSON 구문:

```
{"string": "string"
  ...}
```

`--idempotency-token`은 고객이 선택한 문자열로, `StartRestoreJob`에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

`--resource-type`은 다음 리소스 중 하나에 대한 복구 시점 복원 작업을 시작하는 문자열입니다. SAP HANA on Amazon EC2의 경우 `SAP HANA on Amazon EC2`. 선택적으로 `aws ssm-sap tag-resource` 명령을 사용하여 SAP HANA 리소스에 태그를 지정할 수 있습니다.

출력: `RestoreJobId`는 복구 시점을 복원하는 작업을 고유하게 식별하는 문자열입니다.

문제 해결

백업 작업을 시도하는 동안 다음 오류가 발생하는 경우 관련 해결 방법을 참조하세요.

- 오류: 연속 백업 로그 오류

  연속 백업의 복구 시점을 유지하기 위해 SAP HANA는 모든 변경 사항에 대한 로그를 생성합니다. 로그를 사용할 수 없는 경우 각 연속 복구 시점의 상태는 `STOPPED`입니다. 복원에 사용할 수 있는 마지막 실행 가능한 복구 시점은 상태가 `AVAILABLE`인 복구 시점입니다. `STOPPED` 상태의 복구 시점과 `AVAILABLE` 상태의 복구 시점 사이에 로그 데이터가 누락된 경우 이러한 시간에는 복원이 성공한다는 보장을 할 수 없습니다. 이 범위 내에 있는 날짜 및 시간을 입력하면 AWS Backup 백업은 시도하지만 복구 가능한 가장 가까운 시간을 사용합니다. 이 오류는 메시지 `“Encountered an issue with log backups. Please check SAP HANA for details."`에 표시됩니다.

  해결 방법: 콘솔에는 로그를 기반으로 가장 최근의 복원 가능 시간이 표시됩니다. 표시된 시간보다 더 최근 시간을 입력할 수 있습니다. 하지만 로그에서 이 기간의 데이터를 사용할 수 없는 경우에는 복원 가능한 가장 최근의 시간이 사용됩니다. AWS Backup

- 오류: `Internal error`

  해결 방법: 콘솔에서 지원 케이스를 생성하거나 복원 세부 정보 (예: 복원 작업 ID) 를 포함하여 AWS Support 문의하세요.

- 오류: `The provided role arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  해결 방법: 복원을 호출할 때 수임하는 역할에 서비스 연결 역할을 생성하는 데 필요한 권한이 있는지 확인합니다.

- 오류: `User: arn:aws:sts::ACCOUNT_ID:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:ACCOUNT_ID:...`

  해결 방법: 사전 요구 사항에 설명된 복원 권한을 호출할 때 수임하는 역할을 올바르게 입력했는지 확인합니다.

- 오류: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  해결 방법: Backint 에이전트가 제대로 설치되었는지 확인합니다. 모든 사전 요구 사항, 특히 SAP 애플리케이션 서버에 AWS BackInt 에이전트 및 AWS Systems Manager SAP 설치 요구 사항을 확인한 다음 에이전트를 다시 설치해 보십시오. BackInt

- 오류: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  해결 방법: 복원 작업이 서비스 워크플로에 의해 취소되었습니다. 복원 작업을 다시 시도합니다.

- 오류: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  해결 방법: 인스턴스에서 일시적인 네트워크 불안정이 발생했습니다. 요청을 다시 시도합니다. 이 문제가 지속적으로 발생하는 경우 `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`에 있는 에이전트 구성 파일에 `ForceRetry: "true"`를 추가해 보세요.

기타 AWS Backint 에이전트 관련 문제는 SAP HANA용 Backint AWS 에이전트 문제 해결을 참조하십시오.

DocumentDB 클러스터 복원

AWS Backup 콘솔을 사용하여 Amazon DocumentDB 복구 지점을 복원하십시오.

Amazon DocumentDB 클러스터를 복원하려면 여러 복원 옵션을 지정해야 합니다. 이러한 옵션에 대한 자세한 내용은 Amazon DocumentDB 개발자 안내서의 클러스터 스냅샷에서 복원을 참조하세요.

Amazon DocumentDB 클러스터를 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Amazon DocumentDB 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 구성 창에서 기본값을 수락하거나 클러스터 식별자, 엔진 버전, 인스턴스 클래스 및 인스턴스 수 옵션을 지정합니다.

   - 참고: 복원할 때 기본 VPC가 없는 경우 다른 VPC의 서브넷을 지정해야 합니다.
5. 네트워크 및 보안 창에 '기본 설정 없음'이 표시됩니다.
6. E ncryption-at-rest 창에서 기본값을 그대로 사용하거나 암호화 활성화 또는 암호화 비활성화 설정 옵션을 지정합니다.
7. 클러스터 옵션 창에서 포트를 입력하고 클러스터 파라미터 그룹을 선택합니다.
8. 백업 창에서 point-in-time 복구를 위한 연속 백업 (PITR), 예약된 스냅샷 백업 또는 둘 다를 선택합니다.
9. 로그 내보내기 창에서 Amazon CloudWatch Logs에 게시할 로그 유형을 선택합니다. IAM 역할이 이미 정의되어 있습니다.
10. 유지 관리 창에서 유지 관리 기간을 지정하거나 기본 설정 없음을 선택합니다.
11. 태그 창에서 태그 추가를 선택할 수 있습니다.
12. 삭제 방지 창에서 삭제 방지 활성화를 선택할 수 있습니다.
13. 모든 설정을 지정한 후 백업 복원을 선택합니다.

    복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.
14. 복원이 완료되면 복원된 Amazon DocumentDB 클러스터를 Amazon RDS 인스턴스에 연결합니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Amazon DocumentDB 복구 지점을 복원하십시오.

먼저 클러스터를 복원합니다. `StartRestoreJob`를 사용합니다. Amazon DocumentDB를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

그런 다음 `create-db-instance`를 사용하여 복원된 Amazon DocumentDB 클러스터를 Amazon RDS 인스턴스에 연결합니다.

- Linux, macOS, Unix의 경우:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Windows의 경우:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Neptune 클러스터 복원

AWS Backup 콘솔을 사용하여 Amazon Neptune 복구 지점을 복원하십시오.

Amazon Neptune 데이터베이스를 복원하려면 여러 복원 옵션을 지정해야 합니다. 이러한 옵션에 대한 자세한 내용은 Neptune 사용 설명서의 DB 클러스터 스냅샷에서 복원을 참조하세요.

Neptune 데이터베이스를 복원하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 선택하고 복원하려는 Neptune 리소스 ID를 선택합니다.
3. 리소스 세부 정보 페이지에 선택된 리소스 ID의 복구 시점 목록이 표시됩니다. 리소스를 복원하려면 백업 창에서 리소스의 복구 시점 ID 옆에 있는 라디오 버튼을 선택합니다. 창의 오른쪽 위에서 복원을 선택합니다.
4. 인스턴스 사양 창에서 기본값을 수락하거나 DB 엔진 및 버전을 지정합니다.
5. 설정 창에서 현재 지역의 사용자가 소유한 모든 DB 클러스터 인스턴스에 대해 고유한 이름을 지정합니다. AWS 계정 DB 클러스터 식별자는 대소문자를 구분하지 않지만 'mydbclusterinstance'와 같이 모두 소문자로 저장됩니다. 필수 필드입니다.
6. 데이터베이스 옵션 창에서 기본값을 수락하거나 데이터베이스 포트 및 DB 클러스터 파라미터 그룹 옵션을 지정합니다.
7. 암호화 창에서 기본값을 수락하거나 암호화 활성화 또는 암호화 비활성화 설정의 옵션을 지정합니다.
8. 로그 내보내기 창에서 Amazon CloudWatch Logs에 게시할 로그 유형을 선택합니다. IAM 역할이 이미 정의되어 있습니다.
9. 복원 역할 창에서 AWS Backup 에서 이 복원 수행을 위임할 IAM 역할을 선택합니다.
10. 모든 설정을 지정한 후 백업 복원을 선택합니다.

    복원 작업 창이 나타납니다. 페이지 상단에 복원 작업에 대한 정보를 제공하는 메시지가 나타납니다.
11. 복원이 완료되면 복원된 Neptune 클러스터를 Amazon RDS 인스턴스에 연결합니다.

AWS Backup API, CLI 또는 SDK를 사용하여 Neptune 복구 지점을 복원하십시오.

먼저 클러스터를 복원합니다. `StartRestoreJob`를 사용합니다. Amazon DocumentDB를 복원할 때 다음 메타데이터를 지정할 수 있습니다.

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

그런 다음 `create-db-instance`를 사용하여 복원된 Neptune 클러스터를 Amazon RDS 인스턴스에 연결합니다.

- Linux, macOS, Unix의 경우:

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Windows의 경우:

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

자세한 내용은 Neptune 관리 API 참조의 RestoreDBClusterFromSnapshot 섹션 및 Neptune CLI 설명서의 restore-db-cluster-from-snapshot 섹션을 참조하세요.

스택 백업 복원 CloudFormation

CloudFormation 복합 백업은 CloudFormation 템플릿과 모든 관련 중첩 복구 지점의 조합입니다. 중첩 복구 시점은 원하는 수만큼 복원할 수 있지만 복합 복구 시점(최상위 복구 시점)은 복원할 수 없습니다.

CloudFormation 템플릿 복구 지점을 복원할 때는 백업을 나타내는 변경 세트를 사용하여 새 스택을 생성합니다.

CloudFormation AWS Backup 콘솔을 사용하여 복원하십시오.

CloudFormation 콘솔에서 새 스택과 변경 세트를 볼 수 있습니다. 변경 세트에 대한 자세한 내용은 AWS CloudFormation 사용 설명서에서 변경 세트를 사용하여 스택 업데이트를 참조하세요.

CloudFormation스택으로 복원할 중첩 복구 지점을 결정한 다음 AWS Backup 콘솔을 사용하여 복원하십시오.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 백업 볼트로 이동하여 원하는 복구 시점이 포함된 백업 볼트를 선택한 다음 복구 시점을 클릭합니다.
3. AWS CloudFormation 템플릿 복구 지점을 복원합니다.
   a. 복원하려는 중첩 복구 시점이 들어 있는 복합 복구 시점을 클릭하면 복합 복구 시점의 세부 정보 페이지가 나타납니다.
   b. 중첩 복구 시점 아래에 중첩 복구 시점이 표시됩니다. 각 복구 시점에는 복구 시점 ID, 상태, 리소스 ID, 리소스 유형, 백업 유형 및 해당 복구 시점이 생성된 시간이 있습니다. AWS CloudFormation 복구 지점 옆에 있는 라디오 버튼을 클릭한 다음 복원을 클릭합니다. 리소스 유형: AWS CloudFormation 및 백업 유형: 백업이 지정된 복구 시점을 선택해야 합니다.
4. CloudFormation 템플릿의 복원 작업이 완료되면 복원된 AWS CloudFormation 템플릿이 AWS CloudFormation 콘솔의 스택 아래에 표시됩니다.
5. 스택 이름에서 상태가 `REVIEW_IN_PROGRESS`인 복원된 템플릿을 찾을 수 있습니다.
6. 스택 이름을 클릭하면 스택의 세부 정보를 볼 수 있습니다.
7. 스택 이름 아래에 탭이 있습니다. 변경 세트를 클릭합니다.
8. 변경 세트를 실행합니다.
9. 이 프로세스가 끝나면 원래 스택의 리소스가 새 스택에 다시 생성됩니다. 스테이트풀 리소스는 비어 있는 상태로 다시 생성됩니다. 스테이트풀 리소스를 복구하려면 AWS Backup 콘솔의 복구 지점 목록으로 돌아가서 필요한 복구 지점을 선택하고 복원을 시작하십시오.

를 사용하여 복원하십시오. CloudFormation AWS CLI

명령줄 인터페이스에서 CloudFormation 스택을 `start-restore-job`복원할 수 있습니다.

다음 목록은 CloudFormation 리소스를 복원하기 위해 허용되는 메타데이터입니다.

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

복원 테스트

주제

개요

에서 제공하는 AWS Backup기능인 복원 테스트는 복원 실행 가능성에 대한 자동 및 주기적 평가와 복원 작업 지속 시간을 모니터링하는 기능을 제공합니다.

먼저 계획의 이름, 복원 테스트 빈도, 목표 시작 시간을 지정하는 복원 테스트 계획을 생성합니다. 그런 다음 계획에 포함할 리소스를 할당합니다. 그런 다음 테스트에 특정 복구 지점 또는 임의 복구 지점을 포함하도록 선택합니다. AWS Backup 백업은 복원 작업을 성공적으로 수행하는 데 필요한 메타데이터를 지능적으로 추론합니다.

계획상 예정된 시간이 되면 계획에 따라 복원 작업을 AWS Backup 시작하고 복원을 완료하는 데 걸리는 시간을 모니터링합니다.

복원 테스트 계획의 실행이 완료되면 결과를 사용하여 복원 테스트 시나리오의 성공적인 완료 또는 복원 작업 완료 시간과 같은 조직 또는 거버넌스 요구 사항의 준수 여부를 확인할 수 있습니다.

원하는 경우 를 복원 테스트 검증 사용하여 복원 테스트 결과를 확인할 수 있습니다.

선택적 검증이 완료되거나 검증 창이 닫히면 복원 테스트와 관련된 리소스가 AWS Backup 삭제되고 서비스 SLA에 따라 리소스가 삭제됩니다.

테스트 프로세스가 끝나면 테스트 결과 및 테스트 완료 시간을 확인할 수 있습니다.

복원 테스트와 복원 프로세스 비교

복원 테스트는 온디맨드 복원과 동일한 방식으로 복원 작업을 실행하고 온디맨드 복원과 동일한 복구 시점(백업)을 사용합니다. 복원 테스트를 통해 시작된 각 작업에 `StartRestoreJob` 대해 수신 요청 CloudTrail (선택한 경우) 이 표시됩니다.

하지만 일정에 따른 복원 테스트 작업과 온디맨드 복원 작업 간에는 몇 가지 차이점이 있습니다.

	복원 테스트	복원
계정	권장되는 모범 사례는 복원 테스트에 사용할 계정을 지정하는 것입니다.	계정에서 리소스를 복원할 수 있습니다.
AWS Backup Audit Manager	컨트롤을 켜서 복원 테스트가 지정된 복원 목표를 충족하는지 확인할 수 있습니다.	
케이던스	예정된 계획의 일환으로 정기적으로 수행합니다.	온디맨드
리전 구분	이스라엘 (텔아비브) 을 제외하고 AWS Backup 영업하는 모든 상업 지역에서 이용 가능 AWS GovCloud (미국 동부), (미국 서부), 중국 AWS	영업하는 모든 상업 지역에서 사용 가능 AWS Backup

	복원 테스트	복원
	GovCloud (베이징), 중국 (닝샤) 은 사용할 수 없습니다.	
리소스	테스트 계획에 할당할 수 있는 리소스 유형으로는 Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx(Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS, Amazon S3 등이 있습니다.	모든 리소스를 복원할 수 있습니다.
결과	복원 테스트 작업이 완료되면 복원 테스트 검증 창이 종료된 후 복원된 리소스가 삭제됩니다.	복원 작업이 완료되면 복원된 버전의 리소스는 그대로 유지됩니다.
태그	복원 시 태그를 지원하는 리소스 유형의 경우 테스트에서 복원 시 태그를 적용합니다.	지원되는 리소스의 경우 태그는 선택 사항입니다.

복원 테스트 관리

AWS Backup 콘솔에서 복원 테스트 계획을 생성, 조회, 업데이트 또는 삭제할 수 있습니다.

AWS CLI를 사용하여 복원 테스트 계획의 작업을 프로그래밍 방식으로 수행할 수 있습니다. 각 CLI는 해당 CLI가 시작된 AWS 서비스에 따라 다릅니다. 명령 앞에 `aws backup`을 붙여야 합니다.

데이터 삭제

복원 테스트가 완료되면 테스트와 관련된 리소스 삭제를 AWS Backup 시작합니다. 삭제는 즉각적으로 수행되지 않습니다. 각 리소스에는 해당 리소스의 저장 및 수명 주기 방식을 결정하는 기본 구성이 있습니다. 예를 들어 Amazon S3 버킷이 복원 테스트의 일부인 경우 수명 주기 규칙이 버킷에 추가됩니다. 규칙을 실행하고 버킷과 해당 객체를 완전히 삭제하는 데 최대 며칠이 걸릴 수 있지만, 수명 주기 규

칙이 시작되는 날(기본값은 1일)까지만 이러한 리소스에 대한 요금이 부과됩니다. 삭제 속도는 리소스 유형에 따라 달라집니다.

복원 테스트 계획의 일부인 리소스에는 awsbackup-restore-test라는 태그가 포함되어 있습니다. 사용자가 이 태그를 제거하면 테스트 기간이 끝날 때 리소스를 삭제할 AWS Backup 수 없으며 대신 사용자가 수동으로 삭제해야 합니다.

리소스가 예상대로 삭제되지 않은 이유를 확인하려면 콘솔에서 실패한 작업을 검색하거나 명령줄 인터페이스에서 DescribeRestoreJob API 요청을 호출하여 삭제 상태 메시지를 검색할 수 있습니다.

백업 계획 (비복원 테스트 계획) 은 복원 테스트를 통해 생성된 리소스 (awsbackup-restore-test태그나 이름이 로 시작하는 리소스awsbackup-restore-test) 를 무시합니다.

비용 관리

복원 테스트에는 복원 테스트당 비용이 발생합니다. 복원 테스트 계획에 포함된 리소스에 따라 계획의 일부인 복원 작업에도 비용이 발생할 수 있습니다. 전체 내용은 AWS Backup 요금을 참조하세요.

복원 테스트 계획을 처음 설정하는 경우 기능, 프로세스 및 관련 평균 비용을 숙지할 수 있도록 최소한의 리소스 유형과 보호된 리소스를 포함하는 것이 유용할 수 있습니다. 계획을 만든 후 업데이트하여 더 많은 리소스 유형과 보호된 리소스를 추가할 수 있습니다.

복원 테스트 계획 생성

복원 테스트 계획에는 계획 생성과 리소스 할당이라는 두 부분이 있습니다.

콘솔을 사용하는 경우 이러한 부분은 순차적으로 수행됩니다. 첫 번째 부분에서는 이름, 빈도, 시작 시간을 설정합니다. 두 번째 부분에서는 테스트 계획에 리소스를 할당합니다.

API를 사용할 AWS CLI 때는 먼저 사용하십시오 create-restore-testing-plan. 응답을 성공적으로 받고 계획을 만들었으면 계획에 포함하려는 각 리소스 유형에 대해 create-restore-testing-selection를 사용하세요.

Console

1부: 콘솔을 사용하여 복원 테스트 계획 생성

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색에서 복원 테스트를 찾아 선택합니다.
3. 복원 테스트 계획 생성을 선택합니다.

4. 일반

   a. 이름: 새 복원 테스트 계획의 이름을 입력합니다. 생성한 후에는 이름을 변경할 수 없습니다. 이름은 영숫자와 밑줄로만 구성해야 합니다.

   b. 테스트 빈도: 복원 테스트를 실행할 빈도를 선택합니다.

   c. 시작 시간: 원하는 테스트 시작 시간(시간 및 분)을 설정합니다. 복원 테스트 계획을 실행할 현지 시간대를 설정할 수도 있습니다.

   d. 시작 시간: 이 값 (시간) 은 복원 테스트를 시작하도록 지정된 기간입니다. AWS Backup 시작하는 동안 지정된 모든 복원 작업을 시간 내에 시작하기 위해 최선을 다하고 이 기간 내의 시작 시간을 임의로 지정합니다.

5. 복구 시점 선택: 여기서는 계획에 포함할 복구 시점(백업) 소스 볼트, 복구 시점 범위 및 선택 기준을 설정합니다.

   a. 소스 볼트: 사용 가능한 모든 볼트를 포함할지 아니면 계획에 포함할 수 있는 복구 시점을 필터링하는 데 도움이 되도록 특정 볼트만 포함할지 선택합니다. 특정 볼트를 선택하는 경우 드롭다운 메뉴에서 포함하려는 볼트를 선택합니다.

   b. 적격 복구 시점: 복구 시점을 선택할 기간을 지정합니다. 1~365일, 1~52주, 1~12개월 또는 1년을 선택할 수 있습니다.

   c. 선택 기준: 복구 시점의 날짜 범위를 지정한 후에는 최신 복구 시점을 포함할지 아니면 무작위로 하나를 계획에 포함할지 선택할 수 있습니다. 이전 버전으로의 복원이 보장되는 경우에 대비하여 보다 정기적으로 복구 시점의 전반적인 상태를 측정하기 위해 무작위 방법을 선택할 수 있습니다.

   d. P oint-in-time 복구 지점: 계획에 연속 백업 (point-in-time-restore/PITR) 지점이 있는 리소스가 포함된 경우 이 확인란을 선택하여 테스트 계획에 연속 백업을 적합한 복구 지점으로 포함하도록 할 수 있습니다 (이 기능이 있는 리소스 유형에 대한 리소스별 기능 가용성 참조).

6. (선택 사항) 복원 테스트 계획에 추가된 태그: 복원 테스트 계획에 최대 50개의 태그를 추가할 수 있습니다. 각 태그를 개별적으로 추가해야 합니다. 새 태그를 추가하려면 새 태그 추가를 선택합니다.

2부: 콘솔을 사용하여 계획에 리소스 할당

이 섹션에서는 복원 테스트 계획에 포함하기 위해 백업한 리소스를 선택합니다. 리소스 할당 이름을 선택하고, 복원 테스트에 사용할 역할을 선택하고, 정리 전 보존 기간을 설정합니다. 그런 다음, 리소스 유형을 선택하고 범위를 선택한 후 선택적으로 태그를 사용하여 선택 범위를 좁힐 수 있습니다.

> **Tip**
>
> 리소스를 추가하려는 복원 테스트 계획으로 돌아가려면 AWS Backup 콘솔로 이동하여 복원 테스트를 선택한 다음, 원하는 테스트 계획을 찾아 선택하면 됩니다.

1. 일반

   a. 리소스 할당 이름: 공백 없이 영숫자와 밑줄로 구성된 문자열을 사용하여 이 리소스 할당의 이름을 입력합니다.

   b. IAM 역할 복원: 테스트는 지정한 Identity and Access Management(IAM) 역할을 사용해야 합니다. AWS Backup 기본 역할을 선택하거나 다른 역할을 선택할 수 있습니다. 이 프로세스를 완료할 때 AWS Backup 기본값이 아직 존재하지 않는 경우 필요한 권한을 사용하여 기본값을 AWS Backup 자동으로 생성합니다. 복원 테스트를 위해 선택한 IAM 역할에는 AWSBackupServicePolicyForRestores에 있는 권한이 포함되어야 합니다.

   c. 정리 전 보존 기간: 복원 테스트 중에 백업 데이터가 일시적으로 복원됩니다. 기본적으로 이 데이터는 테스트가 완료된 후에 삭제됩니다. 복원 시 검증을 실행하려는 경우 이 데이터의 삭제를 연기할 수 있습니다.

      검증을 실행하려는 경우 특정 시간 동안 보존을 선택하고 1시간부터 168시간까지의 값을 입력합니다. 참고로, 검증은 프로그래밍 방식으로 실행할 수 있지만 AWS Backup 콘솔에서는 실행할 수 없습니다.

2. 보호된 리소스:

   a. 리소스 유형 선택: 리소스 테스트 계획에 포함할 리소스 유형과 해당 유형의 백업 범위를 선택합니다. 각 계획에는 여러 리소스 유형이 포함될 수 있지만 각 리소스 유형을 계획에 개별적으로 할당해야 합니다.

   b. 리소스 선택 범위: 유형을 선택한 후 해당 유형의 사용 가능한 보호된 리소스를 모두 포함할지 또는 특정 보호된 리소스만 포함할지 선택합니다.

   c. (선택 사항) 태그를 사용하여 리소스 선택 구체화: 백업에 태그가 있는 경우 태그별로 필터링하여 특정 보호된 리소스를 선택할 수 있습니다. 태그 키, 이 키의 조건 포함 여부, 키 값을 입력합니다. 그런 다음 태그 추가 버튼을 선택합니다.

      보호된 리소스의 태그는 보호된 리소스가 포함되어 있는 백업 볼트 내 최신 복구 시점의 태그를 확인하여 평가됩니다.

3. 복원 파라미터: 특정 리소스의 경우 복원 작업을 준비하기 위해 파라미터를 지정해야 합니다. 대부분의 경우 AWS Backup 는 저장된 백업을 기반으로 값을 유추합니다.

대부분의 경우 이러한 파라미터를 유지하는 것이 좋지만 드롭다운 메뉴에서 다른 항목을 선택하여 값을 변경할 수 있습니다. 암호화 키 재정의, 데이터를 추론할 수 없는 Amazon FSx 설정, 서브넷 생성 등의 경우에는 값을 변경하는 것이 좋습니다.

예를 들어 RDS 데이터베이스가 복원 테스트 계획에 할당한 리소스 유형 중 하나인 경우 가용 영역, 데이터베이스 이름, 데이터베이스 인스턴스 클래스, VPC 보안 그룹과 같은 파라미터가 변경할 수 있는 추론된 값과 함께 표시됩니다(해당하는 경우).

AWS CLI

`CreateRestoreTestingPlan` CLI 명령은 복원 테스트 계획을 세우는 데 사용됩니다.

테스트 계획에는 다음을 포함해야 합니다.

- 고유한 `RestoreTestingPlanName`을 포함하는 `RestoreTestingPlan`
- `ScheduleExpression` cron 표현식
- `RecoveryPointSelection`

  이름은 비슷하긴 하지만 `RestoreTestingSelection` 같지는 않습니다.

  `RecoveryPointSelection`매개변수 5개 (필수 3개, 선택 2개) 가 있습니다. 지정한 값에 따라 복원 테스트에 포함되는 복구 지점이 결정됩니다. 내에 최신 복구 지점을 사용할지 `SelectionWindowDays` 아니면 임의 복구 지점을 원하는지 여부를 표시해야 하며, 복구 지점을 선택할 수 있는 저장소를 지정해야 합니다. `Algorithm` `IncludeVaults`

선택한 항목에는 보호된 리소스 ARN이 하나 이상 있거나 조건이 하나 이상 있을 수 있지만 둘 다 포함할 수는 없습니다.

다음을 포함할 수도 있습니다.

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

`create-restore-testing-plan` CLI 명령을 사용합니다.

계획이 성공적으로 생성되었으면 create-restore-testing-selection을 사용하여 계획에 리소스를 할당해야 합니다.

이것은 RestoreTestingSelectionName, ProtectedResourceType 및 다음 중 하나로 구성됩니다.

- ProtectedResourceArns
- ProtectedResourceConditions

각 보호된 리소스 유형은 단일 값을 가질 수 있습니다. 복원 테스트 선택 항목에는 ProtectedResourceArns에 대한 와일드카드 값('*')과 함께 ProtectedResourceConditions를 포함할 수 있습니다. 또는 ProtectedResourceArns에 최대 30개의 특정 보호된 리소스 ARN을 포함할 수 있습니다.

복구 지점 결정

테스트 계획이 실행될 때마다 (지정한 빈도와 시작 시간에 따라), 선택한 보호 리소스당 적합한 복구 지점 하나가 복원 테스트를 통해 복원됩니다. 복구 지점 선택 기준을 충족하는 리소스의 복구 지점이 없는 경우 해당 리소스는 테스트에 포함되지 않습니다.

테스트 선택 항목에 포함된 보호 대상 리소스의 복구 지점은 지정된 기간 및 복원 테스트 계획에 포함된 저장소의 기준을 충족하는 경우에만 사용할 수 있습니다.

리소스 테스트 선택 항목에 리소스 유형이 포함되어 있고 다음 조건 중 하나에 해당하는 경우 보호된 리소스가 선택됩니다.

- 해당 선택 항목에 리소스 ARN이 지정되어 있습니다. 또는
- 해당 선택 항목의 태그 조건은 해당 리소스의 최신 복구 지점의 태그와 일치합니다.

복원 테스트 계획 업데이트

콘솔 또는 AWS CLI를 통해 복원 테스트 계획의 일부와 해당 계획 내의 리소스 선택 항목을 업데이트할 수 있습니다.

Console

콘솔에서 복원 테스트 계획 및 선택 항목 업데이트

콘솔에서 복원 테스트 계획 세부 정보 페이지를 보면 계획의 여러 설정을 편집(업데이트)할 수 있습니다. 방법은 다음과 같습니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색에서 복원 테스트를 찾아 선택합니다.
3. 편집 버튼을 선택합니다.
4. 빈도, 시작 시간 및 선택한 시작 시간 이후에 테스트가 시작될 시간을 조정합니다.
5. 변경 내용을 저장합니다.

AWS CLI

를 통해 복원 테스트 계획 및 선택 항목을 업데이트하십시오. AWS CLI

UpdateRestoreTestingPlan요청하고, 지정된 계획 또는 선택 항목에 대한 부분 업데이트를 전송하는 데 사용할 UpdateRestoreTestingSelection수 있습니다. 이름은 변경할 수 없지만 다른 파라미터는 업데이트할 수 있습니다. 각 요청에서 변경하려는 파라미터만 포함하세요.

업데이트 요청을 보내기 전에 GetRestoreTestingPlan및 GetRestoreTestingSelection를 사용하여 특정 RestoreTestingSelection ARN이 포함되어 있는지 또는 와일드카드 및 조건을 사용하는지 확인하십시오.

복원 테스트 선택 항목에 와일드카드 대신 ARN이 지정되어 있고 이를 조건이 있는 와일드카드로 변경하려면 업데이트 요청에 ARN 와일드카드와 조건을 모두 포함해야 합니다. 선택 항목에는 보호된 리소스 ARN이 있거나 조건이 있는 와일드카드를 사용할 수 있지만 둘 다 포함할 수는 없습니다.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

기존 복원 테스트 계획 보기

Console

콘솔에서 기존 복원 테스트 계획 및 할당된 리소스에 대한 세부 정보 보기

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색에서 복원 테스트를 선택합니다. 디스플레이에 복원 테스트 계획이 표시됩니다. 계획은 기본적으로 마지막 런타임을 기준으로 표시됩니다.
3. 계획에서 링크를 선택하면 계획의 요약, 계획 이름, 빈도, 시작 시간, 시작해야 하는 시간 범위 값 등 세부 정보를 볼 수 있습니다.

또한 이 계획 내의 보호된 리소스, 이 계획에 포함된 최근 30일 동안의 복원 테스트 작업, 이 테스트 계획의 일부로 만들 수 있는 모든 태그를 볼 수 있습니다.

AWS CLI

명령줄을 사용하여 기존 복원 테스트 계획 및 테스트 선택 항목에 대한 세부 정보 보기

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

복원 테스트 작업 보기

Console

콘솔에서 기존 복원 테스트 작업 보기

복원 테스트 작업은 복원 작업 페이지에 포함되어 있습니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 작업 페이지로 이동합니다.

   또는 복원 테스트를 선택한 다음 복원 테스트 계획을 선택하여 세부 정보 및 계획과 관련된 작업을 볼 수 있습니다.
3. 복원 작업 탭을 선택합니다.

이 페이지에서 복원 작업의 상태, 복원 시간, 복원 유형, 리소스 ID, 리소스 유형, 작업이 속한 복원 테스트 계획, 생성 시간 및 복구 지점 ID를 볼 수 있습니다.

복원 테스트 계획에 포함된 작업의 복원 유형은 테스트입니다.

복원 테스트 작업에는 여러 상태 범주가 있습니다.

- 주의가 필요한 상태 유형에는 밑줄이 그어져 있습니다. 상태를 마우스로 가리키면 추가 세부 정보가 있는 경우 확인할 수 있습니다.
- 테스트에서 복원 테스트 검증 시작된 경우 검증 상태가 표시됩니다 (콘솔에서는 사용할 수 없음).
- 삭제 상태는 복원 테스트에서 생성된 데이터의 상태를 나타냅니다. 삭제 상태는 성공, 삭제, 실패의 세 가지가 있습니다.

  복원 테스트 작업 삭제가 실패한 경우 복원 테스트 흐름에서 자동으로 완료할 수 없으므로 리소스를 수동으로 제거해야 합니다. 리소스에서 `awsbackup-restore-test` 태그를 제거하면 삭제에 실패하는 경우가 종종 있습니다.

AWS CLI

명령줄에서 기존 복원 테스트 작업 보기

- `list-restore-jobs-by-protected-resource`

복원 테스트 계획 삭제

Console

콘솔에서 복원 테스트 계획 삭제

1. 현재 복원 테스트 계획을 확인하려면 기존 복원 테스트 계획 보기로 이동합니다.
2. 복원 테스트 계획 세부 정보 페이지에서 삭제를 선택하여 계획을 삭제합니다.
3. 삭제를 선택하면 계획을 삭제할지 확인하는 팝업 확인 화면이 나타납니다. 이 화면에 특정 복원 테스트 계획의 이름이 굵게 표시됩니다. 계속하려면 대/소문자를 구분하고 밑줄, 대시, 마침표를 포함하여 테스트 계획의 이름을 정확히 입력합니다.

복원 테스트 계획 삭제 옵션을 선택할 수 없는 경우 표시된 이름과 일치할 때까지 이름을 다시 입력합니다. 복원 테스트 계획이 정확히 일치하면 복원 테스트 계획을 삭제하는 옵션을 선택할 수 있게 됩니다.

AWS CLI

명령줄을 통해 복원 테스트 계획 삭제

CLI 명령을 사용하여 복원 테스트 선택 항목을 삭제할 DeleteRestoreTestingSelection수 있습니다. 요청에 `RestoreTestingPlanName` 및 `RestoreTestingSelectionName`을 포함하세요.

테스트 계획을 삭제하기 전에 테스트 계획과 관련된 모든 테스트 선택 항목을 삭제해야 합니다. 모든 테스트 선택 항목을 삭제한 후에는 API 요청을 DeleteRestoreTestingPlan사용하여 복원 테스트 계획을 삭제할 수 있습니다. `RestoreTestingPlanName`을 포함해야 합니다.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

복원 테스트 감사

AWS Backup Audit Manager와의 복원 테스트 통합은 복원된 리소스가 목표 복원 시간 내에 완료되었는지 평가하는 데 도움이 됩니다.

자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결에서 리소스 복원 시간 목표 충족을 참조하세요.

복원 테스트 할당량 및 파라미터

- 복원 테스트 계획 100개
- 각 복원 테스트 계획에 태그 50개 추가 가능
- 계획당 선택 항목 30개
- 선택 항목당 보호된 리소스 ARN 30개
- 선택 항목당 보호된 리소스 조건 30개(`StringEquals` 및 `StringNotEquals`에 속하는 조건 포함)
- 선택 항목당 볼트 선택기 30개
- 최대 선택 기간(일): 365일
- 시작 시간의 기간: 최소: 1시간, 최대: 168시간(7일)

- 계획 이름의 최대 길이: 50자
- 선택 항목 이름의 최대 길이: 50자

한도에 관한 추가 정보는 AWS Backup 할당량에서 확인할 수 있습니다.

복원 테스트 실패 문제 해결

복원 상태가 인 복원 테스트 작업이 있는 경우 다음과 같은 이유가 Failed 원인과 해결 방법을 파악하는 데 도움이 될 수 있습니다.

오류 메시지는 AWS Backup 콘솔의 작업 상태 세부 정보 페이지에서 보거나 CLI 명령 list-restore-jobs-by-protected-resource 또는 을 사용하여 볼 수 있습니다. list-restore-jobs

1. 오류: *No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.*

   해결 방법 1: 복원 테스트 선택 항목을 업데이트하고 매개 변수를 재정의합니다. SubnetId AWS Backup 콘솔에는 이 매개 변수가 “서브넷”으로 표시됩니다.

   해결 방법 2: 기본 VPC를 다시 생성합니다.

   영향을 받는 리소스 유형: Amazon EC2

2. 오류: *No subnets found for the default VPC [vpc]. Please specify a subnet.*

   해결 방법 1: 복원 테스트 선택을 업데이트하고 SubnetId 복원 파라미터를 재정의합니다. AWS Backup 콘솔에는 이 매개 변수가 “서브넷”으로 표시됩니다.

   해결 방법 2: 기본 VPC에 기본 서브넷을 생성합니다.

   영향을 받는 리소스 유형: Amazon EC2

3. 오류: *No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

   해결 방법 1: 복원 테스트 선택을 업데이트하고 DBSubnetGroupName 복원 파라미터를 재정의합니다. AWS Backup 콘솔에는 이 매개 변수가 서브넷 그룹으로 표시됩니다.

   해결 방법 2: 기본 VPC에 기본 서브넷을 생성합니다.

영향을 받는 리소스 유형: 아마존 Aurora, Amazon DocumentDB, 아마존 RDS, Neptune

4. ***IAM Role cannot be assumed by AWS Backup***오류:.

   해결 방법: 복원 역할은 가 맡을 수 있어야 합니다. AWS Backup IAM에서 역할의 신뢰 정책을 업데이트하여 역할을 맡도록 "backup.amazonaws.com" 하거나 복원 테스트 선택 항목을 업데이트하여 맡을 수 있는 역할을 사용하도록 하십시오. AWS Backup

   영향을 받는 리소스 유형: 모두

5. 오류: *Access denied to KMS key.* 또는 *The specified AWS KMS key* ARN *does not exist, is not enabled or you do not have permissions to access it.*

   해결 방법: 다음 사항을 확인하십시오.

   a. 복원 역할은 백업을 암호화하는 데 사용되는 AWS KMS 키와 복원된 리소스를 암호화하는 데 사용된 KMS 키 (해당하는 경우) 에 액세스할 수 있습니다.
   b. 위 KMS 키의 리소스 정책은 복원 역할이 해당 키에 액세스할 수 있도록 허용합니다.

   위 조건이 아직 충족되지 않은 경우 적절한 액세스를 위한 복원 역할과 리소스 정책을 구성하십시오. 그런 다음 복원 테스트 작업을 다시 실행합니다.

   영향을 받는 리소스 유형: 모두

6. 오류: *User ARN is not authorized to perform action on resource because no identity based policy allows the action.* 또는*Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*.

   해결 방법: 복원 역할에 적절한 권한이 없습니다. 복원 역할에 대한 IAM의 권한을 업데이트하십시오.

   영향을 받는 리소스 유형: 모두

7. 오류: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* 또는 *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   해결 방법: 복원 역할에 메시지에 지정된 리소스에 대한 적절한 액세스 권한이 없습니다. 언급된 리소스의 리소스 정책을 업데이트하십시오.

영향을 받는 리소스 유형: 모두

테스트 시 추론된 메타데이터 복원

복구 시점을 복원하려면 복원 메타데이터가 필요합니다. 복원 테스트를 수행하기 위해 AWS Backup 은 복원에 성공할 가능성이 있는 메타데이터를 자동으로 추론합니다. 이 명령을 사용하여 AWS Backup 추론할 내용을 미리 볼 `get-restore-testing-inferred-metadata` 수 있습니다. 이 명령은 에서 추론한 메타데이터 세트를 `get-restore-job-metadata` 반환합니다. AWS Backup일부 리소스 유형 (Amazon FSx) AWS Backup 의 경우 전체 메타데이터 세트를 유추할 수 없다는 점에 유의하십시오.

추론된 복원 메타데이터는 복원 테스트 프로세스 중에 결정됩니다. `RestoreTestingSelection`의 본문에 `RestoreMetadataOverrides` 파라미터를 포함하여 특정 복원 메타데이터 키를 재정의할 수 있습니다. 일부 메타데이터 재정의는 콘솔에서 사용할 수 없습니다. AWS Backup

지원되는 각 리소스에는 추론된 복원 메타데이터 키 및 값과 재정의 가능한 복원 메타데이터 키가 모두 있습니다. `#### ### ## ##`로 표시된 `RestoreMetadataOverrides` 키 값 페어나 중첩 키 값 페어만 필수적으로 포함해야 하고 나머지는 선택 사항입니다. 키 값은 대/소문자를 구분하지 않습니다.

> **Important**
>
> AWS Backup 리소스를 기본 설정 (예: Amazon EC2 인스턴스 또는 Amazon RDS 클러스터를 기본 VPC로 복원해야 함) 으로 복원해야 한다고 유추할 수 있습니다. 그러나 기본값이 없는 경우 (예: 기본 VPC 또는 서브넷이 삭제되고 메타데이터 재정의가 입력되지 않은 경우) 복원이 성공하지 못합니다.

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터

DynamoDB	`deletionProtection` (값이 `false`로 설정됨)
	
	다음의 경우 `encryptionType` 이 `Default`로 설정됩니다.
		`encryptionType`
		
		`kmsMasterKeyArn`

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
	targetTableName (값이 awsbackup-restore-test- 로 시작되는 무작위 값으로 설정됨)	
Amazon EBS	availabilityZone (값이 무작작위의 가용 영역으로 설정됨) encrypted (값이 true로 설정됨)	availabilityZone kmsKeyId
Amazon EC2	disableApiTermination 값이 false로 설정됨 instanceType 값이 복원되는 복구 시점의 InstanceType으로 설정됨 requiredImdsV2 값이 true로 설정됨	iamInstanceProfileName 값은 null 또는 null일 수 있습니다. UseBackedUpValue instanceType requireImdsV2 securityGroupIds subnetId

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
Amazon EFS	`encrypted` 값이 `true`로 설정됨 `file-system-id` 값이 복원되는 복구 시점의 파일 시스템 ID로 설정됨 다음의 경우 `kmsKeyId` `value`이 `alias/aws/elasticfilesystem` 로 설정됩니다. `newFileSystem` 값이 `true`로 설정됨 `performanceMode` 값이 `generalPurpose` 로 설정됨	`kmsKeyId`

Amazon FSx for Lustre	`lustreConfiguration` 에 중첩된 키가 있음. 중첩된 키 중 하나는 `automaticBackupRetentionDays` 이며 값이 `0`으로 설정됨	`kmsKeyId`
		
		`lustreConfiguration` 에 중첩된 키 `logConfiguration` 이 있음
		
		`securityGroupIds`
		
		`subnetIds` , `#### ### ####`

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
ONTAP용 아마존 NetApp FSx	name이 awsbackup _restore_test_ 로 시작되는 무작위 값으로 설정됨 ontapConfiguration 에 다음을 포함한 중첩된 키가 있음 • junctionPath (/name은 복원되는 볼륨의 이름을 나타냄) • sizeInMegabytes (이 값은 복원되는 복구 시점의 크기(MB)로 설정됨) • snapshotPolicy (값이 none으로 설정됨)	ontapConfiguration 에 다음을 포함하여 특정 재정의 가능한 중첩 키가 있음 • junctionPath • ontapVolumeType • securityStyle • sizeInMegabytes • storageEfficiencyEnabled • storageVirtualMachineId , #### ### ## ## • tieringPolicy

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
Amazon FSx for OpenZFS	openZfzConfiguration (다음을 포함한 중첩된 키가 있음) • automaticBackupRetentionDays (값이 0으로 설정됨) • deploymentType (값이 복원되는 복구 시점의 배포 유형으로 설정됨) • throughputCapacity (값이 deploymentType 을 기반으로 함). deploymentType 이 SINGLE_AZ_1 이면 값이 64로 설정되고, deploymentType 이 SINGLE_AZ_2 or MULTI_AZ_1 이면 값이 160으로 설정됨	kmsKeyId openZfsConfiguration 에 다음을 포함하여 특정 재정의 가능한 중첩 키가 있음 • deploymentType • throughputCapacity • diskiopsConfiguration securityGroupIds subnetIds

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
Amazon FSx for Windows File Server	windowsConfiguration (다음을 포함한 중첩된 키가 있음) • automaticBackupRetentionDays (값이 0로 설정됨) • deploymentType (값이 복원되는 복구 시점의 배포 유형으로 설정됨) • throughputCapacity (값이 8으로 설정됨)	kmsKeyId securityGroupIds subnetIds , *#### ### ## ##* windowsConfiguration (재정의 가능한 중첩 키가 포함됨) • throughputCapacity • activeDirectoryId *# ### ## ## selfManagedActiveDirectoryConfiguration #### ## ## #####.* • selfManagedActiveDirectoryConfiguration *#### ## ## activeDirectoryId ## ## ### #####.* • preferredSubnetId

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
Amazon RDS, Aurora, Amazon DocumentDB, Amazon Neptune 클러스터	availabilityZones (값이 최대 세 개의 무작위 가용 영역의 목록으로 설정됨) dbClusterIdentifier (awsbackup-restore-test 로 시작되는 무작위 값 포함) engine(값이 복원되는 복구 시점의 엔진으로 설정됨)	availabilityZones databaseName dbClusterParameterGroupName dbSubnetGroupName enableCloudwatchLogsExports enableIamDatabaseAuthentication engine engineMode engineVersion kmskeyId port optionGroupName scalingConfiguration vpcSecurityGroupIds

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터
Amazon RDS 인스턴스	dbInstanceIdentifier (awsbackup-restore-test- 로 시작되는 무작위 값 포함) deletionProtection (값이 false로 설정됨) multiAz(값이 false로 설정됨) publiclyAccessible (값이 false로 설정됨)	allocatedStorage availabilityZones dbInstanceClass dbName dbParameterGroupName dbSubnetGroupName domain domainIamRoleName enableCloudwatchLogsExports enableIamDatabaseAuthentication iops licensemodel multiAz optionGroupName port processorFeatures publiclyAccessible storageType vpcSecurityGroupIds

리소스 유형	추론된 복원 메타데이터 키 및 값	재정의 가능한 메타데이터

Amazon Simple Storage Service(S3)	`destinationBucketName` (awsbackup-restore-test- 로 시작되는 무작위 값 포함)
	
	`encrypted` (값이 `true`로 설정됨)
	
	`encryptionType` (값이 `SSE-S3`로 설정됨)
	
	`newBucket` (값이 `true`로 설정됨)
		`encryptionType`
		
		`kmsKey`

복원 테스트 검증

복원 테스트 작업이 완료될 때 실행되는 이벤트 기반 검증을 생성할 수 있습니다.

먼저 EventBridge Amazon에서 지원하는 대상 (예:) 을 사용하여 검증 워크플로를 생성합니다 AWS Lambda. 두 번째로, 복원 작업이 상태에 `COMPLETED` 도달할 때까지 수신 대기하는 EventBridge 규칙을 추가합니다. 셋째, 복원 테스트 계획을 세우거나 기존 계획을 예정대로 실행하십시오. 마지막으로 복원 테스트를 완료한 후 검증 워크플로의 로그를 모니터링하여 예상대로 실행되었는지 확인합니다 (검증이 실행되고 나면 AWS Backup 콘솔에 검증 상태가 표시됨).

1. 검증 워크플로를 설정합니다.

   Lambda 또는 에서 지원하는 다른 대상을 사용하여 검증 워크플로를 설정할 수 있습니다. EventBridge 예를 들어 Amazon EC2 인스턴스가 포함된 복원 테스트를 검증하는 경우 상태 점검 엔드포인트에 ping을 보내는 코드를 포함할 수 있습니다.

   이벤트의 세부 정보를 사용하여 검증할 리소스를 결정할 수 있습니다.

   사용자 지정 Lambda 계층을 사용하여 최신 SDK를 사용할 수 있습니다 (Lambda SDK를 통해 `PutRestoreValidationResult` 아직 제공되지 않음).

   다음은 샘플입니다.

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. EventBridge 규칙 추가

   복원 작업 COMPLETED이벤트를 수신하는 EventBridge 규칙을 생성합니다.

   필요에 따라 리소스 유형이나 복원 테스트 계획 ARN별로 이벤트를 필터링할 수 있습니다. 1단계에서 정의한 검증 워크플로를 호출하도록 이 규칙의 대상을 설정합니다. 예:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
```

```
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. 복원 테스트 계획을 실행하고 완료하도록 하세요.

   복원 테스트 계획은 구성한 일정에 따라 실행됩니다.

   아직 복원 테스트 계획이 없는 경우 복원 테스트 계획 만들기 또는 설정을 변경하려면 복원 테스트 계획 업데이트를 참조하십시오.
4. 결과를 모니터링하세요.

   복원 테스트 계획이 예정대로 실행되면 검증 워크플로의 로그를 확인하여 제대로 실행되었는지 확인할 수 있습니다.

   API를 `PutRestoreValidationResult` 호출하여 결과를 게시하면 AWS Backup 콘솔과 `DescribeRestoreJob` 또는 `ListRestoreJob` 같은 복원 작업을 설명하고 나열하는 AWS Backup API 호출을 통해 결과를 확인할 수 있습니다.

   검증 상태가 설정되면 변경할 수 없습니다.

백업 목록 보기

AWS Backup 콘솔을 사용하거나 프로그래밍 방식으로 백업 목록을 볼 수 있습니다.

주제

- 콘솔에서 보호된 리소스별로 백업 나열
- 콘솔에서 백업 볼트별로 백업 나열
- 프로그래밍 방식으로 백업 나열

콘솔에서 보호된 리소스별로 백업 나열

다음 단계에 따라 AWS Backup 콘솔에서 특정 리소스에 대한 백업 목록을 봅니다.

1. 에 AWS Management Console로그인하고 https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 보호된 리소스를 선택합니다.
3. 목록에서 보호된 리소스를 선택하여 백업 목록을 봅니다. 에서 백업한 리소스만 보호된 리소스 아래에 AWS Backup 나열됩니다.

리소스에 대한 백업을 볼 수 있습니다. 이 보기에서 백업을 선택하고 복원할 수도 있습니다.

콘솔에서 백업 볼트별로 백업 나열

다음 단계에 따라 백업 볼트에 구성된 백업 목록을 봅니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 백업 섹션에서 이 백업 볼트에 구성된 모든 백업의 목록을 봅니다. 이 보기에서는 열 헤더(상태 포함)를 기준으로 백업을 정렬하고 백업을 선택하여 복원, 편집 또는 삭제할 수 있습니다.

프로그래밍 방식으로 백업 나열

`ListRecoveryPoint` API 작업을 사용하여 프로그래밍 방식으로 백업을 나열할 수 있습니다.

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

예를 들어, 다음 AWS Command Line Interface (AWS CLI) 명령은 `EXPIRED` 상태와 함께 모든 백업을 나열합니다.

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

AWS Backup Audit Manager를 사용하여 정의한 제어 항목에 대한 AWS Backup 정책 준수 여부를 감사할 수 있습니다. 컨트롤은 백업 빈도 또는 백업 보존 기간 등과 같은 백업 요구 사항의 준수 여부를 감사하기 위해 설계된 절차입니다.

AWS Backup Audit Manager는 다음과 같은 질문에 답변할 수 있도록 도와줍니다.

- "모든 리소스를 백업하고 있는가?"
- "모든 백업이 암호화되어 있는가?"
- "백업이 매일 이루어지고 있는가?"

AWS Backup Audit Manager를 사용하면 정의한 컨트롤과 아직 호환되지 않는 백업 활동 및 리소스를 찾을 수 있습니다. 컨트롤이 리소스의 규정 준수 여부를 평가할 경우 활성 리소스만 포함됩니다. 예를 들어, 실행 중인 상태의 Amazon EC2 인스턴스를 평가합니다. 중단된 상태의 EC2 인스턴스는 규정 준수 평가에 포함되지 않습니다.

또한 백업 거버넌스를 위해 일일 및 온디맨드 보고서의 감사 추적을 자동으로 생성하는 데 사용할 수 있습니다.

다음 단계는 AWS Backup Audit Manager를 사용하는 방법에 대한 개요를 제공합니다. 자세한 설명을 보려면 이 페이지 끝에 있는 주제 중 하나를 선택하세요.

1. 하나 이상의 거버넌스 컨트롤 템플릿이 포함된 프레임워크를 만듭니다. 위에 나온 질문은 세 가지 거버넌스 컨트롤 템플릿의 예시입니다. 일부 거버넌스 컨트롤 템플릿의 파라미터를 사용자 지정할 수 있습니다. 예를 들어 마지막의 컨트롤 질문을 사용자 지정하여 '매일' 대신, "백업이 매주 이루어지고 있는가?"라는 질문을 설정할 수 있습니다.
2. 프레임워크를 보고 해당 프레임워크 내에 정의된 컨트롤을 준수하거나 준수하지 않는 리소스의 수를 확인합니다.
3. 백업 및 규정 준수 상태에 대한 보고서를 만듭니다. 이러한 보고서를 규정 준수 방식에 대한 입증할 수 있는 증거로 저장합니다. 또는 이러한 보고서를 저장하여 아직 규정을 준수하지 않은 개별 백업 작업 및 리소스를 식별할 수 있습니다.

   AWS Backup Audit Manager는 24시간마다 자동으로 새 보고서를 생성하여 Amazon S3에 게시합니다. 온디맨드 보고서도 생성할 수 있습니다.

> **Note**
>
> 첫 번째 규정 준수 관련 프레임워크를 만들려면 우선 리소스 추적을 켜야 합니다. 이렇게 하면 AWS Backup 리소스를 AWS Config 추적할 수 있습니다. 리소스 추적을 관리하는 방법에 대한 기술 문서는 AWS Config 개발자 안내서의 콘솔 설정을 AWS Config 참조하십시오.
> 리소스 추적을 켜면 요금이 부과됩니다. AWS Backup Audit Manager의 리소스 추적 가격 및 청구에 대한 자세한 내용은 측정, 비용 및 청구를 참조하십시오.

주제

감사 프레임워크 작업

프레임워크는 백업 방식을 평가하는 데 도움이 되는 컨트롤의 모음입니다. 사전 구축된 사용자 지정 가능한 컨트롤을 사용하여 정책을 정의하고 백업 방식이 정책을 준수하는지 여부를 평가할 수 있습니다. 또한 자동 일일 보고서를 설정하여 프레임워크의 규정 준수 상태에 대한 인사이트를 얻을 수 있습니다.

각 프레임워크는 단일 계정에 적용되며 AWS 리전지역별로 계정당 최대 15개의 프레임워크를 배포할 수 있습니다. 중복 프레임워크(동일한 컨트롤 및 파라미터가 포함된 프레임워크)는 배포할 수 없습니다.

프레임워크에는 두 가지 유형이 있습니다.

- AWS Backup 프레임워크(권장) - AWS Backup 프레임워크를 사용해 모든 사용 가능한 컨트롤을 배포하여 권장되는 모범 사례에 따라 백업 활동, 적용 범위, 리소스를 모니터링할 수 있습니다.
- 사용자가 정의하는 사용자 지정 프레임워크 - 사용자 지정 프레임워크를 사용하여 하나 이상의 특정 컨트롤을 선택하고 컨트롤 파라미터를 사용자 지정할 수 있습니다.

주제

- AWS Backup 콘솔을 사용하여 프레임워크 생성
- API를 사용하여 프레임워크 만들기 AWS Backup
- 프레임워크 규정 준수 상태 보기
- 규정 미준수 리소스 찾기
- 감사 프레임워크 업데이트
- 감사 프레임워크 업데이트

컨트롤 선택

다음 표에는 AWS Backup Audit Manager 컨트롤, 사용자 지정 가능한 매개 변수 및 AWS Config 기록 리소스 유형이 나열되어 있습니다. 이러한 유형은 규정 준수 상태를 기록하므로 모든 컨트롤에는 기록 리소스 유형 `AWS Config: resource compliance`가 필요합니다.

사용 가능한 컨트롤

컨트롤 이름	컨트롤 설명	사용자 지정 가능한 파라미터	AWS Config 기록 리소스 유형
백업 리소스가 백업 계획에 의해 보호됨	리소스가 백업 계획에 의해 보호되고 있는지 평가합니다.	None	`AWS Backup: backup selection`
백업 계획에 최소 빈도 및 최소 보존 기간이 있음	백업 빈도가 [1일] 이상이고 보존 기간이 [35일] 이상인지 평가합니다.	백업 빈도, 보존 기간	`AWS Backup: backup plans`
저장소가 복구 시점의 수동 삭제를 방지함	백업 저장소에서 특정 AWS Identity and Access Management (IAM) 역할을 제외한 복구 지점의 수동 삭제를 허용하지 않는지 평가합니다. 기본적으로 IAM 역할 예외는 없습니다. 프레임워크와 함께 이 컨트롤을 배포	복구 시점을 수동으로 삭제할 수 있는 IAM 역할 최대 5개	`AWS Backup: backup vaults`

컨트롤 이름	컨트롤 설명	사용자 지정 가능한 파라미터	AWS Config 기록 리소스 유형
	할 때도 IAM 역할 예외가 없습니다. AWS Backup		
복구 시점이 암호화됨	복구 시점이 암호화되었는지 평가합니다.	None	`AWS Backup: recovery points`
복구 시점에 설정된 최소 보존 기간	복구 시점 보존 기간이 [35일] 이상인지 평가합니다.	복구 시점 보존 기간	`AWS Backup: recovery points`
교차 리전 백업 복사본이 예약됨	리소스가 다른 AWS 리전에 백업 복사본을 만들도록 구성되어 있는지 평가합니다.	AWS 리전	`AWS Backup: backup selection`
교차 계정 백업 복사본이 예약됨	리소스에 교차 계정 백업 복사본이 구성되어 있는지 평가합니다.	AWS 계정 ID	`AWS Backup: backup selection`
백업은 AWS Backup 볼트 잠금으로 보호됩니다.	잠긴 백업 저장소에 백업을 포함하도록 리소스가 구성되어 있는지 평가합니다.	최소 보존 일수, 최대 보존 일수	`AWS Backup: backup selection`
마지막 복구 시점이 생성됨	지정된 기간 내에 복구 시점이 생성되었는지 평가합니다.	[1~744]시간 또는 [1~31]일 단위의 값입니다.	`AWS Backup recovery points`
리소스 복원 시간 목표 충족	복원 테스트 작업이 목표 복원 시간 내에 완료되었는지 평가합니다.	값(분)	None

이러한 컨트롤에 대한 자세한 정보는 컨트롤 및 문제 해결을 참조하세요.

모든 컨트롤을 지원하지 않는 AWS Backup지원되는 리소스 목록은 리소스별 기능 가용성 표의 AWS Backup Audit Manager 섹션을 참조하십시오.

> **Note**
>
> 위의 제어 기능을 사용하지 않으려는 경우에도 AWS Backup Audit Manager를 사용하여 백업, 복사 및 복원 작업에 대한 일일 보고서를 작성할 수 있습니다. 감사 보고서 작업을 참조하세요.

리소스 추적 켜기

첫 번째 규정 준수 관련 프레임워크를 만들려면 우선 리소스 추적을 켜야 합니다. 이렇게 하면 AWS Backup 리소스를 AWS Config 추적할 수 있습니다. 리소스 추적을 관리하는 방법에 대한 기술 문서는 AWS Config 개발자 안내서의 콘솔 설정을 AWS Config 참조하십시오.

리소스 추적을 켜면 요금이 부과됩니다. AWS Backup Audit Manager의 리소스 추적 가격 및 청구에 대한 자세한 내용은 측정, 비용 및 청구를 참조하십시오.

주제

- 콘솔을 사용하여 리소스 추적 켜기
- AWS Command Line Interface (AWS CLI)를 사용하여 리소스 추적 켜기
- AWS CloudFormation 템플릿을 사용하여 리소스 추적 켜기

콘솔을 사용하여 리소스 추적 켜기

콘솔을 사용하여 리소스 추적 켜기

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Audit Manager 아래에서 프레임워크를 선택합니다.
3. 리소스 추적 관리를 선택하여 리소스 추적을 활성화합니다.
4. AWS Config 설정으로 이동을 선택합니다.
5. 기록 활성화 또는 비활성화를 선택합니다.
6. 아래의 모든 리소스 유형에 대한 기록 활성화를 선택하거나, 일부 리소스 유형에 대한 기록을 활성화하도록 선택합니다. 컨트롤에 필요한 리소스 유형에 대한 내용은 AWS Backup Audit Manager 제어 및 수정을 참조하세요.

    - `AWS Backup: backup plans`

- `AWS Backup: backup vaults`
- `AWS Backup: recovery points`
- `AWS Backup: backup selection`

> **Note**
>
> AWS Backup Audit Manager에는 모든 제어가 필요합니다`AWS Config: resource compliance`.

7. 닫기를 선택하세요.
8. 리소스 추적 켜기라는 문구의 파란색 배너가 리소스 추적 켜짐이라는 문구의 녹색 배너로 전환될 때까지 기다립니다.

AWS Backup 콘솔의 두 위치에서 리소스 추적을 활성화했는지 여부와 활성화한 경우 기록 중인 리소스 유형을 확인할 수 있습니다. 왼쪽 탐색 창에서 다음 중 하나를 선택합니다.

- 프레임워크를 선택한 다음, AWS Config 레코더 상태 아래에서 텍스트를 선택합니다.
- 설정을 선택한 다음, AWS Config 레코더 상태 아래에서 텍스트를 선택합니다.

AWS Command Line Interface (AWS CLI)를 사용하여 리소스 추적 켜기

아직 온보딩하지 않은 경우 를 사용하여 온보딩하는 AWS Config것이 더 빠를 수 있습니다. AWS CLI

AWS CLI를 사용하여 리소스 추적을 켜려면

1. 다음 명령을 입력하여 AWS Config 레코더를 이미 활성화했는지 확인합니다.

```
$ aws configservice describe-configuration-recorders
```

   a. 다음과 같이 `ConfigurationRecorders` 목록이 비어 있는 경우

```
{
  "ConfigurationRecorders": []
}
```

   레코더가 활성화되지 않은 상태입니다. 2단계로 계속 진행하여 레코더를 생성하세요.

b. 모든 리소스에 대해 이미 기록을 활성화한 경우 ConfigurationRecorders 출력은 다음과 같이 표시됩니다.

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

모든 리소스를 활성화했으므로 리소스 추적이 이미 켜져 있습니다. AWS Backup Audit Manager를 사용하기 위해 이 절차의 나머지 부분을 완료할 필요는 없습니다.

c. ConfigurationRecorders이 레코더가 비어 있지는 않지만 모든 리소스에 대한 기록을 활성화하지 않은 경우, 다음 명령을 사용하여 기존 레코더에 백업 리소스를 추가하세요. 그런 다음 3단계로 건너뜁니다.

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
```

```
        ]
      }
    }
  ]
}
```

2. AWS Backup Audit Manager 리소스 유형을 사용하여 AWS Config 레코더 만들기

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. AWS Config 레코더에 대해 설명해 주세요.

```
$ aws configservice describe-configuration-recorders
```

출력을 다음 예상 출력과 비교하여 AWS Backup Audit Manager 리소스 유형이 있는지 확인하십시오.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. AWS Config 구성 파일을 저장할 대상으로 Amazon S3 버킷을 생성합니다.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. *policy.json# #### ### ####* 수 있는 AWS Config 권한을 부여합니다. 아래 샘플 *policy.json*을 참조하세요.

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. 버킷을 전송 채널로 구성하십시오. AWS Config

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. AWS Config 레코딩 활성화

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. 다음과 같은 방법으로 DescribeFramework 출력의 마지막 줄에 있는 "FrameworkStatus":"ACTIVE"를 확인합니다.

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
```

```
            "ParameterValue":"35"
          },
          {
            "ParameterName":"requiredFrequencyValue",
            "ParameterValue":"1"
          }
        ],
        "ControlScope":{

        }
      },
      {
        "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
        "ControlInputParameters":[

        ],
        "ControlScope":{

        }
      },
      {
        "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
        "ControlInputParameters":[

        ],
        "ControlScope":{

        }
      },
      {
        "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
        "ControlInputParameters":[

        ],
        "ControlScope":{

        }
      }
    ],
    "CreationTime":1633463605.233,
    "DeploymentStatus":"COMPLETED",
    "FrameworkStatus":"ACTIVE"
}
```

AWS CloudFormation 템플릿을 사용하여 리소스 추적 켜기

리소스 추적을 AWS CloudFormation 활성화하는 템플릿에 대해서는 AWS Backup Audit Manager와 함께 사용을 참조하십시오 AWS CloudFormation.

AWS Backup 콘솔을 사용하여 프레임워크 생성

리소스 추적을 활성화한 후 다음 단계를 사용하여 프레임워크를 생성합니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크를 선택합니다.
3. 프레임워크 생성을 선택합니다.
4. 프레임워크 이름에 고유한 이름을 입력합니다. 프레임워크 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자여야 합니다.
5. (선택 사항) 프레임워크 설명을 입력합니다.
6. 컨트롤에는 활성 컨트롤이 표시됩니다. 기본적으로 리소스에 사용할 수 있는 모든 컨트롤이 나열됩니다.

   활성 상태인 컨트롤을 변경하려면 컨트롤 편집을 클릭합니다.

   a. 첫 번째 확인란은 컨트롤이 켜져 있는지 나타냅니다. 컨트롤을 끄려면 확인란의 선택을 취소하세요.

   b. 평가할 리소스 선택에서 유형, 태그 또는 단일 리소스별로 리소스를 선택하는 방법을 선택할 수 있습니다.

   AWS Backup Audit Manager 컨트롤 목록은 각 컨트롤의 사용자 지정 옵션을 설명합니다.
7. (선택 사항) 새 태그 추가를 선택하여 프레임워크에 태그를 지정합니다. 태그를 사용하여 프레임워크를 검색 및 필터링하거나 비용을 추적할 수 있습니다.
8. 프레임워크 생성을 선택합니다.

AWS Backup Audit Manager는 프레임워크를 생성하는 데 몇 분 정도 걸릴 수 있습니다.

`AlreadyExists` 오류가 발생할 경우 동일한 컨트롤 및 파라미터를 사용하는 프레임워크가 이미 있는 것입니다. 새 프레임워크를 생성하려면 하나 이상의 컨트롤 또는 파라미터가 기존 프레임워크와 달라야 합니다.

API를 사용하여 프레임워크 만들기 AWS Backup

다음 표에는 각 컨트롤의 CreateFramework에 대한 샘플 API 요청과 해당하는 DescribeFramework 요청에 대한 샘플 API 응답이 함께 포함되어 있습니다. AWS Backup Audit Manager를 프로그래밍 방식으로 사용하려면 다음 코드 스니펫을 참조하십시오.

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Backup resources are protected by a backup plan	{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed",

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
		"IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"}

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
	"Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }	ole/service-role/Q uickSightAction"}], "ControlScope": {"Complia nceResourceIds":[" default"], "Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"}

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
		} }

Backup recovery points are encrypted	{"FrameworkName":
	"Control5",
	"FrameworkDescript
	ion": "This is a test
	framework",
	"FrameworkControls":
	[
	{"ControlName":
	"BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	"ControlInputParam
	eters":
	[],
	"ControlScope":
	{} // Default scope
	(no scope input) is all
	recovery points
	}
	],
	"IdempotencyToken":
	"Control5",
	"FrameworkTags":
	{"key1": "foo"}
	}
		{"FrameworkName":
		"Control5",
		"FrameworkArn":
		"arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		"FrameworkDescript
		ion": "This is a test
		framework",
		"FrameworkControls
		":
		[
		{"ControlName":
		"BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		"ControlInputParam
		eters":
		[],
		"ControlScope": {}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control5",
		"FrameworkTags":
		{"key1": "foo"}
		}

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

컨트롤	**CreateFramework** 요청	**DescribeFramework** 응답
	}	

프레임워크 규정 준수 상태 보기

감사 프레임워크를 생성하면 해당 프레임워크가 프레임워크 테이블에 나타납니다. AWS Backup 콘솔의 왼쪽 탐색 창에서 프레임워크를 선택하여 이 테이블을 볼 수 있습니다. 프레임워크에 대한 감사 결과를 보려면 해당 프레임워크 이름을 선택합니다. 이렇게 하면 요약 및 컨트롤이라는 두 가지 섹션으로 구성된 프레임워크 세부 정보 페이지로 이동합니다.

요약 섹션에는 왼쪽에서 오른쪽으로 다음과 같은 상태가 나열됩니다.

- 규정 준수 상태는 각 컨트롤의 규정 준수 상태에 따라 결정되는 감사 프레임워크의 전반적인 규정 준수 상태입니다. 각 컨트롤의 규정 준수 상태는 컨트롤이 평가하는 각 리소스의 규정 준수 상태에 따라 결정됩니다.

  프레임워크 규정 준수 상태는 컨트롤 평가 범위 내의 모든 리소스가 이러한 평가를 통과한 경우에만 `Compliant`로 표시됩니다. 하나 이상의 리소스가 컨트롤 평가를 통과하지 못한 경우, 규정 준수 상태는 `Non-Compliant`가 됩니다. 규정 미준수 리소스를 찾는 방법에 대한 자세한 내용은 규정 미준수 리소스 찾기를 참조하세요. 리소스가 규정을 준수하도록 하는 방법에 대한 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.
- 프레임워크 상태는 모든 리소스에 대해 리소스 추적을 설정했는지 여부를 나타냅니다. 가능한 상태는 다음과 같습니다.
  - `Active` - 프레임워크가 평가하는 모든 리소스에 대해 기록이 켜진 경우입니다.
  - `Partially active` - 프레임워크가 평가하는 하나 이상의 리소스에 대해 기록이 꺼진 경우입니다.
  - `Inactive` - 프레임워크가 평가하는 모든 리소스에 대해 기록이 꺼진 경우입니다.
  - `Unavailable` AWS Backup Audit Manager가 현재 녹화 상태를 확인할 수 없는 경우

  `Partially active` 또는 **`Inactive`** 상태를 수정하려면

  1. 왼쪽 탐색 창에서 프레임워크를 선택합니다.
  2. 리소스 추적 관리를 선택합니다.
  3. 팝업 창의 지시에 따라, 이전에 리소스 유형에 대해 활성화되지 않았던 기록을 활성화합니다.

프레임워크에 포함한 컨트롤에 기반하여 리소스 추적이 필요한 리소스 유형에 대한 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결의 리소스 구성 요소를 참조하세요.

- 배포 상태는 프레임워크의 배포 상태를 나타냅니다. 이 상태는 대개 `Completed`이지만 `Create in progress`, `Update in progress`, `Delete in progress`, `Failed`일 수도 있습니다.
  - `Failed` 상태는 프레임워크가 제대로 배포되지 않았음을 뜻합니다. 프레임워크를 삭제한 다음, AWS Backup 콘솔 또는 AWS Backup API를 통해 프레임워크를 다시 생성합니다.
- 규정 준수 컨트롤에는 모든 평가를 통과한 프레임워크 컨트롤의 수가 표시됩니다.
- 규정 미준수 컨트롤에는 하나 이상의 평가를 통과하지 못한 프레임워크 컨트롤의 수가 표시됩니다.

컨트롤 섹션에 다음과 같은 정보가 표시됩니다.

- 컨트롤 상태는 각 컨트롤의 규정 준수 상태를 뜻합니다. 컨트롤은 `Compliant` 상태일 수 있으며, 이는 모든 리소스가 평가를 통과했음을 의미합니다. `Non-compliant`는 하나 이상의 리소스가 평가를 통과하지 못했음을 의미하고, `Insufficient data`는 컨트롤이 평가 범위 내에서 평가할 리소스를 찾지 못했음을 의미합니다.
- 감사 프레임워크를 생성할 때 컨트롤을 사용자 지정한 방식에 따라, 평가 범위는 각 컨트롤을 하나 이상의 리소스 유형, 하나의 리소스 ID 또는 하나의 태그 키 및 태그 값으로 제한할 수 있습니다. 모든 필드가 비어 있는 경우(대시, '-'로 표시), 컨트롤은 적용 가능한 모든 리소스를 평가합니다.

규정 미준수 리소스 찾기

AWS Backup Audit Manager를 사용하면 두 가지 방법으로 규정을 준수하지 않는 리소스를 찾을 수 있습니다.

- 프레임워크 규정 준수 상태를 볼 경우 세부 정보 섹션에서 컨트롤 이름을 선택합니다. 그러면 AWS Config 콘솔로 이동하여 리소스 목록을 볼 수 있습니다. `Non-Compliant`
- 프레임워크가 포함된 리소스 규정 준수 템플릿으로 보고서 계획을 만든 후에는 보고서를 보고 모든 컨트롤에 대한 모든 `Non-Compliant` 리소스를 식별할 수 있습니다.

  또한 `Resource compliance report`에는 AWS Backup Audit Manager가 각 컨트롤을 마지막으로 평가한 시간이 표시됩니다.

감사 프레임워크 업데이트

기존의 감사 프레임워크에 대한 설명, 컨트롤, 파라미터를 업데이트할 수 있습니다.

기존 프레임워크를 업데이트하려면

1. AWS Backup 콘솔 왼쪽 탐색 창에서 프레임워크를 선택합니다.
2. 편집하려는 프레임워크를 해당 프레임워크 이름으로 선택합니다.
3. 편집을 선택합니다.

감사 프레임워크 업데이트

기존 프레임워크를 삭제하려면

1. AWS Backup 콘솔 왼쪽 탐색 창에서 프레임워크를 선택합니다.
2. 삭제하려는 프레임워크를 해당 프레임워크 이름으로 선택합니다.
3. 삭제를 선택합니다.
4. 프레임워크 이름을 입력하고 프레임워크 삭제를 선택합니다.

감사 보고서 작업

AWS Backup Audit Manager 보고서는 다음과 같이 자동으로 생성되는 AWS Backup 활동 증거입니다.

- 완료된 백업 작업의 종류 및 완료된 시기
- 백업한 리소스의 종류

보고서에는 두 가지 유형이 있습니다. 보고서를 생성할 경우, 생성하려는 유형을 선택합니다.

첫 번째 유형은 지난 24시간 동안 완료된 작업과 모든 활성화된 작업을 보여주는 작업 보고서입니다. 작업 보고서에는 `completed with issues` 상태가 표시되지 않습니다. 하나 이상의 상태 메시지가 있는 `Completed` 작업을 필터링하여 이 상태를 찾을 수 있습니다. AWS Backup 메시지에 주의를 기울이거나 조치를 취해야 하는 경우에만 상태 메시지가 `Completed` 작업 상태의 일부로 포함됩니다.

두 번째 유형의 보고서는 규정 준수 보고서입니다. 규정 준수 보고서는 리소스 수준 또는 적용 중인 다양한 컨트롤을 모니터링할 수 있습니다.

AWS Backup Audit Manager는 Amazon S3 버킷으로 일일 보고서를 전송합니다. 현재 리전 및 현재 계정에 대한 보고서인 경우, 보고서를 CSV 또는 JSON 형식으로 수신하도록 선택할 수 있습니다. 이렇게 선택하지 않을 경우에는 보고서가 CSV 형식으로 제공됩니다. AWS Backup Audit Manager가 성능을 유지하기 위해 무작위화를 수행하므로 일일 보고서 작성 시간은 몇 시간에 걸쳐 변동될 수 있습니다. 언제든지 온디맨드 보고서를 실행할 수도 있습니다.

모든 계정 소유자는 교차 리전 보고서를 생성할 수 있으며, 관리 및 위임 관리자 계정 소유자도 교차 계정 보고서를 생성할 수 있습니다.

보고서 계획은 한 개당 최대 20개까지 만들 수 있습니다. AWS 계정

> **Note**
>
> RDS처럼 특정 백업의 증분 데이터 바이트를 표시할 수 있는 기능이 없는 리소스는 `backupSizeInBytes` 값을 0으로 표시합니다.

AWS Backup Audit Manager에서 일일 또는 온디맨드 보고서를 생성할 수 있게 하려면 먼저 보고서 템플릿에서 보고서 계획을 만들어야 합니다.

주제

- 보고서 템플릿 선택
- AWS Backup 콘솔을 사용하여 보고서 계획 생성
- API를 사용하여 보고서 계획 생성 AWS Backup
- 온디맨드 보고서 생성
- 감사 보고서 보기
- 보고서 계획 업데이트
- 보고서 계획 삭제

보고서 템플릿 선택

보고서 템플릿은 보고서 계획이 보고서에 포함하는 정보를 정의합니다. 보고서 계획을 사용하여 보고서를 자동화하면 AWS Backup Audit Manager에서 이전 24시간 동안의 보고서를 제공합니다. AWS Backup Audit Manager는 UTC 기준 오전 1시에서 5시 사이에 이러한 보고서를 생성합니다. 다음과 같은 보고서 템플릿을 제공합니다.

백업 보고서 템플릿

백업 보고서 템플릿. 이 템플릿은 백업, 복원 또는 복사 작업에 대한 일일 업데이트를 제공합니다. 이러한 보고서를 사용하여 운영 상태를 모니터링하고 추가 조치가 필요할지도 모르는 장애 문제를 식별할 수 있습니다. 다음 표에는 각 백업 보고서 템플릿 이름 및 샘플 출력이 나와 있습니다.

백업 보고서 템플릿	JSON 형식의 샘플 보고서
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75", "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb", "creationDate": "2021-07-14T23:53:47.229Z", "completionDate": "2021-07-15T00:16:07.282Z", "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5a6dcdf", "jobRunTime": "00:22:20", "backupSizeInBytes": 8589934592, "backupVaultName": "Default",

백업 보고서 템플릿	JSON 형식의 샘플 보고서

```
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

백업 보고서 템플릿	JSON 형식의 샘플 보고서

COPY_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	"jobStatus": "RUNNING",
	"resourceType": "EC2",
	"resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	"backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	"backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	"creationDate": "2021-07-15T15:42:04.771Z",
	"backupSizeInBytes": 8589934592,
	"sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	"destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	"destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}

백업 보고서 템플릿	JSON 형식의 샘플 보고서
	<pre>] }</pre>

RESTORE_JOB_REPORT	<pre>{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-
	14T15:53:30Z - 2021-07-15T15:53:3
	0Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "restoreJobId": "4CACA67D-4E12-
	DC05-6C2B-0E97D01FA41E",
	      "jobStatus": "RUNNING",
	      "recoveryPointArn": "arn:aws:
	ec2:us-west-2::image/ami-00
	201ecb57a5271ae",
	      "creationDate": "2021-07-
	15T15:52:49.797Z",
	      "backupSizeInBytes": 858993459
	2,
	      "percentDone": "0.00%",
	      "iamRoleArn": "arn:aws:
	iam::112233445566:role/service-
	role/AWSBackupDefaultServiceRole"
	    }
	  ]
	}</pre>

규정 준수 보고서 템플릿

규정 준수 보고서 템플릿은 하나 이상의 프레임워크에서 정의한 컨트롤을 기준으로 백업 활동 및 리소스의 규정 준수에 대한 일일 보고서를 제공합니다. 규정 준수 상태가 `Non-compliant`인 프레임워크가 있는 경우, 규정 준수 보고서를 검토하여 규정 미준수 리소스를 식별하세요.

규정 준수 보고서 템플릿의 유형

- `Control compliance report` - 프레임워크에 정의한 컨트롤의 규정 준수 상태를 추적할 수 있습니다.

- `Resource compliance report` - 프레임워크에 정의한 컨트롤을 기준으로 리소스의 규정 준수 상태를 추적할 수 있습니다. 이 보고서에는 이러한 리소스를 식별하고 수정하는 데 사용할 수 있는 규정 미준수 리소스에 대한 식별 정보를 비롯하여, 자세한 평가 결과가 포함됩니다.

다음 표에서는 규정 준수 보고서의 출력 샘플을 보여 줍니다.

규정 준수 보고서 템플릿	JSON 형식의 샘플 보고서
CONTROL_COMPLIANCE_REPORT	{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_R ESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08- 17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_H ours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_P LAN_MIN_FREQUENCY_AND_MIN_R ETENTION_CHECK",

규정 준수 보고서 템플릿	JSON 형식의 샘플 보고서


```
      "controlComplianceStatus":
 "NON_COMPLIANT",
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

규정 준수 보고서 템플릿	JSON 형식의 샘플 보고서

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

AWS Backup 콘솔을 사용하여 보고서 계획 생성

보고서에는 두 가지 유형이 있습니다. 첫 번째 유형은 지난 24시간 동안 완료된 작업과 모든 활성화된 작업을 보여주는 작업 보고서입니다. 두 번째 유형의 보고서는 규정 준수 보고서입니다. 규정 준수 보고서는 리소스 수준 또는 적용 중인 다양한 컨트롤을 모니터링할 수 있습니다. 보고서를 생성할 경우, 생성하려는 보고서 유형을 선택합니다.

참고: 계정 유형에 따라 콘솔 디스플레이가 달라질 수 있습니다. 관리 계정에만 다중 계정 기능이 표시됩니다.

백업 계획과 마찬가지로, 보고서 생성을 자동화하고 해당 보고서의 대상 Amazon S3 버킷을 정의하는 보고서 계획을 만듭니다. 보고서 계획에는 보고서를 수신할 S3 버킷이 있어야 합니다. 새 S3 버킷 설정에 대한 지침은 Amazon Simple Storage Service 사용 설명서의 1단계: 첫 번째 S3 버킷 생성을 참조하세요.

AWS Backup 콘솔에서 보고서 계획을 만들려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 생성을 선택합니다.
4. 드롭다운 목록에서 보고서 템플릿 중 하나를 선택합니다.
5. 고유한 보고서 계획 이름을 입력합니다. 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자여야 합니다.
6. (선택 사항) 보고서 계획 설명을 입력합니다.
7. 규정 준수 보고서 템플릿은 한 계정에만 사용할 수 있습니다. 보고하려는 프레임워크를 하나 이상 선택합니다. 보고서 계획에는 최대 1,000개의 프레임워크를 추가할 수 있습니다.

    1. 드롭다운을 사용하여 AWS 지역을 선택합니다.
    2. 드롭다운 메뉴를 사용하여 해당 리전에서 프레임워크를 선택합니다.
    3. 프레임워크 추가를 선택합니다.
8. (선택 사항) 보고서 계획에 태그를 추가하려면 보고서 계획에 태그 추가를 선택합니다.
9. 관리 계정을 사용하는 경우, 이 보고서 계획에 포함할 계정을 지정할 수 있습니다. 내 계정만을 선택할 수 있습니다. 이렇게 하면 현재 로그인한 계정의 보고서만 생성됩니다. 또는 내 조직에서 하나 이상의 계정을 선택할 수 있습니다 (관리 및 위임된 관리자 계정만 사용 가능).

10. (한 리전에 대해서만 규정 준수 보고서를 만들려면 이 단계를 건너뜁니다.) 보고서에 포함할 리전을 선택할 수 있습니다. 드롭다운 메뉴를 클릭하면 사용 가능한 리전이 표시됩니다. 사용 가능한 모든 리전 또는 원하는 지역을 선택합니다.

    - Backup Audit Manager에 새 리전을 통합할 때 새 리전 포함 확인란을 선택할 경우, 새 리전이 사용 가능해지면 보고서에 새 리전이 포함됩니다.

11. 보고서의 파일 형식을 선택합니다. 모든 보고서를 CSV 형식으로 내보낼 수 있습니다. 또한 단일 리전에 대한 보고서를 JSON 형식으로 내보낼 수 있습니다.
12. 드롭다운 목록을 사용하여 S3 버킷 이름을 선택합니다.
13. (선택 사항) 버킷 접두사를 입력합니다.

    AWS Backup 현재 계정, 현재 지역 보고서를 에 `s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name` 전달합니다.

    AWS Backup 교차 계정 보고서를 다음 주소로 전달합니다. `s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name`

    AWS Backup 지역 간 보고서를 다음 주소로 전송합니다. `s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name`
14. 보고서 계획 생성을 선택합니다.

다음으로, S3 버킷이 보고서를 AWS Backup수신할 수 있도록 허용해야 합니다. 보고서 계획을 생성한 후 AWS Backup Audit Manager는 적용할 S3 버킷 액세스 정책을 자동으로 생성합니다.

사용자 지정 KMS 키를 사용하여 버킷을 암호화하는 경우 KMS 키 정책은 다음 요구 사항을 충족해야 합니다.

- `Principal`속성에는 Backup Audit Manager 서비스 연결 역할 `AWSServiceRolePolicyForBackupReports`ARN이 포함되어야 합니다.

- `Action`속성에는 최소한 가 포함되어야 합니다`kms:GenerateDataKey`. `kms:Decrypt`

`AWSServiceRolePolicyForBackupReports`정책에는 이러한 권한이 있습니다.

이 액세스 정책을 보고 S3 버킷에 적용하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 이름에서 해당하는 이름을 선택하여 보고서 계획을 선택합니다.
4. 편집을 선택합니다.
5. S3 버킷에 대한 액세스 정책 보기를 선택합니다. 이 절차의 마지막 부분에서 정책을 사용할 수도 있습니다.
6. 권한 복사를 선택합니다.
7. 버킷 정책 편집을 선택합니다. 단, 백업 보고서가 처음 생성되기 전까지는 S3 버킷 정책에서 참조하는 서비스 연결 역할이 아직 존재하지 않으므로 “잘못된 주체”라는 오류가 발생합니다.
8. 권한을 정책에 복사합니다.

버킷 정책 샘플

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

사용자 AWS Key Management Service 지정을 사용하여 보고서를 저장하는 대상 S3 버킷을 암호화하는 경우 정책에 다음 작업을 포함하십시오.

```
      "Action":[
```

```
        "kms:GenerateDataKey",
        "kms:Encrypt"
      ],
      "Resource":[
        "*"
      ],
```

API를 사용하여 보고서 계획 생성 AWS Backup

프로그래밍 방식으로 보고서 계획을 사용할 수도 있습니다.

보고서에는 두 가지 유형이 있습니다. 첫 번째 유형은 지난 24시간 동안 완료된 작업과 모든 활성화된 작업을 보여주는 작업 보고서입니다. 두 번째 유형의 보고서는 규정 준수 보고서입니다. 규정 준수 보고서는 리소스 수준 또는 적용 중인 다양한 컨트롤을 모니터링할 수 있습니다. 보고서를 생성할 경우, 생성하려는 보고서 유형을 선택합니다.

백업 계획과 마찬가지로, 보고서 생성을 자동화하고 해당 보고서의 대상 Amazon S3 버킷을 정의하는 보고서 계획을 만듭니다. 보고서 계획에는 보고서를 수신할 S3 버킷이 있어야 합니다. 새 S3 버킷 설정에 대한 지침은 Amazon Simple Storage Service 사용 설명서의 1단계: 첫 번째 S3 버킷 생성을 참조하세요.

사용자 지정 KMS 키를 사용하여 버킷을 암호화하는 경우 KMS 키 정책은 다음 요구 사항을 충족해야 합니다.

- `Principal`속성에는 Backup Audit Manager 서비스 연결 역할 `AWSServiceRolePolicyForBackupReports`ARN이 포함되어야 합니다.

- `Action`속성에는 최소한 가 포함되어야 합니다`kms:GenerateDataKey`. `kms:Decrypt`

AWSServiceRolePolicyForBackupReports정책에는 이러한 권한이 있습니다.

단일 계정, 단일 리전 보고서의 경우 다음 구문을 사용하여 CreateReportPlan을 호출합니다.

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
```

```
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
   },
   "ReportPlanTags": {
       "string" : "string" // Optional.
   },
   "IdempotencyToken": "string"
}
```

보고서 계획의 고유한 이름을 사용하여 DescribeReportPlan을 호출하면 AWS Backup API는 다음과 같은 정보로 응답합니다.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

다중 계정, 다중 리전 보고서의 경우 다음 구문을 사용하여 CreateReportPlan을 호출합니다.

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
```

```
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ], // Use string value of "ROOT" to include all
 organizational units
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"], // Use wildcard value in string to include all Regions
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

보고서 계획의 고유한 이름을 사용하여 DescribeReportPlan을 호출하면 AWS Backup API는 다중 계정, 다중 리전 계획에 대한 다음과 같은 정보로 응답합니다.

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
         "Regions": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "ReportTemplate": "string"
      }
   }
}
```

온디맨드 보고서 생성

다음 단계에 따라 온디맨드 보고서를 생성하여 편리하게 새 보고서를 생성할 수 있습니다. AWS Backup Audit Manager는 보고서 계획에 지정된 Amazon S3 버킷으로 온디맨드 보고서를 전송합니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 이름에서 해당하는 이름을 선택하여 보고서 계획을 선택합니다.
4. 온디맨드 보고서 생성을 선택합니다.

기존 보고서 계획에 대한 온디맨드 보고서를 생성할 수 있습니다.

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 아래에서, 보고서 계획 이름 옆에 있는 라디오 버튼을 클릭하여 보고서 계획을 선택합니다.
4. 작업을 클릭한 다음, 온디맨드 보고서 생성을 클릭합니다.

보고서가 생성되는 동안에도 여러 보고서에 대해 이 작업을 수행할 수 있습니다.

감사 보고서 보기

CSV 또는 JSON 파일 작업에 일반적으로 사용하는 프로그램을 사용하여 AWS Backup Audit Manager 보고서를 열고, 보고, 분석할 수 있습니다. 다중 리전 또는 다중 계정에 대한 보고서는 CSV 형식으로만 제공된다는 점에 유의하세요.

총 파일 크기가 50MB를 초과할 경우 대용량 파일은 여러 개의 보고서로 분할됩니다. 결과 파일이 50MB를 초과하는 경우 AWS Backup Audit Manager는 보고서의 나머지 부분을 사용하여 추가 CSV 파일을 생성합니다.

보고서를 보려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 이름에서 해당하는 이름을 선택하여 보고서 계획을 선택합니다.
4. 보고서를 보려면 보고서 작업 아래에서 보고서 링크를 클릭합니다.

5. 보고서의 보고서 상태에 점선 밑줄이 있는 경우, 해당 항목을 선택하여 보고서에 대한 정보를 확인하세요.
6. 완료 시간을 기준으로 어떤 보고서를 볼지 선택합니다.
7. S3 링크를 선택합니다. 이렇게 하면 대상 S3 버킷이 열립니다.
8. 이름 아래에서, 보려는 보고서의 이름을 선택합니다.
9. 보고서를 컴퓨터에 저장하려면 다운로드를 선택합니다.

보고서 계획 업데이트

기존 보고서 계획의 설명, 전달 대상, 형식을 업데이트할 수 있습니다. 해당하는 경우, 보고서 계획에 프레임워크를 추가하거나 보고서 계획에서 프레임워크를 제거할 수도 있습니다.

기존 보고서 계획을 업데이트하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 이름에서 해당하는 이름을 선택하여 보고서 계획을 선택합니다.
4. 편집을 선택합니다.
5. 보고서 이름, 설명, 보고서에 포함되는 계정 및 리전 등 보고서 계획의 세부 정보를 편집할 수 있습니다.

보고서 계획 삭제

기존 보고서 계획을 삭제할 수 있습니다. 보고서 계획을 삭제할 경우, 이러한 보고서 계획으로 기존에 생성된 모든 보고서는 대상 Amazon S3 버킷에 남아 있게 됩니다.

기존 보고서 계획을 삭제하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 보고서를 선택합니다.
3. 보고서 계획 이름에서 해당하는 이름을 선택하여 보고서 계획을 선택합니다.
4. 삭제를 선택합니다.
5. 보고서 계획의 이름을 입력한 다음, 보고서 계획 삭제를 선택합니다.

AWS Backup Audit Manager를 다음과 함께 사용 AWS CloudFormation

참조할 수 있도록 다음과 같은 샘플 AWS CloudFormation 템플릿을 제공합니다.

주제

리소스 추적 켜기

다음 템플릿은 리소스 추적 켜기에 설명된 대로 리소스 추적을 켭니다.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
```

```
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
  AllSupported:
    Type: String
    Default: True
    Description: Indicates whether to record all supported resource types.
    AllowedValues:
      - True
      - False

  IncludeGlobalResourceTypes:
    Type: String
    Default: True
    Description: Indicates whether AWS Config records all supported global resource
 types.
    AllowedValues:
      - True
      - False

  ResourceTypes:
    Type: List<String>
    Description: A list of valid AWS resource types to include in this recording group,
 such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
    Default: <All>

  DeliveryChannelName:
    Type: String
    Default: <Generated>
    Description: The name of the delivery channel.

  Frequency:
    Type: String
```

```
    Default: 24hours
    Description: The frequency with which AWS Config delivers configuration snapshots.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours

  TopicArn:
    Type: String
    Default: <New Topic>
    Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
 Service (Amazon SNS) topic that AWS Config delivers notifications to.

  NotificationEmail:
    Type: String
    Default: <None>
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>

Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
```

```
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
```

```
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"

  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config
```

```
  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

기본 컨트롤 배포

다음 템플릿은 AWS Backup Audit Manager 컨트롤 및 문제 해결에 설명된 기본 컨트롤을 포함하는 프레임워크를 생성합니다.

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

컨트롤 평가에서 IAM 역할 제외

BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED 컨트롤을 사용하면 복구 시점을 여전히 수동으로 삭제할 수 있는 IAM 역할을 최대 5개까지 제외할 수 있습니다. 다음 템플릿은 이 컨트롤을 배포하고 IAM 역할 두 개도 제외합니다.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

보고서 계획 생성

다음 템플릿은 보고서 계획을 생성합니다.

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"
```

```
Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"

Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

AWS Backup Audit Manager를 다음과 함께 사용 AWS Audit Manager

AWS Backup Audit Manager 컨트롤은 사전 구축된 표준 컨트롤에 AWS Audit Manager매핑되므로 AWS Backup Audit Manager 규정 준수 결과를 AWS Audit Manager 보고서로 가져올 수 있습니다. 조직의 전반적인 규정 준수 태세의 일환으로 백업 활동을 보고하는 규정 준수 책임자, 감사 관리자 또는 그 밖의 동료에게 도움을 주려면 이러한 작업을 수행하는 것이 좋습니다.

AWS Backup Audit Manager 컨트롤의 규정 준수 결과를 AWS Audit Manager 프레임워크로 가져올 수 있습니다. AWS Backup Audit Manager 컨트롤에서 데이터를 자동으로 수집할 수 있도록 AWS Audit Manager 하려면 AWS Audit Manager 사용 설명서의 기존 컨트롤 사용자 지정 지침에 따라 사용자 지정 컨트롤을AWS Audit Manager 만드세요. 이 지침을 따를 때 AWS Backup 컨트롤의 데이터 소스는 다음과 같다는 점에 유의하십시오. AWS Config

AWS Backup 컨트롤 목록은 컨트롤 선택을 참조하십시오.

컨트롤 및 문제 해결

이 페이지에는 AWS Backup Audit Manager에 사용할 수 있는 컨트롤이 나열되어 있습니다. 알맞은 정보 창을 선택하여 컨트롤 목록을 확인하고 특정 컨트롤로 이동할 수 있습니다. 컨트롤을 빠르게 비교하려면 컨트롤 선택의 표를 참조하세요. 컨트롤을 프로그래밍 방식으로 정의하려면 AWS Backup API를 사용하여 프레임워크 생성의 코드 스니펫을 참조하세요.

리전별로 계정당 최대 50개의 컨트롤을 사용할 수 있습니다. 서로 다른 두 프레임워크에서 동일한 컨트롤을 사용하는 것은 컨트롤 한도 50개 중에서 컨트롤 두 개를 사용하는 것과 같습니다.

이 페이지에는 다음 정보와 함께 각 컨트롤이 나열되어 있습니다.

- 설명. 대괄호 안의 값("[]") 은 기본 파라미터 값입니다.
- 컨트롤이 평가하는 리소스.
- 컨트롤의 파라미터.
- 컨트롤 실행이 발생하는 경우.
- 제어 범위는 다음과 같습니다.
  - AWS Backup지원 서비스를 하나 이상 선택하여 유형별로 리소스를 지정할 수 있습니다.
  - 단일 태그 키와 선택적인 값을 사용하여 태그가 지정된 리소스 범위를 지정합니다.
  - 단일 리소스 드롭다운 목록을 사용하여 단일 리소스를 지정할 수 있습니다.
- 적용 가능한 리소스를 규정 준수에 적용하기 위한 문제 해결 단계.

컨트롤이 리소스의 규정 준수 여부를 평가할 경우 활성 리소스만 포함됩니다. 예를 들어, 실행 중인 상태의 Amazon EC2 인스턴스는 마지막 복구 시점이 생성되었습니다라는 컨트롤에 의해 평가됩니다. 중단된 상태의 EC2 인스턴스는 규정 준수 평가에 포함되지 않습니다.

백업 리소스가 백업 계획에 의해 보호됨

설명: 리소스가 백업 계획에 의해 보호되고 있는지 평가합니다.

리소스: `AWS Backup: backup selection`

파라미터: 없음

발생: 24시간마다 자동으로 발생

범위:

- 태그가 지정된 리소스

- 유형별 리소스(기본값)
- 단일 리소스

문제 해결: 백업 계획에 리소스를 할당합니다. AWS Backup 은 백업 계획에 리소스를 할당한 후 리소스를 자동으로 보호합니다. 자세한 내용은 백업 계획에 리소스 할당을 참조하세요.

백업 계획 최소 빈도 및 최소 보존

설명: 백업 계획에 백업 빈도가 [1일] 이상이고 보존 기간이 [35일] 이상인 백업 규칙이 하나 이상 포함되어 있는지 평가합니다.

리소스: `AWS Backup: backup plans`

파라미터:

- 필수 백업 빈도(시간 또는 일수)
- 필수 보존 기간(일, 주, 월 또는 년) 추가 비용이 발생하지 않도록 가능하면 증분 백업을 수행할 수 AWS Backup 있도록 최소 1주일의 웜 스토리지 보존 기간을 권장합니다.

발생: 구성 변경

범위:

- 태그가 지정된 리소스
- 단일 리소스

수정: 백업 계획을 업데이트하여 백업 빈도, 보존 기간 또는 두 가지 모두를 변경합니다. 백업 계획을 업데이트할 경우, 업데이트 후 계획에서 생성하는 복구 시점의 보존 기간이 변경됩니다.

저장소가 복구 시점의 수동 삭제를 방지함

설명: 백업 저장소에서 특정 IAM 역할을 제외한 복구 시점의 수동 삭제를 허용하지 않는지 평가합니다.

리소스: `AWS Backup: backup vaults`

파라미터: IAM 역할(최대 5개)의 Amazon 리소스 이름(ARN)을 사용하여 복구 시점을 수동으로 삭제할 수 있습니다.

발생: 구성 변경

범위:

- 태그가 지정된 리소스
- 단일 리소스

문제 해결: 백업 저장소에 리소스 기반 액세스 정책을 생성하거나 수정합니다. 백업 저장소 액세스 정책을 설정하는 방법에 대한 정책 예시 및 지침을 보려면 백업 저장소에서 복구 시점 삭제에 대한 액세스 거부를 참조하세요.

복구 시점이 암호화됨

설명: 복구 시점이 암호화되었는지 평가합니다.

리소스: `AWS Backup: recovery points`

파라미터: 없음

발생: 구성 변경

범위:

- 태그가 지정된 리소스

문제 해결: 복구 시점의 암호화를 구성합니다. AWS Backup 복구 지점의 암호화를 구성하는 방법은 리소스 유형에 따라 다릅니다.

사용 AWS Backup시 전체 AWS Backup 관리를 지원하는 리소스 유형에 대해 암호화를 구성할 수 있습니다. 리소스 유형이 전체 AWS Backup 관리를 지원하지 않는 경우 해당 서비스의 지침 (예: Amazon Elastic Compute Cloud 사용 설명서의 Amazon EBS 암호화) 에 따라 백업 암호화를 구성해야 합니다. 전체 AWS Backup 관리를 지원하는 리소스 유형 목록을 보려면 리소스별 기능 가용성 표의 “전체 AWS Backup 관리” 섹션을 참조하십시오.

복구 시점에 설정된 최소 보존 기간

설명: 복구 시점 보존 기간이 [35일] 이상인지 평가합니다.

리소스: `AWS Backup: recovery points`

파라미터: 필수 복구 시점 보존 기간(일, 주, 월 또는 년) 가능한 경우 추가 비용을 피하면서 증분 백업을 수행할 수 AWS Backup 있도록 최소 1주 이상의 웜 스토리지 보존 기간을 권장합니다.

발생: 구성 변경

범위:

- 태그가 지정된 리소스

문제 해결: 복구 시점의 보존 기간을 변경합니다. 자세한 내용은 백업 편집을 참조하세요.

교차 리전 백업 복사본이 예약됨

설명: 리소스가 백업 사본을 다른 AWS 지역에 생성하도록 구성되어 있는지 평가합니다.

리소스: `AWS Backup: backup selection`

파라미터:

- 백업 사본이 AWS 리전있어야 하는 위치를 선택합니다 (선택 사항).
- 지역

발생: 24시간마다 자동으로

범위:

- 태그가 지정된 리소스
- 유형별 리소스
- 단일 리소스

수정: 백업 계획을 업데이트하여 백업 사본이 있어야 하는 AWS 리전 위치를 변경하십시오.

교차 계정 백업 복사본이 예약됨

설명: 리소스가 다른 계정에 백업 복사본을 만들도록 구성되어 있는지 평가합니다. 평가할 계정에 대해 최대 5개의 계정을 추가할 수 있습니다. 대상 계정은 AWS Organizations의 소스 계정과 동일한 조직에 있어야 합니다.

리소스: `AWS Backup: backup selection`

파라미터:

- 백업 사본이 있어야 하는 AWS 계정 ID 선택 (선택 사항)

- 계정 ID

발생: 24시간마다 자동으로

범위:

- 태그가 지정된 리소스
- 유형별 리소스
- 단일 리소스

수정: 백업 계획을 업데이트하여 사본이 있어야 하는 AWS 계정 ID를 변경하거나 추가하십시오.

백업은 AWS Backup Vault Lock으로 보호됩니다.

설명: 잠긴 백업 저장소에 변경 불가능한 백업이 저장되어 있는지 리소스를 평가합니다.

리소스: `AWS Backup: backup selection`

파라미터:

- AWS Backup Vault Lock의 최소 및 최대 보존 기간 입력 (선택 사항)
- 최소 보존 일수
- 최대 보존 일수

발생: 24시간마다 자동

범위:

- 태그가 지정된 리소스
- 유형별 리소스
- 단일 리소스

문제 해결: 백업 저장소를 잠가서 이름을 설정하고 최소 보존 일수, 최대 보존 일수 또는 두 가지 모두를 변경합니다. 규정 준수 모드의 저장소 잠금에 `ChangeableForDays`를 포함할 수도 있습니다.

마지막 복구 시점이 생성됨

설명: 이 컨트롤은 지정된 기간(일수 또는 시간) 내에 복구 시점이 생성되었는지 평가합니다.

리소스에 지정된 기간 내에 복구 시점이 생성된 경우 컨트롤은 규정을 준수한 것입니다. 지정된 일수 또는 시간 내에 복구 시점이 생성되지 않은 경우 컨트롤은 규정을 준수하지 않은 것입니다.

리소스: `AWS Backup: recovery points`

파라미터:

- 지정된 기간을 정수(시간 또는 일 단위)로 입력합니다.
- `hours` 값의 범위는 `1~744`입니다.
- `days` 값의 범위는 `1~31`입니다.

발생: 24시간마다 자동으로 발생

범위:

- 태그가 지정된 리소스
- 유형별 리소스
- 단일 리소스

문제 해결:

- 백업 계획을 업데이트하여 복구 시점 생성의 지정된 기간을 변경합니다.
- 온디맨드 백업을 생성할 수도 있습니다.

리소스 복원 시간 목표 충족

설명: 보호된 리소스의 복원이 목표 복원 시간 내에 완료되었는지 평가합니다.

이 컨트롤은 특정 리소스의 복원 시간이 목표 기간을 충족하는지 확인합니다. 리소스 유형의 `LatestRestoreExecutionTimeMinutes`가 분 단위로 `maxRestoreTime`보다 큰 경우 규칙은 NON_COMPLIANT입니다.

파라미터:

- `maxRestoreTime`(분)

발생: 24시간마다 자동으로 발생

범위:

- 태그가 지정된 리소스
- 유형별 리소스
- 단일 리소스

> **Note**
>
> AWS Backup 복원 시간에 대한 서비스 수준 계약 (SLA) 을 제공하지 않습니다. 복원 시간은 시스템 로드 및 용량에 따라 달라질 수 있으며, 동일한 리소스를 포함하는 복원의 경우에도 마찬가지입니다.

여러 곳에 걸친 AWS Backup 리소스 관리 AWS 계정

> **Note**
>
> 여러 AWS 계정 핀의 AWS Backup리소스를 관리하려면 먼저 계정이 AWS Organizations 서비스의 동일한 조직에 속해야 합니다.

의 교차 계정 관리 기능을 사용하여 구성한 전체의 백업, 복원 및 복사 작업을 관리하고 AWS 계정 모니터링할 수 있습니다. AWS Backup AWS OrganizationsAWS Organizations단일 관리 AWS 계정 계정에서 여러 계정에 대한 정책 기반 관리를 제공하는 서비스입니다. 백업 정책을 구현하는 방식을 표준화하여 수동 오류와 노력을 동시에 최소화할 수 있습니다. 고려하고 있는 기준을 충족하는 모든 계정의 리소스를 중앙 보기에서 쉽게 식별할 수 있습니다.

설정하면 AWS Organizations한 곳에서 모든 계정의 활동을 AWS Backup 모니터링하도록 구성할 수 있습니다. 또한 백업 정책을 생성하여 조직에 속한 선택된 계정에 적용하고 AWS Backup 콘솔에서 직접 전체 백업 작업 활동을 볼 수 있습니다. 이 기능을 이용해 백업 관리자는 단일 관리 계정에서 엔터프라이즈 전체에 걸쳐 있는 수백 개 계정의 백업 작업 상태를 효과적으로 모니터링할 수 있습니다. AWS Organizations 할당량이 적용됩니다.

예를 들어 특정 리소스에 대해 일일 백업을 수행하고 7일 동안 백업을 보관하는 백업 정책 A를 정의합니다. 백업 정책 A가 조직 전체에 적용되도록 선택합니다. (즉, 조직의 각 계정에 해당 백업 정책이 적용되므로 계정에 표시된 해당 백업 계획이 생성됩니다.) 그런 다음 Finance라는 OU를 생성하고 백업을 30일 동안만 보관하기로 결정합니다. 이 경우 수명 주기 값을 재정의하는 백업 정책 B를 정의하고 이를 Finance OU에 연결합니다. 그러면 지정된 모든 리소스에 대해 일일 백업을 수행하고 백업을 30일 동안 보관하는 새로운 효과적인 백업 계획이 Finance OU 아래의 모든 계정에 적용됩니다.

이 예에서는 백업 정책 A 및 백업 정책 B가 하나의 단일 백업 정책으로 병합되므로 Finance라는 OU 아래의 모든 계정에 대해 보호 전략이 정의됩니다. 조직의 기타 모든 계정은 백업 정책 A에 의해 여전히 보호됩니다. 병합은 동일한 백업 계획 이름을 공유하는 백업 정책의 경우에만 가능합니다. 또한 병합 없이 해당 계정에서 정책 A와 정책 B가 공존하도록 할 수 있습니다. 콘솔의 JSON 보기에서만 고급 병합 연산자를 사용할 수 있습니다. 병합 정책에 대한 자세한 내용은 정책, 정책 구문, 정책 상속 정의의 AWS Organizations 사용 설명서를 참조하세요. 추가 참조 및 사용 사례는 사용 중인 대규모의 백업 관리 블로그 AWS Backup및 AWS Organizations 사용 중인 대규모 백업 관리 동영상 자습서를 참조하십시오. AWS Organizations AWS Backup

교차 계정 관리 기능을 어디에서 사용할 수 있는지 알아보려면 AWS 지역별 기능 가용성을 참조하십시오.

교차 계정 관리를 사용하려면 다음 단계를 수행해야 합니다.

1. 에서 AWS Organizations 관리 계정을 만들고 관리 계정 아래에 계정을 추가하십시오.
2. 에서 교차 계정 관리 기능을 활성화하십시오. AWS Backup
3. 관리 계정 내 모든 AWS 계정 사용자에게 적용할 백업 정책을 만드세요.

> **Note**
>
> Organizations에서 관리하는 백업 계획의 경우 위임된 관리자 계정을 하나 이상 구성했더라도 관리 계정의 리소스 옵트인 설정이 멤버 계정의 설정을 재정의합니다. 위임된 관리자 계정은 향상된 기능을 갖춘 멤버 계정이며 관리 계정처럼 설정을 재정의할 수 없습니다.

4. 모든 위치에서 백업, 복원 및 복사 작업을 관리할 수 있습니다 AWS 계정.

주제

조직 내 관리 계정 생성

먼저 조직을 만들고 AWS 구성원 계정으로 구성해야 AWS Organizations합니다.

에서 AWS Organizations 관리 계정을 만들고 계정을 추가하려면

- 지침은 AWS Organizations 사용 설명서의 자습서: 조직 생성 및 구성을 참조하세요.

교차 계정 관리 활성화

에서 AWS Backup교차 계정 관리를 사용하려면 먼저 기능을 활성화 (즉, 옵트인) 해야 합니다. 기능을 활성화한 후 여러 계정의 동시 관리를 자동화할 수 있는 백업 정책을 생성할 수 있습니다.

교차 계정 관리를 활성화하려면

1. https://console.aws.amazon.com/backup/ AWS Backup 콘솔 에서 엽니다. 관리 계정의 보안 인증 정보를 사용하여 로그인해야 합니다.
2. 왼쪽 탐색 창에서 설정을 선택하여 교차 계정 관리 페이지를 엽니다.
3. 백업 정책 섹션에서 활성화를 선택합니다.

   이렇게 하면 모든 계정에 액세스할 수 있으며 동시에 조직의 여러 계정 관리를 자동화하는 정책을 생성할 수 있습니다.
4. 교차 계정 모니터링 섹션에서 활성화를 선택합니다.

   이렇게 하면 관리 계정에서 조직에 있는 모든 계정의 백업, 복사 및 복원 활동을 모니터링할 수 있습니다.

위임된 관리자

위임 관리를 사용하면 등록된 회원 계정에 할당된 사용자가 대부분의 AWS Backup 관리 작업을 편리하게 수행할 수 있습니다. 에서 AWS Organizations구성원 계정에 관리를 AWS Backup 위임하도록 선택하여 관리 계정 AWS Backup 외부에서 관리 권한을 조직 전체로 확장할 수 있습니다.

기본적으로 관리 계정은 정책을 편집하고 관리하는 데 사용되는 계정입니다. 위임된 관리자 기능을 사용하면 이러한 관리 기능을 지정한 멤버 계정에 위임할 수 있습니다. 그러면 해당 계정은 관리 계정 외에도 정책을 관리할 수 있습니다.

멤버 계정이 위임 관리를 위해 성공적으로 등록되면 해당 계정은 위임된 관리자 계정이 됩니다. 사용자가 아닌 계정이 위임된 관리자로 지정된다는 점에 유의하세요.

위임된 관리자 계정을 활성화하면 백업 정책을 관리하는 옵션이 허용되고, 관리 계정에 액세스할 수 있는 사용자 수가 최소화되며, 작업의 교차 계정 모니터링이 가능해집니다.

다음은 관리 계정, Backup 관리자로 위임된 계정, AWS 조직 내 구성원인 계정의 기능을 보여주는 표입니다.

> **Note**
>
> 위임된 관리자 계정은 향상된 기능을 갖춘 멤버 계정이지만 관리 계정처럼 다른 멤버 계정의 서비스 옵트인 설정을 재정의할 수 없습니다.

권한	관리 계정	위임된 관리자	멤버 계정
위임된 관리자 계정 등록/등록 취소	예	아니요	아니요
계정 전체의 백업 정책을 관리합니다. AWS Organizations	예	예	아니요
교차 계정 작업 모니터링	예	예	아니요

필수 조건

백업 관리를 위임하려면 먼저 AWS 조직의 구성원 계정을 하나 이상 위임 관리자로 등록해야 합니다. 계정을 위임된 관리자로 등록하려면 먼저 다음을 구성해야 합니다.

- AWS Organizations 기본 관리 계정 외에 하나 이상의 구성원 계정으로 활성화하고 구성해야 합니다.
- AWS Backup 콘솔에서 백업 정책, 계정 간 모니터링 및 계정 간 백업 기능이 켜져 있는지 확인하십시오. 이러한 항목은 콘솔의 위임된 관리자 창 아래에 있습니다. AWS Backup
  - 교차 계정 모니터링을 사용하여 관리 계정과 위임된 관리자 계정에서 조직의 모든 계정에 대한 백업 활동을 모니터링할 수 있습니다.
  - 선택 사항: 교차 계정 백업: 조직의 계정이 백업을 다른 계정에 복사할 수 있도록 합니다 (백업이 지원되는 교차 계정 리소스의 경우).
  - 를 사용하여 서비스 액세스를 활성화합니다. AWS Backup

위임된 관리를 설정하기 위해서는 두 가지 단계가 필요합니다. 첫 번째 단계는 교차 계정 작업 모니터링을 위임하는 것입니다. 두 번째 단계는 백업 정책 관리를 위임하는 것입니다.

멤버 계정을 위임된 관리자 계정으로 등록

첫 번째 섹션은 다음과 같습니다. AWS Backup 콘솔을 사용하여 계정 간 작업 모니터링을 위한 위임된 관리자 계정 등록. AWS Backup 정책을 위임하려면 다음 섹션의 Organizations 콘솔을 사용합니다.

AWS Backup 콘솔을 사용하여 멤버 계정을 등록하려면:

1. https://console.aws.amazon.com/backup/ AWS Backup 콘솔 에서 엽니다. 관리 계정의 보안 인증 정보를 사용하여 로그인해야 합니다.
2. 콘솔 왼쪽 탐색 창의 내 계정에서 설정을 선택합니다.
3. 위임된 관리자 창에서 위임된 관리자 등록 또는 위임된 관리자 추가를 클릭합니다.
4. 위임된 관리자 등록 페이지에서 등록하려는 계정을 선택한 다음, 계정 등록을 선택합니다.

이제 이 위임된 계정은 조직 내 계정 전체의 작업을 모니터링하고 정책을 보고 편집(정책 위임)할 수 있는 관리자 권한을 가진 위임된 관리자로 등록됩니다. 이 멤버 계정은 다른 위임된 관리자 계정을 등록하거나 등록 취소할 수 없습니다. 콘솔을 사용하여 최대 5개의 계정을 위임된 관리자로 등록할 수 있습니다.

프로그래밍 방식으로 멤버 계정을 등록하려면

`register-delegated-administrator` CLI 명령을 사용합니다. CLI 요청에서 다음과 같은 파라미터를 지정할 수 있습니다.

- `service-principal`
- `account-id`

아래는 프로그래밍 방식으로 멤버 계정을 등록하기 위한 CLI 요청의 예입니다.

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

멤버 계정 등록 취소

이전에 위임된 관리자로 지정된 AWS 조직의 구성원 계정을 등록 AWS Backup 취소하여 관리 액세스 권한을 제거하려면 다음 절차를 따르십시오.

콘솔을 사용하여 멤버 계정을 등록 취소하려면

1. https://console.aws.amazon.com/backup/ AWS Backup 콘솔 에서 엽니다. 관리 계정의 보안 인증 정보를 사용하여 로그인해야 합니다.
2. 콘솔 왼쪽 탐색 창의 내 계정에서 설정을 선택합니다.
3. 위임된 관리자 섹션에서 계정 등록 취소를 선택합니다.
4. 등록 취소할 계정을 선택합니다.
5. 계정 등록 취소 대화 상자에서 보안에 미치는 영향을 검토한 다음, `confirm`을 입력하여 등록 취소를 완료합니다.
6. `Deregister account`를 선택합니다.

프로그래밍 방식으로 멤버 계정을 등록 취소하려면

CLI 명령 `deregister-delegated-administrator`를 사용하여 위임된 관리자 계정의 등록을 취소합니다. API 요청에서 다음과 같은 파라미터를 지정할 수 있습니다.

- `service-principal`
- `account-id`

아래는 프로그래밍 방식으로 멤버 계정을 등록 취소하기 위한 CLI 요청의 예입니다.

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

를 통해 AWS Backup 정책을 위임하세요. AWS Organizations

AWS Organizations 콘솔 내에서 Backup 정책을 비롯한 여러 정책의 관리를 위임할 수 있습니다.

AWS Organizations 콘솔에 로그인한 관리 계정에서 조직의 리소스 기반 위임 정책을 생성하거나, 보거나, 삭제할 수 있습니다. 정책을 위임하는 단계는 AWS Organizations 사용 설명서의 리소스 기반 위임 정책 생성을 참조하세요.

백업 정책 생성

교차 계정 관리를 활성화한 후에는 관리 계정에서 교차 계정 백업 정책을 만듭니다.

> **Warning**
>
> JSON으로 정책을 생성하면 중복된 키 이름은 거부됩니다. 단일 정책에 여러 계획, 규칙 또는 선택 항목이 포함된 경우 각 키의 이름은 고유해야 합니다.

콘솔을 AWS Backup 통해 백업 정책을 생성합니다.

1. 왼쪽 탐색 창에서 백업 정책을 선택합니다. 백업 정책 페이지에서 백업 정책 생성을 선택합니다.
2. 세부 정보 섹션에서 백업 정책 이름을 입력하고 설명을 입력합니다.
3. 백업 계획 세부 정보 섹션에서 시각적 편집기 탭을 선택하고 다음을 수행합니다.
   a. 백업 계획 이름에 이름을 입력합니다.
   b. 리전 목록에서 리전을 선택합니다.
4. 백업 규칙 구성 섹션에서 백업 규칙 추가를 선택합니다.

   백업 계획당 최대 규칙 수는 10개입니다. 계획에 10개가 넘는 규칙이 포함된 경우 백업 계획은 무시되고 이 백업 계획을 기반으로 백업이 생성되지 않습니다.

   a. 규칙 이름에 규칙 이름을 입력합니다. 규칙 이름은 대소문자를 구분하며 영숫자 문자 또는 하이픈만 사용할 수 있습니다.
   b. 일정의 빈도 목록에서 백업 빈도를 선택하고 백업 기간 옵션 중 하나를 선택합니다. 백업 기간 기본값 사용—권장을 선택하는 것이 좋습니다.
5. 수명 주기에서 원하는 수명 주기 설정을 선택합니다.
6. 백업 저장소 이름에 이름을 입력합니다. 이는 백업에 의해 생성된 복구 시점이 저장되는 백업 저장소입니다.

   모든 계정에 백업 저장소가 있는지 확인하세요. AWS Backup 는 이를 확인하지 않습니다.
7. (선택 사항) 백업을 다른 AWS 리전지역으로 복사하려면 목록에서 대상 지역을 선택하고 태그를 추가합니다. 교차 리전 복사 설정과 상관없이, 생성된 복구 시점에 대한 태그를 선택할 수 있습니다. 또한 규칙을 더 추가할 수 있습니다.
8. 리소스 할당 섹션에서 AWS Identity and Access Management (IAM) 역할의 이름을 입력합니다. AWS Backup 서비스 역할을 사용하려면 다음을 제공하십시오`service-role/AWSBackupDefaultServiceRole`.

AWS Backup 각 계정에서 이 역할을 맡아 해당하는 경우 암호화 키 권한을 포함하여 백업 및 복사 작업을 수행할 수 있는 권한을 얻습니다. AWS Backup 또한 이 역할을 사용하여 수명 주기 삭제를 수행합니다.

> **Note**
>
> AWS Backup 역할이 존재하는지 또는 역할을 수임할 수 있는지 여부를 확인하지 않습니다.
> 교차 계정 관리를 통해 생성된 백업 계획의 경우 AWS Backup 관리 계정의 옵트인 설정을 사용하고 설정별 계정을 재정의합니다.
> 백업 정책을 추가하려는 각 계정에 대해 저장소 및 IAM 역할을 직접 생성해야 합니다.

9. 태그를 추가하여 백업할 리소스를 선택합니다. 허용되는 최대 태그 수는 30개입니다.

   AWS Organizations Organizations 정책을 통해 백업 계획을 생성하는 경우 정책을 통해 최대 30개의 태그를 지정할 수 있습니다. 여러 리소스 할당을 활용하거나 여러 백업 계획을 사용하여 추가 태그를 포함할 수 있습니다.

   기존 선택 항목을 수정하거나 사용하여 @@append 동일한 백업 선택 항목에서 태그 수가 30개를 초과하는 경우 백업 계획이 무효화되고 로컬 계정에서 제거됩니다.

10. 백업하려는 리소스가 Amazon EC2 인스턴스에서 Microsoft Windows를 실행하는 경우 고급 설정 섹션에서 Windows VSS를 선택합니다. 이렇게 하면 애플리케이션 일관성 Windows VSS 백업을 수행할 수 있습니다.

    > **Note**
    >
    > AWS Backup 현재 Amazon EC2에서 실행되는 애플리케이션 정합성이 보장되는 리소스 백업만 지원합니다. 모든 인스턴스 유형 또는 애플리케이션이 Windows VSS 백업에 대해 지원되는 것은 아닙니다. 자세한 정보는 Windows VSS 백업 생성을 참조하세요.

11. 백업 계획 추가를 선택하여 이를 정책에 추가한 다음 백업 정책 생성을 선택합니다.

    백업 정책을 생성해도 백업 정책을 계정에 연결하지 않으면 리소스가 보호되지 않습니다. 정책 이름을 선택하고 세부 정보를 볼 수 있습니다.

    다음은 백업 계획을 생성하는 예제 AWS Organizations 정책입니다. Windows VSS 백업을 활성화할 경우, 정책의 `advanced_backup_settings` 섹션에 표시된 대로 애플리케이션에 일관되게 적용되는 백업을 수행할 수 있는 권한을 추가해야 합니다.

```
{
  "plans": {
    "PiiBackupPlan": {
      "regions": {
        "@@append":[
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 0/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "60"
          },
          "complete_backup_window_minutes": {
            "@@assign": "604800"
          },
          "target_backup_vault_name": {
            "@@assign": "FortKnox"
          },
          "recovery_point_tags": {
            "owner": {
              "tag_key": {
                "@@assign": "Owner"
              },
              "tag_value": {
                "@@assign": "Backup"
              }
            }
          },
          "lifecycle": {
            "delete_after_days": {
              "@@assign": "365"
            },
            "move_to_cold_storage_after_days": {
              "@@assign": "180"
            }
          },
          "copy_actions": {
```

```
            "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
 {
            "target_backup_vault_arn" : {
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        },
        "selections": {
          "tags": {
            "SelectionDataType": {
              "iam_role_arn": {
                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
              },
              "tag_key": {
                "@@assign": "dataType"
              },
              "tag_value": {
                "@@assign": [
                  "PII",
                  "RED"
                ]
              }
            }
          }
        },
        "backup_plan_tags": {
          "stage": {
            "tag_key": {
              "@@assign": "Stage"
            },
            "tag_value": {
              "@@assign": "Beta"
            }
          }
```

```
        }
      }
    }
  }
```

12. 대상 섹션에서, 정책에 연결하려는 조직 단위 또는 계정을 선택하고 연결을 선택합니다. 정책을 개별 조직 단위 또는 계정에 추가할 수도 있습니다.

> **Note**
>
> 정책을 검증하고 정책에 모든 필수 필드를 포함해야 합니다. 정책의 일부가 유효하지 않은 경우 AWS Backup 은 그러한 부분을 무시하며, 정책의 유효한 부분은 예상대로 작동합니다. 현재는 AWS Organizations 정책의 정확성을 검증하지 AWS Backup 않습니다.
> 한 정책을 관리 계정에 적용하고 멤버 계정에 다른 정책을 적용하여 정책이 충돌할 경우(예: 백업 보존 기간이 다른 경우), 두 정책 모두 문제 없이 실행됩니다. 즉, 정책이 계정마다 독립적으로 실행됩니다. 예를 들어 관리 계정 정책은 하루에 한 번 Amazon EBS 볼륨을 백업하고, 로컬 정책은 일주일에 한 번 EBS 볼륨을 백업하는 경우 두 정책 모두 실행됩니다.
> 계정에 적용될 유효 정책에 필수 필드가 누락된 경우(여러 정책 간의 병합으로 인한 가능성이 높음), AWS Backup 은 해당 정책을 계정에 전혀 적용하지 않습니다. 일부 설정이 유효하지 않은 경우 설정을 AWS Backup 조정합니다.

백업 정책으로 만든 백업 계획의 구성원 계정의 옵트인 설정과 관계없이 조직의 관리 계정에 지정된 옵트인 설정을 사용합니다. AWS Backup

조직 단위에 정책을 연결하면 이 조직 단위에 가입하는 모든 계정에는 이 정책이 자동으로 적용되며 조직 단위에서 제거된 모든 계정에서는 이 정책이 상실됩니다. 해당 백업 계획은 해당 계정에서 자동으로 삭제됩니다.

여러 AWS 계정계정의 활동 모니터링

계정 간 백업, 복사 및 복원 작업을 모니터링하려면 교차 계정 모니터링을 활성화해야 합니다. 이렇게 하면 조직 관리 계정에서 모든 계정의 백업 활동을 모니터링할 수 있습니다. 옵트인을 수행하면, 옵트인 이후에 생성된 조직에 걸쳐 있는 모든 작업이 표시됩니다. 옵트아웃을 수행하면, AWS Backup 은 (종단 상태에 도달하지 않고) 30일 동안 집계 보기에서 작업을 유지합니다. 옵트아웃 이후에 생성된 작업은 표시되지 않으며 새로 생성된 백업 작업도 표시되지 않습니다. 옵트인 지침은 교차 계정 관리 활성화 단원을 참조하십시오.

여러 계정을 모니터링하려면

1. https://console.aws.amazon.com/backup/ AWS Backup 콘솔 에서 엽니다. 관리 계정의 보안 인증 정보를 사용하여 로그인해야 합니다.
2. 왼쪽 탐색 창에서 설정을 선택하여 교차 계정 관리 페이지를 엽니다.
3. 교차 계정 모니터링 섹션에서 활성화를 선택합니다.

   이렇게 하면 관리 계정에서 조직에 있는 모든 계정의 백업 및 복원 활동을 모니터링할 수 있습니다.
4. 왼쪽 탐색 창에서 교차 계정 모니터링을 선택합니다.
5. 교차 계정 모니터링 페이지에서 백업 작업, 복원 작업 또는 복사 작업 탭을 선택하여 모든 계정에서 생성된 모든 작업을 표시합니다. 각 채용공고를 AWS 계정 ID로 볼 수 있으며, 특정 계정의 모든 채용공고를 볼 수 있습니다.
6. 검색 상자에서 계정 ID, 상태 또는 작업 ID별로 작업을 필터링할 수 있습니다.

   예를 들어 백업 작업 탭을 선택하여 모든 계정에서 생성된 모든 백업 작업을 볼 수 있습니다. 계정 ID별로 목록을 필터링하여 해당 계정에서 생성된 모든 백업 작업을 볼 수 있습니다.

리소스 옵트인 규칙

조직 수준 백업 정책에 따라 구성원 계정의 백업 계획을 생성한 경우 Organizations 관리 계정의 AWS Backup 옵트인 설정이 해당 멤버 계정의 옵트인 설정보다 우선하지만 해당 백업 플랜에만 적용됩니다.

멤버 계정에 사용자가 생성한 로컬 수준 백업 계획도 있는 경우, 해당 백업 계획은 Organizations 관리 계정의 옵트인 설정을 참조하지 않고 멤버 계정의 옵트인 설정을 따릅니다.

정책, 정책 구문, 정책 상속 정의

다음 항목은 사용 설명서에 설명되어 있습니다. AWS Organizations

- 백업 정책 - 백업 정책을 참조하세요.
- 정책 구문 - 백업 정책 구문 및 예제를 참조하세요.
- 관리 정책 유형에 대한 상속 - 관리 정책 유형에 대한 상속을 참조하세요.

AWS Backup 및 AWS CloudFormation

개요

AWS CloudFormation을 활용하면 생성한 템플릿을 사용하여 안전하고 반복 가능한 방식으로 AWS 리소스를 프로비저닝하고 관리할 수 있습니다. AWS CloudFormation 템플릿 및 StackSets를 사용하여 백업 계획, 백업 리소스 선택 및 백업 저장소를 관리할 수 있습니다. AWS CloudFormation 사용에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 작동 방식 섹션을 참조하세요.

AWS CloudFormation 템플릿 또는 StackSet을 생성하기 전에 다음 사항을 고려합니다.

- 백업 계획 및 백업 저장소에 대해 별도의 템플릿을 생성합니다. 비어 있는 백업 저장소만 삭제할 수 있습니다. 복구 시점이 들어 있는 백업 저장소가 포함된 스택은 삭제할 수 없습니다.
- 스택을 생성하기 전에 사용 가능한 서비스 역할이 있는지 확인합니다. 백업 계획에 리소스를 처음 할당할 때 AWS Backup 기본 서비스 역할이 생성됩니다. 백업 계획에 리소스를 할당하지 않은 경우 스택을 생성하기 전에 리소스를 할당하세요. 사용자가 생성한 사용자 지정 역할을 지정할 수도 있습니다. 역할에 대한 자세한 내용은 IAM 서비스 역할 단원을 참조하세요.

AWS CloudFormation을 사용하여 백업 저장소, 백업 계획, 리소스 할당 배포

백업 저장소, 백업 계획, 리소스 할당을 배포하는 AWS CloudFormation 템플릿 샘플을 보려면 를 사용하여 리소스를 할당합니다. AWS CloudFormation 섹션을 참조하세요.

AWS CloudFormation을 사용하여 백업 계획 배포

백업 계획을 배포하는 AWS CloudFormation 템플릿 샘플을 보려면 백업 계획을 위한 AWS CloudFormation 템플릿 섹션을 참조하세요.

AWS CloudFormation을 사용하여 AWS Backup Audit Manager 프레임워크 및 보고서 계획 배포

AWS Backup Audit Manager 프레임워크 및 보고서 계획을 배포하는 AWS CloudFormation 템플릿 샘플을 보려면 백업 계획을 위한 AWS CloudFormation 템플릿 섹션을 참조하세요.

AWS CloudFormation을 사용하여 계정 전체에 백업 계획 배포

AWS 조직의 여러 계정 전체에서 AWS CloudFormation StackSets를 사용할 수 있습니다. 템플릿 샘플은 AWS CloudFormation 사용 설명서에서 제공됩니다.

AWS Backup를 사용해 AWS 서비스 간 대규모로 중앙 백업 자동화 게시물은 작업을 시작하기 전에 보면 아주 좋은 참조 자료입니다. Ibukun Oyewumi 및 Sabith Venkitachalapathy 참여(2021년 7월).

AWS CloudFormation에 대해 자세히 알아보기

AWS CloudFormation을 AWS Backup와 함께 사용하는 방법에 대한 내용은 AWS CloudFormation 사용 설명서의 AWS Backup 리소스 유형 레퍼런스 섹션을 참조하세요.

AWS CloudFormation 사용 시 AWS 서비스 리소스에 대한 액세스 제어에 대한 내용은 AWS CloudFormation 사용 설명서의 AWS Identity and Access Management을 통한 액세스 제어 섹션을 참조하세요.

보안 내부 AWS Backup

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오. AWS Backup
- 클라우드 내부의 보안 - 귀하의 AWS Backup 책임에는 다음이 포함되며 이에 국한되지는 않습니다. 또한 데이터의 민감도, 조직의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.
  - 수신한 커뮤니케이션에 대한 응답 AWS.
  - 귀하의 조직에서 사용하는 보안 인증 정보를 관리. 자세한 내용은 의 ID 및 액세스 관리를 참조하십시오 AWS Backup.
  - 조직의 데이터 보호 정책을 반영하여 백업 계획 및 리소스 할당을 구성. 자세한 내용은 백업 계획 관리를 참조하세요.
  - 특정 복구 시점을 검색 및 복원하는 능력을 정기적으로 테스트. 자세한 내용은 백업 작업을 참조하세요.
  - 조직의 재해 복구 및 비즈니스 연속성 서면 AWS Backup 절차에 절차를 통합하십시오. 시작하려면 AWS Backup시작하기를 참조하세요.
  - 긴급 상황 발생 시 직원들이 조직 절차를 숙지하고 그에 AWS Backup 따른 사용을 연습하도록 하십시오. 자세한 내용은 AWS Well-Architected Framework를 참조하세요.

이 설명서는 공동 책임 모델을 사용할 AWS Backup때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS Backup 충족하도록 구성하는 방법을 보여줍니다. 또한 AWS Backup 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- 규정 준수 검증: AWS Backup

- 데이터 보호: AWS Backup
- 내 ID 및 액세스 관리 AWS Backup
- 의 인프라 보안 AWS Backup
- 데이터 무결성 AWS Backup
- 법적 보류 및 AWS Backup
- AWS PrivateLink
- 의 레질리언스 AWS Backup

규정 준수 검증: AWS Backup

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- HIPAA 보안 및 규정 준수를 위한 설계 Amazon Web Services— 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 데 사용할 수 있는 방법을 설명합니다. AWS

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연

구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

데이터 보호: AWS Backup

AWS Backup 데이터 보호를 위한 규정 및 지침을 포함하는 AWS 공동 책임 모델을 준수합니다. AWS 모든 AWS 서비스를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 고객 콘텐츠 및 개인 데이터 처리를 위한 보안 구성 제어를 포함하여 이 인프라에서 호스팅되는 데이터에 대한 제어를 유지합니다. AWS 데이터 컨트롤러 또는 데이터 처리자 역할을 하는 고객 및 AWS 파트너 네트워크 (APN) 파트너는 자신이 입력하는 모든 개인 데이터에 대한 책임을 집니다. AWS 클라우드

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 IAM AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자 계정을 설정하는 것이 좋습니다. 이는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여된다는 것을 의미합니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- 보안 소켓 계층(SSL)/전송 계층 보안(TLS)를 사용하여 AWS 리소스와 통신합니다.
- AWS 서비스 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오.

이름 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마십시오. 여기에는 콘솔 AWS CLI, API AWS Backup 또는 AWS SDK를 사용하여 다른 AWS 서비스를 사용하거나 작업하는 경우가 포함됩니다. AWS Backup 또는 기타 서비스에 입력하는 모든 데이터는 진단 로그

에 포함하기 위해 선택될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함시키지 마십시오.

데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오.

내 백업을 위한 암호화 AWS Backup

> **Note**
>
> AWS Backup Audit Manager를 사용하면 암호화되지 않은 백업을 자동으로 탐지할 수 있습니다.

사용 AWS Backup시 전체 AWS Backup 관리를 지원하는 리소스 유형에 대해 암호화를 구성할 수 있습니다. 리소스 유형이 전체 AWS Backup 관리를 지원하지 않는 경우 해당 서비스의 지침 (예: Amazon Elastic Compute Cloud 사용 설명서의 Amazon EBS 암호화) 에 따라 백업 암호화를 구성해야 합니다. 전체 AWS Backup 관리를 지원하는 리소스 유형 목록을 보려면 리소스별 기능 가용성 표의 “전체 AWS Backup 관리” 섹션을 참조하십시오.

다음 표에는 지원되는 각 리소스 유형, 백업에 대해 암호화가 구성되는 방법 및 백업에 대해 독립 암호화가 지원되는지 여부가 나와 있습니다. AWS Backup 은 독립적으로 백업을 암호화하는 경우 업계 표준 AES-256 암호화 알고리즘을 사용합니다.

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
Amazon Simple Storage Service(S3)	Amazon S3 백업은 백업 저장소와 연결된 AWS KMS (AWS Key Management Service) 키를 사용하여 암호화됩니다. AWS KMS 키는 고객 관리형 CMK 또는 서비스와 관련된 관리형 CMK일 수 있습니다. AWS AWS Backup AWS Backup 원본 Amazon S3 버킷이 암호화되지 않은 경우에도 모든 백업을 암호화합니다.	지원

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
VMware 가상 머신	VM 백업은 항상 암호화됩니다. 가상 컴퓨터 백업의 AWS KMS 암호화 키는 가상 컴퓨터 백업이 저장되는 AWS Backup 저장소에 구성됩니다.	지원
고급 DynamoDB 백업을 활성화한 후의 Amazon DynamoDB	DynamoDB 백업은 항상 암호화됩니다. DynamoDB 백업의 AWS KMS 암호화 키는 DynamoDB 백업이 저장되는 저장소에 구성됩니다. AWS Backup	지원
고급 DynamoDB 백업을 활성화하지 않은 Amazon DynamoDB	DynamoDB 백업은 소스 DynamoDB 테이블을 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 DynamoDB 테이블은 스냅샷도 암호화되지 않습니다. **Note** 암호화된 DynamoDB 테이블의 백업을 AWS Backup 생성하려면 백업에 사용되는 IAM 역할에 `kms:Decrypt` 권한을 `kms:GenerateDataKey` 추가해야 합니다. 또는 기본 서비스 역할을 사용할 수도 있습니다. AWS Backup	지원되지 않음

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
Amazon Elastic File System(Amazon EFS)	Amazon EFS 백업은 항상 암호화됩니다. Amazon EFS 백업의 AWS KMS 암호화 키는 Amazon EFS 백업이 저장되는 저장소에 구성됩니다. AWS Backup	지원
Amazon Elastic Block Store(Amazon EBS)	기본적으로 Amazon EBS 백업은 소스 볼륨을 암호화하는 데 사용된 키를 사용하여 암호화되거나 암호화되지 않습니다. 복원 중에 KMS 키를 지정하여 기본 암호화 방법을 재정의하도록 선택할 수 있습니다.	지원되지 않음
Amazon Elastic Compute Cloud(Amazon EC2) AMI	AMI는 암호화되지 않습니다. EBS 스냅샷은 EBS 백업의 기본 암호화 규칙에 따라 암호화됩니다 (EBS 항목 참조). 데이터 및 루트 볼륨의 EBS 스냅샷을 암호화하여 AMI에 연결할 수 있습니다.	지원되지 않음

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
Amazon Relational Database Service(Amazon RDS)	Amazon RDS 스냅샷은 소스 Amazon RDS 데이터베이스를 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Amazon RDS 데이터베이스는 스냅샷도 암호화되지 않습니다. **Note** AWS Backup 현재 Amazon Aurora를 포함한 모든 Amazon RDS 데이터베이스 엔진을 지원합니다.	지원되지 않음
Amazon Aurora	Aurora 클러스터 스냅샷은 소스 Amazon Aurora 클러스터를 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Aurora 클러스터는 스냅샷도 암호화되지 않습니다.	지원되지 않음

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
AWS Storage Gateway	Storage Gateway 스냅샷은 소스 Storage Gateway 볼륨을 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Storage Gateway 볼륨은 스냅샷도 암호화되지 않습니다. **Note** Storage Gateway를 활성화하기 위해 모든 서비스에서 고객 관리형 키를 사용할 필요는 없습니다. KMS 키를 구성한 볼트에 Storage Gateway 백업을 복사하기만 하면 됩니다. Storage Gateway에는 서비스별 AWS KMS 관리 키가 없기 때문입니다.	지원되지 않음
Amazon FSx	Amazon FSx 파일 시스템의 암호화 기능은 기본 파일 시스템에 따라 다릅니다. 특정 Amazon FSx 파일 시스템에 대해 자세히 알아보려면 해당 FSx 사용 설명서를 참조하세요.	지원되지 않음

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
Amazon DocumentDB	Amazon DocumentDB 클러스터 스냅샷은 소스 Amazon DocumentDB 클러스터를 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Amazon DocumentDB 클러스터는 스냅샷도 암호화되지 않습니다.	지원되지 않음
Amazon Neptune	Neptune 클러스터 스냅샷은 소스 Neptune 클러스터를 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Neptune 클러스터는 스냅샷도 암호화되지 않습니다.	지원되지 않음
Amazon Timestream	Timestream 테이블 스냅샷 백업은 항상 암호화됩니다. Timestream 백업에 대한 AWS KMS 암호화 키는 Timestream 백업이 저장되는 백업 볼트에 구성됩니다.	지원
Amazon Redshift	Amazon Redshift 클러스터는 소스 Amazon Redshift 클러스터를 암호화하는 데 사용된 동일한 암호화 키로 자동 암호화됩니다. 암호화되지 않은 Amazon Redshift 클러스터는 스냅샷도 암호화되지 않습니다.	지원되지 않음

리소스 유형	암호화 구성 방법	독립 AWS Backup 암호화
AWS CloudFormation	CloudFormation 백업은 항상 암호화됩니다. 백업의 CloudFormation 암호화 키는 CloudFormation 백업이 저장되는 CloudFormation 저장소에 구성됩니다. CloudFormation	지원
Amazon EC2 인스턴스의 SAP HANA 데이터베이스	SAP HANA 데이터베이스 백업은 항상 암호화됩니다. SAP HANA 데이터베이스 백업의 AWS KMS 암호화 키는 데이터베이스 백업이 저장되는 AWS Backup 저장소에 구성됩니다.	지원

백업 복사본을 위한 암호화

를 사용하여 계정 또는 지역 간에 백업을 AWS Backup 복사하는 경우 원본 백업이 암호화되지 않은 경우에도 대부분의 리소스 유형에 대해 해당 복사본을 AWS Backup 자동으로 암호화합니다. AWS Backup 대상 저장소의 KMS 키를 사용하여 사본을 암호화합니다. 하지만 암호화되지 않은 Aurora, Amazon DocumentDB 및 Neptune 클러스터의 스냅샷도 암호화되지 않습니다.

암호화 및 백업 사본

에서 완전히 관리되지 않는 리소스에는 AWS 관리형 KMS 키를 사용한 계정 간 복사가 지원되지 않습니다. AWS Backup완전히 관리되는 리소스를 전체 관리 AWS Backup 확인하려면 를 참조하십시오.

에서 완전히 관리되는 리소스의 AWS Backup경우 백업은 백업 저장소의 암호화 키로 암호화됩니다. 완전히 관리되지 않는 리소스의 경우 계정 간 복사본은 소스 리소스와 동일한 KMS 키를 사용합니다. AWS Backup자세한 내용은 암호화 키 및 계정 간 사본 섹션을 참조하세요.

가상 머신 하이퍼바이저 보안 인증 정보 암호화

하이퍼바이저로 관리되는 가상 머신은 AWS Backup 게이트웨이를 사용하여 온프레미스 시스템을 AWS Backup에 연결합니다. 하이퍼바이저도 마찬가지로 강력하고 신뢰할 수 있는 보안을 유지하는 것이 중요합니다. 이러한 보안은 AWS 소유 키 또는 고객 관리 키로 하이퍼바이저를 암호화하여 달성할 수 있습니다.

AWS 소유 및 고객 관리 키

AWS Backup 하이퍼바이저 자격 증명을 암호화하여 AWS 소유한 암호화 키를 사용하여 민감한 고객 로그인 정보를 보호합니다. 고객 관리형 키를 대신 사용할 수도 있습니다.

기본적으로 하이퍼바이저의 자격 증명을 암호화하는 데 사용되는 키는 소유 키입니다.AWS AWS Backup 이러한 키를 사용하여 하이퍼바이저 자격 증명을 자동으로 암호화합니다. AWS 소유 키를 보거나 관리하거나 사용할 수 없으며 사용 여부를 감사할 수도 없습니다. 하지만 데이터를 암호화하는 키를 보호하기 위해 어떤 작업을 수행하거나 어떤 프로그램을 변경할 필요가 없습니다. 자세한 내용은 AWS KMS 개발자 안내서의 AWS 소유 키를 참조하십시오.

또는 고객 관리형 키를 사용하여 보안 인증 정보를 암호화할 수도 있습니다. AWS Backup 은 사용자가 암호화를 수행하기 위해 생성, 소유, 관리하는 대칭 고객 관리형 키의 사용을 지원합니다. 이 암호화를 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.

- 키 정책 수립 및 유지
- IAM 정책 및 권한 수립 및 유지
- 키 정책 활성화 및 비활성화
- 키 암호화 자료 교체
- 태그 추가
- 키 별칭 생성
- 삭제를 위한 스케줄 키

고객 관리 키를 사용하는 경우 백업 또는 복원 작업을 실행하기 전에 역할에 이 키를 사용하여 암호를 해독할 권한이 있는지 AWS Backup 확인합니다. 백업 또는 복원 작업을 시작하는 데 사용되는 역할에 `kms:Decrypt` 작업을 추가해야 합니다.

기본 백업 역할에는 `kms:Decrypt` 작업을 추가할 수 없으므로 고객 관리형 키를 사용하려면 기본 백업 역할 이외의 역할을 사용해야 합니다.

자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리형 키를 참조하세요.

고객 관리형 키 사용 시 필요한 권한 부여

AWS KMS 고객 관리 키를 사용하려면 허가가 필요합니다. 고객 관리 키로 암호화된 하이퍼바이저 구성을 가져오는 경우 에서 `CreateGrant`요청을 전송하여 사용자를 대신하여 권한 부여를 AWS Backup 생성합니다. AWS KMS AWS Backup 권한 부여를 사용하여 고객 계정의 KMS 키에 액세스합니다.

언제든지 고객 관리 키에 대한 권한 부여에 대한 액세스를 취소하거나 고객 관리 키에 대한 액세스를 제거할 AWS Backup수 있습니다. 이렇게 하면 하이퍼바이저와 연결된 모든 게이트웨이가 고객 관리형 키로 암호화된 하이퍼바이저의 사용자 이름 및 암호에 더 이상 액세스할 수 없게 되어 백업 및 복원 작업에 영향을 미칠 수 있습니다. 특히, 이 하이퍼바이저의 가상 머신에서 수행하는 백업 및 복원 작업은 실패합니다.

Backup 게이트웨이는 사용자가 하이퍼바이저를 삭제하면 `RetireGrant` 작업을 사용하여 권한 부여를 제거합니다.

암호화 키 모니터링

AWS Backup 리소스와 함께 AWS KMS 고객 관리 키를 사용하는 경우 Amazon CloudWatch Logs를 사용하여 AWS CloudTrail로 AWS Backup 보내는 요청을 추적할 수 AWS KMS있습니다.

고객 관리 키로 암호화된 데이터에 AWS Backup 액세스하기 위해 호출하는 모니터링 AWS KMS 작업이 있는지 다음 `"eventName"` 필드가 있는 AWS CloudTrail 이벤트를 찾아보십시오.

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

내 ID 및 액세스 관리 AWS Backup

에 액세스하려면 자격 증명이 AWS Backup 필요합니다. 이러한 보안 인증 정보에는 AWS 리소스(예: Amazon DynamoDB 데이터베이스 또는 Amazon EFS 파일 시스템)에 액세스할 수 있는 권한이 있어야 합니다. 또한 일부 AWS Backup지원 서비스에 AWS Backup 대해 에서 생성한 복구 지점은 원본 서비스 (예: Amazon EFS) 를 사용하여 삭제할 수 없습니다. 를 사용하여 AWS Backup이러한 복구 지점을 삭제할 수 있습니다.

다음 섹션에서는 AWS Identity and Access Management (IAM) 사용 방법과 리소스에 대한 보안 AWS Backup 액세스를 지원하는 방법에 대한 세부 정보를 제공합니다.

> **Warning**
>
> AWS Backup 복구 지점 수명 주기를 관리하기 위해 리소스를 할당할 때 선택한 것과 동일한 IAM 역할을 사용합니다. 해당 역할을 삭제하거나 수정하면 복구 지점 수명 AWS Backup 주기를 관리할 수 없습니다. 이 경우 서비스 연결 역할을 사용하여 수명 주기를 관리하려고 시도합

니다. 일부 경우에는 이 방법도 작동하지 않아 스토리지에 EXPIRED 복구 시점이 남아 원치 않는 비용이 발생할 수 있습니다. EXPIRED 복구 시점을 삭제하려면 백업 삭제의 절차를 사용하여 복구 시점을 수동으로 삭제하세요.

주제

- 인증
- 액세스 제어
- IAM 서비스 역할
- 관리형 정책 대상 AWS Backup
- AWS Backup에 서비스 연결 역할 사용
- 교차 서비스 혼동된 대리자 방지

인증

백업하려는 AWS Backup 서비스나 AWS 서비스에 액세스하려면 요청을 인증하는 데 사용할 AWS 수 있는 자격 증명이 필요합니다. 다음 유형의 AWS ID로 액세스할 수 있습니다.

- AWS 계정 루트 사용자 - AWS가입할 때 AWS 계정과 연결된 이메일 주소와 비밀번호를 제공합니다. 이것은 AWS 계정 루트 사용자입니다. 자격 증명을 통해 모든 AWS 리소스에 완전히 액세스할 수 있습니다.

  > **Important**
  >
  > 보안상 관리자를 생성할 때만 루트 사용자를 사용하는 것이 좋습니다. 관리자는 AWS 계정에 대한 모든 권한을 가진 IAM 사용자입니다. 그런 다음 이 관리자 사용자를 사용하여 제한된 권한이 있는 다른 IAM 사용자 및 역할을 만들 수 있습니다. 자세한 내용은 IAM 사용 설명서에서 IAM 모범 사례 및 첫 번째 IAM 관리자 및 그룹 생성을 참조하세요.

- IAM 사용자 – IAM 사용자는 특정 사용자 지정 권한(예: 백업을 저장할 백업 볼트를 생성할 수 있는 권한)이 있는 AWS 계정 내의 자격 증명입니다. IAM 사용자 이름과 암호를 사용하여 AWS 토론 포럼 또는 센터와 같은 보안 AWS 웹 페이지에 로그인할 수 있습니다. AWS Management ConsoleAWS Support

  사용자 이름과 암호 외에도 각 사용자에 대해 액세스 키를 생성할 수 있습니다. 여러 SDK 중 하나를 통해 또는 (AWS Command Line Interface CLI AWS) 를 사용하여 프로그래밍 방식으로 AWS 서비

스에 액세스할 때 이러한 키를 사용할 수 있습니다. SDK 및 AWS CLI 도구는 액세스 키를 사용하여 암호화 방식으로 요청에 서명합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 요청 인증에 대한 자세한 내용은 AWS 일반 참조의 서명 버전 4 서명 프로세스를 참조하십시오.

- IAM 역할 – IAM 역할은 계정에 만들 수 있는, 특정 권한을 지닌 또 하나의 IAM 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. IAM 역할을 사용하면 서비스와 리소스에 액세스하는 데 사용할 수 있는 임시 액세스 키를 얻을 수 있습니다. AWS 임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.
  - 연동 사용자 액세스 — IAM 사용자를 생성하는 대신 엔터프라이즈 사용자 디렉토리 또는 웹 ID 공급자의 기존 사용자 ID를 사용할 수 있습니다. AWS Directory Service이 사용자를 페더레이션 사용자라고 합니다. AWS 에서는 자격 증명 공급자를 통해 액세스가 요청되면 페더레이션 사용자에게 역할을 할당합니다. 페더레이션 사용자에 대한 자세한 정보는 IAM 사용 설명서의 페더레이션 사용자 및 역할을 참조하세요.
  - 교차 계정 관리 — 계정의 IAM 역할을 사용하여 계정의 리소스를 관리할 수 있는 다른 AWS 계정 권한을 부여할 수 있습니다. 예를 들어, IAM 사용 설명서의 자습서: IAM 역할 AWS 계정 사용 전반에 대한 액세스 위임을 참조하십시오.
  - AWS 서비스 액세스 - 계정의 IAM 역할을 사용하여 AWS 서비스에 계정 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 권한을 위임하기 위한 역할 생성을 참조하십시오.
  - Amazon Elastic Compute Cloud (Amazon EC2) 에서 실행되는 애플리케이션 — IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되고 API 요청을 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

액세스 제어

요청을 인증하는 데 필요한 유효한 자격 증명을 가질 수 있지만 적절한 권한이 없으면 백업 저장소와 같은 AWS Backup 리소스에 액세스할 수 없습니다. 또한 Amazon Elastic Block Store (Amazon EBS) 볼륨과 같은 AWS 리소스는 백업할 수 없습니다.

모든 AWS 리소스는 가 AWS 계정소유하며 리소스를 생성하거나 액세스할 수 있는 권한은 권한 정책에 따라 관리됩니다. 계정 관리자는 권한 정책을 AWS Identity and Access Management (IAM) 자격 증

명 (즉, 사용자, 그룹, 역할) 에 연결할 수 있습니다. 일부 서비스에서도 리소스에 권한 정책 연결을 지원합니다.

> **Note**
>
> 계정 관리자(또는 관리자 사용자)는 관리자 권한이 있는 사용자입니다. 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례 단원을 참조하세요.

권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다.

다음 단원에서는 액세스 정책의 작동 방식과 액세스 정책을 사용하여 백업을 보호하는 방법에 대해 설명합니다.

주제

- 리소스 및 작업
- 리소스 소유권
- 정책 요소 지정: 작업, 효과, 보안 주체
- 정책에서 조건 지정
- API 권한: 작업, 리소스 및 조건 참조
- 태그 복사 권한
- 액세스 정책

리소스 및 작업

리소스는 서비스 내에 존재하는 객체입니다. AWS Backup 리소스에는 백업 계획, 백업 저장소 및 백업이 포함됩니다. 백업은 에 있는 다양한 유형의 백업 리소스를 가리키는 일반적인 용어입니다 AWS. 예를 들어 Amazon EBS 스냅샷, Amazon Relational Database Service(Amazon RDS) 스냅샷, Amazon DynamoDB 백업은 모두 백업 리소스 유형입니다.

AWS Backup에서는 백업을 복구 지점이라고도 합니다. 사용할 AWS Backup때는 Amazon EBS 볼륨 또는 DynamoDB 테이블과 같이 보호하려는 다른 AWS 서비스의 리소스도 함께 사용합니다. 이러한 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결됩니다. ARN은 리소스를 고유하게 식별합니다. AWS IAM 정책 또는 API 호출과 같은 모든 AWS에서 리소스를 명료하게 지정해야 하는 경우 ARN이 필요합니다.

다음 표에는 리소스, 하위 리소스, ARN 형식 및 고유 ID 예제가 나와 있습니다.

AWS Backup 리소스 ARN

리소스 유형	ARN 형식	고유 ID 예제
백업 계획	`arn:aws:backup:region:account-id:backup-plan:*`	
백업 저장소	`arn:aws:backup:region:account-id:backup-vault:*`	
Amazon EBS의 복구 시점	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Amazon EC2 이미지의 복구 시점	`arn:aws:ec2:region::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Amazon RDS의 복구 시점	`arn:aws:rds:region:account-id:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Aurora의 복구 시점	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Storage Gateway의 복구 시점	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
DynamoDB의 복구 시점(고급 DynamoDB 백업 없음)	`arn:aws:dynamodb:region:account-id:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`

리소스 유형	ARN 형식	고유 ID 예제
DynamoDB의 복구 시점(고급 DynamoDB 백업 활성화됨)	arn:aws:backup: *region*:*account-id* :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Amazon EFS의 복구 시점	arn:aws:backup: *region*:*account-id* :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e
Amazon FSx의 복구 시점	arn:aws:fsx: *region*:*account-id* :backup/backup-*	backup/backup-1a20e49137e31d9e0
가상 머신의 복구 시점	arn:aws:backup: *region*:*account-id* :recovery-point:*	1801234a-5b6b-7dc8-8032-836f7ffc623b
Amazon S3 연속 백업의 복구 시점	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -5ec207d0
S3 정기 백업의 복구 시점	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -20211231900000-5ec207d0
아마존 DocumentDB의 복구 지점	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Neptune의 복구 지점	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012

리소스 유형	ARN 형식	고유 ID 예제
Amazon Redshift의 복구 지점	`arn:aws:redshift:region:account-id:snapshot:resource/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Amazon Timestream의 복구 시점	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
템플릿의 AWS CloudFormation 복구 지점	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Amazon EC2 인스턴스의 SAP HANA 데이터베이스 복구 지점	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

전체 AWS Backup 관리를 지원하는 리소스에는 모두 복구 지점 형식이 있으므로 권한 정책을 적용하여 해당 복구 지점을 쉽게 보호할 수 있습니다`arn:aws:backup:region:account-id:recovery-point:*`. 전체 AWS Backup 관리를 지원하는 리소스를 확인하려면 리소스별 기능 가용성 표의 해당 섹션을 참조하십시오.

AWS Backup AWS Backup 리소스 작업을 위한 일련의 작업을 제공합니다. 사용 가능한 작업 목록은 AWS Backup 작업 섹션을 참조하십시오.

리소스 소유권

는 누가 리소스를 생성했는지에 상관없이 계정에서 생성된 리소스를 AWS 계정 소유합니다. 구체적으로, 리소스 소유자는 리소스 생성 요청을 인증하는 보안 주체 (즉, AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할) 의 소유자입니다. AWS 계정 다음 예에서는 이러한 작동 방식을 설명합니다.

- 의 AWS 계정 루트 사용자 자격 증명을 사용하여 백업 저장소를 생성하는 경우 해당 저장소의 소유자가 AWS 계정 됩니다. AWS 계정

- 에서 IAM 사용자를 생성하고 해당 AWS 계정 사용자에게 백업 저장소를 생성할 권한을 부여하면 사용자가 백업 저장소를 생성할 수 있습니다. 하지만 백업 볼트 리소스는 그 사용자가 속한 AWS 계정이 소유합니다.
- 백업 저장소를 생성할 권한이 AWS 계정 있는 IAM 역할을 생성하는 경우 해당 역할을 수임할 수 있는 사람은 누구나 저장소를 생성할 수 있습니다. 역할이 속한 사용자가 AWS 계정백업 볼트 리소스를 소유합니다.

정책 요소 지정: 작업, 효과, 보안 주체

서비스는 각 AWS Backup 리소스 (참조리소스 및 작업) 에 대해 API 작업 세트를 정의합니다 (참조작업). 이러한 API 작업에 대한 권한을 부여하려면 정책에서 지정할 수 있는 작업 세트를 AWS Backup 정의합니다. API 작업을 실시하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 가장 기본적인 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. 자세한 정보는 리소스 및 작업을 참조하세요.
- 조치 – 조치 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다.
- 결과 – 사용자가 특정 작업을 요청하는 경우의 결과를 지정합니다. 이는 허용 또는 거부 중에 하나가 될 수 있습니다. 명시적으로 리소스에 대한 액세스 권한을 부여(허용)하지 않는 경우, 액세스는 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.
- 보안 주체 – ID 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다(리소스 기반 정책에만 해당).

IAM 정책 구문 및 설명에 대해 자세히 알아보려면 IAM 사용 설명서의 IAM JSON 정책 참조 단원을 참조하세요.

모든 AWS Backup API 작업을 보여주는 표는 을 참조하십시오API 권한: 작업, 리소스 및 조건 참조.

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책이 적용되는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 설명은 IAM 사용자 가이드의 조건을 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS Backup 자체 조건 키 세트를 정의합니다. AWS Backup 조건 키 목록을 보려면 서비스 권한 부여 AWS Backup참조의 조건 키를 참조하십시오.

API 권한: 작업, 리소스 및 조건 참조

액세스 제어을 설정하고 IAM 자격 증명에 연결할 수 있는 권한 정책(자격 증명 기반 정책)을 작성할 때 다음 목록을 참조로 사용할 수 있습니다. 목록에는 각 AWS Backup API 작업, 작업 수행 권한을 부여할 수 있는 해당 작업, 권한을 부여할 수 있는 AWS 리소스가 포함되어 있습니다. 정책의 `Action`필드에서 작업을 지정하고, 정책의 `Resource`필드에서 리소스 값을 지정합니다. `Resource` 필드가 비어 있는 경우 와일드카드(*)를 사용하여 모든 리소스를 포함할 수 있습니다.

AWS Backup 정책에서 AWS-wide 조건 키를 사용하여 조건을 표현할 수 있습니다. AWS-wide 키의 전체 목록은 IAM 사용 설명서의 사용 가능한 키를 참조하십시오.

[1] 기존 저장소 액세스 정책을 사용합니다.

[2] 리소스별 복구 지점 ARN은 을 참조하십시오AWS Backup 리소스 ARN.

[3에는] 리소스의 메타데이터에 키-값 쌍이 `StartRestoreJob` 있어야 합니다. 리소스의 메타데이터를 가져오려면 `GetRecoveryPointRestoreMetadata` API를 호출합니다.

[4] 백업에 원본 리소스 태그를 포함하거나 백업에 태그를 추가하려는 `backup:TagResource` 경우 특정 리소스 유형에는 백업을 수행하는 역할에 특정 태그 지정 권한이 있어야 합니다. 로 시작하는 ARN을 사용하는 백업 `arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:` 또는 연속 백업에는 이 권한이 필요합니다. `backup:TagResource`권한은 다음에 적용되어야 합니다. "*`resourcetype`*": "`arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*`"

자세한 내용은 서비스 권한 부여 참조에서 AWS Backup에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

태그 복사 권한

백업 또는 복사 작업을 AWS Backup 수행할 때 소스 리소스 (또는 복제의 경우 복구 지점) 에서 복구 지점으로 태그를 복사하려고 시도합니다.

> **Note**
>
> AWS Backup 복원 작업 중에는 기본적으로 태그를 복사하지 않습니다. 복원 작업 중에 태그를 복사하는 이벤트 기반 아키텍처에 대해서는 복원 작업에서 AWS Backup 리소스 태그를 유지하는 방법을 참조하십시오.

백업 또는 복사 작업 중에 백업 계획 (또는 복사 계획 또는 온디맨드 백업) 에서 지정한 태그를 소스 리소스의 태그와 AWS Backup 집계합니다. 하지만 AWS 리소스당 태그 제한은 50개이며, 이를 AWS Backup 초과할 수 없습니다. 백업 또는 복사 작업이 계획과 소스 리소스의 태그를 집계할 때 총 50개가 넘는 태그를 발견할 수 있으며, 이 경우 작업을 완료할 수 없고 작업이 실패합니다. 이는 AWS-wide 태깅 모범 사례와 일치합니다. 자세한 내용을 알아보려면 AWS 일반 참조 가이드의 태그 제한을 참조하세요.

- 백업 작업 태그를 소스 리소스 태그로 집계한 결과 리소스에 태그가 50개가 넘습니다. AWS 리소스당 최대 50개의 태그를 지원합니다. 자세한 내용은 태그 제한을 참조하세요.
- 제공하는 IAM 역할에는 소스 태그를 읽거나 대상 태그를 설정할 권한이 AWS Backup 없습니다. 자세한 내용 및 샘플 IAM 역할 정책은 관리형 정책을 참조하세요.

백업 계획을 사용하여 소스 리소스 태그와 모순되는 태그를 생성할 수 있습니다. 두 태그가 충돌하는 경우 백업 계획의 태그가 우선합니다. 소스 리소스의 태그 값을 복사하지 않으려면 이 방법을 사용하세요. 백업 계획을 사용하여 동일한 태그 키를 지정하되 다른 값 또는 빈 값을 지정합니다.

백업에 태그를 할당하는 데 필요한 사용 권한

리소스 유형	필수 권한
Amazon EFS 파일 시스템	`elasticfilesystem:DescribeTags`
Amazon FSx 파일 시스템	`fsx:ListTagsForResource`
Amazon RDS 데이터베이스 및 Amazon Aurora 클러스터	`rds:AddTagsToResource` `rds:ListTagsForResource`
Storage Gateway 볼륨	`storagegateway:ListTagsForResource`
Amazon EC2 인스턴스 및 Amazon EBS 볼륨	`EC2:CreateTags`

리소스 유형	필수 권한
	`EC2:DescribeTags`

DynamoDB는 먼저 고급 DynamoDB 백업을 활성화하지 않는 한 백업에 태그 할당을 지원하지 않습니다.

Amazon EC2 백업이 이미지 복구 지점과 스냅샷 세트를 생성하면 태그를 결과 AMI에 AWS Backup 복사합니다. AWS Backup 또한 Amazon EC2 인스턴스와 연결된 볼륨의 태그를 결과 스냅샷으로 복사합니다.

액세스 정책

권한 정책은 누가 무엇에 액세스할 수 있는지를 나타냅니다. IAM 자격 증명에 연결된 정책을 자격 증명 기반 정책(IAM 정책)이라고 합니다. 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다. AWS Backup ID 기반 정책과 리소스 기반 정책을 모두 지원합니다.

> **Note**
>
> 이 섹션에서는 다음과 같은 맥락에서 IAM을 사용하는 방법에 대해 설명합니다. AWS Backup IAM 서비스에 대한 자세한 정보는 다루지 않습니다. 전체 IAM 설명은 IAM 사용자 가이드에서 IAM이란 무엇인가?를 참조하십시오. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON Policy Reference를 참조하세요.

자격 증명 기반 정책(IAM 정책)

자격 증명 기반 정책은 사용자 또는 역할과 같은 IAM 자격 증명에 연결할 수 있는 정책입니다. 예를 들어, 사용자가 AWS 리소스를 보고 백업할 수는 있지만 백업을 복원할 수는 없도록 하는 정책을 정의할 수 있습니다.

사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 자격 증명(사용자, 그룹 및 역할)을 참조하세요.

IAM 정책을 사용하여 백업에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 관리형 정책 대상 AWS Backup 단원을 참조하세요.

리소스 기반 정책

AWS Backup 백업 저장소에 대한 리소스 기반 액세스 정책을 지원합니다. 따라서 백업 볼트에 구성된 백업에 대해 어떤 사용자가 어떠한 종류의 권한을 갖는지를 제어하는 액세스 정책을 정의할 수 있습니다. 백업 볼트에 대한 리소스 기반 액세스 정책을 사용하면 백업에 대한 액세스를 쉽게 제어할 수 있습니다.

Backup Vault 액세스 정책은 AWS Backup API를 사용할 때 사용자 액세스를 제어합니다. Amazon Elastic Block Store(Amazon EBS) 및 Amazon Relational Dabase Service(Amazon RDS) 스냅샷과 같은 일부 백업 유형도 해당 서비스의 API를 사용하여 액세스할 수 있습니다. API에 대한 액세스를 제어하는 별도의 액세스 정책을 IAM에 생성하면 백업에 대한 액세스를 완전히 제어할 수 있습니다.

백업 볼트에 대한 액세스 정책을 생성하는 방법에 대한 자세한 내용은 백업 저장소에 대한 액세스 정책 설정 단원을 참조하세요.

IAM 서비스 역할

AWS Identity and Access Management (IAM) 역할은 AWS ID가 수행할 수 있는 작업과 수행할 수 없는 작업을 결정하는 권한 정책이 있는 ID라는 점에서 사용자와 유사합니다. AWS그러나 역할은 한 사람하고만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 AWS 위임하는 역할입니다. 사용자 대신 백업 작업을 수행하는 서비스인 AWS Backup 에 사용자 대신 백업 작업을 수행할 때 맡아야 할 역할을 전달해야 합니다. IAM 역할에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 섹션을 참조하세요.

전달되는 역할에는 백업 생성, 복원 또는 만료와 같은 백업 작업과 관련된 작업을 수행할 수 AWS Backup 있는 권한이 포함된 IAM 정책이 AWS Backup 있어야 합니다. 지원하는 AWS Backup 각 AWS 서비스마다 다른 권한이 필요합니다. 또한 역할은 역할을 수임할 수 있는 신뢰할 수 있는 주체로 AWS Backup 등록되어 있어야 합니다. AWS Backup

백업 계획에 리소스를 할당하거나 온디맨드 백업, 복사 또는 복원을 수행하는 경우 지정된 리소스에서 기본 작업을 수행할 수 있는 액세스 권한이 있는 서비스 역할을 전달해야 합니다. AWS Backup 는 이 역할을 사용하여 계정에서 리소스를 만들고, 태그를 지정하고, 삭제합니다.

AWS 역할을 사용하여 백업에 대한 액세스를 제어합니다.

좁은 범위의 역할을 정의하고 해당 역할을 AWS Backup에 전달할 수 있는 사용자를 지정하여 역할을 통해 백업에 대한 액세스를 제어할 수 있습니다. 예를 들어 Amazon RDS (관계형 데이터베이스 서비스) 데이터베이스를 백업할 권한만 부여하고 Amazon RDS 데이터베이스 소유자에게 해당 역할을 전달할 권한만 부여하는 역할을 생성할 수 있습니다. AWS Backup AWS Backup 지원되는 각 서비스에

대해 미리 정의된 여러 관리형 정책을 제공합니다. 이러한 관리형 정책을 생성한 역할에 연결할 수 있습니다. 따라서 필요한 올바른 권한이 있는 서비스별 역할을 쉽게 만들 수 있습니다. AWS Backup

의 AWS 관리형 정책에 대한 자세한 내용은 AWS Backup을 참조하십시오. 관리형 정책 대상 AWS Backup

의 기본 서비스 역할 AWS Backup

AWS Backup 콘솔을 처음 사용하는 경우 기본 서비스 역할을 AWS Backup 생성하도록 선택할 수 있습니다. 이 역할에는 사용자 대신 백업을 만들고 복원하는 데 AWS Backup 필요한 권한이 있습니다.

> **Note**
>
> AWS Management Console을 사용하면 기본 역할이 자동으로 생성됩니다. AWS Command Line Interface (AWS CLI) 를 사용하여 기본 역할을 생성할 수 있지만 수동으로 수행해야 합니다.

리소스 유형별로 별도의 역할을 사용하는 등 사용자 지정 역할을 사용하려는 경우 그렇게 할 수도 있으며 사용자 지정 역할을 AWS Backup에 전달할 수 있습니다. 개별 리소스 유형에 대해 백업 및 복원을 활성화하는 역할의 예제를 보려면 고객 관리형 정책 표를 참조하세요.

기본 서비스 역할의 이름은 `AWSBackupDefaultServiceRole` 지정됩니다. 이 서비스 역할에는 두 개의 관리형 정책 AWSBackupServiceRolePolicyForBackup및 이 포함되어 AWSBackupServiceRolePolicyForRestores있습니다.

`AWSBackupServiceRolePolicyForBackup`백업되는 리소스를 설명할 수 있는 AWS Backup 권한, 암호화된 AWS KMS 키에 관계없이 백업에 태그를 생성, 삭제, 설명 또는 추가할 수 있는 권한을 부여하는 IAM 정책이 포함되어 있습니다.

`AWSBackupServiceRolePolicyForRestores`암호화된 AWS KMS 키에 관계없이 백업에서 생성되는 새 리소스를 생성, 삭제 또는 설명할 수 있는 AWS Backup 권한을 부여하는 IAM 정책이 포함되어 있습니다. 새로 생성된 리소스에 태그를 지정할 수 있는 권한도 포함됩니다.

Amazon EC2 인스턴스를 복원하려면 새 인스턴스를 시작해야 합니다.

콘솔에서 기본 서비스 역할 생성

AWS Backup 콘솔에서 수행하는 특정 작업에 따라 AWS Backup 기본 서비스 역할이 생성됩니다.

AWS 계정에서 AWS Backup 기본 서비스 역할을 만들려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 계정을 위해 역할을 생성하려면 백업 계획에 리소스를 할당하거나 온디맨드 백업을 생성합니다.
   a. 백업 계획을 생성하고 백업에 리소스를 할당합니다. 예약 백업 생성을 참조하세요.
   b. 또는 온디맨드 백업을 생성합니다. 온디맨드 백업 생성을 참조하세요.
3. 다음 단계에 따라 계정에 AWSBackupDefaultServiceRole이 생성되었는지 확인합니다.
   a. 몇 분간 기다리십시오. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변경 사항이 매번 즉시 표시되는 것은 아닙니다를 참조하세요.
   b. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
   c. 왼쪽 탐색 메뉴에서 역할을 선택합니다.
   d. 검색 창에 AWSBackupDefaultServiceRole를 입력합니다. 이 옵션이 존재한다면 AWS Backup 기본 역할을 생성하고 이 절차를 완료한 것입니다.
   e. 그래도 AWSBackupDefaultServiceRole이 표시되지 않으면 콘솔에 액세스하는 데 사용하는 IAM 사용자 또는 IAM 역할에 다음 권한을 추가합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
```

```
}
```

중국 리전의 경우 *aws*를 *aws-cn*으로 바꿉니다. AWS GovCloud (US) 지역의 경우 *aws#* 로 대체하십시오 *aws-us-gov*.

f. IAM 사용자 또는 IAM 역할에 권한을 추가할 수 없는 경우 관리자에게 `AWSBackupDefaultServiceRole`과 다른 이름으로 역할을 수동으로 생성하고 해당 역할을 다음 관리형 정책에 연결하도록 요청하세요.

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

관리형 정책 대상 AWS Backup

관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 ID 기반 정책입니다. AWS 계정 정책을 보안 주체 엔터티에 추가할 경우 정책에서 정의한 권한까지 엔터티에게 부여하게 됩니다.

AWS 관리형 정책은 에서 생성하고 관리합니다. AWS AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 보안 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다.

고객 관리형 정책을 사용하면 백업에 대한 액세스를 설정할 수 있는 세분화된 제어 기능을 제공합니다. AWS Backup예를 들어 이러한 정책을 사용하여 데이터베이스 백업 관리자에게 Amazon RDS 백업에는 액세스할 수 있지만 Amazon EFS 백업에는 액세스할 수 없는 권한을 부여할 수 있습니다.

자세한 내용은 IAM 사용 설명서의 관리형 정책을 참조하십시오.

AWS 관리형 정책

AWS Backup 일반적인 사용 사례에 대해 다음과 같은 AWS 관리형 정책을 제공합니다. 이러한 정책을 사용하면 쉽게 올바른 권한을 정의하고 백업에 대한 액세스를 제어할 수 있습니다. 두 가지 유형의 관리형 정책이 있습니다. 한 유형은 AWS Backup에 대한 액세스를 제어하기 위해 사용자에게 할당되도록 고안되었습니다. 다른 유형의 관리형 정책은 AWS Backup에 전달하는 역할에 연결되도록 고안되었습니다. 다음 표에는 AWS Backup 이 제공하는 모든 관리형 정책 목록과 정책이 정의된 방식이 설명되어 있습니다. 또한 IAM 콘솔의 정책 섹션에도 이 관리형 정책이 표시됩니다.

정책

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess

- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

이 정책은 사용자에게 AWS Backup 리소스 및 활동에 대한 기대치를 정의하는 제어 및 프레임워크를 만들고 정의된 제어 및 프레임워크에 따라 AWS Backup 리소스 및 활동을 감사할 수 있는 권한을 부여합니다. 이 정책은 감사 수행에 대한 사용자 기대치를 설명하는 권한 AWS Config 및 유사한 서비스에 권한을 부여합니다.

또한 이 정책은 Amazon S3 및 유사한 서비스에 감사 보고서를 전송할 수 있는 권한을 부여하고 사용자가 감사 보고서를 검색하고 열람할 수 있도록 합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupAuditAccess.

AWSBackupDataTransferAccess

이 정책은 AWS Backup 스토리지 플레인 데이터 전송 API에 대한 권한을 제공하여 AWS Backint 에이전트가 AWS Backup 스토리지 플레인을 사용하여 백업 데이터 전송을 완료할 수 있도록 합니다. 이 정책을 Backint 에이전트와 함께 SAP HANA를 실행하는 Amazon EC2 인스턴스가 맡는 역할에 연결할 수 있습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupDataTransferAccess.

AWSBackupFullAccess

백업 관리자는 백업 계획 생성 또는 편집, 백업 계획에 AWS 리소스 할당, 백업 복원 등 모든 AWS Backup 작업에 액세스할 수 있습니다. 백업 관리자는 조직의 비즈니스 및 규제 요건에 맞는 백업 계획을 정의하여 백업 규정 준수를 확인하고 적용해야 합니다. 또한 Backup 관리자는 조직의 AWS 리소스가 적절한 계획에 할당되도록 합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupFullAccess.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오.

AWSBackupOperatorAccess

백업 운영자는 리소스가 적절히 백업되도록 하는 업무를 담당하는 사용자입니다. 백업 관리자는 백업 관리자가 생성하는 백업 계획에 AWS 리소스를 할당할 권한이 있습니다. 또한 AWS 리소스의 온디맨드 백업을 생성하고 온디맨드 백업의 보존 기간을 구성할 수 있는 권한도 있습니다. 백업 계획을 생성 또는 편집하거나 이미 생성되어 예약된 백업을 삭제할 수 있는 권한은 백업 운영자에게 없습니다. 백업 운영자는 백업을 복원할 수 있습니다. 백업 운영자가 백업 계획에 할당하거나 백업에서 복원할 수 있는 리소스 유형을 제한할 수 있습니다. 이를 위해서는 특정 리소스 유형에 대한 권한이 AWS Backup 있는 특정 서비스 역할만 전달되도록 허용하면 됩니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupOperatorAccess.

AWSBackupOrganizationAdminAccess

조직 관리자는 백업 정책 생성, 편집 또는 삭제, 계정 및 조직 단위에 백업 정책 할당, 조직 내 백업 활동 모니터링 등 모든 AWS Organizations 작업에 액세스할 수 있습니다. 조직 관리자는 조직의 비즈니스 및 규제 요건에 맞는 백업 정책을 정의하고 할당하여 조직의 계정을 보호해야 합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupOrganizationAdminAccess.

AWSBackupRestoreAccessForSAPHANA

이 정책은 Amazon EC2에서 SAP HANA의 백업을 복원할 수 있는 AWS Backup 권한을 제공합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupRestoreAccessForSAPHANA.

AWSBackupServiceLinkedRolePolicyForBackup

이 정책은 사용자 대신 서비스를 호출하여 백업을 관리할 수 AWSServiceRoleforBackup AWS Backup 있도록 이름이 지정된 AWS 서비스 연결 역할에 연결됩니다. 자세한 정보는 the section called “백업 및 복사”을 참조하세요.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceLinkedRolePolicyforBackup.

AWSBackupServiceLinkedRolePolicyForBackupTest

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceLinkedRolePolicyForBackupTest.

AWSBackupServiceRolePolicyForBackup

사용자를 대신하여 지원되는 모든 리소스 유형의 백업을 생성할 수 있는 AWS Backup 권한을 제공합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceRolePolicyForBackup.

AWSBackupServiceRolePolicyForRestores

사용자를 대신하여 지원되는 모든 리소스 유형의 백업을 복원할 수 있는 AWS Backup 권한을 제공합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceRolePolicyForRestores.

EC2 인스턴스 복원의 경우 EC2 인스턴스를 시작할 수 있는 다음 권한도 포함해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

이 정책에는 모든 S3 버킷을 AWS Backup 백업하는 데 필요한 권한이 포함되어 있습니다. 여기에는 버킷의 모든 객체 및 관련 AWS KMS 키에 대한 액세스가 포함됩니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceRolePolicyForS3Backup.

AWSBackupServiceRolePolicyForS3Restore

이 정책에는 S3 백업을 AWS Backup 버킷으로 복원하는 데 필요한 권한이 포함되어 있습니다. 여기에는 버킷에 대한 읽기 및 쓰기 권한과 S3 작업과 관련된 모든 AWS KMS 키의 사용이 포함됩니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceRolePolicyForS3Restore.

AWSServiceRolePolicyForBackupReports

AWS Backup 이 정책을 AWSServiceRoleForBackupReports서비스 연결 역할에 사용합니다. 이 서비스 연결 역할은 백업 설정, 작업 및 리소스의 프레임워크 준수 여부를 모니터링하고 보고할 수 있는 AWS Backup 권한을 부여합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSServiceRolePolicyForBackupReports.

AWSServiceRolePolicyForBackupRestoreTesting

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSServiceRolePolicyForBackupRestoreTesting.

고객 관리형 정책

다음 섹션에서는 에서 지원하는 타사 애플리케이션 및 타사 애플리케이션에 대한 권장 백업 AWS 서비스 및 복원 권한을 설명합니다 AWS Backup. 자체 정책 문서를 생성할 때 기존 AWS 관리형 정책을 모델로 사용한 다음 이를 사용자 지정하여 AWS 리소스에 대한 액세스를 추가로 제한할 수 있습니다.

Amazon Aurora

백업

다음 문구로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- DynamoDBBackupPermissions
- RDSClusterModifyPermissions
- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

복원

의 RDSPermissions 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamodbBackupPermissions
- KMSDynamoDBPermissions

복원

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamoDBRestorePermissions
- KMSPermissions

Amazon EBS

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- EBSResourcePermissions
- EBSTagAndDeletePermissions
- EBSCopyPermissions
- EBSSnapshotTierPermissions
- GetResourcesPermissions
- BackupVaultPermissions

복원

의 EBSPermissions 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

다음 명령문을 추가합니다.

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

복원

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

- `EBSPermissions`
- `EC2DescribePermissions`
- `EC2RunInstancesPermissions`
- `EC2TerminateInstancesPermissions`
- `EC2CreateTagsPermissions`

다음 명령문을 추가합니다.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

복원

의 `EFSPermissions` 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

Amazon FSx

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- FsxBackupPermissions
- FsxCreateBackupPermissions
- FsxPermissions
- FsxVolumePermissions
- FsxListTagsPermissions
- FsxDeletePermissions
- FsxResourcePermissions
- KMSPermissions

복원

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

- FsxPermissions
- FsxTagPermissions
- FsxBackupPermissions
- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon RDS

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- DynamoDBBackupPermissions
- RDSBackupPermissions
- RDSClusterModifyPermissions

- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

복원

의 RDSPermissions 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

Amazon S3

백업

AWSBackupServiceRolePolicyForS3Backup 단원에서 시작합니다.

백업을 다른 계정에 복사해야 하는 경우 BackupVaultPermissions 및 BackupVaultCopyPermissions 명령문을 추가하세요.

복원

AWSBackupServiceRolePolicyForS3Restore 단원에서 시작합니다.

AWS Storage Gateway

백업

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForBackup.

- StorageGatewayPermissions
- EBSTagAndDeletePermissions
- GetResourcesPermissions
- BackupVaultPermissions

다음 명령문을 추가합니다.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
```

```
        ],
        "Resource":"*"
},
```

복원

다음 문장으로 시작하십시오 AWSBackupServiceRolePolicyForRestores.

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

가상 머신

백업

의 `BackupGatewayBackupPermissions` 문장으로 시작하세요 AWSBackupServiceRolePolicyForBackup.

복원

의 `GatewayRestorePermissions` 문장으로 시작하세요 AWSBackupServiceRolePolicyForRestores.

암호화된 백업

암호화된 백업을 복원하려면 다음 중 하나를 수행합니다.

- AWS KMS 키 정책의 허용 목록에 내 역할을 추가하세요.
- 복원용 IAM 역할에 다음 명령문을 추가하십시오. AWSBackupServiceRolePolicyForRestores
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

에 대한 정책 업데이트 AWS Backup

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Backup 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하세요.

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup - 기존 정책에 대한 업데이트	AWS Backup 이 정책에 `backup:TagResource` 권한을 추가했습니다. 복구 지점을 만드는 동안 태깅 권한을 얻으려면 권한이 필요합니다.	2024년 5월 17일
AWSBackupServiceRolePolicyForS3Backup-기존 정책 업데이트	AWS Backup 이 정책에 `backup:TagResource` 권한을 추가했습니다. 복구 지점을 만드는 동안 태깅 권한을 얻으려면 권한이 필요합니다.	2024년 5월 17일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	AWS Backup 이 정책에 `backup:TagResource` 권한을 추가했습니다. 복구 지점을 만드는 동안 태깅 권한을 얻으려면 권한이 필요합니다.	2024년 5월 17일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	권한을 `rds:DeleteDBInstanceAutomatedBackups` 추가했습니다. 이 권한은 연속 백업 및 point-in-time-restore Amazon RDS 인스턴스를 지원하는 AWS Backup 데 필요합니다.	2024년 5월 1일
AWSBackupFullAccess-기존 정책 업데이트	AWS Backup Storage Gateway API 모델의 변경을 수용하기 위해 Amazon 리소스 이름 (ARN) `storagega`	2024년 5월 1일

변경 사항	설명	날짜
	teway:ListVolumes 에서 ~까지의 arn:aws:s toragegateway:*:*: gateway/* 권한을 업데이트했습니다. *	
AWSBackupOperatorAccess-기존 정책 업데이트	AWS Backup Storage Gateway API 모델의 변경을 수용하기 위해 Amazon 리소스 이름 (ARN) storagega teway:ListVolumes 에서 ~까지의 arn:aws:s toragegateway:*:*: gateway/* 권한을 업데이트했습니다. *	2024년 5월 1일

변경 사항	설명	날짜
AWSServiceRolePolicyForBackupRestoreTesting- 기존 정책 업데이트	복원 테스트 계획을 수행하기 위해 복구 지점과 보호된 리소스를 설명하고 나열할 수 있는 다음 권한이 추가되었습니다:backup:DescribeRecoveryPoint ,backup:DescribeProtectedResource ,backup:ListProtectedResources ,. backup:ListRecoveryPointsByResource Amazon EBS 아카이브 계층 ec2:DescribeSnapshotTierStatus 스토리지를 지원하는 권한이 추가되었습니다. Amazon Aurora 연속 백업을 지원하는 권한이 rds:DescribeDBClusterAutomatedBackups 추가되었습니다. Amazon Redshift 백업의 복원 테스트를 지원하기 위해 다음과 같은 권한이 추가되었습니다. redshift:DescribeClusters redshift:DeleteCluster Amazon Timestream 백업의 복원 테스트를 지원하는 권한	2024년 2월 14일

변경 사항	설명	날짜
	이 timestream:DeleteTable 추가되었습니다.	
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	권한 추가 ec2:DescribeSnapshotTierStatus 및. ec2:RestoreSnapshotTier 이러한 권한은 사용자가 아카이브 AWS Backup 스토리지에서 함께 저장된 Amazon EBS 리소스를 복원할 수 있는 옵션을 갖기 위해 필요합니다. EC2 인스턴스 복원의 경우 다음 정책 문과 같이 EC2 인스턴스를 시작할 수 있는 권한도 포함해야 합니다.	2023년 11월 27일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	백업된 Amazon EBS 리소스를 아카이브 스토리지 티어로 전환하기 위한 추가 스토리지 옵션을 ec2:DescribeSnapshotTierStatus 지원하고 ec2:ModifySnapshotTier 권한을 추가했습니다. 에 저장된 Amazon EBS 리소스를 아카이브 스토리지로 전환할 수 있는 옵션을 사용자에게 AWS Backup 제공하려면 이러한 권한이 필요합니다.	2023년 11월 27일

변경 사항	설명	날짜
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	백업된 Amazon EBS 리소스를 아카이브 스토리지 티어로 전환하기 위한 추가 스토리지 옵션을 `ec2:DescribeSnapshotTierStatus` 지원하고 `ec2:ModifySnapshotTier` 권한을 추가했습니다. 에 저장된 Amazon EBS 리소스를 아카이브 스토리지로 전환할 수 있는 옵션을 사용자에게 AWS Backup 제공하려면 이러한 권한이 필요합니다. Aurora 클러스터의 PITR (point-in-time 복원) 에 필요한 권한 `rds:DescribeDBClusterSnapshots` 및 `rds:RestoreDBClusterToPointInTime` 를 추가했습니다.	
AWSServiceRolePolicyForBackupRestoreTesting - 새 정책	복원 테스트를 수행하는 데 필요한 권한을 제공합니다. 권한에는 Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx for ONTAP, FSx for OpenZFS, Amazon Neptune, Amazon RDS, Amazon S3 등 복원 테스트에 포함할 서비스에 대한 `list, read, and write` 작업이 포함됩니다.	2023년 11월 27일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	`IamPassRolePermissions` 및 `IamCreateServiceLinkedRolePermissions` 에 `restore-testing.backup.amazonaws.com` 이 추가되었습니다. 이 추가는 고객을 대신하여 복원 테스트를 수행하는 AWS Backup 데 필요합니다.	2023년 11월 27일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	Aurora 클러스터의 PITR (point-in-time 복원) 에 필요한 권한 `rds:DescribeDBClusterSnapshots` 및 `rds:RestoreDBClusterToPointInTime` 를 추가했습니다.	2023년 9월 6일
AWSBackupFullAccess-기존 정책 업데이트	Aurora 클러스터의 연속 백업 및 point-in-time 복원에 필요한 권한이 `rds:DescribeDBClusterAutomatedBackups` 추가되었습니다.	2023년 9월 6일
AWSBackupOperatorAccess-기존 정책 업데이트	Aurora 클러스터의 연속 백업 및 point-in-time 복원에 필요한 권한이 `rds:DescribeDBClusterAutomatedBackups` 추가되었습니다.	2023년 9월 6일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	권한을 `rds:DescribeDBClusterAutomatedBackups` 추가했습니다. 이 권한은 Aurora AWS Backup 클러스터의 연속 백업 및 point-in-time 복원을 지원하는 데 필요합니다. 보존 기간이 끝나면 AWS Backup 수명 주기에서 Amazon Aurora 연속 복구 지점을 삭제하고 연결을 끊을 수 있도록 허용하는 권한이 `rds:DeleteDBClusterAutomatedBackups` 추가되었습니다. 이 권한은 Aurora 복구 시점이 `EXIPIRED` 상태로의 전환을 방지하는 데 필요합니다. Aurora 클러스터와 상호 작용할 수 `rds:ModifyDBCluster` AWS Backup 있는 권한이 추가되었습니다. 이 권한 추가를 통해 사용자는 원하는 구성에 따라 연속 백업을 활성화하거나 비활성화할 수 있습니다.	2023년 9월 6일
AWSBackupFullAccess-기존 정책 업데이트	새 저장소 유형에 대한 리소스 공유 연결을 가져올 수 있는 권한을 사용자에게 `ram:GetResourceShareAssociations` 부여하는 작업을 추가했습니다.	2023년 8월 8일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	새 저장소 유형에 대한 리소스 공유 연결을 가져올 수 있는 권한을 사용자에게 `ram:GetResourceShareAssociations` 부여하는 작업이 추가되었습니다.	2023년 8월 8일
AWSBackupServiceRolePolicyForS3Backup-기존 정책 업데이트	버킷 인벤토리를 사용하여 백업 성능을 향상시킬 수 있는 권한이 `s3:PutInventoryConfiguration` 추가되었습니다.	2023년 8월 1일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	리소스를 복원하기 위해 태그를 추가할 수 있는 권한을 사용자에게 부여하는 다음 작업이 추가되었습니다. `RunInstances` 또는 `storagegateway:AddTagsToResource` `elasticfilesystem:TagResource` `CreateVolume` `fsx:TagResource` , `ec2:CreateTags` 및 중 하나만 `ec2:CreateAction` 포함하는 경우`cloudformation:TagResource` .	2023년 5월 22일
AWSBackupAuditAccess-기존 정책 업데이트	사용자가 리소스를 더 쉽게 선택할 수 있도록 API 내 리소스 선택을 와일드카드 `config:DescribeComplianceByConfigRule` 리소스로 대체했습니다.	2023년 4월 11일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	고객 관리 키를 사용하여 Amazon EFS를 복원할 수 있는 다음 권한이 추가되었습니다`kms:GenerateDataKeyWithoutPlaintext` . 이렇게 하면 사용자가 Amazon EFS 리소스를 복원하는 데 필요한 권한을 갖도록 할 수 있습니다.	2023년 3월 27일
AWSServiceRolePolicyForBackupReports-기존 정책 업데이트	AWS Backup Audit Manager가 감사 관리자가 관리하는 규칙에 액세스할 AWS Backup 수 있도록 `config:DescribeConfigRules` 및 `config:DescribeConfigRuleEvaluationStatus` 작업을 업데이트했습니다 AWS Config .	2023년 3월 9일
AWSBackupServiceRolePolicyForS3Restore-기존 정책 업데이트	정책에 `kms:Decrypt` `s3:PutBucketOwnershipControls` , 및 `s3:GetBucketOwnershipControls` 권한이 추가되었습니다. `AWSBackupServiceRolePolicyForS3Restore` 이러한 권한은 원본 백업에서 KMS 암호화를 사용하는 경우 객체 복원을 지원하는 데 필요하고 원본 버킷에 ACL 대신 객체 소유권이 구성된 경우 객체 복원에 필요합니다.	2023년 2월 13일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	가상 머신의 VMware 태그를 사용하여 백업을 예약하고 스케줄 기반 대역폭 제한을 지원하는 다음 권한이 추가되었습니다:backup-gateway:GetHypervisorPropertyMappings ,,,, backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings , backup-gateway:GetHypervisor 및. backup-gateway:StartVirtualMachinesMetadataSync backup-gateway:GetBandwidthRateLimitSchedule backup-gateway:PutBandwidthRateLimitSchedule	2022년 12월 15일
AWSBackupOperatorAccess-기존 정책 업데이트	가상 시스템의 VMware 태그를 사용하여 백업을 예약하고 스케줄 기반 대역폭 제한을 지원하는 다음 권한이 추가되었습니다:,,,. backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine backup-gateway:GetHypervisor backup-gateway:GetBandwidthRateLimitSchedule	2022년 12월 15일

변경 사항	설명	날짜
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync - 새 정책	AWS Backup Gateway가 온프레미스 네트워크에 있는 가상 시스템의 메타데이터를 Backup Gateway와 동기화할 수 있는 권한을 제공합니다.	2022년 12월 15일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	Timestream 백업 작업을 지원하기 위해 다음과 같은 권한이 추가되었습니다:`timestream:StartAwsBackupJob` ,`timestream:GetAwsBackupStatus` ,`timestream:ListTables` ,, `timestream:ListDatabases` `timestream:ListTagsForResource` `timestream:DescribeTable` , `timestream:DescribeDatabase` 및. `timestream:DescribeEndpoints`	2022년 12월 13일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	타임스트림 복원 작업을 지원하는 다음 권한이 추가되었습니다:timestream:StartAwsRestoreJob ,,timestream:GetAwsRestoreStatus ,timestream:ListTables ,timestream:ListTagsForResource ,timestream:ListDatabases , timestream:DescribeTable timestream:DescribeDatabase s3:GetBucketAcl , 및. timestream:DescribeEndpoints	2022년 12월 13일
AWSBackupFullAccess-기존 정책 업데이트	Timestream 리소스를 지원하기 위해 다음과 같은 권한이 추가되었습니다: timestream:ListTables timestream:ListDatabases , s3:ListAllMyBuckets 및. timestream:DescribeEndpoints	2022년 12월 13일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	Timestream 리소스를 지원하는 다음 권한을 추가했습니다:timestream:ListDatabases , timestream:ListTables s3:ListAllMyBuckets , 및. timestream:DescribeEndpoints	2022년 12월 13일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	Timestream 리소스를 지원하는 다음 권한이 추가되었습니다:timestream:ListDatabases ,,timestream:ListTables ,timestream:ListTagsForResource ,timestream:DescribeDatabase , timestream:DescribeTable timestream:GetAwsBackupStatus timestream:GetAwsRestoreStatus , 및. timestream:DescribeEndpoints	2022년 12월 13일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	Amazon Redshift 리소스를 지원하기 위해redshift:DescribeClusters ,,,,, redshift:DescribeClusterSubnetGroups redshift:DescribeNodeConfigurationOptions redshift:DescribeOrderableClusterOptions redshift:DescribeClusterParameterGroups redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules , 및 권한을 추가했습니다. ec2:DescribeAddresses	2022년 11월 27일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	Amazon Redshift 리소스를 지원하기 위해redshift:DescribeClusters ,,,, redshift:DescribeClusterSubnetGroups redshift:DescribeNodeConfigurationOptions redshift:DescribeOrderableClusterOptions , redshift:DescribeClusterParameterGroups, 다음과 같은 권한이 추가되었습니다. redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules , 및. ec2:DescribeAddresses	2022년 11월 27일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	Amazon Redshift 복원 작업을 지원하기 위해 다음과 같은 권한이 추가되었습니다:redshift:RestoreFromCluster Snapshot , redshift:RestoreTableFromClusterSnapshot redshift:DescribeClusters , 및. redshift:DescribeTableRestoreStatus	2022년 11월 27일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	Amazon Redshift 백업 작업을 지원하는 다음 권한을 추가했습니다:`redshift:CreateClusterSnapshot` ,,`redshift:DescribeClusterSnapshots` , `redshift:DescribeTags` `redshift:DeleteClusterSnapshot` `redshift:DescribeClusters` , 및. `redshift:CreateTags`	2022년 11월 27일
AWSBackupFullAccess-기존 정책 업데이트	CloudFormation 리소스를 지원하기 위해 다음 권한이 추가되었습니다. `cloudformation:ListStacks`	2022년 11월 27일
AWSBackupOperatorAccess-기존 정책 업데이트	CloudFormation 리소스를 지원하기 위해 다음 권한이 추가되었습니다`cloudformation:ListStacks` .	2022년 11월 27일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	CloudFormation 리소스를 지원하는 다음 권한이 추가되었습니다: `redshift:DescribeClusterSnapshots` `redshift:DescribeTags` ,`redshift:DeleteClusterSnapshot` ,`redshift:DescribeClusters` .	2022년 11월 27일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	AWS CloudFormation 애플리케이션 스택 백업 작업을 지원하는 다음 권한이 추가되었습니다: `cloudformation:GetTemplate cloudformation:DescribeStacks ,,cloudformation:ListStackResources .`	2022년 11월 16일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	AWS CloudFormation 애플리케이션 스택 백업 작업을 지원하기 위해 다음 권한이 추가되었습니다. `cloudformation:CreateChangeSet cloudformation:DescribeChangeSet`	2022년 11월 16일
AWSBackupOrganizationAdminAccess-기존 정책 업데이트	조직 관리자가 위임된 관리자 기능을 사용할 수 있도록 이 정책에 다음 권한을 추가했습니다.`organizations:ListDelegatedAdministrator` , 및 `organizations:RegisterDelegatedAdministrator organizations:DeregisterDelegatedAdministrator`	2022년 11월 27일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	Amazon EC2 인스턴스에서 SAP HANA를 지원하는 다음 권한을 추가했습니다:ssm-sap:GetOperation ,,ssm-sap:ListDatabases , ssm-sap:BackupDatabase ssm-sap:UpdateHanaBackupSettings ssm-sap:GetDatabase , 및. ssm-sap:ListTagsForResource	2022년 11월 20일
AWSBackupFullAccess-기존 정책 업데이트	Amazon EC2 인스턴스에서 SAP HANA를 지원하기 위한 다음 권한을 추가했습니다:ssm-sap:GetOperation , ssm-sap:ListDatabases ssm-sap:GetDatabase , 및. ssm-sap:ListTagsForResource	2022년 11월 20일
AWSBackupOperatorAccess-기존 정책 업데이트	Amazon EC2 인스턴스에서 SAP HANA를 지원하기 위한 다음 권한을 추가했습니다:ssm-sap:GetOperation , ssm-sap:ListDatabases ssm-sap:GetDatabase , 및. ssm-sap:ListTagsForResource	2022년 11월 20일

변경 사항	설명	날짜
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	Amazon EC2 인스턴스에서 SAP HANA를 지원하기 위해 다음 권한이 추가되었습니다. `ssm-sap:GetOperation`	2022년 11월 20일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	EC2 인스턴스에 백업 게이트웨이 복원 작업을 지원하는 다음 권한이 추가되었습니다. `ec2:CreateTags`	2022년 11월 20일
AWSBackupDataTransferAccess-기존 정책 업데이트	Amazon EC2 리소스에서 SAP HANA의 안전한 스토리지 데이터 전송을 지원하는 다음 권한을 추가했습니다:`backup-storage:StartObject` ,`backup-storage:PutChunk` ,`backup-storage:GetChunk` , `backup-storage:ListChunks` `backup-storage:ListObjects` `backup-storage:GetObjectMetadata` , 및. `backup-storage:NotifyObjectComplete`	2022년 11월 20일

변경 사항	설명	날짜
AWSBackupRestoreAccessForSAPHANA-기존 정책 업데이트	리소스 소유자가 Amazon EC2 리소스에서 SAP HANA 복원을 수행할 수 있는 다음 권한 (backup:Get* ,,,,backup:List* ,backup:Describe* ,backup:StartBackupJob ,backup:StartRestoreJob ,ssm-sap:GetOperation , ssm-sap:ListDatabases ssm-sap:BackupDatabase ssm-sap:RestoreDatabase ssm-sap:UpdateHanaBackupSettings ssm-sap:GetDatabase , 및) 이 추가되었습니다. ssm-sap:ListTagsForResource	2022년 11월 20일
AWSBackupServiceRolePolicyForS3Backup-기존 정책 업데이트	Amazon S3의 백업 s3:GetBucketAcl 작업을 지원하는 권한이 추가되었습니다. AWS Backup	2022년 8월 24일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	다중 가용 영역 (다중 AZ) 기능을 지원하는 데이터베이스 인스턴스를 생성할 수 있는 액세스 권한을 부여하는 다음 작업을 추가했습니다. rds:CreateDBInstance	2022년 7월 20일

변경 사항	설명	날짜
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	리소스 `s3:GetBucketTagging` 와일드카드를 사용하여 백업할 버킷을 선택할 수 있는 권한을 사용자에게 부여하는 권한을 추가했습니다. 이 권한이 없으면 리소스 와일드카드를 사용하여 백업할 버킷을 선택한 사용자는 성공하지 못합니다.	2022년 5월 6일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	기존 `fsx:CreateBackup` 및 `fsx:ListTagsForResource` 작업 범위에 볼륨 리소스를 추가하고 ONTAP 볼륨 레벨 백업을 위한 `fsx:DescribeVolumes` FSx를 지원하는 새 작업을 추가했습니다.	2022년 4월 27일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	사용자에게 ONTAP `fsx:DescribeVolumes` 볼륨`fsx:CreateVolumeFromBackup` ,, 및 에 대한 FSx를 복원할 수 있는 권한을 부여하는 다음 작업을 추가했습니다. `fsx:DeleteVolume` `fsx:UntagResource`	2022년 4월 27일
AWSBackupServiceRolePolicyForS3Backup-기존 정책 업데이트	백업 작업 중에 Amazon S3 버킷에 대한 변경 알림을 수신할 권한을 사용자에게 부여하는 다음 `s3:GetBucketNotification` 작업이 추가되었습니다. `s3:PutBucketNotification`	2022년 2월 25일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForS3Backup - 새 정책	사용자에게 Amazon S3 버킷을 백업할 수 있는 권한을 부여하는 다음 작업을 추가했습니다. `s3:GetInventoryConfiguration` `s3:PutInventoryConfiguration` ,`s3:ListBucketVersions` , `s3:ListBucket` `s3:GetBucketTagging` ,`s3:GetBucketVersioning` ,`s3:GetBucketNotification` ,`s3:GetBucketLocation` , `s3:ListAllMyBuckets` 사용자에게 Amazon S3 객체를 백업할 수 있는 권한을 부여하는 다음 작업을 추가했습니다:`s3:GetObject` , `s3GetObjectAcl` `s3:GetObjectVersionTagging` ,`s3:GetObjectVersionAcl` ,`s3:GetObjectTagging` , 및`s3:GetObjectVersion` . 암호화된 Amazon S3 데이터를 백업할 권한을 사용자에게 부여하는 다음 작업을 추가했	2022년 2월 17일

변경 사항	설명	날짜
	습니다kms:DescribeKey . kms:Decrypt Amazon EventBridge 규칙을 사용하여 Amazon S3 데이터를 증분 백업할 수 있는 권한을 사용자에게 부여하는 다음 작업을 추가했습니다:events:DescribeRule ,,events:EnableRule ,events:PutRule , events:DeleteRule events:PutTargets ,events:RemoveTargets ,events:ListTargetsByRule , events:DisableRule cloudwatch:GetMetricData , 및events:ListRules .	

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForS3Restore - 새 정책	사용자에게 Amazon S3 버킷을 복원할 수 있는 권한을 부여하는 다음 작업을 추가했습니다:s3:CreateBucket ,s3:ListBucketVersions ,s3:ListBucket , s3:GetBucketVersioning s3:GetBucketLocation , 및s3:PutBucketVersioning . 사용자에게 Amazon S3 버킷을 복원할 수 있는 권한을 부여하는 다음 작업을 추가했습니다:s3:GetObject ,s3:GetObjectVersion , s3:DeleteObject s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging ,s3:PutObjectTagging ,s3:GetObjectAcl , s3:PutObjectAcl s3:PutObject , 및s3:ListMultipartUploadParts . 복원된 Amazon S3 데이터를 암호화할 수 있는 권한을 사용자에게 부여하는 다음 작업이 추가되었습니다: kms:Decry	2022년 2월 17일

변경 사항	설명	날짜
	pt kms:DescribeKey , 및kms:GenerateDataKey .	
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	사용자에게 버킷 목록을 보고 백업 계획에 할당할 버킷을 선택할 수 있는 권한을 s3:ListAllMyBuckets 부여하도록 추가되었습니다.	2022년 2월 14일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	사용자에게 가상 머신 목록을 보고 백업 계획에 할당할 가상 머신을 선택할 수 있는 권한을 부여하기 위해 추가되었습니다backup-gateway:ListVirtualMachines . 사용자에게 가상 머신의 태그를 나열할 수 있는 권한을 backup-gateway:ListTagsForResource 부여하기 위해 추가되었습니다.	2021년 11월 30일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	사용자에게 가상 머신 백업을 복원할 권한을 backup-gateway:Backup 부여하기 위해 추가되었습니다. AWS Backup 또한 사용자에게 가상 머신 백업에 할당된 태그를 나열할 수 있는 권한을 backup-gateway:ListTagsForResource 부여하기 위해 추가되었습니다.	2021년 11월 30일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	사용자에게 가상 머신 백업 복원 권한을 `backup-gateway:Restore` 부여하기 위해 추가되었습니다.	2021년 11월 30일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	사용자에게 AWS Backup 게이트웨이를 사용하여 가상 머신을 백업, 복원 및 관리할 수 있는 권한을 부여하는 작업을 추가했습니다:,backup-gateway:AssociateGatewayToServer ,,,,backup-gateway:CreateGateway ,backup-gateway:DeleteGateway ,backup-gateway:DeleteHypervisor ,backup-gateway:DisassociateGatewayFromServer ,backup-gateway:ImportHypervisorConfiguration ,backup-gateway:ListGateways ,backup-gateway:ListHypervisors ,backup-gateway:ListTagsForResource ,backup-gateway:ListVirtualMachines ,backup-gateway:PutMaintenanceStartTime ,backup-gateway:TagResource ,backup-gateway:TestHypervisorConfiguration ,backup-gateway:UntagResource ,backup-gateway:Upd	2021년 11월 30일

변경 사항	설명	날짜
	ateGatewayInformation , 및backup-gateway:UpdateHypervisor .	
AWSBackupOperatorAccess-기존 정책 업데이트	사용자에게 가상 시스템을 백업할 수 있는 권한을 부여하는 다음 작업을 추가했습니다:backup-gateway:ListGateways , backup-gateway:ListHypervisors backup-gateway:ListTagsForResource ,,backup-gateway:ListVirtualMachines .	2021년 11월 30일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	AWS Backup의 고급 DynamoDB 백업 기능을 사용하여 백업할 DynamoDB 테이블의 태그를 나열할 수 있는 권한을 사용자에게 dynamodb:ListTagsOfResource 부여하도록 추가되었습니다.	2021년 11월 23일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	고급 백업 기능을 사용하여 DynamoDB 테이블을 백업할 수 있는 권한을 사용자에게 `dynamodb:StartAwsBackupJob` 부여하기 위해 추가되었습니다. 소스 DynamoDB 테이블의 태그를 백업으로 복사할 수 있는 권한을 사용자에게 `dynamodb:ListTagsOfResource` 부여하기 위해 추가되었습니다.	2021년 11월 23일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	의 고급 DynamoDB 고급 백업 기능을 사용하여 AWS Backup 백업한 DynamoDB 테이블을 복원할 권한을 사용자에게 `dynamodb:RestoreTableFromAwsBackup` 부여하도록 추가되었습니다.	2021년 11월 23일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	의 고급 DynamoDB 고급 백업 기능을 사용하여 AWS Backup 백업한 DynamoDB 테이블을 복원할 권한을 사용자에게 `dynamodb:RestoreTableFromAwsBackup` 부여하도록 추가되었습니다.	2021년 11월 23일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	작업이 `rds:DescribeDBSnapshots` 중복되었기 때문에 작업이 `backup:GetRecoveryPointRestoreMetadata` 제거되었습니다. AWS Backup 둘 다 `backup:GetRecoveryPointRestoreMetadata` 필요하지도 않았고 `backup:Get*` AWSBackupOperatorAccess 일부로도 필요했습니다. 또한 둘 다 `rds:DescribeDBSnapshots` 필요하지도 AWS Backup 않았고 `rds:describeDBSnapshots` 일부로도 AWSBackupOperatorAccess 필요했습니다.	2021년 11월 23일

변경 사항	설명	날짜
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	고객이 백업 계획에 할당할 리소스를 선택할 때 AWS Backup지원되는 리소스 목록을 보고 선택할 수 있도록 `fsx:DescribeFileSystems` 하는 새 작업 `elasticfilesystem:DescribeFileSystems` `dynamodb:ListTables` `storagegateway:ListVolumes` `ec2:DescribeVolumes` `ec2:DescribeInstances` `rds:DescribeDBInstances` `rds:DescribeDBClusters` ,,,,,, 및 가 추가되었습니다.	2021년 11월 10일
AWSBackupAuditAccess - 새 정책	사용자에게 AWS Backup Audit Manager를 사용할 수 있는 권한을 `AWSBackupAuditAccess` 부여하기 위해 추가되었습니다. 권한에는 규정 준수 프레임워크를 구성하고 보고서를 생성하는 기능이 포함됩니다.	2021년 8월 24일
AWSServiceRolePolicyForBackupReports - 새 정책	사용자가 구성한 프레임워크를 준수하기 위해 백업 설정, 작업 및 리소스의 모니터링을 자동화하는 서비스 연결 역할에 대한 권한을 부여하도록 추가되었습니다`AWSServiceRolePolicyForBackupReports` .	2021년 8월 24일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	만료된 복구 지점을 자동으로 삭제할 수 있도록 최선을 다해 서비스 연결 역할을 `iam:CreateServiceLinkedRole` 생성하도록 추가되었습니다. 이 서비스 연결 역할이 없으면 고객이 복구 지점을 생성하는 데 사용한 원래 IAM 역할을 삭제한 후 만료된 복구 지점을 삭제할 AWS Backup 수 없습니다.	2021년 7월 5일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	백업 계획 수명 주기 설정을 기반으로 만료된 DynamoDB 복구 지점의 삭제를 자동화할 수 있는 `DeleteRecoveryPoint` 권한을 부여하는 새 작업이 `dynamodb:DeleteBackup` 추가되었습니다.	2021년 7월 5일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	작업이 `rds:DescribeDBSnapshots` 중복되었기 때문에 해당 작업을 `backup:GetRecoveryPointRestoreMetadata` 제거했습니다. AWS Backup 둘 다 필요하지 않았고 `backup:GetRecoveryPointRestoreMetadata` Also의 `backup:Get*` 일부로서 둘 다 AWS Backup `rds:DescribeDBSnapshots` 필요하지도 않았고 AWSBackupOperatorAccess 일부로도 필요했습니다. `rds:describeDBSnapshots` AWSBackupOperatorAccess	2021년 5월 25일

변경 사항	설명	날짜
AWSBackupOperatorAccess-기존 정책 업데이트	작업이 backup:GetRecoveryPointRestoreMetadata rds:DescribeDBSnapshots 중복되어 삭제되었습니다. AWS Backup 둘 다 backup:GetRecoveryPointRestoreMetadata 필요하지도 않았고 backup:Get* AWSBackupOperatorAccess 일부로도 필요했습니다. 또한 둘 다 rds:DescribeDBSnapshots 필요하지도 AWS Backup 않았고 rds:describeDBSnapshots 일부로도 AWSBackupOperatorAccess 필요했습니다.	2021년 5월 25일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	복원 프로세스 중에 Amazon FSx 파일 시스템에 태그를 적용할 수 있는 StartRestoreJob 권한을 부여하는 새 작업이 fsx:TagResource 추가되었습니다.	2021년 5월 24일
AWSBackupServiceRolePolicyForRestores-기존 정책 업데이트	Amazon EC2 인스턴스를 복구 지점으로부터 복원할 수 있는 StartRestoreJob 권한을 ec2:DescribeImages 부여하고 ec2:DescribeInstances 새 작업을 추가했습니다.	2021년 5월 24일

변경 사항	설명	날짜
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	Amazon FSx 복구 지점을 지역 및 계정 간에 복사할 수 있는 StartCopyJob 권한을 부여하는 새 작업을 fsx:CopyBackup 추가했습니다.	2021년 4월 12일
AWSBackupServiceLinkedRolePolicyForBackup-기존 정책 업데이트	Amazon FSx 복구 지점을 지역 및 계정 간에 복사할 수 있는 StartCopyJob 권한을 부여하는 새 작업을 fsx:CopyBackup 추가했습니다.	2021년 4월 12일
AWSBackupServiceRolePolicyForBackup-기존 정책 업데이트	다음 요구 사항을 준수하도록 업데이트되었습니다. 암호화된 DynamoDB 테이블의 백업을 AWS Backup 생성하려면 백업에 사용되는 IAM 역할에 kms:Decrypt 권한을 kms:GenerateDataKey 추가해야 합니다.	2021년 3월 10일

변경 사항	설명	날짜
AWSBackupFullAccess-기존 정책 업데이트	다음 요구 사항을 준수하도록 업데이트되었습니다. Amazon RDS 데이터베이스의 연속 백업을 구성하는 AWS Backup 데 사용하려면 백업 계획 구성에서 정의한 IAM 역할에 API 권한이 `rds:ModifyDBInstance` 있는지 확인하십시오. Amazon RDS 연속 백업을 복원하려면 복원 작업을 위해 제출한 IAM 역할에 `rds:RestoreDBInstanceToPointInTime` 권한을 추가해야 합니다. AWS Backup 콘솔에서 point-in-time 복구에 사용할 수 있는 기간을 설명하려면 IAM 관리형 정책에 `rds:DescribeDBInstanceAutomatedBackups` API 권한을 포함해야 합니다.	2021년 3월 10일
AWS Backup 변경 내용 추적 시작	AWS Backup AWS-managed 정책의 변경 사항 추적을 시작했습니다.	2021년 3월 10일

AWS Backup에 서비스 연결 역할 사용

AWS Backup AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Backup서비스 연결 역할은 사전 정

의되며 서비스가 사용자를 AWS Backup 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

주제

- 역할을 사용하여 백업 및 복사
- AWS Backup Audit Manager의 역할 사용
- 복원 테스트를 위한 역할 사용

역할을 사용하여 백업 및 복사

AWS Backup AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Backup서비스 연결 역할은 사전 정의되며 서비스가 사용자를 AWS Backup 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS Backup 더 쉬워집니다. AWS Backup 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS Backup 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Backup 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS Backup

AWS Backup 이름이 지정된 AWSServiceRoleForBackup서비스 연결 역할을 사용합니다. 백업할 수 있는 리소스를 나열하고 백업을 복사할 수 있는 AWS Backup 권한을 제공합니다.

AWS Backup 또한 역할을 사용하여 Amazon EC2를 제외한 모든 리소스 유형의 모든 백업을 삭제합니다.

AWSServiceRoleForBackup 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `backup.amazonaws.com`

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSBackupServiceLinkedRolePolicyforBackup.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 백업할 리소스를 나열하거나 계정 간 백업을 설정하거나, 또는 AWS API에서 백업을 수행하면 서비스 연결 역할이 자동으로 AWS Backup 생성됩니다. AWS Management Console AWS CLI

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 백업할 리소스를 나열하거나, 계정 간 백업을 설정하거나, 백업을 수행하면 서비스 연결 역할이 다시 AWS Backup 생성됩니다.

AWS Backup에 대한 서비스 링크 역할 편집

AWS Backup 서비스 연결 역할을 편집할 수 없습니다. AWSServiceRoleForBackup 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다. 먼저 모든 복구 시점을 삭제해야 합니다. 그런 다음, 모든 백업 저장소를 삭제해야 합니다.

> **Note**
>
> AWS Backup 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForBackup (콘솔) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 모든 복구 시점 및 백업 저장소(기본 저장소 제외)를 삭제하려면 백업 저장소 삭제의 절차를 따릅니다.
2. 기본 저장소를 삭제하려면 AWS CLI에서 다음 명령을 사용합니다.

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

AWSServiceRoleForBackup (AWS CLI) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 복구 지점을 모두 삭제하려면 를 사용하십시오 delete-recovery-point.
2. 모든 백업 저장소를 삭제하려면 `delete-backup-vault`를 사용합니다.

AWSServiceRoleForBackup (API) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 모든 복구 시점을 삭제하려면 `DeleteRecoveryPoint`를 사용합니다.
2. 모든 백업 저장소를 삭제하려면 `DeleteBackupVault`를 사용합니다.

수동으로 서비스 연결 역할 삭제

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForBackup 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하십시오.

AWS Backup 서비스 링크 역할이 지원되는 리전

AWS Backup 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Backup 지원되는 기능 및 리전을 참조하세요.

AWS Backup Audit Manager의 역할 사용

AWS Backup AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Backup서비스 연결 역할은 사전 정

의되며 서비스가 사용자를 AWS Backup 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS Backup 더 쉬워집니다. AWS Backup 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS Backup 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Backup 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS Backup

AWS Backup 이름이 지정된 서비스 연결 역할을 사용합니다. AWSServiceRoleForBackupReports—제어, 프레임워크 및 보고서를 만들 수 AWS Backup 있는 권한을 제공합니다.

AWSServiceRoleForBackupReports 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `backup.amazonaws.com`

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSServiceRolePolicyForBackupReports.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 프레임워크 또는 보고서 계획을 생성하면 AWS Management Console AWS CLI, 또는 AWS API가 서비스 연결 역할을 자동으로 AWS Backup 생성합니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 프레임워크 또는 보고서 계획을 생성하면 서비스 연결 역할이 다시 AWS Backup 생성됩니다.

AWS Backup에 대한 서비스 링크 역할 편집

AWS Backup AWSServiceRoleForBackupReports 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다. 모든 프레임워크와 보고서 계획을 삭제해야 합니다.

> **Note**
>
> AWS Backup 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForBackupReports (콘솔) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 모든 프레임워크를 삭제하려면 프레임워크 삭제를 참조하세요.
2. 모든 보고서 계획을 삭제하려면 보고서 계획 삭제를 참조하세요.

AWSServiceRoleForBackupReports (AWS CLI) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 모든 프레임워크를 삭제하려면 delete-framework를 사용합니다.
2. 모든 보고서 계획을 삭제하려면 를 사용하십시오 delete-report-plan.

AWSServiceRoleForBackupReports (API) 에서 사용하는 AWS Backup 리소스를 삭제하려면

1. 모든 프레임워크를 삭제하려면 DeleteFramework를 사용합니다.
2. 모든 보고서 계획을 삭제하려면 를 사용합니다 DeleteReportPlan.

수동으로 서비스 연결 역할 삭제

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForBackupReports 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

AWS Backup 서비스 링크 역할이 지원되는 리전

AWS Backup 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Backup 지원되는 기능 및 리전을 참조하세요.

복원 테스트를 위한 역할 사용

AWS Backup AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Backup서비스 연결 역할은 사전 정의되며 서비스가 사용자를 AWS Backup 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS Backup 더 쉬워집니다. AWS Backup 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS Backup 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Backup 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS Backup

AWS Backup 이름이 AWSServiceRolePolicyForBackupRestoreTesting지정된 서비스 연결 역할을 사용합니다. 복원 테스트를 수행할 수 있는 백업 권한을 제공합니다.

AWSServiceRolePolicyForBackupRestoreTesting 서비스 연결 역할은 다음 서비스가 역할을 맡을 것으로 신뢰합니다.

- `backup.amazonaws.com`

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSServiceRolePolicyForBackupRestoreTesting.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 복원 테스트를 수행하면 서비스 연결 역할이 자동으로 AWS Backup 생성됩니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 복원 테스트를 수행하면 서비스 연결 역할이 다시 AWS Backup 생성됩니다.

AWS Backup에 대한 서비스 링크 역할 편집

AWS Backup AWSServiceRolePolicyForBackupRestoreTesting 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

AWS Backup에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다. 복원 테스트 계획을 모두 삭제해야 합니다.

> **Note**
>
> AWS Backup 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRolePolicyForBackupRestoreTesting (콘솔) 에서 사용하는 AWS Backup 리소스를 삭제하려면

- 모든 복원 테스트 계획을 삭제하려면 복원 테스트를 참조하세요.

AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI) 에서 사용하는 AWS Backup 리소스를 삭제하려면

- 복원 테스트 계획을 삭제하려면 `delete-restore-testing-plan`을 사용하세요.

AWSServiceRolePolicyForBackupRestoreTesting (API) 에서 사용하는 AWS Backup 리소스를 삭제하려면

- 복원 테스트 계획을 삭제하려면 `DeleteRestoreTestingPlan`을 사용하세요.

수동으로 서비스 연결 역할 삭제

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRolePolicyForBackupRestoreTesting 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

AWS Backup 서비스 링크 역할이 지원되는 리전

AWS Backup 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Backup 지원되는 기능 및 리전을 참조하세요.

교차 서비스 혼동된 대리자 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. AWS에서는 교차 서비스 가장으로 인해 혼동된 대리자 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

AWS Backup이(가) 리소스에 다른 서비스를 제공하는 권한을 제한하려면 리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

AWS Backup을 사용하여 Amazon SNS 주제를 사용자 대신 게시할 경우, `aws:SourceArn`의 값은 AWS Backup 저장소여야 합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용합니다. 예: `arn:aws::servicename::123456789012:*`.

의 인프라 보안 AWS Backup

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS Backup 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 액세스할 AWS Backup 수 있습니다. 클라이언트가 전송 계층 보안(TLS) 1.2 이상을 지원해야 합니다. 클라이언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Diffie-Hellman Ephemeral)와 같은 PFS(전달 완전 보안)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

데이터 무결성 AWS Backup

AWS Backup 데이터 무결성 목표

AWS Backup 데이터를 전송, 저장 및 처리하는 동안 무결성을 유지하고자 합니다. AWS Backup 저장하는 데이터 유형에 관계없이 고객에게 동일한 수준의 보안을 제공한다는 점에서 저장된 리소스 데이터를 콘텐츠에 구애받지 않는 중요 정보로 취급합니다. AWS는 고객의 보안에 만전을 기하고 있으며 무단 액세스에 대해 정교한 기술적 및 물리적 조치를 취했습니다. 귀하는 귀하의 데이터가 분류되는 방식, 데이터를 저장하는 리전, 데이터를 제어, 보관 및 공개되지 않도록 보호하는 방법에 대한 완전한 통제권을 보유합니다.

AWS Backup 데이터 무결성 구현

AWS Backup 다른 서비스 AWS 및 Amazon 서비스와 협력하여 저장하고 상호 작용하는 데이터의 무결성을 유지합니다. 사용되는 도구는 다양하며 다음을 포함할 수 있습니다(이에 국한되지는 않음).

- 객체 손상을 방지하기 위해 지속적으로 객체 체크섬 검증
- 전송 중 데이터 및 유휴 시 데이터의 무결성을 확인하기 위한 내부 체크섬
- 프라이머리 저장소에서 생성된 백업의 데이터를 기반으로 체크섬 계산
- 디스크 손상 또는 디바이스 장애 감지 시 자동으로 객체 스토리지 중복성을 정상 수준으로 복원하기 위해 시도
- 여러 물리적 위치에 데이터를 중복 저장
- 디바이스를 사용할 수 없거나 비트 로트가 감지되는 경우 추가 복제와 결합하여 초기 쓰기 중 여러 가용 영역에 걸쳐 객체 내구성 향상
- 데이터를 저장 또는 검색할 때 데이터 패킷 손상을 감지하기 위해 모든 네트워크 트래픽에서 체크섬 계산

AWS Backup 고급 기능을 갖춘 Amazon DynamoDB, Amazon EFS, Amazon S3, Amazon Timestream 및 백업 게이트웨이를 통해 연결된 VMware와 함께 실행되는 가상 머신에 데이터를 기본적으로 저장합니다. AWS Backup 아마존 오로라, 아마존 DocumentDB, 아마존 DynamoDB, 아마존 EBS, 아마존 EC2, 윈도우 파일 서버용 아마존 FSx, Lustre용 아마존 FSx, OpenZFS용 Amazon FSx 등 다른 서비스

에 저장된 데이터를 쉽게 백업할 수 있습니다. ONTAP, 아마존 넵튠, 아마존 RDS, 아마존 Redshift용 아마존 FSx NetApp

AWS Backup 데이터 무결성에 대한 객관적인 확인 및 감사

직접 저장하는 데이터와 AWS Backup 상호 작용하는 동료 AWS 서비스와 제휴하여 AWS Backup 저장하는 데이터에는 이러한 데이터 무결성을 뒷받침하는 Amazon Simple Storage Service (Amazon S3) 의 엄격한 프로세스가 적용됩니다. 독립적인 외부 감사자가 연간 SOC 감사 보고서를 통해 이러한 무결성을 확인합니다. 이 보고서는 AWS Management Console에서 AWS Artifact를 통해 확인할 수 있습니다.

법적 보류 및 AWS Backup

법적 보존은 보존 기간 중에 백업이 삭제되는 것을 방지하는 데 도움이 되는 관리 도구입니다. 보존이 적용되는 동안에는 보존 상태의 백업을 삭제할 수 없으며, 백업 상태를 변경하는 수명 주기 정책(예: `Deleted` 상태로의 전환)은 법적 보존이 제거될 때까지 연기됩니다. 백업은 둘 이상의 법적 보존을 보유할 수 있습니다.

에서 생성한 하나 이상의 백업 (복구 지점이라고도 함) 에 대해 해당 수명 주기에서 허용하는 AWS Backup 경우 법적 보류를 적용할 수 있습니다. 백업 유형 중 하나인 연속 백업의 최대 수명 주기는 35일입니다. 법적 자료 보존은 연속 백업 수명을 연장하지 않습니다.

법적 보존이 생성되면 리소스 유형 및 리소스 ID와 같은 특정 필터링 기준을 고려할 수 있습니다. 또한 법적 보존에 포함하려는 백업의 생성 날짜 범위를 정의할 수 있습니다. 법적 보존 및 백업은 다대다 관계를 가집니다. 즉, 백업에는 법적 보존 이상의 자료가 있을 수 있고 법적 보존에는 두 개 이상의 백업이 포함될 수 있습니다. 각 계정은 한 번에 최대 50개의 법적 보존을 활성화할 수 있습니다.

법적 보존은 해당 법적 보존이 적용된 원본 백업에만 적용됩니다. 백업이 여러 리전 또는 계정 간에 복사되는 경우(리소스에서 지원하는 경우) 백업은 법적 보존은 유지하지 않습니다. 법적 보전은 다른 리소스와 마찬가지로 고유한 ARN(Amazon 리소스 이름)이 연결되어 있습니다. 에서 생성한 복구 지점만 법적 보존의 일부가 될 AWS Backup 수 있습니다.

AWS Backup 볼트 잠금은 볼트에 추가 보호 및 불변성을 제공하는 반면, 법적 보존은 개별 백업(복구 시점) 삭제를 방지하는 추가 보호를 제공합니다. 법적 보존은 만료되지 않으며 백업 내의 데이터를 무기한 보존합니다. 보존 조치는 충분한 권한을 가진 사용자가 해제할 때까지 유효합니다.

법적 보존 생성

법적 보존이 생성되면 이미 생성된 복구 시점만 포함됩니다. 상태가 EXPIRED 또는 DELETING인 백업(복구 시점)은 법적 보존에 포함되지 않습니다. 상태가 CREATING인 복구 시점(백업)은 완료 시점에 따라 법적 보존에 포함되지 않을 수 있습니다.

법적 보류는 필수 IAM 권한이 있는 사용자가 추가할 수 있습니다.

콘솔을 사용하여 법적 보존 생성

법적 보류를 만들려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 콘솔 왼쪽의 대시보드에서 내 계정을 찾습니다. 법적 보류를 선택합니다.
3. 법적 보류 추가를 선택합니다.
4. 법적 보류 세부 정보, 법적 보류 범위, 법적 보류 태그의 세 가지 패널이 표시됩니다.

    a. 법적 보존 세부 정보에서 제공된 텍스트 상자에 법적 보존 제목 및 해당 보존에 대한 설명을 입력합니다.

    b. 법적 보존 범위 패널에서 보존에 포함할 리소스를 선택하는 방법을 선택합니다. 보존 조치를 생성할 때는 법적 자료 보존 범위 내에 있는 리소스를 선택하는 데 사용되는 방법을 선택합니다. 다음 중 하나를 포함하도록 선택할 수 있습니다.

    - 특정 리소스 유형 및 ID
    - 백업 저장소 선택
    - 계정 내 모든 리소스 유형 또는 모든 백업 저장소

    c. 법적 보존의 날짜 범위를 지정합니다. 날짜를 YYYY:MM:DD 형식(포함)으로 입력합니다.

    d. 필요에 따라 법적 보류 태그에 보존 태그를 추가할 수 있습니다. 태그는 향후 참조 및 정리를 위해 법적 보존을 분류하는 데 도움이 될 수 있습니다. 총 50개까지 태그를 추가할 수 있습니다.
5. 새 법적 보존의 구성에 만족하면 새 보존 추가 버튼을 클릭합니다.

를 사용하여 법적 보존을 생성합니다. AWS CLI

create-legal-hold명령을 사용하여 법적 보존을 생성할 수 있습니다.

```
aws backup create-legal-hold --title "my title" \
```

```
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

법적 보존 보기

AWS Backup 콘솔에서 또는 프로그래밍 방식으로 법적 보류 세부 정보를 볼 수 있습니다.

콘솔을 사용하여 법적 보류 보기

Backup 콘솔을 사용하여 계정 내의 모든 법적 보존을 보려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 대시보드의 왼쪽 부분에 있는 내 계정에서 법적 보존을 클릭합니다.
3. 법적 보존 표에는 기존 보존의 제목, 상태, 설명, ID 및 생성 날짜가 표시됩니다. 선택한 열을 기준으로 테이블을 필터링하려면 테이블 헤더 옆에 있는 캐럿(아래쪽 화살표)을 클릭합니다.

프로그래밍 방식으로 법적 보존 보기

모든 법적 보류를 프로그래밍 방식으로 보려면 다음 API 호출을 사용할 수 있습니다. ListLegalHolds및 GetLegalHold.

다음 JSON 템플릿을 에 사용할 수 있습니다. `GetLegalHold`

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response

{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
```

```
   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
   }
}
```

다음 JSON 템플릿을 에 사용할 수 있습니다. `ListLegalHolds`

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response

{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
```

```
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

가능한 상태 값은 다음과 같습니다.

상태 표시기	설명
생성	요청된 복구 시점은 보존 처리 중이며, 보존 생성이 완료되지 않았으므로 해당 복구 시점의 삭제 요청이 성공할 수 있습니다.
ACTIVE	법적 보존이 생성되었으며, 이 법적 보존에 나열된 모든 복구 시점은 보류됩니다.
취소 중	법적 보존 조치가 제거되는 중이며, 보존 중인 복구 시점에 대한 삭제 요청이 성공할 수 있습니다.
CANCELED	법적 보존이 완전히 해제되어 더 이상 효력이 없습니다. 복구 시점을 삭제할 수 있습니다.

법적 보존 해제

법적 보류는 충분한 권한을 가진 사용자가 제거할 때까지 유효합니다. 법적 보존을 제거하는 것을 법적 보존 취소, 삭제 또는 해제라고도 합니다. 법적 보존을 제거하면 연결된 모든 백업에서 삭제됩니다. 법적 보존 기간 중에 만료된 모든 백업은 법적 보존이 제거된 후 24시간 이내에 삭제됩니다.

콘솔을 사용하여 법적 보존 해제

콘솔을 사용하여 보존 조치를 해제하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 해제와 연결하려는 설명을 입력합니다.
3. 세부 정보를 검토한 다음 보존 해제를 클릭합니다.

4. 보존 해제 대화 상자가 나타나면 텍스트 상자에 `confirm`을 입력하여 보존 해제 의사를 확인합니다.

   - 보존을 취소함을 확인하는 상자를 선택합니다.

법적 보존 페이지에서 모든 보존을 확인할 수 있습니다. 해제가 성공하면 해당 보존의 상태가 `Released`로 표시됩니다.

프로그래밍 방식으로 법적 보류를 해제하십시오.

프로그래밍 방식으로 보류를 제거하려면 API 호출을 사용하세요. CancelLegalHold

다음 JSON 템플릿을 사용하세요.

```
DELETE /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}


DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject to
 this date.

Response

Empty body

200 if successful
other standard codes
```

AWS PrivateLink

AWS PrivateLink 인터페이스 VPC 엔드포인트를 생성하여 가상 사설 클라우드 (“VPC”) 와 AWS Backup 엔드포인트 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 VPC와 AWS Backup Amazon 네트워크 간의 모든 네트워크 트래픽을 제한하여 AWS Backup API에 비공개로 액세스할 수 있는 기술인 에 의해 AWS PrivateLink구동됩니다.

AWS PrivateLink 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결 없이 비공개로 AWS Backup 작업에 액세스할 수 있습니다. AWS Direct Connect VPC의 인스턴스는 AWS Backup API 엔드포인트와 통신하는 데 퍼블릭 IP 주소가 필요하지 않으며, 사용 가능한 API AWS Backup 및 Backup gateway API 작업을 사용하기 위한 퍼블릭 IP 주소도 필요하지 않습니다. VPC와 VPC 사이의 트래픽은 Amazon 네트워크를 AWS Backup 벗어나지 않습니다.

VPC 엔드포인트에 대한 자세한 정보는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트 (AWS PrivateLink)를 참조하세요.

Amazon VPC 엔드포인트에 대한 고려 사항

엔드포인트에 대한 AWS Backup 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 속성 및 제한을 검토하십시오.

를 사용하여 VPC에서 Amazon Backup 리소스 관리와 관련된 모든 AWS Backup 작업을 수행할 수 있습니다. AWS PrivateLink

VPC 엔드포인트 정책은 백업 엔드포인트에 대해 지원됩니다. 기본적으로, 엔드포인트를 통해 백업 작업에 대한 전체 액세스가 허용됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

AWS Backup VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 (AWS Command Line Interface CLI) AWS Backup 를 사용하기 위한 VPC 엔드포인트를 생성할 수 있습니다.AWS 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

서비스 이름을 AWS Backup 사용하기 위한 VPC 엔드포인트를 생성합니다.
`com.amazonaws.region.backup`

중국(베이징) 리전 및 중국(닝샤) 리전에서는 서비스 이름이
`cn.com.amazonaws.region.backup`이어야 합니다.

Backup 게이트웨이 엔드포인트의 경우 `com.amazonaws.region.backup-gateway`를 사용합니다.

Backup 게이트웨이에 대한 VPC 엔드포인트를 생성할 때 보안 그룹에서 다음 TCP 포트를 허용해야 합니다.

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

프로토콜	Port	Direction	소스	대상	사용량
TCP	443(HTTPS)	아웃바운드	Backup Gateway	AWS	Backup Gateway에서 AWS 서비스 엔드포인트로의 통신용

VPC 엔드포인트 사용

엔드포인트에 프라이빗 DNS를 활성화하는 AWS Backup 경우, 예를 들어 AWS 리전의 기본 DNS 이름을 사용하여 VPC 엔드포인트에 API 요청을 할 수 있습니다. `backup.us-east-1.amazonaws.com`

하지만 중국 (베이징) 리전과 중국 (닝샤) 리전의 AWS 리전경우 각각 및 를 사용하여 `backup.cn-north-1.amazonaws.com.cn` VPC 엔드포인트로 API 요청을 해야 합니다. `backup.cn-northwest-1.amazonaws.com.cn`

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하세요.

VPC 엔드포인트 정책 생성

Amazon Backup API에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음을 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

> **Important**
>
> 인터페이스 VPC 엔드포인트에 기본이 아닌 정책을 적용하는 AWS Backup경우 실패한 특정 API 요청 (예: `RequestLimitExceeded` 에서 실패한 요청) 이 Amazon에 AWS CloudTrail 로그인되지 않을 수 있습니다. CloudWatch

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

예: 작업에 대한 VPC 엔드포인트 정책 AWS Backup

다음은 에 대한 AWS Backup엔드포인트 정책의 예입니다. 엔드포인트에 연결할 경우 이 정책은 모든 리소스의 모든 원칙에 대해 나열된 AWS Backup 작업에 대한 액세스 권한을 부여합니다.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

예제: 지정된 AWS 계정의 모든 액세스를 거부하는 VPC 엔드포인트 정책

다음 VPC 엔드포인트 정책은 엔드포인트를 사용하는 AWS 계정의 123456789012 모든 리소스 액세스를 거부합니다. 이 정책은 다른 계정의 모든 작업을 허용합니다.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
```

```
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

사용 가능한 API 응답에 대한 자세한 내용은 API 설명서를 참조하세요.

가용성은 AWS Backup 현재 다음 지역의 VPC 엔드포인트를 지원합니다. AWS

- US East (Ohio) Region
- 미국 동부(버지니아 북부) 리전
- US West (Oregon) Region
- US West (N. California) Region
- 아프리카(케이프타운) 리전
- Asia Pacific (Hong Kong) Region
- Asia Pacific (Mumbai) Region
- Asia Pacific (Osaka) Region
- Asia Pacific (Seoul) Region
- 아시아 태평양(싱가포르) 리전
- 아시아 태평양(시드니) 리전
- 아시아 태평양(도쿄) 리전
- 캐나다(중부) 리전
- Europe (Frankfurt) Region
- 유럽(아일랜드) 리전
- Europe (London) Region

- 유럽(파리) 리전
- Europe (Stockholm) Region
- 유럽(밀라노) 리전
- 중동(바레인) 리전
- South America (São Paulo) Region
- Asia Pacific (Jakarta) Region
- Asia Pacific (Osaka) Region
- 중국(베이징) 리전
- 중국(닝샤) 리전
- AWS GovCloud (미국 동부)
- AWS GovCloud (미국 서부)

> **Note**
>
> AWS Backup VMware의 경우 중국 지역 (중국 (베이징) 지역 및 중국 (닝샤) 지역) 또는 아시아 태평양 (자카르타) 지역에서는 사용할 수 없습니다.

의 레질리언스 AWS Backup

AWS Backup 복원력과 데이터 보안을 매우 중요하게 생각합니다.

AWS Backup 최소한 리소스의 원래 AWS 서비스에 백업한 경우와 동일한 수준의 복원력과 내구성으로 백업을 저장합니다.

AWS Backup 최신 설명서를 준수한다면 AWS 글로벌 인프라를 사용하여 특정 연도에 99.99999999999% (11개 줄) 의 내구성을 유지할 수 있도록 글로벌 인프라를 사용하여 여러 가용 영역에 백업을 복제하도록 설계되었습니다. AWS Backup

AWS Backup 저장 중인 백업 계획을 암호화하고 지속적으로 백업합니다. 또한 AWS Identity and Access Management (IAM) 자격 증명 및 정책을 사용하여 백업 계획에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 인증, 액세스 제어 및 IAM의 보안 모범 사례를 참조하세요.

AWS 글로벌 인프라는 가용 영역을 중심으로 AWS 리전 구축됩니다. AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. AWS Backup 가용 영역 전체에 백업을 저장합니다. 가용 영역은 기존의

단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다. 자세한 내용은 AWS Backup 서비스 수준에 관한 계약(SLA)을 참조하세요.

또한 지역 간에 백업을 복사하여 복원력을 더욱 높일 수 있습니다. AWS Backup AWS Backup 지역 간 복사 기능에 대한 자세한 내용은 백업 복사본 만들기를 참조하십시오.

가용 영역에 대한 AWS 리전 자세한 내용은 AWS 글로벌 인프라를 참조하십시오.

AWS Backup 할당량

을 (를) 사용할 때는 다음 할당량이 적용됩니다. AWS Backup리소스 유형 서비스에서 허용하는 경우 많은 AWS Backup 할당량을 조정할 수 있습니다. 할당량 조정을 요청하려면 AWS Support에 사용 사례를 설명하세요.

AWS Backup 할당량

Resource	할당량	참고
계정당 리전별 백업 저장소 수	300	조정을 요청할 수 있습니다.
백업 저장소당 복구 시점 수	1,000,000	조정을 요청할 수 있습니다.
계정당 리전별 백업 계획 수	300	조정을 요청할 수 있습니다.
백업 계획당 버전 수	2,000	조정을 요청할 수 있습니다.
백업 계획당 리소스 할당 수	100	조정 불가능
계정당 활성 백업 작업 수	무제한	
대상 리전으로 아웃바운드되는 계정당 동시 백업 복사본 수	100	특정 리소스(현재 가상 머신, 고급 DynamoDB, Timestream, Amazon EFS, Amazon EC2의 SAP HANA 데이터베이스)에 대한 조정을 요청할 수 있습니다.
한도(위 항목)에 도달한 후 계정의 대상 백업 저장소당 동시 복사본 수	5	조정 불가능
동일한 대상 리전으로 전송되는 동일한 리소스로 구성될 수 있는 동시 교차 계정 복사본 수	30	조정 불가능합니다.

Resource	할당량	참고
리소스당 동시 백업 및 복사 작업 수	1	조정 불가능합니다. 이 할당량은 워크로드의 성능을 유지하는 데 도움이 됩니다.
백업당 메타데이터 태그 수	50	조정을 요청할 수 없습니다. AWS 이 할당량을 모든 리소스에 적용합니다. AWS General Reference의 Tag naming limits and requirements 섹션을 참조하세요.
계정 간 백업 정책에서 선택한 리소스당 태그 수	30	조정 불가능합니다. 여러 리소스 할당 또는 백업 계획을 활용하여 추가 태그를 포함할 수 있습니다.
하이퍼바이저 수	10	조정 불가능
법적 보존 수	계정당 50개	조정 불가능
애플리케이션 스택의 최대 중첩 백업 레이어 수	10	조정 불가능

AWS Backup Amazon Timestream 리소스 할당량

Resource	할당량	참고
계정당 동시 Timestream 백업 작업 수	4	조정을 요청할 수 있습니다.
계정당 동시 Timestream 복원 작업 수	1	조정을 요청할 수 있습니다.

단일 백업 규칙의 단일 리소스 할당에는 할당량이 있습니다. 여러 백업 규칙이 포함된 백업 계획을 생성할 수 있습니다.

AWS Backup Audit Manager 할당량

Resource	할당량	참고
리전별로 계정당 프레임워크 수	15	조정을 요청할 수 있습니다.
리전별로 계정당 컨트롤 수	50	조정을 요청할 수 있습니다.
계정당 보고서 계획 수	20	조정을 요청할 수 있습니다.
보고서 계획당 프레임워크 수	1,000	조정 불가능
보고서 계획에서 최대 계정 수를 리전 수와 곱한 값	300	조정 불가능

복원 테스트 계획 할당량

Resource	할당량	참고
복원 테스트 계획	100	조정 불가능
각 계획의 태그 수	50	조정 불가능
계획당 선택 항목	30	조정 불가능
복원 테스트 선택 항목당 ARN	30	조정 불가능
선택 항목당 조건	30	`StringEquals` 및 `StringNotEquals`에 포함된 항목을 포함합니다.
복원 테스트 선택 항목당 볼트 선택기	30	조정 불가능
선택 항목 기간의 최댓값(일)	365일	
시작 기간의 범위(시간)	최소: 1시간, 최대: 168시간	

Resource	할당량	참고
복원 테스트 계획 이름의 최대 문자 길이	50자	영숫자 및 밑줄, 공백 없음
복원 테스트 선택 항목 이름의 최대 문자 길이	50자	영숫자 및 밑줄, 공백 없음

AWS Backup gateway 할당량

Resource	할당량	참고
게이트웨이당 백업 또는 복원 작업 수	4	조정을 요청할 수 없습니다. 그 대신 게이트웨이를 추가로 생성한 후 이를 하이퍼바이저에 연결하세요.

를 사용하여 여러 계정의 백업을 관리하는 AWS Organizations경우 할당량이 부과될 수 있습니다. AWS Organizations 이러한 할당량에 대한 내용은 AWS Organizations 사용 설명서의 AWS Organizations에 대한 할당량 섹션을 참조하세요.

지원되는 서비스에서 부과하는 할당량은 다음과 같이 발생할 수도 있습니다 AWS Backup.

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx for Lustre
- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service(S3)

- Amazon Timestream

모니터링

AWS Backup 다른 AWS 도구와 함께 작동하여 워크로드를 모니터링할 수 있습니다. 이러한 도구에는 다음이 포함됩니다.

- AWS Backup 콘솔 대시보드
  - 작업 대시보드는 작업 상태 모니터링 기능을 제공합니다. 상태 모니터링을 통해 작업 성공 및 실패를 보여주는 지표를 사유, 계정, 리전 및 리소스 유형별로 필터링하여 볼 수 있습니다.
  - 채용 대시보드는 AWS Backup Audit Manager가 지원되는 지역에서 사용할 수 있습니다. 사용 가능한 리전은 기능 가용성은 다음과 같습니다. AWS 리전 섹션을 참조하세요. 다른 모든 리전에서는 CloudWatch 대시보드에 액세스할 수 있습니다.
- CloudWatch아마존과 EventBridge 아마존이 AWS Backup 프로세스를 모니터링합니다.
  - 를 CloudWatch 사용하여 지표를 추적하고, 경보를 생성하고, 대시보드를 볼 수 있습니다.
  - 를 사용하여 이벤트를 보고 EventBridge AWS Backup 모니터링할 수 있습니다.

  자세한 내용은 Amazon을 사용한 AWS Backup 이벤트 모니터링 EventBridge 섹션을 참조하세요.
- AWS CloudTrail AWS Backup API 호출을 모니터링합니다. 시간, 소스 IP, 사용자 및 이러한 호출을 하는 계정을 식별할 수 있습니다. 자세한 정보는 를 AWS Backup 사용하여 API 호출을 로깅합니다. CloudTrail 을 참조하세요.
- Amazon 심플 알림 서비스 (Amazon SNS) 를 통해 백업, 복원, 복사 이벤트와 같은 AWS Backup관련 주제를 구독할 수 있습니다. 자세한 정보는 알림 옵션: AWS Backup을 참조하세요.

AWS Backup 콘솔 대시보드

> **Note**
>
> 채용 대시보드는 AWS Backup Audit Manager가 지원되는 모든 지역에서 사용할 수 있습니다. 사용 가능한 리전은 기능 가용성은 다음과 같습니다. AWS 리전 섹션을 참조하세요. 다른 모든 리전에서는 CloudWatch 대시보드에 액세스할 수 있습니다.

주제

- 백업 대시보드 개요
- 작업 대시보드 보기

- 문제가 있는 작업의 사유
- 다음을 통해 대시보드 데이터를 확보합니다. AWS CLI

백업 대시보드 개요

AWS Backup 콘솔에 작업 대시보드를 제공하여 백업, 복사 및 복원 작업의 상태를 모니터링하는 데 도움이 됩니다. 콘솔에 시각적으로 표시된 것과 동일한 데이터를 명령줄을 통해 AWS CLI검색할 수 있습니다.

작업 대시보드를 사용하면 조직 수준 또는 멤버 계정 모니터링을 통해 백업, 복사 및 복원 작업의 문제를 식별할 수 있습니다. 이 정보를 통해 이벤트와 발생 가능한 문제를 식별하고 진단하여 활동의 정확성을 보장할 수 있습니다.

작업 대시보드에는 두 개의 기간이 표시될 수 있습니다. 기본적으로 최근 14일의 데이터가 표시되지만 최근 7일의 데이터를 표시하도록 뷰를 변경할 수 있습니다. 기간을 변경하면 새 시간 간격을 반영하여 데이터가 업데이트됩니다.

참고로 대시보드에는 가장 최근 0:00 UTC까지의 데이터가 표시됩니다. 즉, 오늘의 데이터는 포함되지 않습니다. 대시보드는 매일 약 1:30~2:30 UTC 사이에 업데이트됩니다.

작업 대시보드 보기

작업 대시보드를 보려면 AWS Backup 콘솔에 로그인하고 왼쪽 탐색 표시줄에서 작업 대시보드를 선택합니다.

작업 대시보드 페이지에서 백업, 복사 또는 복원 작업 탭 중에서 선택할 수 있습니다.

작업 대시보드 개요에는 완료된 작업, 문제가 있는 상태로 완료된 작업, 만료된 작업, 실패한 작업을 포함하여 지정된 작업 활동 기간 동안의 집계된 뷰가 표시됩니다. 기본적으로 최근 14일의 데이터가 표시되지만 7일의 데이터를 표시하도록 뷰를 변경할 수 있습니다.

> **Note**
>
> `Completed with issues`는 콘솔에 표시되는 작업 상태로, 상태 메시지가 있는 상태로 완료된 작업을 나타냅니다.

작업 상태

선 차트에는 시간 경과에 따른 성공 및 실패 작업 비율이 선으로 표시됩니다. 성공률 선은 완료된 작업과 문제가 있는 상태로 완료된 작업의 집계를 보여줍니다. 실패율 선은 지정된 시간 범위에서 실패 및 만료된 작업의 합계가 표시됩니다.

완료되지 않았거나 실패하지 않은 상태의 작업(생성됨, 보류 중, 실행 중, 중단됨, 중단 중 또는 일부 상태인 작업)은 포함되지 않습니다. 백분율 합계는 100%가 아닐 수 있습니다.

시간 경과에 따른 작업 상태

막대형 차트를 사용하면 각 범주의 작업 수(완료됨, 문제가 있는 상태로 완료됨, 실패, 만료됨)를 일별로 보여 주는 사용자 지정 막대 차트를 생성할 수 있습니다.

드롭다운 메뉴를 사용하여 차트에 표시하려는 상태, 리소스 유형, AWS 지역을 선택합니다. 선택 항목을 더 자세히 살펴보려면 작업 보기를 선택하여 작업/교차 계정 모니터링 페이지에서 사전 필터링된 부분을 확인하세요.

막대 위에 마우스를 올려 놓으면 선택한 날짜의 자세한 작업 데이터를 보여주는 팝오버가 표시됩니다.

문제가 있는 작업

문제가 있는 작업은 실패, 만료됨 또는 문제가 있는 상태로 완료됨 상태인 작업입니다. 각 차트에는 문제가 있는 작업 중 가장 많은 작업이 속한 계정, 리소스 유형 또는 주요 사유가 포함된 지표가 표시됩니다.

기본 디스플레이는 지정된 지표를 기준으로 대시보드 위젯을 내림차순으로 정렬합니다. 즉, 문제가 있는 작업 수가 가장 많은 지표가 가장 먼저 표시됩니다.

문제가 가장 많은 계정 디스플레이는 Organizations를 통해 액세스할 수 있는 계정(예: 관리자 계정 및 위임된 관리자 계정)에서만 표시됩니다. 표시되는 경우, 계정을 마우스로 가리키면 선택한 계정에 속하는 문제가 있는 작업의 수를 볼 수 있습니다.

그래프 내에서 막대를 선택하여 팝업 창을 열 수 있습니다. 이 창에서 작업 상태를 선택하여 선택한 상태별로 필터링된 작업/교차 계정 모니터링 테이블을 열 수 있습니다.

문제가 있는 작업의 사유

문제의 주요 사유 위젯에는 오류 메시지가 속하는 메시지 코드 범주가 표시됩니다. 하지만 범주로는 작업의 문제가 설명되지 않을 수 있습니다. 아래 메시지 코드 범주를 확장하여 작업에서 발생할 수 있는 특정 메시지 또는 오류에 대한 자세한 내용을 확인하세요.

"VSS_ERROR"

- "인스턴스 또는 SSM 에이전트의 상태가 잘못되었거나 권한이 충분하지 않아 Windows VSS 백업 시도가 실패했습니다."
- "이 작업을 수행할 권한이 충분하지 않아 Windows VSS 백업 시도가 실패했습니다."
- "인스턴스에 ec2-vss-agent.exe가 설치되어 있지 않아 Windows VSS 백업 시도가 실패했습니다."
- "일반 백업을 시도하는 중 Windows VSS 백업 작업 오류가 발생했습니다."
- "VSS 지원 스냅샷 생성 시 시간 초과로 인해 Windows VSS 백업 시도가 실패했습니다."
- "지원되지 않는 Windows Server 버전으로 인해 Windows VSS 백업 시도가 실패했습니다. 지원되는 버전은 Windows Server 2012 이상입니다."
- "VSS 지원 스냅샷 생성 시 시간 초과로 인해 Windows VSS 백업 시도가 실패했습니다."

"LIMIT_EXCEEDED"

- "구독자 한도 초과: 최대 동시 백업 수인 300개에 도달했습니다. 다른 작업이 끝날 때까지 기다린 후 다시 시도하세요. 또한 AWS Support 문의하여 할당량 증가를 요청할 수도 있습니다."
- "단일 볼륨에 대해 허용되는 진행 중 스냅샷의 최대 개수를 초과했습니다."
- "허용되는 활성 스냅샷 최대 한도를 초과했습니다."
- "20개 이상의 사용자 스냅샷을 생성할 수 없습니다."
- "결과 태그 세트는 50개 이상의 사용자 태그를 포함할 수 없습니다."
- "계정/데이터베이스에 지원되는 최대 백업 개수에 도달했습니다. 자세한 내용은 Timestream 개발자 안내서에서 할당량을 참조하세요."
- "이 리전에 허용된 퍼블릭 및 프라이빗 이미지 수가 할당량인 50,000개에 도달했습니다. 사용하지 않는 이미지를 등록 취소하거나 AMI 할당량 상향을 요청하세요."
- "백업은 성공했지만 메타데이터 크기가 내부 한도를 초과하여 NetworkInterfaces 메타데이터를 유지할 수 없었습니다."
- "REGEX#구독자 한도를 초과했습니다."
- "REGEX#태그가 50개 이상 지정되었습니다."
- "REGEX #최대 개수는 다음과 같습니다."

"ACCESS_DENIED"

- "이 작업을 수행할 수 있는 권한이 없습니다."

- “ AWS Backup 서비스 호출 시도 중 액세스가 거부되었습니다.”
- “의 이미지는 다른 AWS 계정으로 복사할 수 AWS Marketplace 없습니다.”
- "대상 백업 볼트가 기본 백업 서비스 관리형 키로 암호화되어 있어서 복사 작업이 실패했습니다. 이 볼트의 콘텐츠를 복사할 수 없습니다. AWS KMS 키로 암호화된 Backup 저장소의 내용만 복사할 수 있습니다.
- 로 암호화된 스냅샷은 공유할 AWS 관리형 키 수 없습니다. 다른 스냅샷을 지정하세요.
- "Amazon EBS 기본 키로 암호화된 스냅샷은 공유할 수 없습니다.
- "복사 작업이 실패했습니다. 소스 계정과 대상 계정이 같은 조직에 속해 있어야 합니다."
- "REGEX#액세스가 거부되었습니다."
- "REGEX#다음 작업에 대한 권한이 없습니다."
- “REGEX #cannot 는 다음과 같이 가정합니다. AWS Backup
- "REGEX#권한이 없습니다."
- "REGEX#권한이 누락되었습니다."

"CONCURRENT_JOB"

- "동일한 리소스에 대해 실행 중인 작업이 있어서 백업 작업이 실패했습니다."

"FEATURE_NOT_ENABLED"

- "복사 작업이 실패했습니다. 현재 조직에서는 계정 간 복사 기능을 사용할 수 없습니다."

"JOB_EXPIRED"

- "백업 작업이 완료되기 전에 만료되었습니다."

"INVALID_LIFECYCLE"

- "복사 작업이 실패했습니다. 작업에 지정된 보존 기간이 대상 백업 볼트에 지정된 범위 내에 있지 않습니다."
- "REGEX#구성된 주간 유지 관리 기간에 속하거나 유지 관리 기간과 너무 가까워서 시작하지 못했습니다."
- "REGEX#구성된 자동 백업 기간에 속하거나 자동 백업 기간과 너무 가까워서 시작하지 못했습니다."

"INVALID_STATE"

- "REGEX#인스턴스가 다음 상태가 아닙니다."
- "REGEX#사용 가능한 상태가 아닙니다."
- "REGEX#사용 가능한 상태가 아님"
- "REGEX#볼륨 스냅샷을 생성할 수 없습니다."

"KMS_KEY_ERROR"

- "KMS 키가 비활성화되었거나 삭제 보류 중이거나 KMS 키에 대한 액세스가 거부되었습니다."
- "지정된 키 ID에 액세스할 수 없습니다."
- "오류가 있는 상태로 AMI 스냅샷 복사 실패함: 지정된 키 ID에 액세스할 수 없습니다. 기본 CMK에 대한 DescribeKey 권한이 있어야 합니다."
- "REGEX#kms 키"

"ACCESS_KEY_ERROR"

- " AWS 액세스 키 ID에는 서비스 구독이 필요합니다."

"HYPERVISOR_OFFLINE"

- "이 작업은 지정된 하이퍼바이저가 온라인 상태가 아니므로 해당 하이퍼바이저에 유효하지 않습니다."

"RESOURCE_NOT_FOUND"

- "지정한 볼륨을 찾을 수 없습니다."
- "가상 머신을 찾을 수 없습니다."
- "지정된 키 ID가 존재하지 않습니다."
- "REGEX#존재하지 않습니다."
- "REGEX#리소스를 찾지 못했습니다."
- "REGEX#cryopod를 찾지 못했습니다."
- "REGEX#복구 시점을 찾을 수 없습니다."
- "REGEX#리소스를 찾을 수 없습니다."

- "REGEX#더 이상 사용할 수 없습니다."
- "REGEX#유효하지 않습니다."

"RESOURCE_NOT_SUPPORTED"

- "REGEX#지원되지 않는 리소스 유형"
- "REGEX#지원되지 않는 리소스 유형입니다."

"TAG_COPY_ERROR"

- "내부 장애로 인해 리소스 태그를 백업에 복사할 수 없습니다."
- "소스 또는 대상 복구 시점을 사용할 수 없기 때문에 리소스 태그를 백업에 복사할 수 없습니다."

"TOKEN_EXPIRED"

- "토큰이 만료되었습니다. 다시 시도해 주세요."

"UNSUPPORTED_OPERATION"

- 스냅샷 생성 중에는 하이퍼바이저에서 "CreateSnapshot 방법이 지원되지 않습니다. 백업 작업을 중단했습니다."
- “UnsupportedOperation : Storage Gateway 백업 복사본에는 대상에 사용자가 만든 백업 볼트와 CMK가 필요합니다.”
- "REGEX#제공된 리소스 유형에는 기능이 지원되지 않습니다."

"FATAL_ERROR"

- "내부 오류가 발생했습니다."
- "복사 작업에서 치명적인 오류가 발생했습니다. 추가 AWS 지원이 필요하면 Support에 문의하십시오.”
- "복사 작업에서 치명적인 오류가 발생했습니다."
- "REGEX#백업 작업에서 치명적인 오류가 발생했습니다."

다음을 통해 대시보드 데이터를 확보합니다. AWS CLI

명령줄을 사용하여 콘솔에 표시되는 것과 동일한 데이터를 검색할 수 있습니다. 다음 CLI 명령 중 하나를 사용합니다.

- list-backup-job-summaries
- list-copy-job-summaries
- list-restore-job-summaries

각 명령에 포함할 수 있는 유효한 파라미터는 다음과 같습니다.

```
BackupJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

이 예에서는 상태가 FAILED인 지난 14일간의 모든 사용 가능한 계정을 반환하도록 요청하기 위한 list-backup-job-summaries 입력의 샘플 요청을 보여줍니다.

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

상태가 `completed with issues`인 작업의 수를 구하려면 `SUCCESS` 상태의 총 작업 수에서 `MessageCategory`가 `COMPLETED`인 `COMPLETED` 상태의 작업 수를 빼면 됩니다.

Amazon을 사용한 AWS Backup 이벤트 모니터링 EventBridge

AWS Backup 백업 또는 복사 작업 상태가 변경될 EventBridge 때 Amazon에 이벤트를 전송합니다. 를 사용하여 AWS Backup 이벤트를 EventBridge 모니터링할 수 있습니다. 예를 들어, 백업 작업이 실패하면 경보를 받을 수 있습니다. AWS Backup 최선을 EventBridge 다해 5분마다 이벤트를 발생시킵니다.

를 사용하여 이벤트를 EventBridge 추적하려면 다음을 참조하십시오.

- 이벤트에 반응하는 규칙 생성 (Amazon EventBridge 사용 설명서)
- Amazon CloudWatch 이벤트 및 지표 AWS Backup (블로그 - Amazon으로 전송할 AWS Backup 이벤트 구성 참조 EventBridge)

일부 이벤트는 `state: COMPLETED`를 보고하는 반면, 다른 이벤트는 `status: COMPLETED`를 보고합니다. 이는 AWS Backup API와 일치합니다. 일부 상태는 AWS Backup 콘솔에만 해당됩니다. 즉, `Completed with issues` 상태 상태는 상태 메시지가 있는 `Completed` 작업을 나타냅니다. `Completed with issues` 이벤트를 모니터링하려면 상태 메시지가 있는 `COMPLETED` 작업을 모니터링하세요.

또는 AWS Backup 알림 API를 사용하여 Amazon Simple Service (Amazon SNS) 로 AWS Backup 이벤트를 추적할 수도 있습니다. 하지만 백업 저장소, 복사 작업 상태, 지역 설정, 콜드 또는 웜 복구 지점 수에 대한 변경 사항을 포함하여 알림 API보다 더 많은 변경 사항을 EventBridge 추적합니다.

이벤트

- Backup Job 이벤트
- 백업 플랜 이벤트
- Backup Vault 이벤트
- Copy Job 이벤트
- 복구 지점 이벤트

- 지역 설정 이벤트
- 복원 작업 이벤트

Backup Job 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 실패
- 상태: 완료
- 상태: 실행 중
- 상태: 중단됨
- 상태: 만료됨
- 상태: 보류 중
- 상태: 생성됨

상태: 실패

```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
```

```
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-
west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.
\"",
    "startBy": "2020-07-30T04:13:07.392Z",
    "percentDone": 0,
    "retryCount": 3
  }
}
```


상태: 완료


```
{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-
b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
```

상태: 실행 중


```
{
  "version": "0",
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```


상태: 중단됨


```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
```

```
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "ABORTED",
    "statusMessage": "\"Backup job was stopped by user.\"",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
  }
}
```


상태: 만료됨


```
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
```

```
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
 resource.\"",
    "completionDate": "2020-07-29T13:02:15.234Z",
    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```

상태: 보류 중

```
{
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}
```

상태: 생성됨

```
{
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```

백업 플랜 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 수정됨
- 상태: 삭제됨
- 상태: 생성됨

상태: 수정됨

```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
```

```
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

상태: 삭제됨

```
{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}
```

상태: 생성됨

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
```

```
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```


Backup Vault 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 생성됨
- 상태: 수정됨
- 상태: 삭제됨

상태: 생성됨


```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

상태: 수정됨

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

상태: 삭제됨

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-
b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```

Copy Job 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 실패
- 상태: 실행 중
- 상태: 완료
- 상태: 생성됨

상태: 실패


```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
```

```
}
```

상태: 실행 중

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

상태: 완료

```
{
  "version": "0",
```

```
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/
snap-0726fe70935586180",
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```


상태: 생성됨


```
{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
  }
}
```

복구 지점 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 완료
- 상태: 삭제됨
- 상태: 수정됨

상태: 완료

```
{
    "version": "0",
    "id": "ab32977c-378d-2122-e985-fgh4596f0709",
    "detail-type": "Recovery Point State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T21:39:07Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
    ],
    "detail": {
        "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
```

```
        "creationDate": "2020-07-15T21:38:31.152Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
        "resourceType": "Aurora",
        "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
        "status": "COMPLETED",
        "isEncrypted": "false",
        "storageClass": "WARM",
        "completionDate": "2020-07-15T21:39:05.689Z",
        "createdBy": {
            "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
            "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
        },
        "lifecycle": {
            "deleteAfterDays": 100
        },
        "calculatedLifeCycle": {
            "deleteAt": "2020-10-23T21:38:31.152Z"
        }
    }
}
```

상태: 삭제됨

```
{
  "version": "0",
  "id": "6089ee76-d856-0d7c-cee7-0a431cd43343",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T22:38:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:157f892e-
fe46-48da-9dbe-4154f91f8acc",
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-c1a6d40a-32d1-4d54-
bd70-bced933ef107"
  ],
  "detail": {
    "state": "DELETED",
    "lifecycle": {
```

```
      "deleteAfterDays": 300
    },
    "calculatedLifeCycle": {
      "deletedAt": "2021-05-25T22:29:02.452Z"
    }
  }
}
```

상태: 수정됨

```
{
  "version": "0",
  "id": "14365bb1-adef-bc00-1ee3-8fac188d7996",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-02T23:33:57Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:helo12312",
    "arn:aws:dynamodb:us-west-2:1112233445566:table/test/
backup/01593730512469-033578ce"
  ],
  "detail": {
    "calculatedLifeCycle": {
      "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
    },
    "state": "MODIFIED"
  }
}
```

지역 설정 이벤트

다음은 이벤트 예제입니다.

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbafcfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
```

```
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
}
```

복원 작업 이벤트

다음은 예제 이벤트입니다.

State

- 상태: 실패
- 상태: 실행 중
- 상태: 완료
- 상태: 보류 중
- 상태: 생성됨

상태: 실패

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "createdBy": [
```

```
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
 EC2 instance. Please restore using the backed up instance profile."
  }
}
```

상태: 실행 중

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

상태: 완료

```
{
```

```
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Restore Job State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2020-07-15T03:14:58Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:rds:us-
west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail":{
    "restoreJobId":"AB123456-78C9-0123-456D-789012E34567",
    "backupSizeInBytes":"0",
    "creationDate":"2020-07-15T03:10:01.742Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn":"arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone":0,
    "resourceType":"RDS",
    "status":"COMPLETED",
    "createdResourceArn":"arn:aws:rds:us-
west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate":"2020-07-15T03:14:53.128Z"
  }
}
```


상태: 보류 중


```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-
b29f4edb47b1"
  ],
```

```
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}
```

상태: 생성됨

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-
efgh939ij32k"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "creationDate": "2020-06-22T18:50:46.407Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "state": "CREATED"
  }
}
```

AWS Backup 아마존을 사용한 지표 CloudWatch

주제

CloudWatch 대시보드

> **Note**
>
> 콘솔 대시보드는 콘솔에 액세스하는 리전에 따라 달라집니다. 작업 대시보드에 액세스할 수 있는 리전을 확인하려면 기능 가용성은 다음과 같습니다. AWS 리전 섹션을 참조하세요. 목록에 없는 지역도 CloudWatch 대시보드에 액세스할 수 있습니다.

AWS Backup 콘솔에는 완료되거나 실패한 백업, 복사 및 복원 작업에 대한 메트릭을 볼 수 있는 대시보드가 포함되어 있습니다. 이 대시보드에서는 원하는 기간에 맞게 사용자 지정된 기간별 작업 상태를 볼 수 있습니다.

대시보드에 액세스하려면

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대시보드를 선택합니다.

대시보드 보기 및 이해

CloudWatch 대시보드에는 여러 위젯이 표시됩니다. 각 위젯은 작업 지표를 개수별로 보여줍니다. 각 위젯에는 여러 개의 선 그래프가 표시됩니다. 각 선은 보호된 리소스에 해당합니다. 예상 리소스가 표시되지 않을 경우 설정에서 해당 리소스가 켜져 있는지 확인하세요. 디스플레이에 진행 중인 작업은 표시되지 않습니다.

y축(세로 값)은 개수를 표시합니다. x축(가로 값)은 시점을 표시합니다. 선택한 작업 상태에 시각화할 데이터 포인트가 없는 경우, 값은 x축의 가로선과 함께 0으로 설정됩니다. 리소스를 보여주는 범례는 계속 표시됩니다.

지표에는 현재 로그인과 관련된 계정별 및 리전별 정보가 표시됩니다. 다른 계정이나 리전을 보려면 선택한 계정으로 로그인해야 합니다.

대시보드 사용자 지정

기본적으로 표시되는 기간은 1주일입니다. 상단 메뉴에는 표시된 기간을 재정의하는 옵션이 있습니다. 1시간, 3시간, 12시간, 1일, 3일, 1주일 중에서 선택할 수 있습니다. 또한 사용자 지정을 선택하여 다른 값을 지정할 수 있습니다. 사용자 지정을 수행하면 현재 보기가 사양에 맞게 일시적으로 변경됩니다.

위젯 위에 커서를 올리면 위젯 오른쪽 상단에 확대 버튼이 표시됩니다. 위젯을 전체 화면 보기로 열려면 확대를 클릭합니다. 전체 화면에서는 기간(모든 데이터 포인트 간의 시간) 변경 등과 같이, 그래프 표시를 사용자 정의할 수 있는 추가 옵션이 있습니다. 전체 화면 보기를 닫으면 변경 내용이 유지되지 않습니다.

한 번에 하나의 리소스 유형만 보려면 그래프 범례에서 보려는 리소스 유형의 레이블 텍스트를 클릭합니다. 이렇게 하면 다른 모든 리소스 유형의 선택이 취소됩니다. 이 작업을 되돌리려면 범례에서 리소스 유형 색상 상자를 클릭합니다. 모든 레이블이 선택된 상태로 모든 리소스 유형의 기본 보기로 돌아가려면 선택한 리소스 유형의 레이블 텍스트를 다시 클릭합니다.

위젯의 오른쪽 상단에 있는 세로 점 3개를 클릭하면 새로 고침, 확대, 지표에서 보기, 로그에서 보기 등의 옵션이 있는 드롭다운 메뉴가 열립니다. '지표로 보기'를 선택하면 위젯에서 사용되는 지표가 CloudWatch 콘솔에서 열립니다. 거기서 위젯을 변경하고 대시보드의 사용자 지정 대시보드에 위젯을 추가할 수 있습니다. CloudWatch CloudWatch 대시보드에서 변경한 내용은 AWS Backup Console의 대시보드에 반영되지 않습니다. '로그로 보기'를 선택하면 CloudWatch 콘솔에서 로그 보기 페이지가 열립니다.

표시된 위젯을 사용자 지정 CloudWatch 대시보드에 추가하려면 대시보드 오른쪽 상단에 있는 대시보드에 추가 버튼을 클릭합니다. 그러면 6개의 위젯을 모두 추가할 사용자 지정 대시보드를 선택할 수 있는 CloudWatch 콘솔이 열립니다.

자세한 내용은 Amazon CloudWatch 지표 사용을 참조하십시오.

다음과 같은 측정치 CloudWatch

AWS Backup 지표를 모니터링하는 CloudWatch 데 사용할 수 있습니다. `AWS/Backup`네임스페이스를 사용하면 다음 지표를 추적할 수 있습니다. AWS Backup CloudWatch 5분마다 업데이트된 지표를 내보냅니다.

이 설명서 페이지의 목적은 CloudWatch AWS Backup모니터링에 사용할 참조 자료를 제공하는 것입니다. 지표를 사용하여 CloudWatch 모니터링하는 방법을 알아보려면 사용 설명서의 Amazon CloudWatch Events and Metrics AWS Backup또는 단일 AWS 서비스의 지표 및 경보에 초점을 맞춘 블로그를 CloudWatch 참조하십시오. 경보를 설정하려면 사용 CloudWatch 설명서의 Amazon CloudWatch Alarms 사용을 참조하십시오.

범주	측정치	차원 예시	사용 사례
작업	각 상태 전체의 백업, 복원, 복사 작업 수 (CREATED, PENDING, RUNNING, ABORTED, COMPLETED , FAILED, EXPIRED 포함). 작업 유형마다 사용 가능한 상태가 다릅니다.	리소스 유형, 저장소 이름. 복사 작업의 저장소 이름은 대상 저장소의 이름입니다.	하나 이상의 특정 백업 저장소 내에 있는 실패한 백업 작업 수를 모니터링합니다. 1시간 이내에 실패 작업이 5개 이상 발생하면 Amazon SNS를 사용하여 이메일 또는 SMS를 보내거나, 엔지니어링 팀에 티켓을 개설하여 문제를 조사하세요. 보고 기준: 0이 아닌 값이 있을 때
복구 시점	각 상태 전체의 원 및 콜드 복구 시점 수: MODIFIED, COMPLETED , PARTIAL, EXPIRED, DELETED.	리소스 유형, 저장소 이름.	Amazon EBS 볼륨의 삭제된 복구 시점 수를 추적하고, 각 백업 저장소의 원 및 콜드 복구 시점 수를 별도로 추적합니다. 보고 기준: 0이 아닌 값이 있을 때

> **Note**
>
> 의 Completed with issues 작업 상태는 콘솔에만 해당되며 AWS Backup 콘솔을 통해 추적할 수 없습니다. CloudWatch

다음 표에는 사용 가능한 모든 지표가 나와 있습니다.

지표	설명
NumberOfBackupJobsCreated	AWS Backup 생성된 백업 작업 수.
NumberOfBackupJobsPending	AWS Backup에서 실행하려는 백업 작업의 수입니다.
NumberOfBackupJobsRunning	현재 실행 중인 백업 작업 수 AWS Backup.
NumberOfBackupJobsAborted	사용자가 취소한 백업 작업 수입니다.
NumberOfBackupJobsCompleted	AWS Backup 완료된 백업 작업 수.
NumberOfBackupJobsFailed	상태가 Failed인 백업 작업의 수입니다. 데이터베이스 리소스 1시간 전 또는 Amazon FSx 유지 관리 기간 또는 자동 백업 기간 이전 또는 4시간 중에 백업 작업을 예약하고 복원을 위한 연속 백업을 수행하는 데 AWS Backup 사용하지 않는 경우에 주로 발생합니다. point-in-time 지원되는 서비스 목록 및 연속 백업을 수행하거나 백업 작업을 다시 예약하는 AWS Backup 데 사용하는 방법에 대한 지침은 지정 시간 복구를 참조하십시오.
NumberOfBackupJobsExpired	상태가 인 백업 작업의 수입니다. EXPIRED 백업 작업의 상태가 시작 기간 내에 백업을 시작할 수 없는 CREATED EXPIRED 경우로 변경됩니다.
NumberOfCopyJobsCreated	AWS Backup 이 생성한 교차 계정 및 교차 리전 복사 작업의 수입니다.
NumberOfCopyJobsRunning	AWS Backup에서 현재 실행 중인 교차 계정 및 교차 리전 복사 작업의 수입니다.
NumberOfCopyJobsCompleted	AWS Backup 이 완료한 교차 계정 및 교차 리전 복사 작업의 수입니다.

지표	설명
NumberOfCopyJobsFailed	AWS Backup 시도했지만 완료하지 못한 교차 계정 및 지역 간 복사 작업의 수입니다.
NumberOfRestoreJobsPending	AWS Backup에서 실행하려는 복원 작업의 수입니다.
NumberOfRestoreJobsRunning	현재 실행 중인 복원 작업 수 AWS Backup
NumberOfRestoreJobsCompleted	AWS Backup 완료된 복원 작업 수.
NumberOfRestoreJobsFailed	AWS Backup 시도했지만 완료하지 못한 복원 작업 수.
NumberOfRecoveryPointsCompleted	AWS Backup 생성된 복구 지점 수.
NumberOfRecoveryPointsPartial	만들기를 AWS Backup 시작했지만 완료하지 못한 복구 지점의 수. AWS 프로세스를 나중에 다시 시도하지만 나중에 다시 시도하므로 부분 복구 지점이 유지됩니다.
NumberOfRecoveryPointsExpired	백업 보존 주기를 기준으로 삭제를 AWS Backup 시도했지만 삭제할 수 없는 복구 지점 수입니다. 만료된 백업이 사용하는 스토리지에 대해 요금이 청구되므로 이러한 백업은 수동으로 삭제해야 합니다.
NumberOfRecoveryPointsDeleting	삭제 중인 복구 지점의 수입니다. AWS Backup
NumberOfRecoveryPointsCold	콜드 스토리지로 AWS Backup 계층화된 복구 지점의 수.

표에 나열된 것 외에도 더 많은 차원을 사용할 수 있습니다. 지표의 모든 차원을 보려면 콘솔의 Metrics 섹션의 **AWS/Backup** 네임스페이스에 해당 지표의 이름을 입력합니다. CloudWatch

를 AWS Backup 사용하여 API 호출을 로깅합니다. CloudTrail

AWS Backup 사용자, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스 서비스와 AWS CloudTrail통합됩니다. CloudTrail 모든 API 호출을 AWS Backup 이벤트로 캡처합니다. 캡처된 호출에는 AWS Backup 콘솔에서의 호출 및 AWS Backup API 작업에 대한 코드 호출이 포함됩니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Backup, 요청한 IP 주소, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청을 루트 사용자로 했는지 사용자 보안 인증으로 했는지 여부.
- IAM Identity Center 사용자를 대신하여 요청이 이루어졌는지 여부입니다.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

CloudTrail 계정을 만들 AWS 계정 때 활성화되며 자동으로 CloudTrail 이벤트 기록에 액세스할 수 있습니다. CloudTrail 이벤트 기록은 지난 90일간의 기록된 관리 이벤트를 보고, 검색하고, 다운로드할 수 있고, 변경할 수 없는 기록을 제공합니다. AWS 리전자세한 내용은 사용 설명서의 CloudTrail 이벤트 기록 사용을 참조하십시오.AWS CloudTrail 이벤트 기록 조회에는 CloudTrail 요금이 부과되지 않습니다.

AWS 계정 지난 90일 동안 진행 중인 이벤트 기록을 보려면 트레일 또는 CloudTrail호수 이벤트 데이터 저장소를 생성하세요.

CloudTrail 트레일

트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 를 사용하여 생성된 모든 트레일은 다중 AWS Management Console 지역입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정의 모든 활동을 기록할 수 있으므로 멀티 리전 트레일을 생성하는 것이 좋습니다 AWS 리전 . 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Creating a trail for your AWS 계정 및 Creating a trail for an organization을 참조하세요.

트레일을 CloudTrail 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수 있지만 Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하십시오. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail 레이크 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대한 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 사용 설명서의 Lake 사용을 참조하십시오. AWS CloudTrail AWS CloudTrail

CloudTrail Lake 이벤트 데이터 저장 및 쿼리로 인해 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하십시오.

AWS Backup 의 이벤트 CloudTrail

AWS Backup 백업, 복원, 복사 또는 알림을 수행할 때 이러한 CloudTrail 이벤트를 생성합니다. 이러한 이벤트는 반드시 AWS Backup 퍼블릭 API를 사용하여 생성되는 것은 아닙니다. 자세한 내용은 AWS CloudTrail 사용 설명서의AWS 서비스 이벤트를 참조하십시오.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

AWS Backup 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는StartBackupJob,,StartRestoreJob, DeleteRecoveryPoint 작업 및 BackupJobCompleted 이벤트를 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
```

```
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
```

```
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
```

```
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```


교차 계정 관리 이벤트 로깅

AWS Backup를 사용하면 AWS Organizations구조 AWS 계정 내 모든 영역에서 백업을 관리할 수 있습니다. AWS Backup AWS Organizations 백업 정책 (구성원 계정에 백업 플랜 적용) 을 생성, 업데이트 또는 삭제할 때 또는 잘못된 조직 백업 계획이 있는 경우 다음 CloudTrail 이벤트를 생성합니다.

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`

- DeleteOrganizationalBackupPlan
- InvalidOrganizationalBackupPlan

예: 계정 간 관리를 위한 AWS Backup 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 CreateOrganizationalBackupPlan 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
```

```
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
        "creationDate": {
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```


다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `DeleteOrganizationalBackupPlan`


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
```

```
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

다음 예는 AWS Backup Organizations로부터 잘못된 백업 계획을 받았을 때 전송되는 이벤트를 `InvalidOrganizationBackupPlan` 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
```

```
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
                    "enableContinuousBackup": true
                }
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    },
    "eventCategory": "Management"
}
```

알림 옵션: AWS Backup

다음과 같은 두 가지 방법으로 알림을 받을 수 있습니다 AWS Backup.

- AWS 사용자 알림은 Amazon CloudWatch 알람 및 기타 서비스의 알림을 비롯한 알림을 전송할 수 있습니다. AWS Support
- Amazon 심플 알림 서비스는 AWS Backup 이벤트를 알려줄 수 있습니다.

AWS 사용자 알림 및 AWS Backup

AWS Backup AWS 사용자 알림 콘솔에서 백업 알림을 관리할 수 있습니다. AWS 사용자 알림을 사용하면 사용자 알림 센터에서 백업, 복사, 복원 작업의 진행 상황과 백업 정책, 저장소, 복구 시점, 설정에 대한 변경 사항을 볼 수 있습니다.

Amazon CloudWatch, Amazon EventBridge 경보 및 AWS Support 사례 업데이트는 콘솔에서 관리할 수 있는 다른 유형의 알림입니다. 또한 이메일, 알림, AWS Console Mobile Application 푸시 AWS Chatbot 알림 등 여러 전송 옵션을 설정할 수 있습니다.

아마존 SNS 및 AWS Backup 이벤트

AWS Backup Amazon Simple Notification 서비스 (Amazon SNS) 에서 제공하는 강력한 알림을 활용합니다. Amazon SNS 콘솔에서 AWS Backup 이벤트를 알리도록 Amazon SNS를 구성할 수 있습니다.

제한 사항

- Amazon SNS 서비스는 계정 간 알림을 허용하지만, 현재 이 기능은 지원하지 AWS Backup 않습니다. 사용자 고유의 AWS 계정 ID와 주제의 리소스 ARN을 지정해야 합니다.
- AWS Backup SNS 최선의 중복 제거를 위한 표준 주제를 지원하지만 엄격한 중복 제거를 위한 SNS FIFO 주제는 현재 지원하지 AWS Backup 않습니다.

일반 사용 사례

- 실패한 작업에 대한 알림을 받으려면 어떻게 해야 합니까? 의 단계에 따라 실패한 백업 작업에 대한 알림을 설정하십시오. AWS Backup AWS 프리미엄 지원에서.
- 아래의 이벤트 예제 표에서 완료, 실패, 만료된 백업 작업에 대한 Amazon SNS 알림 JSON 샘플을 검토합니다.

Amazon SNS에 대한 전반적인 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요.

AWS Backup 알림 API

Amazon SNS 콘솔 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 주제를 생성한 후 다음 AWS Backup API 작업을 사용하여 백업 알림을 관리할 수 있습니다.

- DeleteBackupVaultNotifications — 지정된 백업 저장소에 대한 이벤트 알림을 삭제합니다.

- GetBackupVaultNotifications — 지정된 백업 저장소에 대한 이벤트 알림을 모두 나열합니다.
- PutBackupVaultNotifications — 지정된 주제 및 이벤트에 대한 알림을 설정합니다.

AWS Backup 다음 이벤트를 지원합니다.

작업 유형	Event
백업 작업	BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | CONTINUOUS_BACKUP_INTERRUPTED
복사 작업	COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED
복원 작업	RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED
복구 시점	RECOVERY_POINT_MODIFIED

AWS Backup for S3는 두 가지 추가 이벤트를 지원합니다.

- S3_BACKUP_OBJECT_FAILED는 백업 작업 도중 AWS Backup 에서 백업에 실패한 모든 S3 객체를 사용자에게 알립니다.
- S3_RESTORE_OBJECT_FAILED는 복원 작업 도중 AWS Backup 에서 복원에 실패한 모든 S3 객체를 사용자에게 알립니다.

이벤트 예

Example 예: 백업 작업 완료

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
```

```
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job was completed successfully. Recovery point
 ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"COMPLETED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example 예: 백업 작업 실패

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"FAILED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
```

```
            }
        }
    }]
}
```

Example 예: 백업 기간 중에 백업 작업을 완료할 수 없습니다.

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes" : {
              "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
              "State" : {"Type":"String","Value":"EXPIRED"},
              "AccountId" : {"Type":"String","Value":"123456789012"},
              "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
              "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

AWS Backup 알림 명령 예제

AWS CLI 명령을 사용하여 AWS Backup 이벤트에 대한 Amazon SNS 알림을 구독, 나열 및 삭제할 수 있습니다.

백업 저장소 알림 넣기 예

다음 명령은 복원 작업이 시작되거나 완료될 때 또는 복구 시점이 수정될 때 알려주도록 지정된 백업 저장소에 대한 Amazon SNS 주제를 구독합니다.

```
aws backup put-backup-vault-notifications
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

백업 저장소 알림 가져오기 예

다음 명령은 지정된 백업 저장소의 Amazon SNS 주제를 현재 구독하고 있는 모든 이벤트를 나열합니다.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

샘플 출력은 다음과 같습니다.

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

백업 저장소 알림 삭제 예

다음 명령은 지정된 백업 저장소에 대한 Amazon SNS 주제의 구독을 취소합니다.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

서비스 보안 AWS Backup 주체로 지정

> **Note**
>
> 사용자를 대신하여 SNS 주제를 게시할 수 있게 AWS Backup 하려면 서비스 AWS Backup 주체로 지정해야 합니다.

AWS Backup 이벤트를 추적하는 데 사용하는 Amazon SNS 주제의 액세스 정책에 다음 JSON을 포함하십시오. 주제의 리소스 Amazon 리소스 이름(ARN)을 지정해야 합니다.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Amazon SNS 액세스 정책에서 서비스 보안 주체를 지정하는 방법에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 모든 AWS 리소스가 주제에 게시하도록 허용을 참조하십시오.

> **Note**
>
> 주제가 암호화된 경우 게시할 수 있도록 AWS Backup 정책에 추가 권한을 포함해야 합니다. 서비스가 암호화된 주제에 게시할 수 있도록 하는 방법에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 AWS 서비스의 이벤트 소스와 암호화된 주제 간 호환성 활성화를 참조하십시오.

문제 해결 AWS Backup

을 (를) 사용할 AWS Backup때 문제가 발생할 수 있습니다. 다음 단원은 발생할 수 있는 몇 가지 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

에 대한 일반적인 질문은 AWS Backup FAQ를 참조하십시오. AWS BackupAWS Backup 포럼에서 답을 검색하고 질문을 올릴 수도 있습니다.

주제

일반적인 문제 해결

리소스를 백업하고 복원할 때는 보호할 리소스에 대한 사용 AWS Backup 권한과 액세스 권한이 있어야 합니다. 적절한 권한을 갖는 가장 쉬운 방법은 백업 계획에 리소스를 할당할 때 기본 역할을 선택하는 것입니다. AWS Identity and Access Management (IAM) 을 사용한 액세스 제어에 대한 자세한 내용은 을 AWS Backup참조하십시오액세스 제어.

백업 저장소와 같은 AWS Backup 리소스에 액세스하려고 할 때 `AccessDenied` 오류가 발생하는 경우 해당 리소스가 없거나 해당 리소스에 액세스할 권한이 없는 것입니다.

특정 리소스 유형을 백업 및 복원하는 데 문제가 발생하면 해당 리소스에 대한 백업 및 복원 문제 해결 주제를 검토하는 것이 도움이 될 수 있습니다. 자세한 내용은 지원되는 AWS 서비스와의 AWS Backup 작동 방식 아래의 링크를 참조하십시오.

리소스 생성 또는 삭제에 AWS Backup 실패한 경우 를 사용하여 AWS CloudTrail 오류 메시지 또는 로그를 확인하여 문제에 대해 자세히 알아볼 수 있습니다. CloudTrailwith 사용에 대한 자세한 내용은 AWS Backup을 참조하십시오를 AWS Backup 사용하여 API 호출을 로깅합니다. CloudTrail .

리소스 생성 문제 해결

다음 정보는 백업 생성과 관련된 문제를 해결하는 데 도움이 될 수 있습니다.

- 일반적으로 AWS 데이터베이스 서비스는 유지 관리 기간이나 자동 백업 기간 1시간 전에 또는 도중에 백업을 시작할 수 없습니다. Amazon FSx는 유지 관리 기간이나 자동 백업 기간 4시간 이전에 또는 도중에 백업을 시작할 수 없습니다(Amazon Aurora는 이 유지 관리 기간 제한에서 제외됨). 이 기간에 예약된 스냅샷 백업은 오류가 발생합니다. 한 가지 예외: 지원되는 서비스에 대해 스냅샷과 연속 백업을 모두 사용하도록 AWS Backup 선택하면 AWS Backup 자동으로 스케줄링되므로 더 이상 해당 창에 대해 걱정할 필요가 없습니다. 지원되는 서비스 목록 및 연속 백업을 수행하는 AWS Backup 데 사용하는 방법에 대한 지침은 지정 시간 복구를 참조하십시오.
- DynamoDB 테이블을 생성하는 동안에는 해당 테이블에 대한 백업 생성이 실패합니다. DynamoDB 테이블을 생성하는 데는 일반적으로 몇 분이 걸립니다.
- 파일 시스템이 매우 큰 경우에는 Amazon EFS 파일 시스템을 백업하는 데 최대 7일이 소요될 수 있습니다. 한 번에 한 개의 동시 백업만 Amazon EFS 파일 시스템의 대기열에 넣을 수 있습니다. 이전 백업이 여전히 진행되는 동안 후속 백업이 대기열에 있으면 백업 창이 만료되고 백업이 생성되지 않습니다.
- Amazon EBS의 소프트 할당량은 AWS 리전 계정당 100,000개의 백업이며, 이 할당량에 도달하면 추가 백업이 실패합니다. 이 할당량에 도달하면 초과 백업을 삭제하거나 할당량 증가를 요청할 수 있습니다. 할당량 증가 요청에 대한 자세한 내용은 AWS 서비스 할당량을 참조하십시오.
- Amazon Relational Database Service(RDS) 백업을 생성할 경우, 다음 사항을 고려하세요.
  - Amazon RDS 스냅샷과 point-in-time 복구가 포함된 연속 백업을 모두 관리하는 AWS Backup 데 사용하지 않는 경우, 사용자가 구성할 수 있는 일일 30분 백업 기간 동안 일정에 따라 시작하거나 필요에 따라 백업을 수행하면 백업이 실패합니다. Amazon RDS 자동 백업에 대한 자세한 내용은 Amazon RDS 사용 설명서의 백업 작업 섹션을 참조하세요. 를 AWS Backup 사용하여 Amazon RDS 스냅샷과 복구를 포함한 연속 백업을 모두 관리하면 이러한 제한을 피할 수 있습니다. point-in-time
  - Amazon RDS 콘솔에서 백업 작업을 시작하면 Aurora 클러스터 백업 작업과 충돌하여 `Backup job expired before completion.` 오류가 발생할 수 있습니다. 이 경우 AWS Backup에서 백업 기간을 더 길게 구성합니다.
  - AWS Backup 복사 작업이 생성될 때 현재 TDE 옵션 그룹을 전달하지 않습니다. 복사 작업 생성에 이 옵션 그룹을 사용하려는 경우, AWS Backup 도구 대신 Amazon RDS 콘솔 또는 Amazon RDS API를 사용해야 합니다. 자세한 내용은 Amazon Relational Database Service 사용 설명서의 옵션 그룹 복사를 참조하세요.
  - 오류: 온디맨드 백업이 완료되었지만 예약된 백업이 실패하고 "The source snapshot KMS key does not exist, is not enabled or you do not have permissions to access it"이라는 오류 메시지가 발생합니다. 온디맨드 작업은 KMS 액세스가 필요하지 않은 API 호출 `CopyDBSnapshot`을 사용하기 때문에 완료된 것입니다.

해결 방법: KMS 키에 IAM 역할을 추가합니다. KMS 키 정책에서 역할을 허용하면 이 작업을 수행할 수 있습니다.

정책을 편집하려면

1. KMS 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 고객 관리형 키를 선택합니다.
3. 편집하려는 고객 관리 키를 클릭합니다.
4. 키 정책에서 정책 보기로 전환을 선택합니다.
5. 편집을 클릭합니다.
6. 역할을 추가합니다.

리소스 삭제 문제 해결

에서 생성한 복구 지점은 보호된 리소스의 콘솔 창에서 삭제할 AWS Backup 수 없습니다. 저장되어 있는 저장소에서 해당 항목을 선택한 다음 삭제를 선택하여 AWS Backup 콘솔에서 삭제할 수 있습니다.

복구 시점 또는 백업 저장소를 삭제하려면 적절한 사용 권한이 필요합니다. IAM을 사용한 액세스 제어에 대한 자세한 내용은 을 AWS Backup참조하십시오액세스 제어.

복원 리소스 문제 해결

API를 사용하여 복원

백업을 프로그래밍 방식으로 복원하려면 StartRestoreJob API 작업을 사용합니다.

백업을 생성할 때 사용한 구성 메타데이터를 가져오려면 GetRecoveryPointRestoreMetadata를 직접적으로 호출할 수 있습니다.

자세한 내용은 백업 복원을 참조하세요.

콘솔을 사용하여 백업 복원

- Amazon S3 데이터 복원
- 가상 머신 복원
- Amazon FSx 파일 시스템 복원
- Amazon EBS 볼륨 복원

- Amazon EFS 파일 시스템 복원
- Amazon DynamoDB 테이블 복원
- Amazon RDS 데이터베이스 복원
- Aurora 클러스터 복원
- Amazon EC2 인스턴스 복원
- Storage Gateway 볼륨 복원
- Amazon DocumentDB 클러스터 복원
- Neptune 클러스터 복원

형식 지정 오류 문제 해결

매개 변수의 값에 와일드카드 (*) 가 포함된 경우 와일드카드는 공백 이외의 값을 포함하도록 처리됩니다. 공백이 포함된 키-값 쌍의 값은 와일드카드의 일부로 포함되지 않습니다.

AWS Backup API

콘솔을 사용하는 것 외에도 AWS Backup API 작업 및 데이터 형식을 사용하면 AWS Backup 및 그 리소스를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 이 섹션에서는 AWS Backup 작업 및 데이터 형식에 대해 설명합니다. 여기에는 AWS Backup에 대한 API 참조가 포함되어 있습니다.

AWS Backup API

- AWS Backup 작업
- AWS Backup 데이터 형식

작업

다음 작업이 AWS Backup에서 지원됩니다.

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework
- DeleteRecoveryPoint

- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection
- GetSupportedResourceTypes

- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob
- StartCopyJob

- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

다음 작업이 AWS Backup gateway에서 지원됩니다.

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines

- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

다음 작업이 AWS Backup에서 지원됩니다.

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

서비스: AWS Backup

복구 지점에서 지정된 법적 보류를 제거합니다. 이 작업은 충분한 권한이 있는 사용자만 수행할 수 있습니다.

Request Syntax

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

CancelDescription

문자열은 법적 보류를 제거하는 이유를 설명합니다.

필수 여부: 예

legalHoldId

법적 보존의 ID.

필수 여부: 예

RetainRecordInDays

법적 보류를 해제하기 위한 정수 금액 (일).

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 201
```

Response Elements

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 201 응답을 다시 전송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidResourceStateException

AWS Backup 이 복구 지점에서 이미 작업을 수행하고 있습니다. 첫 번째 작업이 완료될 때까지 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateBackupPlan

서비스: AWS Backup

백업 계획 이름 및 백업 규칙을 사용하여 백업 계획을 생성합니다. 백업 계획은 리소스의 복구 지점을 만드는 작업을 예약하는 데 AWS Backup 사용되는 정보가 들어 있는 문서입니다.

이미 존재하는 플랜으로 `CreateBackupPlan`을 호출하면 `AlreadyExistsException` 예외를 받습니다.

Request Syntax

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
```

```
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupPlan

백업 계획의 본문. BackupPlanName과 하나 이상의 Rules 집합을 포함합니다.

유형: BackupPlanInput객체

필수 여부: 예

BackupPlanTags

백업 계획에 할당할 태그.

유형: 문자열 간 맵

필수 여부: 아니요

CreatorRequestId

요청을 식별하며 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 합니다. 요청에 기존 백업 계획과 일치하는 CreatorRequestId가 포함된 경우, 해당 계획이 반환됩니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AdvancedBackupSettings

리소스 유형에 대한 설정. 이 옵션은 Windows VSS(Volume Shadow Copy Service) 백업 작업에만 사용할 수 있습니다.

유형: AdvancedBackupSetting객체 어레이

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`)입니다.

타입: 문자열

BackupPlanId

백업 계획의 ID.

타입: 문자열

CreationDate

백업 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateBackupSelection

서비스: AWS Backup

백업 계획에 할당할 리소스 집합을 지정하는 JSON 문서를 생성합니다. 예를 들어, 프로그래밍 방식으로 리소스 할당을 참조하세요.

Request Syntax

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
```

```
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획의 ID.

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupSelection

백업 계획에 리소스 세트를 할당하기 위한 요청 본문입니다.

유형: BackupSelection객체

필수 여부: 예

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanId

백업 계획의 ID.

타입: 문자열

CreationDate

백업 선택 항목이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

SelectionId

리소스 집합을 백업 계획에 할당하는 요청의 본문을 고유하게 식별합니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateBackupVault

서비스: AWS Backup

백업이 저장되는 논리 컨테이너를 생성합니다. `CreateBackupVault` 요청에는 이름, 선택적으로 하나 이상의 리소스 태그, 암호화 키 및 요청 ID가 포함됩니다.

> **Note**
>
> 여권 번호처럼 민감한 데이터를 백업 저장소 이름에 포함하지 마세요.

Request Syntax

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다. 백업 저장소는 문자, 숫자, 하이픈(-)으로 구성됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupVaultTags

백업 저장소에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

EncryptionKeyArn

백업을 보호하는 데 사용되는 서버 측 암호화 키(예: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`)입니다.

유형: String

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다. 백업 저장소는 소문자, 숫자, 하이픈(-)으로 구성됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

백업 저장소가 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateFramework

서비스: AWS Backup

하나 이상의 컨트롤이 있는 프레임워크를 생성합니다. 프레임워크는 백업 방식을 평가하는 데 사용할 수 있는 컨트롤의 모음입니다. 사전 구축된 사용자 지정 가능한 컨트롤을 사용하여 정책을 정의하면 백업 방식이 정책을 준수하는지 여부와 아직 준수하지 않는 리소스를 평가할 수 있습니다.

Request Syntax

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

FrameworkControls

프레임워크를 구성하는 컨트롤. 목록의 각 컨트롤에는 이름, 입력 파라미터, 범위가 있습니다.

유형: FrameworkControl객체 어레이

필수 여부: 예

FrameworkDescription

프레임워크에 대한 최대 1,024자의 설명(선택 사항)입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

FrameworkName

프레임워크의 고유 이름입니다. 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자여야 합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

FrameworkTags

프레임워크에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

IdempotencyToken

고객이 선택한 문자열로, CreateFrameworkInput에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

FrameworkArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

FrameworkName

프레임워크의 고유 이름입니다. 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자여야 합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: [a-zA-Z][_a-zA-Z0-9]*

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK

- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateLegalHold

서비스: AWS Backup

복구 지점 (백업) 에 대한 법적 보류를 생성합니다. 법적 보존은 승인된 사용자가 법적 보존을 취소할 때까지 백업을 변경하거나 삭제하는 것을 제한하는 것입니다. 복구 시점에 하나 이상의 유효한 법적 보존이 있는 경우, 복구 시점을 삭제하거나 연결을 해제하려는 작업은 오류 메시지가 표시되면서 실패합니다.

Request Syntax

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

Description

법적 보류에 대한 설명.

타입: 문자열

필수 항목 여부: 예

IdempotencyToken

이 문자열은 동일한 호출을 구분하기 위해 사용자가 선택한 문자열입니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

RecoveryPointSelection

리소스 유형 또는 백업 보관소와 같은 리소스 세트를 할당하기 위한 기준.

유형: RecoveryPointSelection객체

필수 항목 여부: 아니요

Tags

포함하려는 선택적인 태그입니다. 태그는 리소스를 관리, 필터링, 검색하는 데 사용할 수 있는 키-값 페어입니다. 허용되는 문자는 UTF-8 문자, 숫자, 공백 및 + - = . _ : /입니다.

유형: 문자열 간 맵

필수 여부: 아니요

Title

법적 보류의 제목.

타입: 문자열

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
```

```
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationDate

법적 보존이 생성된 시점.

유형: 타임스탬프

Description

법적 보류에 대한 설명.

타입: 문자열

LegalHoldArn

법적 보류의 Amazon 리소스 이름 (ARN).

타입: 문자열

LegalHoldId

법적 보류의 ID.

타입: 문자열

RecoveryPointSelection

리소스 유형 또는 백업 보관소와 같은 리소스 집합에 할당할 기준.

유형: RecoveryPointSelection객체

Status

법적 보류 상태.

타입: 문자열

유효 값: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

법적 보류의 제목.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateLogicallyAirGappedBackupVault

서비스: AWS Backup

백업을 복사할 수 있는 논리적 컨테이너를 만듭니다.

이 요청에는 이름, 리전, 최대 보존 일수, 최소 보존 일수가 포함되며 선택에 따라 태그와 작성자 요청 ID를 포함할 수 있습니다.

> **Note**
>
> 여권 번호처럼 민감한 데이터를 백업 저장소 이름에 포함하지 마세요.

Request Syntax

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 논리적 에어 갭 처리 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupVaultTags

저장소에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

CreatorRequestId

생성 요청의 ID.

이 파라미터는 선택 사항입니다. 이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

MaxRetentionDays

저장소에 복구 시점이 보존되는 최대 보존 기간입니다. 이 파라미터가 지정되지 않으면 AWS Backup 은 저장소의 복구 시점에 최대 보존 기간을 적용하지 않습니다(무제한 저장 가능).

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최대 보존 기간보다 짧거나 같은 수명 주기 정책이 있어야 합니다. 작업 보존 기간이 최대 보존 기간보다 길면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다.

타입: Long

필수 여부: 예

MinRetentionDays

이 설정은 저장소가 복구 시점을 유지하는 최소 보존 기간을 지정합니다. 이 파라미터가 지정되지 않으면 최소 보존 기간이 적용되지 않습니다.

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최소 보존 기간보다 길거나 같은 수명 주기 정책이 있어야 합니다. 작업 보존 기간이 최소 보존 기간보다 짧으면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다.

타입: Long

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

저장소의 ARN (아마존 리소스 이름).

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 논리적 에어 갭 처리 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

저장소가 생성된 날짜 및 시간입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

VaultState

저장소의 현재 상태.

타입: 문자열

유효 값: `CREATING | AVAILABLE | FAILED`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateReportPlan

서비스: AWS Backup

보고서 계획을 생성합니다. 보고서 계획은 보고서 내용 및 보고서 전달 위치에 AWS Backup 대한 정보가 포함된 문서입니다.

이미 존재하는 플랜으로 `CreateReportPlan`을 호출하면 `AlreadyExistsException` 예외를 받습니다.

Request Syntax

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

IdempotencyToken

고객이 선택한 문자열로, CreateReportPlanInput에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

ReportDeliveryChannel

보고서를 전송하는 위치와 방법, 특히 Amazon S3 버킷 이름, S3 키 접두사 및 보고서 형식에 대한 정보가 들어 있는 구조입니다.

유형: ReportDeliveryChannel객체

필수 여부: 예

ReportPlanDescription

보고서 계획에 대한 최대 1,024자의 설명(선택 사항)입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

ReportPlanName

보고서 계획의 고유 이름입니다. 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자여야 합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

ReportPlanTags

보고서 계획에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

ReportSetting

보고서에 대한 보고서 템플릿을 식별합니다. 보고서는 보고서 템플릿을 사용하여 작성됩니다. 보고서 템플릿은 다음과 같습니다.

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

보고서 템플릿이 RESOURCE_COMPLIANCE_REPORT CONTROL_COMPLIANCE_REPORT OR인 경우 이 API 리소스는 AWS 리전 및 프레임워크의 보고서 적용 범위도 설명합니다.

유형: ReportSetting객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

백업 저장소가 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationTime의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

ReportPlanArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

ReportPlanName

보고서 계획의 고유 이름입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateRestoreTestingPlan

서비스: AWS Backup

복원 테스트 계획을 작성합니다.

복원 테스트 계획을 만드는 두 단계 중 첫 번째 단계입니다. 이 요청이 성공하면 를 사용하여 절차를 CreateRestoreTestingSelection 완료하십시오.

Request Syntax

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다. 이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

RestoreTestingPlan

복원 테스트 계획에는 사용자가 만든 고유한 `RestoreTestingPlanName` 문자열과 `ScheduleExpression` cron이 포함되어야 합니다. 선택적으로 `StartWindowHours` 정수와 `CreatorRequestId` 문자열을 포함할 수 있습니다.

`RestoreTestingPlanName`은 복원 테스트 계획의 이름을 나타내는 고유한 문자열입니다. 이 값은 만든 후에는 변경할 수 없으며 영숫자와 밑줄로만 구성되어야 합니다.

유형: RestoreTestingPlanForCreate객체

필수 여부: 예

Tags

복원 테스트 계획에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

응답 구문

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

복원 테스트 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

RestoreTestingPlanArn

생성된 복원 테스트 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

RestoreTestingPlanName

이 고유한 문자열은 복원 테스트 계획의 이름을 나타냅니다.

생성한 후에는 이름을 변경할 수 없습니다. 이름은 영숫자와 밑줄로만 구성해야 합니다. 최대 길이는 50자입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

ConflictException

AWS Backup 이전 작업의 수행을 완료할 때까지는 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateRestoreTestingSelection

서비스: AWS Backup

요청이 성공적으로 반환된 후에 이 CreateRestoreTestingPlan 요청을 보낼 수 있습니다. 이 단계는 리소스 테스트 계획 생성의 두 번째 부분이며 순차적으로 완료해야 합니다.

이것은 `RestoreTestingSelectionName`, `ProtectedResourceType` 및 다음 중 하나로 구성됩니다.

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

각 보호된 리소스 유형은 단일 값을 가질 수 있습니다.

복원 테스트 선택 항목에는 `ProtectedResourceArns`에 대한 와일드카드 값('*')과 함께 `ProtectedResourceConditions`를 포함할 수 있습니다. 또는 `ProtectedResourceArns`에 최대 30개의 특정 보호된 리소스 ARN을 포함할 수 있습니다.

보호된 리소스 유형과 특정 ARN 둘 다로는 선택할 수 없습니다. 둘 다 포함되면 요청이 실패합니다.

Request Syntax

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
```

```
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

관련 CreateRestoreTestingPlan 요청에서 반환된 복원 테스트 계획 이름을 입력합니다.

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 선택적인 고유 문자열입니다. 이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

RestoreTestingSelection

이것은 `RestoreTestingSelectionName`, `ProtectedResourceType` 및 다음 중 하나로 구성됩니다.

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

각 보호된 리소스 유형은 단일 값을 가질 수 있습니다.

복원 테스트 선택 항목에는 ProtectedResourceArns에 대한 와일드카드 값('*')과 함께 ProtectedResourceConditions를 포함할 수 있습니다. 또는 ProtectedResourceArns에 최대 30개의 특정 보호된 리소스 ARN을 포함할 수 있습니다.

유형: RestoreTestingSelectionForCreate객체

필수 여부: 예

응답 구문

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

리소스 테스트 선택 항목이 생성된 시간.

유형: 타임스탬프

RestoreTestingPlanArn

복원 테스트 선택과 관련된 복원 테스트 계획의 ARN입니다.

타입: 문자열

RestoreTestingPlanName

복원 테스트 계획의 이름.

생성한 후에는 이름을 변경할 수 없습니다. 이름은 영숫자와 밑줄로만 구성해야 합니다. 최대 길이는 50자입니다.

타입: 문자열

RestoreTestingSelectionName

관련 복원 테스트 계획의 복원 테스트 선택 이름입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupPlan

서비스: AWS Backup

백업 계획을 삭제합니다. 리소스의 모든 연결된 선택 항목이 삭제된 후에만 백업 계획을 삭제할 수 있습니다. 백업 계획을 삭제하면 백업 계획의 현재 버전이 삭제됩니다. 이전 버전(있는 경우)은 계속 존재합니다.

Request Syntax

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`)입니다.

타입: 문자열

BackupPlanId

백업 계획을 고유하게 식별합니다.

타입: 문자열

DeletionDate

백업 계획이 삭제된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `DeletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupSelection

서비스: AWS Backup

`SelectionId`에서 지정한 백업 계획과 관련된 리소스 선택 항목을 삭제합니다.

Request Syntax

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 여부: 예

selectionId

리소스 집합을 백업 계획에 할당하는 요청의 본문을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupVault

서비스: AWS Backup

이름으로 식별되는 백업 저장소를 삭제합니다. 저장소는 비어 있는 경우에만 삭제할 수 있습니다.

Request Syntax

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupVaultAccessPolicy

서비스: AWS Backup

백업 저장소에 대한 권한을 관리하는 정책 문서를 삭제합니다.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다. 백업 저장소는 소문자, 숫자, 하이픈(-)으로 구성됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupVaultLockConfiguration

서비스: AWS Backup

백업 AWS Backup 저장소 이름으로 지정된 백업 저장소에서 저장소 잠금을 삭제합니다.

저장소 잠금 구성을 변경할 수 없는 경우 API 작업을 사용하여 저장소 잠금을 삭제할 수 없으며, 삭제하려고 할 경우 `InvalidRequestException`이 표시됩니다. 자세한 내용은 AWS Backup 개발자 안내서의 Vault Lock을 참조하십시오.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

AWS Backup 저장소 잠금을 삭제할 백업 저장소의 이름.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK

- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteBackupVaultNotifications

서비스: AWS Backup

지정된 백업 저장소에 대한 이벤트 알림을 삭제합니다.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteFramework

서비스: AWS Backup

프레임워크 이름으로 지정된 프레임워크를 삭제합니다.

Request Syntax

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

frameworkName

프레임워크의 고유 이름입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

AWS Backup 이전 작업의 수행이 완료될 때까지 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteRecoveryPoint

서비스: AWS Backup

복구 시점 ID로 지정된 복구 시점을 삭제합니다.

복구 시점 ID가 연속 백업에 속하는 경우, 이 엔드포인트를 호출하면 기존 연속 백업이 삭제되고 향후 연속 백업이 중지됩니다.

IAM 역할의 권한이 부족하여 이 API를 호출할 수 없는 경우, 서비스에서 HTTP 본문이 비어 있는 HTTP 200 응답을 다시 보내지만 복구 시점은 삭제되지 않습니다. 그 대신 `EXPIRED` 상태가 됩니다.

IAM 역할이 `iam:CreateServiceLinkedRole` 작업을 수행하면 이 API를 사용하여 `EXPIRED` 복구 시점을 삭제할 수 있습니다. 이 역할을 추가하는 방법을 자세히 알아보려면 수동 삭제 문제 해결을 참조하세요.

사용자 또는 역할을 삭제하거나 역할 내의 권한을 제거하면 삭제에 실패하고 `EXPIRED` 상태가 됩니다.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidResourceStateException

AWS Backup 이 복구 지점에서 이미 작업을 수행하고 있습니다. 첫 번째 작업이 완료될 때까지 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteReportPlan

서비스: AWS Backup

보고서 계획 이름으로 지정된 보고서 계획을 삭제합니다.

Request Syntax

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

reportPlanName

보고서 계획의 고유 이름입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

AWS Backup 이전 작업의 수행이 완료될 때까지 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteRestoreTestingPlan

서비스: AWS Backup

이 요청은 지정된 복원 테스트 계획을 삭제합니다.

먼저 연결된 복원 테스트 선택 항목을 모두 삭제한 경우에만 성공적으로 삭제할 수 있습니다.

Request Syntax

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

삭제하려는 복원 테스트 계획의 필수 고유 이름입니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteRestoreTestingSelection

서비스: AWS Backup

복원 테스트 계획 이름과 복원 테스트 선택 항목 이름을 입력합니다.

복원 테스트 계획을 삭제하려면 먼저 복원 테스트 계획과 연결된 모든 테스트 선택 항목을 삭제해야 합니다.

Request Syntax

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

삭제하려는 복원 테스트 선택 항목이 포함된 복원 테스트 계획의 필수 고유 이름입니다.

필수 여부: 예

RestoreTestingSelectionName

삭제하려는 복원 테스트 선택 항목의 필수 고유 이름입니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeBackupJob

서비스: AWS Backup

지정된 BackupJobId에 대한 백업 작업 세부 정보를 반환합니다.

Request Syntax

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupJobId

리소스 백업 요청을 고유하게 AWS Backup 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
   "CompletionDate": number,
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "ExpectedCompletionDate": number,
   "IamRoleArn": "string",
   "InitiationDate": number,
   "IsParent": boolean,
   "MessageCategory": "string",
   "NumberOfChildJobs": number,
   "ParentJobId": "string",
   "PercentDone": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "StartBy": number,
   "State": "string",
   "StatusMessage": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccountId

백업 작업을 소유한 계정 ID를 반환합니다.

유형: String

패턴: `^[0-9]{12}$`

BackupJobId

리소스 백업 요청을 고유하게 AWS Backup 식별합니다.

타입: 문자열

BackupOptions

백업 계획 또는 온디맨드 백업 작업의 일부로 지정된 옵션을 나타냅니다.

유형: String 간 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

값 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

백업의 크기(바이트 단위)입니다.

타입: Long

BackupType

백업 작업을 위해 선택한 실제 백업 유형을 나타냅니다. 예를 들어, Windows VSS(Volume Shadow Copy Service) 백업이 성공적으로 수행된 경우 `BackupType`은 `"WindowsVSS"`를 반환합니다. `BackupType`이 비어 있는 경우 백업 유형은 일반 백업입니다.

타입: 문자열

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

작업 상태를 쿼리할 때 백업 저장소로 전송된 크기(바이트)입니다.

타입: Long

ChildJobsInState

포함된 하위(중첩) 백업 작업의 통계를 반환합니다.

유형: String과 Long 간의 맵

유효한 키: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

백업 작업을 생성하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CreatedBy

백업 작업을 생성하는 데 사용되는 백업 계획의 `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, `BackupRuleId`를 비롯하여, 백업 작업의 생성에 대한 식별 정보를 포함합니다.

유형: RecoveryPointCreator객체

CreationDate

백업 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

ExpectedCompletionDate

리소스를 백업하는 작업이 완료될 것으로 예상되는 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `ExpectedCompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

InitiationDate

백업 작업이 시작된 날짜.

유형: 타임스탬프

IsParent

백업 작업이 상위(복합) 작업인 부울 값을 반환합니다.

타입: 부울

MessageCategory

지정된 메시지 범주의 작업 수입니다.

예시 문자열에는 `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL`, `INVALIDPARAMETERS` 등이 있습니다. 허용된 MessageCategory 문자열 목록에 대한 모니터링 보기.

타입: 문자열

NumberOfChildJobs

하위(중첩) 백업 작업 수를 반환합니다.

타입: Long

ParentJobId

상위(복합) 리소스 백업 작업 ID를 반환합니다.

타입: 문자열

PercentDone

작업 상태를 쿼리할 때 작업의 예상 완료율을 포함합니다.

타입: 문자열

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

ResourceArn

저장된 리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

ResourceType

백업할 AWS 리소스 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스).

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

백업 작업을 취소하기 전에 시작해야 하는 시간을 Unix 형식 및 협정 세계시(UTC)로 지정합니다. 이 값은 시작 기간을 예약된 시간에 더하여 계산됩니다. 따라서 예약된 시간이 오후 6시이고 시작 기간이 2시간인 경우, `StartBy` 시간은 지정된 날짜의 오후 8시가 됩니다. `StartBy`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

State

백업 작업의 현재 상태입니다.

타입: 문자열

유효 값: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

리소스를 백업하기 위한 작업의 상태를 설명하는 자세한 메시지입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

DependencyFailureException

종속 AWS 서비스 또는 리소스가 서비스에 오류를 반환하여 작업을 완료할 수 없습니다. AWS Backup

HTTP 상태 코드: 500

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeBackupVault

서비스: AWS Backup

이름으로 지정된 백업 저장소에 대한 메타데이터를 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

지정된 백업 저장소의 계정 ID입니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
   "Locked": boolean,
   "MaxRetentionDays": number,
```

```
    "MinRetentionDays": number,
    "NumberOfRecoveryPoints": number,
    "VaultType": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

타입: 문자열

CreationDate

백업 저장소가 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다. 이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

EncryptionKeyArn

백업을 보호하는 데 사용되는 서버 측 암호화 키(예: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`)입니다.

타입: 문자열

LockDate

AWS Backup 저장소 잠금 구성을 변경하거나 삭제할 수 없는 날짜 및 시간입니다.

잠금 날짜를 지정하지 않고 저장소 잠금을 저장소에 적용한 경우, 언제든지 저장소 잠금 설정을 변경하거나 저장소에서 저장소 잠금을 완전히 삭제할 수 있습니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

Locked

AWS Backup 저장소 잠금이 현재 백업 저장소를 보호하고 있는지 여부를 나타내는 부울 `True`저장소 잠금으로 인해 저장소에 저장된 복구 지점의 삭제 또는 업데이트 작업이 실패한다는 의미입니다.

타입: 부울

MaxRetentionDays

AWS Backup 저장소 잠금 설정은 저장소에서 복구 지점을 보존하는 최대 보존 기간을 지정합니다. 이 파라미터가 지정되지 않으면 저장소 잠금은 저장소의 복구 시점에 최대 보존 기간을 적용하지 않습니다(무제한 저장 가능).

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최대 보존 기간보다 짧거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최대 보존 기간보다 길면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 시점은 영향을 받지 않습니다.

타입: Long

MinRetentionDays

AWS Backup 저장소 잠금 설정은 저장소에서 복구 지점을 보존하는 최소 보존 기간을 지정합니다. 이 파라미터가 지정되지 않으면 저장소 잠금이 최소 보존 기간을 적용하지 않습니다.

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최소 보존 기간보다 길거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최소 보존 기간보다 짧으면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 시점은 영향을 받지 않습니다.

타입: Long

NumberOfRecoveryPoints

백업 저장소에 저장된 복구 시점의 수입니다.

타입: Long

VaultType

저장소 유형이 설명되어 있습니다.

타입: 문자열

유효 값: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeCopyJob

서비스: AWS Backup

리소스의 복사본 생성과 관련된 메타데이터를 반환합니다.

Request Syntax

```
GET /copy-jobs/copyJobId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

copyJobId

복사 작업을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
```

```
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "MessageCategory": "string",
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CopyJob

복사 작업에 대한 세부 정보를 포함합니다.

유형: CopyJob객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeFramework

서비스: AWS Backup

지정된 FrameworkName에 대한 프레임워크 세부 정보를 반환합니다.

Request Syntax

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

frameworkName

프레임워크의 고유 이름입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: [a-zA-Z][_a-zA-Z0-9]*

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
```

```
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

프레임워크가 생성된 날짜 및 시간이며, ISO 8601 형식으로 표시됩니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 2020-07-10T15:00:00.000-08:00은 UTC보다 8시간 늦은 2020년 7월 10일 오후 3시를 나타냅니다.

유형: 타임스탬프

DeploymentStatus

프레임워크의 배포 상태입니다. 상태는 다음과 같습니다.

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

타입: 문자열

FrameworkArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

FrameworkControls

프레임워크를 구성하는 컨트롤. 목록의 각 컨트롤에는 이름, 입력 파라미터, 범위가 있습니다.

유형: FrameworkControl객체 어레이

FrameworkDescription

프레임워크에 대한 설명입니다(선택 사항).

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

FrameworkName

프레임워크의 고유 이름입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

프레임워크는 하나 이상의 컨트롤로 구성됩니다. 각 컨트롤은 백업 계획, 백업 선택, 백업 저장소 또는 복구 시점과 같은 리소스를 제어합니다. 또한 각 리소스에 대한 AWS Config 기록을 켜거나 끌 수 있습니다. 상태는 다음과 같습니다.

- `ACTIVE` - 프레임워크가 제어하는 모든 리소스에 대해 기록이 켜진 경우입니다.
- `PARTIALLY_ACTIVE` - 프레임워크가 제어하는 하나 이상의 리소스에 대해 기록이 꺼진 경우입니다.
- `INACTIVE` - 프레임워크가 제어하는 모든 리소스에 대해 기록이 꺼진 경우입니다.
- `UNAVAILABLE` AWS Backup 현재 녹화 상태를 확인할 수 없는 경우.

타입: 문자열

IdempotencyToken

고객이 선택한 문자열로, `DescribeFrameworkOutput`에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript

- AWS PHP V3용 SDK
- AWS 파이썬용 SDK
- AWS 루비 V3용 SDK

DescribeGlobalSettings

서비스: AWS Backup

계정이 교차 AWS 계정 백업을 선택했는지 여부를 설명합니다. 계정이 Organizations 조직의 멤버가 아닌 경우 오류를 반환합니다. 예제: `describe-global-settings --region us-west-2`

Request Syntax

```
GET /global-settings HTTP/1.1
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GlobalSettings

`isCrossAccountBackupEnabled` 플래그의 상태입니다.

유형: 문자열-문자열 맵

LastUpdateTime

`isCrossAccountBackupEnabled` 플래그를 마지막으로 업데이트한 날짜와 시간입니다. 이 업데이트는 Unix 형식 및 협정 세계시(UTC)로 표시됩니다. `LastUpdateTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeProtectedResource

서비스: AWS Backup

마지막으로 백업한 시간, Amazon 리소스 이름 (ARN), 저장된 리소스의 AWS 서비스 유형을 포함하여 저장된 리소스에 대한 정보를 반환합니다.

Request Syntax

```
GET /resources/resourceArn HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

resourceArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LastBackupTime

리소스가 마지막으로 백업된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastBackupTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

LastBackupVaultArn

가장 최근의 백업 복구 지점이 포함된 백업 저장소의 ARN (Amazon 리소스 이름).

타입: 문자열

LastRecoveryPointArn

가장 최근 복구 지점의 ARN (Amazon 리소스 이름).

타입: 문자열

LatestRestoreExecutionTimeMinutes

가장 최근의 복원 작업을 완료하는 데 걸린 시간 (분).

타입: Long

LatestRestoreJobCreationDate

가장 최근 복원 작업을 만든 날짜.

유형: 타임스탬프

LatestRestoreRecoveryPointCreationDate

가장 최근 복구 지점이 생성된 날짜.

유형: 타임스탬프

ResourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

ResourceName

지정된 백업에 속하는 리소스의 이름.

타입: 문자열

ResourceType

복구 지점으로 저장된 AWS 리소스 유형 (예: Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스).

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeRecoveryPoint

서비스: AWS Backup

ID, 상태, 암호화, 수명 주기 등 복구 시점과 관련된 메타데이터를 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

지정된 백업 저장소의 계정 ID.

패턴: `^[0-9]{12}$`

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupSizeInBytes

백업의 크기(바이트 단위)입니다.

타입: Long

BackupVaultArn

백업 저장소를 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

`DeleteAt` 및 `MoveToColdStorageAt` 타임스탬프를 포함하는 `CalculatedLifecycle` 객체입니다.

유형: CalculatedLifecycle객체

CompletionDate

복구 시점을 생성하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CompositeMemberIdentifier

복합 그룹 내 리소스의 식별자 (예: 복합 (부모) 스택에 속하는 중첩된 (하위) 복구 지점) ID는 스택 내의 논리적 ID 전송됩니다.

타입: 문자열

CreatedBy

복구 시점을 생성하는 데 사용되는 백업 계획의 BackupPlanArn, BackupPlanId, BackupPlanVersion, BackupRuleId를 비롯하여, 복구 시점의 생성에 대한 식별 정보를 포함합니다.

유형: RecoveryPointCreator객체

CreationDate

복구 시점이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

EncryptionKeyArn

백업을 보호하는 데 사용되는 서버 측 암호화 키입니다(예: arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab).

타입: 문자열

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: arn:aws:iam::123456789012:role/S3Access).

타입: 문자열

IsEncrypted

지정된 복구 시점이 암호화된 경우 TRUE로 반환되거나, 복구 시점이 암호화되지 않은 경우 FALSE로 반환되는 부울 값입니다.

타입: 부울

IsParent

복구 시점이 상위(복합) 작업인 부울 값을 반환합니다.

타입: 부울

LastRestoreTime

복구 시점이 마지막으로 복원된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. LastRestoreTime의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

유형: Lifecycle객체

ParentRecoveryPointArn

상위(복합) 복구 시점을 고유하게 식별하는 ARN입니다(예: arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45).

타입: 문자열

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45).

타입: 문자열

ResourceArn

저장된 리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

ResourceName

지정된 백업에 속하는 리소스의 이름.

타입: 문자열

ResourceType

복구 지점으로 저장할 AWS 리소스 유형 (예: Amazon Elastic Block Store (Amazon EBS) 볼륨 또는 Amazon RDS (아마존 관계형 데이터베이스 서비스) 데이터베이스).

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

리소스가 원래 백업되었던 소스 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다 (예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`). 복구가 동일한 AWS 계정 또는 지역에 복원되는 경우 이 값은 다음과 같습니다. `null`

타입: 문자열

Status

복구 시점의 상태를 지정하는 상태 코드입니다.

`PARTIAL`상태는 백업 창이 닫히기 전에 복구 지점을 만들 AWS Backup 수 없음을 나타냅니다. API를 사용하여 백업 계획 기간을 늘리려면 을 참조하십시오 UpdateBackupPlan. 콘솔을 사용하여 백업 계획을 선택하고 편집하여 백업 계획 기간을 늘릴 수도 있습니다.

`EXPIRED`상태는 복구 지점이 보존 기간을 초과했지만 권한이 AWS Backup 없거나 삭제할 수 없는 상태임을 나타냅니다. 이러한 복구 시점을 수동으로 삭제하려면 시작하기의 리소스 정리 섹션에서 3단계: 복구 시점 삭제를 참조하세요.

`STOPPED` 상태는 연속 백업에서 사용자가 연속 백업을 비활성화하는 작업을 수행한 경우에 발생합니다. 권한 제거, 버전 관리 해제, 전송 대상 이벤트 해제, 적용 EventBridge 규칙 비활성화 EventBridge 등이 원인일 수 있습니다. AWS Backup

`STOPPED` 상태를 해결하려면 요청된 모든 권한이 부여되고 S3 버킷에서 버전 관리가 활성화되어 있는지 확인합니다. 이러한 조건이 충족되면 백업 규칙의 다음 인스턴스를 실행하면 새로운 연속 복구 시점이 생성될 것입니다. 중지됨 상태인 복구 시점은 삭제할 필요가 없습니다.

Amazon EC2에 대한 SAP HANA의 경우 사용자 작업, 애플리케이션 구성 오류 또는 백업 실패로 인해 `STOPPED` 상태가 발생합니다. 향후 연속 백업이 성공하도록 보장하려면 복구 시점 상태를 살펴보고 SAP HANA의 세부 사항을 확인하세요.

타입: 문자열

유효 값: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

복구 시점의 상태를 설명하는 상태 메시지입니다.

타입: 문자열

StorageClass

복구 시점의 스토리지 클래스를 지정합니다. 유효한 값은 `WARM` 또는 `COLD`입니다.

타입: 문자열

유효 값: `WARM | COLD | DELETED`

VaultType

설명된 복구 지점이 저장되는 저장소의 유형입니다.

타입: 문자열

유효 값: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeRegionSettings

서비스: AWS Backup

리전에 대한 현재 서비스 옵트인 설정을 반환합니다. 서비스에 대해 서비스 옵트인이 활성화된 경우, 리소스가 온디맨드 백업 또는 예약 백업 계획에 포함되어 있을 때 이 지역에서 해당 서비스의 리소스를 AWS Backup 보호하려고 시도합니다. 그렇지 않은 경우에는 AWS Backup 이 이 리전에서 해당 서비스의 리소스를 보호하려고 하지 않습니다.

Request Syntax

```
GET /account-settings HTTP/1.1
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ResourceTypeManagementPreference

리소스 유형에 대한 백업을 AWS Backup 완전히 관리하는지 여부를 반환합니다.

전체 관리의 이점은 전체 AWS Backup 관리를 참조하십시오. AWS Backup

리소스 유형 목록 및 각 리소스 유형 전체 AWS Backup 관리 지원 여부는 리소스별 기능 가용성 테이블을 참조하세요.

"DynamoDB":false경우 AWS Backup의 고급 DynamoDB 백업 기능을 활성화하여 DynamoDB 백업을 완벽하게 AWS Backup 관리할 수 있습니다.

유형: String과 부울 간의 맵

키 패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

ResourceTypeOptInPreference

서비스는 해당 지역의 옵트인 기본 설정과 함께 제공됩니다.

유형: String과 부울 간의 맵

키 패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeReportJob

서비스: AWS Backup

`ReportJobId`에서 지정한 대로 보고서 생성과 관련된 세부 정보를 반환합니다.

Request Syntax

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

reportJobId

보고서 작업의 식별자입니다. 임의로 생성되는 최대 1,024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 보고서 작업 ID는 편집할 수 없습니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
```

```
    }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ReportJob

완료 및 생성 시간, 보고서 대상, 고유한 보고서 작업 ID, Amazon Resource Name (ARN), 보고서 템플릿, 상태, 상태 메시지 등 보고서 작업에 대한 정보.

유형: ReportJob객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeReportPlan

서비스: AWS Backup

AWS 계정 및 에 대한 모든 보고서 계획 목록을 반환합니다 AWS 리전.

Request Syntax

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

reportPlanName

보고서 계획의 고유 이름입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
```

```
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ReportPlan

이름으로 지정된 보고서 계획에 대한 세부 정보를 반환합니다. 이러한 세부 정보에는 보고서 계획의 Amazon 리소스 이름(ARN), 설명, 설정, 전송 채널, 배포 상태, 생성 시간, 마지막 시도 시간 및 성공적인 실행 시간이 포함됩니다.

유형: ReportPlan객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DescribeRestoreJob

서비스: AWS Backup

작업 ID로 지정된 복원 작업과 관련된 메타데이터를 반환합니다.

Request Syntax

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

restoreJobId

복구 시점을 복원하는 작업을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
```

```
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccountId

복원 작업을 소유한 계정 ID를 반환합니다.

유형: String

패턴: `^[0-9]{12}$`

BackupSizeInBytes

복원된 리소스의 크기(바이트 단위)입니다.

타입: Long

CompletionDate

복구 시점을 복원하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CreatedBy

복원 작업 생성에 대한 식별 정보가 포함되어 있습니다.

유형: RestoreJobCreator객체

CreatedResourceArn

복원 작업으로 생성된 리소스의 Amazon 리소스 이름 (ARN).

ARN의 형식은 백업된 리소스의 리소스 유형에 따라 달라집니다.

타입: 문자열

CreationDate

복원 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

DeletionStatus

복원 테스트에서 생성된 데이터의 상태.

타입: 문자열

유효 값: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

복원 작업 삭제 상태를 설명합니다.

타입: 문자열

ExpectedCompletionTimeMinutes

복구 시점을 복원하는 작업에 소요될 것으로 예상되는 시간(분)입니다.

타입: Long

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

PercentDone

작업 상태를 쿼리할 때 작업의 예상 완료율을 포함합니다.

타입: 문자열

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

RecoveryPointCreationDate

지정된 복원 작업에 의해 만들어진 복구 지점의 생성 날짜.

유형: 타임스탬프

ResourceType

복원 작업과 관련된 메타데이터를 리소스 유형별로 나열하여 반환합니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

복구 시점을 복원하는 작업을 고유하게 식별합니다.

타입: 문자열

Status

복구 지점을 AWS Backup 복원하기 위해 시작한 작업의 상태를 지정하는 상태 코드입니다.

타입: 문자열

유효 값: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

복구 시점을 복원하기 위한 작업의 상태를 보여 주는 메시지입니다.

타입: 문자열

ValidationStatus

지정된 복원 작업에 대한 검증 실행 상태입니다.

타입: 문자열

유효 값: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

상태 메시지입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

DependencyFailureException

종속 AWS 서비스 또는 리소스가 AWS Backup 서비스에 오류를 반환하여 작업을 완료할 수 없습니다.

HTTP 상태 코드: 500

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DisassociateRecoveryPoint

서비스: AWS Backup

Amazon RDS와 같은 소스 서비스에서 지정된 연속 백업 복구 지점을 AWS Backup 삭제하고 해당 연속 백업에 대한 제어를 해제합니다. 소스 서비스는 원래 백업 계획에 지정된 수명 주기를 사용하여 연속 백업을 계속 생성하고 유지합니다.

스냅샷 백업 복구 시점은 지원하지 않습니다.

Request Syntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

저장소의 고유한 이름. AWS Backup

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

복구 지점을 고유하게 식별하는 Amazon 리소스 이름 (ARN). AWS Backup

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidResourceStateException

AWS Backup 이미 이 복구 지점에서 작업을 수행하고 있습니다. 첫 번째 작업이 완료될 때까지 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DisassociateRecoveryPointFromParent

서비스: AWS Backup

특정 하위(중첩) 복구 시점에 대한 이 작업을 수행하면 지정된 복구 시점과 상위(복합) 복구 시점 간의 관계가 제거됩니다.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

하위 (중첩된) 복구 지점이 저장되는 논리적 컨테이너의 이름입니다. Backup Vault는 생성에 사용된 계정 및 저장소가 생성된 AWS 지역의 고유한 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

하위 (중첩된) 복구 지점을 고유하게 식별하는 Amazon 리소스 이름 (ARN). 예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ExportBackupPlanTemplate

서비스: AWS Backup

계획 ID로 지정된 백업 계획을 백업 템플릿으로 반환합니다.

Request Syntax

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanTemplateJson

JSON 형식의 백업 계획 템플릿 본문입니다.

> **Note**
>
> 이 문서는 서명된 JSON 문서이므로 `GetBackupPlanFromJSON.`에 전달되기 전에는 수정할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBackupPlan

서비스: AWS Backup

지정된 BackupPlanId에 대한 BackupPlan 세부 정보를 반환합니다. 세부 정보는 JSON 형식의 백업 계획 본문과 계획 메타데이터입니다.

Request Syntax

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 여부: 예

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
```

```
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
```

```
    "CreatorRequestId": "string",
    "DeletionDate": number,
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AdvancedBackupSettings

각 리소스 유형에 대한 BackupOptions 목록이 포함됩니다. 백업 계획에 고급 옵션이 설정된 경우에만 목록이 채워집니다.

유형: AdvancedBackupSetting객체 어레이

BackupPlan

백업 계획의 본문을 지정합니다. BackupPlanName과 하나 이상의 Rules 집합을 포함합니다.

유형: BackupPlan객체

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50)입니다.

타입: 문자열

BackupPlanId

백업 계획을 고유하게 식별합니다.

타입: 문자열

CreationDate

백업 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다.

타입: 문자열

DeletionDate

백업 계획이 삭제된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `DeletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

LastExecutionDate

이 백업 계획을 마지막으로 실행한 시간. 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastExecutionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBackupPlanFromJSON

서비스: AWS Backup

백업 계획 또는 오류를 지정하는 유효한 JSON 문서를 반환합니다.

Request Syntax

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupPlanTemplateJson

JSON 형식의 고객이 제공한 백업 계획 문서입니다.

타입: 문자열

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlan

백업 계획의 본문을 지정합니다. BackupPlanName과 하나 이상의 Rules 집합을 포함합니다.

유형: BackupPlan객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBackupPlanFromTemplate

서비스: AWS Backup

`templateId`로 지정된 템플릿을 백업 계획으로 반환합니다.

Request Syntax

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

templateId

저장된 백업 계획 템플릿을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanDocument

계획의 이름, 규칙, 백업 저장소를 포함하여 대상 템플릿을 기반으로 백업 계획의 본문을 반환합니다.

유형: BackupPlan객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS 루비 V3용 SDK

GetBackupSelection

서비스: AWS Backup

선택 메타데이터 및 백업 계획과 관련된 리소스 목록을 지정하는 JSON 형식의 문서를 반환합니다.

Request Syntax

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 여부: 예

selectionId

리소스 집합을 백업 계획에 할당하는 요청의 본문을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanId

백업 계획을 고유하게 식별합니다.

타입: 문자열

BackupSelection

백업 계획에 리소스 세트를 할당하기 위한 요청 본문을 지정합니다.

유형: BackupSelection객체

CreationDate

백업 선택 항목이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다.

타입: 문자열

SelectionId

리소스 집합을 백업 계획에 할당하는 요청의 본문을 고유하게 식별합니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBackupVaultAccessPolicy

서비스: AWS Backup

이름이 지정된 백업 저장소와 관련된 액세스 정책 문서를 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

JSON 형식의 백업 저장소 액세스 정책 문서입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBackupVaultNotifications

서비스: AWS Backup

지정된 백업 저장소에 대한 이벤트 알림을 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

BackupVaultEvents

백업 저장소에 리소스를 백업할 작업의 상태를 나타내는 이벤트 어레이입니다.

유형: 문자열 어레이

유효 값: `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

Amazon Simple Notification Service(Amazon SNS) 주제를 고유하게 식별하는 ARN(예: `arn:aws:sns:us-west-2:111122223333:MyTopic`)입니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetLegalHold

서비스: AWS Backup

이 작업을 수행하면 지정된 법적 보존에 대한 세부 정보가 반환됩니다. 세부 정보는 JSON 형식의 법적 보존 본문과 메타데이터입니다.

Request Syntax

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

legalHoldId

법적 보류의 ID.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
```

```
      "VaultNames": [ "string" ]
   },
   "RetainRecordUntil": number,
   "Status": "string",
   "Title": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CancelDescription

법적 보류를 취소한 이유.

타입: 문자열

CancellationDate

법적 보존이 취소된 시간.

유형: 타임스탬프

CreationDate

법적 보존이 생성된 시간.

유형: 타임스탬프

Description

법적 보류에 대한 설명.

타입: 문자열

LegalHoldArn

지정된 법적 보존에 대한 프레임워크 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

LegalHoldId

법적 보류의 ID.

타입: 문자열

RecoveryPointSelection

리소스 유형 또는 백업 보관소와 같은 리소스 세트를 할당하기 위한 기준.

유형: RecoveryPointSelection객체

RetainRecordUntil

법적 보존 기록이 보존되는 날짜 및 시간.

유형: 타임스탬프

Status

법적 보류 상태.

타입: 문자열

유효 값: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

법적 보류의 제목.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetRecoveryPointRestoreMetadata

서비스: AWS Backup

백업을 생성하는 데 사용된 메타데이터 키-값 페어 집합을 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

지정된 백업 저장소의 계정 ID.

패턴: `^[0-9]{12}$`

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

ResourceType

복구 지점의 리소스 유형.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

백업된 리소스의 원래 구성을 설명하는 메타데이터 키-값 페어 집합입니다. 이러한 값은 복원 중인 서비스에 따라 달라집니다.

유형: 문자열-문자열 맵

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS 루비 V3용 SDK

GetRestoreJobMetadata

서비스: AWS Backup

이 요청은 지정된 복원 작업에 대한 메타데이터를 반환합니다.

Request Syntax

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

restoreJobId

이 식별자는 내 복원 작업의 고유 식별자입니다 AWS Backup.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Metadata

여기에는 지정된 백업 작업의 메타데이터가 포함됩니다.

유형: 문자열-문자열 맵

RestoreJobId

이는 해당 복원 작업의 고유 식별자입니다 AWS Backup.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetRestoreTestingInferredMetadata

서비스: AWS Backup

이 요청은 보안 기본 설정으로 복원 작업을 시작하는 데 필요한 최소한의 메타데이터 세트를 반환합니다. `BackupVaultName` 및 `RecoveryPointArn`은 필수 파라미터입니다. `BackupVaultAccountId`는 선택적인 파라미터입니다.

Request Syntax

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

지정된 백업 저장소의 계정 ID.

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. Backup Vault는 생성에 사용된 계정 및 생성된 AWS 지역의 고유한 이름으로 식별됩니다. 백업 볼트는 문자, 숫자, 하이픈(-)으로 구성됩니다.

필수 여부: 예

RecoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

InferredMetadata

요청에서 추론된 메타데이터의 문자열 맵입니다.

유형: 문자열-문자열 맵

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS 파이썬용 SDK
- AWS 루비 V3용 SDK

GetRestoreTestingPlan

서비스: AWS Backup

지정된 RestoreTestingPlanName에 대한 RestoreTestingPlan 세부 정보를 반환합니다. 세부 정보는 JSON 형식의 복원 테스트 계획 본문과 계획 메타데이터입니다.

Request Syntax

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

복원 테스트 계획의 필수 고유 이름입니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
```

```
        "RestoreTestingPlanArn": "string",
        "RestoreTestingPlanName": "string",
        "ScheduleExpression": "string",
        "ScheduleExpressionTimezone": "string",
        "StartWindowHours": number
    }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

RestoreTestingPlan

복원 테스트 계획의 본문을 지정합니다. RestoreTestingPlanName을 포함합니다.

유형: RestoreTestingPlanForGet객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetRestoreTestingSelection

서비스: AWS Backup

반환 RestoreTestingSelection: 복원 테스트 계획의 리소스 및 요소를 표시합니다.

Request Syntax

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

복원 테스트 계획의 필수 고유 이름입니다.

필수 여부: 예

RestoreTestingSelectionName

복원 테스트 선택 항목의 필수 고유 이름입니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
```

```
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

RestoreTestingSelection

복원 테스트 선택 항목의 고유 이름입니다.

유형: RestoreTestingSelectionForGet객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetSupportedResourceTypes

서비스: AWS Backup

에서 지원하는 AWS 리소스 유형을 반환합니다 AWS Backup.

Request Syntax

```
GET /supported-resource-types HTTP/1.1
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ResourceTypes

지원되는 AWS 리소스 유형이 포함된 문자열을 포함합니다.

- Amazon Aurora의 `Aurora`
- `CloudFormation`(AWS CloudFormation 일 때)
- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`
- Amazon DynamoDB의 `DynamoDB`
- Amazon Elastic Block Store의 `EBS`

- Amazon Elastic Compute Cloud의 EC2
- Amazon Elastic File System의 EFS
- Amazon FSx의 FSX
- Amazon Neptune의 Neptune
- Amazon Relational Database Service의 RDS
- Amazon Redshift의 Redshift
- SAP HANA on Amazon EC2아마존 엘라스틱 컴퓨트 클라우드 인스턴스의 SAP HANA 데이터베이스용
- S3아마존 심플 스토리지 서비스 (아마존 S3) 용
- Storage Gateway(AWS Storage Gateway 일 때)
- Amazon Timestream의 Timestream
- VirtualMachineVMware 가상 머신의 경우

유형: 문자열 어레이

패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK

- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListBackupJobs

서비스: AWS Backup

지난 30일간 인증된 계정의 기존 백업 작업 목록을 반환합니다. 기간이 더 긴 경우, 이러한 모니터링 도구를 사용하는 방안을 고려해 보세요.

Request Syntax

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByAccountId

작업을 나열할 계정 ID입니다. 지정된 계정 ID와 관련된 백업 작업만 반환합니다.

AWS Organizations 관리 계정에서 사용하는 경우 전달하면 조직 전체의 모든 작업이 * 반환됩니다.

패턴: `^[0-9]{12}$`

ByBackupVaultName

지정된 백업 저장소에 저장될 백업 작업만 반환합니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이후에 완료된 백업 작업만 반환합니다.

ByCompleteBefore

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이전에 완료된 백업 작업만 반환합니다.

ByCreatedAfter

지정된 날짜 이후에 생성된 백업 작업만 반환합니다.

ByCreatedBefore

지정된 날짜 이전에 생성된 백업 작업만 반환합니다.

ByMessageCategory

이는 입력한 값과 일치하는 작업을 필터링하는 데 사용할 수 MessageCategory 있는 선택적 매개 변수입니다.

예시 문자열에는 `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL`, `InvalidParameters` 등이 있습니다.

모니터링 보기

와일드카드 ()는 모든 메시지 범주의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

ByParentJobId

상위 작업 ID를 기준으로 하위(중첩) 작업을 나열하는 필터입니다.

ByResourceArn

지정된 리소스 Amazon 리소스 이름(ARN)과 일치하는 백업 작업만 반환합니다.

ByResourceType

지정된 리소스에 대한 백업 작업만 반환합니다.

- Amazon Aurora의 `Aurora`
- `CloudFormation`(AWS CloudFormation 일 때)
- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`
- Amazon DynamoDB의 `DynamoDB`
- Amazon Elastic Block Store의 `EBS`
- Amazon Elastic Compute Cloud의 `EC2`
- Amazon Elastic File System의 `EFS`
- Amazon FSx의 `FSx`
- Amazon Neptune의 `Neptune`
- Amazon Redshift의 `Redshift`
- Amazon Relational Database Service의 `RDS`
- SAP HANA 데이터베이스용 `SAP HANA on Amazon EC2`
- `Storage Gateway`(AWS Storage Gateway 일 때)
- Amazon S3용 `S3`

- Amazon Timestream의 `Timestream`
- 가상 머신의 `VirtualMachine`

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

지정된 상태에 있는 백업 작업만 반환합니다.

`Completed with issues`는 AWS Backup 콘솔에서만 확인할 수 있는 상태입니다. API의 경우 이 상태는 상태가 `COMPLETED`이고 `MessageCategory` 값이 `SUCCESS`가 아닌 작업을 의미합니다. 즉, 상태는 완료되었지만 상태 메시지가 함께 표시됩니다.

`Completed with issues`에 해당하는 작업 수를 가져오려면 GET 요청 두 개를 실행하고 더 작은 두 번째 수를 뺍니다.

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

유효 값: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupJobs

JSON 형식으로 반환되는 백업 작업에 대한 메타데이터가 들어 있는 구조의 배열입니다.

유형: BackupJob객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListBackupJobSummaries

서비스: AWS Backup

최근 30일 이내에 생성되거나 실행된 백업 작업의 요약에 대한 요청입니다. AccountID, 상태,, ResourceType MessageCategory AggregationPeriod MaxResults, NextToken 또는 매개 변수를 포함하여 결과를 필터링할 수 있습니다.

이 요청은 지역, 계정, 주,,, ResourceType MessageCategory StartTime EndTime, 포함된 작업 수가 포함된 요약을 반환합니다.

Request Syntax

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

AccountId

지정된 계정의 작업 수를 반환합니다.

회원 계정 또는 AWS Organizations에 속하지 않은 계정에서 요청을 보낸 경우 요청자 계정 내의 작업이 반환됩니다.

루트, 관리자 및 위임된 관리자 계정은 ANY 값을 사용하여 조직 내 모든 계정의 작업 수를 반환할 수 있습니다.

AGGREGATE_ALL은 인증된 조직 내 모든 계정의 작업 수를 집계한 다음 합계를 반환합니다.

패턴: ^[0-9]{12}$

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

유효 값: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

반환할 항목의 최대 수입니다.

값은 정수입니다. 허용되는 값 범위는 1에서 500까지입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수를 반환합니다.

허용되는 문자열의 예로는 AccessDenied, Success, InvalidParameters 등이 있습니다. 허용된 MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

AGGREGATE_ALL은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

ResourceType

지정된 리소스 유형에 대한 작업 수를 반환합니다. GetSupportedResourceTypes 요청을 사용하여 지원되는 리소스 유형의 문자열을 가져옵니다.

ANY 값은 모든 리소스 유형의 개수를 반환합니다.

AGGREGATE_ALL은 모든 리소스 유형의 작업 수를 집계하고 그 합계를 반환합니다.

백업할 AWS 리소스 유형 (예: Amazon Elastic Block Store (Amazon EBS) 볼륨 또는 Amazon RDS (아마존 관계형 데이터베이스 서비스) 데이터베이스)

패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

State

이 파라미터는 지정된 상태의 작업 수를 반환합니다.

ANY 값은 모든 상태의 개수를 반환합니다.

AGGREGATE_ALL은 모든 상태의 작업 수를 집계하고 그 합계를 반환합니다.

Completed with issues는 AWS Backup 콘솔에서만 확인할 수 있는 상태입니다. API의 경우 이 상태는 상태가 COMPLETED이고 MessageCategory 값이 SUCCESS가 아닌 작업을 의미합니다. 즉, 상태는 완료되었지만 상태 메시지가 함께 표시됩니다. Completed with issues에 해당하는 작업 수를 가져오려면 GET 요청 두 개를 실행하고 더 작은 두 번째 수를 뺍니다.

/audit/ 받나요? backup-job-summaries AggregationPeriod=14일&상태=완료됨

GET /audit/? backup-job-summaries AggregationPeriod=14일& =성공&상태=완료됨 MessageCategory

유효 값: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

타입: 문자열

BackupJobSummaries

요약 정보.

유형: BackupJobSummary객체 어레이

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListBackupPlans

서비스: AWS Backup

계정의 활성 백업 계획을 나열합니다.

Request Syntax

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

IncludeDeleted

기본값이 FALSE인 부울 값으로, TRUE로 설정되면 삭제된 백업 계획을 반환합니다.

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
         "AdvancedBackupSettings": [
```

```
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlansList

백업 계획에 대한 정보.

유형: BackupPlansListMember객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS 파이썬용 SDK
- AWS 루비 V3용 SDK

ListBackupPlanTemplates

서비스: AWS Backup

백업 계획 템플릿을 나열합니다.

Request Syntax

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 최대 항목 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanTemplatesList

저장된 템플릿에 대한 메타데이터가 들어 있는 템플릿 목록 항목의 배열입니다.

유형: BackupPlanTemplatesListMember객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListBackupPlanVersions

서비스: AWS Backup

Amazon 리소스 이름(ARN), 백업 계획 ID, 생성 및 삭제 날짜, 계획 이름, 버전 ID를 비롯하여, 백업 계획의 버전 메타데이터를 반환합니다.

Request Syntax

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 여부: 예

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupPlanVersionsList": [
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupPlanVersionsList

백업 계획에 대한 메타데이터가 들어 있는 버전 목록 항목의 배열입니다.

유형: BackupPlansListMember객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS 루비 V3용 SDK

ListBackupSelections

서비스: AWS Backup

대상 백업 계획과 관련된 리소스의 메타데이터가 들어 있는 배열을 반환합니다.

Request Syntax

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획을 고유하게 식별합니다.

필수 여부: 예

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "BackupSelectionsList": [
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupSelectionsList

목록에 있는 각 리소스에 대한 메타데이터가 들어 있는 백업 선택 목록 항목의 배열입니다.

유형: BackupSelectionsListMember객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListBackupVaults

서비스: AWS Backup

복구 시점 스토리지 컨테이너 목록 및 이에 대한 정보를 함께 반환합니다.

Request Syntax

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByShared

이 파라미터는 저장소 목록을 공유 저장소별로 정렬합니다.

ByVaultType

이 파라미터는 저장소 목록을 저장소 유형별로 정렬합니다.

유효 값: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultList

Amazon 리소스 이름(ARN), 표시 이름, 생성 날짜, 저장된 복구 시점 수, 암호화 정보(백업 저장소에 저장된 리소스가 암호화된 경우) 등 저장소 메타데이터가 들어 있는 백업 저장소 목록 멤버의 배열입니다.

유형: BackupVaultListMember객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListCopyJobs

서비스: AWS Backup

복사 작업에 대한 메타데이터를 반환합니다.

Request Syntax

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByAccountId

작업을 나열할 계정 ID입니다. 지정된 계정 ID와 관련된 복사 작업만 반환합니다.

패턴: `^[0-9]{12}$`

ByCompleteAfter

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이후에 완료된 복사 작업만 반환합니다.

ByCompleteBefore

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이전에 완료된 복사 작업만 반환합니다.

ByCreatedAfter

지정된 날짜 이후에 생성된 복사 작업만 반환합니다.

ByCreatedBefore

지정된 날짜 이전에 생성된 복사 작업만 반환합니다.

ByDestinationVaultArn

복사하는 위치인 소스 백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

ByMessageCategory

입력한 값과 일치하는 작업을 필터링하는 데 사용할 수 MessageCategory 있는 선택적 매개 변수입니다.

예시 문자열에는 `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL`, `INVALIDPARAMETERS` 등이 있습니다.

모니터링에서 허용되는 문자열 목록을 확인하세요.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

ByParentJobId

상위 작업 ID를 기준으로 하위(중첩) 작업을 나열하는 필터입니다.

ByResourceArn

지정된 리소스 Amazon 리소스 이름(ARN)과 일치하는 복사 작업만 반환합니다.

ByResourceType

지정된 리소스에 대한 백업 작업만 반환합니다.

- Amazon Aurora의 `Aurora`
- `CloudFormation`(AWS CloudFormation 일 때)
- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`
- Amazon DynamoDB의 `DynamoDB`
- Amazon Elastic Block Store의 `EBS`
- Amazon Elastic Compute Cloud의 `EC2`
- Amazon Elastic File System의 `EFS`
- Amazon FSx의 `FSx`
- Amazon Neptune의 `Neptune`
- Amazon Redshift의 `Redshift`
- Amazon Relational Database Service의 `RDS`
- SAP HANA 데이터베이스용 `SAP HANA on Amazon EC2`
- `Storage Gateway`(AWS Storage Gateway 일 때)
- Amazon S3용 `S3`
- Amazon Timestream의 `Timestream`
- 가상 머신의 `VirtualMachine`

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

지정된 상태에 있는 복사 작업만 반환합니다.

유효 값: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, MaxResults 여러 개의 항목을 반환하라는 요청이 있는 경우 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 더 많은 항목을 반환할 수 있습니다. NextToken

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
```

```
            "CreationDate": number,
            "DestinationBackupVaultArn": "string",
            "DestinationRecoveryPointArn": "string",
            "IamRoleArn": "string",
            "IsParent": boolean,
            "MessageCategory": "string",
            "NumberOfChildJobs": number,
            "ParentJobId": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string",
            "SourceBackupVaultArn": "string",
            "SourceRecoveryPointArn": "string",
            "State": "string",
            "StatusMessage": "string"
        }
    ],
    "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CopyJobs

JSON 형식으로 반환되는 복사 작업에 대한 메타데이터가 들어 있는 구조의 배열.

유형: CopyJob객체 어레이

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, MaxResults 여러 개의 항목을 반환해 달라는 요청이 있는 경우 목록에서 다음 토큰이 가리키는 위치부터 시작하여 더 많은 항목을 반품할 수 있습니다. NextToken

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListCopyJobSummaries

서비스: AWS Backup

이 요청은 최근 30일 이내에 생성되거나 실행된 복사 작업의 목록을 가져옵니다. AccountID, 상태,, ResourceType MessageCategory AggregationPeriod MaxResults, NextToken 또는 매개 변수를 포함하여 결과를 필터링할 수 있습니다.

이 요청은 지역, 계정, 주,,, RestourceType MessageCategory StartTime EndTime, 포함된 작업 수가 포함된 요약을 반환합니다.

Request Syntax

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

AccountId

지정된 계정의 작업 수를 반환합니다.

회원 계정 또는 AWS Organizations에 속하지 않은 계정에서 요청을 보낸 경우 요청자 계정 내의 작업이 반환됩니다.

루트, 관리자 및 위임된 관리자 계정은 ANY 값을 사용하여 조직 내 모든 계정의 작업 수를 반환할 수 있습니다.

AGGREGATE_ALL은 인증된 조직 내 모든 계정의 작업 수를 집계한 다음 합계를 반환합니다.

패턴: ^[0-9]{12}$

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

유효 값: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

이 파라미터는 반환할 항목의 최대 수를 설정합니다.

값은 정수입니다. 허용되는 값 범위는 1에서 500까지입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수를 반환합니다.

허용되는 문자열의 예로는 `AccessDenied`, `Success`, `InvalidParameters` 등이 있습니다. 허용된 MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

ResourceType

지정된 리소스 유형에 대한 작업 수를 반환합니다. `GetSupportedResourceTypes` 요청을 사용하여 지원되는 리소스 유형의 문자열을 가져옵니다.

ANY 값은 모든 리소스 유형의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 리소스 유형의 작업 수를 집계하고 그 합계를 반환합니다.

백업할 AWS 리소스 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스).

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

이 파라미터는 지정된 상태의 작업 수를 반환합니다.

ANY 값은 모든 상태의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 상태의 작업 수를 집계하고 그 합계를 반환합니다.

유효 값: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

타입: 문자열

CopyJobSummaries

이 보고서에는 지역, 계정, 주,,, ResourceType MessageCategory StartTime EndTime, 포함된 작업 수가 포함된 요약이 표시됩니다.

유형: CopyJobSummary객체 어레이

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListFrameworks

서비스: AWS Backup

AWS 계정 및 AWS 리전에 대한 모든 프레임워크 목록을 반환합니다.

Request Syntax

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

원하는 결과 수는 1~1,000입니다. 선택 사항입니다. 지정하지 않으면 쿼리는 1MB 데이터를 반환합니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
```

```
            "FrameworkName": "string",
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Frameworks

프레임워크 이름, Amazon Resource Name (ARN), 설명, 제어 개수, 생성 시간, 배포 상태 등 각 프레임워크에 대한 세부 정보가 포함된 프레임워크.

유형: Framework객체 어레이

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListLegalHolds

서비스: AWS Backup

이 작업을 수행하면 활성화된 법적 보존 및 이전의 법적 보존에 대한 메타데이터가 반환됩니다.

Request Syntax

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 리소스 목록 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
         "LegalHoldId": "string",
```

```
            "Status": "string",
            "Title": "string"
        }
    ],
    "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LegalHolds

활성화된 또는 이전의 반환된 법적 보존이 둘 다 들어 있는 배열입니다.

유형: LegalHold객체 어레이

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListProtectedResources

서비스: AWS Backup

리소스가 저장된 시간 AWS Backup, 리소스의 Amazon 리소스 이름 (ARN), 리소스 유형을 포함하여 성공적으로 백업한 리소스 배열을 반환합니다.

Request Syntax

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
```

```
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Results

리소스가 저장된 시간, 리소스의 Amazon 리소스 이름 (ARN), 리소스 유형을 AWS Backup 포함하여 성공적으로 백업된 리소스 배열입니다.

타입: ProtectedResource 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListProtectedResourcesByBackupVault

서비스: AWS Backup

이 요청은 각 백업 저장소에 해당하는 보호된 리소스를 나열합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

계정 ID로 지정한 저장소 내의 백업 저장소별 보호 리소스 목록입니다.

패턴: `^[0-9]{12}$`

backupVaultName

이름별로 지정한 저장소 내 백업 저장소별 보호 리소스 목록.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Results

다음은 요청에 대해 반환된 ListProtectedResourcesByBackupVault 결과입니다.

타입: ProtectedResource 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRecoveryPointsByBackupVault

서비스: AWS Backup

백업 저장소에 저장된 복구 시점에 대한 자세한 정보를 반환합니다.

Request Syntax

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

BackupVaultAccountId

이 파라미터는 계정 ID별로 복구 시점 목록을 정렬합니다.

패턴: `^[0-9]{12}$`

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

> **Note**
> 지원되는 서비스가 백업을 생성할 경우 백업 저장소 이름을 사용하지 못할 수 있습니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

ByBackupPlanId

지정된 백업 계획 ID와 일치하는 복구 시점만 반환합니다.

ByCreatedAfter

지정된 타임스탬프 이후에 생성된 복구 시점만 반환합니다.

ByCreatedBefore

지정된 타임스탬프 이전에 생성된 복구 시점만 반환합니다.

ByParentRecoveryPointArn

이렇게 하면 지정된 상위(복합) 복구 시점 Amazon 리소스 이름(ARN)과 일치하는 복구 시점만 반환합니다.

ByResourceArn

지정된 리소스 Amazon 리소스 이름(ARN)과 일치하는 복구 시점만 반환합니다.

ByResourceType

지정된 리소스 유형과 일치하는 복구 시점만 반환합니다.

- Amazon Aurora의 `Aurora`
- `CloudFormation`(AWS CloudFormation 일 때)
- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`
- Amazon DynamoDB의 `DynamoDB`
- Amazon Elastic Block Store의 `EBS`
- Amazon Elastic Compute Cloud의 `EC2`
- Amazon Elastic File System의 `EFS`
- Amazon FSx의 `FSx`
- Amazon Neptune의 `Neptune`
- Amazon Redshift의 `Redshift`
- Amazon Relational Database Service의 `RDS`
- SAP HANA 데이터베이스용 `SAP HANA on Amazon EC2`
- `Storage Gateway`(AWS Storage Gateway 일 때)
- Amazon S3용 `S3`
- Amazon Timestream의 `Timestream`
- 가상 머신의 `VirtualMachine`

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IamRoleArn": "string",
         "IsEncrypted": boolean,
         "IsParent": boolean,
         "LastRestoreTime": number,
         "Lifecycle": {
            "DeleteAfterDays": number,
            "MoveToColdStorageAfterDays": number,
```

```
            "OptInToArchiveForSupportedResources": boolean
         },
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RecoveryPoints

백업 저장소에 저장된 복구 시점에 대한 세부 정보가 포함된 객체 배열입니다.

타입: RecoveryPointByBackupVault 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRecoveryPointsByLegalHold

서비스: AWS Backup

이 작업은 지정된 법적 보존의 복구 시점 Amazon 리소스 이름(ARN)을 반환합니다.

Request Syntax

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

legalHoldId

법적 보류의 ID.

필수 여부: 예

MaxResults

반환할 리소스 목록 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
```

```
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다.

타입: 문자열

RecoveryPoints

복구 시점.

타입: RecoveryPointMember 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRecoveryPointsByResource

서비스: AWS Backup

리소스 Amazon 리소스 이름 (ARN) 으로 지정된 유형의 복구 지점에 대한 정보.

> **Note**
>
> Amazon EFS 및 Amazon EC2의 경우, 이 작업은 AWS Backup에서 생성한 복구 시점만 나열됩니다.

Request Syntax

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ManagedByAWSBackupOnly

이 속성은 소유권을 기준으로 복구 지점을 필터링합니다.

이 값을 로 TRUE 설정하면 응답에는 에서 관리하는 선택된 리소스와 관련된 복구 지점이 포함됩니다 AWS Backup.

로 FALSE 설정하면 선택한 리소스와 관련된 모든 복구 지점이 응답에 포함됩니다.

타입: 부울

MaxResults

반환할 항목의 최대 수입니다.

> **Note**
>
> Amazon RDS에는 최소 20 이상의 값이 필요합니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

resourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RecoveryPoints

지정된 리소스 유형의 복구 시점에 대한 세부 정보가 포함된 객체 배열입니다.

> **Note**
>
> Amazon EFS와 Amazon EC2 복구 지점만 반환됩니다. BackupVaultName

타입: RecoveryPointByResource 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListReportJobs

서비스: AWS Backup

보고서 작업에 대한 세부 정보를 반환합니다.

Request Syntax

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByCreationAfter

Unix 형식 및 UTC(협정 세계시)로 지정된 날짜 및 시간 이후에 생성된 보고서 작업만 반환합니다. 예를 들어, 1516925490이라는 값은 2018년 1월 26일 금요일 오전 12:11:30을 나타냅니다.

ByCreationBefore

Unix 형식 및 UTC(협정 세계시)로 지정된 날짜 및 시간 이전에 생성된 보고서 작업만 반환합니다. 예를 들어, 1516925490이라는 값은 2018년 1월 26일 금요일 오전 12:11:30을 나타냅니다.

ByReportPlanName

지정된 보고서 계획 이름을 가진 보고서 작업만 반환합니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

지정된 상태에 있는 보고서 작업만 반환합니다. 상태는 다음과 같습니다.

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

원하는 결과 수는 1~1,000입니다. 선택 사항입니다. 지정하지 않으면 쿼리는 1MB 데이터를 반환합니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

타입: 문자열

ReportJobs

JSON 형식의 보고서 작업에 대한 세부 정보입니다.

타입: ReportJob 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListReportPlans

서비스: AWS Backup

보고서 계획 목록을 반환합니다. 단일 보고서 계획에 대한 자세한 내용은 `DescribeReportPlan` 섹션을 참조하세요.

Request Syntax

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

원하는 결과 수는 1~1,000입니다. 선택 사항입니다. 지정하지 않으면 쿼리는 1MB 데이터를 반환합니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
```

```
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

이 작업에 대한 이전 호출에서 반환된 식별자로, 목록의 다음 항목 집합을 반환하는 데 사용할 수 있습니다.

타입: 문자열

ReportPlans

보고서 계획에는 각 계획에 대한 자세한 정보가 포함되어 있습니다. 이 정보에는 Amazon 리소스 이름(ARN), 보고서 계획 이름, 설명, 설정, 전송 채널, 배포 상태, 생성 시간, 보고서 계획을 시도하고 성공적으로 실행한 마지막 시간이 포함됩니다.

타입: ReportPlan 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRestoreJobs

서비스: AWS Backup

복구 프로세스에 대한 세부 정보를 포함하여 저장된 리소스를 복원하기 위해 AWS Backup 시작된 작업 목록을 반환합니다.

Request Syntax

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByAccountId

작업을 나열할 계정 ID입니다. 지정된 계정 ID와 관련된 복원 작업만 반환합니다.

패턴: `^[0-9]{12}$`

ByCompleteAfter

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이후에 완료된 복사 작업만 반환합니다.

ByCompleteBefore

Unix 형식 및 협정 세계시(UTC)로 표시된 날짜 이전에 완료된 복사 작업만 반환합니다.

ByCreatedAfter

지정된 날짜 이후에 생성된 복원 작업만 반환합니다.

ByCreatedBefore

지정된 날짜 이전에 생성된 복원 작업만 반환합니다.

ByResourceType

지정된 리소스에 대한 복원 작업만 반환하려면 다음 파라미터를 포함하세요.

- Amazon Aurora의 `Aurora`
- `CloudFormation`(AWS CloudFormation 일 때)

- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`
- Amazon DynamoDB의 `DynamoDB`
- Amazon Elastic Block Store의 `EBS`
- Amazon Elastic Compute Cloud의 `EC2`
- Amazon Elastic File System의 `EFS`
- Amazon FSx의 `FSx`
- Amazon Neptune의 `Neptune`
- Amazon Redshift의 `Redshift`
- Amazon Relational Database Service의 `RDS`
- SAP HANA 데이터베이스용 `SAP HANA on Amazon EC2`
- `Storage Gateway`(AWS Storage Gateway 일 때)
- Amazon S3용 `S3`
- Amazon Timestream의 `Timestream`
- 가상 머신의 `VirtualMachine`

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

지정된 리소스의 Amazon 리소스 이름(ARN)과 일치하는 복원 테스트 작업만 반환합니다.

ByStatus

지정된 작업 상태와 관련된 복원 작업만 반환합니다.

유효 값: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RestoreJobs

저장된 리소스를 복원하기 위한 작업에 대한 세부 정보가 포함된 객체 배열입니다.

타입: RestoreJobsListMember 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRestoreJobsByProtectedResource

서비스: AWS Backup

지정된 보호된 리소스가 포함되어 있는 복원 작업이 반환됩니다.

`ResourceArn`을 포함해야 합니다. 선택적으로 `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` 및 `ByRecoveryPointCreationDateBefore`를 포함할 수 있습니다.

Request Syntax

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

ByRecoveryPointCreationDateAfter

지정된 날짜 후에 생성된 복구 시점의 복원 작업만 반환합니다.

ByRecoveryPointCreationDateBefore

지정된 날짜 전에 생성된 복구 시점의 복원 작업만 반환합니다.

ByStatus

지정된 작업 상태와 관련된 복원 작업만 반환합니다.

유효 값: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

resourceArn

지정된 리소스의 Amazon 리소스 이름(ARN)과 일치하는 복원 작업만 반환합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RestoreJobs

저장된 리소스를 복원하기 위한 작업에 대한 세부 정보가 포함된 객체 배열입니다.

타입: RestoreJobsListMember 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRestoreJobSummaries

서비스: AWS Backup

이 요청은 최근 30일 이내에 생성되거나 실행된 복원 작업의 요약을 가져옵니다. AccountID, 상태, ResourceType AggregationPeriod MaxResults, NextToken 또는 매개 변수를 포함하여 결과를 필터링할 수 있습니다.

이 요청은 지역, 계정, 주,,, RestourceType MessageCategory StartTime EndTime, 포함된 작업 수가 포함된 요약을 반환합니다.

Request Syntax

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

AccountId

지정된 계정의 작업 수를 반환합니다.

회원 계정 또는 AWS Organizations에 속하지 않은 계정에서 요청을 보낸 경우 요청자 계정 내의 작업이 반환됩니다.

루트, 관리자 및 위임된 관리자 계정은 ANY 값을 사용하여 조직 내 모든 계정의 작업 수를 반환할 수 있습니다.

AGGREGATE_ALL은 인증된 조직 내 모든 계정의 작업 수를 집계한 다음 합계를 반환합니다.

패턴: ^[0-9]{12}$

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

유효 값: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

이 파라미터는 반환할 항목의 최대 수를 설정합니다.

값은 정수입니다. 허용되는 값 범위는 1에서 500까지입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

ResourceType

지정된 리소스 유형에 대한 작업 수를 반환합니다. GetSupportedResourceTypes 요청을 사용하여 지원되는 리소스 유형의 문자열을 가져옵니다.

ANY 값은 모든 리소스 유형의 개수를 반환합니다.

AGGREGATE_ALL은 모든 리소스 유형의 작업 수를 집계하고 그 합계를 반환합니다.

백업할 AWS 리소스 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스).

패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

State

이 파라미터는 지정된 상태의 작업 수를 반환합니다.

ANY 값은 모든 상태의 개수를 반환합니다.

AGGREGATE_ALL은 모든 상태의 작업 수를 집계하고 그 합계를 반환합니다.

유효 값: CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AggregationPeriod

결과가 반환되는 기간.

- ONE_DAY- 이전 14일 동안의 일일 작업 수입니다.
- SEVEN_DAYS- 이전 7일간 집계된 작업 수입니다.
- FOURTEEN_DAYS- 이전 14일 동안 집계된 작업 수입니다.

타입: 문자열

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RestoreJobSummaries

이 보고서에는 지역, 계정, 주,,, ResourceType MessageCategory StartTime EndTime, 포함된 작업 수가 포함된 요약이 포함됩니다.

타입: RestoreJobSummary 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRestoreTestingPlans

서비스: AWS Backup

복원 테스트 계획의 목록을 반환합니다.

Request Syntax

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 nexttoken이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
```

```
            "RestoreTestingPlanName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 nexttoken이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RestoreTestingPlans

반환된 복원 테스트 계획 목록입니다.

타입: RestoreTestingPlanForList 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListRestoreTestingSelections

서비스: AWS Backup

복원 테스트 선택 항목의 목록을 반환합니다. `MaxResults` 및 `RestoreTestingPlanName`을 기준으로 필터링할 수 있습니다.

Request Syntax

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 nexttoken이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

RestoreTestingPlanName

지정된 복원 테스트 계획 이름을 기준으로 복원 테스트 선택 항목을 반환합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 nexttoken이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

RestoreTestingSelections

복원 테스트 계획과 연결된 반환된 복원 테스트 선택 항목입니다.

타입: RestoreTestingSelectionForList 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListTags

서비스: AWS Backup

대상 복구 지점, 백업 계획 또는 백업 저장소와 같이 리소스에 할당된 태그를 반환합니다.

`ListTags`는 백업의 전체 AWS Backup 관리를 지원하는 리소스 유형에만 사용할 수 있습니다. 이러한 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다.

Request Syntax

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

MaxResults

반환할 항목의 최대 수입니다.

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

resourceArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다. `ListTags`의 유효한 대상은 복구 시점, 백업 계획, 백업 저장소입니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 항목의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 항목의 MaxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

타입: 문자열

Tags

태그에 대한 정보.

유형: 문자열-문자열 맵

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutBackupVaultAccessPolicy

서비스: AWS Backup

대상 백업 저장소에 대한 액세스 권한을 관리하는 데 사용되는 리소스 기반 정책을 설정합니다. 백업 저장소 이름과 JSON 형식의 액세스 정책 문서가 필요합니다.

Request Syntax

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

Policy

JSON 형식의 백업 저장소 액세스 정책 문서입니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutBackupVaultLockConfiguration

서비스: AWS Backup

AWS Backup Vault Lock을 백업 저장소에 적용하여 백업 저장소에 저장되거나 생성된 복구 지점을 삭제하려는 시도를 방지합니다. 또한 저장소 잠금은 현재 백업 저장소에 저장된 복구 시점의 보존 기간을 제어하는 수명 주기 정책을 업데이트하려는 시도를 방지합니다. 지정된 경우, 저장소 잠금은 백업 저장소를 대상으로 하는 향후 백업 및 복사 작업에 최소 및 최대 보존 기간을 적용합니다.

> **Note**
>
> AWS Backup 코하셋 어소시에이츠는 SEC 17a-4, CFTC 및 FINRA 규정이 적용되는 환경에서 사용할 수 있는지 Vault Lock을 평가했습니다. AWS Backup Vault Lock이 이러한 규정과 어떤 관련이 있는지에 대한 자세한 내용은 코하셋 어소시에이츠 규정 준수 평가를 참조하십시오.

자세한 내용은 AWS Backup Vault Lock을 참조하세요.

Request Syntax

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

보호하는 백업 저장소의 이름을 지정하는 AWS Backup Vault Lock 구성.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

ChangeableForDays

잠금 날짜까지 남은 일 수를 지정하는 AWS Backup 저장소 잠금 구성입니다. 예를 들어, 2022년 1월 1일 오후 8시 UTC에 ChangeableForDays를 30으로 설정하면 잠금 날짜가 2022년 1월 31일 오후 8시 UTC로 설정됩니다.

AWS Backup 볼트 잠금이 적용되어 변경할 수 없게 되기까지 72시간의 쿨링 오프 기간을 적용합니다. 따라서 ChangeableForDays를 3 이상으로 설정해야 합니다.

잠금 날짜 이전에 DeleteBackupVaultLockConfiguration을 사용하여 저장소에서 저장소 잠금을 삭제하거나 PutBackupVaultLockConfiguration을 사용하여 저장소 잠금 구성을 변경할 수 있습니다. 잠금 날짜 이후에는 저장소 잠금이 변경 불가능 상태가 되고 변경하거나 삭제할 수 없습니다.

이 파라미터가 지정되지 않으면 DeleteBackupVaultLockConfiguration을 사용하여 저장소에서 저장소 잠금을 삭제하거나 언제든지 PutBackupVaultLockConfiguration을 사용하여 저장소 잠금 구성을 변경할 수 있습니다.

유형: Long

필수 여부: 아니요

MaxRetentionDays

AWS Backup 저장소 잠금 구성은 저장소가 복구 지점을 보존하는 최대 보존 기간을 지정합니다. 이 설정은 예를 들어, 조직의 정책에 따라 특정 데이터를 4년(1,460일) 동안 보관한 후 폐기해야 하는 경우에 유용할 수 있습니다.

이 파라미터가 포함되지 않으면 저장소 잠금은 저장소의 복구 시점에 최대 보존 기간을 적용하지 않습니다. 이 파라미터가 값 없이 포함되면 저장소 잠금은 최대 보존 기간을 적용하지 않습니다.

이 파라미터가 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최대 보존 기간보다 짧거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최대 보존 기간보다 길면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 지정할 수 있는 최대 보존 기간은 36,500일(약 100년)입니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 지점은 영향을 받지 않습니다.

유형: Long

필수 여부: 아니요

MinRetentionDays

AWS Backup 저장소 잠금 구성은 저장소가 복구 지점을 보존하는 최소 보존 기간을 지정합니다. 이 설정은 예를 들어, 조직의 정책에 따라 특정 데이터를 7년(2,555일) 이상 유지해야 하는 경우에 유용할 수 있습니다.

이 매개 변수는 저장소 잠금을 만들 때 필요하며 AWS CloudFormation그렇지 않은 경우 이 매개 변수는 선택 사항입니다. 이 파라미터가 지정되지 않으면 저장소 잠금이 최소 보존 기간을 적용하지 않습니다.

이 파라미터가 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최소 보존 기간보다 길거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최소 보존 기간보다 짧으면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 지정할 수 있는 가장 짧은 최소 보존 기간은 1일입니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 지점은 영향을 받지 않습니다.

유형: Long

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutBackupVaultNotifications

서비스: AWS Backup

지정된 주제 및 이벤트에 대한 알림을 백업 저장소에서 켭니다.

Request Syntax

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupVaultEvents

백업 저장소에 리소스를 백업할 작업의 상태를 나타내는 이벤트 어레이입니다.

일반적인 사용 사례 및 코드 샘플은 Amazon SNS를 사용하여 AWS Backup 이벤트 추적을 참조하십시오.

지원되는 이벤트는 다음과 같습니다.

- `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED`
- `COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED`

- RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED
- S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

> **Note**
>
> 아래 목록에는 지원되는 이벤트와 더 이상 사용되지 않는 (참조용) 더 이상 사용되지 않는 이벤트가 모두 포함되어 있습니다. 지원 중단된 이벤트는 상태나 알림을 반환하지 않습니다. 지원되는 이벤트는 위 목록을 참조하십시오.

유형: 문자열 어레이

유효 값: BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

필수 사항 여부: 예

SNSTopicArn

백업 저장소의 이벤트 주제를 지정하는 Amazon 리소스 이름(ARN)입니다(예: arn:aws:sns:us-west-2:111122223333:MyVaultTopic).

타입: 문자열

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutRestoreValidationResult

서비스: AWS Backup

이 요청을 통해 독립적인 자체 실행 복원 테스트 검증 결과를 전송할 수 있습니다. `RestoreJobId` 및 `ValidationStatus`는 필수입니다. 선택적으로 `ValidationStatusMessage`를 입력할 수 있습니다.

Request Syntax

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

restoreJobId

이 식별자는 내 복원 작업의 고유 식별자입니다 AWS Backup.

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

ValidationStatus

복원 검증 상태.

타입: 문자열

유효 값: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

필수 사항 여부: 예

ValidationStatusMessage

복원 테스트 검증의 검증 상태를 설명하기 위해 입력할 수 있는 선택적 메시지 문자열입니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 204
```

Response Elements

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StartBackupJob

서비스: AWS Backup

지정한 리소스에 대한 온디맨드 백업 작업을 시작합니다.

Request Syntax

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupOptions

선택한 리소스의 백업 옵션입니다. 이 옵션은 Windows VSS(Volume Shadow Copy Service) 백업 작업에만 사용할 수 있습니다.

유효한 값: `WindowsVSS` 백업 옵션을 활성화하고 Windows VSS 백업을 생성하려면 `"WindowsVSS":"enabled"`로 설정합니다. 정기 백업을 생성하려면 `"WindowsVSS""disabled"`로 설정합니다. `WindowsVSS` 옵션은 기본적으로 활성화되어 있습니다.

유형: String 간 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

값 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

CompleteWindowMinutes

성공적으로 시작된 백업을 완료해야 하는 기간(분)입니다. 완료하지 않으면 AWS Backup 이 작업을 취소합니다. 이 값은 선택 사항입니다. 이 값은 백업이 예약된 시점부터 감소되기 시작합니다. 백업이 일정보다 늦게 시작된 경우에도 `StartWindowMinutes`에 대한 추가 시간이 추가되지 않습니다.

`StartWindowMinutes`와 마찬가지로, 이 파라미터의 최대값은 100년(52,560,000분)입니다.

유형: Long

필수 여부: 아니요

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수 항목 여부: 예

IdempotencyToken

고객이 선택한 문자열로, StartBackupJob에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

이 파라미터의 최대값은 100년(36,500일)입니다.

유형: Lifecycle객체

필수 항목 여부: 아니요

RecoveryPointTags

리소스에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

ResourceArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

필수 항목 여부: 예

StartWindowMinutes

백업이 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(분)입니다. 이 값은 선택 사항이며, 기본값은 8시간입니다. 이 값이 포함된 경우 오류를 방지하려면 60분 이상이어야 합니다.

이 파라미터의 최대값은 100년(52,560,000분)입니다.

시작 기간 동안에는 백업 작업이 성공적으로 시작되거나 시작 기간이 만료될 때까지 백업 작업 상태가 CREATED 상태로 유지됩니다. 시작 시간 AWS Backup 내에 작업을 재시도할 수 있는 오류가 발생하면 백업이 성공적으로 시작 (작업 상태가 로 변경RUNNING) 되거나 작업 상태가 로 변경될 때까지 (시작 시간이 끝나면 발생할 것으로 예상됨) 최소 10분마다 AWS Backup 자동으로 작업을 다시 시도합니다. EXPIRED

유형: Long

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupJobId

리소스 백업 요청을 고유하게 AWS Backup 식별합니다.

타입: 문자열

CreationDate

백업 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

IsParent

상위(복합) 백업 작업이라는 것을 나타내는 반환된 부울 값입니다.

타입: 부울

RecoveryPointArn

참고: 이 필드는 Amazon EFS 및 고급 DynamoDB 리소스에 대해서만 반환됩니다.

복구 시점을 고유하게 식별하는 ARN입니다(예: arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45).

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StartCopyJob

서비스: AWS Backup

지정된 리소스의 일회성 복사본을 생성하는 작업을 시작합니다.

연속 백업은 지원하지 않습니다.

Request Syntax

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

DestinationBackupVaultArn

복사할 위치인 대상 백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

필수 항목 여부: 예

IamRoleArn

대상 복구 시점을 복사하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수 항목 여부: 예

IdempotencyToken

고객이 선택한 문자열로, `StartCopyJob`에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

Lifecycle

복구 지점이 콜드 스토리지로 전환되거나 삭제되기까지의 기간 (일) 을 지정합니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 콘솔의 보존 설정은 며칠 후 콜드 전환으로의 전환보다 90일 더 커야 합니다. 백업이 콜드 백업으로 전환된 후에는 [며칠 후 콜드] 로의 전환 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

기존 수명 주기 및 보존 기간을 제거하고 복구 지점을 무기한으로 유지하려면 및 에 `MoveToColdStorageAfterDays` -1을 지정하십시오. `DeleteAfterDays`

유형: Lifecycle객체

필수 항목 여부: 아니요

RecoveryPointArn

복사 작업에 사용할 복구 시점을 고유하게 식별하는 ARN입니다(예: arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45).

타입: 문자열

필수 항목 여부: 예

SourceBackupVaultName

백업이 저장되는 논리적 소스 컨테이너의 이름입니다. Backup Vault는 생성에 사용된 계정 및 저장소가 생성된 AWS 지역의 고유한 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CopyJobId

복사 작업을 고유하게 식별합니다.

타입: 문자열

CreationDate

복사 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

IsParent

상위(복합) 복사 작업이라는 것을 나타내는 반환된 부울 값입니다.

타입: 부울

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StartReportJob

서비스: AWS Backup

지정된 보고서 계획에 대한 온디맨드 보고서 작업을 시작합니다.

Request Syntax

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

reportPlanName

보고서 계획의 고유 이름입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

IdempotencyToken

고객이 선택한 문자열로, `StartReportJobInput`에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ReportJobId

보고서 작업의 식별자입니다. 임의로 생성되는 최대 1,024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 보고서 작업 ID는 편집할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StartRestoreJob

서비스: AWS Backup

Amazon 리소스 이름(ARN)으로 식별되는 저장된 리소스를 복구합니다.

Request Syntax

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

CopySourceTagsToRestoredResource

이는 선택 가능한 파라미터입니다. 이 파라미터가 `True`이면, 백업에 포함된 태그가 복원된 리소스에 복사됩니다.

를 통해 생성된 백업에만 적용할 수 AWS Backup있습니다.

타입: 부울

필수 항목 여부: 아니요

IamRoleArn

대상 리소스를 생성하는 데 AWS Backup 사용하는 IAM 역할의 Amazon 리소스 이름 (ARN). 예:. `arn:aws:iam::123456789012:role/S3Access`

타입: 문자열

필수사항: 아니요

IdempotencyToken

고객이 선택한 문자열로, StartRestoreJob에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

Metadata

메타데이터 키-값 페어의 집합입니다.

GetRecoveryPointRestoreMetadata를 호출하여 백업했던 당시의 리소스에 대한 구성 메타데이터를 가져올 수 있습니다. 하지만 리소스를 복원하려면 GetRecoveryPointRestoreMetadata에서 제공한 값 외에 다른 값이 필요할 수 있습니다. 예를 들어, 원본이 이미 있는 경우 새 리소스 이름을 제공해야 할 수 있습니다.

각 리소스의 메타데이터에 대한 자세한 내용은 다음을 참조하십시오.

- Amazon Aurora용 메타데이터
- 아마존 DocumentDB용 메타데이터
- 에 대한 메타데이터 AWS CloudFormation
- Amazon DynamoDB용 메타데이터
- 아마존 EBS용 메타데이터
- Amazon EC2용 메타데이터
- Amazon EFS용 메타데이터
- 아마존 FSx용 메타데이터
- Amazon Neptune용 메타데이터
- Amazon RDS용 메타데이터
- 아마존 Redshift용 메타데이터
- 에 대한 메타데이터 AWS Storage Gateway
- Amazon S3용 메타데이터
- Amazon Timestream용 메타데이터

- 가상 머신의 메타데이터

유형: 문자열-문자열 맵

필수 여부: 예

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

필수 항목 여부: 예

ResourceType

다음 리소스 중 하나에 대한 복구 시점을 복원하는 작업을 시작합니다.

- `Aurora`- 아마존 Aurora
- `DocumentDB`- 아마존 DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- 아마존 다이나모DB
- `EBS`- 아마존 엘라스틱 블록 스토어
- `EC2`- 아마존 엘라스틱 컴퓨트 클라우드
- `EFS`- 아마존 Elastic File System
- `FSx`- 아마존 FSx
- `Neptune`- 아마존 넵튠
- `RDS`- 아마존 관계형 데이터베이스 서비스
- `Redshift`- 아마존 레드시프트
- `Storage Gateway` - AWS Storage Gateway
- `S3`- Amazon 심플 스토리지 서비스
- `Timestream`- 아마존 타임스트림
- `VirtualMachine`- 가상 머신

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

RestoreJobId

복구 시점을 복원하는 작업을 고유하게 식별합니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StopBackupJob

서비스: AWS Backup

리소스의 일회성 백업을 생성하는 작업을 취소하려고 시도합니다.

이 작업은 다음 서비스에서는 지원되지 않습니다. Windows File Server용 Amazon FSx, Lustre용 Amazon FSx, ONTAP용 Amazon FSx, OpenZFS용 Amazon FSX, NetApp Amazon DocumentDB (MongoDB 호환 가능), 아마존 RDS, 아마존 오로라 Aurora와 Amazon Neptune.

Request Syntax

```
POST /backup-jobs/backupJobId HTTP/1.1
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupJobId

리소스 백업 AWS Backup 요청을 고유하게 식별합니다.

필수 사항 여부: Yes

Request Body

해당 요청에는 본문이 없습니다.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

TagResource

서비스: AWS Backup

Amazon 리소스 이름(ARN)으로 식별되는 복구 시점, 백업 계획 또는 백업 저장소에 키-값 페어 집합을 할당합니다.

이 API는 Aurora, Amazon DocumentDB를 비롯한 리소스 유형의 복구 지점에 지원됩니다. 아마존 EBS, 아마존 FSx, 넵튠, 아마존 RDS

Request Syntax

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

resourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 태그가 지정된 리소스 유형에 따라 달라집니다.

포함되지 않은 ARN은 태깅과 호환되지 않습니다. backup TagResourceUntagResourceARN이 유효하지 않으면 오류가 발생합니다. 허용되는 ARN 콘텐츠에는 다음이 포함될 수 있습니다. `arn:aws:backup:us-east` 잘못된 ARN 콘텐츠는 다음과 같이 보일 수 있습니다. `arn:aws:ec2:us-east`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

Tags

리소스를 구성하는 데 사용되는 키-값 페어입니다. 생성하는 리소스에 고유한 메타데이터를 할당할 수 있습니다. 명확하게 설명하자면, 태그를 할당하는 구조는 아래와 같습니다.

유형: 문자열-문자열 맵

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UntagResource

서비스: AWS Backup

Amazon 리소스 이름(ARN)으로 식별되는 복구 시점, 백업 계획 또는 백업 저장소에서 키-값 페어 집합을 제거합니다.

Aurora, Amazon DocumentDB를 비롯한 리소스 유형의 복구 지점에는 이 API가 지원되지 않습니다. 아마존 EBS, 아마존 FSx, 넵튠, 아마존 RDS

Request Syntax

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

resourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 태그가 지정된 리소스 유형에 따라 달라집니다.

포함되지 않은 ARN은 태깅과 호환되지 않습니다. backup TagResourceUntagResourceARN이 유효하지 않으면 오류가 발생합니다. 허용되는 ARN 콘텐츠에는 다음이 포함될 수 있습니다. `arn:aws:backup:us-east` 잘못된 ARN 콘텐츠는 다음과 같이 보일 수 있습니다. `arn:aws:ec2:us-east`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

TagKeyList

리소스에서 제거할 키-값 태그를 식별하는 키입니다.

유형: 문자열 어레이

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateBackupPlan

서비스: AWS Backup

지정된 백업 계획을 업데이트합니다. 새 버전은 해당 ID로 고유하게 식별됩니다.

Request Syntax

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
```

```
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupPlanId

백업 계획의 ID.

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

BackupPlan

백업 계획의 본문. BackupPlanName과 하나 이상의 Rules 집합을 포함합니다.

유형: BackupPlanInput객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
```

```
            "ResourceType": "string"
        }
    ],
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "CreationDate": number,
    "VersionId": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AdvancedBackupSettings

각 리소스 유형에 대한 BackupOptions 목록이 포함됩니다.

유형: AdvancedBackupSetting객체 어레이

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50)입니다.

타입: 문자열

BackupPlanId

백업 계획을 고유하게 식별합니다.

타입: 문자열

CreationDate

백업 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateFramework

서비스: AWS Backup

지정된 프레임워크를 업데이트합니다.

Request Syntax

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

frameworkName

프레임워크의 고유 이름입니다. 이 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자 사이입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

FrameworkControls

프레임워크를 구성하는 컨트롤. 목록의 각 컨트롤에는 이름, 입력 파라미터, 범위가 있습니다.

타입: FrameworkControl객체 배열

필수: 아니요

FrameworkDescription

프레임워크에 대한 최대 1,024자의 설명(선택 사항)입니다.

유형: String

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

IdempotencyToken

고객이 선택한 문자열로, `UpdateFrameworkInput`에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
```

```
    "CreationTime": number,
    "FrameworkArn": "string",
    "FrameworkName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

프레임워크가 생성된 날짜 및 시간이며, ISO 8601 형식으로 표시됩니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 2020-07-10T15:00:00.000-08:00은 UTC보다 8시간 늦은 2020년 7월 10일 오후 3시를 나타냅니다.

유형: 타임스탬프

FrameworkArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

타입: 문자열

FrameworkName

프레임워크의 고유 이름입니다. 이 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자 사이입니다.

유형: String

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AlreadyExistsException

필수 리소스가 이미 존재합니다.

HTTP 상태 코드: 400

ConflictException

AWS Backup 이전 작업의 수행을 완료할 때까지는 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

LimitExceededException

요청의 한도가 초과되었습니다(예: 요청에 허용되는 최대 항목 수).

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateGlobalSettings

서비스: AWS Backup

계정이 교차 AWS 계정 백업을 선택했는지 여부를 업데이트합니다. 계정이 Organizations 관리 계정이 아닌 경우 오류가 반환됩니다. `DescribeGlobalSettings` API를 사용하여 현재 설정을 확인하세요.

Request Syntax

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

GlobalSettings

`isCrossAccountBackupEnabled` 및 리전에 대한 값입니다. 예: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

유형: 문자열 간 맵

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS 루비 V3용 SDK

UpdateRecoveryPointLifecycle

서비스: AWS Backup

복구 시점의 전환 수명 주기를 설정합니다.

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

이 작업은 연속 백업을 지원하지 않습니다.

Request Syntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

backupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

recoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

유형: Lifecycle객체

필수 항목 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
```

```
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BackupVaultArn

백업 저장소를 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

CalculatedLifecycle

`DeleteAt` 및 `MoveToColdStorageAt` 타임스탬프를 포함하는 `CalculatedLifecycle` 객체입니다.

유형: CalculatedLifecycle객체

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

유형: Lifecycle객체

RecoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

InvalidRequestException

요청에 대한 입력에 문제가 있음을 나타냅니다. 예를 들어, 파라미터의 유형이 잘못된 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS 파이썬용 SDK
- AWS 루비 V3용 SDK

UpdateRegionSettings

서비스: AWS Backup

리전에 대한 현재 서비스 옵트인 설정을 업데이트합니다.

`DescribeRegionSettings` API를 사용하여 지원되는 리소스 유형을 확인하세요.

Request Syntax

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceTypeManagementPreference

리소스 유형에 대한 백업의 전체 AWS Backup 관리를 활성화하거나 비활성화합니다. 고급 DynamoDB 백업 기능과 함께AWS Backup DynamoDB에 대한 전체 AWS Backup 관리를 활성화하려면 절차에 따라 고급 DynamoDB 백업을 프로그래밍 방식으로 활성화하십시오.

유형: String과 부울 간의 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

ResourceTypeOptInPreference

리전의 옵트인 기본 설정과 함께 서비스 목록을 업데이트합니다.

태그만 기준으로 하여 리소스를 할당할 경우 서비스 옵트인 설정이 적용됩니다. Amazon S3, Amazon EC2 또는 Amazon RDS 같은 백업 계획에 리소스 유형이 명시적으로 할당된 경우, 이러한 특정 서비스에 대한 옵트인이 활성화되지 않아도 백업에 포함됩니다. 리소스 할당에 리소스 유형과 태그가 둘 다 지정된 경우, 백업 계획에 지정된 리소스 유형이 태그 조건보다 우선합니다. 이 경우 서비스 옵트인 설정이 무시됩니다.

유형: String과 부울 간의 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오. AWS

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateReportPlan

서비스: AWS Backup

지정된 보고서 계획을 업데이트합니다.

Request Syntax

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

reportPlanName

보고서 계획의 고유 이름입니다. 이 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자 사이입니다.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

IdempotencyToken

고객이 선택한 문자열로, UpdateReportPlanInput에 대한 동일한 호출을 구분하는 데 사용할 수 있습니다. 동일한 멱등성 토큰으로 성공적인 요청을 다시 시도하면 아무런 작업 없이 성공 메시지가 표시됩니다.

타입: 문자열

필수사항: 아니요

ReportDeliveryChannel

보고서를 전송할 위치에 대한 정보, 특히 Amazon S3 버킷 이름, S3 키 접두사 및 보고서 형식.

유형: ReportDeliveryChannel객체

필수 항목 여부: 아니요

ReportPlanDescription

보고서 계획에 대한 최대 1,024자의 설명(선택 사항)입니다.

유형: String

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

ReportSetting

보고서의 보고서 템플릿입니다. 보고서는 보고서 템플릿을 사용하여 작성됩니다. 보고서 템플릿은 다음과 같습니다.

```
RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT
```

보고서 템플릿이 RESOURCE_COMPLIANCE_REPORT CONTROL_COMPLIANCE_REPORT OR인 경우 이 API 리소스는 AWS 리전 및 프레임워크의 보고서 적용 범위도 설명합니다.

유형: ReportSetting객체

필수 항목 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

보고서 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationTime의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

ReportPlanArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

ReportPlanName

보고서 계획의 고유 이름입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

AWS Backup 이전 작업의 수행이 완료될 때까지는 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateRestoreTestingPlan

서비스: AWS Backup

이 요청은 지정된 복원 테스트 계획의 변경 내용을 전송합니다. 생성 후에는 `RestoreTestingPlanName`을 업데이트할 수 없습니다.

`RecoveryPointSelection`에는 다음을 포함할 수 있습니다.

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Request Syntax

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

복원 테스트 계획의 이름

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

RestoreTestingPlan

복원 테스트 계획의 본문을 지정합니다.

유형: RestoreTestingPlanForUpdate객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

리소스 테스트 계획이 생성된 시간.

유형: 타임스탬프

RestoreTestingPlanArn

복원 테스트 계획의 고유 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

RestoreTestingPlanName

생성한 후에는 이름을 변경할 수 없습니다. 이름은 영숫자와 밑줄로만 구성해야 합니다. 최대 길이는 50자입니다.

타입: 문자열

UpdateTime

복원 테스트 계획의 업데이트가 완료된 시간입니다.

유형: 타임스탬프

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

AWS Backup 이전 작업의 수행이 완료될 때까지는 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateRestoreTestingSelection

서비스: AWS Backup

지정된 복원 테스트 선택 항목을 업데이트합니다.

`RestoreTestingSelectionName`을 제외한 대부분의 요소를 이 요청으로 업데이트할 수 있습니다.

보호된 리소스 ARN 또는 조건 중 하나를 사용할 수 있지만 둘 다 사용할 수는 없습니다.

Request Syntax

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

URI 요청 파라미터

요청은 다음 URI 파라미터를 사용합니다.

RestoreTestingPlanName

표시된 테스트 계획을 업데이트하려면 복원 테스트 계획 이름이 필요합니다.

필수 여부: 예

RestoreTestingSelectionName

업데이트하려는 복원 테스트 선택 항목의 필수 복원 테스트 선택 이름입니다.

필수 사항 여부: Yes

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

RestoreTestingSelection

복원 테스트 선택 항목을 업데이트하려면 보호된 리소스 ARN 또는 조건을 사용할 수 있지만 둘 다 사용할 수는 없습니다. 즉, 선택 항목에 `ProtectedResourceArns`가 포함된 경우 `ProtectedResourceConditions` 파라미터를 사용한 업데이트 요청은 실패합니다.

유형: RestoreTestingSelectionForUpdate객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

리소스 테스트 선택이 성공적으로 업데이트된 시간입니다.

유형: 타임스탬프

RestoreTestingPlanArn

복원 테스트 계획의 이름을 나타내는 고유한 문자열입니다.

타입: 문자열

RestoreTestingPlanName

업데이트된 복원 테스트 선택과 관련된 복원 테스트 계획입니다.

타입: 문자열

RestoreTestingSelectionName

반환된 복원 테스트 선택 이름.

타입: 문자열

UpdateTime

복원 테스트 선택 항목에 대한 업데이트가 완료된 시간입니다.

유형: 타임스탬프

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

AWS Backup 이전 작업의 수행을 완료할 때까지는 요청한 작업을 수행할 수 없습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 400

InvalidParameterValueException

파라미터의 값에 문제가 있음을 나타냅니다. 예를 들어 값이 범위를 벗어난 경우가 이에 해당합니다.

HTTP 상태 코드: 400

MissingParameterValueException

필수 파라미터가 누락되었음을 나타냅니다.

HTTP 상태 코드: 400

ResourceNotFoundException

작업에 필요한 리소스가 존재하지 않습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

요청이 서버의 일시적 장애 때문에 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

AWS Backup gateway

다음 작업이 AWS Backup gateway에서 지원됩니다.

- AssociateGatewayToServer
- CreateGateway

- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

서비스: AWS Backup gateway

백업 게이트웨이를 서버와 연결합니다. 연결 프로세스를 완료한 후 게이트웨이를 통해 VM을 백업 및 복원할 수 있습니다.

구문 요청

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. `ListGateways`작업을 사용하여 계정 및 AWS 리전에 대한 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수: 예

ServerArn

가상 머신을 호스팅하는 서버의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

CreateGateway

서비스: AWS Backup gateway

백업 게이트웨이를 생성합니다. 게이트웨이를 생성한 후에는 `AssociateGatewayToServer` 작업을 사용하여 게이트웨이를 서버와 연결할 수 있습니다.

구문 요청

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ActivationKey

생성된 게이트웨이의 활성화 키입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

패턴: `^[0-9a-zA-Z\-]+$`

필수 사항 여부: Yes

GatewayDisplayName

생성된 게이트웨이의 표시 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

필수 사항 여부: Yes

GatewayType

생성된 게이트웨이 유형입니다.

타입: 문자열

유효 값: `BACKUP_VM`

필수 사항 여부: 예

Tags

게이트웨이에 할당할 최대 50개의 태그 목록입니다. 각 태그는 키-값 페어입니다.

타입: Tag객체 배열

필수: 아니요

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

생성하는 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteGateway

서비스: AWS Backup gateway

백업 게이트웨이를 삭제합니다.

구문 요청

```
{
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

삭제할 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

삭제한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DeleteHypervisor

서비스: AWS Backup gateway

하이퍼바이저를 삭제합니다.

구문 요청

```
{
   "HypervisorArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

삭제할 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "HypervisorArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

삭제한 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

권한이 부족하여 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

DisassociateGatewayFromServer

서비스: AWS Backup gateway

지정된 서버에서 백업 게이트웨이의 연결을 해제합니다. 연결 해제 프로세스가 끝나면 게이트웨이는 더 이상 서버의 가상 머신에 액세스할 수 없습니다.

구문 요청

```
{
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

연결 해제할 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

연결 해제한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetBandwidthRateLimitSchedule

서비스: AWS Backup gateway

지정된 게이트웨이의 대역폭 속도 제한 일정을 검색합니다. 기본적으로 게이트웨이에는 대역폭 속도 제한 일정이 없으므로, 대역폭 속도 제한이 적용되지 않습니다. 이를 사용하여 게이트웨이의 대역폭 속도 제한 일정을 가져올 수 있습니다.

구문 요청

```
{
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. ListGateways작업을 사용하여 계정 및 AWS 리전에 대한 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
```

```
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
         }
      ],
      "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BandwidthRateLimitIntervals

게이트웨이의 대역폭 속도 제한 일정 간격이 포함된 배열입니다. 대역폭 속도 제한 간격이 예약되지 않은 경우, 배열은 비어 있습니다.

유형: BandwidthRateLimitInterval객체 어레이

배열 항목: 최소 항목 수는 0개. 최대 항목 수는 20개.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. ListGateways작업을 사용하여 계정 및 AWS 리전의 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetGateway

서비스: AWS Backup gateway

이 API는 Amazon 리소스 이름(ARN)을 제공하여 게이트웨이를 반환합니다.

구문 요청

```
{
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
         "DayOfWeek": number,
```

```
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Gateway

이 API는 Amazon 리소스 이름(ARN)을 제공하여 게이트웨이를 반환합니다.

유형: GatewayDetails객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetHypervisor

서비스: AWS Backup gateway

이 작업은 게이트웨이가 연결할 지정된 하이퍼바이저에 대한 정보를 요청합니다. 하이퍼바이저는 가상 머신을 생성 및 관리하고, 가상 머신에 리소스를 할당하는 하드웨어, 소프트웨어 또는 펌웨어입니다.

구문 요청

```
{
   "HypervisorArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
```

```
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Hypervisor

요청한 하이퍼바이저에 대한 세부 정보입니다.

유형: HypervisorDetails객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetHypervisorPropertyMappings

서비스: AWS Backup gateway

이 작업은 지정된 하이퍼바이저의 속성 매핑을 검색합니다. 하이퍼바이저 속성 매핑은 하이퍼바이저에서 사용 가능한 개체 속성과 에서 사용 가능한 속성 간의 관계를 표시합니다. AWS

구문 요청

```
{
   "HypervisorArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
```

```
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

IAM 역할의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

AWS 태그에 대한 VMware 태그의 매핑을 표시합니다.

타입: VmwareToAwsTagMapping 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

GetVirtualMachine

서비스: AWS Backup gateway

이 API는 Amazon 리소스 이름(ARN)을 제공하여 가상 머신을 반환합니다.

구문 요청

```
{
   "ResourceArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceArn

가상 머신의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

VirtualMachine

이 객체에는 GetVirtualMachine 출력에 의해 포함된 VirtualMachine의 기본 속성이 들어 있습니다.

유형: VirtualMachineDetails객체

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ImportHypervisorConfiguration

서비스: AWS Backup gateway

하이퍼바이저의 구성을 가져와서 하이퍼바이저에 연결합니다.

구문 요청

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Host

하이퍼바이저의 서버 호스트입니다. 이는 IP 주소 또는 정규화된 도메인 이름(FQDN)일 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 128.

패턴: `^.+$`

필수 사항 여부: Yes

KmsKeyArn

AWS Key Management Service 하이퍼바이저용입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Required: No

Name

하이퍼바이저의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

필수 사항 여부: Yes

Password

하이퍼바이저의 암호입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[ -~]+$`

Required: No

Tags

가져오려는 하이퍼바이저 구성의 태그입니다.

타입: Tag객체 배열

필수: 아니요

Username

하이퍼바이저의 사용자 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

필수 여부: 아니요

응답 구문

```
{
   "HypervisorArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

연결 해제한 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

권한이 부족하여 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListGateways

서비스: AWS Backup gateway

inan이 소유한 백업 게이트웨이를 AWS 계정 나열합니다. AWS 리전반환되는 목록은 게이트웨이 ARN(Amazon 리소스 이름) 순으로 반환됩니다.

구문 요청

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MaxResults

나열할 최대 게이트웨이 수입니다.

타입: 정수

유효 범위: 최소값 1.

필수 여부: 아니요

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `MaxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: `^.+$`

필수 여부: 아니요

응답 구문

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Gateways

게이트웨이 목록입니다.

유형: Gateway객체 어레이

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 maxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: ^.+$

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListHypervisors

서비스: AWS Backup gateway

하이퍼바이저를 나열합니다.

구문 요청

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MaxResults

나열할 최대 하이퍼바이저 수입니다.

타입: 정수

유효 범위: 최소값 1.

필수 여부: 아니요

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 `maxResults` 수를 반환하기 위한 요청을 한 경우, `NextToken`을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: `^.+$`

필수 여부: 아니요

응답 구문

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Hypervisors

Amazon 리소스 이름(ARN) 순으로 정렬된 Hypervisor 객체 목록입니다.

유형: Hypervisor객체 어레이

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 maxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: ^.+$

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListTagsForResource

서비스: AWS Backup gateway

Amazon 리소스 이름(ARN)을 기준으로 식별되는 리소스에 적용된 태그를 나열합니다.

구문 요청

```
{
   "ResourceArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceArn

나열할 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ResourceArn

나열한 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

리소스의 태그 목록입니다.

타입: Tag 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

ListVirtualMachines

서비스: AWS Backup gateway

가상 머신을 나열합니다.

구문 요청

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

가상 머신에 연결된 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

MaxResults

나열할 최대 가상 머신 수입니다.

타입: 정수

유효 범위: 최소값 1.

필수 여부: 아니요

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 maxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: ^.+$

필수 여부: 아니요

응답 구문

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환된 리소스의 일부 목록 다음에 나오는 다음 항목입니다. 예를 들어, 리소스의 maxResults 수를 반환하기 위한 요청을 한 경우, NextToken을 사용하면 다음 토큰이 가리키는 위치에서 시작하여 목록에 있는 추가 항목을 반환할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 1,000입니다.

패턴: `^.+$`

VirtualMachines

Amazon 리소스 이름(ARN) 순으로 정렬된 `VirtualMachine` 객체 목록입니다.

타입: VirtualMachine 객체 배열

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK

- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutBandwidthRateLimitSchedule

서비스: AWS Backup gateway

이 작업은 지정된 게이트웨이의 대역폭 속도 제한 일정을 설정합니다. 기본적으로 게이트웨이에는 대역폭 속도 제한 일정이 없으므로, 대역폭 속도 제한이 적용되지 않습니다. 이를 사용하여 게이트웨이의 대역폭 속도 제한 일정을 시작할 수 있습니다.

구문 요청

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

BandwidthRateLimitIntervals

게이트웨이의 대역폭 속도 제한 일정 간격이 포함된 배열입니다. 대역폭 속도 제한 간격이 예약되지 않은 경우, 배열은 비어 있습니다.

유형: BandwidthRateLimitInterval객체 어레이

배열 항목: 최소 항목 수는 0개. 최대 항목 수는 20개.

필수 여부: 예

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. ListGateways작업을 사용하여 계정 및 AWS 리전에 대한 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. ListGateways작업을 사용하여 계정 및 AWS 리전의 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutHypervisorPropertyMappings

서비스: AWS Backup gateway

이 작업은 지정된 하이퍼바이저의 속성 매핑을 설정합니다. 하이퍼바이저 속성 매핑은 하이퍼바이저에서 사용 가능한 개체 속성과 에서 사용 가능한 속성 간의 관계를 표시합니다. AWS

구문 요청

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

IamRoleArn

IAM 역할의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

필수 사항 여부: Yes

VmwareToAwsTagMappings

이 작업은 AWS 태그에 대한 VMware 태그의 매핑을 요청합니다.

유형: VmwareToAwsTagMapping객체 어레이

필수 여부: 예

응답 구문

```
{
   "HypervisorArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

권한이 부족하여 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK

- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

PutMaintenanceStartTime

서비스: AWS Backup gateway

게이트웨이의 유지 관리 시작 시간을 설정합니다.

구문 요청

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

DayOfMonth

게이트웨이의 유지 관리를 시작하는 날짜입니다.

사용할 수 있는 값은 Sunday~Saturday입니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 31입니다.

필수 여부: 아니요

DayOfWeek

게이트웨이의 유지 관리를 시작하는 요일입니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 6입니다.

필수 여부: 아니요

GatewayArn

유지 관리 시작 시간을 지정하는 데 사용되는 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

HourOfDay

게이트웨이의 유지 관리를 시작하는 시각입니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 23입니다.

필수 여부: 예

MinuteOfHour

게이트웨이의 유지 관리를 시작하는 시간(분)입니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 59입니다.

필수 여부: 예

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

유지 관리 시작 시간을 설정한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

StartVirtualMachinesMetadataSync

서비스: AWS Backup gateway

이 작업은 지정된 가상 머신 전체에서 메타데이터를 동기화하라는 요청을 보냅니다.

구문 요청

```
{
   "HypervisorArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
   "HypervisorArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

권한이 부족하여 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

TagResource

서비스: AWS Backup gateway

리소스에 태그를 지정합니다.

구문 요청

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceARN

태그를 지정할 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

Tags

리소스에 할당할 태그 목록입니다.

유형: Tag객체 어레이

필수 여부: 예

응답 구문

```
{
   "ResourceARN": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ResourceARN

태그를 지정한 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

TestHypervisorConfiguration

서비스: AWS Backup gateway

하이퍼바이저 구성을 테스트하여 백업 게이트웨이가 하이퍼바이저 및 해당 리소스와 연결할 수 있는지 확인합니다.

구문 요청

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

테스트할 하이퍼바이저에 대한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

Host

하이퍼바이저의 서버 호스트입니다. 이는 IP 주소 또는 정규화된 도메인 이름(FQDN)일 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 128.

패턴: ^.+$

필수 사항 여부: Yes

Password

하이퍼바이저의 암호입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: ^[-~]+$

Required: No

Username

하이퍼바이저의 사용자 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: ^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

필수 여부: 아니요

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UntagResource

서비스: AWS Backup gateway

리소스에서 태그를 제거합니다.

구문 요청

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceARN

태그를 제거할 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

TagKeys

제거할 태그를 지정하는 태그 키 목록입니다.

유형: 문자열 어레이

길이 제약: 최소 길이 1. 최대 길이 128.

패턴: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

필수 항목 여부: 예

응답 구문

```
{
   "ResourceARN": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ResourceARN

태그를 제거한 리소스의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateGatewayInformation

서비스: AWS Backup gateway

게이트웨이의 이름을 업데이트합니다. 요청 시 게이트웨이의 Amazon 리소스 이름(ARN)을 사용하여 업데이트할 게이트웨이를 지정합니다.

구문 요청

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

업데이트할 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

GatewayDisplayName

게이트웨이의 업데이트된 표시 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

필수 여부: 아니요

응답 구문

```
{
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

업데이트한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateGatewaySoftwareNow

서비스: AWS Backup gateway

게이트웨이 가상 머신(VM) 소프트웨어를 업데이트합니다. 요청은 소프트웨어 업데이트를 즉시 트리거합니다.

> **Note**
>
> 이 요청을 할 경우, `200 OK` 성공 응답을 즉시 받게 됩니다. 그러나 업데이트가 완료되는 데 다소 시간이 걸릴 수 있습니다.

구문 요청

```
{
   "GatewayArn": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

GatewayArn

업데이트할 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 항목 여부: 예

응답 구문

```
{
```

```
   "GatewayArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

GatewayArn

업데이트한 게이트웨이의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS 루비 V3용 SDK

UpdateHypervisor

서비스: AWS Backup gateway

호스트, 사용자 이름, 암호를 포함한 하이퍼바이저 메타데이터를 업데이트합니다. 요청 시 하이퍼바이저의 Amazon 리소스 이름(ARN)을 사용하여 업데이트할 하이퍼바이저를 지정합니다.

구문 요청

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

요청 파라미터

모든 작업에서 사용하는 파라미터에 대한 자세한 내용은 범용 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Host

하이퍼바이저의 업데이트된 호스트입니다. 이는 IP 주소 또는 정규화된 도메인 이름(FQDN)일 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 128.

패턴: ^.+$

Required: No

HypervisorArn

업데이트할 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 사항 여부: Yes

LogGroupArn

요청한 로그 내 게이트웨이 그룹의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2,048.

패턴: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Required: No

Name

하이퍼바이저의 업데이트된 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

Password

하이퍼바이저의 업데이트된 암호입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[ -~]+$`

Required: No

Username

하이퍼바이저의 업데이트된 사용자 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

필수 여부: 아니요

응답 구문

```
{
   "HypervisorArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

HypervisorArn

업데이트된 하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errors

모든 작업에서 발생하는 일반적인 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

권한이 부족하여 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

ConflictException

지원되지 않기 때문에 작업을 계속할 수 없습니다.

HTTP 상태 코드: 400

InternalServerException

내부 오류가 발생하여 작업에 성공하지 못했습니다. 나중에 다시 시도해 주십시오.

HTTP 상태 코드: 500

ResourceNotFoundException

작업에 필요한 리소스를 찾을 수 없습니다.

HTTP 상태 코드: 400

ThrottlingException

TPS는 의도적이거나 의도하지 않은 대량 요청으로부터 보호하기 위해 제한되었습니다.

HTTP 상태 코드: 400

ValidationException

검증 오류가 발생하여 작업에 성공하지 못했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2를 위한 SDK
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS 루비 V3용 SDK

데이터 형식

다음 데이터 형식이 AWS Backup에서 지원됩니다.

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue

- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

다음 데이터 형식이 AWS Backup gateway에서 지원됩니다.

- BandwidthRateLimitInterval
- Gateway

- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

다음 데이터 형식이 AWS Backup에서 지원됩니다.

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope

- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate

- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

서비스: AWS Backup

각 리소스 유형에 대한 백업 옵션

내용

BackupOptions

선택한 리소스에 대한 백업 옵션을 지정합니다. 이 옵션은 Windows VSS 백업 작업에만 사용할 수 있습니다.

유효한 값:

`WindowsVSS` 백업 옵션을 활성화하고 Windows VSS 백업을 생성하려면 `"WindowsVSS":"enabled"`로 설정합니다.

정기 백업을 생성하려면 `"WindowsVSS":"disabled"`로 설정합니다. `WindowsVSS` 옵션은 기본적으로 활성화되어 있습니다.

잘못된 옵션을 지정하면 `InvalidParameterValueException` 예외가 발생합니다.

Windows VSS 백업에 대한 자세한 내용은 VSS 지원 Windows 백업 생성을 참조하세요.

유형: String 간 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

값 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

ResourceType

리소스 유형 및 백업 옵션을 포함하는 객체를 지정합니다. 지원되는 유일한 리소스 유형은 Windows VSS(Volume Shadow Copy Service)를 사용하는 Amazon EC2 인스턴스입니다. CloudFormation 예를 들어 사용 설명서의 Windows VSS를 활성화하기 위한 샘플 CloudFormation 템플릿을 참조하십시오. AWS Backup

유효한 값: `EC2`.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupJob

서비스: AWS Backup

백업 작업에 대한 세부 정보를 포함합니다.

내용

AccountId

백업 작업을 소유한 계정 ID를 반환합니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

BackupJobId

리소스 백업 요청을 고유하게 AWS Backup 식별합니다.

타입: 문자열

필수사항: 아니요

BackupOptions

선택한 리소스에 대한 백업 옵션을 지정합니다. 이 옵션은 Windows VSS(Volume Shadow Copy Service) 백업 작업에만 사용할 수 있습니다.

유효한 값: `WindowsVSS` 백업 옵션을 활성화하고 Windows VSS 백업을 생성하려면 `"WindowsVSS":"enabled"`로 설정합니다. 정기 백업을 생성하려면 `"WindowsVSS":"disabled"`로 설정합니다. 잘못된 옵션을 지정하면 `InvalidParameterValueException` 예외가 발생합니다.

유형: String 간 맵

키 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

값 패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

BackupSizeInBytes

백업의 크기(바이트 단위)입니다.

유형: Long

필수 여부: 아니요

BackupType

백업 작업의 백업 유형을 나타냅니다.

타입: 문자열

필수사항: 아니요

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

필수사항: 아니요

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: No

BytesTransferred

작업 상태를 쿼리할 때 백업 저장소로 전송된 크기(바이트)입니다.

유형: Long

필수 여부: 아니요

CompletionDate

백업 작업을 생성하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreatedBy

백업 작업을 생성하는 데 사용되는 백업 계획의 BackupPlanArn, BackupPlanId, BackupPlanVersion, BackupRuleId를 비롯하여, 백업 작업의 생성에 대한 식별 정보를 포함합니다.

유형: RecoveryPointCreator객체

필수 항목 여부: 아니요

CreationDate

백업 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. CreationDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

ExpectedCompletionDate

리소스를 백업하는 작업이 완료될 것으로 예상되는 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. ExpectedCompletionDate의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다. 기본 역할 이외의 IAM 역할은 역할 이름에 AWSBackup 또는 AwsBackup을 포함해야 합니다. 예를 들어 arn:aws:iam::123456789012:role/AWSBackupRDSAccess입니다. 이러한 문자열이 없는 역할 이름은 백업 작업을 수행할 수 있는 권한이 없습니다.

타입: 문자열

필수사항: 아니요

InitiationDate

백업 작업이 시작된 날짜.

유형: 타임스탬프

필수 여부: 아니요

IsParent

상위(복합) 백업 작업이라는 것을 나타내는 부울 값입니다.

타입: 부울

필수 항목 여부: 아니요

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수입니다.

예시 문자열에는 `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL`, `INVALIDPARAMETERS` 등이 있습니다. MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

타입: 문자열

필수사항: 아니요

ParentJobId

리소스를 백업하기 위한 AWS Backup 에 대한 요청을 고유하게 식별합니다. 반환되는 항목은 상위(복합) 작업 ID입니다.

타입: 문자열

필수사항: 아니요

PercentDone

작업 상태를 쿼리할 때 작업의 예상 완료율을 포함합니다.

유형: String

필수사항: 아니요

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

유형: String

필수사항: 아니요

ResourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

필수사항: 아니요

ResourceType

백업할 AWS 리소스 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스). Windows VSS(Volume Shadow Copy Service)의 경우, 지원되는 유일한 리소스 유형은 Amazon EC2입니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

StartBy

백업 작업을 취소하기 전에 시작해야 하는 시간을 Unix 형식 및 협정 세계시(UTC)로 지정합니다. 이 값은 시작 기간을 예약된 시간에 더하여 계산됩니다. 따라서 예약된 시간이 오후 6시이고 시작 기간이 2시간인 경우, `StartBy` 시간은 지정된 날짜의 오후 8시가 됩니다. `StartBy`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

State

백업 작업의 현재 상태입니다.

타입: 문자열

유효 값: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

필수 여부: 아니요

StatusMessage

리소스를 백업하기 위한 작업의 상태를 설명하는 자세한 메시지입니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupJobSummary

서비스: AWS Backup

최근 30일 이내에 생성되거나 실행된 작업의 요약입니다.

반환된 요약에는 지역, 계정, 주,,, RestourceType MessageCategory StartTime EndTime, 포함된 작업 수 등이 포함될 수 있습니다.

내용

AccountId

요약 내의 작업을 소유한 계정 ID입니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

Count

작업 요약의 작업 수를 나타낸 값입니다.

유형: 정수

필수 항목 여부: 아니요

EndTime

작업 종료 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수입니다.

예시 문자열에는 `AccessDenied`, `Success`, `InvalidParameters` 등이 있습니다. MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

AGGREGATE_ALL은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

타입: 문자열

필수사항: 아니요

Region

작업 요약 내 AWS 지역.

타입: 문자열

필수사항: 아니요

ResourceType

이 값은 지정된 리소스 유형의 작업 수입니다. GetSupportedResourceTypes 요청은 지원되는 리소스 유형의 문자열을 반환합니다.

유형: String

패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

Required: No

StartTime

작업 시작 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

State

이 값은 지정된 상태의 작업 수입니다.

타입: 문자열

유효 값: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupPlan

서비스: AWS Backup

선택적 백업 계획 표시 이름과 각각 백업 규칙을 지정하는 `BackupRule` 객체의 배열을 포함합니다. 백업 계획의 각 규칙은 별도의 예약 태스크이며 선택한 다른 AWS 리소스를 백업할 수 있습니다.

내용

BackupPlanName

백업 계획의 표시 이름입니다. 1~50자의 영숫자 또는 '-_.'로 구성되어야 합니다.

타입: 문자열

필수 항목 여부: 예

Rules

각각 다양한 리소스를 백업하는 데 사용되는 예약된 작업을 지정하는 `BackupRule` 객체의 어레이입니다.

유형: BackupRule객체 어레이

필수 여부: 예

AdvancedBackupSettings

각 리소스 유형에 대한 `BackupOptions` 목록이 포함됩니다.

타입: AdvancedBackupSetting객체 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupPlanInput

서비스: AWS Backup

선택적 백업 계획 표시 이름과 각각 백업 규칙을 지정하는 `BackupRule` 객체의 배열을 포함합니다. 백업 계획의 각 규칙은 별도의 예약된 태스크입니다.

내용

BackupPlanName

백업 계획의 표시 이름입니다. 1~50자의 영숫자 또는 '-_.'로 구성되어야 합니다.

타입: 문자열

필수 항목 여부: 예

Rules

각각 다양한 리소스를 백업하는 데 사용되는 예약된 작업을 지정하는 `BackupRule` 객체의 어레이입니다.

유형: BackupRuleInput객체 어레이

필수 여부: 예

AdvancedBackupSettings

각 리소스 유형에 대한 `BackupOptions` 목록을 지정합니다. 이러한 설정은 Windows VSS(Volume Shadow Copy Service) 백업 작업에만 사용할 수 있습니다.

타입: AdvancedBackupSetting객체 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupPlansListMember

서비스: AWS Backup

백업 계획에 대한 메타데이터를 포함합니다.

내용

AdvancedBackupSettings

리소스 유형에 대한 `BackupOptions` 목록이 포함됩니다.

타입: AdvancedBackupSetting객체 배열

필수: 아니요

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`)입니다.

유형: String

필수사항: 아니요

BackupPlanId

백업 계획을 고유하게 식별합니다.

유형: String

필수사항: 아니요

BackupPlanName

저장된 백업 계획의 표시 이름입니다.

타입: 문자열

필수사항: 아니요

CreationDate

리소스 백업 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

DeletionDate

백업 계획이 삭제된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `DeletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

LastExecutionDate

이 백업 계획을 마지막으로 실행한 시간. 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastExecutionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

VersionId

임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupPlanTemplatesListMember

서비스: AWS Backup

백업 계획 템플릿과 관련된 메타데이터를 지정하는 객체입니다.

내용

BackupPlanTemplateId

저장된 백업 계획 템플릿을 고유하게 식별합니다.

타입: 문자열

필수사항: 아니요

BackupPlanTemplateName

백업 계획 템플릿의 표시 이름입니다(선택 사항).

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupRule

서비스: AWS Backup

다양한 리소스를 백업하는 데 사용되는 예약된 태스크를 지정합니다.

내용

RuleName

백업 규칙의 표시 이름입니다. 1~50자의 영숫자 또는 '-_.'로 구성되어야 합니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 사항 여부: Yes

TargetBackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

CompletionWindowMinutes

백업 작업이 성공적으로 시작된 후 완료되거나 AWS Backup에 의해 취소되기 전까지의 값(분)입니다. 이 값은 선택 사항입니다.

유형: Long

필수 여부: 아니요

CopyActions

복사 작업의 세부 정보를 포함하는 `CopyAction` 객체의 배열입니다.

타입: CopyAction객체 배열

필수: 아니요

EnableContinuousBackup

연속 백업 AWS Backup 생성 여부를 지정합니다. point-in-time 복원이 가능한 연속 백업 (PITR) AWS Backup 을 생성하는 진정한 원인. 잘못된 (또는 지정되지 않은) 원인으로 AWS Backup 인해 스냅샷 백업이 생성됩니다.

타입: 부울

필수 항목 여부: 아니요

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

유형: Lifecycle객체

필수 항목 여부: 아니요

RecoveryPointTags

백업에서 복원할 때 이 규칙과 관련된 리소스에 할당되는 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

RuleId

다양한 리소스의 백업을 예약하는 데 사용되는 규칙을 고유하게 식별합니다.

타입: 문자열

필수사항: 아니요

ScheduleExpression

백업 AWS Backup 작업을 시작하는 시기를 지정하는 UTC의 cron 표현식입니다. AWS 크론 표현식에 대한 자세한 내용은 Amazon CloudWatch Events 사용 설명서의 규칙에 대한 스케줄 표현식을

참조하십시오. . AWS cron 표현식의 두 가지 예로는 `15 * ? * * *` (1시간 이후 15분에 1시간마다 백업 생성) 과 `0 12 * * ? *` (UTC 기준 매일 정오 12시에 백업 생성) 이 있습니다. 예시 표를 보려면 이전 링크를 클릭하고 페이지를 아래로 스크롤하세요.

타입: 문자열

필수사항: 아니요

ScheduleExpressionTimezone

스케줄 표현식이 설정된 시간대입니다. 기본적으로 UTC ScheduleExpressions 기준입니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowMinutes

백업이 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(분)입니다. 이 값은 선택 사항입니다. 이 값이 포함된 경우 오류를 방지하려면 60분 이상이어야 합니다.

시작 기간 동안에는 백업 작업이 성공적으로 시작되거나 시작 기간이 만료될 때까지 백업 작업 상태가 `CREATED` 상태로 유지됩니다. 시작 시간 AWS Backup 내에 작업을 재시도할 수 있는 오류가 발생하면 백업이 성공적으로 시작 (작업 상태가 로 변경`RUNNING`) 되거나 작업 상태가 로 변경될 때까지 (시작 시간이 끝나면 발생할 것으로 예상됨) 최소 10분마다 AWS Backup 자동으로 작업을 다시 시도합니다. `EXPIRED`

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupRuleInput

서비스: AWS Backup

다양한 리소스를 백업하는 데 사용되는 예약된 태스크를 지정합니다.

내용

RuleName

백업 규칙의 표시 이름입니다. 1~50자의 영숫자 또는 '-_.'로 구성되어야 합니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 사항 여부: Yes

TargetBackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

필수 사항 여부: Yes

CompletionWindowMinutes

백업 작업이 성공적으로 시작된 후 완료되거나 AWS Backup에 의해 취소되기 전까지의 값(분)입니다. 이 값은 선택 사항입니다.

유형: Long

필수 여부: 아니요

CopyActions

복사 작업의 세부 정보를 포함하는 `CopyAction` 객체의 배열입니다.

타입: CopyAction객체 배열

필수: 아니요

EnableContinuousBackup

연속 백업 AWS Backup 생성 여부를 지정합니다. point-in-time 복원이 가능한 연속 백업 (PITR) AWS Backup 을 생성하는 진정한 원인. 잘못된 (또는 지정되지 않은) 원인으로 AWS Backup 인해 스냅샷 백업이 생성됩니다.

타입: 부울

필수 항목 여부: 아니요

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드 스토리지로 전환된 후에는 "며칠 후 콜드 스토리지로 전환" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

이 파라미터의 최대값은 100년(36,500일)입니다.

유형: Lifecycle객체

필수 항목 여부: 아니요

RecoveryPointTags

리소스에 할당할 태그입니다.

유형: 문자열 간 맵

필수 여부: 아니요

ScheduleExpression

백업 AWS Backup 작업을 시작하는 시기를 지정하는 UTC의 CRON 표현식입니다.

타입: 문자열

필수사항: 아니요

ScheduleExpressionTimezone

스케줄 표현식이 설정된 시간대입니다. 기본적으로 UTC ScheduleExpressions 기준입니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowMinutes

백업이 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(분)입니다. 이 값은 선택 사항입니다. 이 값이 포함된 경우 오류를 방지하려면 60분 이상이어야 합니다.

이 파라미터의 최대값은 100년(52,560,000분)입니다.

시작 기간 동안에는 백업 작업이 성공적으로 시작되거나 시작 기간이 만료될 때까지 백업 작업 상태가 CREATED 상태로 유지됩니다. 시작 시간 AWS Backup 내에 작업을 재시도할 수 있는 오류가 발생하면 백업이 성공적으로 시작 (작업 상태가 로 변경RUNNING) 되거나 작업 상태가 로 변경될 때까지 (시작 시간이 끝나면 발생할 것으로 예상됨) 최소 10분마다 AWS Backup 자동으로 작업을 다시 시도합니다. EXPIRED

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupSelection

서비스: AWS Backup

백업 계획에 대한 리소스 집합을 지정하는 데 사용됩니다.

포함하거나 제외할 조건, 태그 또는 리소스를 지정하는 것이 좋습니다. 그렇지 않으면 Backup은 지원되고 옵트인된 모든 스토리지 리소스를 선택하려고 시도하므로 의도하지 않은 비용 문제가 발생할 수 있습니다.

자세한 내용은 프로그래밍 방식으로 리소스 할당을 참조하십시오.

내용

IamRoleArn

대상 리소스를 백업할 때 인증에 AWS Backup 사용하는 IAM 역할의 ARN (예:). `arn:aws:iam::123456789012:role/S3Access`

타입: 문자열

필수 항목 여부: 예

SelectionName

리소스 선택 문서의 표시 이름입니다. 1~50자의 영숫자 또는 '-_.'로 구성되어야 합니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 사항 여부: Yes

Conditions

태그를 사용하여 백업 계획에 리소스를 할당하기 위해 정의하는 조건 예를 들어 `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`입니다.

`ConditionsStringEquals`, `StringLikeStringNotEquals`, 및 을 지원합니다`StringNotLike`. 조건 연산자는 대/소문자를 구분합니다.

조건을 여러 개 지정하는 경우 리소스가 모든 조건 (AND 로직) 과 거의 일치합니다.

유형: Conditions객체

필수 항목 여부: 아니요

ListOfTags

태그를 사용하여 백업 계획에 리소스를 할당하기 위해 정의하는 조건 예를 들어 `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`입니다.

`ListOfTags`만 지원합니다`StringEquals`. 조건 연산자는 대/소문자를 구분합니다.

조건을 여러 개 지정하는 경우 리소스가 모든 조건 (OR 로직) 과 거의 일치합니다.

타입: Condition객체 배열

필수: 아니요

NotResources

백업 계획에서 제외할 리소스의 Amazon 리소스 이름 (ARN) 최대 ARN 수는 와일드카드가 없는 경우 500개, 와일드카드가 있는 경우 30개입니다.

백업 계획에서 많은 리소스를 제외해야 하는 경우 하나 또는 몇 개의 리소스 유형만 할당하거나 태그를 사용하여 리소스 선택을 구체화하는 등 다른 리소스 선택 전략을 고려하세요.

유형: String 배열

필수 여부: 아니요

Resources

백업 계획에 할당할 리소스의 Amazon 리소스 이름 (ARN) 최대 ARN 수는 와일드카드가 없는 경우 500개, 와일드카드가 있는 경우 30개입니다.

백업 계획에 많은 리소스를 할당해야 하는 경우, 한 리소스 유형의 모든 리소스를 할당하거나 태그를 사용하여 리소스 선택을 구체화하는 등 다른 리소스 선택 전략을 고려하세요.

ARN을 여러 개 지정하는 경우 리소스는 모든 ARN (OR 로직) 과 거의 일치합니다.

유형: String 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupSelectionsListMember

서비스: AWS Backup

`BackupSelection` 객체에 대한 메타데이터를 포함합니다.

내용

BackupPlanId

백업 계획을 고유하게 식별합니다.

유형: String

필수사항: 아니요

CreationDate

백업 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 Amazon 리소스 이름(ARN)을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수사항: 아니요

SelectionId

리소스 세트를 백업 계획에 할당하는 요청을 고유하게 식별합니다.

타입: 문자열

필수사항: 아니요

SelectionName

리소스 선택 문서의 표시 이름입니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

BackupVaultListMember

서비스: AWS Backup

백업 저장소에 대한 메타데이터를 포함합니다.

내용

BackupVaultArn

백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`)입니다.

타입: 문자열

필수사항: 아니요

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: No

CreationDate

리소스 백업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreatorRequestId

요청을 식별하고 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 하는 고유 문자열입니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

EncryptionKeyArn

전체 AWS Backup 관리를 지원하는 서비스의 백업을 암호화하기 위해 지정할 수 있는 서버 측 암호화 키 (예:). `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 키를 지정하는 경우 별칭이 아닌 ARN을 지정해야 합니다. 키를 지정하지 않으면 AWS Backup 이 기본적으로 KMS 키를 생성합니다.

전체 AWS Backup 관리를 지원하는 AWS Backup 서비스와 아직 전체를 지원하지 않는 서비스의 백업에 대한 암호화를 AWS Backup 처리하는 방법을 알아보려면 의 백업 암호화를 참조하십시오. AWS Backup AWS Backup

타입: 문자열

필수사항: 아니요

LockDate

AWS Backup Vault Lock 구성을 변경할 수 없게 되는 날짜 및 시간 (즉, 변경하거나 삭제할 수 없음)

잠금 날짜를 지정하지 않고 저장소 잠금을 저장소에 적용한 경우, 언제든지 저장소 잠금 설정을 변경하거나 저장소에서 저장소 잠금을 완전히 삭제할 수 있습니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

Locked

선택한 백업 AWS Backup 저장소에 저장소 잠금을 적용할지 여부를 나타내는 부울 값입니다. `true`인 경우, 저장소 잠금은 선택한 저장소의 복구 시점에 대한 삭제 및 업데이트 작업을 방지합니다.

타입: 부울

필수 항목 여부: 아니요

MaxRetentionDays

AWS Backup 저장소 잠금 설정은 저장소가 복구 지점을 보존하는 최대 보존 기간을 지정합니다. 이 파라미터가 지정되지 않으면 저장소 잠금은 저장소의 복구 시점에 최대 보존 기간을 적용하지 않습니다(무제한 저장 가능).

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최대 보존 기간보다 짧거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최대 보존 기간보다 길면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 시점은 영향을 받지 않습니다.

유형: Long

필수 여부: 아니요

MinRetentionDays

AWS Backup 저장소 잠금 설정은 저장소에서 복구 지점을 보존하는 최소 보존 기간을 지정합니다. 이 파라미터가 지정되지 않으면 저장소 잠금이 최소 보존 기간을 적용하지 않습니다.

이 설정이 지정되면 저장소에 대한 모든 백업 또는 복사 작업에 보존 기간이 최소 보존 기간보다 길거나 같은 수명 주기 정책이 있어야 합니다. 작업의 보존 기간이 최소 보존 기간보다 짧으면 저장소가 백업 또는 복사 작업에 실패하므로 수명 주기 설정을 수정하거나 다른 저장소를 사용해야 합니다. 저장소 잠금 이전에 저장소에 이미 저장된 복구 시점은 영향을 받지 않습니다.

유형: Long

필수 여부: 아니요

NumberOfRecoveryPoints

백업 저장소에 저장된 복구 시점의 수입니다.

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++

- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

CalculatedLifecycle

서비스: AWS Backup

복구 시점의 수명 주기를 지정하는 데 사용되는 `DeleteAt` 및 `MoveToColdStorageAt` 타임스탬프를 포함합니다.

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

내용

DeleteAt

복구 시점을 삭제할 시기를 지정하는 타임스탬프입니다.

유형: 타임스탬프

필수 여부: 아니요

MoveToColdStorageAt

복구 시점을 콜드 스토리지로 전환할 시기를 지정하는 타임스탬프입니다.

유형: 타임스탬프

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Condition

서비스: AWS Backup

조건 유형(예: `StringEquals`), 키 및 값으로 구성된 세 쌍의 배열을 포함합니다. 태그를 사용하여 리소스를 필터링하고 백업 계획에 할당하는 데 사용됩니다. 대소문자 구분.

내용

ConditionKey

키-값 페어의 키입니다. 예를 들어, 태그 `Department: Accounting`에서 키는 `Department`입니다.

타입: 문자열

필수 항목 여부: 예

ConditionType

백업 계획에 리소스를 할당하는 데 사용되는 키-값 쌍에 적용되는 작업입니다. `StringEquals`만 지원하는 조건입니다. `StringLike` 및 백업 계획에서 리소스를 제외하는 기능을 비롯하여 더 유연한 할당 옵션을 원할 경우, `BackupSelection`에 `Conditions`(끝에 "s" 포함)를 사용하세요.

타입: 문자열

유효 값: `STRINGEQUALS`

필수 사항 여부: 예

ConditionValue

키-값 페어의 값입니다. 예를 들어, 태그 `Department: Accounting`에서 값은 `Accounting`입니다.

타입: 문자열

필수 항목 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++

- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ConditionParameter

서비스: AWS Backup

태그가 지정된 리소스를 백업 계획에 할당하기 위해 정의하는 태그에 대한 정보를 포함합니다.

태그에 접두사를 `aws:ResourceTag` 포함하세요. 예를 들어 `"aws:ResourceTag/TagKey1": "Value1"`입니다.

내용

ConditionKey

키-값 페어의 키입니다. 예를 들어, 태그 `Department: Accounting`에서 키는 `Department`입니다.

타입: 문자열

필수사항: 아니요

ConditionValue

키-값 페어의 값입니다. 예를 들어, 태그 `Department: Accounting`에서 값은 `Accounting`입니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Conditions

서비스: AWS Backup

해당 태그를 사용하여 백업 계획에서 포함하거나 제외할 리소스에 대한 정보를 포함합니다. 조건은 대/소문자를 구분합니다.

내용

StringEquals

동일한 값으로 태그를 지정한 리소스에 대해서만 태그가 지정된 리소스의 값을 필터링합니다. '하드 매칭'이라고도 합니다.

타입: ConditionParameter객체 배열

필수: 아니요

StringLike

문자열에 와일드카드 문자(*)를 사용하여 일치하는 태그 값에 대해 태그가 지정된 리소스의 값을 필터링합니다. 예를 들어, 'prod*' 또는 '*rod*'는 태그 값 'production'과 일치합니다.

타입: ConditionParameter객체 배열

필수: 아니요

StringNotEquals

태그를 지정한 리소스 중 값이 동일하지 않은 리소스에 대해서만 태그가 지정된 리소스의 값을 필터링합니다. '부정 매칭'이라고도 합니다.

타입: ConditionParameter객체 배열

필수: 아니요

StringNotLike

문자열의 아무 곳에나 와일드카드 문자(*)를 사용하여 일치하지 않는 태그 값에 대해 태그가 지정된 리소스의 값을 필터링합니다.

타입: ConditionParameter객체 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ControlInputParameter

서비스: AWS Backup

컨트롤의 파라미터. 제어에 0개, 1개 또는 2개 이상의 파라미터가 있을 수 있습니다. 2개의 파라미터가 있는 제어의 예로 '백업 계획 빈도는 최소 `daily`이고 보존 기간은 최소 `1 year`입니다.'가 있습니다. 첫 번째 파라미터는 `daily`입니다. 두 번째 파라미터는 `1 year`입니다.

내용

ParameterName

파라미터의 이름(예: `BackupPlanFrequency`)입니다.

타입: 문자열

필수사항: 아니요

ParameterValue

파라미터의 값(예: `hourly`)입니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ControlScope

서비스: AWS Backup

프레임워크는 하나 이상의 컨트롤로 구성됩니다. 컨트롤마다 자체 제어 범위가 있습니다. 제어 범위에는 하나 이상의 리소스 유형, 태그 키 및 값의 조합 또는 리소스 유형 하나 및 리소스 ID 하나의 조합이 포함될 수 있습니다. 범위가 지정되지 않으면 기록 그룹의 리소스가 구성에서 변경될 때 규칙에 대한 평가가 트리거됩니다.

> **Note**
>
> 특정 리소스를 모두 포함하는 제어 범위를 설정하려면 `ControlScope`를 비워 두거나 `CreateFramework` 호출 시 전달하지 마세요.

내용

ComplianceResourceIds

제어 범위에 포함하려는 유일한 AWS 리소스의 ID입니다.

유형: 문자열 어레이

배열 멤버: 최소수는 1개입니다. 최대 항목 수는 100개입니다.

필수 여부: 아니요

ComplianceResourceTypes

제어 범위에 `EFS` 또는 `RDS`와 같은 리소스 유형이 하나 이상 포함되는지 여부를 설명합니다.

유형: String 배열

필수 여부: 아니요

Tags

규칙 평가를 트리거하려는 AWS 리소스에 적용된 태그 키-값 쌍입니다. 최대 하나의 키-값 페어가 제공될 수 있습니다. 태그 값은 선택 사항이지만 콘솔에서 프레임워크를 만들거나 편집하는 경우에는 빈 문자열이 될 수 없습니다. 단, CloudFormation 템플릿에 포함된 값은 빈 문자열이 될 수 있습니다.

태그를 할당하는 구조는 `[{"Key":"string","Value":"string"}]`입니다.

유형: 문자열 간 맵

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

CopyAction

서비스: AWS Backup

복사 작업의 세부 정보입니다.

내용

DestinationBackupVaultArn

복사된 백업의 대상 백업 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN). 예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

타입: 문자열

필수 항목 여부: 예

Lifecycle

복구 지점이 콜드 스토리지로 전환되거나 삭제되기까지의 기간 (일) 을 지정합니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 콘솔의 보존 설정은 며칠 후 콜드 전환으로의 전환보다 90일 더 커야 합니다. 백업이 콜드 백업으로 전환된 후에는 [며칠 후 콜드] 로의 전환 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

기존 수명 주기 및 보존 기간을 제거하고 복구 지점을 무기한으로 유지하려면 및 에 `MoveToColdStorageAfterDays` `-1`을 지정하십시오. `DeleteAfterDays`

유형: Lifecycle객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

CopyJob

서비스: AWS Backup

복사 작업에 대한 세부 정보를 포함합니다.

내용

AccountId

복사 작업을 소유한 계정 ID입니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

BackupSizeInBytes

복사 작업의 크기(바이트 단위)입니다.

유형: Long

필수 여부: 아니요

ChildJobsInState

포함된 하위(중첩) 복사 작업의 통계를 반환합니다.

유형: String과 Long 간의 맵

유효한 키: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

필수 여부: 아니요

CompletionDate

복사 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CompositeMemberIdentifier

복합 그룹 내의 리소스 식별자 (예: 복합 (상위) 스택에 속하는 중첩된 (하위) 복구 지점) ID는 스택 내의 논리적 ID 전송됩니다.

유형: String

필수사항: 아니요

CopyJobId

복사 작업을 고유하게 식별합니다.

타입: 문자열

필수사항: 아니요

CreatedBy

복구 지점 백업을 시작하는 데 AWS Backup 사용된 백업 계획 및 규칙에 대한 정보가 들어 있습니다.

유형: RecoveryPointCreator객체

필수 항목 여부: 아니요

CreationDate

복사 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

DestinationBackupVaultArn

대상 복사 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

필수사항: 아니요

DestinationRecoveryPointArn

대상 복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

필수사항: 아니요

IamRoleArn

대상 복구 시점을 복사하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수사항: 아니요

IsParent

상위(복합) 복사 작업이라는 것을 나타내는 부울 값입니다.

타입: 부울

필수 항목 여부: 아니요

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수입니다.

예시 문자열에는 `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL`, `InvalidParameters` 등이 있습니다. MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

`AGGREGATE_ALL`은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

타입: 문자열

필수사항: 아니요

NumberOfChildJobs

하위 (중첩) 복사 작업 수

유형: Long

필수 여부: 아니요

ParentJobId

AWS Backup 에 대한 리소스 복사 요청을 고유하게 식별합니다. 반환되는 항목은 상위(복합) 작업 ID입니다.

타입: 문자열

필수사항: 아니요

ResourceArn

복사할 AWS 리소스 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스)

타입: 문자열

필수사항: 아니요

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

필수사항: 아니요

ResourceType

복사할 AWS 리소스의 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스)

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

SourceBackupVaultArn

소스 복사 저장소를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

타입: 문자열

필수사항: 아니요

SourceRecoveryPointArn

소스 복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

타입: 문자열

필수사항: 아니요

State

복사 작업의 현재 상태입니다.

타입: 문자열

유효 값: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

필수 여부: 아니요

StatusMessage

리소스를 복사하기 위한 작업의 상태를 설명하는 자세한 메시지입니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

CopyJobSummary

서비스: AWS Backup

최근 30일 이내에 생성되거나 실행된 복사 작업의 요약입니다.

반환된 요약에는 지역, 계정, 주,,, RestourceType MessageCategory StartTime EndTime, 포함된 작업 수 등이 포함될 수 있습니다.

내용

AccountId

요약 내의 작업을 소유한 계정 ID입니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

Count

작업 요약의 작업 수를 나타낸 값입니다.

유형: 정수

필수 항목 여부: 아니요

EndTime

작업 종료 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

MessageCategory

이 파라미터는 지정된 메시지 범주의 작업 수입니다.

예시 문자열에는 `AccessDenied`, `Success`, `InvalidParameters` 등이 있습니다. MessageCategory 문자열 목록은 모니터링을 참조하십시오.

ANY 값은 모든 메시지 범주의 개수를 반환합니다.

AGGREGATE_ALL은 모든 메시지 범주의 작업 수를 집계하고 그 합계를 반환합니다.

타입: 문자열

필수사항: 아니요

Region

작업 요약 내 AWS 지역.

타입: 문자열

필수사항: 아니요

ResourceType

이 값은 지정된 리소스 유형의 작업 수입니다. GetSupportedResourceTypes 요청은 지원되는 리소스 유형의 문자열을 반환합니다.

유형: String

패턴: ^[a-zA-Z0-9\-_\.]{1,50}$

Required: No

StartTime

작업 시작 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

State

이 값은 지정된 상태의 작업 수입니다.

타입: 문자열

유효 값: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

DateRange

서비스: AWS Backup

이것은 FromDate ToDate: DateTime 및 :를 포함하는 리소스 DateTime 필터입니다. 두 값은 모두 필수입니다. 미래 DateTime 값은 허용되지 않습니다.

날짜 및 시간은 Unix 형식 및 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다(밀리초는 선택 사항). 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

내용

FromDate

이 값은 시작 날짜입니다(경계값 포함).

날짜 및 시간은 Unix 형식 및 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다(밀리초는 선택 사항).

유형: 타임스탬프

필수 여부: 예

ToDate

이 값은 종료 날짜입니다(경계값 포함).

날짜 및 시간은 Unix 형식 및 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다(밀리초는 선택 사항).

유형: 타임스탬프

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Framework

서비스: AWS Backup

프레임워크에 대한 자세한 정보를 포함합니다. 프레임워크에는 백업 이벤트 및 리소스를 평가하고 보고하는 컨트롤이 포함되어 있습니다. 프레임워크는 일일 규정 준수 결과를 생성합니다.

내용

CreationTime

프레임워크가 생성된 날짜 및 시간이며, ISO 8601 형식으로 표시됩니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 2020-07-10T15:00:00.000-08:00은 UTC보다 8시간 늦은 2020년 7월 10일 오후 3시를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

DeploymentStatus

프레임워크의 배포 상태입니다. 상태는 다음과 같습니다.

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

유형: String

필수사항: 아니요

FrameworkArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

FrameworkDescription

프레임워크에 대한 최대 1,024자의 설명(선택 사항)입니다.

유형: String

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

FrameworkName

프레임워크의 고유 이름입니다. 이 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자 사이입니다.

유형: String

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

Required: No

NumberOfControls

프레임워크에 포함된 컨트롤의 수입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

FrameworkControl

서비스: AWS Backup

프레임워크의 모든 컨트롤에 대한 자세한 정보가 들어 있습니다. 각 프레임워크에 하나 이상의 제어가 들어 있어야 합니다.

내용

ControlName

제어의 이름입니다. 이 이름은 1~256자입니다.

유형: String

필수 항목 여부: 예

ControlInputParameters

이름/값 쌍.

타입: ControlInputParameter객체 배열

필수: 아니요

ControlScope

제어 범위입니다. 제어 범위는 제어가 평가할 대상을 정의합니다. 제어 범위의 3가지 예로 특정 백업 계획, 특정 태그가 있는 모든 백업 계획 또는 모든 백업 계획이 있습니다.

자세한 내용은 `ControlScope` 섹션을 참조하세요.

유형: ControlScope객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

KeyValue

서비스: AWS Backup

두 개의 관련 문자열 쌍입니다. 허용되는 문자는 문자, 공백 및 UTF-8로 표시할 수 있는 숫자와 + - = . _ : /입니다.

내용

Key

태그 키(문자열)입니다. 키는 aws:로 시작할 수 없습니다.

길이 제약: 최소 길이 1. 최대 길이 128.

패턴: ^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

타입: 문자열

필수 항목 여부: 예

Value

키의 값입니다.

길이 제약: 최대 길이 256.

패턴: ^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

타입: 문자열

필수 항목 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

LegalHold

서비스: AWS Backup

법적 보존은 보존 기간 중에 백업이 삭제되는 것을 방지하는 데 도움이 되는 관리 도구입니다. 보존이 적용되는 동안에는 보존 상태의 백업을 삭제할 수 없으며, 백업 상태를 변경하는 수명 주기 정책(예: 콜드 스토리지로의 전환)은 법적 보존이 제거될 때까지 연기됩니다. 백업은 둘 이상의 법적 보존을 보유할 수 있습니다. 법적 보존은 하나 이상의 백업(복구 시점이라고도 함)에 적용됩니다. 이러한 백업은 리소스 유형 및 리소스 ID별로 필터링할 수 있습니다.

내용

CancellationDate

법적 보류가 취소된 시기입니다.

유형: 타임스탬프

필수 여부: 아니요

CreationDate

법적 보존이 생성된 시간.

유형: 타임스탬프

필수 여부: 아니요

Description

법적 보류에 대한 설명.

타입: 문자열

필수사항: 아니요

LegalHoldArn

법적 보존의 Amazon 리소스 이름 (ARN) (예:) `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

타입: 문자열

필수사항: 아니요

LegalHoldId

법적 보류의 ID.

타입: 문자열

필수사항: 아니요

Status

법적 보류 상태.

타입: 문자열

유효 값: `CREATING | ACTIVE | CANCELING | CANCELED`

필수 여부: 아니요

Title

법적 보류의 제목.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Lifecycle

서비스: AWS Backup

복구 지점이 콜드 스토리지로 전환되거나 삭제되기까지의 기간 (일) 을 지정합니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 콘솔의 보존 설정은 며칠 후 콜드 전환으로의 전환보다 90일 더 커야 합니다. 백업이 콜드 백업으로 전환된 후에는 [며칠 후 콜드] 로의 전환 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

기존 수명 주기 및 보존 기간을 제거하고 복구 지점을 무기한으로 유지하려면 및 에 `MoveToColdStorageAfterDays` -1을 지정하십시오. `DeleteAfterDays`

내용

DeleteAfterDays

복구 지점을 만든 후 복구 지점이 삭제되기까지 경과한 일수입니다. 이 값은 에서 지정한 일수로부터 최소 90일 이후여야 `MoveToColdStorageAfterDays` 합니다.

유형: Long

필수 여부: 아니요

MoveToColdStorageAfterDays

복구 지점이 생성된 후 콜드 스토리지로 이동되는 기간 (일)

유형: Long

필수 여부: 아니요

OptInToArchiveForSupportedResources

값이 true인 경우 백업 계획은 라이프사이클 설정에 따라 지원되는 리소스를 아카이브 (콜드) 스토리지 계층으로 전환합니다.

타입: 부울

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ProtectedResource

서비스: AWS Backup

백업된 리소스에 대한 정보가 포함된 구조입니다.

내용

LastBackupTime

리소스가 마지막으로 백업된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastBackupTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

LastBackupVaultArn

가장 최근의 백업 복구 지점이 포함된 백업 저장소의 ARN (Amazon 리소스 이름).

타입: 문자열

필수사항: 아니요

LastRecoveryPointArn

가장 최근 복구 지점의 ARN (Amazon 리소스 이름).

타입: 문자열

필수사항: 아니요

ResourceArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

필수사항: 아니요

ResourceType

AWS 리소스 유형 (예: 아마존 엘라스틱 블록 스토어 (Amazon EBS) 볼륨 또는 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스). Windows VSS(Volume Shadow Copy Service)의 경우, 지원되는 유일한 리소스 유형은 Amazon EC2입니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ProtectedResourceConditions

서비스: AWS Backup

태그를 사용하여 복원 테스트 계획의 리소스에 대해 정의하는 조건.

예를 들어 `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`입니다. 조건 연산자는 대/소문자를 구분합니다.

내용

StringEquals

동일한 값으로 태그를 지정한 리소스에 대해서만 태그가 지정된 리소스의 값을 필터링합니다. '하드 매칭'이라고도 합니다.

타입: KeyValue객체 배열

필수: 아니요

StringNotEquals

태그를 지정한 리소스 중 값이 동일하지 않은 리소스에 대해서만 태그가 지정된 리소스의 값을 필터링합니다. '부정 매칭'이라고도 합니다.

타입: KeyValue객체 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RecoveryPointByBackupVault

서비스: AWS Backup

백업 저장소에 저장된 복구 시점에 대한 자세한 정보를 포함합니다.

내용

BackupSizeInBytes

백업의 크기(바이트 단위)입니다.

유형: Long

필수 여부: 아니요

BackupVaultArn

백업 저장소를 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`).

유형: String

필수사항: 아니요

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: No

CalculatedLifecycle

`DeleteAt` 및 `MoveToColdStorageAt` 타임스탬프를 포함하는 `CalculatedLifecycle` 객체입니다.

유형: CalculatedLifecycle객체

필수 항목 여부: 아니요

CompletionDate

복구 시점을 복원하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CompositeMemberIdentifier

복합 그룹 내 리소스의 식별자 (예: 복합 (상위) 스택에 속하는 중첩된 (하위) 복구 지점). ID는 스택 내의 논리적 ID 전송됩니다.

유형: String

필수사항: 아니요

CreatedBy

복구 시점을 생성하는 데 사용되는 백업 계획의 `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, `BackupRuleId`를 비롯하여, 복구 시점의 생성에 대한 식별 정보를 포함합니다.

유형: RecoveryPointCreator객체

필수 항목 여부: 아니요

CreationDate

복구 시점이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

EncryptionKeyArn

백업을 보호하는 데 사용되는 서버 측 암호화 키(예: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`)입니다.

유형: String

필수사항: 아니요

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

유형: String

필수사항: 아니요

IsEncrypted

지정된 복구 시점이 암호화된 경우 `TRUE`로 반환되거나, 복구 시점이 암호화되지 않은 경우 `FALSE`로 반환되는 부울 값입니다.

타입: 부울

필수 항목 여부: 아니요

IsParent

상위(복합) 복구 시점이라는 것을 나타내는 부울 값입니다.

타입: 부울

필수 항목 여부: 아니요

LastRestoreTime

복구 시점이 마지막으로 복원된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastRestoreTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

Lifecycle

수명 주기는 보호된 리소스가 콜드 스토리지로 전환되는 시기와 만료되는 시기를 정의합니다. AWS Backup 정의한 수명 주기에 따라 백업이 자동으로 전환되고 만료됩니다.

콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 따라서 '보존' 설정은 '콜드로 전환 전 보관 일수' 설정보다 90일 이상 커야 합니다. 백업이 콜드로 전환된 후 "콜드로 전환 전 보관 일수" 설정을 변경할 수 없습니다.

콜드 스토리지로 전환할 수 있는 리소스 유형은 리소스별 기능 가용성 테이블에 나열되어 있습니다. AWS Backup 다른 리소스 유형에서는 이 표현식을 무시합니다.

유형: Lifecycle객체

필수 항목 여부: 아니요

ParentRecoveryPointArn

상위 (복합) 복구 지점의 Amazon 리소스 이름 (ARN).

타입: 문자열

필수사항: 아니요

RecoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

유형: String

필수사항: 아니요

ResourceArn

리소스를 고유하게 식별하는 ARN입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

필수사항: 아니요

ResourceType

복구 지점으로 저장된 AWS 리소스 유형 (예: Amazon Elastic Block Store (Amazon EBS) 볼륨 또는 Amazon RDS (아마존 관계형 데이터베이스 서비스) 데이터베이스). Windows VSS(Volume Shadow Copy Service)의 경우, 지원되는 유일한 리소스 유형은 Amazon EC2입니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

SourceBackupVaultArn

복구 지점이 원래 복사된 백업 저장소입니다. 복구 시점이 동일한 계정에 복원되는 경우, 이 값은 `null`이 됩니다.

유형: String

필수사항: 아니요

Status

복구 시점의 상태를 지정하는 상태 코드입니다.

유형: String

유효 값: `COMPLETED | PARTIAL | DELETING | EXPIRED`

필수 여부: 아니요

StatusMessage

복구 지점의 현재 상태를 설명하는 메시지입니다.

타입: 문자열

필수사항: 아니요

VaultType

설명된 복구 지점이 저장되는 저장소의 유형입니다.

타입: 문자열

유효 값: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++

- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RecoveryPointByResource

서비스: AWS Backup

저장된 복구 시점의 세부 정보를 포함합니다.

내용

BackupSizeBytes

백업의 크기(바이트 단위)입니다.

유형: Long

필수 여부: 아니요

BackupVaultName

백업이 저장되는 논리 컨테이너의 이름입니다. 백업 저장소는 백업 저장소가 생성된 AWS 리전 및 백업 저장소를 생성하는 데 사용된 계정에 고유 이름으로 식별됩니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: No

CreationDate

복구 시점이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

EncryptionKeyArn

백업을 보호하는 데 사용되는 서버 측 암호화 키(예: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`)입니다.

유형: String

필수사항: 아니요

IsParent

상위(복합) 복구 시점이라는 것을 나타내는 부울 값입니다.

타입: 부울

필수 항목 여부: 아니요

ParentRecoveryPointArn

상위 (복합) 복구 지점의 Amazon 리소스 이름 (ARN).

타입: 문자열

필수사항: 아니요

RecoveryPointArn

복구 시점을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

유형: String

필수사항: 아니요

ResourceName

지정된 백업에 속하는 리소스의 고유하지 않은 이름.

타입: 문자열

필수사항: 아니요

Status

복구 시점의 상태를 지정하는 상태 코드입니다.

유형: String

유효 값: `COMPLETED | PARTIAL | DELETING | EXPIRED`

필수 여부: 아니요

StatusMessage

복구 지점의 현재 상태를 설명하는 메시지입니다.

타입: 문자열

필수사항: 아니요

VaultType

설명된 복구 지점이 저장되는 저장소의 유형입니다.

타입: 문자열

유효 값: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RecoveryPointCreator

서비스: AWS Backup

복구 지점 백업을 시작하는 데 AWS Backup 사용된 백업 계획 및 규칙에 대한 정보가 들어 있습니다.

내용

BackupPlanArn

백업 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)(예: `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`)입니다.

유형: String

필수사항: 아니요

BackupPlanId

백업 계획을 고유하게 식별합니다.

유형: String

필수사항: 아니요

BackupPlanVersion

버전 ID는 임의로 생성되는 최대 1024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 버전 ID는 편집할 수 없습니다.

유형: String

필수사항: 아니요

BackupRuleId

다양한 리소스의 백업을 예약하는 데 사용되는 규칙을 고유하게 식별합니다.

유형: String

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RecoveryPointMember

서비스: AWS Backup

상위(복합) 복구 시점의 하위(중첩) 복구 시점인 복구 지점입니다. 이러한 복구 시점은 상위(복합) 복구 시점과의 연결을 해제할 수 있으며, 이 경우 해당 복구 시점은 더 이상 멤버가 아닙니다.

내용

BackupVaultName

백업 저장소 (백업이 저장되는 논리적 컨테이너) 의 이름

유형: String

패턴: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: No

RecoveryPointArn

상위 (복합) 복구 지점의 Amazon 리소스 이름 (ARN).

타입: 문자열

필수사항: 아니요

ResourceArn

저장된 리소스를 고유하게 식별하는 Amazon 리소스 이름 (ARN).

타입: 문자열

필수사항: 아니요

ResourceType

복구 지점으로 저장되는 AWS 리소스 유형.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RecoveryPointSelection

서비스: AWS Backup

리소스 유형 또는 백업 저장소 같은 리소스 집합을 할당하기 위한 기준을 지정합니다.

내용

DateRange

이것은 FromDate ToDate: DateTime 및 :를 포함하는 리소스 DateTime 필터입니다. 두 값은 모두 필수입니다. 미래 DateTime 값은 허용되지 않습니다.

날짜 및 시간은 Unix 형식 및 협정 세계시(UTC)로 표시되며, 밀리초 단위로 정확합니다(밀리초는 선택 사항). 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: DateRange객체

필수 항목 여부: 아니요

ResourceIdentifiers

리소스 선택에 포함되는 리소스입니다(리소스 유형 및 저장소 포함).

유형: String 배열

필수 여부: 아니요

VaultNames

선택한 복구 시점이 포함된 저장소의 이름입니다.

유형: String 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ReportDeliveryChannel

서비스: AWS Backup

보고서를 전달할 위치에 대한 보고서 계획, 특히 Amazon S3 버킷 이름, S3 키 접두사 및 보고서 형식에 대한 정보가 들어 있습니다.

내용

S3BucketName

보고서를 수신하는 S3 버킷의 고유 이름입니다.

유형: String

필수 항목 여부: 예

Formats

보고서 형식: `CSV`, `JSON`, 또는 둘 다 지정하지 않은 경우 기본 형식은 `CSV`입니다.

유형: String 배열

필수 여부: 아니요

S3KeyPrefix

AWS Backup Audit Manager가 Amazon S3에 보고서를 전송하는 위치의 접두사입니다. 접두사는 s3://your-bucket-name`prefix`/backup/US-WEST-2/년/월/일/보고서 이름 경로의 이 부분입니다. 지정하지 않으면 접두사가 없습니다.

유형: String

필수 항목 여부: 아니요

참고

언어별 SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오. AWS

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ReportDestination

서비스: AWS Backup

보고서 대상과 관련된 보고서 작업의 정보를 포함합니다.

내용

S3BucketName

보고서를 수신하는 Amazon S3 버킷의 고유 이름입니다.

유형: String

필수사항: 아니요

S3Keys

S3 버킷의 보고서를 고유하게 식별하는 객체 키입니다.

유형: String 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ReportJob

서비스: AWS Backup

보고서 작업에 대한 세부 정보를 포함합니다. 보고서 작업은 보고서 계획을 기반으로 보고서를 컴파일하고 이를 Amazon S3에 게시합니다.

내용

CompletionTime

보고서 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreationTime

보고서 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

ReportDestination

보고서 작업이 보고서를 게시하는 대상의 S3 버킷 이름과 S3 키입니다.

유형: ReportDestination객체

필수 항목 여부: 아니요

ReportJobId

보고서 작업의 식별자입니다. 임의로 생성되는 최대 1,024바이트의 UTF-8 인코딩된 고유한 Unicode 문자열입니다. 보고서 작업 ID는 편집할 수 없습니다.

유형: String

필수사항: 아니요

ReportPlanArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

ReportTemplate

보고서에 대한 보고서 템플릿을 식별합니다. 보고서는 보고서 템플릿을 사용하여 작성됩니다. 보고서 템플릿은 다음과 같습니다.

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

유형: String

필수사항: 아니요

Status

보고서 작업의 상태입니다. 상태는 다음과 같습니다.

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED`는 지정된 대상에서 보고서를 검토할 수 있다는 의미입니다. 상태가 `FAILED`인 경우, `StatusMessage`를 검토하여 이유를 확인하세요.

유형: String

필수사항: 아니요

StatusMessage

보고서 작업의 상태를 설명하는 메시지입니다.

유형: String

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ReportPlan

서비스: AWS Backup

보고서 계획에 대한 세부 정보를 포함합니다.

내용

CreationTime

보고서 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

DeploymentStatus

보고서 계획의 배포 상태입니다. 상태는 다음과 같습니다.

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

유형: String

필수사항: 아니요

LastAttemptedExecutionTime

이 보고서 계획과 관련된 보고서 작업을 실행하려고 마지막으로 시도한 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastAttemptedExecutionTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

LastSuccessfulExecutionTime

이 보고서 계획과 관련된 보고서 작업을 마지막으로 실행한 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastSuccessfulExecutionTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

ReportDeliveryChannel

보고서를 전송하는 위치와 방법, 특히 Amazon S3 버킷 이름, S3 키 접두사 및 보고서 형식에 대한 정보가 들어 있습니다.

유형: ReportDeliveryChannel객체

필수 항목 여부: 아니요

ReportPlanArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

ReportPlanDescription

보고서 계획에 대한 최대 1,024자의 설명(선택 사항)입니다.

유형: String

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `.*\S.*`

Required: No

ReportPlanName

보고서 계획의 고유 이름입니다. 이 이름은 문자로 시작하고 문자(a~z, A~Z), 숫자(0~9) 및 밑줄(_)로 구성된 1~256자 사이입니다.

유형: String

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `[a-zA-Z][_a-zA-Z0-9]*`

Required: No

ReportSetting

보고서에 대한 보고서 템플릿을 식별합니다. 보고서는 보고서 템플릿을 사용하여 작성됩니다. 보고서 템플릿은 다음과 같습니다.

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

보고서 템플릿이 `RESOURCE_COMPLIANCE_REPORT` `CONTROL_COMPLIANCE_REPORT` OR인 경우 이 API 리소스는 AWS 리전 및 프레임워크의 보고서 적용 범위도 설명합니다.

유형: ReportSetting객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

ReportSetting

서비스: AWS Backup

보고서 설정에 대한 세부 정보를 포함합니다.

내용

ReportTemplate

보고서에 대한 보고서 템플릿을 식별합니다. 보고서는 보고서 템플릿을 사용하여 작성됩니다. 보고서 템플릿은 다음과 같습니다.

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

유형: String

필수 항목 여부: 예

Accounts

보고서에 포함될 계정입니다.

모든 조직 단위를 `ROOT` 포함하려면 문자열 값 1을 사용합니다.

유형: String 배열

필수 여부: 아니요

FrameworkArns

보고서에서 다루는 프레임워크의 Amazon 리소스 이름(ARN)입니다.

유형: String 배열

필수 여부: 아니요

NumberOfFrameworks

보고서에서 다루는 프레임워크의 수입니다.

유형: 정수

필수 항목 여부: 아니요

OrganizationUnits

보고서에 포함될 조직 단위입니다.

유형: String 배열

필수 여부: 아니요

Regions

보고서에 포함될 리전입니다.

와일드카드를 문자열 값으로 사용하여 모든 지역을 포함하세요.

유형: String 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreJobCreator

서비스: AWS Backup

AWS Backup 이 복원 작업을 시작하는 데 사용한 복원 테스트 계획에 대한 정보가 포함되어 있습니다.

내용

RestoreTestingPlanArn

복원 테스트 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreJobsListMember

서비스: AWS Backup

복원 작업에 대한 메타데이터를 포함합니다.

내용

AccountId

복원 작업을 소유한 계정 ID입니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

BackupSizeInBytes

복원된 리소스의 크기(바이트 단위)입니다.

유형: Long

필수 여부: 아니요

CompletionDate

복구 시점을 복원하기 위한 작업이 완료된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CompletionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

CreatedBy

복원 작업 생성에 대한 식별 정보가 포함되어 있습니다.

유형: RestoreJobCreator객체

필수 항목 여부: 아니요

CreatedResourceArn

리소스를 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다. ARN의 형식은 리소스 유형에 따라 달라집니다.

유형: String

필수사항: 아니요

CreationDate

복원 작업이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

DeletionStatus

복원 테스트에서 생성된 데이터의 상태를 나타냅니다. 상태는 `Deleting`, `Failed` 또는 `Successful`일 수 있습니다.

타입: 문자열

유효 값: `DELETING | FAILED | SUCCESSFUL`

필수 여부: 아니요

DeletionStatusMessage

복원 작업 삭제 상태를 설명합니다.

타입: 문자열

필수사항: 아니요

ExpectedCompletionTimeMinutes

복구 시점을 복원하는 작업에 소요될 것으로 예상되는 시간(분)입니다.

유형: Long

필수 여부: 아니요

IamRoleArn

대상 복구 시점을 생성하는 데 사용되는 IAM 역할 ARN을 지정합니다(예: `arn:aws:iam::123456789012:role/S3Access`).

유형: String

필수사항: 아니요

PercentDone

작업 상태를 쿼리할 때 작업의 예상 완료율을 포함합니다.

유형: String

필수사항: 아니요

RecoveryPointArn

복구 시점을 고유하게 식별하는 ARN입니다(예: `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`).

유형: String

필수사항: 아니요

RecoveryPointCreationDate

복구 시점이 생성된 날짜입니다.

유형: 타임스탬프

필수 여부: 아니요

ResourceType

나열된 복원 작업의 리소스 유형입니다(예: Amazon Elastic Block Store(Amazon EBS) 볼륨 또는 Amazon Relational Database Service(Amazon RDS) 데이터베이스). Windows Volume Shadow Copy Service(VSS)의 경우, 지원되는 유일한 리소스 유형은 Amazon EC2입니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

RestoreJobId

복구 시점을 복원하는 작업을 고유하게 식별합니다.

유형: String

필수사항: 아니요

Status

복구 지점을 AWS Backup 복원하기 위해 시작한 작업의 상태를 지정하는 상태 코드입니다.

타입: 문자열

유효 값: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

필수 여부: 아니요

StatusMessage

복구 시점을 복원하기 위한 작업의 상태를 설명하는 자세한 메시지입니다.

유형: String

필수사항: 아니요

ValidationStatus

표시된 복원 작업에 대한 검증 실행 상태입니다.

타입: 문자열

유효 값: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

필수 여부: 아니요

ValidationStatusMessage

표시된 복원 작업에 대한 검증 실행 상태를 설명합니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreJobSummary

서비스: AWS Backup

최근 30일 이내에 생성되거나 실행된 복원 작업의 요약입니다.

반환된 요약에는 지역, 계정, 주,,, ResourceType MessageCategory StartTime EndTime, 포함된 작업 수 등이 포함될 수 있습니다.

내용

AccountId

요약 내의 작업을 소유한 계정 ID입니다.

유형: String

패턴: `^[0-9]{12}$`

Required: No

Count

작업 요약의 작업 수를 나타낸 값입니다.

유형: 정수

필수 항목 여부: 아니요

EndTime

작업 종료 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

Region

작업 요약 내 AWS 지역.

타입: 문자열

필수사항: 아니요

ResourceType

이 값은 지정된 리소스 유형의 작업 수입니다. `GetSupportedResourceTypes` 요청은 지원되는 리소스 유형의 문자열을 반환합니다.

유형: String

패턴: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

StartTime

작업 시작 시간을 숫자 형식으로 나타낸 시간 값입니다.

이 값은 Unix 형식의 협정 세계시(UTC)로 표시된 시간이며, 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

State

이 값은 지정된 상태의 작업 수입니다.

타입: 문자열

유효 값: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingPlanForCreate

서비스: AWS Backup

여기에는 복원 테스트 계획에 대한 메타데이터가 포함되어 있습니다.

내용

RecoveryPointSelection

RecoveryPointSelection매개변수 5개 (필수 3개, 선택 2개) 가 있습니다. 지정한 값에 따라 복원 테스트에 포함되는 복구 지점이 결정됩니다. 내에 최신 복구 지점을 지정할지 SelectionWindowDays 또는 임의 복구 지점을 원하는지 여부를 표시해야 하며, 복구 지점을 선택할 수 있는 저장소를 지정해야 합니다. Algorithm IncludeVaults

Algorithm(필수) 유효한 값: "LATEST_WITHIN_WINDOW" 또는 "RANDOM_WITHIN_WINDOW”.

Recovery point types(필수) 유효한 값: "SNAPSHOT" 및/또는 "CONTINUOUS”. 스냅샷 복구 지점만 복원하는 경우 포함CONTINUOUS, 연속 복구 시점 복원 (특정 시점 복원/PITR) 에 포함, 스냅샷 또는 연속 복구 지점 복원에 둘 다 사용합니다. SNAPSHOT 복구 지점은 의 값에 Algorithm 따라 결정됩니다.

IncludeVaults(필수). 백업 저장소를 하나 이상 포함해야 합니다. 와일드카드 ["*"] 또는 특정 ARN을 사용하십시오.

SelectionWindowDays(선택 사항) 값은 1~365 사이의 정수 (일수) 여야 합니다. 포함되지 않은 경우 기본값은 입니다. 30

ExcludeVaults(선택 사항). 하나 이상의 특정 백업 저장소 ARN을 입력하여 해당 저장소의 콘텐츠를 복원 자격에서 제외하도록 선택할 수 있습니다. 또는 선택기 목록을 포함할 수 있습니다. 이 매개 변수와 해당 값이 포함되지 않은 경우 기본적으로 빈 목록이 됩니다.

유형: RestoreTestingRecoveryPointSelection객체

필수 여부: 예

RestoreTestingPlanName

RestoreTestingPlanName 는 복원 테스트 계획의 이름을 나타내는 고유한 문자열입니다. 이 값은 만든 후에는 변경할 수 없으며 영숫자와 밑줄로만 구성되어야 합니다.

타입: 문자열

필수 항목 여부: 예

ScheduleExpression

복원 테스트 계획이 실행될 때 지정된 시간대의 cron 표현식입니다.

타입: 문자열

필수 항목 여부: 예

ScheduleExpressionTimezone

선택 사항입니다. 예약 표현식이 설정된 표준시간대입니다. 기본적으로 UTC로 ScheduleExpressions 표시됩니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowHours

기본값은 24시간입니다.

복원 테스트가 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(시간 단위)입니다. 이 값은 선택 사항입니다. 이 값을 포함하는 경우 이 파라미터의 최댓값은 168시간(1주)입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingPlanForGet

서비스: AWS Backup

여기에는 복원 테스트 계획에 대한 메타데이터가 포함되어 있습니다.

내용

CreationTime

복원 테스트 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 예

RecoveryPointSelection

복구 시점 유형 또는 백업 볼트와 같은 리소스 세트를 할당하기 위해 지정된 기준입니다.

유형: RestoreTestingRecoveryPointSelection객체

필수 여부: 예

RestoreTestingPlanArn

복원 테스트 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

필수 항목 여부: 예

RestoreTestingPlanName

복원 테스트 계획 이름.

타입: 문자열

필수 항목 여부: 예

ScheduleExpression

복원 테스트 계획이 실행될 때 지정된 시간대의 cron 표현식입니다.

타입: 문자열

필수 항목 여부: 예

CreatorRequestId

요청을 식별하며 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 합니다. 요청에 기존 백업 계획과 일치하는 `CreatorRequestId`가 포함된 경우, 해당 계획이 반환됩니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

LastExecutionTime

지정된 복원 테스트 계획을 사용하여 복원 테스트를 마지막으로 실행한 시간입니다. 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastExecutionDate`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

LastUpdateTime

복원 테스트 계획이 업데이트된 날짜 및 시간입니다. 이 업데이트는 Unix 형식 및 협정 세계시(UTC)로 표시됩니다. `LastUpdateTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

ScheduleExpressionTimezone

선택 사항입니다. 예약 표현식이 설정된 표준시간대입니다. 기본적으로 UTC로 ScheduleExpressions 표시됩니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowHours

기본값은 24시간입니다.

복원 테스트가 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(시간 단위)입니다. 이 값은 선택 사항입니다. 이 값을 포함하는 경우 이 파라미터의 최댓값은 168시간(1주)입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingPlanForList

서비스: AWS Backup

여기에는 복원 테스트 계획에 대한 메타데이터가 포함되어 있습니다.

내용

CreationTime

복원 테스트 계획이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 예

RestoreTestingPlanArn

복원 테스트 계획을 고유하게 식별하는 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

필수 항목 여부: 예

RestoreTestingPlanName

복원 테스트 계획 이름.

타입: 문자열

필수 항목 여부: 예

ScheduleExpression

복원 테스트 계획이 실행될 때 지정된 시간대의 cron 표현식입니다.

타입: 문자열

필수 항목 여부: 예

LastExecutionTime

지정된 복원 테스트 계획을 사용하여 복원 테스트를 마지막으로 실행한 시간입니다. 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `LastExecutionDate`의 값은 밀리초 단위로 정확합니

다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

LastUpdateTime

복원 테스트 계획이 업데이트된 날짜 및 시간입니다. 이 업데이트는 Unix 형식 및 협정 세계시(UTC)로 표시됩니다. `LastUpdateTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087을 나타냅니다.

유형: 타임스탬프

필수 여부: 아니요

ScheduleExpressionTimezone

선택 사항입니다. 예약 표현식이 설정된 표준시간대입니다. 기본적으로 UTC로 ScheduleExpressions 표시됩니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowHours

기본값은 24시간입니다.

복원 테스트가 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(시간 단위)입니다. 이 값은 선택 사항입니다. 이 값을 포함하는 경우 이 파라미터의 최댓값은 168시간(1주)입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK

- AWS 루비 V3용 SDK

RestoreTestingPlanForUpdate

서비스: AWS Backup

여기에는 복원 테스트 계획에 대한 메타데이터가 포함되어 있습니다.

내용

RecoveryPointSelection

필수 사항: `Algorithm`, `RecoveryPointTypes`, `IncludeVaults`(하나 이상)

선택 사항: SelectionWindowDays(지정되지 않은 경우 '30'); `ExcludeVaults` (나열되지 않은 경우 기본적으로 빈 목록으로 설정됨).

유형: RestoreTestingRecoveryPointSelection객체

필수 항목 여부: 아니요

ScheduleExpression

복원 테스트 계획이 실행될 때 지정된 시간대의 cron 표현식입니다.

타입: 문자열

필수사항: 아니요

ScheduleExpressionTimezone

선택 사항입니다. 예약 표현식이 설정된 표준시간대입니다. 기본적으로 UTC로 ScheduleExpressions 표시됩니다. 이를 지정된 표준시간대로 수정할 수 있습니다.

타입: 문자열

필수사항: 아니요

StartWindowHours

기본값은 24시간입니다.

복원 테스트가 예약된 후 작업이 성공적으로 시작되지 않은 경우 취소되기 전까지의 시간(시간 단위)입니다. 이 값은 선택 사항입니다. 이 값을 포함하는 경우 이 파라미터의 최댓값은 168시간(1주)입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingRecoveryPointSelection

서비스: AWS Backup

RecoveryPointSelection매개변수 5개 (필수 3개, 선택 2개) 가 있습니다. 지정한 값에 따라 복원 테스트에 포함되는 복구 지점이 결정됩니다. 내에 최신 복구 지점을 사용할지 SelectionWindowDays 아니면 임의 복구 지점을 원하는지 여부를 표시해야 하며, 복구 지점을 선택할 수 있는 저장소를 지정해야 합니다. Algorithm IncludeVaults

Algorithm(필수) 유효한 값: "LATEST_WITHIN_WINDOW" 또는 "RANDOM_WITHIN_WINDOW”.

Recovery point types(필수) 유효한 값: "SNAPSHOT" 및/또는 "CONTINUOUS”. 스냅샷 복구 지점만 복원하는 경우 포함CONTINUOUS, 연속 복구 시점 복원 (특정 시점 복원/PITR) 에 포함, 스냅샷 또는 연속 복구 지점 복원에 둘 다 사용합니다. SNAPSHOT 복구 지점은 의 값에 Algorithm 따라 결정됩니다.

IncludeVaults(필수). 백업 저장소를 하나 이상 포함해야 합니다. 와일드카드 ["*"] 또는 특정 ARN을 사용하십시오.

SelectionWindowDays(선택 사항) 값은 1~365 사이의 정수 (일수) 여야 합니다. 포함되지 않은 경우 기본값은 입니다. 30

ExcludeVaults(선택 사항). 하나 이상의 특정 백업 저장소 ARN을 입력하여 해당 저장소의 콘텐츠를 복원 자격에서 제외할 수 있습니다. 또는 선택기 목록을 포함할 수 있습니다. 이 매개 변수와 해당 값이 포함되지 않은 경우 기본적으로 빈 목록이 됩니다.

내용

Algorithm

사용할 수 있는 값은 'LATEST_WITHIN_WINDOW' 또는 'RANDOM_WITHIN_WINDOW'입니다.

타입: 문자열

유효 값: LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW

필수 여부: 아니요

ExcludeVaults

허용되는 값에는 특정 ARN 또는 선택기 목록이 포함됩니다. 목록에 없는 경우 기본적으로 빈 목록이 됩니다.

유형: String 배열

필수 여부: 아니요

IncludeVaults

허용되는 값에는 와일드카드["*"] 또는 특정 ARN 또는 ARN 와일드카드 대체["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]가 있습니다.

유형: String 배열

필수 여부: 아니요

RecoveryPointTypes

복구 시점의 유형은 다음과 같습니다.

스냅샷 복구 지점만 복원하는 경우 포함CONTINUOUS, 연속 복구 지점 복원 (지정 시간 복원/PITR)에는 포함, 스냅샷 또는 연속 복구 지점을 복원하려면 둘 다 사용하십시오. SNAPSHOT 복구 지점은의 값에 Algorithm 따라 결정됩니다.

유형: 문자열 어레이

유효 값: CONTINUOUS | SNAPSHOT

필수 여부: 아니요

SelectionWindowDays

허용되는 값은 1에서 365까지의 정수입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingSelectionForCreate

서비스: AWS Backup

여기에는 복원 테스트 선택 항목에 대한 특정 메타데이터가 포함되어 있습니다.

ProtectedResourceType Amazon EBS 또는 Amazon EC2와 같이 필요합니다.

이것은 `RestoreTestingSelectionName`, `ProtectedResourceType` 및 다음 중 하나로 구성됩니다.

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

각 보호된 리소스 유형은 단일 값을 가질 수 있습니다.

복원 테스트 선택 항목에는 `ProtectedResourceArns`에 대한 와일드카드 값('*')과 함께 `ProtectedResourceConditions`를 포함할 수 있습니다. 또는 `ProtectedResourceArns`에 최대 30개의 특정 보호된 리소스 ARN을 포함할 수 있습니다.

`ProtectedResourceConditions`의 예로는 `StringEquals` 및 `StringNotEquals`가 있습니다.

내용

IamRoleArn

AWS Backup 이 대상 리소스를 생성하기 위해 사용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수 항목 여부: 예

ProtectedResourceType

복원 테스트 선택 항목에 포함된 AWS 리소스 유형 (예: Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스)

지원되는 리소스 유형으로 허용되는 것은 다음과 같습니다.

- Amazon Aurora의 `Aurora`
- Amazon DocumentDB(MongoDB 호환)의 `DocumentDB`

- Amazon DynamoDB의 DynamoDB
- Amazon Elastic Block Store의 EBS
- Amazon Elastic Compute Cloud의 EC2
- Amazon Elastic File System의 EFS
- Amazon FSx의 FSx
- Amazon Neptune의 Neptune
- Amazon Relational Database Service의 RDS
- Amazon S3용 S3

타입: 문자열

필수 항목 여부: 예

RestoreTestingSelectionName

관련 복원 테스트 계획에 속하는 복원 테스트 선택 항목의 고유한 이름.

타입: 문자열

필수 항목 여부: 예

ProtectedResourceArns

각 보호된 리소스는 자체 ARN(예: ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]) 또는 와일드카드(ProtectedResourceArns: ["*"])로 필터링할 수 있지만 둘 다 사용할 수는 없습니다.

유형: String 배열

필수 여부: 아니요

ProtectedResourceConditions

와일드카드를 포함시킨 경우 다음과 같은 ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }] 리소스 조건을 포함할 수 있습니다. ProtectedResourceArns

유형: ProtectedResourceConditions객체

필수 항목 여부: 아니요

RestoreMetadataOverrides

`RestoreTestingSelection`의 본문에 `RestoreMetadataOverrides` 파라미터를 포함하여 특정 복원 메타데이터 키를 재정의할 수 있습니다. 키 값은 대/소문자를 구분하지 않습니다.

복원 테스트 추론 메타데이터의 전체 목록을 참조하세요.

유형: 문자열 간 맵

필수 여부: 아니요

ValidationWindowHours

데이터에 대한 검증 스크립트를 실행하는 데 사용할 수 있는 시간(1~168)입니다. 데이터는 검증 스크립트 완료 시 또는 지정된 보존 기간 종료 시(둘 중 먼저 도래하는 시점)에 삭제됩니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingSelectionForGet

서비스: AWS Backup

여기에는 복원 테스트 선택 항목에 대한 메타데이터가 포함되어 있습니다.

내용

CreationTime

복원 테스트 선택 항목이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 예

IamRoleArn

AWS Backup 이 대상 리소스를 생성하기 위해 사용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수 항목 여부: 예

ProtectedResourceType

AWS 리소스 테스트 선택 항목에 포함된 리소스 유형 (예: Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스)

타입: 문자열

필수 항목 여부: 예

RestoreTestingPlanName

RestoreTestingPlanName 는 복원 테스트 계획의 이름을 나타내는 고유한 문자열입니다.

타입: 문자열

필수 항목 여부: 예

RestoreTestingSelectionName

관련 복원 테스트 계획에 속하는 복원 테스트 선택 항목의 고유한 이름입니다.

타입: 문자열

필수 항목 여부: 예

CreatorRequestId

요청을 식별하며 작업을 두 번 실행할 위험 없이 실패한 요청을 다시 시도할 수 있도록 합니다. 요청에 기존 백업 계획과 일치하는 CreatorRequestId가 포함된 경우, 해당 계획이 반환됩니다. 이 파라미터는 선택 사항입니다.

이를 사용할 경우 이 파라미터에는 1~50개의 영숫자 또는 '-_.' 문자를 포함해야 합니다.

타입: 문자열

필수사항: 아니요

ProtectedResourceArns

특정 ARN(예: ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."])을 포함하거나 와일드카드(ProtectedResourceArns: ["*"])를 포함할 수 있지만 둘 다 포함할 수는 없습니다.

유형: String 배열

필수 여부: 아니요

ProtectedResourceConditions

리소스 테스트 선택 시 이 파라미터는 StringEquals 또는 StringNotEquals와 같은 특정 조건을 기준으로 필터링합니다.

유형: ProtectedResourceConditions객체

필수 항목 여부: 아니요

RestoreMetadataOverrides

RestoreTestingSelection의 본문에 RestoreMetadataOverrides 파라미터를 포함하여 특정 복원 메타데이터 키를 재정의할 수 있습니다. 키 값은 대/소문자를 구분하지 않습니다.

복원 테스트 추론 메타데이터의 전체 목록을 참조하세요.

유형: 문자열 간 맵

필수 여부: 아니요

ValidationWindowHours

데이터에 대한 검증 스크립트를 실행하는 데 사용할 수 있는 시간(1~168)입니다. 데이터는 검증 스크립트 완료 시 또는 지정된 보존 기간 종료 시(둘 중 먼저 도래하는 시점)에 삭제됩니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingSelectionForList

서비스: AWS Backup

여기에는 복원 테스트 선택 항목에 대한 메타데이터가 포함되어 있습니다.

내용

CreationTime

복원 테스트 선택 항목이 생성된 날짜 및 시간(Unix 형식 및 협정 세계시(UTC))입니다. `CreationTime`의 값은 밀리초 단위로 정확합니다. 예를 들어, 1516925490.087이라는 값은 2018년 1월 26일 금요일 오전 12:11:30.087를 나타냅니다.

유형: 타임스탬프

필수 여부: 예

IamRoleArn

AWS Backup 이 대상 리소스를 생성하기 위해 사용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:iam::123456789012:role/S3Access`).

타입: 문자열

필수 항목 여부: 예

ProtectedResourceType

복원 테스트 선택 항목에 포함된 AWS 리소스 유형 (예: Amazon EBS 볼륨 또는 Amazon RDS 데이터베이스)

타입: 문자열

필수 항목 여부: 예

RestoreTestingPlanName

복원 테스트 계획의 이름을 나타내는 고유한 문자열입니다.

생성한 후에는 이름을 변경할 수 없습니다. 이름은 영숫자와 밑줄로만 구성해야 합니다. 최대 길이는 50자입니다.

타입: 문자열

필수 항목 여부: 예

RestoreTestingSelectionName

복원 테스트 선택 항목의 고유 이름입니다.

타입: 문자열

필수 항목 여부: 예

ValidationWindowHours

이 값은 선택적 검증을 완료할 수 있도록 복원 테스트 후 데이터가 보존되는 시간(시간 단위)을 나타냅니다.

허용되는 값은 0에서 168(7일) 사이의 정수입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

RestoreTestingSelectionForUpdate

서비스: AWS Backup

여기에는 복원 테스트 선택 항목에 대한 메타데이터가 포함되어 있습니다.

내용

IamRoleArn

AWS Backup 이 대상 리소스를 생성하기 위해 사용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다(예: `arn:aws:iam::123456789012:role/S3Access`).

유형: String

필수사항: 아니요

ProtectedResourceArns

특정 ARN(예: `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`)의 목록을 포함하거나 와일드카드(`ProtectedResourceArns: ["*"]`)를 포함할 수 있지만 둘 다 포함할 수는 없습니다.

유형: String 배열

필수 여부: 아니요

ProtectedResourceConditions

태그를 사용하여 복원 테스트 계획의 리소스에 대해 정의하는 조건.

예를 들어 `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`입니다. 조건 연산자는 대/소문자를 구분합니다.

유형: ProtectedResourceConditions객체

필수 항목 여부: 아니요

RestoreMetadataOverrides

`RestoreTestingSelection`의 본문에 `RestoreMetadataOverrides` 파라미터를 포함하여 특정 복원 메타데이터 키를 재정의할 수 있습니다. 키 값은 대/소문자를 구분하지 않습니다.

복원 테스트 추론 메타데이터의 전체 목록을 참조하세요.

유형: 문자열 간 맵

필수 여부: 아니요

ValidationWindowHours

이 값은 선택적 검증을 완료할 수 있도록 복원 테스트 후 데이터가 보존되는 시간(시간 단위)을 나타냅니다.

허용되는 값은 0에서 168(7일) 사이의 정수입니다.

유형: 정수

필수 항목 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

AWS Backup gateway

다음 데이터 형식이 AWS Backup gateway에서 지원됩니다.

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

서비스: AWS Backup gateway

게이트웨이의 대역폭 속도 제한 간격을 설명합니다. 대역폭 속도 제한 일정은 하나 이상의 대역폭 속도 제한 간격으로 구성됩니다. 대역폭 속도 제한 간격은 일주일 중 1일 이상의 기간을 정의하며, 이 기간에는 업로드, 다운로드 또는 두 가지 모두에 대해 대역폭 속도 제한이 지정됩니다.

내용

DaysOfWeek

대역폭 속도 제한 간격의 요일 구성 요소로, 0에서 6까지의 서수로 표시됩니다. 여기서 0은 일요일, 6은 토요일을 나타냅니다.

유형: 정수 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 5개입니다.

유효한 범위: 최소값 0. 최대값은 6입니다.

필수 여부: 예

EndHourOfDay

하루 중 대역폭 속도 제한 간격을 종료하는 시간입니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 23입니다.

필수 여부: 예

EndMinuteOfHour

대역폭 속도 제한 간격을 종료하는 시간(분)입니다.

> **Important**
>
> 대역폭 속도 제한 간격은 지정된 분이 끝날 때 종료됩니다. 한 시간이 끝날 때 간격을 종료하려면 값 59를 사용합니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 59입니다.

필수 여부: 예

StartHourOfDay

하루 중 대역폭 속도 제한 간격을 시작하는 시간입니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 23입니다.

필수 여부: 예

StartMinuteOfHour

대역폭 속도 제한 간격을 시작하는 시간(분)입니다. 간격은 해당 분이 시작할 때 시작됩니다. 시간이 시작될 때 정확히 간격을 시작하려면 값 `0`을 사용합니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 59입니다.

필수 여부: 예

AverageUploadRateLimitInBitsPerSec

대역폭 속도 제한 간격의 평균 업로드 속도 제한 구성 요소입니다(초당 비트 수). 업로드 속도 제한이 설정되지 않은 경우 이 필드는 응답에 나타나지 않습니다.

타입: Long

유효한 범위: 최소값은 51200입니다. 최대값은 8000000000000입니다.

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Gateway

서비스: AWS Backup gateway

게이트웨이는 고객 네트워크에서 실행되어 AWS 클라우드의 백업 스토리지에 대한 원활한 연결을 제공하는 AWS Backup 게이트웨이 어플라이언스입니다.

내용

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. `ListGateways`작업을 사용하여 계정 및 AWS 리전의 게이트웨이 목록을 반환하십시오.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

GatewayDisplayName

게이트웨이의 표시 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

GatewayType

게이트웨이의 유형입니다.

타입: 문자열

유효 값: `BACKUP_VM`

필수 여부: 아니요

HypervisorId

게이트웨이의 하이퍼바이저 ID입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

필수 여부: 아니요

LastSeenTime

AWS Backup 게이트웨이가 게이트웨이와 마지막으로 통신한 시간 (Unix 형식 및 UTC 시간).

유형: 타임스탬프

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

GatewayDetails

서비스: AWS Backup gateway

게이트웨이 세부 정보입니다.

내용

GatewayArn

게이트웨이의 Amazon 리소스 이름(ARN)입니다. `ListGateways` 작업을 사용하여 계정 및 AWS 리전의 게이트웨이 목록을 반환합니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 180입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

GatewayDisplayName

게이트웨이의 표시 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

GatewayType

게이트웨이 유형의 유형입니다.

타입: 문자열

유효 값: `BACKUP_VM`

필수 여부: 아니요

HypervisorId

게이트웨이의 하이퍼바이저 ID입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

필수 여부: 아니요

LastSeenTime

AWS Backup 게이트웨이가 클라우드와 마지막으로 통신한 시간을 Unix 형식 및 UTC 시간으로 보여주는 세부 정보

유형: 타임스탬프

필수 여부: 아니요

MaintenanceStartTime

주중의 요일 및 시간을 포함한 게이트웨이의 주별 유지 관리 시작 시간을 반환합니다. 참고로, 값은 게이트웨이의 표준시간대를 기준으로 합니다. 주별 또는 월별일 수 있습니다.

유형: MaintenanceStartTime객체

필수 항목 여부: 아니요

NextUpdateAvailabilityTime

게이트웨이의 다음 업데이트 이용 가능 시간을 보여 주는 세부 정보입니다.

유형: 타임스탬프

필수 여부: 아니요

VpcEndpoint

게이트웨이가 백업 게이트웨이의 클라우드에 연결하기 위해 사용하는 Virtual Private Cloud(VPC) 엔드포인트의 DNS 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Hypervisor

서비스: AWS Backup gateway

게이트웨이가 연결할 하이퍼바이저의 권한을 나타냅니다.

하이퍼바이저는 가상 머신을 생성 및 관리하고, 가상 머신에 리소스를 할당하는 하드웨어, 소프트웨어 또는 펌웨어입니다.

내용

Host

하이퍼바이저의 서버 호스트입니다. 이는 IP 주소 또는 정규화된 도메인 이름(FQDN)일 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 128.

패턴: `^.+$`

Required: No

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

KmsKeyArn

하이퍼바이저를 암호화하는 AWS Key Management Service 데 사용되는 Amazon 리소스 이름(ARN).

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Required: No

Name

하이퍼바이저의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

State

하이퍼바이저의 상태입니다.

타입: 문자열

유효 값: `PENDING | ONLINE | OFFLINE | ERROR`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

HypervisorDetails

서비스: AWS Backup gateway

지정된 하이퍼바이저의 세부 정보입니다. 하이퍼바이저는 가상 머신을 생성 및 관리하고, 가상 머신에 리소스를 할당하는 하드웨어, 소프트웨어 또는 펌웨어입니다.

내용

Host

하이퍼바이저의 서버 호스트입니다. 이는 IP 주소 또는 정규화된 도메인 이름(FQDN)일 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 128.

패턴: `^.+$`

Required: No

HypervisorArn

하이퍼바이저의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

KmsKeyArn

하이퍼바이저를 암호화하는 데 사용되는 AWS KMS 의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Required: No

LastSuccessfulMetadataSyncTime

가장 최근에 메타데이터가 성공적으로 동기화된 시간입니다.

유형: 타임스탬프

필수 여부: 아니요

LatestMetadataSyncStatus

표시된 메타데이터 동기화의 최신 상태입니다.

타입: 문자열

유효 값: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

필수 여부: 아니요

LatestMetadataSyncStatusMessage

표시된 메타데이터 동기화의 최신 상태입니다.

타입: 문자열

필수사항: 아니요

LogGroupArn

요청한 로그 내 게이트웨이 그룹의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2,048.

패턴: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Required: No

Name

지정된 하이퍼바이저의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

State

지정된 하이퍼바이저의 현재 상태입니다.

가능한 상태는`PENDING`, `ONLINE`, `OFFLINE` 또는 `ERROR`입니다.

타입: 문자열

유효 값: `PENDING | ONLINE | OFFLINE | ERROR`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

MaintenanceStartTime

서비스: AWS Backup gateway

주중의 요일 및 시간을 포함한 게이트웨이의 주별 유지 관리 시작 시간을 반환합니다. 참고로, 값은 게이트웨이의 표준시간대를 기준으로 합니다. 주별 또는 월별일 수 있습니다.

내용

HourOfDay

유지 관리 시작 시간의 시간 구성 요소는 hh로 표시되며, 여기서 hh는 시(0~23)입니다. 하루 중 시간은 게이트웨이의 표준시간대를 기준으로 합니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 23입니다.

필수 여부: 예

MinuteOfHour

유지 관리 시작 시간의 분 구성 요소는 mm으로 표시되며, 여기서 mm은 분(0~59)입니다. 하루 중 분은 게이트웨이의 표준시간대를 기준으로 합니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 59입니다.

필수 여부: 예

DayOfMonth

유지 관리 시작 시간의 일 구성 요소는 1부터 28까지의 서수로 표시됩니다. 여기서 1은 월의 첫 날을 나타내고 28은 월의 마지막 날을 나타냅니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 31입니다.

필수 여부: 아니요

DayOfWeek

요일을 나타내는 0에서 6 사이의 서수입니다. 여기서 0은 일요일을 나타내고, 6은 토요일을 나타냅니다. 주중 요일은 게이트웨이의 표준시간대를 기준으로 합니다.

유형: 정수

유효한 범위: 최소값은 0. 최대값은 6입니다.

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

Tag

서비스: AWS Backup gateway

리소스를 관리, 필터링, 검색하는 데 사용할 수 있는 키-값 페어입니다. 허용되는 문자는 UTF-8 문자, 숫자, 공백 및 + - = . _ : /입니다.

내용

Key

태그 키-값 페어의 키 부분입니다. 키는 `aws:`로 시작할 수 없습니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

패턴: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

필수 사항 여부: Yes

Value

태그 키-값 페어의 값 부분입니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[^\x00]*$`

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

VirtualMachine

서비스: AWS Backup gateway

하이퍼바이저에 있는 가상 머신입니다.

내용

HostName

가상 머신의 호스트 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

HypervisorId

가상 머신 하이퍼바이저의 ID입니다.

타입: 문자열

필수사항: 아니요

LastBackupDate

가상 머신이 백업된 가장 최신 날짜(Unix 형식 및 UTC 시간)입니다.

유형: 타임스탬프

필수 여부: 아니요

Name

가상 머신의 이름.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

Path

가상 머신의 경로입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 4096자입니다.

패턴: `^[^\x00]+$`

Required: No

ResourceArn

가상 머신의 Amazon 리소스 이름(ARN)입니다. 예: `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

VirtualMachineDetails

서비스: AWS Backup gateway

Amazon 리소스 이름(ARN) 순으로 정렬된 `VirtualMachine` 객체입니다.

내용

HostName

가상 머신의 호스트 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

HypervisorId

가상 머신 하이퍼바이저의 ID입니다.

타입: 문자열

필수사항: 아니요

LastBackupDate

가상 머신이 백업된 가장 최신 날짜(Unix 형식 및 UTC 시간)입니다.

유형: 타임스탬프

필수 여부: 아니요

Name

가상 머신의 이름.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^[a-zA-Z0-9-]*$`

Required: No

Path

가상 머신의 경로입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 4096자입니다.

패턴: `^[^\x00]+$`

Required: No

ResourceArn

가상 머신의 Amazon 리소스 이름(ARN)입니다. 예: `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

타입: 문자열

길이 제약: 최소 길이는 50입니다. 최대 길이는 500입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Required: No

VmwareTags

지정된 가상 머신과 관련된 VMware 태그의 세부 정보입니다.

타입: VmwareTag객체 배열

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

VmwareTag

서비스: AWS Backup gateway

VMware 태그는 특정 가상 머신에 연결된 태그입니다. 태그는 리소스를 관리, 필터링, 검색하는 데 사용할 수 있는 키-값 페어입니다.

VMware 태그의 내용을 태그와 일치시킬 AWS 수 있습니다.

내용

VmwareCategory

VMware의 범주입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 80.

필수 여부: 아니요

VmwareTagDescription

VMware 태그에 대한 사용자 정의 설명입니다.

타입: 문자열

필수사항: 아니요

VmwareTagName

VMware 태그에 대한 사용자 정의 이름입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 80.

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK

- AWS 루비 V3용 SDK

VmwareToAwsTagMapping

서비스: AWS Backup gateway

그러면 VMware 태그와 해당 AWS 태그의 매핑이 표시됩니다.

내용

AwsTagKey

AWS 태그의 키-값 쌍의 핵심 부분.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

패턴: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

필수 사항 여부: Yes

AwsTagValue

AWS 태그의 키-값 쌍의 값 부분.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[^\x00]*$`

필수 사항 여부: Yes

VmwareCategory

VMware의 범주입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 80입니다.

필수 여부: 예

VmwareTagName

VMware 태그에 대한 사용자 정의 이름입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 80입니다.

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS 루비 V3용 SDK

공통 파라미터

다음 목록에는 모든 작업이 쿼리 문자열을 사용하여 Signature Version 4 요청에 서명하는 데 사용하는 파라미터가 포함되어 있습니다. 작업별 파라미터는 그 작업에 대한 항목에 나열되어 있습니다. Signature Version 4에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

Action

수행할 작업입니다.

유형: 문자열

필수 항목 여부: 예

Version

요청이 작성되는 API 버전으로 YYYY-MM-DD 형식으로 표시됩니다.

유형: 문자열

필수 항목 여부: 예

X-Amz-Algorithm

요청 서명을 생성하는 데 사용된 해시 알고리즘입니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

유효한 값: AWS4-HMAC-SHA256

필수 항목 여부: 조건부

X-Amz-Credential

자격 증명 범위 값이며 액세스 키, 날짜, 대상으로 하는 리전, 요청하는 서비스 및 종료 문자열("aws4_request")이 포함된 문자열입니다. 값은 다음 형식으로 표시됩니다. access_key/YYYYMMDD/region/service/aws4_request.

자세한 내용은 IAM 사용 설명서의 서명된 AWS API 요청 생성을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Date

서명을 만드는 데 사용되는 날짜입니다. 형식은 ISO 8601 기본 형식(YYYYMMDD'T'HHMMSS'Z') 이어야 합니다. 예를 들어 다음 날짜 시간은 유효한 X-Amz-Date 값: 20120325T120000Z.

조건: X-Amz-Date는 모든 요청에서 옵션이지만 서명 요청에 사용되는 날짜보다 우선할 때 사용됩니다. 날짜 헤더가 ISO 8601 기본 형식으로 지정된 경우 X-Amz-Date가 필요하지 않습니다. X-Amz-Date를 사용하는 경우 항상 Date 헤더의 값을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명의 요소를 참조하세요.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Security-Token

AWS Security Token Service(AWS STS)에 대한 호출을 통해 받은 임시 보안 토큰입니다. AWS STS의 임시 보안 인증 정보를 지원하는 서비스 목록은 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요.

조건: AWS STS의 임시 보안 인증 정보를 사용하는 경우 보안 토큰을 포함시켜야 합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Signature

서명할 문자열과 파생된 서명 키에서 계산된 16진수로 인코딩된 서명을 지정합니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-SignedHeaders

표준 요청의 일부로 포함된 모든 HTTP 헤더를 지정합니다. 서명된 헤더 지정에 대한 자세한 내용은 IAM 사용 설명서의 서명된 AWS API 요청 생성을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

일반적인 오류

이 단원에는 모든 AWS 서비스의 API 작업에 대한 일반 오류가 나와 있습니다. 이 서비스의 API 작업에 대한 오류는 해당 API 작업 항목을 참조하십시오.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

IncompleteSignature

요청 서명이 AWS 표준을 준수하지 않습니다.

HTTP 상태 코드: 400

InternalFailure

알 수 없는 오류, 예외 또는 장애 때문에 요청 처리가 실패했습니다.

HTTP 상태 코드: 500

InvalidAction

요청된 동작 또는 작업이 유효하지 않습니다. 작업을 올바로 입력했는지 확인합니다.

HTTP 상태 코드: 400

InvalidClientTokenId

제공된 X.509 인증서 또는 AWS 액세스 키 ID가 AWS의 레코드에 존재하지 않습니다.

HTTP 상태 코드: 403

NotAuthorized

이 작업을 수행하려면 권한이 있어야 합니다.

HTTP 상태 코드: 400

OptInRequired

AWS 액세스 키 ID는 서비스에 대한 구독이 필요합니다.

HTTP 상태 코드: 403

RequestExpired

요청이 요청상의 날짜 스탬프로부터 15분 이상, 또는 요청 만료 날짜(예: 미리 서명된 URL)로부터 15분 이상 경과한 후 서비스에 도달했거나, 요청상의 날짜 스탬프가 15분 이상 미래입니다.

HTTP 상태 코드: 400

ServiceUnavailable

서버의 일시적 장애로 인해 요청이 실패하였습니다.

HTTP 상태 코드: 503

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

ValidationError

입력이 AWS 서비스에서 지정한 제약에 충족되지 않습니다.

HTTP 상태 코드: 400

에 대한 문서 기록 AWS Backup

- API 버전: 2023년 12월 6일
- 최신 설명서 업데이트: 2024년 6월 3일

다음 표에는 2019년 1월 서비스 AWS Backup 출시 이후 현재까지 출시된 모든 목록이 나와 있습니다. 이 설명서에 대한 업데이트 알림을 받으려면 위의 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
AWS Backup 특징: 지역 확장	AWS Backup Amazon EBS 스냅샷 아카이브 티어에 대한 지원이 이제 다음 지역에서 제공됩니다. • 중국(베이징) • 중국(닝샤) • AWS GovCloud (미국 서부) • AWS GovCloud (미국 동부)	2024년 6월 3일
AWS 관리형 정책 업데이트	AWS Backup 다음 관리형 정책에 `backup:TagResource` 권한을 추가했습니다. • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup 자세한 내용은 정책 업데이트를 참조하십시오.	2024년 5월 17일

변경 사항	설명	날짜
AWS Backup 이제 캐나다 서부 (캘거리) 지역에서 사용할 수 있습니다.	이제 AWS 리전 캐나다 서부 (캘거리) 에서 다양한 리소스 유형에 대한 백업 및 복원을 사용할 수 있습니다. 호환되는 백업 기능에 대해서는 기능 가용성별을 참조하십시오. AWS 리전 지원되는 리소스 유형에 대해서는 지원 서비스 제공자를 참조하십시오 AWS 리전.	2024년 3월 14일
관리형 정책에 권한 추가	AWS Backup 복원 테스트 기능 내에서 추가 리소스 유형을 지원하는 권한을 AWSServiceRolePolicyForBackupRestoreTesting추가하여 정책을 업데이트했습니다. 추가된 특정 권한에 대한 자세한 내용은 정책 업데이트를 참조하십시오.	2024년 2월 14일
ONTAP 볼륨용 FSx에 대한 백업 및 복원 지원 FlexGroup	AWS Backup 이제 대부분의 FlexGroup ONTAP 볼륨에 대한 FSx 백업 및 복원을 지원합니다. AWS 리전 자세한 내용은 Amazon FSx 파일 시스템 복원을 참조하세요. .	2024년 1월 10일

변경 사항	설명	날짜
SAP HANA HA 백업 및 복원 지원	AWS Backup 이제 Amazon EC2 백업 및 복원에 대한 SAP HANA 고가용성 데이터베이스를 지원합니다. 자세한 내용은 SAP HANA on Amazon EC2 backups 및 Restoring an SAP HANA High Availability system을 참조하세요.	2023년 12월 21일
AWS Backup 복원 테스트를 위한 Audit Manager 제어	AWS Backup Audit Manager는 이제 복원 시간을 모니터링하는 데 도움이 되도록 리소스가 목표를 충족할 수 있도록 복원 시간을 제어할 수 있는 기능을 제공합니다. 이 컨트롤은 리소스의 복원 시간이 목표 기간을 충족하는지 확인합니다. 자세한 내용은 컨트롤 및 문제 해결 및 복원 테스트 감사 섹션을 참조하세요.	2023년 12월 18일
Amazon EBS 콜드 스토리지 지원	AWS Backup 이제 EBS 백업을 웜 스토리지에서 콜드 스토리지로 전환할 수 있습니다. 자세한 내용을 알아보려면 다음 섹션을 참조하세요. • 콜드 스토리지용 Amazon EBS 아카이브 계층 • 수명 주기 및 스토리지 계층 • 백업 계획 생성	2023년 11월 27일

변경 사항	설명	날짜
복원 테스트 도입	AWS Backup 복원 실행 가능성에 대한 자동 및 주기적 평가와 복원 작업 지속 시간을 모니터링하는 기능을 제공하는 복원 테스트를 소개합니다. 자세한 내용은 복원 테스트 섹션을 참조하세요.	2023년 11월 27일

변경 사항	설명	날짜
AWS 관리형 정책 업데이트	AWS Backup 관리형 정책에 AWSBackupServiceRolePolicyForBackups 권한 ec2:DescribeSnapshotTierStatus 및 ec2:ModifySnapshotTier 추가 AWSBackupServiceLinkedRolePolicyForBackup AWS Backup 권한 ec2:DescribeSnapshotTierStatus 및 ec2:RestoreSnapshotTier 관리형 정책에도 추가되었습니다AWSBackupServiceRolePolicyForRestores . 이러한 권한은 에 저장된 Amazon EBS 리소스를 아카이브 스토리지로 전환하고 아카이브 스토리지 계층에서 리소스를 복원할 수 있는 AWS Backup 옵션을 사용자에게 제공하는 데 필요합니다. 자세한 내용은 Policy updates를 참조하세요.	2023년 11월 27일

변경 사항	설명	날짜
복원 테스트를 지원하는 역할 전달 권한을 추가했습니다.	AWS Backup `IamPassRolePermissions` 및 `restore-testing.backup.amazonaws.com` `IamCreateServiceLinkedRolePermissions`에 추가되었습니다. 이 추가는 고객을 대신하여 복원 테스트를 수행하는 AWS Backup 데 필요합니다.	2023년 11월 27일
새 서비스 연결 역할 추가	AWS Backup 복원 테스트를 수행할 수 있는 백업 권한을 제공하는 새로운 서비스 연결 역할을 추가했습니다. `AWSServiceRoleForBackupRestoreTesting` 이 새로운 서비스 연결 역할은 복원 테스트를 수행하는 데 필요한 권한을 제공합니다 AWS Backup . 권한에는 Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx for ONTAP, FSx for OpenZFS, Amazon Neptune, Amazon RDS, Amazon S3 등 복원 테스트에 포함할 서비스에 대한 `list, read, and write` 작업이 포함됩니다.	2023년 11월 27일

변경 사항	설명	날짜
콘솔의 새 작업 지표 대시보드 AWS Backup	이제 AWS Backup 콘솔에 작업 대시보드가 표시되어 새로운 시각적 사용자 인터페이스와 에서 지원하는 서비스에 대한 집계된 백업, 복사 및 복원 메트릭을 통해 대규모 백업 상태 모니터링을 단순화할 수 있습니다. AWS Backup 채용 대시보드는 AWS Backup Audit Manager를 사용할 수 있는 모든 지역에서 사용할 수 있습니다. 목록에 없는 지역은 계속 CloudWatch 대시보드에 액세스할 수 있습니다. 자세한 내용은 AWS Backup 콘솔 대시보드를 참조하세요.	2023년 11월 15일
중첩된 스택 백업 지원	AWS Backup AWS CloudFormation 리소스 백업에 대한 지원을 확대했습니다. 스택이 중첩된 CloudFormation 애플리케이션 스택을 백업에 포함할 수 있습니다. 자세한 내용을 알아보려면 CloudFormation stack backups 섹션을 참조하세요.	2023년 11월 8일

변경 사항	설명	날짜
중국(베이징) 및 중국(닝샤) 리전에서 Amazon S3 지원	AWS Backup Amazon S3에 대한 지원은 이제 중국 (베이징) 및 중국 (닝샤) 지역에서 제공됩니다. 자세한 내용은 Feature availability by Region 섹션을 참조하세요.	2023년 10월 26일
Amazon Aurora 연속 백업 및 IP 복원에 대한 지원 oint-in-time	AWS Backup 이제 Aurora 리소스에 대한 연속 백업 및 point-in-time 복원 (PITR) 을 지원합니다. 자세한 내용은 연속 백업 및 Point-in-time 복구를 참조하십시오.	2023년 9월 7일
AWS CloudFormation 스택은 리소스 제외를 지원합니다.	AWS Backup 이제 스택에서 선택한 리소스를 제외하는 옵션이 지원됩니다. AWS CloudFormation 자세한 내용을 알아보려면 AWS CloudFormation stack backups 섹션을 참조하세요.	2023년 9월 6일
백업 계획 규칙에 표준시간대 유연성 도입	AWS Backup 이제 계획 규칙에 백업 기간을 지정한 시간대를 지정할 수 있습니다. 자세한 내용은 백업 계획 관리 섹션을 참조하세요.	2023년 8월 28일

변경 사항	설명	날짜
AWS Backup 이제 이스라엘 (텔아비브) 지역에서 사용할 수 있습니다.	이제 새 이스라엘 (텔아비브) 지역에서 많은 AWS Backup 기능을 사용할 수 있습니다. 어떤 리소스가 지원되는지 알아보려면 Feature availability by AWS 리전 섹션을 참조하세요.	2023년 8월 22일
AWS Backup Audit Manager는 이제 위임된 관리자 계정을 지원합니다.	AWS Backup 이제 위임된 관리자 계정으로 Audit Manager 보고서 생성에 액세스할 수 있습니다. 자세한 내용을 알아보려면 다음 섹션을 참조하세요. • Audit Manager를 사용하여 백업을 AWS Backup 감사하고 보고서를 생성합니다. • 감사 보고서 작업 • 위임된 관리자	2023년 8월 16일
논리적 에어 갭 처리 저장소의 평가판	AWS Backup 이제 데이터 보호 작업을 보완하는 데 도움이 되는 새로운 유형의 백업 저장소를 미리 볼 수 있습니다. 자세한 내용은 논리적 에어 갭 처리 저장소(평가판) 섹션을 참조하세요.	2023년 8월 8일
AWS Backup Amazon S3 백업을 개선합니다	AWS Backup S3 버킷 백업의 성능, 크기 및 속도 기능이 향상되었습니다. 자세한 내용은 Amazon S3 backups 섹션을 참조하세요.	2023년 8월 1일

변경 사항	설명	날짜
이제 중국 리전에서 복원 시 태그 기능 사용 가능	이제 중국(베이징) 또는 중국(닝샤) 리전에서 복원 작업을 생성할 때 백업의 일부인 태그를 복사할 수 있습니다. 자세한 내용은 Copy tags during a restore 섹션을 참조하세요.	2023년 7월 17일
AWS Backup 이제 추가 지역에서 Amazon S3를 지원합니다.	AWS Backup 이제 유럽 (스페인), 유럽 (취리히), 아시아 태평양 (하이데라바드) 및 아시아 태평양 (멜버른) 지역에서 Amazon S3에 대한 지원을 이용할 수 있습니다. 자세한 내용은 Feature availability by Region 섹션을 참조하세요.	2023년 7월 6일
교차 계정 복사를 추가 리전으로 확장	AWS Backup 이제 아시아 태평양 (자카르타), 중동 (바레인), 아시아 태평양 (홍콩), 아프리카 (케이프타운), 유럽 (밀라노), 아시아 태평양 (오사카), 중동 (UAE), 유럽 (스페인), 유럽 (취리히), 아시아 태평양 (하이데라바드), 아시아 태평양 (멜버른) 지역에서 대부분의 리소스에 대한 계정 간 백업 복사본을 지원합니다. 자세한 내용은 Feature availability by Region 섹션을 참조하세요.	2023년 7월 5일

변경 사항	설명	날짜
Backup Audit Manager는 GovCloud 지역에서 사용할 수 있습니다.	AWS Backup AWS Backup Audit Manager를 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 로 확장했습니다. 자세한 내용은 Feature availability by Region 섹션을 참조하세요.	2023년 6월 29일
이제 지역별로 교차 계정 관리를 사용할 수 있습니다. GovCloud	AWS Backup 이제 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 리소스의 계정 간 관리를 지원합니다. 자세한 내용은 Managing AWS Backup resources across multiple AWS accounts를 참조하세요.	2023년 6월 29일
추가 리전에서 Amazon Aurora의 교차 리전 복사본 지원	AWS Backup 이제 아시아 태평양 (자카르타), 중동 (바레인), 아시아 태평양 (홍콩), 아프리카 (케이프타운), 유럽 (밀라노), 중동 (UAE), 유럽 (스페인), 유럽 (취리히), 아시아 태평양 (하이데라바드), 아시아 태평양 (멜버른) 간의 Aurora 클러스터 간 백업 복제본을 지원합니다.	2023년 6월 5일

변경 사항	설명	날짜
복원 시 태그 복사	이제 복원 작업을 생성할 때 백업의 일부인 태그를 복사할 수 있습니다. 자세한 내용은 Copy tags during a restore 섹션을 참조하세요.	2023년 5월 22일
AWS Backup 사용자 알림과 통합됩니다. AWS	이제 AWS 사용자 알림 콘솔을 통해 백업, 복사, 복원 이벤트와 관련된 알림을 수신하도록 선택할 수 있습니다. 자세한 내용은 AWS 사용자 알림 시작하기를 참조하십시오.	2023년 5월 10일
새로운 네 가지 리전에서 교차 리전 백업 사용 가능	AWS Backup 이제 중동 (UAE) 지역, 유럽 (스페인) 지역, 유럽 (취리히) 지역 및 아시아 태평양 (하이데라바드) 지역에서 지역 간 백업이 지원됩니다.	2023년 4월 28일
AWS Backup 지역 간 복사 지원 확대	이제 아시아 태평양(자카르타), 중동(바레인), 아시아 태평양(홍콩), 아프리카(케이프타운), 유럽(밀라노) 리전에서 Amazon EFS, VMware, DynamoDB 리소스의 교차 리전 백업을 수행할 수 있습니다.	2023년 4월 28일

변경 사항	설명	날짜
남아메리카(상파울루) 리전에서 Amazon S3 백업 및 복원	AWS Backup Amazon S3 (Amazon 심플 스토리지 서비스) 에 대한 지원이 이제 남아메리카 (상파울루) 지역에서 제공됩니다. 자세한 내용은 Amazon S3 backups 섹션을 참조하세요.	2023년 4월 20일
AWS Backup 아시아 태평양 (멜버른) 지역으로 확장	AWS Backup 이제 아시아 태평양 (멜버른) 지역에서 사용할 수 있습니다. 자세한 내용은 AWS 지역별 기능 가용성을 참조하십시오.	2023년 4월 20일
Amazon S3에 대한 지원이 리전별로 확장	AWS Backup Amazon S3 (Amazon 심플 스토리지 서비스) 에 대한 지원이 이제 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 지역에서 제공됩니다. 자세한 내용은 Amazon S3 backups 섹션을 참조하세요.	2023년 4월 19일
Amazon EC2 인스턴스의 SAP HANA 데이터베이스 백업 및 복원	AWS Backup 이제 대부분의 지역에서 Amazon EC2 인스턴스에서 실행되는 SAP HANA 데이터베이스를 백업 및 복원하는 기능을 제공합니다. 자세한 내용은 SAP HANA databases on Amazon EC2 instances backup을 참조하세요.	2023년 4월 17일

변경 사항	설명	날짜
AWS Backup 이제 유럽 (스페인), 유럽 (취리히), 아시아 태평양 (하이데라바드) 지역에서 사용할 수 있습니다.	AWS Backup 유럽 (스페인), 유럽 (취리히), 아시아 태평양 (하이데라바드) 등 새로운 지역으로 지원이 확대되었습니다. 지원되는 리소스를 이러한 리전에서 백업 및 복원할 수 있습니다. 자세한 내용은 지역별 기능 가용성을 참조하십시오. AWS	2023년 4월 13일
업데이트된 AWS 관리형 정책 `AWSBackupAuditAccess`	AWS 관리형 정책이 업데이트되었습니다 AWSBackupAuditAccess. AWS Backup API `config:DescribeComplianceByConfigRule` 내 리소스 선택을 와일드카드 리소스로 대체했습니다. 자세한 내용은 Policy updates for AWS Backup 섹션을 참조하세요.	2023년 4월 11일
Amazon 로그를 사용하는 하이퍼바이저 CloudWatch	AWS Backup 게이트웨이 사용자는 이제 하이퍼바이저를 CloudWatch 로그와 통합하여 로그를 유지할 수 있습니다. 자세한 내용은 하이퍼바이저 구성 및 로그 편집을 참조하십시오. CloudWatch	2023년 3월 29일
Amazon S3에 대한 지원이 리전별로 확장	AWS Backup Amazon S3에 대한 지원은 이제 아시아 태평양 (자카르타) 및 중동 (UAE) 지역에서 사용할 수 있습니다.	2023년 3월 22일

변경 사항	설명	날짜
가상 머신 증분 백업 개선	이제 CBT(Changed Block Tracking) 데이터 문제가 발생하는 VMware 가상 머신(VM) 백업에는 문제 해결에 도움이 되는 추가 정보가 포함됩니다. 자세한 내용은 증분 VM 백업 및 Troubleshoot your virtual machines 섹션을 참조하세요.	2023년 3월 15일
AWS Backup 다중 네트워크 어댑터 지원	AWS Backup 게이트웨이는 이제 다중 네트워크 어댑터 구성을 지원합니다. 네트워크 어댑터 구성에 대한 자세한 내용은 AWS Backup 개발자 안내서의 VMware에서 여러 NIC에 대한 게이트웨이 구성 섹션을 참조하세요.	2023년 3월 8일
AWS Backup vSphere 8에 대한 지원	AWS Backup 이제 VMware vSphere 8에서 실행되는 가상 시스템의 백업 및 복원을 지원합니다. 지원되는 VMware 옵션에 대한 자세한 내용은 AWS Backup 개발자 안내서의 지원되는 VM 섹션을 참조하세요.	2023년 3월 8일

변경 사항	설명	날짜
AWS Backup Audit Manager는 Amazon RDS 다중 AZ 백업을 지원합니다	이제 Backup Audit Manager가 Amazon Relational Database Service 다중 가용 영역 백업에 대한 지원을 제공합니다. 자세한 내용은 Audit Manager를 사용하여 AWS Backup 백업을 감사하고 보고서를 만드는 방법을 참조하십시오.	2023년 2월 1일
AWS Backup Amazon Timestream 테이블에 대한 증분 백업을 제공합니다.	AWS Backup 이제 타임스트림 백업을 위한 확장된 백업 기능을 제공합니다. 이제 백업 계획을 통해 증분 백업을 수행하여 Timestream 리소스를 백업하는 데 필요한 시간을 줄이고 스토리지 비용을 절감할 수 있습니다. 자세한 내용은 Amazon Timestream backups를 참조하세요.	2023년 1월 23일
AWS Backup 이제 두바이에서 사용할 수 있습니다.	AWS Backup 중동 (UAE) 지역으로 확장되었습니다. 지원되는 리소스를 이 리전에서 백업 및 복원할 수 있습니다.	2023년 1월 17일

변경 사항	설명	날짜
추가 리전에서 교차 리전 복사 사용 가능	AWS Backup 이제 대부분의 리소스에 대해 아시아 태평양 (자카르타) 지역, 중동 (바레인) 지역, 아시아 태평양 (홍콩) 지역, 아프리카 (케이프타운) 지역, 유럽 (밀라노) 지역에서 지역 간 백업을 제공합니다. 자세한 내용은 Creating backup copies across AWS 리전 섹션을 참조하세요.	2022년 12월 21일
백업 게이트웨이 대역폭 한도 및 제한	AWS Backup 이제 게이트웨이에서 게이트웨이에서의 업로드 처리량을 AWS Backup 제한하여 게이트웨이가 사용하는 네트워크 대역폭의 양을 제어할 수 있습니다. 이 기능을 지원하기 위해 AWS Backup 는 및 을 포함한 AWSBackupFullAccess 관리형 정책을 만들고 업데이트했습니다. AWSBackupOperatorAccess 자세한 내용은 백업 게이트웨이 대역폭 제한 섹션을 참조하세요.	2022년 12월 15일

변경 사항	설명	날짜
백업 게이트웨이 VMware 태그 지원	AWS Backup 게이트웨이는 이제 VMware 태그를 지원합니다. 사용자는 가상 시스템에 사용되는 AWS 태그와 일치하는 태그를 더욱 유연하게 만들 수 있습니다. 이 기능을 지원하기 위해, AWS Backup 및 를 포함한 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 관리형 정책을 만들고 AWSBackupOperatorAccess 업데이트했습니다. AWSBackupFullAccess 자세한 내용은 VMware 태그 섹션을 참조하세요.	2022년 12월 15일
AWS Backup Amazon Timestream 지원	AWS Backup 이제 Amazon Timestream 테이블 백업 및 복원을 지원합니다. 자세한 내용은 Amazon Timestream backup 섹션을 참조하세요.	2022년 12월 13일
AWS Backup 법적 보류를 제공합니다.	AWS Backup 법적 보류를 통해 복구 지점을 보호하는 데 도움이 되는 새로운 도구를 소개합니다. 자세한 내용은 법적 보존 섹션을 참조하세요.	2022년 11월 27일

변경 사항	설명	날짜
AWS Backup Audit Manager 지역 간 및 계정 간 보고	AWS Backup Audit Manager는 규정 준수 및 작업 보고서에 추가 기능을 제공합니다. 사용자는 여러 리전 및 여러 계정을 통합하는 보고서를 생성할 수 있습니다. 자세한 내용은 감사 보고서 작업 섹션을 참조하세요.	2022년 11월 27일
AWS Backup 아마존 Redshift를 지원합니다	AWS Backup 이제 Amazon Redshift 클러스터를 백업하고 Amazon Redshift 클러스터 및 테이블을 복원할 수 있는 지원을 제공합니다. 자세한 내용은 Amazon Redshift 백업 섹션을 참조하세요.	2022년 11월 27일
AWS Backup 애플리케이션 스택 백업을 AWS CloudFormation 지원합니다.	AWS Backup 스택을 CloudFormation 백업하고 스택에 포함된 리소스를 복원하여 여러 리소스가 포함된 애플리케이션을 백업 및 복원하는 기능을 제공합니다. 자세한 내용은 Application stack backups 섹션을 참조하세요.	2022년 11월 27일

변경 사항	설명	날짜
AWS Backup 위임된 관리자 계정과 백업 정책 위임을 제공합니다.	AWS Backup 에 등록된 계정은 구성원 계정을 위임된 관리자 계정으로 지정할 AWS Organizations 수 있습니다. 자세한 내용은 여러 계정 관리를 참조하십시오. AWS Organizations	2022년 11월 27일
Amazon EC2 인스턴스 백업 및 복원에 대한 SAP HANA 공개 평가판	AWS Backup 그리고 AWS Backint는 EC2 인스턴스에서 SAP HANA 데이터베이스를 백업 및 복원하는 기능에 대한 통합된 공개 미리 보기를 제공합니다. 자세한 내용은 Public Preview of SAP HANA on Amazon EC2 instances 섹션을 참조하세요. 이 미리 보기를 지원하기 위해 이러한 AWS Backup 기능에 대한 정책 업데이트와 새로운 AWS 관리형 정책을 제공했습니다.	2022년 11월 20일

변경 사항	설명	날짜
VMware를 Amazon EC2 인스턴스로 복원	AWS Backup 이제 가상 머신을 Amazon EC2 인스턴스로 복원하는 기능과 EBS, VMware, VMware 클라우드 온 및 VMware 클라우드 AWS온으로 시스템을 복원하는 기능을 제공합니다. AWS Outposts 자세한 내용은 AWS Backup 콘솔을 사용하여 가상 시스템 복구 지점을 복원하는 방법에 대한 설명서를 참조하십시오.	2022년 11월 9일
확장된 AWS Backup Vault Lock 기능	AWS Backup 이제 추가 IAM 보호를 위해 거버넌스 모드에서 Vault Lock을 생성하거나 불변성을 보장하기 위한 규정 준수 모드에서 생성할 수 있습니다. AWS Backup Vault Lock에서 자세한 내용을 알아보세요.	2022년 10월 4일
AWS Backup 이제 아프리카 (케이프타운) 지역 및 유럽 (밀라노) 지역에서 Audit Manager를 사용할 수 있습니다.	AWS Backup Audit Manager는 아프리카 (케이프타운) 지역 및 유럽 (밀라노) 지역으로 확장했습니다. 백업 감사 관리자에 대한 자세한 내용은 Audit Manager를 사용한 백업 AWS Backup 감사 및 보고서 작성을 참조하십시오.	2022년 9월 14일

변경 사항	설명	날짜
AWS Backup Amazon CloudWatch 메트릭을 Backup 콘솔 대시보드로 가져옵니다.	AWS Backup 백업 콘솔 대시보드를 개선하여 백업 및 복원 작업에 대한 통합 Amazon CloudWatch 메트릭을 표시하여 모니터링 기능 및 유연성을 높였습니다.	2022년 9월 8일
복원하는 동안 추가적인 Amazon EBS 암호화 유연성 지원	AWS Backup 이제 Amazon EBS 스냅샷을 복원하는 동안 암호화를 선택할 수 있는 추가 옵션이 제공됩니다.	2022년 9월 1일
AWS Backup Amazon S3 계정 간 및 지역 간 백업 복사 지원	AWS Backup 이제 Amazon S3 백업을 위한 지역 간 및 계정 간 백업 복사를 제공합니다. 자세한 내용은 Amazon S3 backups 섹션을 참조하세요.	2022년 7월 28일
AWS Backup Audit Manager는 ONTAP용 FSx에 대한 추가 제어 지원을 제공합니다.	AWS Backup Audit Manager는 이제 백업 계획으로 보호되는 백업 리소스 및 마지막 복구 지점 생성을 포함하여 ONTAP 볼륨의 FSx 모니터링 및 감사를 지원하는 추가 제어 기능을 제공합니다. 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.	2022년 7월 22일

변경 사항	설명	날짜
AWS Backup PostgreSQL 및 MySQL 클러스터용 Amazon RDS 다중 AZ 클러스터에 대한 백업 및 복원 지원을 추가합니다.	AWS Backup 기본 데이터베이스 인스턴스 1개와 읽기 가능한 대기 데이터베이스 인스턴스 2개가 포함된 다중 가용 영역 클러스터 백업 및 복원 옵션이 추가되었습니다. 자세한 내용은 Amazon RDS Multi-AZ backups 섹션을 참조하세요.	2022년 7월 20일
AWS Backup Audit Manager는 복구 지점 생성을 위한 새로운 제어 기능을 추가합니다.	AWS Backup Audit Manager는 규정 준수 지원을 강화하기 위한 새로운 감사 제어 기능을 제공합니다. `Last recovery point created`는 지정된 기간 내에 복구 시점이 생성되도록 보장하기 위한 선택적 추가 컨트롤입니다. 자세한 내용은 마지막으로 생성된 복구 시점 컨트롤 섹션을 참조하세요.	2022년 6월 29일
AWS Backup 게이트웨이 엔드포인트 샘플 추가	AWS Backup Gateway는 사용자가 VPN (가상 사설망) 에 연결할 수 있도록 지원하는 샘플 엔드포인트를 제공했습니다. 자세한 내용은 AWS Backup VPC 엔드포인트 만들기를 참조하십시오.	2022년 6월 14일

변경 사항	설명	날짜
AWS Backup 이제 VMware용 Amazon VPC 엔드포인트를 제공합니다.	AWS Backup 이제 VMware용 Amazon VPC 엔드포인트를 지원하므로 VMware 환경과 사용자 간에 가상 사설망을 사용할 수 있습니다. AWS AWS PrivateLink 자세한 내용은 게이트웨이 생성 및 AWS Backup 및 AWS PrivateLink 섹션을 참조하세요.	2022년 6월 1일
AWS Backup Audit Manager는 Amazon S3에 대한 추가 제어 지원을 제공합니다.	이제 Backup Audit Manager는 S3 리소스 유형에 대한 규정 준수 컨트롤인 백업 계획으로 보호되는 백업 리소스에 대한 지원을 제공합니다. 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.	2022년 5월 25일
AWS Backup Audit Manager는 Storage Gateway에 대한 추가 제어 지원을 제공합니다.	이제 Backup Audit Manager는 Storage Gateway 리소스 유형에 대한 규정 준수 컨트롤인 백업 계획으로 보호되는 백업 리소스에 대한 지원을 제공합니다. 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.	2022년 5월 25일

변경 사항	설명	날짜
Amazon FSx for OpenZFS 지원	AWS Backup 이제 OpenZFS 파일 시스템의 FSX 백업 및 복원을 위한 추가 데이터 보호 관리 기능을 제공합니다.	2022년 5월 18일
AWS Backup VM웨어에 대한 Audit Manager 지원	AWS Backup 이제 Backup Audit Manager의 제어 및 문제 해결에서 가상 시스템에 대한 지원을 제공합니다. 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.	2022년 5월 11일
이제 아시아 태평양(오사카) 리전에서 Amazon FSx 지원	AWS Backup 이제 Amazon FSx를 아시아 태평양 (오사카) 지역 내에서 백업하고 지역 간 복사본을 백업할 수 있습니다.	2022년 4월 26일
Amazon FSx for Lustre Persistent_2 지원	AWS Backup 이제 Persisten t_1 파일 시스템에 비해 스토리지 단위당 더 높은 수준의 처리량을 지원하는 Amazon FSx for Lustre에 대한 일반 지원을 제공합니다.	2022년 4월 5일
VMware 개선	AWS Backup 이제 Amazon EBS 볼륨으로의 복원, 디스크 수준 복원 및 VMware 온에 대한 지원을 제공합니다. AWS Outposts자세한 내용은 Restoring a virtual machine 섹션을 참조하세요.	2022년 3월 31일
AWS Backup 아시아 태평양 (자카르타) 이용 가능	AWS Backup 이제 아시아 태평양 (자카르타) 지역의 고객이 이용할 수 있습니다.	2022년 3월 17일

변경 사항	설명	날짜
AWS Backup Audit Manager를 위한 새로운 제어	AWS Backup Audit Manager에는 지역 간 복사, 계정 간 복사, Backup Vault Lock이라는 세 가지 새로운 감사 제어 기능이 도입되었습니다. 자세한 내용은 AWS Backup Audit Manager 컨트롤 및 문제 해결 섹션을 참조하세요.	2022년 3월 17일
에 대한 지원 AWS PrivateLink	AWS PrivateLink for를 AWS Backup사용하면 퍼블릭 인터넷을 통해 연결하는 대신 VPC의 인터페이스 엔드포인트를 AWS Backup 사용하여 직접 연결할 수 있습니다. 인터페이스 엔드포인트는 온프레미스 또는 다른 AWS 지역에 있는 애플리케이션에서 직접 액세스할 수 있습니다. 자세한 내용은 AWS Backup 및 AWS PrivateLink 섹션을 참조하세요.	2022년 2월 28일
Amazon Simple Storage Service(S3) 지원	Amazon AWS 리전 S3는 중국 (베이징) 지역, 중국 (닝샤) 지역, (미국 서부) 및 AWS GovCloud AWS GovCloud (미국 동부) 지역을 제외한 모든 지역에서 사용할 수 있습니다. AWS Backup 자세한 내용은 Working with Amazon S3 data 섹션을 참조하세요.	2022년 2월 14일

변경 사항	설명	날짜
중국 지역의 고급 DynamoDB 백업 지원 AWS	이제 중국(베이징) 리전 및 중국(닝샤) 리전에서 고급 DynamoDB 백업을 사용할 수 있습니다. 자세한 내용은 Advanced DynamoDB backup 섹션을 참조하세요.	2022년 1월 18일
Amazon S3의 공개 평가판 지원	AWS Backup Amazon S3 백업의 공개 미리 보기를 제공합니다. 자세한 정보는 Amazon S3 데이터 작업을 참조하세요.	2021년 11월 30일
VMware 가상 머신(VM) 지원	이제 를 사용하여 VMware AWS Backup VM을 자동으로 백업할 수 있습니다. 자세한 정보는 가상 머신 백업을 참조하세요.	2021년 11월 30일
고급 DynamoDB 백업 지원	이제 새로 생성하는 모든 DynamoDB 테이블 백업에 대해 콜드 스토리지 계층화, 비용 할당 태깅, 교차 리전 복사, 계정 간 복사, 독립 암호화, 소스 DynamoDB 테이블의 태그 복사 등의 기능을 사용할 AWS Backup 수 있습니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서 및 DynamoDB와 함께 사용을 AWS Backup 참조하십시오고급 DynamoDB 백업.	2021년 11월 23일

변경 사항	설명	날짜
AWS 중국 지역의 AWS Backup 리소스 배정 개선 지원	AWS Backup 이제 중국 (베이징) 지역 및 중국 (닝샤) 지역에서 리소스 배정 개선 기능을 사용할 수 있습니다. 자세한 내용은 백업 계획에 리소스 할당 섹션을 참조하세요.	2021년 11월 16일
리소스 배정 개선 기능 AWS Backup 시작	향상된 백업 리소스 할당 기능을 통해 수십만 개의 리소스를 보호하는 백업 계획을 구축할 수 있는 추가적이고 세분화된 제어 기능과 새롭고 간소화된 프로세스를 제공합니다. AWS AWS Backup을 사용하여 데이터를 보호할 때 이 기능을 사용하면 속도, 유연성, 정밀도를 높일 수 있습니다. 자세한 내용은 백업 계획에 리소스 할당 섹션을 참조하세요.	2021년 11월 10일
Amazon Neptune 클러스터 지원	이제 Amazon Neptune AWS Backup 클러스터를 백업하는 데 사용할 수 있습니다. 자세한 내용은 AWS Backup이란 무엇입니까?를 참조하십시오.	2021년 11월 5일
Amazon DocumentDB 지원	이제 Amazon DocumentDB AWS Backup 클러스터를 백업하는 데 사용할 수 있습니다. 자세한 내용은 AWS Backup이란 무엇입니까?를 참조하십시오.	2021년 11월 5일

변경 사항	설명	날짜
AWS 중국 지역의 AWS Backup 볼트 락 지원	AWS Backup 이제 중국 (베이징) 지역 및 중국 (닝샤) 지역에서 Vault Lock을 사용할 수 있습니다. 자세한 내용은 AWS Backup Vault Lock 섹션을 참조하세요.	2021년 11월 3일
볼트 락 출시 AWS Backup	AWS Backup Vault Lock을 사용하면 AWS Backup 백업 저장소에 저장된 백업이 삭제되는 것을 방지할 수 있습니다. 자세한 내용은 AWS Backup Vault Lock 섹션을 참조하세요.	2021년 10월 7일
AWS Backup Audit Manager 규정 준수 보고서 출시	규정 준수 보고서를 사용하면 AWS Backup Audit Manager 프레임워크에서 정의한 제어 항목을 기준으로 백업 활동 및 리소스의 규정 준수에 대한 일일 보고서를 생성할 수 있습니다. 자세한 내용은 규정 준수 보고서 템플릿 섹션을 참조하세요.	2021년 10월 5일
AWS CloudFormation AWS Backup Audit Manager 지원	를 사용하면 이제 대규모로 안전하고 반복 가능한 방식으로 AWS Backup Audit Manager 프레임워크, 제어 및 보고 계획을 배포할 수 있습니다. AWS CloudFormation자세한 내용은 Audit Manager를 사용한 백업 AWS Backup 감사 및 보고서를 참조하십시오.	2021년 10월 4일

변경 사항	설명	날짜
AWS Backup Audit Manager 런칭	이제 AWS Backup Audit Manager를 사용하여 백업 활동 및 리소스에 대한 제어를 정의하고 제어를 준수하지 않는 활동 및 리소스를 식별할 수 있습니다. 또한 AWS Backup Audit Manager를 사용하여 일정 기간 동안 정의된 규제 준수의 증거로 사용되는 일일 및 온디맨드 보고서를 생성할 수 있습니다. 자세한 내용은 Audit Manager를 사용한 백업 AWS Backup 감사 및 보고서를 참조하십시오.	2021년 8월 24일
새로운 비동기식 복구 시점 작업 지원	AWS Backup 이제 원래 IAM 역할을 수정하거나 삭제한 경우 백업 수명 주기 규칙을 관리하는 서비스 연결 역할을 맡습니다. 자세한 내용은 Deleting backups 섹션을 참조하세요.	2021년 8월 23일
Amazon EBS 다중 볼륨, 중단 일관성 백업 지원	이제 를 AWS Backup 사용하여 Amazon EC2 인스턴스를 보호할 때 기본적으로 각 Amazon EC2 인스턴스에 연결된 모든 Amazon EBS 볼륨을 충돌 시에도 일관되게 여러 볼륨으로 백업합니다. AWS Backup 자세한 내용은 Creating Amazon EBS multi-volume, crash-consistent backup 섹션을 참조하세요.	2021년 6월 14일

변경 사항	설명	날짜
아마존 FSx 지원 (추가) AWS 리전	이제 유럽 (밀라노) 지역, 아프리카 (케이프타운) 지역, 중동 (바레인) 지역에서 Amazon FSx 파일 시스템을 보호하는 데 사용할 AWS Backup 수 AWS GovCloud (US)있습니다. 자세한 내용을 알아보려면 AWS 일반 참조의 AWS Backup 엔드포인트 및 할당량을 참조하세요.	2021년 4월 15일
Amazon FSx 교차 리전 및 교차 계정 백업 지원	이제 를 AWS Backup 사용하여 및 계정 간에 Amazon FSx 백업을 AWS 리전 복사할 수 있습니다. 자세한 내용은 Creating a Backup Copy 섹션을 참조하세요. 고객 관리형 정책을 사용할 경우 새 권한 `fsx:CopyBackup` 을 추가하여 기존 백업 작업이 실패하지 않도록 해야 합니다. 이러한 권한에 대한 내용은 고객 관리형 정책에서 Amazon FSx 백업 정책의 마지막 명령문을 참조하세요.	2021년 4월 12일
Amazon EFS 백업에 비용 할당 태그 지원	이제 비용 할당 태그를 사용하여 Amazon EFS 백업 비용을 세부 수준에서 추적하고, 를 사용하여 해당 태그를 보고 필터링할 수 AWS Cost Explorer있습니다. 자세한 내용은 비용 할당 태그 사용하기를 참조하세요.	2021년 4월 7일

변경 사항	설명	날짜
FedRAMP High 권한 부여	AWS Backup 이제 FedRAMP 하이 워크로드를 지원할 수 있는 권한이 부여되었습니다. 자세한 내용은 규정 준수 프로그램 제공 범위 내AWS 서비스를 참조하세요.	2021년 3월 25일
신규 AWS 리전	AWS Backup 이제 아시아 태평양 (오사카) 지역에서 사용할 수 있습니다. 이 리전의 경우, 현재 AWS Backup 은 이 리전에서 Storage Gateway, Amazon FSx, 교차 계정 백업을 지원하지 않습니다. 자세한 내용을 알아보려면 AWS 일반 참조의 AWS Backup 엔드포인트 및 할당량을 참조하세요.	2021년 3월 25일
복구 시점 배치 작업 지원	이제 AWS Backup 콘솔을 사용하여 백업 저장소의 복구 지점을 정리하는 배치 작업을 자동화할 수 있습니다. 자세한 내용은 Deleting backups 섹션을 참조하세요.	2021년 3월 23일
Amazon EFS One Zone 스토리지 클래스로 복원 지원	이제 Amazon EFS 백업을 Amazon EFS One Zone 스토리지 클래스로 복원할 수 있습니다. 자세한 내용은 Restoring an Amazon EFS file system 섹션을 참조하세요.	2021년 3월 12일

변경 사항	설명	날짜
Amazon 관계형 데이터베이스 point-in-time 서비스 복원 및 연속 백업 지원	이제 스냅샷 백업을 AWS Backup 오케스트레이션하는 것 외에도 Amazon RDS 연속 백업을 자동화하고 point-in-time 복원 (PITR) 을 수행할 수 있습니다. 자세한 내용은 복구를 사용하여 지정된 시간으로 복원을 참조하십시오. point-in-time	2021년 3월 10일
아마존 지원 CloudWatch	이제 CloudWatch AWS Backup 메트릭을 모니터링하는 데 사용할 수 있습니다. 자세한 내용은 Amazon 및 Amazon을 통한 이벤트 및 지표 CloudWatch 모니터링을 참조하십시오 EventBridge.	2021년 2월 3일
아마존 지원 EventBridge	이제 AWS Backup 이벤트를 모니터링하는 EventBridge 데 사용할 수 있습니다. 자세한 내용은 Amazon 및 Amazon을 통한 이벤트 및 지표 CloudWatch 모니터링을 참조하십시오 EventBridge.	2021년 2월 3일
교차 계정 백업 지원	이제 를 AWS Backup 사용하여 여러 리소스의 리소스를 백업할 수 AWS 계정있습니다. 자세한 내용은 AWS 계정 간 백업 복사본 만들기를 참조하십시오.	2020년 11월 18일

변경 사항	설명	날짜
Amazon FSx 파일 시스템 백업 및 복원 지원	이제 Amazon FSx 파일 시스템을 AWS Backup 백업하는 데 사용할 수 있습니다. 자세한 내용은 Working with Amazon FSx file systems 섹션을 참조하세요.	2020년 11월 9일
신규 AWS 리전	AWS Backup 이제 아프리카 (케이프타운) 와 유럽 (밀라노) 에서 사용할 수 AWS 리전있습니다. 자세한 내용을 알아보려면 AWS 일반 참조의 AWS Backup 엔드포인트 및 할당량을 참조하세요.	2020년 10월 21일
VSS 지원 Windows 백업 지원	이제 Amazon EC2 인스턴스에서 실행되는 VSS(Volume Shadow Copy Service) 지원 Windows 애플리케이션을 백업 및 복원할 수 있습니다. 이 기능에 대한 자세한 내용은 Creating Windows VSS backups 섹션을 참조하세요.	2020년 9월 22일
Amazon EFS 자동 백업 지원	이제 Amazon EFS 파일 시스템을 자동으로 AWS Backup 백업하는 데 사용할 수 있습니다. 자세한 내용은 시작하기 4: Amazon EFS 자동 백업 생성 섹션을 참조하세요.	2020년 7월 16일

변경 사항	설명	날짜
신규 AWS 리전	AWS Backup 이제 에서 사용할 수 있습니다 AWS GovCloud (US) Region. 자세한 내용을 알아보려면 AWS 일반 참조의 AWS Backup 엔드포인트 및 할당량을 참조하세요.	2020년 6월 24일
여러 곳에 걸친 백업 관리 지원 AWS 계정	이제 를 사용하여 여러 AWS 계정 백업의 백업을 관리할 수 AWS Organizations있습니다. 자세한 내용은 교차 계정 관리 작동 방식을 참조하십시오.	2020년 6월 24일
아마존 Aurora에 대한 지원이 추가되었습니다. AWS Backup	이제 Amazon Aurora의 리소스를 AWS Backup 백업하도록 구성할 수 있습니다. 자세한 내용은 Amazon Aurora 사용 설명서의 Aurora DB 클러스터 백업 및 복원에 대한 개요를 참조하세요.	2020년 6월 10일
함께 사용할 서비스 구성 지원 AWS Backup	이제 특정 AWS 서비스의 리소스를 AWS Backup 백업하도록 구성할 수 있습니다. 자세한 내용은 서비스 관리 옵트인을 참조하십시오 AWS Backup.	2020년 5월 20일
Amazon EC2 인스턴스 백업 지원 및 교차 리전 백업에 대한 지원도 추가됨	이제 전체 Amazon EC2 인스턴스를 백업하고 AWS 리전전체에서 리소스도 복사할 수 있습니다. 자세한 내용은 Creating backup copies across AWS 리전 섹션을 참조하세요.	2020년 1월 13일

변경 사항	설명	날짜
새 안내서	AWS 출시 AWS Backup 및 AWS Backup 개발자 가이드.	2019년 1월 15일

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