Entwicklerhandbuch

AWS Backup

AWS Backup: Entwicklerhandbuch

Table of Contents

Was ist AWS Backup?

AWS Backup ist ein vollständig verwalteter Service, der es einfach macht, den Datenschutz AWS dienstübergreifend, in der Cloud und vor Ort zu zentralisieren und zu automatisieren. Mit diesem Service können Sie Backup-Richtlinien konfigurieren und die Aktivitäten für Ihre AWS Ressourcen von einem zentralen Ort aus überwachen. Er ermöglicht Ihnen die Automatisierung und Konsolidierung von Backup-Aufgaben, die zuvor ausgeführt wurden service-by-service, und macht die Erstellung benutzerdefinierter Skripts und manueller Prozesse überflüssig. Mit ein paar Klicks in der AWS Backup -Konsole können Sie Ihre Datenschutzrichtlinien und Zeitpläne automatisieren.

AWS Backup steuert keine Backups, die Sie in Ihrer AWS Umgebung außerhalb von erstellen AWS Backup. Wenn Sie also eine zentralisierte end-to-end Lösung für geschäftliche und behördliche Compliance-Anforderungen suchen, sollten Sie AWS Backup noch heute damit beginnen.

Überblick über die Features

AWS Backup bietet viele Funktionen und Fähigkeiten, darunter die folgenden.

Zentralisierte Sicherungsverwaltung

AWS Backup bietet eine zentrale Backup-Konsole, eine Reihe von Backup-APIs und die AWS Command Line Interface (AWS CLI) zur Verwaltung von Backups für alle AWS Dienste, die Ihre Anwendungen verwenden. Mit AWS Backup können Sie Backup-Richtlinien zentral verwalten, die Ihren Backup-Anforderungen entsprechen. Sie können sie dann AWS dienstübergreifend auf Ihre AWS Ressourcen anwenden, sodass Sie Ihre Anwendungsdaten konsistent und gesetzeskonform sichern können. Die AWS Backup zentrale Backup-Konsole bietet eine konsolidierte Ansicht Ihrer Backups und Backup-Aktivitätsprotokolle, was es einfacher macht, Ihre Backups zu überprüfen und die Einhaltung von Vorschriften sicherzustellen.

Richtlinienbasiertes Backup

Mit können Sie Backup-Richtlinien erstellen AWS Backup, die als Backup-Pläne bezeichnet werden. Verwenden Sie diese Backup-Pläne, um Ihre Backup-Anforderungen zu definieren und sie dann auf die AWS Ressourcen anzuwenden, die Sie in den von Ihnen verwendeten AWS Diensten schützen möchten. Sie können separate Sicherungspläne erstellen, die jeweils bestimmten geschäftlichen oder regulatorischen Compliance-Anforderungen entsprechen. Auf diese Weise können Sie sicherstellen,

dass jede AWS Ressource Ihren Anforderungen entsprechend gesichert wird. Sicherungspläne erleichtern die Durchsetzung Ihrer Sicherungsstrategie für Ihre gesamte Organisation und für alle Ihre Anwendungen in skalierbarer Weise.

Alle Konfigurationsoptionen für Backup-Pläne finden Sie unter Optionen und Konfiguration eines Backup-Plans.

Auf Tags basierende Backup-Richtlinien

Sie können AWS Backup Backup-Pläne auf vielfältige Weise auf Ihre AWS Ressourcen anwenden und diese auch taggen. Durch Tagging ist es einfacher, Ihre Backup-Strategie für alle Ihre Anwendungen zu implementieren und sicherzustellen, dass all Ihre AWS Ressourcen gesichert und geschützt sind. AWS Tags sind eine hervorragende Möglichkeit, Ihre AWS Ressourcen zu organisieren und zu klassifizieren. Durch die Integration mit AWS Tags können Sie schnell einen Backup-Plan auf eine Gruppe von AWS Ressourcen anwenden, sodass diese auf konsistente und konforme Weise gesichert werden.

Alle Möglichkeiten, wie Sie Ihre Ressourcen Backup-Plänen zuweisen können, finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan.

Richtlinien für das Lebenszyklus-Management

AWS Backup ermöglicht es Ihnen, Compliance-Anforderungen zu erfüllen und gleichzeitig die Kosten für Backup-Speicher zu minimieren, indem Sie Backups auf einer kostengünstigen Kühlspeicherebene speichern. Sie können Lebenszyklusrichtlinien konfigurieren, die Sicherungen automatisch nach einem von Ihnen festgelegten Zeitplan vom warmen in den kalten Speicher verschieben.

Eine Liste der Ressourcen, die zu Cold Storage übertragen werden können, finden Sie unter Verfügbarkeit von Features nach Ressource. Schritte zur Aktivierung von Cold Storage in Ihrem Backup-Plan finden Sie unter Lebenszyklus und Speicherstufen.

Regionsübergreifende Backups

Mit dieser AWS Backup Option können Sie Backups bei Bedarf oder automatisch im Rahmen eines geplanten Backup-Plans AWS-Regionen auf mehrere verschiedene Backups kopieren. Regionsübergreifende Sicherungen sind besonders dann wertvoll, wenn Betriebskontinuität oder Compliance-Anforderungen das Speichern der Sicherungen in einem Mindestabstand von Ihren

Produktionsdaten erfordern. Weitere Informationen finden Sie unter Erstellen von Backup-Kopien über AWS-Regionen hinweg.

Kontoübergreifende Verwaltung und kontoübergreifende Backups

Sie können es verwenden AWS Backup , um Ihre Backups AWS-Konten innerhalb Ihrer gesamten AWS OrganizationsStruktur zu verwalten. Mit der kontenübergreifenden Verwaltung können Sie automatisch Backup-Richtlinien verwenden, um Backup-Pläne über die AWS-Konten in Ihrer Organisation hinweg anzuwenden. So werden Compliance und Datenschutz effizient und skalierbar, außerdem reduziert sich der Betriebsaufwand. Auch lässt sich damit die manuelle Duplizierung von Sicherungsplänen über einzelne Konten hinweg vermeiden. Weitere Informationen finden Sie unter Verwalten von AWS Backup -Ressourcen über mehrere AWS-Konten hinweg.

Sie können Backups auch in mehrere verschiedene Bereiche AWS-Konten innerhalb Ihrer AWS Organizations Verwaltungsstruktur kopieren. Auf diese Weise können Sie Backups in ein einzelnes Repository-Konto „einbinden“ und dann „verteilen“, um die Ausfallsicherheit zu erhöhen. Erstellen von Backup-Kopien über mehrere AWS-Konten hinweg.

Bevor Sie die Features für kontenübergreifende Verwaltung und Backups verwenden können, muss in AWS Organizations eine vorhandene Organisationsstruktur konfiguriert werden. Eine Organisationseinheit (OU) ist eine Gruppe von Konten, die als eine Einheit verwaltet werden können. AWS Organizations ist eine Liste von Konten, die in Organisationseinheiten gruppiert und als eine Einheit verwaltet werden können.

Prüfung und Berichterstattung mit AWS Backup Audit Manager

AWS Backup Audit Manager hilft Ihnen dabei, die Datenverwaltung und das Compliance-Management Ihrer Backups in allen Bereichen zu vereinfachen AWS. AWS Backup Audit Manager bietet integrierte, anpassbare Kontrollen, die Sie an Ihre organisatorischen Anforderungen anpassen können. Sie können diese Steuerelemente auch verwenden, um Ihre Backup-Aktivitäten und -Ressourcen automatisch zu verfolgen.

AWS Backup Audit Manager kann Ihnen dabei helfen, bestimmte Aktivitäten und Ressourcen zu finden, die den von Ihnen definierten Kontrollen noch nicht entsprechen. Außerdem werden tägliche Berichte erstellt, anhand derer Sie nachweisen können, dass Ihre Kontrollen im Laufe der Zeit eingehalten wurden.

Um Ihre Backup-Compliance mit Ihrem allgemeinen Compliance-Status zu verknüpfen, können Sie die Ergebnisse von AWS Backup Audit Manager automatisch in importieren AWS Audit Manager.

Inkrementelle Sicherungen

AWS Backup speichert Ihre regelmäßigen Backups effizient inkrementell. Beim ersten Backup einer AWS -Ressource wird eine vollständige Kopie Ihrer Daten gesichert. Bei jedem aufeinanderfolgenden inkrementellen Backup werden nur die Änderungen an Ihren AWS Ressourcen gesichert. Durch inkrementelle Backups können Sie vom Datenschutz häufiger Backups profitieren und gleichzeitig die Speicherkosten minimieren.

Eine Liste der Ressourcen, die inkrementelle Backups unterstützen, finden Sie unter Verfügbarkeit von Features nach Ressource.

Vollständige Verwaltung AWS Backup

Einige Ressourcentypen unterstützen die vollständige AWS Backup Verwaltung. Zu den Vorteilen einer vollständigen AWS Backup Verwaltung gehören:

- Unabhängige Verschlüsselung. AWS Backup verschlüsselt Ihre Backups automatisch mit dem KMS-Schlüssel Ihres AWS Backup Tresors, anstatt denselben Verschlüsselungsschlüssel wie Ihre Quellressource zu verwenden. Dies erhöht Ihre Schutzebenen. Weitere Informationen finden Sie unter Verschlüsselung für Backups in AWS Backup.
- **`awsbackup`** Amazon-Ressourcennamen (ARNs). Backup-ARNs beginnen mit `arn:aws:backup` statt `arn:aws:`*`source-resource`*. Auf diese Weise können Sie Zugriffsrichtlinien erstellen, die speziell für Backups und nicht für die Quellressourcen gelten. Weitere Informationen finden Sie unter Zugriffskontrolle.
- Zentralisierte Backup-Abrechnung und Kostenzuordnungs-Tags von Cost Explorer. Gebühren für AWS Backup (einschließlich Speicherung, Datenübertragungen, Wiederherstellungen und vorzeitiges Löschen) werden in Ihrer Amazon Web Services Rechnung unter „Backup“ aufgeführt und nicht unter jeder unterstützten Ressource. Sie können auch Kostenzuordnungs-Tags von Cost Explorer verwenden, um Ihre Backup-Kosten zu verfolgen und zu optimieren. Weitere Informationen finden Sie unter Messung, Kosten und Abrechnung.

Informationen darüber, welche Ressourcentypen für die vollständige AWS Backup Verwaltung in Frage kommen, finden Sie unterVerfügbarkeit von Features nach Ressource.

Überwachung von Backup-Aktivitäten

AWS Backup bietet ein Dashboard, mit dem Sie die Sicherungs- und Wiederherstellungsaktivitäten auf einfache Weise AWS dienstübergreifend überprüfen können. Mit nur wenigen Klicks auf der

AWS Backup Konsole können Sie den Status der letzten Backup-Jobs einsehen. Sie können Jobs auch AWS dienstübergreifend wiederherstellen, um sicherzustellen, dass Ihre AWS Ressourcen ordnungsgemäß geschützt sind.

AWS Backup integriert sich in Amazon CloudWatch und Amazon EventBridge. CloudWatch ermöglicht es Ihnen, Metriken zu verfolgen und Alarme zu erstellen. EventBridge ermöglicht es Ihnen, AWS Backup Ereignisse anzuzeigen und zu überwachen. Weitere Informationen finden Sie unter AWS Backup Ereignisse überwachen mit EventBridge und AWS Backup Metriken überwachen mit CloudWatch.

AWS Backup integriert mit AWS CloudTrail. CloudTrail bietet Ihnen eine konsolidierte Ansicht der Backup-Aktivitätsprotokolle, anhand derer Sie schnell und einfach überprüfen können, wie Ihre Ressourcen gesichert werden. AWS Backup lässt sich auch in Amazon Simple Notification Service (Amazon SNS) integrieren und bietet Ihnen Benachrichtigungen über Backup-Aktivitäten, z. B. wenn ein Backup erfolgreich ist oder eine Wiederherstellung eingeleitet wurde. Weitere Informationen finden Sie unter Protokollieren von AWS Backup API-Aufrufen mit CloudTrail und Verwenden von Amazon SNS zur AWS Backup Ereignisverfolgung.

Schützen Ihrer Daten in Backup-Tresoren

Der Inhalt jedes AWS Backup Backups ist unveränderlich, was bedeutet, dass niemand diesen Inhalt ändern kann. AWS Backup schützt Ihre Backups zusätzlich in Backup-Tresoren, wodurch sie sicher von ihren Quellinstanzen getrennt werden. In Ihrem Tresor werden beispielsweise Ihre Amazon-EC2- und Amazon-EBS-Backups gemäß der von Ihnen ausgewählten Lebenszyklusrichtlinie aufbewahrt, auch wenn Sie die Amazon-EC2-Quell-Instance und die Amazon-EBS-Volumes löschen.

Backup-Tresore bieten ressourcenbasierte Zugriffsrichtlinien, um festzulegen, wer auf Ihre Backups zugreifen kann. Sie können Zugriffsrichtlinien für einen Sicherungstresor definieren, die festlegen, wer auf die Sicherungen in dem Tresor zugreifen kann, und welche Aktionen dort möglich sind. Dies bietet eine einfache und sichere Möglichkeit, den Zugriff auf Ihre Backups dienstübergreifend AWS zu kontrollieren. Informationen zu den AWS vom Kunden verwalteten Richtlinien für AWS Backup finden Sie unter Verwaltete Richtlinien für AWS Backup.

Sie können AWS Backup Vault Lock verwenden, um zu verhindern, dass jemand (auch Sie) Backups löscht oder deren Aufbewahrungszeitraum ändert. AWS Backup Vault Lock hilft Ihnen dabei, ein write-once-read-many(WORM-) Modell durchzusetzen und Ihre Verteidigung um eine weitere Sicherheitsebene zu erweitern. Informationen zu den ersten Schritten finden Sie unter AWS Backup Vault Lock.

Unterstützung bei Compliance-Verpflichtungen

AWS Backup hilft Ihnen dabei, Ihre globalen Compliance-Verpflichtungen zu erfüllen. AWS Backup fällt in den Geltungsbereich der folgenden AWS Compliance-Programme:

- FedRAMP High
- DSGVO
- SOC 1, 2 und 3
- PCI
- HIPAA
- und viele mehr

Erste Schritte

Um mehr darüber zu erfahren AWS Backup, empfehlen wir Ihnen, mit zu beginnenErste Schritte mit AWS Backup.

Unterstützte AWS Ressourcen und Anwendungen

Im Folgenden finden Sie AWS Ressourcen und Drittanbieteranwendungen, mit denen Sie Backups erstellen und wiederherstellen können AWS Backup. Weitere Informationen finden Sie unter the section called “Verfügbarkeit von Funktionen”.

Service	Unterstützte Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon-EC2-Instances (ausgenommen Instance-Speicher-gestützte AMIs)
Amazon-Simple-Storage-Service (Amazon-S3)	Amazon-S3-Daten
Amazon Elastic Block Store (Amazon EBS)	Amazon-EBS-Volumes
Amazon-DynamoDB	Amazon-DynamoDB-Tabellen

Service	Unterstützte Ressourcentypen
Amazon Relational Database Service (Amazon RDS)	Amazon-RDS-Datenbank-Instances (einschließlich aller Datenbank-Engines); Cluster mit mehreren Availability Zones
Amazon Aurora	Aurora-Cluster
Amazon Elastic File System (Amazon EFS)	Amazon-EFS-Dateisysteme
FSx für Lustre	FSx-für-Lustre-Dateisysteme
FSx für Windows File Server	FSx-für-Windows-File-Server-Dateisysteme
Amazon FSx für ONTAP NetApp	FSx-für-ONTAP-Dateisysteme
Amazon FSx für OpenZFS	FSx-für-OpenZFS-Dateisysteme
AWS Storage Gateway (Volume-Gateway)	AWS Storage Gateway Bände
Amazon DocumentDB	Instanzbasierte Amazon DocumentDB-Cluster
Amazon Neptune	Amazon Neptune-Cluster
Amazon-Redshift	Amazon-Redshift-Cluster
Amazon Timestream	Amazon Timestream Timestream-Tabellen
VMware Cloud™ aktiviert AWS	Virtuelle Maschinen von VMware Cloud™ auf AWS
VMware Cloud™ aktiviert AWS Outposts	Virtuelle Maschinen von VMware Cloud™ auf AWS Outposts
AWS CloudFormation	AWS CloudFormation stapelt

Service	Unterstützte Ressourcentypen
SAP-HANA-Datenbanken	SAP HANA-Datenbanken auf Amazon EC2-Instances

Preisgestaltung

Mit AWS Backup zahlen Sie für Backup-Speicher, Datenwiederherstellung, Wiederherstellungstests, regionsübergreifende Datenübertragung und AWS Backup Audit Manager. Weitere Informationen finden Sie unter AWS Backup -Preisgestaltung.

AWS Backup Verfügbarkeit von Funktionen

AWS Backup Funktionen werden je nach Ressource und Ressource angeboten AWS-Region. Die folgenden Abschnitte und Tabellen können Ihnen helfen, die Verfügbarkeit von Features zu ermitteln.

Inhalt

Features, die für alle unterstützten Ressourcen verfügbar sind

AWS Backup bietet die folgenden Funktionen für seine unterstützten AWS Dienste sowie für unterstützte Anwendungen von Drittanbietern. Sofern nicht ausdrücklich erwähnt, sollte nicht davon ausgegangen werden, dass ein Feature oder Service unterstützt wird.

- Automatisierte Backup-Zeitpläne und Aufbewahrungsmanagement
- Zentralisierte Backup-Überwachung
- Verschlüsselte Backups
- Inkrementelle Backups
- Kontoübergreifende Verwaltung mit AWS Organizations
- Automatisierte Backup-Audits und Berichte mit AWS Backup Audit Manager
- Write-once, read-many (WORM) mit Vault Lock AWS Backup

Verfügbarkeit von Features nach Ressource

Um den Dienst AWS Backup mit einem unterstützten AWS Dienst in einer bestimmten Region verwenden zu können, muss der Dienst in der Region verfügbar sein. Um die Verfügbarkeit von Diensten in einer Region zu ermitteln, sehen Sie sich die Dienstendpunkte in der Allgemeine AWS-Referenzan.

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Lebenszyklus bis zur Kühllagerung	Wiederherstellung auf Objektebene [1]	Testen wiederherstellen
Amazon EC2	✓	✓	✓	✓					✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Amazon RDS-Einzelinstanz	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Amazon-RDS-Cluster	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Lebenszyklus bis zur Kühllagerung	Wiederherstellung auf Objektebene 1	Testen wiederherstellen
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx für Lustre	✓	✓	✓	✓					✓
FSx für Windows File Server	✓	✓	✓	✓					✓
FSx für ONTAP			✓ [2]	✓					✓
FSx für OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon DocumentDB	✓ [3]	✓ [3]	✓						✓

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Lebenszyklus bis zur Kühllagerung	Wiederherstellung auf Objektebene [1]	Testen wiederherstellen
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon-Redshift								✓	
Timestream	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					
Virtuelle Maschine	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation Vorlagen	✓	✓		✓ [5]		✓	✓ [5]		
Amazon-DynamoDB			✓						✓

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Lebenszyklus bis zur Kühllagerung	Wiederherstellung auf Objektebene 1	Testen wiederherstellen
Dynamol mit erweiterten AWS Backup -Features	✓	✓	✓			✓	✓		✓
SAP HANA-Datenbanken auf Amazon EC2-Instances				✓	✓	✓	✓		

Bei einigen Ressourcentypen sind sowohl kontinuierliche Backups als auch regions- und kontoübergreifende Kopien verfügbar. Wenn eine regionsübergreifende oder kontoübergreifende Kopie eines kontinuierlichen Backups erstellt wird, wird aus dem kopierten Recovery Point (Backup) ein Snapshot-Backup (regelmäßiges Backup). Amazon RDS und Amazon S3 unterstützen inkrementelle Snapshot-Kopien; Amazon Aurora unterstützt nur vollständige Snapshot-Kopien. Zeitpunktbezogene Wiederherstellung (Point-in-Time Restore, PITR) ist für diese Kopien nicht verfügbar.

[1] Das „Element“ bei einer Wiederherstellung auf Elementebene hängt von der unterstützten Ressource ab. Ein Dateisystemelement ist beispielsweise eine Datei oder ein Verzeichnis, wohingegen ein S3-Element ein S3-Objekt ist. Ein VMware-Objekt ist eine Festplatte. Weitere Informationen dazu finden Sie im Abschnitt Wiederherstellen eines Backups für die unterstützte Ressource.

[2] AWS Backup Audit Manager unterstützt diese Ressource für alle Kontrollen außer kontenübergreifendem Kopieren und regionsübergreifendem Kopieren.

[3] RDS, Aurora, DocumentDB und Neptune unterstützen keine einzelne Kopieraktion, die sowohl regionsübergreifende ALS auch kontoübergreifende Backups durchführt. Sie können sich für eine Option entscheiden. Sie können auch ein AWS Lambda Skript verwenden, um die Fertigstellung Ihrer ersten Kopie abzuwarten, Ihre zweite Kopie auszuführen und dann die erste Kopie zu löschen. RDS-Multi-AZ-Datenbank-Instances (Multi Availability Zone) können kopiert werden, aber Multi-AZ-Cluster unterstützen derzeit kein regionsübergreifendes oder kontoübergreifendes Kopieren. Überlegungen zum regionsübergreifenden Kopieren mit bestimmten RessourcenWeitere Informationen finden Sie unter.

[4] Regionen, in denen Backup Audit Manager unterstützt wird, finden Sie unter Backups mit mehreren Verfügbarkeitszonen in RDS.

[5] Bei CloudFormation Stack-Backups behalten verschachtelte Ressourcen die Funktionen ihrer Quellressourcen bei. Ressourcen innerhalb des Stacks behalten jedoch keine Point-in-Time Restore-Funktionalität (PITR) bei (wie Amazon S3 und Amazon RDS). Die Eigenschaften in der obigen Matrix gelten nur für CloudFormation Vorlagen und nicht für die Ressourcen innerhalb des Stacks.

[6] Für Aurora sind die Snapshots voll und inkrementelle Backups werden über PITR angeboten.

Verfügbarkeit der Funktionen von AWS-Region

AWS Backup ist in allen folgenden Bereichen verfügbar AWS-Regionen. AWS Backup Funktionen sind in all diesen Regionen verfügbar, sofern in der folgenden Tabelle nichts anderes angegeben ist.

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Verwaltung	Kontenübergreifende Backups	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut
USA Ost (Nord-Virginia)	✓	✓	✓	✓	✓
USA Ost (Ohio)	✓	✓	✓	✓	✓
USA West (Nordkalifornien)	✓	✓	✓	✓	✓
USA West (Oregon)	✓	✓	✓	✓	✓
Africa (Cape Town)	✓		✓	✓	✓
Asien-Pazifik (Hongkong)	✓		✓	✓	✓
Asien-Pazifik (Hyderabad)	✓		✓		✓
Asien-Pazifik (Jakarta)	✓		✓		✓
Asien-Pazifik (Melbourne)	✓		✓		✓
Asien-Pazifik (Mumbai)	✓	✓	✓	✓	✓

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Verwaltung	Kontenübergreifende Backups	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut
Asia Pacific (Osaka)	✓	✓	✓		✓
Asia Pacific (Seoul)	✓	✓	✓	✓	✓
Asien-Pazifik (Singapur)	✓	✓	✓	✓	✓
Asien-Pazifik (Sydney)	✓	✓	✓	✓	✓
Asien-Pazifik (Tokio)	✓	✓	✓	✓	✓
Canada (Central)	✓	✓	✓	✓	✓
Kanada West (Calgary)	✓ (außer Amazon S3)		✓		
China (Peking)	✓				
China (Ningxia)	✓				
Europe (Frankfurt)	✓	✓	✓	✓	✓
Europa (Irland)	✓	✓	✓	✓	✓

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Verwaltung	Kontenübergreifende Backups	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut
Europa (London)	✓	✓	✓	✓	✓
Europa (Milan)	✓		✓	✓	✓
Europa (Paris)	✓	✓	✓	✓	✓
Europa (Spain)	✓		✓		✓
Europa (Stockholm)	✓	✓	✓	✓	✓
Europa (Zürich)	✓		✓		✓
Israel (Tel Aviv)	✓		✓		
Naher Osten (Bahrain)	✓		✓	✓	✓
Naher Osten (VAE)	✓		✓		✓
Südamerika (São Paulo)	✓	✓	✓	✓	✓
AWS GovCloud (US-Ost)	✓	✓	✓	✓	

AWS Backup unterstützt	Regionsübergreifende Backups	Kontenübergreifende Verwaltung	Kontenübergreifende Backups	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut
AWS GovCloud (US-West)	✓	✓	✓	✓	

China (Peking) und China (Ningxia) unterstützen das regionsübergreifende Kopieren von einer dieser beiden Regionen in die andere. Regionsübergreifendes Kopieren von diesen Regionen in andere Regionen oder in diese Regionen wird nicht unterstützt. Kontoübergreifendes Kopieren wird für diese Regionen nicht unterstützt.

Das Job-Dashboard ist in AWS GovCloud (US-Ost) und AWS GovCloud (US-West) nicht verfügbar. Die Aggregation von Jobs-Dashboards ist nur in Regionen verfügbar, die kontenübergreifende Verwaltung und AWS Backup Audit Manager unterstützen.

Amazon FSx for Windows File Server und Amazon Neptune unterstützen keine regionsübergreifenden Backup-Kopien in Opt-in-Regionen.

Unterstützte Dienste von AWS-Region

AWS Backup unterstützt in allen unterstützten Regionen Folgendes:

- Aurora
- DynamoDB
- DynamoDB mit erweiterten Funktionen AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon-Redshift
- Amazon RDS

Die folgende Tabelle zeigt die AWS Backup Unterstützung für andere AWS-Services nach Regionen.

Region und Service	Amazon FSx	SAP HANA auf EC2-Instances	Amazon S3	Storage Gateway	Amazon Timestream	VMware und Backup-Gateway
USA Ost (Nord-Virginia)	✓	✓	✓	✓	✓	✓
USA Ost (Ohio)	✓	✓	✓	✓	✓	✓
USA West (Nordkalifornien)	Windows; Lustre; ONTAP	✓	✓	✓		✓
USA West (Oregon)	Windows; Lustre; ONTAP	✓	✓	✓	✓	✓
Afrika (Kapstadt)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Asien-Pazifik (Hongkong)	✓	✓	✓ [1]	✓		✓
Asien-Pazifik (Hyderabad)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asien-Pazifik (Jakarta)	Windows; Lustre; ONTAP		✓	✓		

Region und Service	Amazon FSx	SAP HANA auf EC2-Instances	Amazon S3	Storage Gateway	Amazon Timestream	VMware und Backup-Gateway
Asien-Pazifik (Melbourne)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asien-Pazifik (Mumbai)	✓	✓	✓	✓		✓
Asien-Pazifik (Osaka)	Windows; Lustre	✓	✓ [1]	✓		✓
Asien-Pazifik (Seoul)	✓	✓	✓	✓		✓
Asien-Pazifik (Singapur)	✓	✓	✓	✓		✓
Asien-Pazifik (Sydney)	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Tokio)	✓	✓	✓	✓	✓	✓
Canada (Central)	✓	✓	✓	✓		✓
Kanada West (Calgary)						

Region und Service	Amazon FSx	SAP HANA auf EC2-Instances	Amazon S3	Storage Gateway	Amazon Timestream	VMware und Backup-Gateway
China (Peking)	Windows; Lustre		✓ [1]	✓	✓	
China (Ningxia)	Windows; Lustre		✓ [1]	✓	✓	
Europe (Frankfurt)	✓	✓	✓	✓	✓	✓
Europa (Irland)	✓	✓	✓	✓	✓	✓
Europa (London)	✓	✓	✓	✓		✓
Europa (Milan)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Europa (Paris)	Windows; Lustre; ONTAP	✓	✓	✓		✓
Europa (Spain)	Windows; Lustre; ONTAP		✓ [1]	✓		
Europa (Stockholm)	✓	✓	✓	✓		✓
Europa (Zürich)	Windows; Lustre; ONTAP		✓ [1]	✓		

Region und Service	Amazon FSx	SAP HANA auf EC2-Instances	Amazon S3	Storage Gateway	Amazon Timestream	VMware und Backup-Gateway
Israel (Tel Aviv)	Windows; Lustre; ONTAP		✓ [1]	✓		
Naher Osten (Bahrain)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Naher Osten (VAE)			✓ [1]	✓		
Südamerika (São Paulo)		✓	✓	✓		✓
AWS GovCloud (USA West)	Windows; Lustre; ONTAP		✓ [1]	✓		✓
AWS GovCloud (US-Ost)	Windows; Lustre; ONTAP		✓ [1]	✓		✓

Eine Überprüfung unter Amazon FSx zeigt an, dass FSx for Windows File Server, FSx for Lustre, FSx für ONTAP und FSx für OpenZFS alle in dieser Region von unterstützt werden AWS Backup; andernfalls werden die unterstützten Konfigurationen aufgelistet.

1 Regions- und kontoübergreifendes Kopieren wird nicht unterstützt.

AWS Backup: Funktionsweise

AWS Backup ist ein vollständig verwalteter Backup-Service, der es einfach macht, die Sicherung von Daten AWS dienstübergreifend zu zentralisieren und zu automatisieren. Mit können Sie Backup-Richtlinien erstellen AWS Backup, die als Backup-Pläne bezeichnet werden. Mit diesen Plänen können Sie Ihre Sicherungsanforderungen definieren, z. B. wie häufig Ihre Daten gesichert werden sollen und wie lange diese Sicherungen aufbewahrt werden sollen.

AWS Backup ermöglicht es Ihnen, Backup-Pläne auf Ihre AWS Ressourcen anzuwenden, indem Sie sie einfach taggen. AWS Backup erstellt dann automatisch Backups Ihrer AWS Ressourcen gemäß dem von Ihnen definierten Backup-Plan.

In den folgenden Abschnitten werden die AWS Backup Funktionsweise, Einzelheiten zur Implementierung und Sicherheitsaspekte beschrieben.

Themen

Wie AWS Backup funktioniert mit unterstützten AWS Diensten

Einige AWS Backup unterstützte AWS Dienste bieten ihre eigenen, eigenständigen Backup-Funktionen. Diese Funktionen stehen Ihnen unabhängig davon zur Verfügung, ob Sie AWS Backup nutzen. Die von anderen AWS Diensten erstellten Backups sind jedoch nicht für die zentrale Verwaltung verfügbar. AWS Backup

Um die zentrale Verwaltung des Datenschutzes für all Ihre unterstützten Dienste AWS Backup zu konfigurieren, müssen Sie sich dafür entscheiden, diesen Service mit zu verwalten AWS Backup, ein On-Demand-Backup zu erstellen oder Backups mithilfe eines Backup-Plans zu planen und Ihre Backups in Backup-Tresoren zu speichern.

Themen

- Arbeiten mit Amazon DynamoDB
- Arbeiten mit Amazon-FSx-Dateisystemen
- Arbeiten mit Amazon EC2
- Arbeiten mit Amazon EFS
- Arbeiten mit Amazon EBS
- Arbeiten mit Amazon RDS und Aurora
- Arbeitet mit AWS BackInt
- Arbeiten mit AWS Storage Gateway
- Arbeiten mit Amazon DocumentDB
- Arbeiten mit Amazon Neptune
- Arbeiten mit Amazon Timestream
- Arbeitet mit AWS Organizations
- Arbeitet mit AWS CloudFormation
- Arbeiten mit AWS BackInt, AWS Systems Manager für SAP und SAP HANA
- Wie AWS Dienste ihre eigenen Ressourcen sichern

Entscheiden Sie sich für die Verwaltung von Diensten mit AWS Backup

Wenn neue AWS Dienste verfügbar werden, müssen Sie die Nutzung dieser Dienste aktivieren AWS Backup . Wenn Sie versuchen, eine On-Demand-Sicherung oder einen Sicherungsplan mithilfe von Ressourcen aus einem Service zu erstellen, der nicht aktiviert ist, wird eine Fehlermeldung angezeigt, und der Vorgang kann nicht abgeschlossen werden.

Die AWS Backup Konsole bietet zwei Möglichkeiten, Ressourcentypen in einen Backup-Plan aufzunehmen: Sie können den Ressourcentyp explizit in einem Backup-Plan zuweisen oder alle Ressourcen einbeziehen. Nachfolgend erfahren Sie, wie diese Auswahlmöglichkeiten mit Serviceanmeldungen funktionieren.

- Wenn Ressourcenzuweisungen nur auf Tags basieren, werden die Service-Opt-In-Einstellungen angewendet.
- Wenn ein Ressourcentyp explizit einem Backup-Plan zugewiesen wird, wird er in das Backup aufgenommen, auch wenn das Opt-In für diesen bestimmten Dienst nicht aktiviert ist. Dies gilt nicht für Aurora, Neptune und Amazon DocumentDB. Damit diese Dienste enthalten sind, muss das Opt-In aktiviert sein.

- Wenn in einer Ressourcenzuweisung sowohl der Ressourcentyp als auch die Tags angegeben sind, werden die angegebenen Ressourcentypen zuerst gefiltert, und dann werden diese Ressourcen durch Tags weiter gefiltert.

  Die Opt-In-Einstellungen für Dienste werden für die meisten Ressourcentypen ignoriert. Aurora, Neptune und Amazon DocumentDB erfordern jedoch eine Service-Anmeldung.
- Wenden Sie bei Amazon FSx for NetApp ONTAP bei Verwendung der tagbasierten Ressourcenauswahl Tags auf einzelne Volumes statt auf das gesamte Dateisystem an.

Die Einstellungen für die Service-Anmeldung sind regionsspezifisch. Wenn ein Konto in einer Region verwendet AWS Backup (erstellt einen Backup-Tresor oder einen Backup-Plan), wird das Konto automatisch für alle Ressourcentypen aktiviert, die zu diesem Zeitpunkt AWS Backup in der Region unterstützt werden. Unterstützte Dienste, die zu einem späteren Zeitpunkt zu dieser Region hinzugefügt werden, werden nicht automatisch in einen Backup-Plan aufgenommen. Sie können sich für diese Ressourcentypen entscheiden, sobald sie unterstützt werden.

Um die Dienste zu konfigurieren, die verwendet werden mit AWS Backup

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Service opt-in (Service-Opt-In) die Option Configure resources (Ressourcen konfigurieren) aus.
4. Verwenden Sie die Kippschalter, um die mit AWS Backup verwendeten Dienste zu aktivieren oder zu deaktivieren.

   > **Important**
   >
   > RDS, Aurora, Neptune und DocumentDB haben denselben Amazon-Ressourcennamen (ARN). Wenn Sie sich für die Verwaltung eines dieser Ressourcentypen entscheiden, stimmen Sie bei AWS Backup der Zuweisung zu einem Backup-Plan für alle diese Ressourcentypen zu. Unabhängig davon empfehlen wir Ihnen, sich für alle Optionen zu entscheiden, um Ihren Opt-in-Status korrekt wiederzugeben.

5. Wählen Sie Bestätigen aus.

Arbeiten mit Daten in Amazon S3

AWS Backup bietet vollständig verwaltete Backups und Wiederherstellungen für Amazon S3 S3-Backups. Weitere Informationen hierzu finden Sie unter Amazon-S3-Backups.

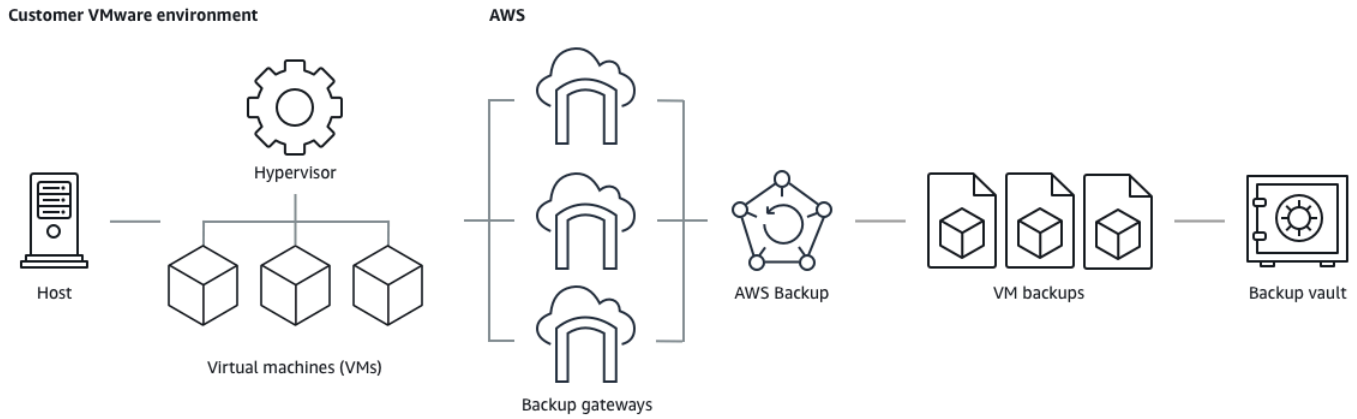
- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon S3 S3-Daten wieder her mit AWS Backup: Wiederherstellen von S3-Daten

Detaillierte Informationen über S3-Daten finden Sie in der Amazon-S3-Dokumentation.

Arbeiten mit virtuellen VMware-Maschinen

AWS Backup unterstützt zentralisierten und automatisierten Datenschutz für lokale virtuelle Maschinen (VMs) von VMware zusammen mit virtuellen Maschinen in der VMware Cloud™ (VMC). AWS Sie können Backups von Ihren lokalen und virtuellen VMC-Computern aus auf erstellen. AWS Backup Anschließend können Sie entweder lokal oder auf VMC wiederherstellen. AWS Backup

Backup Gateway ist herunterladbare AWS Backup Software, die Sie auf Ihren VMware-VMs bereitstellen, um sie mit ihnen zu AWS Backup verbinden. Das Gateway stellt eine Verbindung zu Ihrem VM-Managementserver her, um VMs zu erkennen, Ihre VMs zu erkennen, Daten zu verschlüsseln und Daten effizient an AWS Backup zu übertragen. Das folgende Diagramm zeigt, wie sich das Backup-Gateway mit Ihren VMs verbindet:



- So sichern Sie Ressourcen: Backups virtueller Maschinen
- So stellen Sie VM-Ressourcen wieder her: Wiederherstellen einer virtuellen Maschine mit AWS Backup

Arbeiten mit Amazon DynamoDB

AWS Backup unterstützt das Sichern und Wiederherstellen von Amazon DynamoDB-Tabellen. DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung nahtlos skalierbar bereitstellt.

Seit seiner Einführung AWS Backup hat DynamoDB immer unterstützt. Ab November 2021 wurden AWS Backup auch erweiterte Funktionen für DynamoDB-Backups eingeführt. Zu diesen erweiterten Funktionen gehören das Kopieren Ihrer Backups zwischen AWS-Regionen Konten, das Tiering von Backups in Cold Storage und die Verwendung von Tags für Berechtigungen und Kostenmanagement.

Bei AWS Backup Neukunden, die nach November 2021 bei uns einsteigen, sind die erweiterten DynamoDB-Backup-Funktionen standardmäßig aktiviert.

Wir empfehlen allen AWS Backup Bestandskunden, erweiterte Funktionen für DynamoDB zu aktivieren. Sobald Sie die erweiterten Features aktiviert haben, gibt es keinen Unterschied bei den Preisen für warmen Backup-Speicher. Sie können Geld sparen, indem Sie Backups in Cold Storage verschieben und Ihre Kosten mithilfe von Kostenzuweisungs-Tags optimieren.

Eine vollständige Liste der erweiterten Features und wie Sie sie aktivieren finden Sie unter Erweitertes DynamoDB-Backup.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie DynamoDB-Ressourcen wieder her: Wiederherstellen einer Amazon-DynamoDB-Tabelle

Detaillierte Informationen über DynamoDB finden Sie unter Was ist Amazon DynamoDB? im Amazon-DynamoDB-Entwicklerhandbuch.

Arbeiten mit Amazon-FSx-Dateisystemen

AWS Backup unterstützt das Sichern und Wiederherstellen von Amazon FSx-Dateisystemen. Amazon FSx bietet vollständig verwaltete Dateisysteme von Drittanbietern mit systemeigener Kompatibilität und Funktionsumfang für Workloads. AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx. Backups, die über die AWS Backup Konsole erstellt wurden, haben also dieselbe Konsistenz und Leistung des Dateisystems und dieselben Wiederherstellungsoptionen wie Backups, die über die Amazon-FSx-Konsole erstellt wurden.

Wenn Sie AWS Backup diese Backups verwalten, erhalten Sie zusätzliche Funktionen, wie z. B. unbegrenzte Aufbewahrungsoptionen und die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Darüber hinaus werden Ihre Backups auch nach dem Löschen des Quelldateisystems AWS Backup beibehalten. Dies schützt vor versehentlichem oder böswilligem Löschen.

Wird AWS Backup zum Schutz von Amazon FSx-Dateisystemen verwendet, wenn Sie Backup-Richtlinien konfigurieren und Backup-Aufgaben von einer zentralen Backup-Konsole aus überwachen möchten, die auch die Unterstützung für andere AWS Services erweitert.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon-FSx-Ressourcen wieder her: Wiederherstellen eines FSx-Dateisystems

Ausführliche Informationen zu Amazon-FSx-Dateisystemen finden Sie in der Amazon-FSx-Dokumentation.

Arbeiten mit Amazon EC2

AWS Backup unterstützt Amazon EC2 EC2-Instances.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon-EC2-Ressourcen wieder her: Wiederherstellen einer Amazon-EC2-Instance

Sie können On-Demand-Backup-Jobs planen oder ausführen, die ganze EC2-Instances einschließlich der zugehörigen Amazon EBS-Volumes umfassen. Daher können Sie eine gesamte Amazon EC2 EC2-Instance von einem einzigen Wiederherstellungspunkt aus wiederherstellen, einschließlich des Root-Volumes, der Datenvolumes und einiger Instance-Konfigurationseinstellungen, wie Instance-Typ und key pair.

Sie können auch Ihre VSS-fähigen Microsoft-Windows-Anwendungen sichern und wiederherstellen. Sie können anwendungskonsistente Backups planen, Lebenszyklusrichtlinien definieren und konsistente Wiederherstellungen als Teil eines On-Demand-Backups oder eines geplanten Sicherungsplans durchführen. Weitere Informationen finden Sie unter Erstellen von Windows-VSS-Backups.

AWS Backup startet Ihre EC2-Instances zu keinem Zeitpunkt neu.

Bilder und Schnappschüsse

Erstellt beim Sichern einer Amazon EC2 EC2-Instance AWS Backup einen Snapshot des Amazon EBS-Stammspeicher-Volumes, der Startkonfigurationen und aller zugehörigen EBS-Volumes. AWS Backup speichert bestimmte Konfigurationsparameter der EC2-Instance, einschließlich Instance-Typ, Sicherheitsgruppen, Amazon VPC, Überwachungskonfiguration und Tags. Die Backup-Daten werden als volumengestütztes Amazon EBS (Amazon Machine Image (AMI)) gespeichert.

Wenn Sie einen Amazon Machine Image (AMI) - oder Amazon EBS-Snapshot löschen, der AWS Backup mithilfe von verwendet wird, AWS Backup und Sie den Amazon EC2-Papierkorb konfiguriert haben, können für das Image oder den Snapshot Gebühren gemäß der Amazon EC2-Papierkorb-Richtlinie anfallen. Snapshots und Bilder im Amazon EC2-Papierkorb werden nicht mehr von AWS Backup Richtlinien verwaltet AWS Backup und werden auch nicht mehr verwaltet, wenn Sie sie aus dem Papierkorb wiederherstellen.

AWS Backup verwaltete Amazon EBS-Snapshots und Snapshots, die mit einem AWS Backup verwalteten Amazon EC2 EC2-AMI verknüpft sind und auf die Amazon EBS Snapshot Lock angewendet wurde, dürfen nicht als Teil des Wiederherstellungspunkt-Lebenszyklus gelöscht werden, wenn die Dauer der Snapshot-Sperre den Backup-Lebenszyklus überschreitet. Stattdessen haben diese Wiederherstellungspunkte den Status `EXPIRED`. Diese Wiederherstellungspunkte können manuell gelöscht werden, wenn Sie zuerst das Amazon EBS Snapshot Lock entfernen.

AWS Backup kann EBS-Snapshots verschlüsseln, die mit einem Amazon EC2 EC2-Backup verknüpft sind. Dies ähnelt der Verschlüsselung von EBS-Snapshots. AWS Backup verwendet dieselbe Verschlüsselung, die auf die zugrunde liegenden EBS-Volumes angewendet wurde, wenn ein Snapshot des Amazon EC2 EC2-AMI erstellt wird, und die Konfigurationsparameter der ursprünglichen Instance werden in den Wiederherstellungsmetadaten beibehalten.

Ein Snapshot leitet seine Verschlüsselung vom Volume ab, und dieselbe Verschlüsselung wird auf die entsprechenden Snapshots angewendet. EBS-Snapshots eines kopierten AMI sind immer verschlüsselt. Wenn Sie beim Kopieren einen KMS-Schlüssel angeben, wird der angegebene Schlüssel angewendet. Wenn Sie keinen KMS-Schlüssel angeben, wird ein Standard-KMS-Schlüssel angewendet.

Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch und Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

Arbeiten mit Amazon EFS

AWS Backup unterstützt Amazon Elastic File System (Amazon EFS).

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup

- So stellen Sie Amazon-EFS-Ressourcen wieder her: Wiederherstellen eines Amazon-EFS-Dateisystems

Ausführliche Informationen zu Amazon-EFS-Dateisystemen finden Sie unter Was ist Amazon Elastic File System? im Amazon-Elastic-File-System-Benutzerhandbuch.

Arbeiten mit Amazon EBS

AWS Backup unterstützt Amazon Elastic Block Store (Amazon EBS) -Volumes.

AWS Backup verwaltete Amazon EBS-Snapshots und Snapshots, die mit einem AWS Backup verwalteten Amazon EC2 EC2-AMI verknüpft sind und auf die Amazon EBS Snapshot Lock angewendet wurde, dürfen nicht als Teil des Wiederherstellungspunkt-Lebenszyklus gelöscht werden, wenn die Dauer der Snapshot-Sperre den Backup-Lebenszyklus überschreitet. Stattdessen haben diese Wiederherstellungspunkte den Status `EXPIRED`. Diese Wiederherstellungspunkte können manuell gelöscht werden, wenn Sie zuerst das Amazon EBS Snapshot Lock entfernen.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon-EBS-Volumes wieder her: Wiederherstellen eines Amazon-EBS-Volumes

Weitere Informationen finden Sie unter Amazon EBS-Volumes im Amazon EBS-Benutzerhandbuch.

Arbeiten mit Amazon RDS und Aurora

AWS Backup unterstützt Amazon RDS-Datenbank-Engines und Aurora-Cluster.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon-RDS-Ressourcen wieder her: Wiederherstellen einer RDS-Datenbank
- So stellen Sie Aurora-Cluster wieder her: Wiederherstellung eines Amazon-Aurora-Clusters

Weitere Informationen zu Amazon RDS finden Sie unter Was ist Amazon Relational Database Service? im Amazon-RDS-Benutzerhandbuch.

Ausführliche Informationen zu Aurora finden Sie unter Was ist Amazon Aurora? im Amazon-Aurora-Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen Backup-Auftrag von der Amazon-RDS-Konsole aus starten, kann dies zu einem Konflikt mit einem Backup-Auftrag für Aurora Cluster führen, was zu dem Fehler Backup-Auftrag ist vor Abschluss abgelaufen führt. In diesem Fall konfigurieren Sie ein längeres Backup-Fenster in AWS Backup.

> **Note**
>
> RDS Custom für SQL Server und RDS Custom für Oracle werden derzeit von AWS Backup nicht unterstützt.

> **Note**
>
> AWS berechnet keine Gebühren für Aurora-Snapshots, die in einem Backup-Tresor gespeichert sind, solange Aurora automatisierte Backups aktiviert hat und die Aufbewahrungsdauer für automatische Aurora-Snapshots länger ist als die Aufbewahrungsdauer von Aurora-Snapshots. Alle Snapshots im Backup-Tresor werden in Rechnung gestellt, wenn die Datenbank der Snapshots gelöscht wird (Löschungen können versehentlich oder während der Blau/Grün-Bereitstellung erfolgen).
> Große Snapshots und häufige Backups aus einer gelöschten Datenbank können zu erheblichen Speichergebühren führen. Verwenden Sie den AWS Backup -Rechner, um die möglichen AWS Backup -Gebühren zu schätzen.

Arbeitet mit AWS BackInt

AWS Backup arbeitet mit AWS Backint zusammen, um die Sicherung und Wiederherstellung von SAP HANA-Datenbanken auf Amazon EC2 EC2-Instances zu unterstützen.

- Anweisungen zum Sichern und Wiederherstellen von SAP HANA-Ressourcen: Sicherung und Wiederherstellung von SAP HANA Amazon EC2 EC2-Instances
- Backint Agent einrichten: AWS AWS Backint Agent für SAP HANA

Arbeiten mit AWS Storage Gateway

AWS Backup unterstützt Storage Gateway Volume Gateway. Sie können Amazon-EBS-Snapshots auch als Storage-Gateway-Volumes wiederherstellen.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Storage-Gateway-Ressourcen wieder her: Wiederherstellen eines Storage-Gateway-Volumes.

Arbeiten mit Amazon DocumentDB

AWS Backup unterstützt Amazon DocumentDB-Cluster.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon DocumentDB DocumentDB-Ressourcen wieder her:Wiederherstellen eines DocumentDB-Clusters.

Arbeiten mit Amazon Neptune

AWS Backup unterstützt Amazon Neptune Neptune-Cluster.

- So sichern Sie Ressourcen: Erste Schritte mit AWS Backup
- So stellen Sie Amazon-Neptune-Cluster wieder her: Wiederherstellen eines Neptun-Clusters.

Arbeiten mit Amazon Timestream

AWS Backup unterstützt Amazon Timestream Timestream-Tabellen.

- So sichern Sie Timestream-Tabellen.
- So stellen Sie Timestream-Tabellen wieder her.

Arbeitet mit AWS Organizations

AWS Backup arbeitet mit AWS Organizations , um die kontenübergreifende Überwachung und Verwaltung zu vereinfachen

- Erstellen Sie ein Verwaltungskonto in Organizations.

- Aktivieren Sie kontoübergreifende Verwaltung.
- Benennen Sie delegierte Administratorkonten und delegieren Sie Richtlinien.

Arbeitet mit AWS CloudFormation

AWS Backup unterstützt AWS CloudFormation Vorlagen und Anwendungsstapel

- AWS CloudFormation Backups stapeln

Arbeiten mit AWS BackInt, AWS Systems Manager für SAP und SAP HANA

AWS Backup arbeitet mit AWS BackInt und mit SSM für SAP zur Unterstützung der Sicherungs- und Wiederherstellungsfunktionen von SAP HANA.

- Backup von SAP-HANA-Datenbanken auf Amazon-EC2-Instances
- Beginnen Sie mit AWS Systems Manager für SAP
- AWS Backint Agent für SAP HANA

Wie AWS Dienste ihre eigenen Ressourcen sichern

Informationen zum Sicherungs- und Wiederherstellungsprozess eines bestimmten AWS Dienstes können Sie in der technischen Dokumentation nachschlagen, insbesondere dann, wenn Sie während einer Wiederherstellung eine neue Instanz dieses AWS Dienstes konfigurieren müssen. Es folgt eine Liste der Dokumentation:

- Services rund um Amazon EC2
- Verwendung AWS Backup mit Amazon EFS
- On-Demand-Backup und Wiederherstellung für DynamoDB
- Amazon-EBS-Snapshots
- Sichern und Wiederherstellen einer Amazon-RDS-DB-Instance
  - Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters
- Verwendung AWS Backup mit FSx for Windows File Server
- Verwendung AWS Backup mit FSx for Lustre
- Sichern Sie Ihre Volumes in AWS Storage Gateway

- Sichern und Wiederherstellen in Amazon DocumentDB
- Sichern und Wiederherstellen eines Amazon-Neptune-Clusters

Messung, Kosten und Abrechnung

AWS Backup Preisgestaltung

Aktuelle AWS Backup Preise finden Sie unter AWS Backup Preise.

> **Important**
>
> Um zusätzliche Gebühren zu vermeiden, sollten Sie Ihre Aufbewahrungsrichtlinie mit einer Speicherdauer von mindestens einer Woche für häufig abgerufene Daten konfigurieren. Nehmen wir zum Beispiel an, Sie erstellen tägliche Backups und behalten diese für einen Tag bei. Gehen Sie außerdem davon aus, dass Ihre geschützten Ressourcen so groß sind, dass es den ganzen Tag dauert, bis Ihr Backup abgeschlossen ist. AWS Backup implementiert Ihre Aufbewahrungsfrist von einem Tag und entfernt Ihr Backup aus dem warmen Speicher, wenn Ihr Backup-Job abgeschlossen ist. Am nächsten Tag AWS Backup kann kein inkrementelles Backup erstellt werden, da Sie kein Backup im Warmspeicher haben. Da dieser Aufbewahrungszeitraum nicht den bewährten Methoden entsprach, besteht die Gefahr, dass Sie jeden Tag ein vollständiges Backup erstellen müssen, was mit hohen Kosten verbunden ist.
> Kontaktieren Sie uns AWS Support für weitere Unterstützung.

AWS Backup Abrechnung

Wenn ein Ressourcentyp die vollständige AWS Backup Verwaltung unterstützt, werden die Gebühren für AWS Backup Aktivitäten (einschließlich Speicherung, Datenübertragungen, Wiederherstellungen und vorzeitiges Löschen) im Abschnitt „Backup“ Ihrer Amazon Web Services Rechnung aufgeführt. Eine Liste der Dienste, die eine vollständige AWS Backup Verwaltung unterstützen, finden Sie im Abschnitt Vollständige AWS Backup Verwaltung in der Verfügbarkeit von Features nach Ressource Tabelle.

Wenn ein Ressourcentyp keine vollständige AWS Backup Verwaltung unterstützt, werden einige Ihrer AWS Backup Aktivitäten, z. B. die Speicherkosten für Ihre Backups, vom jeweiligen AWS Dienst abgerechnet.

Fehler beim Kopierauftrag

Ihnen wird erst etwas in Rechnung gestellt, wenn im Zieltresor ein Wiederherstellungspunkt erstellt wurde. Es fallen keine Gebühren an, wenn ein Kopierauftrag fehlschlägt und kein Wiederherstellungspunkt erstellt wird.

Kostenzuordnungs-Tags

Mithilfe von Tags zur Kostenzuweisung können Sie die AWS Backup Kosten detailliert verfolgen und optimieren und diese Tags mithilfe von Tags anzeigen und filtern AWS Cost Explorer.

Informationen zur Verwendung von Kostenzuweisungs-Tags finden Sie unter Automating backups and optimizing backup costs for Amazon EFS using AWS Backup und Verwenden von AWS-Kostenzuordnungs-Markierungen.

AWS Backup Preisgestaltung für Audit Manager

AWS Backup Audit Manager berechnet die Nutzung auf der Grundlage der Anzahl der Kontrollbewertungen. Eine Kontrollbewertung ist die Bewertung einer Ressource anhand einer Kontrolle. Die Gebühren für die Kontrollbewertung werden auf Ihrer AWS Backup Rechnung ausgewiesen. Die aktuellen Preise für die Kontrollbewertung finden Sie unter AWS Backup – Preise.

Um die Steuerelemente von AWS Backup Audit Manager verwenden zu können, müssen Sie die AWS Config Aufzeichnung aktivieren, um Ihre Backup-Aktivitäten nachzuverfolgen. AWS Config Gebühren für jedes aufgezeichnete Konfigurationselement, und diese Gebühren erscheinen auf Ihrer AWS Config Rechnung. Aktuelle Preise für die aufgezeichneten Konfigurationselemente finden Sie unter AWS Config – Preise.

Amazon Aurora – Preise

Während des konfigurierten Aufbewahrungszeitraums für kontinuierliche Aurora-Backups (bis zu 35 Tage) fallen für Snapshots keine Speichergebühren an. Snapshots, die nach Ablauf dieses Zeitfensters beibehalten werden, werden als vollständige Backups berechnet.

AWS Backup Blogs, Videos, Tutorials und andere Ressourcen

Weitere Informationen zu AWS Backup finden Sie unter:

- Backup und Wiederherstellen von virtuellen VMware-Maschinen vor Ort mithilfe von AWS Backup. Mit Olumuyiwa Koya und Ezekiel Oyerinde (Juni 2022).

- Wird AWS Backup zum Schutz von Amazon Aurora Aurora-Datenbanken verwendet. Mit Chris Hendon, Brandon Rubadou und Thomas Liddle (Mai 2022).
- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups. Mit Evan Peck und Sabith Venkitachalapathy (Mai 2022).
- Automatisieren und verbessern Sie Ihre Sicherheitslage mithilfe von AWS Backup und AWS PrivateLink. Mit Bilal Alam (April 2022).
- Erhalten Sie täglich aggregierte, kontenübergreifende Berichte für mehrere Regionen AWS Backup. Mit Wali Akbari und Sabith Venkitachalapathy (Feb. 2022).
- Automatisieren Sie die Sichtbarkeit von Backup-Ergebnissen mithilfe von und. AWS Backup AWS Security Hub Mit Kanishk Mahajan (Jan. 2022).
- Die 10 besten Sicherheitsmethoden zur Sicherung von Backups in AWS. Mit Ibukun Oyewumi (Jan. 2022).
- Optimierung von SAS Grid on AWS mit FSx for Lustre (und Optimierung der Notfallwiederherstellung mithilfe von AWS Backup). Mit Matt Saeger und Shea Lutton (Jan. 2022).
- Zentralisierung von Datenschutz und Compliance in Amazon Neptune mit. AWS Backup Mit Brian O'Keefe (Nov. 2021).
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. Mit Karthik Vijayraghavan (Nov. 2021).
- Vereinfachen Sie die Prüfung Ihrer Datenschutzrichtlinien mit AWS Backup Audit Manager. Mit Jordan Bjorkman und Harshitha Putta (Nov. 2021).
- Verbessern Sie den Sicherheitsstatus Ihrer Backups mit AWS Backup Vault Lock. Mit Rolland Miller (Okt. 2021).
- So behalten Sie Ressourcen-Tags bei AWS Backup Wiederherstellungsaufträgen bei. Mit Ibukun Oyewumi, Amee Shah und Sabith Venkitachalapathy (Sep. 2021).
- Verwaltung des Zugriffs auf Backups mithilfe von Dienststeuerungsrichtlinien mit AWS Backup. Mit Sabith Venkitachalapathy und Ibukun Oyewumi (Aug. 2021).
- Automatisieren Sie zentralisierte Backups in großem Umfang für alle AWS Dienste mithilfe von AWS Backup. Mit Ibukun Oyewumi und Sabith Venkitachalapathy (Juli 2021).
- Blog: So vereinfachen Sie Microsoft SQL Server-Backups mithilfe von AWS Backup VSS. Mit Siavash Irani und Sepehr Samiei (Juli 2021).
- Automatisieren Sie die Validierung der Datenwiederherstellung mit AWS Backup. Mit Mahanth Jayadeva (Juni 2021).

- Konfiguration von Benachrichtigungen zur Überwachung von AWS Backup Jobs. Mit Virgil Ennes (Juni 2021).
- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup. Mit Prachi Gupta und Rohit Verma (Juni 2021).
- Verwaltung der Amazon EFS-Backup-Kosten: AWS Backup Unterstützung für Kostenzuweisungs-Tags. Mit Aditya Maruvada (Mai 2021).
- Erstellen und teilen Sie verschlüsselte Backups über Konten und Regionen hinweg mit AWS Backup. Mit Prachi Gupta (Mai 2021).
- AWS Backup ist jetzt FedRAMP High für Ihre Compliance- und Datenschutzanforderungen zugelassen. Mit Andy Grimes (Mai 2021).
- ZS Associates verbessert die Backup-Effizienz mit. AWS Backup Mit Mitesh Naik, Hiranand Mulchandani und Sushant Jadhav (Mai 2021).
- Tutorial: Amazon EBS Backup and Restore mit AWS Backup. Mit Fathima Kamal (April 2021).
- Video Tutorial: Managing Cross-Region Copies of Backups. Mit David DeLuca (April 2021).
- Löschen Sie mehrere AWS Backup Wiederherstellungspunkte mithilfe von AWS Tools für PowerShell. Mit Sherif Talaat (April 2021).
- Regions- und kontoübergreifende Backups für Amazon FSx verwenden. AWS Backup Mit Adam Hunter und Fathima Kamal (April 2021).
- CloudWatch Amazon-Ereignisse und -Metriken für AWS Backup. Mit Rolland Miller (März 2021).
- Tutorial: Backup und Wiederherstellung mit Amazon Relational Database Service (RDS) mithilfe von AWS Backup. Mit Fathima Kamal (März 2021).
- oint-in-time P-Wiederherstellung und kontinuierliches Backup für Amazon RDS mit AWS Backup. Mit Kelly Griffin (März 2021).
- Automatisieren Sie AWS Backup mit AWS Service Catalog. mit John Husemoller (Januar 2021).
- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup. Mit Cher Simon (Jan. 2021).
- AWS Zusammenfassung von re:Invent: Datenschutz und Einhaltung von. AWS Backup Mit Nancy Wang (Dez. 2020).
- AWS Backup bietet zentralisierten Datenschutz für alle Ihre Ressourcen. AWS Mit Nancy Wang (Nov. 2020).
- Tech Talk: Data protection at scale with AWS Backup. Mit Kareem Behairy (Sep. 2020).
- Zentralisiertes kontenübergreifendes Management mit regionsübergreifender Kopierfunktion. AWS Backup Mit Cher Simon (Sep. 2020).

- Video-Tutorial: Verwaltung von Backups in großem Umfang bei Ihrer AWS Organizations Nutzung. AWS Backup Mit Ildar Sharafeev (Juli 2020).
- Verwaltung von Backups in großem Umfang bei Ihrer AWS Organizations Nutzung AWS Backup. Mit Nancy Wang, Avi Drabkin, Ganesh Sundaresan und Vikas Shah (Juni 2020).
- Stellen Sie Amazon EFS-Dateien und -Ordner wieder her mit AWS Backup. Mit Abrar Hussain und Gurudath Pai (Mai 2020).
- Scheduling automated backups using Amazon EFS and AWS Backup. Mit Rob Barnes (Dez. 2019).
- re:Invent-Aufzeichnung: AWS re:Invent 2019: Tiefer Einblick in ft. AWS Backup Rackspace. Mit Nancy Wang und Jason Pavao (Dez. 2019).
- Schützen Sie Ihre Daten mit AWS Backup. Mit Anthony Fiore (Juli 2019).
- Marketing Video: Introducing AWS Backup. Jan. 2019.
- Video: Introduction to AWS Backup. Mit AWS Schulung und Zertifizierung.

AWS Zum ersten Mal einrichten

Bevor Sie ihn AWS Backup zum ersten Mal verwenden, führen Sie die folgenden Aufgaben aus:

1. Melde dich an für AWS
2. Erstellen eines IAM-Benutzers
3. Erstellen einer IAM-Rolle

Melde dich an für AWS

Wenn Sie sich für Amazon Web Services (AWS) registrieren, AWS-Konto wird Ihr automatisch für alle Dienste in angemeldet AWS, einschließlich AWS Backup. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Weitere Informationen zu den AWS Backup Nutzungstarifen finden Sie auf der Seite mit den AWS Backup Preisen.

Wenn Sie AWS-Konto bereits eine haben, fahren Sie mit der nächsten Aufgabe fort. Wenn Sie kein AWS -Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos aus.

Um eine zu erstellen AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

Notieren Sie sich Ihre AWS-Konto Nummer, da Sie sie für die nächste Aufgabe benötigen.

Erstellen eines IAM-Benutzers

Dienste in AWS, wie, erfordern AWS Backup, dass Sie Anmeldeinformationen angeben, wenn Sie auf sie zugreifen, damit der Dienst feststellen kann, ob Sie über Berechtigungen für den Zugriff auf seine Ressourcen verfügen. AWS empfiehlt, dass Sie nicht den AWS-Konto Root-Benutzer verwenden, um Anfragen zu stellen. Erstellen Sie stattdessen einen IAM-Benutzer, dem Sie vollständigen Zugriff gewähren. Wir bezeichnen diese Benutzer als Administratorbenutzer. Sie können die Admin-Benutzeranmeldedaten anstelle der AWS-Konto Root-Benutzeranmeldedaten verwenden, um mit ihnen zu interagieren AWS und Aufgaben auszuführen, z. B. einen Bucket zu erstellen, Benutzer zu erstellen und ihnen Berechtigungen zu erteilen. Weitere Informationen finden Sie unterAWS-Konto -Root-Benutzeranmeldeinformationen vs. IAM-Benutzeranmeldeinformationen in der AWS Allgemeinen Referenz und IAM Best Practices im IAM User Guide.

Wenn Sie sich für einen IAM-Benutzer registriert haben, AWS aber noch keinen für sich selbst erstellt haben, können Sie mit der IAM-Konsole einen erstellen.

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie die Konfiguration AWS CLI für die Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch vornehmen.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
	Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.		
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren.

Um sich als dieser neue IAM-Benutzer anzumelden, melden Sie sich von der ab. AWS Management Console Verwenden Sie dann die folgende URL, wobei your_aws_account_id Ihre AWS-Konto Nummer ohne Bindestriche ist (wenn Ihre Nummer beispielsweise lautet, ist Ihre ID): AWS-Konto `1234-5678-9012` AWS-Konto `123456789012`

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

Geben Sie den IAM-Benutzernamen und das von Ihnen soeben erstellte Passwort ein. Nachdem Sie sich angemeldet haben, wird in der Navigationsleiste your_user_name@your_aws_account_id angezeigt.

Wenn Sie nicht möchten, dass die URL für Ihre Anmeldeseite Ihre ID enthält, können Sie einen Kontoalias erstellen. AWS-Konto Klicken Sie im IAM-Dashboard auf Konto-Alias erstellen und geben Sie einen Alias, beispielsweise Ihren Firmennamen, ein. Nach dem Erstellen eines Konto-Alias verwenden Sie die folgende URL, um sich anzumelden:

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

Öffnen Sie die IAM-Konsole, um den Anmeldelink für IAM-Benutzer in Ihrem Konto zu prüfen. Sie finden den Link auf dem Dashboard unter AWS-Konto -Alias.

Erstellen einer IAM-Rolle

Sie können die IAM-Konsole verwenden, um eine IAM-Rolle zu erstellen, die AWS Backup Berechtigungen für den Zugriff auf unterstützte Ressourcen gewährt. Nachdem Sie die IAM-Rolle erstellt haben, können Sie Richtlinien erstellen und diese der Rolle anfügen.

So erstellen Sie eine IAM-Rolle mit der Konsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole.
2. Klicken Sie in der IAM-Konsole im Navigationsbereich auf Rollen und wählen Sie Rolle erstellen aus.
3. Wählen Sie AWS Servicerollen und anschließend Auswählen bei AWS Backup. Wählen Sie Weiter: Berechtigungen aus.
4. Aktivieren Sie auf der Seite Berechtigungsrichtlinie anfügen sowohl `AWSBackupServiceRolePolicyForBackup` als auch `AWSBackupServiceRolePolicyForRestores`. Diese AWS verwalteten Richtlinien gewähren die AWS Backup Erlaubnis, alle unterstützten AWS Ressourcen zu sichern und wiederherzustellen. Weitere Informationen zu verwalteten Richtlinien und Beispiele finden Sie unter Verwaltete Richtlinien.

   Klicken Sie dann auf Next: Tags (Weiter: Tags).
5. Wählen Sie Weiter: Prüfen aus.
6. Geben Sie unter Role Name (Rollenname) einen Namen ein, der den Zweck der Rolle beschreibt. Rollennamen müssen innerhalb Ihres Unternehmens eindeutig sein AWS-Konto. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung nicht bearbeitet werden.

Wählen Sie Create Role (Rolle erstellen) aus.

7. Wählen Sie auf der Seite Roles (Rollen) die erstellte Rolle aus, um deren Detailseite zu öffnen.

Erste Schritte mit AWS Backup

Dieses Tutorial zeigt Ihnen die allgemeinen Schritte zur Verwendung von AWS Backup Features und Funktionen. Wie bei jedem Teil dieser technischen Dokumentation sollten Sie den Anweisungen der AWS Managementkonsole im anderen Fenster folgen.

In den folgenden Tutorials erfahren Sie auch, wie Sie einen bestimmten Dienst verwenden AWS Backup können:

- Backup und Wiederherstellung mit Amazon Relational Database Service (Amazon RDS) AWS Backup
- Tutorial: Amazon EBS Backup and Restore mit AWS Backup

Themen

Voraussetzungen

Beginnen Sie erst, wenn Folgendes vorliegt:

- Ein AWS-Konto. Weitere Informationen finden Sie unter AWS Zum ersten Mal einrichten.
- Mindestens eine Ressource wird unterstützt von AWS Backup.
- Sie sollten mit den AWS Diensten und Ressourcen, die Sie sichern, vertraut sein. Sehen Sie sich die Liste der unterstützten AWS -Ressourcen und -Anwendungen von Drittanbietern an.

Wenn neue AWS Dienste verfügbar werden, aktivieren Sie AWS Backup die Nutzung dieser Dienste.

Um die AWS Dienste für die Verwendung mit zu konfigurieren AWS Backup

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Service opt-in (Service-Opt-In) die Option Configure resources (Ressourcen konfigurieren) aus.
4. Verwenden Sie auf der Seite Ressourcen konfigurieren die Kippschalter, um die Dienste zu aktivieren oder zu deaktivieren, die mit AWS Backup verwendet werden. Wählen Sie Confirm (Bestätigen) aus, wenn Ihre Services konfiguriert sind. Stellen Sie sicher, dass der AWS Dienst, für den Sie sich entscheiden, in Ihrem verfügbar ist. AWS-Region

Weitere Informationen Zuweisen von Ressourcen zu einem Backup-Plan finden Sie unter. Die AWS Backup Konsole ermöglicht es einem Benutzer, einem Backup-Plan einen Ressourcentyp zuzuweisen. Dieser Wert wird auch dann berücksichtigt, wenn das Opt-In für diesen bestimmten Dienst nicht aktiviert ist.

- Stellen Sie sicher, dass sich die Ressourcen, die Sie sichern, alle in derselben AWS-Region befinden.

Um dieses Tutorial abzuschließen, können Sie sich mit Ihrem AWS-Konto Root-Benutzer bei der AWS Management Console anmelden. AWS Identity and Access Management (IAM) empfiehlt jedoch, den AWS-Konto Root-Benutzer nicht zu verwenden. Erstellen Sie stattdessen einen Administrator in Ihrem Konto und verwenden Sie dessen Anmeldeinformationen für die Verwaltung der Ressourcen in Ihrem Konto. Weitere Informationen finden Sie unter AWS Zum ersten Mal einrichten.

Die AWS Backup Konsole bietet verschiedene Optionen zum Sichern Ihrer Ressourcen. Sie können ein On-Demand-Backup erstellen, planen und konfigurieren, wie die Ressource gesichert werden soll, oder Ressourcen so konfigurieren, dass sie bei der Erstellung der Ressource automatisch gesichert werden.

Erste Schritte 1: Service-Opt-In

Die AWS Backup Konsole bietet zwei Möglichkeiten, Ressourcentypen in einen Backup-Plan aufzunehmen: Sie können den Ressourcentyp explizit in einem Backup-Plan zuweisen oder alle Ressourcen einbeziehen. Nachfolgend erfahren Sie, wie diese Auswahlmöglichkeiten mit Serviceanmeldungen funktionieren.

- Wenn Ressourcenzuweisungen nur auf Tags basieren, werden die Service-Opt-In-Einstellungen angewendet.
- Wenn ein Ressourcentyp explizit einem Backup-Plan zugewiesen wird, wird er in das Backup aufgenommen, auch wenn das Opt-In für diesen bestimmten Dienst nicht aktiviert ist. Dies gilt nicht für Aurora, Neptune und Amazon DocumentDB. Damit diese Dienste enthalten sind, muss das Opt-In aktiviert sein.
- Wenn in einer Ressourcenzuweisung sowohl der Ressourcentyp als auch die Tags angegeben sind, werden die angegebenen Ressourcentypen zuerst gefiltert, und dann werden diese Ressourcen durch Tags weiter gefiltert.

  Die Opt-In-Einstellungen für Dienste werden für die meisten Ressourcentypen ignoriert. Aurora, Neptune und Amazon DocumentDB erfordern jedoch eine Service-Anmeldung.
- Wenden Sie bei Amazon FSx for NetApp ONTAP bei Verwendung der tagbasierten Ressourcenauswahl Tags auf einzelne Volumes statt auf das gesamte Dateisystem an.

Die Opt-in-Optionen gelten für das jeweilige Konto und. AWS-Region Wenn ein Konto in einer Region verwendet AWS Backup (erstellt einen Backup-Tresor oder einen Backup-Plan), wird das Konto automatisch für alle Ressourcentypen aktiviert, die zu diesem Zeitpunkt von AWS Backup in der Region unterstützt werden. Unterstützte Dienste, die zu einem späteren Zeitpunkt zu dieser Region hinzugefügt werden, werden nicht automatisch in einen Backup-Plan aufgenommen. Sie können sich für diese Ressourcentypen entscheiden, sobald sie unterstützt werden.

Da immer mehr AWS Dienste und Anwendungen von Drittanbietern AWS Backup unterstützt werden, müssen Sie diesen Schritt möglicherweise noch einmal wiederholen, um sich für diese neu unterstützten Ressourcen zu entscheiden.

AWS Backup steuert oder verwaltet keine Backups, die in anderen AWS Umgebungen erstellt wurden als. AWS Backup

Um sich für die Verwendung AWS Backup zum Schutz aller unterstützten Ressourcentypen zu entscheiden

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie unter Service-Opt-In die Option Ressourcen konfigurieren aus.
4. Melden Sie sich für alle AWS Backup unterstützten Ressourcen an, indem Sie alle Schalter nach rechts bewegen.
5. Klicken Sie auf Confirm.

Nächste Schritte

Um ein On-Demand-Backup mit zu erstellen AWS Backup, fahren Sie fort mit. Erste Schritte 2: Ein On-Demand-Backup erstellen

Erste Schritte 2: Ein On-Demand-Backup erstellen

In der AWS Backup Konsole werden auf der Seite Geschützte Ressourcen Ressourcen aufgeführt, von denen AWS Backup mindestens einmal ein Backup erstellt wurde. Wenn Sie es AWS Backup zum ersten Mal verwenden, sind auf dieser Seite keine Ressourcen wie Amazon EBS-Volumes oder Amazon RDS-Datenbanken aufgeführt. Dies gilt auch, wenn eine Ressource einem Sicherungsplan zugewiesen wurde, der Sicherungsplan aber noch nicht mindestens einmal eine geplante Sicherung durchgeführt hat.

In diesem ersten Schritt erstellen Sie eine On-Demand-Sicherung einer Ihrer Ressourcen. Sie sehen dann diese Ressource auf der Seite Protected resources (Geschützte Ressourcen).

So erstellen Sie ein On-Demand-Backup:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und anschließend On-Demand-Backup erstellen aus.
3. Wählen Sie auf der Seite On-Demand-Backup erstellen den Ressourcentyp, den Sie sichern möchten, beispielsweise DynamoDB für Amazon-DynamoDB-Tabellen.

4. Wählen Sie den Namen oder die ID der Ressource aus, die geschützt werden soll. Vergewissern Sie sich, dass es sich bei der ausgewählten Ressource um die gewünschte handelt.

> **Note**
>
> Für Amazon FSx für Lustre werden die Bereitstellungstypen „Persistent“ und „Persistent_2“ unterstützt.

5. Stellen Sie sicher, dass Jetzt Backup erstellen ausgewählt ist. Dies löst sofort ein Backup aus und ermöglicht Ihnen, Ihre gespeicherte Ressource früher auf der Seite Geschützte Ressourcen zu sehen.
6. Geben Sie einen Wert für die Übertragung in das Archiv (falls gewünscht) und ein Ablaufdatum an.

> **Note**
>
> - Eine Liste der Ressourcen, die Sie in den Cold Storage übertragen können, finden Sie unter „Lebenszyklus bis zu Cold Storage“ in der Verfügbarkeit von Features nach Ressource Tabelle. Alle anderen Ressourcentypen werden im Warmspeicher gespeichert und ignorieren den Ausdruck „Übergang zur Kühllagerung“. Der Ablauf-Wert gilt für alle Ressourcentypen.
> - Wenn Backups ablaufen und im Rahmen Ihrer Lebenszyklus-Richtlinie zum Löschen markiert sind, werden die Backups zu einem zufällig ausgewählten Zeitpunkt innerhalb der folgenden 8 Stunden AWS Backup gelöscht. Dieses Zeitfenster trägt dazu bei, eine gleichbleibende Leistung zu ermöglichen.

7. Wählen Sie einen vorhandenen Sicherungstresor. Bei Auswahl von Create new backup vault (Neuen Sicherungstresor auswählen) wird eine neue Seite für die Erstellung des Tresors geöffnet; anschließend kehren Sie zur Seite Create on-demand backup (On-Demand-Sicherung erstellen) zurück.
8. Wählen Sie unter IAM role (IAM-Rolle) Default role (Standard-Rolle).

> **Note**
>
> Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine Rolle mit den richtigen Berechtigungen für Sie erstellt.

9. Wenn Sie Ihrer On-Demand-Sicherung einen oder mehrere Tags zuweisen möchten, geben Sie einen key (Schlüssel) und optional einen value (Wert) ein und wählen Sie Add tag (Tag hinzufügen).

> **Note**
>
> - Kopiert bei Amazon EC2 EC2-Ressourcen AWS Backup automatisch bestehende Gruppen- und einzelne Ressourcen-Tags sowie alle Tags, die Sie zu dieser Sicherung hinzufügen. Weitere Informationen finden Sie unter Tags auf Backups kopieren.
> - Wenn Sie bei der Erstellung eines tagbasierten Backup-Plans eine andere Rolle als die Standardrolle wählen, stellen Sie sicher, dass diese über die erforderlichen Berechtigungen verfügt, um alle markierten Ressourcen zu sichern. AWS Backup versucht, alle Ressourcen mit den ausgewählten Tags zu verarbeiten. Wenn eine Ressource gefunden wird, auf die sie keine Zugriffsberechtigung hat, schlägt der Sicherungsplan fehl.

10. Wählen Sie On-Demand-Backup erstellen. Dadurch gelangen Sie zur Seite Jobs (Aufträge), die eine Liste von Aufträgen anzeigt.
11. Wenn Ihr Ressourcentyp EC2 ist, wird der Abschnitt Erweiterte Backup-Einstellungen angezeigt. Wählen Sie Windows VSS, wenn auf Ihrer EC2-Instance Microsoft Windows ausgeführt wird. Auf diese Weise können Sie anwendungskonsistente Windows-VSS-Backups erstellen.

> **Note**
>
> AWS Backup unterstützt derzeit nur anwendungskonsistente Backups von Ressourcen, die auf Amazon EC2 ausgeführt werden. Nicht alle Instance-Typen oder Anwendungen werden für Windows-VSS-Backups unterstützt. Weitere Informationen finden Sie unter Erstellen von Windows-VSS-Backups.

12. Wählen Sie die Backup job ID (Sicherungsaufgaben-ID) für die Ressource aus, die Sie für die Sicherung ausgewählt haben, um die Details der Aufgabe anzuzeigen.

Nächste Schritte

Zur Automatisierung Ihrer Backup-Aktivität fahren Sie mit Erste Schritte, Schritt 3: Erstellen einer geplanten Sicherung fort.

Erste Schritte, Schritt 3: Erstellen einer geplanten Sicherung

In diesem Schritt des AWS Backup Tutorials erstellen Sie einen Backup-Plan, weisen ihm Ressourcen zu und erstellen dann einen Backup-Tresor.

Stellen Sie zuerst sicher, dass die erforderlichen Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter Erste Schritte mit AWS Backup.

Themen

Schritt 1: Einen Backup-Plan basierend auf einem bestehenden erstellen

Ein Backup-Plan ist ein Richtlinienausdruck, der definiert, wann und wie Sie Ihre AWS -Ressourcen, wie beispielsweise Amazon-DynamoDB-Tabellen oder Dateisysteme von Amazon Elastic File System (Amazon EFS), sichern möchten. Sie weisen den Backup-Plänen Ressourcen zu und erstellen AWS Backup dann automatisch Backups für diese Ressourcen und bewahren sie entsprechend dem Backup-Plan auf. Weitere Informationen finden Sie unter Verwalten von Backups mithilfe von Backup-Plänen.

Es gibt zwei Möglichkeiten, einen neuen Sicherungsplan zu erstellen: Sie können einen solchen von Grund auf oder basierend auf einem vorhandenen Sicherungsplan erstellen. In diesem Beispiel wird die AWS Backup Konsole verwendet, um einen Backup-Plan zu erstellen, indem ein vorhandener Backup-Plan geändert wird.

So erstellen Sie einen Sicherungsplan aus einem vorhandenen Sicherungsplan

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Dashboard Manage Backup plans (Sicherungspläne verwalten) aus. Sie können auch im Navigationsbereich Backup-Pläne und Backup-Plan erstellen auswählen.
3. Wählen Sie Mit Vorlage beginnen aus. Wählen Sie anschließend einen Plan aus der Liste aus (z. B. `Daily-Monthly-1yr-Retention`) und geben Sie einen Namen in das Feld Name des Backup-Plans ein.

> **Note**
>
> Wenn Sie versuchen, einen Sicherungsplan zu erstellen, der mit einem vorhandenen Plan identisch ist, erhalten Sie einen `AlreadyExistsException`-Fehler.

4. Wählen Sie auf der Übersichtsseite des Plans die gewünschte Backup-Regel und dann Bearbeiten aus.
5. Prüfen und wählen Sie die Werte, die Sie für Ihre Regel verwenden möchten (für die Regeloptionen siehe Optionen und Konfiguration eines Backup-Plans).
6. Wählen Sie für den Backup-Tresor Standard aus oder wählen Sie Neuen Sicherungstresor erstellen aus, um einen neuen Tresor zu erstellen.
7. (Optional) — Wählen Sie eine AWS-Region aus der Liste unter Zielregion aus, um das Backup in eine andere Region zu kopieren. Um weitere Regionen hinzuzufügen, wählen Sie Kopie hinzufügen aus.
8. Wenn Sie mit der Bearbeitung der Regel fertig sind, wählen Sie Backup-Regel speichern aus.

Wählen Sie auf der Seite Summary (Zusammenfassung) die Option Assign resources (Ressourcen zuweisen) aus, um den nächsten Abschnitt vorzubereiten.

Schritt 2: Ressourcen zu einem Backup-Plan zuweisen

Nachdem Sie einen Backup-Plan erstellt haben, müssen Sie Ihre AWS Ressourcen diesem Backup-Plan zuweisen. Weitere Informationen zum Zuweisen von Ressourcen finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan.

Wenn Sie noch nicht über AWS Ressourcen verfügen, die Sie einem Backup-Plan zuweisen möchten, erstellen Sie einige neue Ressourcen, die Sie für diese Übung verwenden möchten. Erstellen Sie eine oder zwei Ressourcen mithilfe unterstützter AWS -Ressourcen und Drittanbieteranwendungen.

So weisen Sie Ressourcen einem Sicherungsplan zu:

1. Die vorherigen Schritte sollten Sie zur Seite Ressourcen zuweisen geführt haben.
2. Geben Sie unter Name der Ressourcenzuweisung einen Namen ein.
3. Wählen Sie für die IAM-Rolle die Standardrolle aus. Wenn Sie eine andere Rolle auswählen, muss sie über die Berechtigung verfügen, alle Ressourcen zu sichern, die Sie zuweisen.

4. Wählen Sie im Abschnitt Ressourcen zuweisen die Option Alle Ressourcentypen einschließen aus. Ein Ressourcentyp ist ein AWS Backup unterstützter AWS Dienst oder eine Drittanbieteranwendung. Dieser Backup-Plan schützt jetzt alle Ressourcentypen, für deren Schutz Sie sich entschieden haben AWS Backup
5. Wählen Sie Ressourcen zuweisen aus.

Sie kehren zur Seite mit der Zusammenfassung des Backup-Plans zurück. Wählen Sie Backup-Plan erstellen aus, um Ihren ersten Backup-Plan einzurichten!

Schritt 3: Einen Backup-Tresor erstellen

Anstatt den Standard-Sicherungstresor zu verwenden, der für Sie automatisch in der AWS Backup -Konsole erstellt wird, können Sie spezifische Sicherungstresore erstellen, um Gruppen von Sicherungen in einem Tresor zu speichern und zu organisieren.

Weitere Informationen zu Sicherungstresoren finden Sie unter Sicherungstresore.

So erstellen Sie einen Sicherungstresor:

1. Wählen Sie auf der AWS Backup Konsole im Navigationsbereich Backup-Tresore aus.

> **Note**
>
> Wenn der Navigationsbereich auf der linken Seite nicht sichtbar ist, können Sie ihn öffnen, indem Sie auf das Menüsymbol in der oberen linken Ecke der Konsole klicken. AWS Backup

2. Wählen Sie Create backup vault (Sicherungstresor erstellen) aus.
3. Geben Sie einen Namen für Ihren Sicherungstresor ein. Sie können den Namen Ihres Tresors so wählen, dass er angibt, was in ihm gespeichert wird, oder so, dass die Suche nach den benötigten Sicherungen erleichtert wird. Geben Sie ihm beispielsweise den Namen **`FinancialBackups`**.
4. Wählen Sie eine Taste AWS Key Management Service (AWS KMS) aus. Sie können entweder einen Schlüssel verwenden, den Sie bereits erstellt haben, oder den AWS Backup Standard-KMS-Schlüssel auswählen.

> **Note**
>
> Der hier angegebene AWS KMS Schlüssel gilt nur für Backups von Diensten, die AWS Backup unabhängige Verschlüsselung unterstützen. Eine Liste der Ressourcentypen, die AWS Backup unabhängige Verschlüsselung unterstützen, finden Sie im Abschnitt „Vollständige AWS Backup Verwaltung“ der Verfügbarkeit von Features nach Ressource Tabelle.

5. Optional können Sie Tags hinzufügen, die Ihnen dabei helfen, Ihren Sicherungstresor zu finden und zu identifizieren. Beispielsweise können Sie den Tag **`BackupType:Financial`** hinzufügen.
6. Wählen Sie Create backup vault (Sicherungstresor erstellen) aus.
7. Wählen Sie im Navigationsbereich die Option Backup vaults (Sicherungstresore), und prüfen Sie, ob Ihr Sicherungstresor hinzugefügt wurde.

> **Note**
>
> Sie können jetzt eine Sicherungsregel in einem Ihrer Sicherungspläne bearbeiten, um Sicherungen, die mit dieser Regel erstellt wurden, im soeben erstellten Sicherungstresor zu speichern.

Nächste Schritte

Um speziell Amazon-EFS-Dateisysteme zu sichern, fahren Sie mit Erste Schritte 4: Automatische Amazon-EFS-Backups erstellen fort.

Erste Schritte 4: Automatische Amazon-EFS-Backups erstellen

Wenn Sie ein Amazon Elastic File System (Amazon EFS)-Dateisystem mit der Amazon-EFS-Konsole erstellen, sind automatische Backups standardmäßig aktiviert. Wenn Sie ein vorhandenes Amazon-EFS-Dateisystem automatisch sichern möchten, können Sie dies mithilfe der Amazon-EFS-Konsole, API oder CLI tun.

Um ein vorhandenes Amazon-EFS-Dateisystem mithilfe der Konsole automatisch zu sichern,

1. öffnen Sie die Amazon-EKS-Konsole unter https://console.aws.amazon.com/efs.

2. Wählen Sie auf der Seite Dateisysteme ein Dateisystem aus, um automatische Backups zu aktivieren.
3. Wählen Sie Bearbeiten im Bereich der Allgemeinen Einstellungen aus.
4. Um automatische Backups zu aktivieren, wählen Sie Automatische Backups aktivieren aus.

Die Standardeinstellung für den Backup-Plan ist `daily backups, 35-day retention`. Das Standard-Backup-Fenster (der Zeitrahmen, in dem das Backup durchgeführt wird) ist so eingestellt, dass es um 5.00 Uhr UTC (Coordinated Universal Time) beginnt und 8 Stunden dauert.

> **Note**
>
> Der automatische Backup-Tresor von Amazon EFS `aws/efs/automatic-backup-vault` ist nur für diese automatischen Backups reserviert.
> Dieser Tresor sollte nicht zum Erstellen von kontoübergreifenden Kopien oder als Ziel für Backups verwendet werden, die im Rahmen anderer nicht automatisierter Backup-Pläne erstellt wurden. Wenn Sie ihn als Ziel für andere Backup-Pläne verwenden, erhalten Sie die Fehlermeldung „unzureichende Berechtigungen“.

AWS Backup erstellt in Ihrem Namen eine dienstbezogene Rolle in Ihrem Konto. Diese Rolle hat die erforderlichen Berechtigungen für die Durchführung von Amazon-EFS-Backups. Ausführliche Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Backup.

step-by-step Anweisungen zum Ein- und Ausschalten von automatischen Backups mithilfe der Amazon EFS-Konsole, API oder CLI finden Sie unter Automatische Backups im Amazon Elastic File System-Benutzerhandbuch.

Nächste Schritte

Wenn Sie die von Ihnen erstellten Backups anzeigen möchten, fahren Sie mit Erste Schritte 5: Ihre Backup-Aufträge und Wiederherstellungspunkte anzeigen fort.

Erste Schritte 5: Ihre Backup-Aufträge und Wiederherstellungspunkte anzeigen

Mit AWS Backup können Sie den Status und andere Details der Sicherungs- und Wiederherstellungsaktivitäten der von Ihnen verwendeten AWS Dienste einsehen.

Auf dem AWS Backup Dashboard können Sie Sicherungspläne verwalten, On-Demand-Backups erstellen, Backups wiederherstellen und den Status von Sicherungs- und Wiederherstellungsaufträgen einsehen.

Themen

Den Status von Backup-Aufträgen anzeigen

Verwenden Sie das AWS Backup Dashboard, um schnell den Status Ihrer Sicherungs- und Wiederherstellungsaktivitäten einzusehen.

So zeigen Sie den Status der Sicherungsaufgabe an

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wählen Sie zur Anzeige des Status Ihrer Sicherungsaktivitäten Backup jobs details (Sicherungsauftragsdetails). Dadurch gelangen Sie zur Seite Backup jobs (Sicherungsaufgaben), auf der Tabellen mit den Sicherungs- und Wiederherstellungsaufgaben angezeigt werden.
4. Sie können die Aufgaben, die nach Zeit angezeigt werden, filtern. Beispielsweise Aufgaben, die in den letzten 24 Stunden, in der letzten Woche oder in den letzten 30 Tagen erstellt wurden. Sie können auch mithilfe des Zahnradsymbols die Anzahl der pro Seite anzuzeigenden Aufträge festlegen.

Alle Backups in einem Tresor anzeigen

Befolgen Sie diese Schritte, um die Sicherungen anzuzeigen, die in einem bestimmten Tresor in AWS Backup erstellt wurden.

So zeigen Sie alle Sicherungen in einem Tresor an

1. Wählen Sie auf der AWS Backup Konsole im Navigationsbereich Backup-Tresore aus.
2. Wählen Sie den Tresor, den Sie beim Erstellen einer On-Demand- oder geplanten Sicherung verwendet haben, und zeigen Sie alle Sicherungen an, die in diesem Tresor erstellt wurden.

> **Note**
>
> Jedes Backup hat einen Status, der normalerweise Abgeschlossen lautet. Wenn ein Backup aus irgendeinem Grund nicht gemäß seiner Lebenszykluskonfiguration gelöscht werden AWS Backup kann, wird dieses Backup als Abgelaufen markiert. Ihnen wird der Speicherplatz in Rechnung gestellt, den abgelaufene Backups belegen. Sie sollten diese löschen.

Anzeigen der Details geschützter Ressourcen

Auf der Seite Protected resources (Geschützte Ressourcen) finden Sie Details zu den in AWS Backup gesicherten Ressourcen.

So zeigen Sie geschützte Ressourcen an

1. Wählen Sie auf der AWS Backup Konsole im Navigationsbereich die Option Geschützte Ressourcen aus.
2. Sehen Sie sich die AWS Ressourcen an, die gesichert werden. Wählen Sie eine Ressource in der Liste, um Ihre Sicherungen für diese Ressource zu betrachten.

Nächste Schritte

Um einen von Ihnen angezeigten Wiederherstellungspunkt wiederherzustellen, fahren Sie mit Erste Schritte 6: Ein Backup wiederherstellen fort.

Erste Schritte 6: Ein Backup wiederherstellen

Nachdem eine Ressource mindestens einmal gesichert wurde, gilt sie als geschützt und kann mit ihr wiederhergestellt werden AWS Backup. Gehen Sie wie folgt vor, um eine Ressource mit der AWS Backup -Konsole wiederherzustellen.

Informationen zu Wiederherstellungsparametern für bestimmte Dienste oder zum Wiederherstellen eines Backups mithilfe der AWS CLI oder der AWS Backup API finden Sie unter Backup wiederherstellen.

So stellen Sie eine Ressource wieder her

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Protected resources (Geschützte Ressourcen) und die Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Eine Liste Ihrer Wiederherstellungspunkte, einschließlich des Ressourcentyps, wird nach Resource ID (Ressourcen-ID) angezeigt. Wählen Sie eine Ressource aus, um die Seite Resource details (Ressourcendetails) zu öffnen.
4. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
5. Geben Sie die Wiederherstellungsparameter an. Die Wiederherstellungsparameter werden für den jeweils ausgewählten Ressourcentyp angezeigt.

   > **Note**
   >
   > Wenn Sie nur eine Sicherung beibehalten, können Sie den Status des Dateisystems nur zum Zeitpunkt der Sicherung wiederherstellen. Sie können keine vorherigen inkrementellen Sicherungen wiederherstellen.

   Anweisungen zum Wiederherstellen bestimmter Ressourcen finden Sie unter Wiederherstellen eines Backups.
6. Wählen Sie bei Restore role (Rolle Wiederherstellen) die Option Default role (Standardrolle).

> **Note**
>
> Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine Rolle mit den richtigen Berechtigungen für Sie erstellt.

7. Wählen Sie Restore backup aus.

   Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

> **Note**
>
> Wenn Sie eine Wiederherstellung durchführen, um bestimmte Elemente innerhalb einer Amazon-EFS-Instance wiederherzustellen, können Sie diese Elemente entweder in einem neuen oder einem vorhandenen Dateisystem wiederherstellen. Wenn Sie die Elemente in einem vorhandenen Dateisystem wiederherstellen, AWS Backup erstellt ein neues Amazon EFS-Verzeichnis aus dem Stammverzeichnis, das die Elemente enthält. Die vollständige Hierarchie der angegebenen Elemente bleibt im Wiederherstellungsverzeichnis erhalten. Wenn Verzeichnis A beispielsweise die Unterverzeichnisse B, C und D enthält, wird die hierarchische Struktur AWS Backup beibehalten, wenn A, B, C und D wiederhergestellt werden.
> Unabhängig davon, ob Sie eine teilweise Amazon-EFS-Wiederherstellung eines vorhandenen Dateisystems oder eines neuen Dateisystems durchführen, erstellt jeder Wiederherstellungsversuch ein neues Wiederherstellungsverzeichnis aus dem Stammverzeichnis, das die wiederhergestellten Dateien enthält. Wenn Sie mehrere Wiederherstellungen für denselben Pfad versuchen, existieren möglicherweise mehrere Verzeichnisse, die die wiederhergestellten Elemente enthalten.

Stellen Sie eine Amazon-EFS-Instance wie folgt wieder her:

Wenn Sie eine Amazon–EFS-Instance wiederherstellen, können Sie eine Vollständige Wiederherstellung durchführen, mit der das gesamte Dateisystem wiederherstellt wird. Sie können auch bestimmte Dateien und Verzeichnisse mithilfe der Wiederherstellung auf Elementebene wiederherstellen (Wiederherstellungen auf Elementebene haben Beschränkungen). Weitere Informationen finden Sie unter Wiederherstellen eines EFS-Dateisystems). Informationen zum Wiederherstellen anderer Ressourcentypen finden Sie unter Wiederherstellen eines Backups.

> **Note**
>
> Um eine Amazon-EFS-Instance wiederherzustellen, müssen Sie `backup:startrestorejob` „Zulassen“.

Ausführliche Informationen zur Wiederherstellung eines Backups finden Sie unter Wiederherstellen eines Backups.

Nächste Schritte

Mit AWS Backup Audit Manager können Sie Ihre Backup-Aktivitäten und Ressourcen überprüfen. Sie können auch Berichte erstellen, die Sie als Nachweis für Ihre Backup-, Wiederherstellungs- und Kopieraufträge verwenden können. Informationen zum Erstellen eines Berichts finden Sie unter Erste Schritte 7: Einen Auditbericht erstellen:

Erste Schritte 7: Einen Auditbericht erstellen

In Erste Schritte 5: Ihre Backup-Aufträge und Wiederherstellungspunkte anzeigen haben Sie Ihre Backup-Aktivitäten in den Ansichten AWS Backup Dashboard, Backup-Tresor und Geschützte Ressourcen beobachtet. Diese Ansichten sind jedoch dynamisch und werden je nachdem, wann Sie sie aufrufen, aktualisiert. Sie sind nicht unbedingt der beste Beweis für die kontinuierliche Einhaltung der Datenschutzanforderungen und -kontrollen Ihres Unternehmens im Laufe der Zeit.

In diesem Schritt erstellen Sie mit AWS Backup Audit Manager einen Bericht über On-Demand-Backup-Jobs.

AWS Backup Audit Manager liefert täglich und auf Abruf eine Vielzahl von Auditberichten in CSV-, JSON- oder beiden Formaten an Ihren Amazon S3 S3-Bucket. Sie können die Konformität Ihrer Backup-Aktivitäten und Ressourcen anhand einer Reihe anpassbarer Kontrollen überprüfen und Berichte über Ihre Backup-, Kopier- und Wiederherstellungsaufträge erhalten. Der Bericht zum Backup-Auftrag belegt, dass Ihre Backup-Aufträge durchgeführt wurden.

Es folgt ein Beispiel für einen Backup-Plan.

```
{
  "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"
    }
  ]
}
```


Zum Erstellen eines Backup-Berichts (einschließlich eines On-Demand-Backup-Berichts), erstellen Sie zunächst einen Berichtsplan, um Ihre Berichte zu automatisieren und sie an einen Amazon-S3-Bucket zu senden.

Ein Berichtsplan setzt voraus, dass Sie über einen Amazon-S3-Bucket verfügen, um Ihre Berichte zu empfangen. Anweisungen zur Einrichtung eines neuen S3-Buckets finden Sie unter Schritt 1: Erstellen des ersten S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Gehen Sie wie folgt vor, um einen Berichtsplan zu skalieren:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie Berichtsplan erstellen aus.
4. Wählen Sie Bericht zu Sicherungsaufträgen aus der Dropdown-Liste aus.
5. Geben Sie für Name des Berichtsplans **`TestBackupJobReport`** ein.
6. Wählen Sie als Dateiformat sowohl CSV als auch JSON aus.

7. Wählen Sie für den Namen des S3-Buckets das Ziel für Ihre Berichte aus der Dropdown-Liste aus.
8. Wählen Sie Berichtsplan erstellen aus.

Als Nächstes müssen Sie zulassen, dass Ihr S3-Bucket Berichte von empfängt AWS Backup. AWS Backup Audit Manager generiert automatisch eine S3-Zugriffsrichtlinie für Sie.

Gehen Sie wie folgt vor, um diese Zugriffsrichtlinie anzuzeigen und anzuwenden:

1. Wählen Sie im linken Navigationsbereich Berichte aus.
2. Wählen Sie unter Name des Berichtsplans den Namen Ihres Berichtsplans aus (`TestBackupJobReport`).
3. Wählen Sie Bearbeiten aus.
4. Wählen Sie Zugriffsrichtlinie für S3-Bucket anzeigen aus.
5. Wählen Sie Berechtigungen kopieren aus.
6. Wählen Sie Bucket-Richtlinie bearbeiten aus, um die Richtlinie Ihres Ziel-S3-Buckets so zu bearbeiten, dass dieser Ihre Berichte über Backup-Aufträge empfangen kann.
7. Kopieren Sie die Berechtigungen oder fügen Sie sie der Ziel-S3-Bucket-Richtlinie hinzu.

Erstellen Sie als Nächstes Ihren ersten Bericht über Backup-Aufträge

Gehen Sie wie folgt vor, um einen On-Demand-Backup-Bericht zu erstellen:

1. Wählen Sie im linken Navigationsbereich Berichte aus.
2. Wählen Sie unter Name des Berichtsplans den Namen Ihres Berichtsplans aus (`TestBackupJobReport`).
3. Wählen Sie On-Demand-Bericht erstellen aus.

Sehen Sie sich abschließend Ihren Bericht an.

Gehen Sie wie folgt vor, um Ihren Bericht anzuzeigen:

1. Wählen Sie im linken Navigationsbereich Berichte aus.
2. Wählen Sie unter Name des Berichtsplans den Namen Ihres Berichtsplans aus (`TestBackupJobReport`).

3. Wählen Sie im Abschnitt Aufträge melden den S3-Link aus. Dadurch werden Sie zum Ziel-S3-Bucket geleitet.
4. Wählen Sie Herunterladen aus.
5. Öffnen Sie den Bericht mit dem Programm, das Sie für die Arbeit mit CSV- oder JSON-Dateien verwenden.

Nächste Schritte

Um Ihre Ressourcen für die ersten Schritte zu bereinigen und unerwünschte Gebühren zu vermeiden, fahren Sie mit Erste Schritte 8: Ressourcen bereinigen fort.

Erste Schritte 8: Ressourcen bereinigen

Nachdem Sie alle Aufgaben in Erste Schritte mit AWS Backup durchgeführt haben, sollten Sie bereinigen, was Sie erstellt haben, um unnötige Gebühren zu vermeiden.

Themen

Schritt 1: Löschen Sie die wiederhergestellten Ressourcen AWS

Um AWS Ressourcen zu löschen, die Sie von einem Recovery Point wiederhergestellt haben, wie Amazon Elastic Block Store (Amazon EBS) -Volumes oder Amazon DynamoDB-Tabellen, verwenden Sie die Konsole für diesen Service. Verwenden Sie zum Beispiel zum Löschen eines Amazon Elastic File System (Amazon EFS)-Dateisystems die Amazon-EFS-Konsole.

> **Note**
>
> Diese Informationen beziehen sich auf wiederhergestellte Ressourcen, nicht auf Wiederherstellungspunkte, die in einem Sicherungstresor gespeichert sind.

Schritt 2: Backup-Plan löschen

Wenn Sie keine geplanten Sicherungen erstellen möchten, sollten Sie Ihre Sicherungspläne löschen. Sie müssen alle Ressourcenzuweisungen für einen Backup-Plan löschen, bevor der Backup-Plan selbst gelöscht werden kann.

Gehen Sie zum Löschen eines Sicherungsplans wie folgt vor:

So löschen Sie einen Sicherungsplan

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.
3. Wählen Sie auf der Seite Backup plans (Sicherungspläne) den Sicherungsplan, den Sie löschen möchten. Dadurch gelangen Sie zur Seite mit den Details für diese Sicherung.
4. Wählen Sie zum Löschen der Ressourcenzuweisungen für Ihren Plan das Optionsfeld neben dem Namen der Zuweisung und wählen Sie dann Delete (Löschen).
5. Wählen Sie zum Löschen des Sicherungsplans oben rechts auf der Seite Delete (Löschen).
6. Geben Sie auf der Bestätigungsseite den Namen des Plans ein und wählen Sie Delete plan (Plan löschen).

Schritt 3: Wiederherstellungspunkte löschen

Als Nächstes können Sie die Sicherungs-Wiederherstellungspunkte löschen, die sich in Ihrem Sicherungstresor befinden.

So löschen Sie Wiederherstellungspunkte

1. Wählen Sie auf der AWS Backup Konsole im Navigationsbereich Backup-Tresore aus.
2. Wählen Sie auf der Seite Backup vaults (Sicherungstresore) den Sicherungstresor, in dem Sie die Sicherungen gespeichert haben.
3. Überprüfen Sie den Wiederherstellungspunkt und wählen Sie Löschen aus.
4. Gehen Sie wie folgt vor, wenn Sie mehrere Wiederherstellungspunkte löschen:

    a. Wenn Ihre Liste ein kontinuierliches Backup enthält, wählen Sie aus, ob Sie Ihre kontinuierlichen Backup-Daten behalten oder löschen möchten.

    b. Um alle aufgelisteten Wiederherstellungspunkte zu löschen**`delete`**, geben Sie Folgendes ein und wählen Sie dann Wiederherstellungspunkte löschen aus.

Lassen Sie Ihre Browser-Registerkarte geöffnet, bis oben auf der Seite ein grünes Erfolgsbanner angezeigt wird. Wenn Sie diese Registerkarte vorzeitig schließen, wird der Löschvorgang beendet und es können einige der Wiederherstellungspunkte zurückbleiben, die Sie eigentlich löschen wollten. Weitere Informationen finden Sie unter Löschen von Backups.

Schritt 4: Backup-Tresor löschen

Der Standard-Backup-Tresor kann normalerweise nicht gelöscht werden. Wenn jedoch ein oder mehrere andere Tresore in einer Region vorhanden sind, kann der Standard-Backup-Tresor in dieser Region mit der AWS CLI gelöscht werden.

Sie können andere Tresore löschen, die nicht dem Standard entsprechen, sobald alle darin enthaltenen Backups (Wiederherstellungspunkte) gelöscht wurden. Wählen Sie dazu im leeren Tresor die Option Löschen aus.

Schritt 5: Berichtsplan löschen

Ihr Berichtsplan sendet täglich automatisch einen neuen Bericht. Löschen Sie den Berichtsplan, um dies zu verhindern.

Gehen Sie wie folgt vor, um den Berichtsplan zu löschen:

1. Wählen Sie auf der AWS Backup Konsole im Navigationsbereich Berichte aus.
2. Wählen Sie unter Name des Berichtsplans den Namen Ihres Berichtsplans aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen Ihres Berichtsplans ein und wählen Sie Berichtsplan löschen aus.

Schritt 6: Berichte löschen

Sie können Ihre Berichte löschen, indem Sie den Anweisungen zum Löschen eines einzelnen Objekts für jeden Ihrer Berichte folgen. Wenn Sie Ihren Ziel-S3-Bucket nicht mehr benötigen, können Sie nach dem Löschen aller Objekte aus dem Bucket den Bucket löschen, indem Sie den Anweisungen zum Löschen eines Buckets folgen.

Verwalten von Backups mithilfe von Backup-Plänen

In AWS Backup ist ein Sicherungsplan ein Richtlinienausdruck, der definiert, wann und wie Sie Ihre AWS Ressourcen sichern möchten, z. B. Amazon DynamoDB-Tabellen oder Amazon Elastic File System (Amazon EFS) -Dateisysteme. Sie können Ressourcen Backup-Plänen zuweisen und Backups für diese Ressourcen AWS Backup automatisch entsprechend dem Backup-Plan sichern und aufbewahren. Sie können mehrere Sicherungspläne erstellen, wenn Sie Workloads mit unterschiedlichen Sicherungsanforderungen haben. Backup-Fenster werden standardmäßig AWS Backup von optimiert. Sie können das Backup-Fenster in der Konsole oder programmgesteuert anpassen.

AWS Backup speichert Ihre regelmäßigen Backups effizient inkrementell. Beim ersten Backup einer AWS -Ressource wird eine vollständige Kopie Ihrer Daten gesichert. Bei jedem aufeinanderfolgenden inkrementellen Backup werden nur die Änderungen an Ihren AWS Ressourcen gesichert. Durch inkrementelle Backups können Sie vom Datenschutz häufiger Backups profitieren und gleichzeitig die Speicherkosten minimieren.

AWS Backup verwaltet außerdem den Lebenszyklus Ihres Backup-Plans auf der Grundlage Ihrer Aufbewahrungseinstellungen nahtlos, sodass Sie bei Bedarf Daten wiederherstellen können.

In den folgenden Abschnitten finden Sie die Grundlagen der Verwaltung Ihrer Backup-Strategie in AWS Backup.

Themen

Erstellen eines Backup-Plans

Sie können einen Backup-Plan mithilfe der AWS Backup Konsole, der API, der CLI, des SDK oder einer AWS CloudFormation Vorlage erstellen.

Themen

- Erstellen von Backup-Plänen mit dem AWS CLI
- Optionen und Konfiguration eines Backup-Plans
- AWS CloudFormation Vorlagen für Backup-Pläne

Erstellen von Backup-Plänen mithilfe der AWS Backup -Konsole

Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup. Wählen Sie im Dashboard Manage Backup plans (Sicherungspläne verwalten) aus. Sie können auch im Navigationsbereich Backup-Pläne und Backup-Plan erstellen auswählen.

Startoptionen

Sie haben drei Möglichkeiten für Ihren neuen Backup-Plan:

- Schritt 1: Einen Backup-Plan basierend auf einem bestehenden erstellen
- Erstellen eines neuen Plans
- Erstellen von Backup-Plänen mit dem AWS CLI

In diesem Tutorial wählen wir Erstellen eines neuen Plans. Jeder Teil der Konfiguration enthält einen Link zu einem erweiterten Abschnitt später auf der Seite, in dem Sie nach weiteren Informationen suchen können.

1. Geben Sie einen Plannamen in ein Name des Backup-Plans. Sie können den Namen eines Plans nicht mehr ändern, nachdem er erstellt wurde.

   Wenn Sie versuchen, einen Backup-Plan zu erstellen, der mit einem vorhandenen Plan identisch ist, erhalten Sie eine `AlreadyExistsException` Fehlermeldung.
2. Optional können Sie Ihrem Backup-Plan Tags hinzufügen.
3. Konfiguration der Backup-Regeln: Im Abschnitt zur Konfiguration der Backup-Regeln legen Sie den Backup-Zeitplan, das Backup-Zeitfenster und den Lebenszyklus fest.
4. Zeitplan:

   a. Geben Sie einen Namen für die Backup-Regel in das Textfeld ein.

   b. Wählen Sie im Backup-Tresor-Dropdown-Menü Standard aus oder wählen Sie Neuen Backup-Tresor erstellen aus, um einen neuen Tresor zu erstellen.

c. Wählen Sie im Dropdown-Menü für die Backup-Häufigkeit aus, wie oft dieser Plan ein Backup erstellen soll.

5. Backup-Zeitfenster:

   a. Die Startzeit ist standardmäßig 12:30 Uhr (00:30 Uhr in 24 Stunden) in der lokalen Zeitzone Ihres Systems.

   b. Die Standardeinstellung für Start innerhalb von ist 8 Stunden. Sie können dies ändern, um ein Zeitfenster anzugeben, in dem das Backup gestartet werden soll.

   c. Abschluss innerhalb von ist standardmäßig 7 Tage.

6. Kontinuierliche Backups und point-in-time Wiederherstellung (PITR): Sie können „Kontinuierliche Backups zur Wiederherstellung aktivieren“ (PITR) auswählen. point-in-time Informationen dazu, welche Ressourcen für diese Art von Backup unterstützt werden, finden Sie in der Verfügbarkeit von Features nach Ressource-Matrix.

7. Lebenszyklus

   a. Cold Storage: Wählen Sie dieses Feld aus, damit berechtigte Ressourcentypen gemäß dem Zeitplan, den Sie für den gesamten Aufbewahrungszeitraum angegeben haben, auf Cold Storage umgestellt werden können. Um Cold Storage verwenden zu können, müssen Sie über eine Aufbewahrungsdauer von insgesamt 90 Tagen oder mehr verfügen.

   b. Cold Storage für Amazon EBS ist Amazon EBS Snapshots Archive. Snapshots, die auf die Archiv-Speicherebene umgestellt wurden, werden in der Konsole als „Cold Tier“ angezeigt. Wenn Cold Storage aktiviert ist und Ihre Backup-Frequenz monatlich oder seltener ist, können Sie Ihren Backup-Plan auf EBS-Snapshots umstellen lassen.

   c. Die gesamte Aufbewahrungsdauer ist die Anzahl der Tage, für die Sie Ihre Ressource in AWS Backup speichern. Dies ist die Gesamtzahl der Warm-Storage-Tage plus Cold Storage.

8. (Optional) Verwenden Sie Zum Ziel kopieren, um eine regionsübergreifende Kopie der berechtigten Ressourcen zu erstellen, wenn Sie eine Kopie eines Backups in einer anderen AWS-Region speichern möchten.

9. (Optional) Zu Wiederherstellungspunkten hinzugefügte Tags.

10. Wenn alle Abschnitte Ihren Spezifikationen entsprechen, wählen Sie Backup-Regel speichern.

Erstellen von Backup-Plänen mit dem AWS CLI

Sie können Ihren Backup-Plan auch in einem JSON-Dokument definieren und ihn mithilfe der AWS Backup -Konsole oder der AWS CLI bereitstellen. Das folgende JSON-Dokument enthält ein Beispiel für einen Sicherungsplan, mit dem ein tägliches Backup um 1:00 Uhr MEZ erstellt wird (die Ortszeit wird gegebenenfalls an Tageslicht, Standard- oder Sommerzeit angepasst). Es löscht ein Backup automatisch nach einem Jahr.

```
{
  "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
        }
      }
    ]
  }
}
```

Sie können Ihr JSON-Dokument unter einem von Ihnen gewählten Namen speichern. Der folgende CLI-Befehl zeigt `create-backup-plan` mit einer JSON-Datei mit dem Namen `test-backup-plan.json`:

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

Beachten Sie, dass einige Systeme die Wochentage zwar von 0 bis 6 nummerieren, wir sie jedoch von 1 bis 7. Weitere Informationen finden Sie unter Cron-Ausdrücke. Weitere Informationen zu Zeitzonen finden Sie TimeZonein der Amazon Location Service API-Referenz.

Optionen und Konfiguration eines Backup-Plans

Wenn Sie in der AWS Backup Konsole einen Backup-Plan definieren, konfigurieren Sie die folgenden Optionen:

Name des Backup-Plans

Sie müssen einen eindeutigen Namen für den Sicherungsplan angeben.

Wenn Sie einen Namen wählen, der mit dem Namen eines vorhandenen Plans identisch ist, wird eine Fehlermeldung angezeigt.

Sicherungsregeln

Sicherungspläne bestehen aus einer oder mehreren Sicherungsregeln. So fügen Sie einem Backup-Plan Backup-Regeln hinzu oder bearbeiten bestehende Regeln in einem Backup-Plan

1. Wählen Sie in der AWS Backup Konsole im linken Navigationsbereich Backup-Pläne aus.
2. Wählen Sie unter Name des Backup-Plans einen Backup-Plan aus.
3. Gehen Sie im Abschnitt Backup-Regeln wie folgt vor:

   - Um eine Backup-Regel hinzuzufügen, wählen Sie Backup-Regel hinzufügen aus.
   - Wählen Sie zum Bearbeiten einer vorhandenen Backup-Regel eine Regel und dann Bearbeiten aus.

> **Note**
>
> Wenn Sie einen Backup-Plan mit mehreren Regeln haben und sich die Zeitrahmen der beiden Regeln überschneiden, AWS Backup optimiert das Backup und erstellt ein Backup für die Regel mit der längeren Aufbewahrungszeit. Bei der Optimierung wird das gesamte Startfenster berücksichtigt, nicht nur der Zeitpunkt, an dem das tägliche Backup erstellt wird.

Jede Sicherungsregel umfasst die folgenden Elemente.

Name der Backup-Regel

Bei den Namen von Sicherungsregeln muss die Groß- und Kleinschreibung beachtet werden. Sie müssen zwischen 1 und 50 alphanumerischen Zeichen oder Bindestriche enthalten.

Backup frequency (Sicherungshäufigkeit)

Die Backup-Frequenz bestimmt, wie oft ein Snapshot-Backup AWS Backup erstellt wird. Sie können in der Konsole auswählen, ob alle 12 Stunden, täglich, wöchentlich und monatlich ein Backup erstellt wird. Sie können auch einen Cron-Ausdruck erstellen, der sogar stündlich Snapshot-Backups erstellt. Mithilfe der AWS Backup CLI können Sie Snapshot-Backups bis zu stündlich planen.

Wenn Sie eine wöchentliche Frequenz wählen, können Sie festlegen, an welchem Wochentag die Backups erstellt werden sollen. Wenn Sie eine monatliche Frequenz wählen, können Sie einen bestimmten Tag im Monat auswählen.

Sie können auch das Kontrollkästchen Kontinuierliche Backups für unterstützte Ressourcen aktivieren aktivieren aktivieren, um eine Regel für kontinuierliche Backups zu erstellen, die für die point-in-time Wiederherstellung (PITR) aktiviert ist. Im Gegensatz zu Snapshot-Backups können Sie mit kontinuierlichen Backups eine Wiederherstellung durchführen point-in-time . Weitere Informationen zu fortlaufenden Backups finden Sie unter Kontinuierliche Backups und zeitpunktbezogene Wiederherstellung (PITR).

Backup-Fenster

Sicherungsfenster bestehen aus der Zeit, zu der das Sicherungsfenster beginnt, und der Dauer des Fensters in Stunden. Sicherungsaufträge werden in diesem Fenster gestartet. Die Standardeinstellungen in der Konsole sind:

- 12:30 Uhr lokal in der Zeitzone Ihres Systems (0:30 Uhr bei 24-Stunden-Systemen)
- Start innerhalb von 8 Stunden
- Fertigstellung innerhalb von 7 Tagen

  (Der Parameter Abschluss innerhalb von gilt nicht für Amazon-FSx-Ressourcen)

Sie können die Sicherungshäufigkeit und die Anfangszeit des Sicherungsfensters mithilfe eines cron-Ausdrucks anpassen. Die sechs Felder mit AWS Cron-Ausdrücken finden Sie unter Cron-Ausdrücke im Amazon CloudWatch Events-Benutzerhandbuch. Zwei Beispiele für AWS Cron-Ausdrücke sind `15 * ? * * *` (jede Stunde 15 Minuten nach der Stunde ein Backup erstellen) und `0 12 * * ? *` (täglich um 12 Uhr UTC ein Backup erstellen). Eine Tabelle mit Beispielen finden Sie, wenn Sie auf den vorherigen Link klicken und auf der Seite nach unten scrollen.

AWS Backup wertet Cron-Ausdrücke zwischen 00:00 und 23:59 aus. Wenn Sie eine Backup-Regel für „alle 12 Stunden“ erstellen, aber als Startzeit später als 11:59 Uhr angeben, wird sie nur einmal pro Tag ausgeführt.

Kontinuierliche Sicherungen point-in-time und Wiederherstellungen (PITR) verweisen auf die Änderungen, die über einen bestimmten Zeitraum aufgezeichnet wurden. Daher können sie nicht mit einer Uhrzeit oder einem Cron-Ausdruck geplant werden.

> **Note**
>
> Im Allgemeinen können AWS Datenbankdienste keine Backups 1 Stunde vor oder während ihres Wartungsfensters starten und Amazon FSx kann Backups nicht 4 Stunden vor oder während ihres Wartungsfensters oder automatischen Backupfensters starten (Amazon Aurora ist von dieser Einschränkung des Wartungsfensters ausgenommen). Zu diesen Zeiten geplante Snapshot-Backups schlagen fehl.
> Eine Ausnahme tritt auf, wenn Sie sich dafür entscheiden, AWS Backup sowohl für Snapshot-Backups als auch für fortlaufende Backups für einen unterstützten Service zu nutzen. AWS Backup plant Backup-Fenster automatisch, um Konflikte zu vermeiden. Unter Point-in-Time Recovery finden Sie eine Liste der unterstützten Dienste und Anweisungen AWS Backup zur Erstellung kontinuierlicher Backups.

Überschneidende Backup-Regeln

Gelegentlich kann ein Backup-Plan mehrere, überlappende Regeln enthalten. Wenn sich die Startfenster verschiedener Regeln überschneiden, wird das Backup gemäß der Regel mit dem längeren Aufbewahrungszeitraum AWS Backup beibehalten. Nehmen wir beispielsweise einen Backup-Plan mit zwei Regeln:

1. Stündliches Backup mit einem Startfenster von einer Stunde und Aufbewahrung für 1 Tag.
2. Backup alle 12 Stunden mit einem Startfenster von 8 Stunden und Aufbewahrung für 1 Woche.

Nach 24 Stunden erstellt die zweite Regel zwei Backups (weil sie die längere Aufbewahrungsfrist hat). Die erste Regel erstellt acht Backups (weil das 8-stündige Startfenster der zweiten Regel die Ausführung weiterer stündlicher Backups verhinderte). Das heißt:

Während dieses Startfensters	erstellt diese Regel 1 Backup
Mitternacht bis 8 Uhr	12 Stunden
8:00 Uhr bis 9:00 Uhr	Stündlich
9:00 Uhr bis 10:00 Uhr	Stündlich
10:00 Uhr bis 11:00 Uhr	Stündlich
11:00 Uhr bis 12:00 Uhr	Stündlich
12:00 Uhr bis 20:00 Uhr	12 Stunden
8:00 Uhr bis 9:00 Uhr	Stündlich
9:00 Uhr bis 10:00 Uhr	Stündlich
10:00 Uhr bis 11:00 Uhr	Stündlich
23:00 Uhr bis Mitternacht	Stündlich

Während des Startfensters bleibt der Status des Backup-Auftrags so lange im `CREATED`-Status, bis er erfolgreich gestartet wurde oder bis die Startfensterzeit abgelaufen ist. AWS Backup Erhält Time innerhalb des Startfensters einen Fehler, sodass der Job erneut versucht werden kann, AWS Backup wird automatisch mindestens alle 10 Minuten erneut versucht, den Job zu starten, bis die Sicherung erfolgreich gestartet wurde (der Jobstatus ändert sich auf`RUNNING`) oder bis sich der Jobstatus auf ändert `EXPIRED` (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Lebenszyklus und Speicherstufen

Backups werden für die von Ihnen angegebene Anzahl von Tagen gespeichert, was als Backup-Lebenszyklus bezeichnet wird. Backups können bis zum Ende ihres Lebenszyklus wiederhergestellt werden.

Dieser Wert wird im Abschnitt „Lebenszyklus“ der Konfiguration der Backup-Regeln in der Konsole als gesamte Aufbewahrungsdauer festgelegt. AWS Backup

Wenn Sie verwenden AWS CLI, wird dies mithilfe des Parameters festgelegt `DeleteAfterDays`. Die Aufbewahrungsdauer für Snapshots kann zwischen 1 Tag und 100 Jahren liegen (oder für

unbestimmte Zeit gelten, wenn Sie keine Dauer angeben). Die Aufbewahrungsfrist für fortlaufende Backups dagegen kann zwischen 1 Tag und 35 Tagen liegen. Das Erstellungsdatum einer Sicherung ist das Datum, an dem die Sicherungsaufgabe gestartet wurde, nicht das Datum, an dem sie abgeschlossen wurde. Wenn Ihr Backup-Job nicht am selben Tag abgeschlossen wird, an dem er gestartet wurde, verwenden Sie das Datum, an dem er begonnen hat, um die Aufbewahrungsfristen zu berechnen.

Backups werden auf einer Speicherebene verwaltet. Für jede Stufe fallen unterschiedliche Kosten für Speicher und Wiederherstellung an, wie unter AWS Backup -Preise beschrieben. Jedes Backup wird erstellt und in Warm Storage gespeichert. Je nachdem, wie lange Sie Ihr Backup speichern möchten, können Sie Ihr Backup möglicherweise auf eine kostengünstigere Stufe, den sogenannten Cold Storage, umstellen. Verfügbarkeit von Features nach Ressource zeigt an, welche Ressourcen über dieses optionale Feature verfügen.

Console

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Erstellen oder bearbeiten eines Backup-Plans.
3. Markieren Sie im Abschnitt „Lebenszyklus“ der Konfiguration der Backup-Regeln das Kontrollkästchen Backups von Warm zu Cold Storage verschieben.
4. (optional) Wenn Amazon EBS zu den Ressourcen gehört, die Sie sichern, und Ihre Backup-Frequenz monatlich oder weniger häufig ist, können Sie sie mithilfe der EBS-Snapshot-Archivierung auf die „Cold“-Stufe umstellen.
5. Geben Sie einen Wert (in Tagen) ein, mit dem Ihre Backups im Warmspeicher verbleiben sollen. AWS Backup empfiehlt mindestens 8 Tage.
6. Geben Sie einen Wert (in Tagen) für die gesamte Aufbewahrungsdauer ein. Die Differenz zwischen der gesamten Aufbewahrungsdauer und der Warm-Storage-Zeit ergibt sich aus der Anzahl der Tage, die die Backups im Cold Storage verbleiben.

AWS CLI

1. Verwenden Sie `create-backup-plan` oder `update-backup-plan`.
2.
3. Schließen Sie den booleschen Parameter `OptInToArchiveForSupportedResources` für EBS-Ressourcen ein.

4. Schließen Sie den Parameter `MoveToColdStorageAfterdays` ein.
5. Verwenden Sie den Parameter `DeleteAfterDays`. Dieser Wert muss 90 (Tage) plus dem Wert sein, den Sie für `MoveToColdStorageAfterDays` eingegeben haben.

Cold Storage ist derzeit für die folgenden Ressourcentypen verfügbar:

Ressourcentyp	Inkrementelles oder vollständiges Backup im Cold Storage
AWS CloudFormation	Inkrementell
DynamoDB mit erweiterten Features	Vollständig; keine inkrementellen Backups auf keiner Stufe
Amazon EBS (mit EBS Snapshot Archive)	Vollständig; inkrementelle Backups werden nach der Umstellung vollständig.
Amazon EFS	Inkrementell
SAP-HANA-Datenbanken auf Amazon-EC2-Instances	Inkrementell
Amazon Timestream	Inkrementell
Virtuelle VMware-Maschinen	Inkrementell

Sobald Sie die Übertragung zu Cold Storage über die Konsole oder die Befehlszeile aktiviert haben, gelten die folgenden Bedingungen für Backups in Cold Storage (oder Archiv):

- Übertragene Backups müssen zusätzlich zu der Zeit im Warmspeicher für mindestens 90 Tage im kalten Speicher aufbewahrt werden. AWS Backup erfordert, dass die Aufbewahrung 90 Tage länger dauert als bei der Einstellung „Umstellung auf kalt nach Tagen“. Sie können die Einstellung „Übertragung in Archivspeicher nach Tagen“ nicht ändern, sobald eine Sicherung in den Archivspeicher übertragen wurde.
- Manche Services unterstützen inkrementelle Backups. Für inkrementelle Backups benötigen Sie mindestens ein warmes, vollständiges Backup. AWS Backup empfiehlt, dass Sie Ihre Lebenszykluseinstellungen so einrichten, dass Ihr Backup erst nach mindestens 8 Tagen in den

Cold Storage verschoben wird. Wenn das vollständige Backup zu früh auf einen kalten Speicher umgestellt wird (z. B. ein Wechsel zu einem kalten Speicher nach einem Tag), AWS Backup wird ein weiteres warmes, vollständiges Backup erstellt.

- Bei Ressourcentypen, die inkrementelle Backups unterstützen AWS Backup , werden Daten vom warmen in den kalten Speicher übertragen, wenn die übertragenen Daten nicht mehr von warmen Backups referenziert werden. Daten in Cold Storage, auf die nur in anderen Cold Backups verwiesen wird, werden zu den Preisen für die Cold-Storage-Stufe abgerechnet. Für andere Backups gelten weiterhin die Preise für die Warm-Speicherstufe.

Sicherungstresor

Ein Sicherungstresor ist ein Container zum Organisieren Ihrer Sicherungen. Von einer Sicherungsregel erstellte Sicherungen werden im Sicherungstresor organisiert, den Sie in der Sicherungsregel angeben. Sie können Backup-Tresore verwenden, um den Verschlüsselungsschlüssel AWS Key Management Service (AWS KMS) festzulegen, der zur Verschlüsselung von Backups im Backup-Tresor und zur Steuerung des Zugriffs auf die Backups im Backup-Tresor verwendet wird. Sie können auch Tags zu den Sicherungstresoren hinzufügen, um sie leichter zu organisieren. Wenn Sie den standardmäßigen Tresor nicht verwenden wollen, können Sie Ihren eigenen erstellen. step-by-step Anweisungen zum Erstellen eines Backup-Tresors finden Sie unter. Schritt 3: Einen Backup-Tresor erstellen

In Regionen kopieren

Als Teil Ihres Backup-Plans können Sie optional eine Backup-Kopie in einer anderen AWS-Region erstellen. Weitere Informationen zu Backup-Kopien finden Sie unter Erstellen von Backup-Kopien über AWS-Regionen hinweg.

Wenn Sie eine Sicherungskopie definieren, konfigurieren Sie die folgenden Optionen:

Zielregion

Die Zielregion für die Sicherungskopie.

(Erweiterte Einstellungen) Backup-Tresor

Der Zielsicherungstresor für die Kopie.

(Erweiterte Einstellungen) IAM-Rolle

Die IAM-Rolle, die beim Erstellen der Kopie AWS Backup verwendet wird. Die Rolle muss außerdem als vertrauenswürdige Entität AWS Backup aufgeführt sein, sodass AWS Backup sie übernommen

werden kann. Wenn Sie Standard wählen und die AWS Backup Standardrolle nicht in Ihrem Konto vorhanden ist, wird eine Rolle mit den richtigen Berechtigungen für Sie erstellt.

(Erweiterte Einstellungen) Lebenszyklus

Gibt an, wann die Sicherungskopie in den Cold Storage übergestellt werden soll und wann die Kopie abläuft (gelöscht werden soll). In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Sie können diesen Wert nicht ändern, nachdem eine Kopie in den Cold Storage übergegangen ist.

Expire (Ablaufdatum) gibt die Anzahl der Tage nach der Erstellung an, nach denen die Kopie gelöscht wird. Dieser Wert muss mehr als 90 Tage über den Wert für den Transition to cold storage (Übergang zu Cold Storage) hinausgehen.

Zu Wiederherstellungspunkten hinzugefügte Tags

Die Tags, die Sie hier auflisten, werden automatisch zu Sicherungen hinzugefügt, wenn diese erstellt werden.

Zu Backup-Plänen hinzugefügte Tags

Diese Tags sind dem Sicherungsplan selbst zugeordnet, um Sie beim Organisieren und Nachverfolgen Ihres Sicherungsplans zu unterstützen.

Erweiterte Backup-Einstellungen

Ermöglicht anwendungskonsistente Backups für Drittanbieteranwendungen, die auf Amazon-EC2-Instances ausgeführt werden. AWS Backup Unterstützt derzeit Windows VSS-Backups. AWS Backup schließt bestimmte Amazon EC2 EC2-Instance-Typen von Windows VSS-Backups aus. Weitere Informationen finden Sie unter Erstellen von Windows-VSS-Backups.

AWS CloudFormation Vorlagen für Backup-Pläne

Wir stellen Ihnen zwei AWS CloudFormation Beispielvorlagen als Referenz zur Verfügung. Die erste Vorlage erstellt einen einfachen Backup-Plan. Die zweite Vorlage ermöglicht VSS-Backups in einem Backup-Plan.

> **Note**
>
> Wenn Sie die Standard-Servicerolle verwenden, ersetzen Sie *service-role* durch `AWSBackupServiceRolePolicyForBackup`.

```
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
```

Zuweisen von Ressourcen zu einem Backup-Plan

Die Ressourcenzuweisung gibt an, AWS Backup welche Ressourcen mithilfe Ihres Backup-Plans geschützt werden. AWS Backup bietet Ihnen sowohl einfache Standardeinstellungen als auch

detaillierte Steuerelemente, mit denen Sie Ihrem Backup-Plan Ressourcen zuweisen können. Jedes Mal, wenn Ihr Backup-Plan ausgeführt wird, werden Sie AWS-Konto nach allen Ressourcen durchsucht, die Ihren Ressourcenzuweisungskriterien entsprechen. Dieser Automatisierungsgrad ermöglicht es Ihnen, Ihren Backup-Plan und Ihre Ressourcenzuweisung genau einmal zu definieren. AWS Backup nimmt Ihnen die Arbeit ab, neue Ressourcen zu finden und zu sichern, die zu Ihrer zuvor definierten Ressourcenzuweisung passen.

Sie können alle AWS Backup unterstützten Ressourcentypen, für die Sie sich entschieden haben, zur Verwaltung zuweisen. AWS Backup Anweisungen dazu, wie Sie sich für mehr AWS Backup unterstützte Ressourcentypen anmelden können, finden Sie unter Erste Schritte 1: Service-Opt-In.

Die AWS Backup Konsole bietet zwei Möglichkeiten, Ressourcentypen in einen Backup-Plan aufzunehmen: Sie können den Ressourcentyp explizit in einem Backup-Plan zuweisen oder alle Ressourcen einbeziehen. Nachfolgend erfahren Sie, wie diese Auswahlmöglichkeiten mit Serviceanmeldungen funktionieren.

- Wenn Ressourcenzuweisungen nur auf Tags basieren, werden die Service-Opt-In-Einstellungen angewendet.
- Wenn ein Ressourcentyp explizit einem Backup-Plan zugewiesen wird, wird er in das Backup aufgenommen, auch wenn das Opt-In für diesen bestimmten Dienst nicht aktiviert ist. Dies gilt nicht für Aurora, Neptune und Amazon DocumentDB. Damit diese Dienste enthalten sind, muss das Opt-In aktiviert sein.
- Wenn in einer Ressourcenzuweisung sowohl der Ressourcentyp als auch die Tags angegeben sind, werden die angegebenen Ressourcentypen zuerst gefiltert, und dann werden diese Ressourcen durch Tags weiter gefiltert.

  Die Opt-In-Einstellungen für Dienste werden für die meisten Ressourcentypen ignoriert. Aurora, Neptune und Amazon DocumentDB erfordern jedoch eine Service-Anmeldung.
- Wenn ein Konto in einer Region verwendet AWS Backup (erstellt einen Backup-Tresor oder einen Backup-Plan), wird das Konto automatisch für alle Ressourcentypen aktiviert, die zu diesem Zeitpunkt AWS Backup in der Region unterstützt werden. Unterstützte Dienste, die zu einem späteren Zeitpunkt zu dieser Region hinzugefügt werden, werden nicht automatisch in einen Backup-Plan aufgenommen. Sie können sich für diese Ressourcentypen entscheiden, sobald sie unterstützt werden.
- Wenden Sie bei Amazon FSx for NetApp ONTAP bei Verwendung der tagbasierten Ressourcenauswahl Tags auf einzelne Volumes statt auf das gesamte Dateisystem an.

Ihre Ressourcenzuweisung kann Ressourcentypen und Ressourcen einschließen (oder ausschließen).

- Ein Ressourcentyp umfasst jede Instanz oder Ressource eines AWS Backup unterstützten AWS Dienstes oder einer Drittanbieteranwendung. Der DynamoDB-Ressourcentyp beispielsweise bezieht sich auf all Ihre DynamoDB-Tabellen.
- Eine Ressource ist eine einzelne Instance eines Ressourcentyps, z. B. eine Ihrer DynamoDB-Tabellen. Sie können eine Ressource anhand ihrer eindeutigen Ressourcen-ID angeben.

Sie können eine Ressourcenzuweisung mithilfe von Tags und Bedingungsoperatoren weiter verfeinern.

Themen

Zuweisen von Ressourcen über die Konsole

So navigieren Sie zur Seite Ressourcen zuweisen

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie Backup-Pläne aus.
3. Wählen Sie Backup-Plan erstellen aus.
4. Wählen Sie in der Dropdown-Liste Vorlage auswählen eine beliebige Vorlage und dann Plan erstellen aus.
5. Geben Sie unter Name des Backup-Plans einen Namen ein.
6. Wählen Sie Plan erstellen aus.
7. Wählen Sie Ressourcen zuweisen aus.

Gehen Sie im Abschnitt Allgemein folgendermaßen vor, um mit der Ressourcenzuweisung zu beginnen:

1. Geben Sie unter Name der Ressourcenzuweisung einen Namen ein.

2. Wählen Sie die Standardrolle oder die Option Eine IAM-Rolle wählen aus.

> **Note**
>
> Wenn Sie eine IAM-Rolle auswählen, stellen Sie sicher, dass sie über die Berechtigung verfügt, alle Ressourcen zu sichern, die Sie zuweisen möchten. Wenn Ihre Rolle eine Ressource findet, auf die sie keine Zugriffsberechtigung hat, schlägt der Backup-Plan fehl.

Um Ihre Ressourcen zuzuweisen, wählen Sie im Abschnitt Ressourcen zuweisen eine der beiden Optionen unter Ressourcenauswahl definieren aus:

- Alle Ressourcentypen einschließen. Diese Option konfiguriert Ihren Backup-Plan so, dass er alle aktuellen und future AWS Backup unterstützten Ressourcen schützt, die Ihrem Backup-Plan zugewiesen sind. Verwenden Sie diese Option, um Ihren Datenbestand schnell und einfach zu schützen.

  Wenn Sie diese Option auswählen, können Sie im nächsten Schritt optional die Option Auswahl mithilfe von Tags verfeinern anwenden.
- Spezifische Ressourcentypen einschließen. Wenn Sie diese Option auswählen, müssen Sie mit den folgenden Schritten die Option Bestimmte Ressourcentypen auswählen ausführen:

  1. Weisen Sie mithilfe des Dropdown-Menüs Ressourcentypen auswählen einen oder mehrere Ressourcentypen zu.

  > **Important**
  >
  > RDS, Aurora, Neptune und DocumentDB haben denselben Amazon-Ressourcennamen (ARN). Durch das Anmelden für die Verwaltung eines dieser Ressourcentypen mit AWS Backup werden bei der Zuweisung zu einem Backup-Plan alle dieser Typen angemeldet. Verwenden Sie Tags und Bedingungsoperatoren, um Ihre Auswahl zu verfeinern.

  Wenn Sie fertig sind, wird AWS Backup Ihnen die Liste der ausgewählten Ressourcentypen und deren Standardeinstellung angezeigt, die darin besteht, alle Ressourcen für jeden ausgewählten Ressourcentyp zu schützen.

2. Wenn Sie bestimmte Ressourcen von einem ausgewählten Ressourcentyp ausschließen möchten, können Sie optional folgendermaßen vorgehen:

    1. Verwenden Sie das Dropdown-Menü Ressourcen auswählen und deaktivieren Sie die Standardauswahl.
    2. Wählen Sie die spezifischen Ressourcen aus, die Sie Ihrem Backup-Plan zuweisen möchten.
3. Optional können Sie die Option Bestimmte Ressourcen-IDs aus den ausgewählten Ressourcentypen ausschließen anwenden. Verwenden Sie diese Option, wenn Sie eine oder mehrere Ressourcen von vielen ausschließen möchten, da dies möglicherweise schneller ist, als im vorherigen Schritt viele Ressourcen auszuwählen. Sie müssen einen Ressourcentyp angeben, bevor Sie Ressourcen von diesem Ressourcentyp ausschließen können. Schließen Sie eine Ressourcen-ID aus, indem Sie die folgenden Schritte ausführen:

    1. Wählen Sie unter Bestimmte Ressourcen-IDs aus den ausgewählten Ressourcentypen ausschließen einen oder mehrere der Ressourcentypen aus, die Sie mithilfe der Option Ressourcentypen auswählen eingeschlossen haben.
    2. Verwenden Sie für jeden Ressourcentyp das Menü Ressourcen auswählen, um eine oder mehrere Ressourcen auszuwählen, die ausgeschlossen werden sollen.

Zusätzlich zu den vorher ausgewählten Optionen können Sie mit der optionalen Funktion Auswahl mithilfe von Tags verfeinern eine noch detailliertere Auswahl treffen. Mit dieser Funktion können Sie mithilfe von Tags Ihre aktuelle Auswahl so präzisieren, dass eine Teilmenge Ihrer Ressourcen einbezogen wird.

Tags sind Schlüssel-Wert-Paare, die Sie bestimmten Ressourcen zuweisen können, um Ihre Ressourcen zu identifizieren, zu organisieren und zu filtern. Bei Tags muss die Groß- und Kleinschreibung beachtet werden. Weitere Informationen finden Sie unter Markieren von AWS -Ressourcen in der Allgemeinen AWS -Referenz.

Wenn Sie die Auswahl mithilfe von zwei oder mehr Tags verfeinern, ist die Auswirkung eine UND-Bedingung. Wenn Sie beispielsweise Ihre Auswahl mithilfe von zwei Tags verfeinern, `env: prod` und `role: application`, weisen Sie nur Ressourcen mit BEIDEN Tags Ihrem Backup-Plan zu.

So verfeinern Sie die Auswahl mithilfe von Tags

1. Wählen Sie unter Auswahl mithilfe von Tags verfeinern in der Dropdown-Liste einen Schlüssel aus.

2. Wählen Sie in der Dropdown-Liste eine Bedingung für den Wert aus.

   - Wert bezieht sich auf die nächste Eingabe, den Wert Ihres Schlüssel-Wert-Paares.
   - Bedingung kann `Equals`, `Contains`, `Begins with` oder `Ends with` oder ihre Umkehrung sein: `Does not equal`, `Does not contain`, `Does not begin with` oder `Does not end with`.

3. Wählen Sie Wert in der Dropdown-Liste aus.
4. Wählen Sie Tag hinzufügen aus, um mithilfe eines anderen Tags die Auswahl weiter zu verfeinern.

Programmgesteuertes Zuweisen von Ressourcen

Sie können eine Ressourcenzuweisung in einem JSON-Dokument definieren. Diese Beispielressourcenzuweisung weist alle Amazon-EC2-Instances dem Backup-Plan *BACKUP-PLAN-ID* zu:

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

Davon ausgehend, dass diese JSON-Datei unter dem Namen `backup-selection.json` gespeichert ist, können Sie diese Ressourcen mit dem folgenden CLI-Befehl Ihrem Backup-Plan zuweisen:

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

Im Folgenden finden Sie Beispiele für Ressourcenzuweisungen sowie das entsprechende JSON-Dokument. Damit diese Tabelle leichter lesbar ist, wurden in den Beispielen die Felder `"BackupPlanId"`, `"SelectionName"` und `"IamRoleArn"` weggelassen. Der Platzhalter `*` steht für null oder mehr Zeichen, die keine Leerzeichen sind.

Example Beispiel: Wählen Sie alle Ressourcen in meinem Konto aus

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

Example Beispiel: Wählen Sie alle Ressourcen in meinem Konto aus, schließen Sie jedoch EBS-Volumes aus

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

Example Beispiel: Wählen Sie alle Ressourcen aus, die mit markiert sind"backup":"true", aber schließen Sie EBS-Volumes aus

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

```
    }
  }
}
```

Example Beispiel: Wählen Sie alle EBS-Volumes und RDS-DB-Instances aus, die sowohl mit als auch gekennzeichnet sind "backup":"true""stage":"prod"

Die boolesche Arithmetik ähnelt der in IAM-Richtlinien: Die in "Resources" sind mithilfe eines booleschen Wertes OR kombiniert und die in `"Conditions"` sind mit einem booleschen Wert AND kombiniert.

Der `"Resources"`-Ausdruck `"arn:aws:rds:*:*:db:*"` wählt nur RDS-DB-Instances aus, da es keine entsprechenden Aurora-, Neptune- oder DocumentDB-Ressourcen gibt.

```
{
  "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 Beispiel: Wählen Sie alle EBS-Volumes und RDS-Instances aus, die mit"backup":"true", aber nicht markiert sind "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 Beispiel: Wählen Sie alle Ressourcen aus, die mit einem Tag versehen sind, "key1" und einen Wert, der mit dem "include" Wort beginnt, aber nicht mit einem "key2" Wert, der das Wort enthält "exclude"

Sie können das Platzhalterzeichen am Anfang, am Ende und in der Mitte einer Zeichenfolge verwenden. Beachten Sie die Verwendung des Platzhalterzeichens (*) in `include*` und `*exclude*` im obigen Beispiel. Sie können das Platzhalterzeichen auch in der Mitte einer Zeichenfolge verwenden, wie im vorherigen Beispiel `arn:aws:rds:*:*:db:*` gezeigt.

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

```
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
  }
}
```

Example Beispiel: Wählen Sie alle Ressourcen aus, die mit markiert sind, "backup":"true" außer FSx-Dateisystemen und RDS-, Aurora-, Neptune- und DocumentDB-Ressourcen

Elemente in `NotResources` werden mit dem booleschen Wert OR kombiniert.

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

Example Beispiel: Wählen Sie alle Ressourcen aus, die mit einem Tag und einem beliebigen Wert gekennzeichnet sind "backup"

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

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

Example Beispiel: Wählen Sie alle FSx-Dateisysteme, den Aurora-Cluster und alle Ressourcen aus"my-aurora-cluster", die mit markiert sind"backup":"true", mit Ausnahme der Ressourcen, die mit gekennzeichnet sind "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 Beispiel: Wählen Sie alle Ressourcen aus, die mit einem Tag gekennzeichnet sind, mit **`"backup":"true"`** Ausnahme der EBS-Volumes, die mit dem Tag gekennzeichnet sind **`"stage":"test"`**

Verwenden Sie zwei CLI-Befehle, um zwei Auswahlen zu erstellen, um diese Ressourcengruppe auszuwählen. Die erste Auswahl gilt für alle Ressourcen mit Ausnahme von EBS-Volumes. Die zweite Auswahl gilt für EBS-Volumes.

```
{
  "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"
        }
      ]
    }
  }
}
```

Zuweisen von Ressourcen mit AWS CloudFormation

Diese end-to-end AWS CloudFormation Vorlage erstellt eine Ressourcenzuweisung, einen Backup-Plan und einen Ziel-Backup-Tresor:

- Ein Backup-Tresor mit dem Namen *`CloudFormationTestBackupVault`*.
- Ein Backup-Plan mit dem Namen *`CloudFormationTestBackupPlan`*. Dieser Plan führt zwei Backup-Regeln aus, die beide täglich um 12 Uhr UTC Backups erstellen und sie 210 Tage lang aufbewahren.
- Eine Ressourcenauswahl mit dem Namen *`BackupSelectionName`*.
- • Die Ressourcenzuweisung sichert die folgenden Ressourcen:
  - Jede Ressource, die mit dem Schlüssel-Wert-Paar `backupplan:dsi-sandbox-daily` markiert ist
  - Jede Ressource, die mit dem Wert `prod` oder Werten, die mit `prod/` beginnen, markiert ist
  - Folgende Ressourcen werden von der Ressourcenzuweisung nicht gesichert:
    - Alle RDS-, Aurora-, Neptune- oder DocumentDB-Cluster
    - Jede Ressource, die mit dem Wert `test` oder Werten, die mit `test/` beginnen, markiert ist

```
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/*
```

Kontingente für die Ressourcenzuweisung

Die folgenden Kontingente gelten für eine einzelne Ressourcenzuweisung:

- 500 Amazon-Ressourcennamen (ARNs) ohne Platzhalter
- 30 ARNs mit Platzhalterausdrücken
- 30 Bedingungen
- 30 Tags pro Ressourcenzuweisung (und eine unbegrenzte Anzahl von Ressourcen pro Tag)

Löschen eines Backup-Plans

Sie können einen Sicherungsplan erst löschen, wenn alle zugehörigen Ressourcenauswahlen gelöscht wurden. Diese Auswahlen werden auch als Ressourcenzuweisungen bezeichnet. Wenn diese vor dem Löschen des Backup-Plans nicht gelöscht wurden, zeigt die Konsole die folgende Fehlermeldung an: „Die Auswahl verwandter Backup-Pläne muss vor dem Löschen des Backup-Plans gelöscht werden.“ Verwenden Sie die Konsole oder verwenden Sie `DeleteBackupSelection`.

Das Löschen eines Sicherungsplans löscht die aktuelle Version des Plans. Die aktuelle und die vorherige Versionen, sofern vorhanden, bestehen weiterhin, sie werden jedoch nicht mehr in der Konsole unter Backup plans (Sicherungspläne) aufgeführt.

> **Note**
>
> Wenn ein Sicherungsplan gelöscht wird, werden vorhandene Sicherungen nicht gelöscht. Um vorhandene Backups zu entfernen, löschen Sie sie mithilfe der Schritte unter Löschen von Backups aus dem Backup-Tresor.

Um einen Backup-Plan mit der AWS Backup Konsole zu löschen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich auf der linken Seite Backup plans (Sicherungspläne) aus.
3. Wählen Sie Ihren Sicherungsplan in der Liste aus.
4. Wählen Sie alle Ressourcenzuweisungen, die mit dem Sicherungsplan verbunden sind.
5. Wählen Sie Löschen aus.

Aktualisieren eines Backup-Plans

Nachdem Sie einen Backup-Plan erstellt haben, können Sie ihn bearbeiten und beispielsweise Tags hinzufügen oder Backup-Regeln hinzufügen, bearbeiten oder löschen. Änderungen, die Sie an einem Sicherungsplan vornehmen, wirken sich nicht auf von diesem Sicherungsplan erstellte vorhandene Sicherungen aus. Die Änderungen gelten nur für Sicherungen, die zukünftig erstellt werden.

Wenn Sie beispielsweise in einer Sicherungsregel den Aufbewahrungszeitraum aktualisieren, bleibt der Aufbewahrungszeitraum für die Sicherungen, die vor dieser Aktualisierung erstellt wurden, unverändert. Alle Sicherungen, die künftig von dieser Regel erstellt werden, verwenden den aktualisierten Aufbewahrungszeitraum.

Sie können den Namen eines Plans nicht ändern, nachdem er erstellt wurde.

Um einen Backup-Plan mit der AWS Backup Konsole zu bearbeiten

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.
3. Im zweiten Bereich, Backup-Pläne, werden bestehende Back-Pläne angezeigt. Wählen Sie den unterstrichenen Link in der Spalte Name des Backup-Plans, um Details zum ausgewählten Backup-Plan zu sehen.

4. Sie können eine Backup-Regel bearbeiten, Ressourcenzuweisungen anzeigen, Backup-Jobs anzeigen, Tags verwalten oder Windows VSS-Einstellungen ändern.
5. Um eine Backup-Regel zu aktualisieren, wählen Sie den Namen der Backup-Regel aus.

   Wählen Sie Tags verwalten aus, um Stichwörter hinzuzufügen oder zu löschen.

   Wählen Sie neben Erweiterte Backup-Einstellungen die Option Bearbeiten aus, um Windows VSS ein- oder auszuschalten.
6. Ändern Sie die gewünschten Einstellungen und wählen Sie dann Speichern aus.

Sicherungstresore

> **Note**
>
> bietet ab dem 9. August 2023 eine Vorschau auf die Nutzung eines Tresors mit logischem Air-Gap. AWS Backup
> `<Um sich für diese Vorversion anzumelden, senden Sie eine Anfrage per E-Mail`
> Die Funktionen können sich während und nach der Vorversion ändern oder angepasst werden. Wenn der Service allgemein verfügbar (generally available, GA) wird, sind die in der Vorversion bereitgestellten Daten und Konfigurationen nicht mehr verfügbar. AWS empfiehlt, in der Vorversion Testdaten anstelle von Produktionsdaten zu verwenden.

In AWS Backup einem Backup-Tresor handelt es sich um einen Container, in dem Ihre Backups gespeichert und organisiert werden.

Wenn Sie einen Backup-Tresor erstellen, müssen Sie den Verschlüsselungsschlüssel AWS Key Management Service (AWS KMS) angeben, mit dem einige der in diesem Tresor gespeicherten Backups verschlüsselt werden. Die Verschlüsselung für andere Backups wird von ihren AWS Quelldiensten verwaltet. Weitere Informationen zur Verschlüsselung finden Sie in der Tabelle in Verschlüsselung für Backups in AWS.

Ihr Konto verfügt immer über einen Standard-Backup-Tresor. Wenn Sie verschiedene Verschlüsselungsschlüssel oder Zugriffsrichtlinien für verschiedene Gruppen von Backups benötigen, können Sie auch mehrere Backup-Tresore erstellen.

Dieser Abschnitt enthält eine Übersicht über die Verwaltung Ihrer Sicherungstresore in AWS Backup.

Themen

Logische Air-Gapped Vaults (Vorversion)

> **Note**
>
> bietet ab dem 9. August 2023 eine Vorschau auf die Nutzung eines Tresors mit logischem Air-Gap an. AWS Backup
> <Um sich für diese Vorversion anzumelden, senden Sie eine Anfrage per E-Mail
> Die Funktionen können sich während und nach der Vorversion ändern oder angepasst werden. Wenn der Service allgemein verfügbar (generally available, GA) wird, sind die in der Vorversion bereitgestellten Daten und Konfigurationen nicht mehr verfügbar. AWS empfiehlt, in der Vorversion Testdaten anstelle von Produktionsdaten zu verwenden.

Übersicht

AWS Backup zeigt eine Vorschau eines sekundären Tresortyps an, der Kopien von Backups in anderen Tresoren speichern kann. Ein logischer Air-Gapped Vault ist ein spezialisierter Tresor, der zusätzlich zu den Sicherheitsfunktionen eines Backup-Tresors weitere Sicherheitsfunktionen bereitstellt und die Möglichkeit bietet, den Zugriff auf den Tresor für andere Konten und Organisationen freizugeben, sodass die Wiederherstellungszeit (Recovery Time Objective, RTO) im Fall eines Vorfalls, der eine schnelle Wiederherstellung von Ressourcen erfordert, kürzer ist und flexibler gestaltet werden kann.

Tresore mit logischem Air-Gap sind mit zusätzlichen Schutzfunktionen ausgestattet: Jeder dieser Tresore ist mit einem AWS eigenen Schlüssel verschlüsselt, und jeder Tresor verfügt über eine Tresorsperre, die im Compliance-Modus aktiviert ist.

Sie können einen logischen Air-Gapped Vault auch organisations- und kontenübergreifend gemeinsam nutzen, sodass die darin gespeicherten Backups bei Bedarf von einem Konto wiederhergestellt werden können, mit dem der Tresor gemeinsam genutzt wird.

Während der Vorversion fallen keine zusätzlichen Gebühren für die Speicherung in logischen Air-Gapped Vaults an. Backups in Standard-Backup-Tresoren und regionsübergreifende Kopien werden weiterhin zu den veröffentlichten Preisen berechnet (siehe AWS Backup – Preise), auch wenn für Kopien dieser Backups in logischen Air-Gapped Vaults keine Gebühren anfallen.

Anwendungsfall

Ein logischer Air-Gapped Vault ist ein sekundärer Tresor, der als Teil einer Datenschutzstrategie dient. Dieser Tresor kann Ihnen helfen, die Aufbewahrung und Wiederherstellung in Ihrer Organisation zu verbessern, wenn Sie einen Tresor für Ihre Backups möchten, der

- automatisch mit einer Tresorsperre im Compliance-Modus eingerichtet ist;
- Backups enthält, die mit einem anderen Konto als dem Konto, das den Backup erstellt hat, gemeinsam genutzt und von diesem Konto wiederhergestellt werden können;
- Wird mit einem eigenen Schlüssel verschlüsselt geliefert AWS

Zu den Ressourcen, die in einem logischen Air-Gapped Vault unterstützt werden, gehören

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

Diese Vorversion von logischen Air-Gapped Vaults ist nur in der Region USA Ost (Nord-Virginia) verfügbar. Da dieses Feature derzeit nur in einer Region verfügbar ist, wird regionsübergreifendes Kopieren während dieses Vorversionszeitraums nicht unterstützt.

Vergleich und Gegenüberstellung mit einem Standard-Backup-Tresor

Ein Backup-Tresor ist der primäre und standardmäßige Tresorttyp, der in verwendet wird AWS Backup. Jedes Backup wird beim Erstellen in einem Backup-Tresor gespeichert. Sie können ressourcenbasierte Richtlinien zuweisen, um die im Tresor gespeicherten Backups zu verwalten, z. B. den Lebenszyklus von im Tresor gespeicherten Backups.

Ein logischer Air-Gapped Vault ist ein spezialisierter Tresor mit zusätzlicher Sicherheit und flexibler gemeinsamer Nutzung für eine kürzere Wiederherstellungszeit (Recovery Time Objective, RTO). In diesem Tresor werden Kopien von Backups gespeichert, die ursprünglich in einem Standard-Backup-Tresor erstellt und gespeichert wurden.

Backup-Tresore können mit einem Schlüssel verschlüsselt werden, einem Sicherheitsmechanismus, der den Zugriff auf vorgesehene Benutzer beschränkt. Diese Schlüssel können vom Kunden

verwaltet oder AWS verwaltet werden. Darüber hinaus kann ein Backup-Tresor durch eine Tresorsperre noch besser geschützt werden. Logische Air-Gapped Vaults verfügen über eine Tresorsperre im Compliance-Modus.

Wenn der AWS KMS Schlüssel zum Zeitpunkt der Erstellung der ursprünglichen Ressource nicht manuell geändert oder als vom Kunden verwalteter Schlüssel (CMK) festgelegt wurde, kann ein Backup nicht in einen Tresor mit logischem Air-Gap kopiert werden.

Funktion	Sicherungstresor	Logischer Air-Gapped Vault (Vorversion)
Backup-Erstellung	Wenn ein Backup erstellt wird, wird es als Wiederherstellungspunkt gespeichert.	Backups werden bei der Erstellung nicht in diesem Tresor gespeichert.
Backup-Speicher	Kann erste Backups von Ressourcen und Kopien von Backups speichern	Kann Kopien von Backups von anderen Tresoren speichern
Sicherheit	Kann optional mit einem Schlüssel verschlüsselt werden (vom Kunden verwaltet oder verwaltet) AWS Kann optional mit einer Tresorsperre gesperrt werden	Ist mit einem AWS eigenen Schlüssel verschlüsselt Ist immer mit einer Tresorsperre im Compliance-Modus gesperrt
Gemeinsame Nutzbarkeit	Zugriff kann über Richtlinien und AWS Organizations verwaltet werden. Nicht kompatibel mit AWS Resource Access Manager	Kann optional mit AWS RAM über mehrere Konten hinweg gemeinsam genutzt werden
Wiederherstellung	Backups können von demselben Konto wiederhergestellt werden, dem der Tresor gehört.	Backups können von einem anderen Konto als dem, dem das Backup gehört, wiederhergestellt werden, wenn der

Funktion	Sicherungstresor	Logischer Air-Gapped Vault (Vorversion)
		Tresor für dieses separate Konto freigegeben wird.
Regionalität	Verfügbar in allen Regionen, in denen es AWS Backup tätig ist	Im Rahmen der Vorversion in der Region USA Ost (Nord-Virginia) verfügbar
Ressourcen	Kann Backups speichern, die alle AWS Backup unterstützten Ressourcen enthalten	Kann Backups speichern, die Amazon-EC2-, Amazon-EBS-, Amazon-EFS-, Amazon-S3- oder Amazon-RDS-Daten enthalten

Erstellen eines logischen Air-Gapped Vault von der Konsole aus

> **Important**
>
> Ist der Tresor erstellt, können weder Tresorname, Tresortyp noch der Mindest- und der Höchstaufbewahrungszeitraum geändert werden. Darüber hinaus kann die Tresorsperre nicht aufgehoben werden.
> Sobald der Dienst allgemein verfügbar ist, sind die in der Vorversion bereitgestellten Daten und Konfigurationen nicht mehr verfügbar. AWS empfiehlt, in der Vorschau Testdaten anstelle von Produktionsdaten zu verwenden.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Tresore aus.
3. Beide Tresortypen werden angezeigt. Wählen Sie Neuen Tresor erstellen aus.
4. Geben Sie einen Namen für Ihren Sicherungstresor ein. Sie können den Namen Ihres Tresors so wählen, dass er angibt, was in ihm gespeichert wird, oder so, dass die Suche nach den benötigten Sicherungen erleichtert wird. Geben Sie ihm beispielsweise den Namen `FinancialBackups`.
5. Aktivieren Sie das Optionsfeld für Logischer luftdicht verschlossenen Tresor.

6. Legen Sie den Mindestaufbewahrungszeitraum fest.

   Dieser Wert (in Tagen, Monaten oder Jahren) ist der kürzeste Zeitraum, für den ein Backup in diesem Tresor aufbewahrt werden kann. Backups mit Aufbewahrungszeiträumen, die kürzer sind als dieser Wert, können nicht in diesen Tresor kopiert werden.

7. Legen Sie den Höchstaufbewahrungszeitraum fest.

   Dieser Wert (in Tagen, Monaten oder Jahren) ist der längste Zeitraum, für den ein Backup in diesem Tresor aufbewahrt werden kann. Backups mit Aufbewahrungszeiträumen, die diesen Wert überschreiten, können nicht in diesen Tresor kopiert werden.

8. (Optional) Fügen Sie Tags hinzu, die Ihnen helfen, Ihren logischen Air-Gapped Vault zu suchen und zu identifizieren. Beispielsweise können Sie den Tag `BackupType:Financial` hinzufügen.

9. Wählen Sie Tresor erstellen aus.

10. Überprüfen Sie die Einstellungen. Wenn alle Einstellungen wie gewünscht angezeigt werden, wählen Sie Logischen luftdicht verschlossenen Tresor erstellen aus.

11. Die Konsole leitet Sie zur Detailseite Ihres neuen Tresors weiter. Vergewissern Sie sich, dass die Tresordetails wie gewünscht festgelegt sind.

Anzeigen der Details des logischen Air-Gapped Vault in der Konsole

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.

2. Wählen Sie im linken Navigationsbereich die Option Tresore aus.

3. Unter den Beschreibungen der Tresore finden Sie zwei Listen: Tresore, die diesem Konto gehören und Mit diesem Konto geteilte Tresore. Wählen Sie die gewünschte Registerkarte aus, um die Tresore anzuzeigen.

4. Klicken Sie unter Tresorname auf den Namen des Tresors, um die Detailseite zu öffnen. Sie können die Zusammenfassung, die Wiederherstellungspunkte, die geschützten Ressourcen, die Kontofreigabe, die Zugriffsrichtlinie und Tag-Details einsehen.

Kopieren aus einem Standard-Backup-Tresor in einen logischen Air-Gapped Vault über die Konsole

Logische Air-Gapped Vaults können nur ein Kopierauftragsziel in einem Backup-Plan oder ein Ziel für einen On-Demand-Kopierauftrag sein.

Um einen Kopierauftrag zu initiieren, benötigen Sie

- einen Backup-Tresor;
- einen logischen Air-Gapped Vault;
- ein Backup mit Amazon-EC2-, Amazon-EBS-, Amazon-RDS-, Amazon-S3- oder Amazon-EFS-Daten;
- die Berechtigung `kms:CreateGrant` für die Rolle, die zum Erstellen der Kopie verwendet wird;
- Keine mit einem AWS verwalteten Schlüssel verschlüsselten Backups als Teil Ihres Kopierauftrags in den Tresor mit logischem Air-Gap

Sobald Sie bestätigt haben, dass die obigen Bedingungen erfüllt sind, gehen Sie folgendermaßen vor:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Tresore aus.
3. Auf der Tresordetailseite werden alle Wiederherstellungspunkte innerhalb dieses Tresors angezeigt. Aktivieren Sie das Kontrollkästchen neben dem Wiederherstellungspunkt, den Sie kopieren möchten.
4. Wählen Sie Aktionen und dann im Dropdown-Menü Kopieren aus.
5. Geben Sie auf dem nächsten Bildschirm die Details des Ziels ein.
    a. Die Region muss auf USA Ost (Nord-Virginia) eingestellt sein.
    b. Das Dropdown-Menü für den Ziel-Backup-Tresor zeigt die geeigneten Zieltresore an. Wählen Sie einen vom Typ `logically air-gapped vault` aus.
6. Wählen Sie Kopieren aus, sobald alle Details Ihren Präferenzen entsprechen.

Auf der Seite Aufträge in der Konsole können Sie Kopieraufträge auswählen, um die aktuellen Kopieraufträge einzusehen.

Weitere Informationen finden Sie unter Kopieren eines Backups, Erstellen von Backup-Kopien über AWS-Regionen hinweg und Erstellen von Backup-Kopien über AWS-Konten hinweg.

Freigeben eines logischen Air-Gapped Vault über die Konsole

> **Note**
>
> Nur Konten mit bestimmten IAM-Berechtigungen können Konten freigeben und die Freigabe von Konten verwalten.

Sie können AWS RAM einen Tresor mit logischem Air-Gap gemeinsam mit anderen von Ihnen angegebenen Konten verwenden. Stellen Sie für die gemeinsame Nutzung sicher AWS RAM, dass Sie über Folgendes verfügen:

- Zwei oder mehr Konten, auf die zugegriffen werden kann AWS Backup
- Ein Konto, über das die Freigabe durchgeführt werden soll, das über die notwendigen RAM-Berechtigungen verfügt. Die Berechtigung `ram:CreateResourceShare` ist für dieses Verfahren erforderlich. Die Richtlinie `AWSResourceAccessManagerFullAccess` enthält alle erforderlichen RAM-bezogenen Berechtigungen.
- Mindestens einen logischen Air-Gapped Vault

Gehen Sie folgendermaßen vor, um einen logischen Air-Gapped Vault freizugeben:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Tresore aus.
3. Unter den Beschreibungen der Tresore finden Sie zwei Listen: Tresore, die diesem Konto gehören und Mit diesem Konto geteilte Tresore. Wählen Sie die gewünschte Liste aus, um die Tresore anzuzeigen.
4. Wählen Sie unter Tresorname den Namen des logischen Air-Gapped Vault aus, um die Detailseite zu öffnen.
5. Im Bereich Gemeinsame Nutzung von Konten wird angezeigt, mit welchen Konten der Tresor gemeinsam genutzt wird.
6. Um mit der Freigabe für ein anderes Konto zu beginnen oder Konten zu bearbeiten, die bereits gemeinsam genutzt werden, wählen Sie Freigabe verwalten aus.

AWS RAM Die Konsole wird geöffnet, wenn „Teilen verwalten“ ausgewählt ist. Anweisungen zur gemeinsamen Nutzung einer Ressource mithilfe von AWS RAM finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM.

Stellen Sie sicher, dass Sie über die entsprechenden Berechtigungen verfügen. Die Backup-Administrator-IAM-Richtlinie [AWSBackupFullAccess] und die Backup-Operator-IAM-Richtlinie [AWSBackupOperatorAccess] enthalten die erforderlichen Rechte zum Anzeigen gemeinsam genutzter Konten. Für die Rolle, die Sie für die gemeinsame Nutzung verwenden, sind jedoch Resource Access Manager Manager-Schreibberechtigungen erforderlich, um das Konto aus dem RAM gemeinsam zu nutzen, z. B. `ram:CreateResourceShare`

Das Konto, das aufgefordert wurde, eine Einladung anzunehmen, um eine Freigabe zu erhalten, hat 12 Stunden Zeit, die Einladung anzunehmen. Weitere Informationen finden Sie unter Annehmen und Ablehnen von Einladungen zur Ressourcenfreigabe im AWS -RAM-Benutzerhandbuch.

Wenn die Schritte für die Freigabe abgeschlossen und akzeptiert wurden, wird die Seite mit der Tresorübersicht unter Gemeinsame Nutzung von Konten = Geteilt – siehe Tabelle zur gemeinsamen Nutzung von Konten unten angezeigt.

Wiederherstellen eines Backups aus einem logischen Air-Gapped Vault mithilfe der Konsole

Sie können ein in einem logischen Air-Gapped Vault gespeichertes Backup entweder von dem Konto, dem der Tresor gehört, oder von einem beliebigen Konto, für das der Tresor freigegeben ist, wiederherstellen.

Informationen zum Wiederherstellen eines Backups finden Sie unter Wiederherstellen eines Backups.

Löschen eines logischen Air-Gapped Vault mithilfe der Konsole

> **Important**
>
> Sobald der Service allgemein verfügbar ist, sind die in der Vorversion bereitgestellten Daten und Konfigurationen nicht mehr verfügbar. AWS empfiehlt, in der Vorschau Testdaten anstelle von Produktionsdaten zu verwenden.

Informationen zum Löschen eines Tresors finden Sie unter Löschen eines Backup-Tresors. Tresore können nicht gelöscht werden, wenn sie noch Backups (Wiederherstellungspunkte) enthalten. Stellen Sie sicher, dass der Tresor keine Backups enthält, bevor Sie einen Löschvorgang starten.

Logische Air-Gapped Vaults über die CLI/API

Sie können AWS CLI es verwenden, um programmgesteuert Operationen für Tresore mit logischem Air-Gap auszuführen. Jede CLI ist spezifisch für den AWS Dienst, aus dem sie stammt. Befehlen, die sich auf Freigaben beziehen, wird `aws ram` vorangestellt. Allen anderen Befehlen sollte `aws backup` vorangestellt werden.

Erstellen

Der folgende CLI-Beispielbefehl `CreateLogicallyAirGappedBackupVault` kann abgeändert werden, um einen logischen Air-Gapped Backup-Vault zu erstellen:

```
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
```

View details (Details anzeigen)

Der folgende CLI-Beispielbefehl `DescribeBackupVault` kann geändert werden, um Details zu einem Tresor abzurufen:

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

Freigeben

> **Note**
>
> Nur Konten mit ausreichenden IAM-Berechtigungen können Konten freigeben und die Freigabe von Konten verwalten.

Sie können einen logischen Air-Gapped Vault über AWS Resource Access Manager (RAM) freigeben. Dabei handelt es sich um einen Service, der Benutzern hilft, Ressourcen freizugeben.

AWS RAM verwendet den CLI-Befehl`create-resource-share`. Der Zugriff auf diesen Befehl steht nur Administratorkonten mit ausreichenden Berechtigungen zur Verfügung. Die CLI-Schritte finden Sie unter Erstellen einer Ressourcenfreigabe in AWS RAM.

Die Schritte 1 bis 4 werden mit dem Konto ausgeführt, dem der logische Air-Gapped Vault gehört. Die Schritte 5 bis 8 werden mit dem Konto ausgeführt, für das der logische Air-Gapped Vault freigegeben werden soll.

1. Melden Sie sich bei dem Eigentümerkonto an ODER fordern Sie einen Benutzer in Ihrer Organisation, der über ausreichende Anmeldeinformationen für den Zugriff auf das Quellkonto verfügt, auf, diese Schritte durchzuführen.

   - Wenn zuvor eine Ressourcenfreigabe erstellt wurde und Sie ihr eine zusätzliche Ressource hinzufügen möchten, verwenden Sie stattdessen die CLI `associate-resource-share` mit dem ARN des neuen Tresors.

2. Rufen Sie die Anmeldeinformationen einer Rolle mit ausreichenden Berechtigungen für die Freigabe über RAM ab. Geben Sie diese in die CLI ein.

   - Die Berechtigung `ram:CreateResourceShare` ist für dieses Verfahren erforderlich. Die Richtlinie AWSResourceAccessManagerFullAccessenthält alle RAM-bezogenen Berechtigungen.

3. Benutzen create-resource-share.

   a. Geben Sie den ARN des logischen Air-Gapped Vault an.

   b. Beispieleingabe:

```
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
```

   Beispielausgabe:

```
{
```

```
   "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. Kopieren Sie den Ressourcenfreigabe-ARN in die Ausgabe (benötigt für nachfolgende Schritte). Geben Sie den ARN an den Betreiber des Kontos weiter, das Sie einladen, die Freigabe zu erhalten.
5. Abrufen des Ressourcenfreigabe-ARN

   a. Wenn Sie die Schritte 1 bis 4 nicht durchgeführt haben, holen Sie sich das resourceShareArn von demjenigen, der es getan hat.

   b. Beispiel: `arn:aws:ram:us-east-1:`*`123456789012`*`:resource-share/`*`12345678-abcd-09876543`*
6. Übernehmen Sie in der CLI die Anmeldeinformationen des Empfängerkontos.
7. Rufen Sie mit `get-resource-share-invitations` die Ressourcenfreigabeeinladung ab. Weitere Informationen finden Sie unter Annehmen und Ablehnen von Ressourcenfreigabeeinladungen im AWS RAM -Benutzerhandbuch.
8. Nehmen Sie die Einladung im Zielkonto (Wiederherstellungskonto) an.

   - Verwenden Sie `accept-resource-share-invitation` (`reject-resource-share-invitation` auch möglich).

Auflisten

Der CLI-Befehl `ListBackupVaults` kann so geändert werden, dass er alle Tresore auflistet, die dem Konto gehören und in diesem vorhanden sind:

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

Um nur die logischen Air-Gapped Vaults aufzulisten, fügen Sie diesen Parameter hinzu:

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Um die für das Konto freigegebenen Tresore aufzulisten, verwenden Sie:

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

Kopieren

Ein logischer Air-Gapped Vault kann nur ein Ziel für einen Kopierauftrag eines Backups sein, nicht aber das Ziel für einen ursprünglichen Backup-Auftrag. Verwenden Sie `StartCopyJob`, um ein vorhandenes Backup in einem Backup-Tresor in einen logischen Air-Gapped Vault zu kopieren.

Die Rolle, die verwendet wird, um den Kopierauftrag in den logischen Air-Gapped Vault zu erstellen, muss über die Berechtigung `kms:CreateGrant` verfügen.

CLI-Beispieleingabe:

```
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
```

Wiederherstellung

Sobald ein Backup von einem logischen Air-Gapped Vault für Ihr Konto freigegeben wurde, können Sie `StartRestoreJob` zum Wiederherstellen des Backups verwenden. CLI-Beispieleingabe:

```
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
```

Löschen

Der folgende CLI-Beispielbefehl `DeleteBackupVault` kann verwendet werden, um einen Tresor zu löschen. Ein Tresor kann nur gelöscht werden, wenn sich innerhalb des Tresors keine Backups (Wiederherstellungspunkte) befinden.

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

Zu den weiteren verfügbaren programmgesteuerten Optionen gehören:

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Erstellen eines Backup-Tresors

Sie müssen mindestens einen Tresor erstellen, bevor Sie einen Backup-Plan erstellen oder einen Backup-Auftrag starten können.

Wenn Sie die AWS Backup Konsole zum ersten Mal in einem verwenden AWS-Region, erstellt die Konsole automatisch einen Standardtresor.

Wenn Sie jedoch das AWS Backup AWS CLI AWS SDK oder AWS CloudFormation verwenden, wird kein Standardtresor erstellt. Sie müssen einen eigenen Tresor erstellen.

Erforderliche Berechtigungen

Sie benötigen die folgenden Berechtigungen, um einen Backup-Tresor mit zu erstellen AWS Backup.

```
{
  "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": "*"
    }
  ]
}
```

Erstellen eines Backup-Tresors (Konsole)

step-by-step Anweisungen zum Erstellen eines Backup-Tresors mithilfe der AWS Backup Konsole finden Sie Schritt 3: Einen Backup-Tresor erstellen im Handbuch Erste Schritte.

Erstellen eines Backup-Tresors (programmgesteuert)

Der folgende AWS Command Line Interface Befehl erstellt einen Backup-Tresor:

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

Sie können auch die folgenden Konfigurationen für einen Backup-Tresor festlegen.

Name des Backup-Tresors

Bei Namen von Sicherungstresoren wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen zwischen 2 und 50 alphanumerische Zeichen, Bindestriche oder Unterstriche enthalten.

AWS KMS Verschlüsselungsschlüssel

Der AWS KMS Verschlüsselungsschlüssel schützt Ihre Backups in diesem Backup-Tresor. Standardmäßig erstellt AWS Backup für Sie einen KMS-Schlüssel mit dem Alias `aws/backup`. Sie können diesen Schlüssel oder einen anderen Schlüssel in Ihrem Konto auswählen (kontenübergreifende KMS-Schlüssel können über die CLI verwendet werden).

Sie können einen neuen Verschlüsselungsschlüssel erstellen, indem Sie dem Verfahren zum Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch folgen.

Nachdem Sie einen Backup-Tresor erstellt und den AWS KMS Verschlüsselungsschlüssel festgelegt haben, können Sie den Schlüssel für diesen Backup-Tresor nicht mehr bearbeiten.

Der in einem AWS Backup Tresor angegebene Verschlüsselungsschlüssel gilt für die Backups bestimmter Ressourcentypen. Weitere Informationen zur Verschlüsselung von Sicherungen finden Sie unter Verschlüsselung für Backups in AWS Backup im Abschnitt „Sicherheit“. Sicherungen aller anderen Ressourcentypen werden mit dem Schlüssel gesichert, der zum Verschlüsseln der Quellressource verwendet wurde.

Backup-Tresor-Tags

Diese Tags sind dem Sicherungstresor zugeordnet, um Sie beim Organisieren und Nachverfolgen Ihrer Sicherungstresore zu unterstützen.

Festlegen von Zugriffsrichtlinien für Backup-Tresore

Mit AWS Backup können Sie Backup-Tresoren und den darin enthaltenen Ressourcen Richtlinien zuweisen. Durch das Zuweisen von Richtlinien können Sie beispielsweise Benutzern Zugriff gewähren, um Sicherungspläne und On-Demand-Sicherungen zu erstellen, dabei aber die Möglichkeit, Wiederherstellungspunkte nach ihrer Erstellung zu löschen, einschränken.

Informationen zur Verwendung von Richtlinien für das Gewähren oder Einschränken des Zugriffs auf Ressourcen finden Sie unter Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien im IAM-Benutzerhandbuch. Sie können den Zugriff auch mithilfe von Tags steuern.

Sie können die folgenden Beispielrichtlinien als Leitfaden verwenden, um den Zugriff auf Ressourcen einzuschränken, wenn Sie mit AWS Backup Tresoren arbeiten. Im Gegensatz zu anderen IAM-basierten Richtlinien unterstützen AWS Backup Zugriffsrichtlinien keinen Platzhalter im Schlüssel. `Action`

Eine Liste der Amazon-Ressourcennamen (ARNs), mit denen Sie Wiederherstellungspunkte für verschiedene Ressourcentypen identifizieren können, finden Sie unter AWS Backup Ressourcen-ARNs für ressourcenspezifische Wiederherstellungspunkt-ARNs.

Vault-Zugriffsrichtlinien regeln nur den Benutzerzugriff auf APIs. AWS Backup Auf einige Backup-Typen, wie Snapshots von Amazon Elastic Block Store (Amazon EBS) und Amazon Relational Database Service (Amazon RDS), kann auch über die APIs dieser Services zugegriffen werden. Sie können separate Zugriffsrichtlinien in IAM erstellen, die den Zugriff auf diese APIs steuern, um den Zugriff auf diese Backup-Typen vollständig kontrollieren zu können.

Unabhängig von der Zugriffsrichtlinie für den AWS Backup Tresor `backup:CopyIntoBackupVault` wird der kontoübergreifende Zugriff für alle Aktionen abgelehnt. Das heißt, es AWS Backup wird jede andere Anfrage von einem Konto abgelehnt, das sich von dem Konto der Ressource unterscheidet, auf die verwiesen wird.

Themen

- Verweigern des Zugriffs auf einen Ressourcentyp in einem Backup-Tresor
- Verweigern des Zugriffs auf einen Backup-Tresor
- Verweigern des Zugriffs zum Löschen von Wiederherstellungspunkten in einem Backup-Tresor

Verweigern des Zugriffs auf einen Ressourcentyp in einem Backup-Tresor

Diese Richtlinie verweigert den Zugriff auf die angegebenen API-Operationen für alle Amazon–EBS-Snapshots in einem Backup-Tresor.

```
{
    "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/*"]
        }
    ]
}
```

Verweigern des Zugriffs auf einen Backup-Tresor

Diese Richtlinie verweigert den Zugriff auf die angegebenen API-Operationen, die auf einen Sicherungstresor abzielen.

```
{
    "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"
        }
    ]
}
```

Verweigern des Zugriffs zum Löschen von Wiederherstellungspunkten in einem Backup-Tresor

Der Zugriff auf Tresore sowie die Fähigkeit zum Löschen der darin gespeicherten Wiederherstellungspunkte wird durch den Zugriff gesteuert, den Sie Ihren Benutzern gewähren.

Gehen Sie wie folgt vor, um eine ressourcenbasierte Zugriffsrichtlinie für einen Sicherungstresor zu erstellen, die das Löschen von Sicherungen in dem Sicherungstresor verhindert.

So erstellen Sie eine ressourcenbasierte Zugriffsrichtlinie für einen Sicherungstresor:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich auf der linken Seite Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Sicherungstresor in der Liste aus.
4. Fügen Sie im Abschnitt Access policy (Zugriffsrichtlinie) das folgende JSON-Beispiel ein. Diese Richtlinie verhindert, dass Personen, die nicht der Prinzipal sind, einen Wiederherstellungspunkt im Zielsicherungstresor löschen.

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

Verwenden Sie den globalen Bedingungsschlüssel `aws:PrincipalArn` im folgenden Beispiel, um das Auflisten von IAM-Identitäten mithilfe ihres ARN zu ermöglichen.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Informationen zum Abrufen einer eindeutigen ID für eine IAM-Entität finden Sie unter Abrufen des eindeutigen Bezeichners im IAM-Benutzerhandbuch.

Wenn Sie dies auf bestimmte Ressourcentypen beschränken möchten, können Sie anstelle von `"Resource": "*"` die zu verweigernden Wiederherstellungspunkttypen explizit einschließen. Ändern Sie beispielsweise für Amazon-EBS-Snapshots den Ressourcentyp wie folgt.

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

5. Wählen Sie Richtlinie anfügen aus.

AWS Backup Vault Lock

> **Note**
>
> AWS Backup Vault Lock wurde von Cohasset Associates für den Einsatz in Umgebungen geprüft, die den Vorschriften von SEC 17a-4, CFTC und FINRA unterliegen. Weitere Informationen darüber, wie AWS Backup Vault Lock mit diesen Vorschriften zusammenhängt, finden Sie in der Compliance-Bewertung von Cohasset Associates.

AWS Backup Vault Lock ist eine optionale Funktion eines Backup-Tresors, die Ihnen zusätzliche Sicherheit und Kontrolle über Ihre Backup-Tresore bieten kann. Wenn eine Sperre im Compliance-Modus aktiv und die Kulanzzeit abgelaufen ist, kann die Tresorkonfiguration nicht von einem Kunden, Konto-/Dateneigentümer oder AWS geändert oder gelöscht werden. Jeder Tresor kann eine Tresorsperre haben.

AWS Backup stellt sicher, dass Ihre Backups für Sie verfügbar sind, bis ihre Aufbewahrungsfristen abgelaufen sind. Wenn ein Benutzer (einschließlich des Root-Benutzers) versucht, ein Backup zu löschen oder die Lebenszykluseigenschaften in einem gesperrten Tresor zu ändern, AWS Backup wird der Vorgang verweigert.

- Bei im Governance-Modus gesperrten Tresoren kann die Sperre von Benutzern mit ausreichenden IAM-Berechtigungen aufgehoben werden.
- Im Compliance-Modus gesperrte Tresore können nicht mehr gelöscht werden, wenn die Bedenkzeit (Kulanzzeit) abgelaufen ist. Während der Kulanzzeit können Sie die Tresorsperre weiterhin aufheben und die Sperrkonfiguration ändern.

Modi der Tresorsperre

Wenn Sie eine Tresorsperre erstellen, haben Sie die Wahl zwischen zwei Modi: dem Governance-Modus und dem Compliance-Modus. Im Governance-Modus kann ein Tresor nur von Benutzern mit ausreichenden IAM-Berechtigungen verwaltet werden. Der Governance-Modus unterstützt eine Organisation bei der Erfüllung von Governance-Anforderungen und stellt sicher, dass nur speziell bestimmtes Personal Änderungen an einem Backup-Tresor vornehmen kann. Der Compliance-Modus ist für Backup-Tresore vorgesehen, bei denen davon ausgegangen wird, dass der Tresor (und damit auch sein Inhalt) vor Ablauf des Datenaufbewahrungszeitraums niemals gelöscht oder

verändert wird. Sobald ein Tresor im Compliance-Modus gesperrt ist, ist er unveränderlich, d. h. die Sperre kann nicht aufgehoben werden.

Ein im Governance-Modus gesperrter Tresor kann von Benutzern verwaltet oder gelöscht werden, die über die entsprechenden IAM-Berechtigungen verfügen.

Eine Tresorsperre im Compliance-Modus kann weder von Benutzern noch von AWS geändert oder gelöscht werden. Eine Tresorsperre im Compliance-Modus hat eine von Ihnen festgelegte Kulanzzeit, bevor die Sperre einsetzt und unveränderlich wird.

Vorteile der Tresorsperre

AWS Backup Vault Lock bietet mehrere Vorteile, darunter:

- WORM-Konfiguration (Write Once, Read Many) für alle Backups, die Sie in einem Backup-Tresor speichern und erstellen;
- Eine zusätzliche Schutzebene, die Backups (Wiederherstellungspunkte) in Ihren Backup-Tresoren vor versehentlichem oder böswilligem Löschen schützt;
- Durchsetzung von Aufbewahrungsfristen, die vorzeitige Löschungen durch privilegierte Benutzer (einschließlich AWS-Konto Root-Benutzer) verhindern und die Datenschutzrichtlinien und -verfahren Ihres Unternehmens einhalten.

Sperren eines Backup-Tresors über die Konsole

Sie können Ihrem Tresor mithilfe der Backup-Konsole eine AWS Backup Tresorsperre hinzufügen.

So fügen Sie Ihrem Backup-Tresor eine Tresorsperre hinzu

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Suchen Sie im Navigationsbereich die Option Backup-Tresore. Klicken Sie auf den Link unterhalb der Backup-Tresore mit dem Namen Tresorsperren.
3. Klicken Sie unter So funktionieren Tresorverriegelungen oder Tresorsperren auf + Tresorsperre erstellen.
4. Wählen Sie im Bereich Details zur Tresorsperre den Tresor aus, auf den die Sperre angewendet werden soll.

5. Wählen Sie unter Modus der Tresorsperre aus, in welchem Modus Ihr Tresor gesperrt werden soll. Weitere Informationen zur Auswahl Ihrer Modi finden Sie unter Modi der Tresorsperre weiter oben auf dieser Seite.
6. Wählen Sie für den Aufbewahrungszeitraum die Mindest- und Höchstdauer aus (Aufbewahrungszeiträume sind optional). Neue, im Tresor erstellte Backup- und Kopieraufträge schlagen fehl, wenn sie nicht den von Ihnen festgelegten Aufbewahrungszeiträumen entsprechen. Diese Zeiträume gelten nicht für Wiederherstellungspunkte, die sich bereits im Tresor befinden.
7. Wenn Sie den Compliance-Modus gewählt haben, wird ein Abschnitt mit der Bezeichnung Startdatum der Tresorverriegelung angezeigt. Wenn Sie den Governance-Modus gewählt haben, wird dieser Abschnitt nicht angezeigt und dieser Schritt kann übersprungen werden.

   Im Compliance-Modus gilt für eine Tresorsperre ab dem Zeitpunkt der Erstellung der Tresorsperre eine Bedenkzeit, ehe der Tresor und seine Sperre unveränderlich werden. Sie selbst entscheiden über die Dauer dieses Zeitraums (die sogenannte Kulanzzeit), sie muss jedoch mindestens 3 Tage (72 Stunden) betragen.

   > **Important**
   >
   > Sobald die Kulanzzeit abgelaufen ist, sind der Tresor und seine Sperre unveränderbar. Er kann weder von einem Benutzer, noch von AWS geändert oder gelöscht werden.

8. Wenn Sie mit den Konfigurationseinstellungen zufrieden sind, klicken Sie auf Tresorsperre erstellen.
9. Um zu bestätigen, dass Sie diese Sperre im ausgewählten Modus erstellen möchten, geben Sie `confirm` in das Textfeld ein und aktivieren Sie dann das Kontrollkästchen, um zu bestätigen, dass die Konfiguration Ihren Anforderungen entspricht.

Wenn die Schritte erfolgreich abgeschlossen wurden, erscheint oben in der Konsole ein Erfolgsbanner.

Programmgesteuertes Sperren eines Backup-Tresors

Verwenden Sie die API, um AWS Backup Vault Lock zu konfigurieren`PutBackupVaultLockConfiguration`. Die einzubeziehenden Parameter hängen davon ab, welchen Modus der Tresorsperre Sie zu verwenden beabsichtigen. Wenn Sie eine

Tresorsperre im Governance-Modus einrichten möchten, schließen Sie **`ChangeableForDays`** nicht ein. Wenn dieser Parameter enthalten ist, wird die Tresorsperre im Compliance-Modus erstellt.

Hier ist ein CLI-Beispiel für die Erstellung einer Tresorsperre im Compliance-Modus:

```
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
```

Hier ist ein CLI-Beispiel für die Erstellung einer Tresorsperre im Governance-Modus:

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

Sie können vier Optionen konfigurieren.

1. **`BackupVaultName`**

   Der Name des zu sperrenden Tresors.
2. **`ChangeableForDays`** (nur für den Compliance-Modus einzuschließen)

   Dieser Parameter weist AWS Backup an, die Tresorsperre im Compliance-Modus zu erstellen. Lassen Sie diesen Parameter weg, wenn Sie vorhaben, die Sperre im Governance-Modus zu erstellen.

   Dieser Wert wird in Tagen ausgedrückt. Er muss eine Zahl sein, die nicht kleiner als 3 und nicht größer als 36.500 ist. Andernfalls wird ein Fehler zurückgegeben.

   Von der Erstellung dieser Tresorsperre bis zum Ablauf des angegebenen Datums kann die Tresorsperre mithilfe von `DeleteBackupVaultLockConfiguration` aus dem Tresor entfernt werden. Alternativ können Sie während dieser Zeit die Konfiguration mithilfe von `PutBackupVaultLockConfiguration` ändern.

   An und nach dem von diesem Parameter festgelegten spezifischen Datum wird der Backup-Tresor unveränderlich und kann nicht geändert oder gelöscht werden.
3. **`MaxRetentionDays`** (optional)

Dies ist ein numerischer Wert, der in Tagen ausgedrückt wird. Dies ist die maximale Aufbewahrungsdauer, in der der Tresor seine Wiederherstellungspunkte beibehält.

Der von Ihnen gewählte maximale Aufbewahrungszeitraum sollte mit den Richtlinien Ihrer Organisation für die Aufbewahrung von Daten in Einklang stehen. Wenn Ihre Organisation vorschreibt, dass Daten für einen bestimmten Zeitraum aufbewahrt werden müssen, kann dieser Wert auf diesen Zeitraum (in Tagen) festgelegt werden. Beispielsweise müssen Finanz- oder Bankdaten möglicherweise 7 Jahre lang aufbewahrt werden (ca. 2 557 Tage, abhängig von Schaltjahren).

Wenn nicht angegeben, erzwingt AWS Backup Vault Lock keinen maximalen Aufbewahrungszeitraum. Falls angegeben, schlagen Backup- und Kopieraufträge in diesen Tresor mit Lebenszyklus-Aufbewahrungsfristen, die die maximale Aufbewahrungsdauer überschreiten, fehl. Wiederherstellungspunkte, die bereits vor der Erstellung der Tresorsperre im Tresor gespeichert wurden, sind nicht betroffen. Die längste maximale Aufbewahrungsdauer, die Sie angeben können, beträgt 36.500 Tage (ungefähr 100 Jahre).

4. **`MinRetentionDays`**(optional; erforderlich für CloudFormation)

   Dies ist ein numerischer Wert, der in Tagen ausgedrückt wird. Dies ist der Mindestaufbewahrungszeitraum, in dem der Tresor seine Wiederherstellungspunkte beibehält. Diese Einstellung sollte auf die Zeitdauer festgelegt werden, die in Ihrer Organisation für die Datenverwaltung erforderlich ist. Wenn beispielsweise Vorschriften oder Gesetze vorschreiben, dass Daten mindestens sieben Jahre aufbewahrt werden müssen, würde der Wert in Tagen je nach Schaltjahren etwa 2 557 betragen.

   Falls nicht angegeben, erzwingt AWS Backup Vault Lock keine Mindestaufbewahrungsdauer. Falls angegeben, schlagen Backup- und Kopieraufträge in diesen Tresor mit Lebenszyklus-Aufbewahrungsfristen, die die Mindestaufbewahrungsdauer unterschreiten, fehl. Wiederherstellungspunkte, die bereits vor AWS Backup Vault Lock im Tresor gespeichert wurden, sind davon nicht betroffen. Die kürzeste Mindestaufbewahrungsdauer, die Sie angeben können, ist 1 Tag.

Überprüfen Sie einen Backup-Tresor auf seine AWS Backup Vault Lock-Konfiguration

Sie können die Details von AWS Backup Vault Lock in einem Tresor jederzeit telefonisch über `DescribeBackupVault` unsere `ListBackupVaults` APIs überprüfen.

Um festzustellen, ob Sie eine Tresorsperre auf einen Backup-Tresor angewendet haben, rufen Sie `DescribeBackupVault` auf und überprüfen Sie die `Locked`-Eigenschaft. Wenn Sie`"Locked": true`, wie im folgenden Beispiel, AWS Backup Vault Lock auf Ihren Backup-Tresor angewendet haben.

```
{
    "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"
}
```

Die vorherige Ausgabe bestätigt die folgenden Optionen:

1. `Locked`ist ein boolescher Wert, der angibt, ob Sie AWS Backup Vault Lock auf diesen Backup-Tresor angewendet haben. `True`bedeutet, dass AWS Backup Vault Lock dazu führt, dass Lösch- oder Aktualisierungsvorgänge an den im Tresor gespeicherten Wiederherstellungspunkten fehlschlagen (unabhängig davon, ob Sie sich noch in der Bedenkzeit befinden).
2. `LockDate` benennt UTC-Datum und -Uhrzeit, zu der Ihre Bedenkzeit abläuft. Nach Ablauf dieser Zeit können Sie die Sperre für diesen Tresor nicht mehr löschen oder ändern. Verwenden Sie öffentlich verfügbare Zeitkonverter, um diese Zeichenfolge in Ihre Ortszeit zu konvertieren.

Im Fall von `"Locked":false`, wie im folgenden Beispiel, haben Sie keine Tresorsperre angewendet (oder eine vorherige wurde gelöscht).

```
{
    "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
}
```

Aufheben der Tresorsperre während der Kulanzzeit (Compliance-Modus)

Um Ihre Tresorsperre während der Kulanzzeit (die Zeit nach dem Sperren des Tresors, aber vor Ihrem`LockDate`) mithilfe der AWS Backup Konsole zu löschen,

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie in der linken Navigationsleiste unter Mein Konto auf „Backup-Tresore“ und dann auf „Backup-Tresorsperre“.
3. Klicken Sie auf Vault Lock, die Sie entfernen möchten, und dann auf Tresorsperre verwalten.
4. Klicken Sie auf Tresorsperre löschen.
5. Es erscheint ein Warnfeld, in dem Sie aufgefordert werden, Ihre Absicht, die Tresorsperre zu löschen, zu bestätigen. Geben Sie `confirm` in das Textfeld ein und klicken Sie dann auf Bestätigen.

Nachdem die Schritte erfolgreich abgeschlossen wurden, erscheint oben im Konsolenbildschirm ein Erfolgsbanner.

Verwenden Sie `DeleteBackupVaultLockConfiguration` wie in diesem CLI-Beispiel, um Ihre Tresorsperre während der Kulanzzeit mithilfe eines CLI-Befehls zu löschen:

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

AWS-Konto Schließung mit einem verschlossenen Tresor

Wenn Sie einen schließen AWS-Konto , der einen Backup-Tresor enthält, AWS und Ihr Konto für 90 Tage AWS Backup sperren, während Ihre Backups intakt sind. Wenn Sie Ihr Konto während dieser 90 Tage nicht erneut öffnen, wird der Inhalt Ihres Backup-Tresors AWS gelöscht, auch wenn AWS Backup Vault Lock aktiviert war.

Zusätzliche Sicherheitsüberlegungen

AWS Backup Vault Lock erweitert Ihren umfassenden Datenschutz um eine zusätzliche Sicherheitsebene. Vault Lock kann mit diesen weiteren Sicherheitsfunktionen kombiniert werden:

- Verschlüsselung für Ihre Wiederherstellungspunkte
- AWS Backup Zugriffsrichtlinien für Tresore und Wiederherstellungspunkte, mit denen Sie Berechtigungen auf Tresorebene gewähren oder verweigern können,
- AWS Backup bewährte Sicherheitsmethoden, einschließlich der Bibliothek mit vom Kunden verwalteten Richtlinien, mit denen Sie dem AWS unterstützten Dienst Sicherungs- und Wiederherstellungsberechtigungen gewähren oder verweigern können, und
- AWS Backup Audit Manager, mit dem Sie Konformitätsprüfungen für Ihre Backups anhand einer von Ihnen definierten Liste von Kontrollen automatisieren können.

  Sie können für die Kontrolle von Backups werden durch AWS Backup Vault Lock geschützt mit AWS Backup Audit Manager Frameworks mithilfe der AWS Backup API erstellen durchgehen, um sicherzustellen, dass Ihre vorgesehenen Ressourcen durch eine Tresorsperre geschützt sind.
- Mechanismen, die Ressourcen inaktiv machen, können sich auf die Fähigkeit auswirken, sie wiederherzustellen. Sie können in einem gesperrten Tresor zwar immer noch nicht gelöscht werden, können sich aber auch in einem anderen Status als aktiv befinden. Beispielsweise kann die Amazon Elastic Compute Cloud-Einstellung, mit der Sie ein AMI deaktivieren können, vorübergehend die Wiederherstellung von Backups von EC2-Instances blockieren. Dies wirkt sich auf alle EC2-Wiederherstellungspunkte aus, auch auf Backups, die von einer Tresorsperre oder einer gesetzlichen Sperre betroffen sind.

  Wenn ein EC2-Backup deaktiviert ist, können Sie ein deaktiviertes AMI erneut aktivieren. Sobald es wieder aktiviert ist, kann es wiederhergestellt werden. Um die AMI-Deaktivierungsfunktion zu blockieren, können Sie IAM-Richtlinien verwenden, um sie nicht zuzulassen`ec2:DisableImage`.

> **Note**
>
> AWS Backup Vault Lock ist nicht dieselbe Funktion wie Amazon S3 Glacier Vault Lock, das nur mit S3 Glacier kompatibel ist.

Löschen eines Backup-Tresors

Als Schutz vor versehentlicher oder böswilliger Massenlöschung können Sie einen Backup-Tresor in AWS Backup erst löschen, nachdem Sie alle Wiederherstellungspunkte in Ihrem Backup-Tresor (oder die Lebenszyklen Ihres Backup-Plans) gelöscht haben. Informationen zum manuellen Löschen Ihrer Wiederherstellungspunkte finden Sie unter Ressourcen bereinigen.

Wenn Sie einen Sicherungstresor löschen, aktualisieren Sie Ihre Sicherungspläne so, dass sie auf andere Sicherungstresore verweisen. Ein Sicherungsplan, der auf einen gelöschten Sicherungstresor verweist, führt dazu, dass die Erstellung einer Sicherung fehlschlägt.

> **Note**
>
> Sie können nicht zwei Backup-Tresore löschen: den AWS Backup Standard-Backup-Tresor und den automatischen Backup-Tresor von Amazon EFS.

Um einen Backup-Tresor mithilfe der AWS Backup Konsole zu löschen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie den Namen des Backup-Tresors, um dessen Detailseite zu öffnen.
4. Wählen Sie alle Backups aus, die mit dem Backup-Tresor verbunden sind, und löschen Sie sie.
5. Wählen Sie Tresor löschen. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie den Namen des Speichers ein und wählen Sie dann Backup-Tresor löschen.

Arbeiten mit Backups

Ein Backup oder Wiederherstellungspunkt steht für den Inhalt einer Ressource, etwa eines Amazon-EBS-Volumes (Amazon Elastic Block Storage) oder einer Amazon-DynamoDB-Tabelle, zu einem bestimmten Zeitpunkt. Recovery Point ist ein Begriff, der sich im Allgemeinen auf die verschiedenen Backups in AWS Diensten bezieht, wie Amazon EBS-Snapshots und DynamoDB-Backups. Die Begriffe Wiederherstellungspunkt und Backup werden gleichbedeutend verwendet.

AWS Backup speichert Wiederherstellungspunkte in Backup-Tresoren, die Sie entsprechend Ihren Geschäftsanforderungen organisieren können. So können Sie beispielsweise einen Satz von Ressourcen speichern, die finanzielle Informationen für das Geschäftsjahr 2020 enthalten. Wenn Sie eine Ressource wiederherstellen müssen, können Sie entweder die AWS Backup Konsole oder die AWS Command Line Interface (AWS CLI) verwenden, um die benötigte Ressource zu finden und wiederherzustellen.

Jeder Wiederherstellungspunkt hat eine eindeutige ID. Die eindeutige ID steht am Ende des Amazon-Ressourcennamens (ARN) des Wiederherstellungspunkts. Beispiele für ARNs und eindeutige IDs von Wiederherstellungspunkten finden Sie in der Tabelle in Ressourcen und Operationen.

> **Important**
>
> Um zusätzliche Gebühren zu vermeiden, sollten Sie Ihre Aufbewahrungsrichtlinie mit einer Speicherdauer von mindestens einer Woche für häufig abgerufene Daten konfigurieren. Weitere Informationen finden Sie unter Messung, Kosten und Abrechnung.

In den folgenden Abschnitten finden Sie eine Übersicht über die grundlegenden Aufgaben für die Backup-Verwaltung in AWS Backup.

Themen

- Erstellen eines Backups
- Kopieren eines Backups
- Löschen eines Backups
- Bearbeiten eines Backups
- Wiederherstellen eines Backups
- Wiederherstellungstests

- Anzeigen einer Liste von Backups

Erstellen eines Backups

Mit AWS Backup können Sie Backups automatisch mithilfe von Backup-Plänen oder manuell erstellen, indem Sie ein On-Demand-Backup initiieren.

Erstellen automatischer Backups

Wenn Backups automatisch durch Backup-Pläne erstellt werden, werden sie mit den Lebenszykluseinstellungen konfiguriert, die Sie in dem Backup-Plan eingestellt haben. Sie sind in dem Backup-Tresor organisiert, der im Backup-Plan angegeben ist. Ihnen werden dazu auch die Tags zugewiesen, die im Backup-Plan aufgeführt sind. Weitere Informationen zu Backup-Plänen finden Sie unter Verwalten von Backups mithilfe von Backup-Plänen.

Erstellen eines On-Demand-Backups

Wenn Sie ein On-Demand-Backup erstellen, können Sie diese Einstellungen für das zu erstellende Backup konfigurieren. Wenn ein Backup automatisch oder manuell erstellt wird, wird ein Backup-Auftrag initiiert. Weitere Informationen zum Erstellen eines On-Demand-Backups erhalten Sie unter Erstellen eines On-Demand-Backups mit AWS Backup.

Hinweis: Bei einem On-Demand-Backup wird ein Backup-Auftrag erstellt. Der Backup-Auftrag wird innerhalb einer Stunde (oder zum angegebenen Zeitpunkt) in den `Running`-Status überführt. Sie können ein On-Demand-Backup wählen, wenn Sie ein Backup zu einem anderen als dem im Backup-Plan festgelegten Zeitpunkt erstellen möchten. Ein On-Demand-Backup kann beispielsweise verwendet werden, um das Backup und die Funktionalität jederzeit zu testen.

On-Demand-Backups können nicht zusammen mit point-in-time Restore (PITR) verwendet werden, da bei einem On-Demand-Backup Ressourcen in dem Zustand erhalten bleiben, in dem sie sich zum Zeitpunkt der Sicherung befinden, wohingegen PITR kontinuierliche Backups verwendet, bei denen Änderungen über einen bestimmten Zeitraum aufgezeichnet werden.

Status von Backup-Aufträgen

Jeder Backup-Auftrag hat eine eindeutige ID. Zum Beispiel: `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Sie können den Status eines Backup-Auftrags auf der Seite Aufträge der AWS Backup -Konsole anzeigen. Zu den Status von Backup-Jobs gehören `CREATED` `PENDINGRUNNING`,`ABORTING`,`ABORTED`,,`COMPLETED`, `FAILEDEXPIRED`, und`PARTIAL`.

Funktionsweise von inkrementellen Backups

Viele Ressourcen unterstützen inkrementelles Backup mit. AWS Backup Eine vollständige Liste ist im Abschnitt inkrementelle Backups der Verfügbarkeit von Features nach Ressource Tabelle verfügbar.

Obwohl jedes Backup nach dem ersten inkrementell ist (d. h. es werden nur Änderungen aus dem vorherigen Backup erfasst), AWS Backup behalten alle Backups, die mit erstellt wurden, die erforderlichen Referenzdaten, um eine vollständige Wiederherstellung zu ermöglichen. Dies gilt auch dann, wenn das ursprüngliche (vollständige) Backup das Ende seines Lebenszyklus erreicht hat und gelöscht wurde.

Wenn beispielsweise Ihr (vollständiges) Backup am ersten Tag aufgrund einer 3-Tage-Lebenszyklusrichtlinie gelöscht wurde, können Sie immer noch eine vollständige Wiederherstellung mit den Backups der Tage 2 und 3 durchführen. AWS Backup behält dafür die erforderlichen Referenzdaten vom ersten Tag an bei.

Zugriff auf Quellressourcen

AWS Backup benötigt Zugriff auf Ihre Quellressourcen, um sie zu sichern. Beispielsweise:

- Um eine Amazon-EC2-Instance zu sichern, kann sich die Instance im `running`- oder `stopped`-Status, aber nicht im `terminated`-Status befinden. Das liegt daran, dass eine `running` `stopped` Oder-Instanz mit kommunizieren kann AWS Backup, eine `terminated` Instanz jedoch nicht.
- Um eine virtuelle Maschine zu sichern, muss ihr Hypervisor den Backup-Gateway-Status `ONLINE` haben. Weitere Informationen finden Sie im Abschnitt zum Verstehen von Hypervisor-Status.
- Um eine Amazon-RDS-Datenbank, ein Amazon-Aurora- oder Amazon-DocumentDB-Cluster zu sichern, müssen diese Ressourcen den Status `AVAILABLE` haben.
- Um ein Amazon Elastic File System (Amazon EFS) zu sichern, muss die Ressource den Status `AVAILABLE` haben.
- Um ein Amazon-FSx-Dateisystem zu sichern, muss sie den Status `AVAILABLE` haben. Wenn der Status `UPDATING` lautet, wird die Backup-Anfrage in die Warteschlange gestellt, bis das Dateisystem `AVAILABLE` anzeigt.

FSx für ONTAP unterstützt das Backup von bestimmten Volume-Typen nicht, darunter DP-Volumes (Datenschutz), LS-Volumes (Load-Sharing), FlexGroup-Volumes, vollständige Volumes oder Volumes auf Dateisystemen, die voll sind. Weitere Informationen finden Sie unter Arbeiten mit FSx-für-ONTAP-Backups.

AWS Backup bewahrt zuvor erstellte Backups im Einklang mit Ihrer Lebenszyklusrichtlinie auf, unabhängig vom Zustand Ihrer Quellressource.

Themen

Erstellen eines On-Demand-Backups mit AWS Backup

In der AWS Backup Konsole werden auf der Seite Geschützte Ressourcen Ressourcen aufgeführt, von denen AWS Backup mindestens einmal ein Backup erstellt wurde. Wenn Sie es AWS Backup zum ersten Mal verwenden, sind auf dieser Seite keine Ressourcen (wie Amazon EBS-Volumes oder Amazon RDS-Datenbanken) aufgeführt. Dies gilt auch, wenn eine Ressource einem Backup-Plan zugewiesen wurde und der Backup-Plan noch nicht mindestens einmal einen geplanten Backup-Auftrag durchgeführt hat.

Hinweis: Bei einem On-Demand-Backup werden Ihre Ressourcen sofort gesichert. Sie können ein On-Demand-Backup wählen, wenn Sie ein Backup zu einem anderen als dem im Backup-Plan festgelegten Zeitpunkt erstellen möchten. Ein On-Demand-Backup kann beispielsweise verwendet werden, um das Backup und die Funktionalität jederzeit zu testen.

On-Demand-Backups können nicht zusammen mit point-in-time Restore (PITR) verwendet werden, da bei einem On-Demand-Backup Ressourcen in dem Zustand erhalten bleiben, in dem sie sich zum Zeitpunkt der Sicherung befinden, wohingegen PITR kontinuierliche Backups verwendet, bei denen Änderungen über einen bestimmten Zeitraum aufgezeichnet werden.

Überlegungen

- Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine für Sie mit den richtigen Berechtigungen erstellt.
- Wenn Backups ablaufen und im Rahmen der Lebenszyklusrichtlinie zum Löschen markiert sind, löscht AWS Backup die Backups zu einem zufällig ausgewählten Zeitpunkt innerhalb der darauffolgenden 8 Stunden. Dieses Zeitfenster trägt dazu bei, eine gleichbleibende Leistung zu ermöglichen.
- Kopiert bei Amazon EC2 EC2-Ressourcen AWS Backup automatisch bestehende Gruppen- und einzelne Ressourcen-Tags sowie alle Tags, die Sie in diesem Schritt hinzufügen.
- AWS Backup verwendet EC2-Backups mit „Kein Neustart“ als Standardverhalten. AWS Backup unterstützt derzeit Ressourcen, die auf Amazon EC2 ausgeführt werden, und bestimmte Instance-Typen werden nicht unterstützt. Weitere Informationen finden Sie unter Erstellen von Windows-VSS-Backups.

So erstellen Sie ein On-Demand-Backup:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Dashboard die Option On-Demand-Backup erstellen aus. Alternativ wählen Sie im Navigationsbereich Geschützte Ressourcen und dann On-Demand-Backup erstellen aus.
3. Wählen Sie auf der Seite Ressourcentyp den Ressourcentyp aus, den Sie sichern möchten. Wählen Sie beispielsweise DynamoDB für Amazon DynamoDB-Tabellen.
4. Wählen Sie den Namen oder die ID der zu schützenden Ressource. Wählen Sie beispielsweise den Namen der DynamoDB-Tabelle für Amazon DynamoDB.
5. Stellen Sie sicher, dass Jetzt Backup erstellen ausgewählt ist.

6. Wenn der Ressourcentyp den Übergang zu Cold Storage unterstützt, ist Cold Storage vorhanden. Weitere Informationen finden Sie in der Spalte Lebenszyklus bis zum Kühlhaus in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen.

   Um anzugeben, wann diese Sicherung in den kalten Speicher verschoben wird, wählen Sie Backups vom warmen in den kalten Speicher verschieben und geben Sie dann die Zeit im warmen Speicher an.
7. Geben Sie unter Gesamter Aufbewahrungszeitraum die Anzahl der Tage an. Wenn Sie eine Kühlzeit angegeben haben, wird die Aufbewahrungszeit zwischen Warm- und Kaltlagerung aufgeteilt.
8. Wählen Sie einen vorhandenen Backup-Tresor aus oder erzeugen Sie einen neuen. Bei Auswahl von Neuen Backup-Tresor erstellen wird eine neue Seite für die Erstellung des Tresors geöffnet. Anschließend kehren Sie zur Seite On-Demand-Backup erstellen zurück.
9. Wählen Sie für die IAM-Rolle die Standardrolle oder eine von Ihnen erstellte Rolle aus.
10. Um Ihrem On-Demand-Backup ein Tag zuzuweisen, erweitern Sie den Bereich Zu Wiederherstellungspunkten hinzugefügte Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tagschlüssel und einen Tagwert ein.
11. Wenn der Ressourcentyp EC2 ist, ist die Option Erweiterte Backup-Einstellungen vorhanden. Um mithilfe des Windows Volume Shadow Copy Service (VSS) anwendungskonsistente Snapshots zu erstellen, wählen Sie Windows VSS.
12. Wählen Sie On-Demand-Backup erstellen. Dadurch wird die Seite Jobs geöffnet, auf der Sie eine Liste der Jobs und den Auftragsstatus sehen können.

Kontinuierliche Backups und point-in-time Wiederherstellung (PITR)

Themen

- Überlegungen zur PC-Wiederherstellung oint-in-time

AWS Backup Unterstützt bei einigen Ressourcen zusätzlich zu Snapshot-Backups auch kontinuierliche Backups und point-in-time Recovery (PITR).

Mit kontinuierlichen Backups können Sie Ihre AWS Backup unterstützte Ressource wiederherstellen, indem Sie sie innerhalb von 1 Sekunde genau auf einen bestimmten Zeitpunkt zurückdrehen (maximal 35 Tage). Bei kontinuierlichen Backups wird zunächst ein vollständiges Backup Ihrer Ressource erstellt und anschließend die Transaktionsprotokolle Ihrer Ressource kontinuierlich gesichert. Bei der PITR-Wiederherstellung wird auf Ihr vollständiges Backup zugegriffen und das Transaktionsprotokoll bis zu dem Zeitpunkt wiedergegeben, zu dem Sie es für die Wiederherstellung angegeben haben. AWS Backup

Alternativ können stündlich Snapshot-Backups erstellt werden. Snapshot-Backups können bis zu einem Maximum von 100 Jahren gespeichert werden. Snapshots können für vollständige oder inkrementelle Backups kopiert werden.

Da kontinuierliche Backups und Snapshot-Backups unterschiedliche Vorteile bieten, empfehlen wir Ihnen, Ihre Ressourcen sowohl mit Regeln für kontinuierliche Backups als auch mit Snapshot-Backups zu schützen.

Hinweis: Bei einem On-Demand-Backup werden Ihre Ressourcen sofort gesichert. Sie können ein On-Demand-Backup wählen, wenn Sie ein Backup zu einem anderen als dem im Backup-Plan festgelegten Zeitpunkt erstellen möchten. Ein On-Demand-Backup kann beispielsweise verwendet werden, um das Backup und die Funktionalität jederzeit zu testen.

On-Demand-Backups können nicht zusammen mit point-in-time Restore (PITR) verwendet werden, da bei einem On-Demand-Backup Ressourcen in dem Zustand erhalten bleiben, in dem sie sich zum Zeitpunkt der Sicherung befinden, wohingegen PITR kontinuierliche Backups verwendet, bei denen Änderungen über einen bestimmten Zeitraum aufgezeichnet werden.

Sie können sich für kontinuierliche Backups für unterstützte Ressourcen entscheiden, wenn Sie AWS Backup mithilfe der AWS Backup Konsole oder der API einen Backup-Plan erstellen.

Aktivieren des kontinuierlichen Backups mithilfe der Konsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie im Hauptnavigationsbereich auf Backup-Pläne und auf Backup-Plan erstellen.

3. Wählen Sie unter Backup-Regeln die Option Backup-Regel hinzufügen aus.
4. Wählen Sie im Abschnitt Konfiguration der Backup-Regeln die Option Fortlaufende Backups aktivieren für unterstützte Ressourcen aus.

Unterstützte Dienste für kontinuierliches Backup und Point-in-Time-Wiederherstellung (PITR)

AWS Backup unterstützt kontinuierliche Backups und point-in-time Wiederherstellungen für die folgenden Dienste und Anwendungen:

Amazon S3

Um PITR für S3-Backups zu aktivieren, müssen kontinuierliche Backups Teil des Backup-Plans sein.

Bei diesem ursprünglichen Backup des Quell-Buckets kann PITR zwar aktiv sein, aber für regionsübergreifende oder kontoübergreifende Zielkopien wird kein PITR verwendet, und bei der Wiederherstellung aus diesen Kopien wird der Zeitpunkt wiederhergestellt, zu dem sie erstellt wurden (die Kopien sind Snapshot-Kopien), anstatt sie zu einem festgelegten Zeitpunkt wiederherzustellen.

RDS

Backup-Zeitpläne: Wenn ein AWS Backup Plan sowohl Amazon RDS-Snapshots als auch kontinuierliche Backups erstellt, AWS Backup werden Ihre Backup-Fenster intelligent so geplant, dass sie mit dem Amazon RDS-Wartungsfenster koordiniert werden, um Konflikte zu vermeiden. Um Konflikte weiter zu vermeiden, ist die manuelle Konfiguration des automatischen Backupfensters von Amazon RDS nicht verfügbar. RDS erstellt Snapshots einmal täglich, unabhängig davon, ob ein Backup-Plan eine andere Häufigkeit für Snapshot-Backups als einmal pro Tag vorsieht.

Einstellungen: Nachdem Sie eine Regel für AWS Backup kontinuierliches Backup auf eine Amazon RDS-Instance angewendet haben, können Sie in Amazon RDS keine Einstellungen für kontinuierliche Backups für diese Instance erstellen oder ändern. Änderungen müssen über die AWS Backup Konsole oder die AWS Backup CLI vorgenommen werden.

Steuerung des kontinuierlichen Backups für eine Amazon RDS-Instance zurück zu Amazon RDS:

Console

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.

3. Löschen Sie alle Amazon-RDS-Backup-Pläne mit kontinuierlichem Backup, um diese Ressource zu schützen.
4. Wählen Sie Backup vaults (Sicherungstresore) aus. Löschen Sie den Wiederherstellungspunkt des kontinuierlichen Backups aus Ihrem Backup-Tresor. Oder warten Sie, bis die Aufbewahrungsfrist abgelaufen ist, wodurch AWS Backup der Wiederherstellungspunkt automatisch gelöscht wird.

Nachdem Sie diese Schritte abgeschlossen haben, AWS Backup wird die kontinuierliche Backup-Kontrolle Ihrer Ressource wieder auf Amazon RDS übertragen.

AWS CLI

Rufen Sie den `DisassociateRecoveryPoint`-API-Vorgang auf.

Weitere Informationen hierzu finden Sie unter DisassociateRecoveryPoint.

Erforderliche IAM-Berechtigungen für kontinuierliche Amazon RDS-Backups

- Um kontinuierliche Backups für Ihre Amazon RDS-Datenbank AWS Backup zu konfigurieren, stellen Sie sicher, dass die API-Berechtigung in der IAM-Rolle `rds:ModifyDBInstance` vorhanden ist, die in Ihrer Backup-Plan-Konfiguration definiert ist. Um kontinuierliche Amazon-RDS-Backups wiederherzustellen, müssen Sie die Berechtigung `rds:RestoreDBInstanceToPointInTime` zu der IAM-Rolle hinzufügen, die Sie für den Wiederherstellungsauftrag eingereicht haben. Sie können die `AWS Backup default service role` verwenden, um Backups und Wiederherstellungen durchzuführen.
- AWS Backup Rufen `rds:DescribeDBInstanceAutomatedBackupsAPI` Sie auf, um den Zeitraum zu beschreiben, der für die point-in-time Wiederherstellung zur Verfügung steht. In der AWS Backup Konsole müssen Sie in Ihrer AWS Identity and Access Management (IAM) verwalteten Richtlinie über die `rds:DescribeDBInstanceAutomatedBackups` API-Berechtigung verfügen. Sie können die von `AWSBackupFullAccess` oder `AWSBackupOperatorAccess` verwalteten Richtlinien verwenden. Beide Richtlinien verfügen über alle erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Verwaltete Richtlinien.

Aufbewahrungsfristen: Wenn Sie Ihre PITR-Aufbewahrungsfrist ändern, wird diese Änderung `ModifyDBInstance` sofort AWS Backup aufgerufen und angewendet. Wenn im nächsten Wartungsfenster noch weitere Konfigurationsupdates anstehen, werden bei einer Änderung der PITR-Aufbewahrungsfrist auch diese Konfigurationsupdates sofort angewendet. Weitere

Informationen finden Sie unter `ModifyDBInstance` in der API-Referenz zum Amazon Relational Database Service.

Kopien von kontinuierlichen Amazon RDS-Backups:

- Inkrementelle Snapshot-Kopieraufträge werden schneller verarbeitet als vollständige Snapshot-Kopieraufträge. Wenn Sie eine vorherige Snapshot-Kopie behalten, bis der neue Kopierauftrag abgeschlossen ist, kann sich die Dauer des Kopierauftrags verringern. Wenn Sie sich dafür entscheiden, Snapshots von RDS-Datenbank-Instances zu kopieren, ist es wichtig zu beachten, dass durch das vorherige Löschen früherer Kopien vollständige Snapshot-Kopien (statt inkrementeller) erstellt werden. Weitere Informationen zur Optimierung des Kopierens finden Sie unter Inkrementelles Kopieren von Snapshots im Amazon-RDS-Benutzerhandbuch
- Erstellen von Kopien kontinuierlicher Amazon RDS-Backups — Sie können keine Kopien von kontinuierlichen Amazon RDS-Backups erstellen, da AWS Backup Amazon RDS das Kopieren von Transaktionsprotokollen nicht zulässt. AWS Backup Erstellt stattdessen einen Snapshot und kopiert ihn mit der im Backup-Plan angegebenen Häufigkeit.

Wiederherstellungen: Sie können eine point-in-time Wiederherstellung entweder mit Amazon RDS AWS Backup oder mit Amazon RDS durchführen. Anweisungen für die AWS Backup Konsole finden Sie unter Wiederherstellen einer Amazon RDS-Datenbank. Anweisungen zu Amazon RDS finden Sie unter Wiederherstellen einer DB-Instance zu einer bestimmten Zeit im Amazon-RDS-Benutzerhandbuch.

> **Tip**
>
> Bei einer Multi-AZ-Datenbank-Instance (Availability Zone), die auf eingestellt ist, `Always On` sollte die Backup-Aufbewahrung nicht auf Null gesetzt sein. Wenn Fehler auftreten, verwenden Sie `disassociate-recovery-point` stattdessen AWS CLI command `delete-recovery-point` und ändern Sie dann die Aufbewahrungseinstellung in Ihren Amazon RDS-Einstellungen auf 1.

Weitere Informationen zum Arbeiten mit Amazon RDS finden Sie im Amazon-RDS-Benutzerhandbuch.

Aurora

Um ein kontinuierliches Backup Ihrer Aurora-Ressourcen zu aktivieren, folgen Sie den Schritten im ersten Abschnitt dieser Seite.

Das Verfahren zur Wiederherstellung eines Aurora-Clusters auf einen bestimmten Zeitpunkt ist eine Variante der Schritte zur Wiederherstellung eines Snapshots eines Aurora-Clusters.

Wenn Sie eine zeitpunktbezogene Wiederherstellung durchführen, zeigt die Konsole einen Abschnitt mit der Wiederherstellungszeit an. Weitere Informationen finden Sie unter Wiederherstellen eines kontinuierlichen Backups weiter unten auf dieser Seite unter Arbeiten mit kontinuierlichen Backups.

SAP HANA auf Amazon-EC2-Instances

Sie können kontinuierliche Backups erstellen, die zusammen mit point-in-time Restore (PITR) verwendet werden können (beachten Sie, dass bei On-Demand-Backups Ressourcen in dem Zustand erhalten bleiben, in dem sie erstellt wurden; PITR hingegen verwendet kontinuierliche Backups, die Änderungen über einen bestimmten Zeitraum aufzeichnen).

Mit kontinuierlichen Backups können Sie Ihre SAP-HANA-Datenbank auf einer EC2-Instance bis zu einem bestimmten, von Ihnen gewählten, Zeitpunkt zurückspulen, bis auf 1 Sekunde genau (innerhalb der letzten 35 Tage). Bei kontinuierlichen Backups wird zunächst ein vollständiges Backup Ihrer Ressource erstellt und anschließend die Transaktionsprotokolle Ihrer Ressource kontinuierlich gesichert. Bei der PITR-Wiederherstellung wird auf Ihr vollständiges Backup zugegriffen und das Transaktionsprotokoll bis zu dem Zeitpunkt wiedergegeben, zu dem Sie für die Wiederherstellung angegeben haben. AWS Backup

Sie können sich für kontinuierliche Backups entscheiden, wenn Sie AWS Backup mithilfe der AWS Backup Konsole oder der API einen Backup-Plan erstellen.

Aktivieren des kontinuierlichen Backups mithilfe der Konsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie im Hauptnavigationsbereich auf Backup-Pläne und auf Backup-Plan erstellen.
3. Wählen Sie unter Backup-Regeln die Option Backup-Regel hinzufügen aus.
4. Wählen Sie im Abschnitt Konfiguration der Backup-Regeln die Option Fortlaufende Backups aktivieren für unterstützte Ressourcen aus.

Nachdem Sie PITR (point-in-timeWiederherstellung) für SAP HANA-Datenbanksicherungen deaktiviert haben, werden weiterhin Protokolle an gesendet, AWS Backup bis der Wiederherstellungspunkt abläuft (Status entsprichtEXPIRED). Um die Übertragung der Protokolle an AWS Backup zu beenden, können Sie in SAP HANA einen alternativen Protokoll-Backup-Speicherort festlegen.

Ein kontinuierlicher Wiederherstellungspunkt mit dem Status von STOPPED gibt an, dass ein kontinuierlicher Wiederherstellungspunkt unterbrochen wurde. Das heißt, die von SAP HANA an diese übermittelten Protokolle, die zeigen, AWS Backup dass die inkrementellen Änderungen an einer Datenbank zeigen, eine Lücke aufweisen. Die Wiederherstellungspunkte, die innerhalb dieser Zeitrahmenlücke auftreten, haben den Status STOPPED..

Informationen zu Problemen, die bei der Wiederherstellung kontinuierlicher Backups (Wiederherstellungspunkte) auftreten können, finden Sie im Abschnitt zur Problembehebung bei der Wiederherstellung von SAP HANA in diesem Handbuch.

Finden eines kontinuierlichen Backups

Sie können die AWS Backup Konsole verwenden, um Ihr kontinuierliches Backup zu finden.

So finden Sie mithilfe der AWS Backup Konsole ein kontinuierliches Backup

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Tresore und wählen Sie dann Ihren Backup-Tresor in der Liste aus.
3. Sortieren Sie im Abschnitt Backups in der Spalte Backup-Typ nach der Einstellung Kontinuierlich für Wiederherstellungspunkte. Sie können auch nach der Wiederherstellungspunkt-ID für das Präfix Kontinuierlich sortieren.

Wiederherstellen eines kontinuierlichen Backups

Um ein kontinuierliches Backup mit der AWS Backup Konsole wiederherzustellen

- Während des PITR-Wiederherstellungsvorgangs zeigt die AWS Backup Konsole den Abschnitt Wiederherstellungszeit an. In diesem Abschnitt führen Sie folgenden Aufgaben aus:
  - Wählen Sie die Option Späteste Wiederherstellungszeit aus.
  - Wählen Sie Datum und Uhrzeit angeben, um Ihr eigenes Datum und Ihre eigene Uhrzeit innerhalb Ihres Aufbewahrungszeitraums einzugeben.

Um ein kontinuierliches Backup mithilfe der AWS Backup API wiederherzustellen

1. Informationen zu Amazon S3 finden Sie unter Verwenden der AWS Backup API, CLI oder des SDK zur Wiederherstellung von S3-Wiederherstellungspunkten.
2. Informationen zu Amazon RDS finden Sie unter Verwenden der AWS Backup API, der CLI oder des SDK zur Wiederherstellung von Amazon RDS-Wiederherstellungspunkten.

Anhalten oder Löschen kontinuierlicher Backups

Sie können die Erstellung kontinuierlicher Backups beenden oder bestimmte Backups (point-in-time-recovery oder PITR-Punkte) löschen.

Wenn Sie kontinuierliche Backups beenden möchten, müssen Sie die Regel für kontinuierliche Backups aus Ihrem Backup-Plan löschen. Wenn Sie kontinuierliche Backups für eine oder mehrere Ressourcen, aber nicht für alle Ressourcen beenden möchten, erstellen Sie einen neuen Backup-Plan mit der Regel für kontinuierliche Backups für die Ressourcen, die Sie dennoch kontinuierlich sichern möchten. Wenn Sie stattdessen nur einen kontinuierlichen Backup-Wiederherstellungspunkt aus Ihrem Backup-Tresor löschen, führt Ihr Backup-Plan weiterhin die Regel für kontinuierliches Backup aus, wodurch ein neuer Wiederherstellungspunkt erstellt wird.

Aber auch nach dem Löschen Ihrer Regel für kontinuierliche Backups AWS Backup merkt sich der Aufbewahrungszeitraum aus Ihrer jetzt gelöschten Backup-Regel. Es löscht Ihren Wiederherstellungspunkt für kontinuierliche Backups automatisch aus Ihrem Backup-Tresor, basierend auf der von Ihnen angegebenen Aufbewahrungsdauer.

Beachten Sie beim Löschen von Amazon RDS-Wiederherstellungspunkten Folgendes:

- Bei einer Multi-AZ-Datenbank-Instance (Availability Zone), die auf eingestellt ist, `Always On` sollte die Backup-Aufbewahrung nicht auf Null gesetzt sein. Wenn Fehler auftreten, verwenden Sie `disassociate-recovery-point` stattdessen AWS CLI command `delete-recovery-point` und ändern Sie dann die Aufbewahrungseinstellung in Ihren Amazon RDS-Einstellungen auf 1.
- Wenn ein point-in-time Wiederherstellungspunkt (ein durch kontinuierliches Backup erstelltes Backup) für Amazon RDS gelöscht wird, wird ein Datenbankneustart ausgelöst und die Binärprotokolle werden deaktiviert. Weitere Informationen finden Sie unter Aufbewahrungszeitraum für Backup im Amazon-RDS-Benutzerhandbuch.

Beachten Sie beim Löschen von Aurora-Wiederherstellungspunkten Folgendes:

Wenn dies für einen Amazon Aurora Aurora-Erholungspunkt ausgewählt ist, wird die Aufbewahrungsfrist auf 1 Tag AWS Backup festgelegt. Aurora-Backups können erst vollständig gelöscht werden, wenn auch der Quell-Cluster gelöscht wurde.

Kopieren kontinuierlicher Backups

Wenn in einer Regel für kontinuierliches Backup auch eine konto- oder regionsübergreifende Kopie angegeben ist, wird von AWS Backup ein Snapshot des kontinuierlichen Backups erstellt und dieser Snapshot in den Zielspeicher kopiert. Weitere Informationen zum Kopieren Ihrer Wiederherstellungspunkte zwischen Konten und Regionen finden Sie unter Kopieren eines Backups.

Kontinuierliche Backups erstellen regelmäßige Backups entsprechend der Häufigkeit, die in der Regel für den Backup-Plan im Zielkonto und/oder in der Region festgelegt ist.

AWS Backup unterstützt keine On-Demand-Kopien kontinuierlicher Backups.

Ändern Ihrer Aufbewahrungsfrist

Sie können AWS Backup damit den Aufbewahrungszeitraum für Ihre bestehende Regel für kontinuierliche Backups verlängern oder verkürzen. Der Mindestaufbewahrungszeitraum beträgt 1 Tag. Die maximale Aufbewahrungsfrist beträgt 35 Tage.

Eine Verlängerung der Aufbewahrungsfrist tritt sofort in Kraft. Wenn Sie Ihre Aufbewahrungsfrist verkürzen, AWS Backup wird gewartet, bis genügend Zeit verstrichen ist, bevor die Änderung zum Schutz vor Datenverlust angewendet wird. Wenn Sie beispielsweise Ihre Aufbewahrungsfrist von 35 auf 20 Tage verringern, AWS Backup werden weiterhin 35 Tage ununterbrochenes Backup beibehalten, bis 15 Tage vergangen sind. Dieses Design schützt Ihre Backups der letzten 15 Tage zum Zeitpunkt der Änderung.

Entfernen der einzigen Regel für kontinuierliche Backups aus einem Backup-Plan

Wenn Sie einen Backup-Plan mit einer Regel für kontinuierliches Backup erstellen und dann diese Regel entfernen, AWS Backup merkt sich die Aufbewahrungsfrist aus Ihrer jetzt gelöschten Regel. Nach Ablauf der Aufbewahrungsfrist wird der kontinuierliche Backup aus Ihrem Backup-Tresor gelöscht.

Überlappende kontinuierliche Backups auf derselben Ressource

Im Allgemeinen sollten Sie jede Ressource mit nicht mehr als einer Regel für kontinuierliche Backups schützen. Dies liegt daran, dass zusätzliche kontinuierliche Backups überflüssig sind. Wenn Sie

jedoch Ihren Backup-Bestand vergrößern, kann es vorkommen, dass sich mehrere Backup-Pläne, Regeln und Tresore auf einer einzigen Ressource überschneiden. AWS Backup behandelt diese Überschneidungen wie folgt.

Wenn Sie dieselbe Ressource in mehr als einen Backup-Plan mit einer Regel für kontinuierliches Backup aufnehmen, AWS Backup wird nur für den ersten Backup-Plan, den es bewertet, ein kontinuierliches Backup erstellt. Es erstellt Snapshot-Backups für alle anderen Backup-Pläne.

Wenn Sie mehrere Regeln für kontinuierliche Backups in einen einzigen Backup-Plan aufnehmen:

- Wenn Ihre Regeln auf denselben Backup-Tresor verweisen, wird AWS Backup nur für die Regel mit der längsten Aufbewahrungsdauer ein kontinuierliches Backup erstellt. Es missachtet alle anderen Regeln.
- Wenn Ihre Regeln auf unterschiedliche Backup-Tresore verweisen, AWS Backup lehnt der Plan als ungültig ab.

Überlegungen zur PC-Wiederherstellung oint-in-time

Beachten Sie bei der point-in-time Wiederherstellung die folgenden Überlegungen:

- Automatischer Fallback auf Snapshots – Wenn AWS Backup kein kontinuierliches Backup durchführen kann, versucht es stattdessen, ein Snapshot-Backup durchzuführen.
- Keine Unterstützung für kontinuierliche On-Demand-Backups — Kontinuierliche On-Demand-Backups werden AWS Backup nicht unterstützt, da On-Demand-Backups einen bestimmten Zeitpunkt aufzeichnen, wohingegen kontinuierliche Backups Änderungen über einen bestimmten Zeitraum aufzeichnen.
- Keine Unterstützung für den Übergang zu Cold Storage – Kontinuierliche Backups unterstützen den Übergang zu Cold Storage nicht, da für den Übergang zu Cold Storage eine Übergangszeit von mindestens 90 Tagen erforderlich ist, wohingegen kontinuierliche Backups eine maximale Aufbewahrungsdauer von 35 Tagen haben.
- Wiederherstellung der letzten Aktivitäten – Amazon-RDS-Aktivitäten ermöglichen Wiederherstellungen bis zu den letzten 5 Minuten Aktivität; Amazon S3 ermöglicht Wiederherstellungen bis zu den letzten 15 Minuten Aktivität.

Amazon-S3-Backups

AWS Backup unterstützt die zentrale Sicherung und Wiederherstellung von Anwendungen, die Daten allein oder zusammen mit anderen Datenbank-, Speicher- und AWS Rechendiensten in S3 speichern. Für S3-Backups sind viele Features verfügbar, darunter Backup Audit Manager.

Sie können eine einzige Backup-Richtlinie verwenden AWS Backup , um die Erstellung von Backups Ihrer Anwendungsdaten zentral zu automatisieren. AWS Backup organisiert automatisch Backups für verschiedene AWS Dienste und Drittanbieteranwendungen an einem zentralen, verschlüsselten Ort (einem sogenannten Backup-Tresor), sodass Sie Backups Ihrer gesamten Anwendung zentral verwalten können. Für S3 können Sie kontinuierliche Backups erstellen und Ihre in S3 gespeicherten Anwendungsdaten wiederherstellen und die Backups point-in-time mit einem einzigen Klick wiederherstellen.

Mit AWS Backup können Sie die folgenden Arten von Backups Ihrer S3-Buckets erstellen, darunter Objektdaten, Tags, Zugriffskontrolllisten (ACLs) und benutzerdefinierte Metadaten:

- Mit kontinuierlichen Backups können Sie die Wiederherstellung auf jeden beliebigen Zeitpunkt innerhalb der letzten 35 Tage vornehmen. Kontinuierliche Backups für einen S3-Bucket sollten nur in einem Backup-Plan konfiguriert werden.

  Eine Liste der unterstützten Services und Anweisungen zur Erstellung kontinuierlicher Backups mit AWS Backup finden Sie unter Zeitpunktbezogene Wiederherstellung (Point-in-Time Recovery, PITR).
- Bei regelmäßigen Backups werden Snapshots Ihrer Daten verwendet, sodass Sie Daten für die angegebene Dauer von bis zu 99 Jahren aufbewahren können. Sie können regelmäßige Backups in Intervallen wie 1 Stunde, 12 Stunden, 1 Tag, 1 Woche oder 1 Monat planen. AWS Backup erstellt regelmäßige Backups während des Backup-Fensters, das Sie in Ihrem Backup-Plan definiert haben.

  Unter Erstellen eines Backup-Plans erfahren Sie, wie Ihr Backup-Plan auf Ihre Ressourcen AWS Backup angewendet wird.

Konten- und regionsübergreifende Kopien sind für S3-Backups verfügbar, Kopien kontinuierlicher Backups verfügen jedoch nicht über point-in-time Wiederherstellungsfunktionen.

Kontinuierliche und regelmäßige Backups von S3-Buckets müssen sich beide im selben Backup-Tresor befinden.

Bei beiden Backup-Typen handelt es sich beim ersten Backup um ein vollständiges Backup, während nachfolgende Backups inkrementell auf Objektebene durchgeführt werden.

> **Note**
>
> Sie müssen die S3-Versionierung in Ihrem S3-Bucket aktivieren, um sie AWS Backup für Amazon S3 verwenden zu können. Wir haben diese Voraussetzung beibehalten, da wir in AWS die S3-Versionsverwaltung als bewährte Methode für Datenschutz empfehlen. Wir empfehlen Ihnen, einen Ablaufzeitraum für den Lebenszyklus Ihrer S3-Versionen festzulegen. Wenn Sie keinen Ablaufzeitraum für den Lebenszyklus einrichten, können sich Ihre S3-Kosten erhöhen, da alle noch nicht abgelaufenen Versionen Ihrer S3-Daten AWS Backup gesichert und gespeichert werden. Um mehr über die Einrichtung von S3-Lebenszyklusrichtlinien zu erfahren, folgen Sie den Anweisungen auf dieser Seite.

Vergleichen von S3-Backup-Typen

Ihre Backup-Strategie für S3-Ressourcen kann nur kontinuierliche Backups, nur regelmäßige Backups (Snapshot) oder eine Kombination aus beidem beinhalten. Die folgenden Informationen können Ihnen bei der Auswahl helfen, was für Ihr Unternehmen am besten geeignet ist:

Nur kontinuierliche Backups:

- Nachdem das erste vollständige Backup Ihrer vorhandenen Daten abgeschlossen ist, werden Änderungen an Ihren S3-Bucket-Daten nachverfolgt, sobald sie auftreten.
- Die nachverfolgten Änderungen ermöglichen es Ihnen, PITR (point-in-time Wiederherstellung) für die Aufbewahrungsdauer der kontinuierlichen Sicherung zu verwenden. Um einen Wiederherstellungsauftrag auszuführen, wählen Sie den Zeitpunkt aus, zu dem Sie die Wiederherstellung durchführen möchten.
- Die Aufbewahrungsdauer jedes kontinuierlichen Backups beträgt maximal 35 Tage.

Nur regelmäßige Backups (Snapshots), geplant oder auf Abruf:

- AWS Backup scannt den gesamten S3-Bucket, ruft die ACL und Tags jedes Objekts ab und initiiert eine Head-Anfrage für jedes Objekt, das im vorherigen Snapshot enthalten war, aber in dem gerade erstellten Snapshot nicht gefunden wurde.
- Das Backup ist konsistent point-in-time .

- Bei Datum und Uhrzeit der Datensicherung handelt es sich um den Zeitpunkt, zu dem die Bearbeitung des Buckets AWS Backup abgeschlossen ist, nicht um den Zeitpunkt, zu dem ein Backup-Job erstellt wurde.
- Das erste Backup eines Buckets ist ein vollständiges Backup. Jedes nachfolgende Backup ist inkrementell und stellt die Datenänderung seit dem letzten Snapshot dar.
- Der Snapshot, der durch das regelmäßige Backup erstellt wird, kann eine Aufbewahrungsdauer von bis zu 99 Jahren haben.

Kontinuierliche Backups kombiniert mit periodischen Backups oder Snapshot-Backups:

- Nachdem das erste vollständige Backup Ihrer vorhandenen Daten (jeder Bucket) abgeschlossen ist, werden Änderungen an Ihrem Bucket nachverfolgt, sobald sie auftreten.
- Sie können eine point-in-time Wiederherstellung von einem kontinuierlichen Wiederherstellungspunkt aus durchführen.
- Schnappschüsse sind point-in-time konsistent.
- Snapshots werden direkt vom Punkt der kontinuierlichen Wiederherstellung aus aufgenommen, sodass ein Bucket nicht erneut gescannt werden muss, um schnellere Prozesse zu ermöglichen.
- Snapshots und Punkte für kontinuierliche Wiederherstellung haben dieselbe Datenherkunft. Die Speicherung von Daten zwischen Snapshot-Punkten und Punkten für kontinuierliche Wiederherstellung erfolgt nicht doppelt.

Unterstützte S3-Speicherklassen

AWS Backup ermöglicht es Ihnen, Ihre in den folgenden S3-Speicherklassen gespeicherten S3-Daten zu sichern:

- S3 Standard
- S3-Standard — Seltener Zugriff (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

Backups eines Objekts der Speicherklasse S3 Intelligent-Tiering (INT) greifen auf diese Objekte zu. Dieser Zugriff veranlasst S3 Intelligent-Tiering, diese Objekte automatisch in den häufigen Zugriff zu verschieben.

Backups, die auf die Stufen „Seltener Zugriff“ zugreifen, einschließlich der Klassen S3 Standard — Seltener Zugriff (IA) und S3 One Zone — IA, fallen unter die S3-Speichergebühr „Häufiger Zugriff“ (gilt für die Tarife „Infrequent Access“ oder „Archive Instant Access“).

Mit Ausnahme von Glacier Instant Retrieval werden archivierte Speicherklassen nicht unterstützt.

Weitere Informationen zu den Speicherpreisen für Amazon S3 finden Sie unter Amazon S3 S3-Preise.

Überlegungen AWS Backup für Amazon S3

Die folgenden Punkte sollten beim Backup von S3-Ressourcen beachtet werden:

- Unterstützung für fokussierte Objektmetadaten: AWS Backup unterstützt die folgenden Metadaten: Tags, Zugriffskontrolllisten (ACLs), benutzerdefinierte Metadaten, das ursprüngliche Erstellungsdatum und die Versions-ID. Sie können auch alle gesicherten Daten und Metadaten mit Ausnahme des ursprünglichen Erstellungsdatums, der Versions-ID, der Speicherklasse und der E-Tags wiederherstellen.
- Ein S3-Objektschlüsselname kann aus den meisten UTF-8-kodierbaren Zeichenketten bestehen. Die folgenden Unicode-Zeichen sind zulässig: `#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF`.

  Objektschlüsselnamen, die Zeichen enthalten, die nicht in dieser Liste enthalten sind, können von Backups ausgeschlossen werden. Weitere Informationen finden Sie in der W3C-Spezifikation für Zeichen.
- Die Lifecycle-Management-Richtlinie AWS Backup von Cold Storage ermöglicht es Ihnen, den Zeitplan für das Ablaufen von Backups zu definieren. Derzeit wird jedoch die Umstellung von S3-Backups auf Cold Storage nicht unterstützt.
- Backups von S3-Buckets mit vielen Versionen desselben Objekts, die in derselben Sekunde erstellt wurden, werden derzeit nicht unterstützt.
- bemüht AWS Backup sich bei regelmäßigen Backups nach besten Kräften, alle Änderungen an Ihren Objektmetadaten nachzuverfolgen. Wenn Sie jedoch ein Tag oder eine ACL innerhalb einer Minute mehrmals aktualisieren, werden in AWS Backup möglicherweise nicht alle Zwischenstatus erfasst.

- AWS Backup bietet derzeit keine Unterstützung für Backups von SSE-C-verschlüsselten Objekten. AWS Backup unterstützt derzeit auch keine Backups von Bucket-Konfigurationen, einschließlich Bucket-Richtlinien, Einstellungen, Namen oder Zugriffspunkten.
- AWS Backup unterstützt derzeit keine Backups von S3 on AWS Outposts.

> **Important**
>
> Bei Konten, die Datenleseereignisse protokollieren, müssen die CloudTrail Zugriffsprotokolle für S3-Buckets mit aktivierten Protokollen in einem anderen Ziel-Bucket gespeichert werden. Wenn CloudTrail Protokolle in demselben Bucket gespeichert werden, in dem sie protokollieren, entsteht eine Endlosschleife. Diese Schleife kann zu unerwarteten und unerwünschten Gebühren führen.
> Weitere Informationen finden Sie unter Datenereignisse im CloudTrail Benutzerhandbuch.

Zeitfenster für den Abschluss des S3-Backups

Die folgende Tabelle enthält Beispiel-Buckets verschiedener Größen, um Ihnen bei der Schätzung der Abschlusszeit des ersten vollständigen Backups eines S3-Buckets behilflich zu sein. Die Backup-Zeiten variieren je nach Größe, Inhalt, Konfiguration und Einstellungen der einzelnen Buckets.

Bucket-Größe	Anzahl der Objekte	Geschätzte Zeit bis zum Abschluss des ersten Backups
425 GB (Gigabyte)	135 Mio.	31 Stunden
800 TB (Terabyte)	670 Mio.	38 Stunden
6 PB (Petabyte)	5 Milliarden	100 Stunden
370 TB (Terabyte)	7,5 Milliarden	180 Stunden

Berechtigungen und Richtlinien für Amazon-S3-Backup und -Wiederherstellung

Um S3-Ressourcen sichern, kopieren und wiederherstellen zu können, müssen Sie in Ihrer Rolle über die richtigen Richtlinien verfügen. Um diese Richtlinien hinzuzufügen, gehen Sie zu Durch AWS verwaltete Richtlinien. Fügen Sie den Rollen AWSBackupServiceRolePolicyForS3Restore, die Sie

zum Sichern AWSBackupServiceRolePolicyForS3Backupund Wiederherstellen von S3-Buckets verwenden möchten, das und hinzu.

Wenn Sie nicht über ausreichende Berechtigungen verfügen, bitten Sie den Manager des Administratorkontos (Admin) Ihres Unternehmens, die Richtlinien den vorgesehenen Rollen hinzuzufügen.

Weitere Informationen hierzu finden Sie unter Verwaltete Richtlinien und eingebundene Richtlinien im IAM-Benutzerhandbuch.

AWS Backup für S3 ist auf den Empfang von S3-Ereignissen über Amazon angewiesen EventBridge. Wenn diese Einstellung in den S3-Bucket-Benachrichtigungseinstellungen deaktiviert ist, werden fortlaufende Backups für diese Buckets gestoppt, bei denen die Einstellung deaktiviert ist. Weitere Informationen finden Sie unter Verwenden EventBridge.

Bewährte Methoden und Kostenüberlegungen für S3-Backups

Bewährte Methoden

Für Buckets mit mehr als 300 Millionen Objekten:

- Bei Buckets mit mehr als 300 Millionen Objekten kann die Backup-Rate beim ersten vollständigen Backup des Buckets bis zu 17.000 Objekte pro Sekunde erreichen (inkrementelle Backups haben eine andere Geschwindigkeit). Buckets mit weniger als 300 Millionen Objekten werden mit einer Geschwindigkeit von fast 1.000 Objekten pro Sekunde gesichert.
- Kontinuierliche Backups werden empfohlen.
- Wenn der Backup-Lebenszyklus für mehr als 35 Tage geplant ist, können Sie auch Snapshot-Backups für den Bucket in demselben Tresor aktivieren, in dem Ihre kontinuierlichen Backups gespeichert sind.

Überlegungen zu den Kosten

- S3-Lebenszyklusrichtlinien verfügen über ein optionales Feature namens Löschmarkierungen für abgelaufenes Objekt löschen. Wenn dieses Feature weggelassen wird, laufen Löschmarkierungen, manchmal in Millionenhöhe, ab, ohne dass ein Bereinigungsplan erforderlich ist. Wenn Buckets ohne dieses Feature gesichert werden, wirken sich zwei Probleme auf den Zeit- und Kostenaufwand aus:

  - Löschmarken werden genauso wie Objekte gesichert. Die Backup-Zeit und die Wiederherstellungszeit können abhängig vom Verhältnis von Objekten zu Löschmarkierungen beeinflusst werden.
  - Für jedes Objekt und jede Markierung, für die ein Backup erstellt wird, wird eine Mindestgebühr berechnet. Jeder Löschmarker wird genauso berechnet wie für ein 128-KB-Objekt.
- Für Konten, die mindestens täglich oder häufiger Backups erstellen, können Kostenvorteile durch kontinuierliche Backups erzielt werden, wenn sich die Daten in den Backups zwischen den Backups nur minimal ändern.
- Größere Buckets, die sich nicht häufig ändern, können von kontinuierlichen Backups profitieren, da dies zu niedrigeren Kosten führen kann, wenn Scans des gesamten Buckets zusammen mit mehreren Anfragen pro Objekt nicht an bereits vorhandenen Objekten (Objekten, die gegenüber dem vorherigen Backup unverändert sind) durchgeführt werden müssen.
- Buckets, die mehr als 100 Millionen Objekte enthalten und im Vergleich zur Gesamtgröße des Backups eine geringe Löschrate aufweisen, können mit einem Backup-Plan, der sowohl ein kontinuierliches Backup mit einer Aufbewahrungsdauer von 2 Tagen als auch Snapshots einer längeren Aufbewahrung beinhaltet, Kostenvorteile erzielen.
- Die regelmäßige Backup-Zeit (Snapshot) richtet sich nach dem Beginn des Backup-Vorgangs, wenn kein Bucket-Scan erforderlich ist. In einem Bucket, der sowohl kontinuierliche Backups als auch Snapshots enthält, sind keine Scans erforderlich, da in diesen Fällen Snapshots von einem kontinuierlichen Wiederherstellungspunkt stammen.
- AWS Backup Führt für jedes Objekt in einem einzelnen S3-GIR (Amazon S3 Glacier Instant Retrieval) mehrere Aufrufe durch, wodurch Abrufgebühren anfallen, wenn ein Backup durchgeführt wird.

  Ähnliche Abrufkosten fallen für Buckets mit Objekten der Speicherklassen S3-IA und S3 One Zone-IA an.
- AWS KMS CloudTrail, und CloudWatch Amazon-Funktionen, die Teil Ihrer Backup-Strategie sind, können zu zusätzlichen Kosten führen, die über den S3-Bucket-Datenspeicher hinausgehen. Weitere Informationen zum Anpassen dieser Features enthalten die folgenden Abschnitte:
  - Reduzieren der Kosten von SSE-KMS mit Amazon-S3-Bucket-Schlüsseln im Amazon-S3-Benutzerhandbuch.
  - Sie können die CloudTrail Kosten senken, indem Sie AWS KMS Ereignisse ausschließen und S3-Datenereignisse deaktivieren:
    - AWS KMS Ereignisse ausschließen: Im CloudTrail Benutzerhandbuch gibt es unter Creating a trail in der Konsole (einfache Event-Selektoren) die Option, AWS KMS Ereignisse

auszuschließen, um diese Ereignisse aus Ihrem Trail herauszufiltern (die Standardeinstellung umfasst alle KMS-Ereignisse):

- Die Option zum Protokollieren oder Ausschließen von KMS-Ereignissen ist nur verfügbar, wenn Sie Verwaltungsereignisse in Ihrem Trail protokollieren. Wenn Sie Verwaltungsereignisse nicht protokollieren möchten, werden KMS-Ereignisse nicht protokolliert und Sie können die Einstellungen für die KMS-Ereignisprotokollierung nicht ändern.
- AWS KMS Aktionen wie `EncryptDecrypt`, und erzeugen `GenerateDataKey` in der Regel eine große Menge (mehr als 99%) von Ereignissen. Diese Aktionen werden nun als Leseereignisse protokolliert. Relevante KMS-Aktionen mit geringem Volume wie `Disable`, `Delete` und `ScheduleKey` (die normalerweise weniger als 0,5 % des KMS-Ereignis-Volumes ausmachen) werden als Schreib-Ereignisse protokolliert.
- Um Ereignisse mit hohem Volume wie `Encrypt`, `Decrypt` und `GenerateDataKey` auszuschließen, aber dennoch relevante Ereignisse wie `Disable`, `Delete` und `ScheduleKey` zu protokollieren, wählen Sie Schreib-Verwaltungsereignisse protokollieren und deaktivieren Sie das Kontrollkästchen für AWS KMS -Ereignisse ausschließen.
- Deaktivieren von S3-Datenereignissen: Standardmäßig werden Datenereignisse nicht von Trails und Ereignisdatenspeichern protokolliert. Deaktivieren Sie S3-Datenereignisse vor Ihrem ersten Backup, um die Kosten zu senken.

- Um die CloudWatch Kosten zu senken, können Sie das Senden von CloudTrail Ereignissen an CloudWatch Logs beenden, wenn Sie einen Trail aktualisieren, um die CloudWatch Protokolleinstellungen zu deaktivieren.

Wiederherstellen eines S3-Backups

Sie können Ihre S3-Daten, die Sie mit AWS Backup der Klasse S3 Standard Storage gesichert haben, wiederherstellen. Sie können Ihre S3-Daten in einem vorhandenen Bucket wiederherstellen, einschließlich des ursprünglichen Buckets. Während der Wiederherstellung können Sie auch einen neuen S3-Bucket als Wiederherstellungsziel erstellen. Sie können S3-Backups nur AWS-Region dort wiederherstellen, wo sich Ihr Backup befindet.

Sie können den gesamten S3-Bucket oder Ordner oder Objekte innerhalb des Buckets wiederherstellen. AWS Backup stellt die aktuelle Version dieses Objekts wieder her.

Informationen zum Wiederherstellen Ihrer S3-Daten mit AWS Backup finden Sie unterWiederherstellen von S3-Daten.

Backups virtueller Maschinen

AWS Backup unterstützt zentralisierten und automatisierten Datenschutz für lokale virtuelle Maschinen (VMs) von VMware sowie für VMs in der VMware Cloud™ (VMC) auf AWS und VMware Cloud™ (VMC) auf. AWS Outposts Sie können Backups von Ihren lokalen und virtuellen VMC-Computern auf erstellen. AWS Backup Anschließend können Sie Daten von AWS Backup auf On-Premises-VMs, VMs in der VMC oder VMC auf AWS Outposts wiederherstellen.

AWS Backup bietet Ihnen außerdem vollständig verwaltete, AWS native VM-Backup-Managementfunktionen wie VM-Erkennung, Backup-Planung, Aufbewahrungsmanagement, eine kostengünstige Speicherstufe, regionsübergreifendes und kontoübergreifendes Kopieren, Unterstützung für AWS Backup Vault Lock und AWS Backup Audit Manager, Verschlüsselung, die unabhängig von Quelldaten ist, und Backup-Zugriffsrichtlinien. Eine vollständige Liste der Funktionen und Details finden Sie in der Verfügbarkeit von Features nach Ressource-Tabelle.

Sie können es verwenden AWS Backup , um Ihre virtuellen Maschinen auf VMware Cloud™ zu schützen. AWS Outposts AWS Backup speichert Ihre VM-Backups in AWS-Region dem Ordner, mit dem Ihre VMware Cloud™ verbunden AWS Outposts ist. Sie können AWS Backup es verwenden, um Ihre VMware Cloud™ auf AWS Backup VMs zu schützen, wenn Sie VMware Cloud™ verwenden, AWS Outposts um Ihre Anforderungen an niedrige Latenz und lokale Datenverarbeitung für Ihre Anwendungsdaten zu erfüllen. Je nach Ihren Anforderungen an die Datenresidenz können Sie sich dafür entscheiden, Backups Ihrer Anwendungsdaten in dem übergeordneten System AWS Backup AWS-Region zu speichern, mit dem Sie verbunden sind. AWS Outposts

Unterstützte VMs

AWS Backup kann virtuelle Maschinen sichern und wiederherstellen, die von einem VMware vCenter verwaltet werden.

Derzeit unterstützt:

- vSphere 8, 7.0 und 6.7
- Virtuelle Festplattengrößen, die ein Vielfaches von 1 KiB sind
- NFS-, VMFS- und VSAN-Datenspeicher vor Ort und in VMC auf AWS
- SCSI Hot-Add- und Network Block Device Secure Sockets Layer (NBDSSL) -Transportmodi zum Kopieren von Daten von Quell-VMs auf lokale VMWare AWS
- Hot-Add-Modus zum Schutz von VMs auf VMware Cloud on AWS

Derzeit nicht unterstützt:

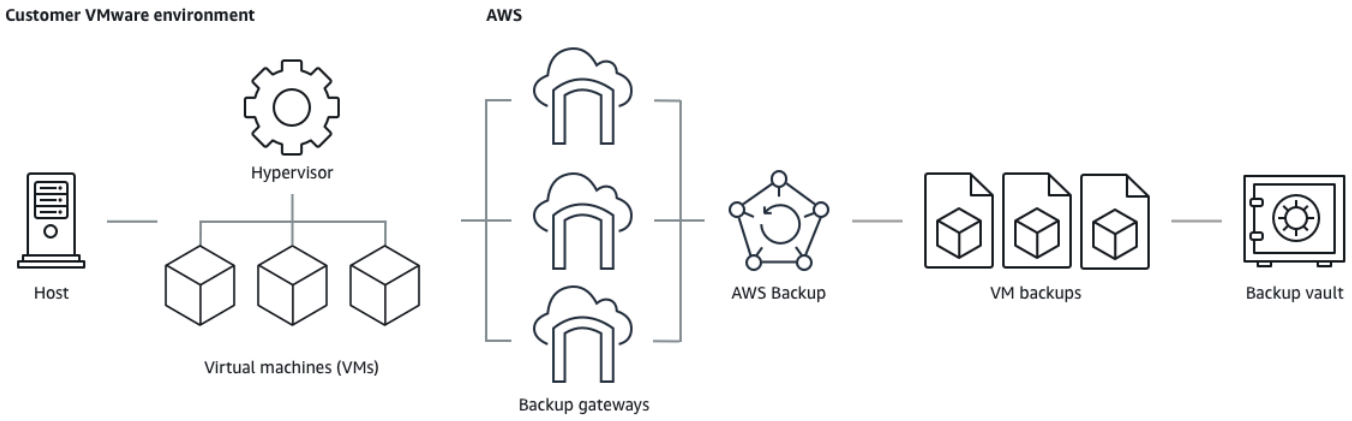
- RDM-Laufwerke (Raw Disk Mapping) oder NVMe-Controller und ihre Festplatten
- Modi für unabhängige persistente und unabhängige, nicht persistente Festplatten

Backup-Konsistenz

AWS Backup erfasst standardmäßig anwendungskonsistente Backups von VMs mithilfe der VMware-Tools-Ruheeinstellung auf der VM. Ihre Backups sind anwendungskonsistent, wenn Ihre Anwendungen mit VMware-Tools kompatibel sind. Wenn die Ruhefunktion nicht verfügbar ist, werden absturzsichere Backups erfasst. AWS Backup Stellen Sie sicher, dass Ihre Backups den Anforderungen Ihres Unternehmens entsprechen, indem Sie Ihre Wiederherstellungen testen.

Backup-Gateway

Backup Gateway ist herunterladbare AWS Backup Software, die Sie in Ihrer VMware-Infrastruktur bereitstellen, um Ihre VMware-VMs mit dieser zu AWS Backup verbinden. Das Gateway stellt eine Verbindung zu Ihrem VM-Managementserver her, um VMs zu erkennen, Ihre VMs zu erkennen, Daten zu verschlüsseln und Daten effizient an AWS Backup zu übertragen. Das folgende Diagramm zeigt, wie sich das Backup-Gateway mit Ihren VMs verbindet:



Folgen Sie dem Verfahren für Arbeiten mit Gateways, um die Backup-Gateway-Software herunterzuladen.

Informationen zu VPC-Endpunkten (Virtual Private Cloud) finden Sie unter AWS Backup und AWS PrivateLink Konnektivität.

Das Backup-Gateway verfügt über eine eigene API, die separat von der AWS Backup -API verwaltet wird. Eine Liste der Backup-Gateway-API-Aktionen finden Sie unter Backup-Gateway-Aktionen. Eine Liste der Backup-Gateway-API-Datentypen finden Sie unter Backup-Gateway-Datentypen.

Endpunkte

Bestehende Benutzer, die derzeit einen öffentlichen Endpunkt verwenden und zu einem VPC-Endpunkt (Virtual Private Cloud) wechseln möchten, können ein neues Gateway mit einem VPC-Endpunkt erstellen mithilfe von AWS PrivateLink, den vorhandenen Hypervisor dem Gateway zuordnen und dann das Gateway löschen, das den öffentlichen Endpunkt enthält.

Konfigurieren der Infrastruktur für die Verwendung des Backup-Gateways

Für das Backup Gateway sind die folgenden Netzwerk-, Firewall- und Hardwarekonfigurationen erforderlich, um Ihre virtuellen Maschinen zu sichern und wiederherzustellen.

Netzwerkkonfiguration

Ein Backup-Gateway erfordert, dass bestimmte Ports für den Betrieb zugelassen werden. Erlauben Sie die folgenden Ports:

1. TCP 443 Outbound
   - Quelle: Backup-Gateway
   - Ziel: AWS
   - Verwendung: Erlaubt dem Backup-Gateway die Kommunikation mit AWS.
2. TCP 80 Inbound
   - Quelle: Der Host, mit dem Sie eine Verbindung herstellen AWS Management Console
   - Ziel: Backup-Gateway
   - Verwendung: Durch lokale Systeme zum Abrufen des Backup-Gateway-Aktivierungsschlüssels. Port 80 wird nur während der Aktivierung des Backup-Gateways verwendet. AWS Backup erfordert nicht, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie Ihr Gateway über aktivieren, muss der Host AWS Management Console, von dem aus Sie eine Verbindung zur Konsole herstellen, Zugriff auf den Port 80 Ihres Gateways haben.
3. UDP 53 Outbound
   - Quelle: Backup-Gateway
   - Ziel: Domain Name Service-Server (DNS)

- Verwendung: Erlaubt dem Backup-Gateway die Kommunikation mit dem DNS.

4. TCP 443 Outbound
   - Quelle: Backup-Gateway
   - Ziel: AWS Support
   - Verwendung: Ermöglicht AWS Support den Zugriff auf Ihr Gateway, um Ihnen bei Problemen zu helfen. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich.
5. UDP 53 Outbound
   - Quelle: NTP-Client
   - Ziel: NTP-Server
   - Verwendung: Wird verwendet von lokalen Systemen zur Synchronisierung der VM-Zeit mit der Host-Zeit.
6. TCP 443 Outbound
   - Quelle: Backup-Gateway
   - Ziel: VMware vCenter
   - Verwendung: Erlaubt dem Backup-Gateway die Kommunikation mit VMware vCenter.
7. TCP 443 Outbound
   - Quelle: Backup-Gateway
   - Ziel: ESXi-Hosts
   - Verwendung: Erlaubt dem Backup-Gateway die Kommunikation mit ESXi-Hosts.
8. TCP 443 Outbound
   - Quelle: Backup-Gateway
   - Ziel: VMware-ESXi-Hosts
   - Verwendung: Wird für die Datenübertragung über das Backup-Gateway verwendet.

Die oben genannten Ports sind für das Backup-Gateway erforderlich. Weitere Informationen Einen AWS Backup VPC-Endpunkt erstellen zur Konfiguration von Amazon VPC-Endpunkten für finden Sie unter. AWS Backup

Firewall-Konfiguration

Das Backup-Gateway benötigt Zugriff auf die folgenden Dienstendpunkte, um mit Amazon Web Services ihnen kommunizieren zu können. Falls Sie den Netzwerkdatenverkehr mithilfe einer

Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation mit AWS verwendet werden dürfen. Die Verwendung eines HTTP-Proxys zwischen dem Backup-Gateway und den Service Points wird nicht unterstützt.

```
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
```

Konfigurieren des Gateways für mehrere NICs in VMware

Sie können separate Netzwerke für Ihren internen und externen Datenverkehr verwalten, indem Sie mehrere virtuelle Netzwerkschnittstellenverbindungen (NICs) an Ihr Gateway anschließen und dann den internen Verkehr (Gateway zum Hypervisor) und den externen Verkehr (Gateway zu) getrennt weiterleiten. AWS

Standardmäßig verfügen virtuelle Maschinen, die mit dem AWS Backup Gateway verbunden sind, über einen Netzwerkadapter (). `eth0` Dieses Netzwerk umfasst den Hypervisor, die virtuellen Maschinen und das Netzwerk-Gateway (Backup-Gateway), das mit dem breiteren Internet kommuniziert.

Hier ist ein Beispiel für ein Setup mit mehreren virtuellen Netzwerkschnittstellen:

```
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
```

- In diesem Beispiel erfolgt die Verbindung zu einem Hypervisor mit IP-`10.0.3.123`, das Gateway verwendet `eth0`, da die Hypervisor-IP Teil des `10.0.3.0/24`-Blocks ist.
- Um eine Verbindung zu einem Hypervisor mit IP-`10.0.0.234` herzustellen, verwendet das Gateway `eth1`.

- Um eine Verbindung zu einer IP außerhalb der lokalen Netzwerke herzustellen (z. B. `34.193.121.211`), greift das Gateway auf das Standard-Gateway zurück (`10.0.0.1`) das sich im `10.0.0.0/24`-Block befindet, und durchläuft somit `eth1`.

Die erste Sequenz zum Hinzufügen eines zusätzlichen Netzwerkadapters erfolgt im vSphere-Client:

1. Öffnen Sie im VMware-vSphere-Client (mit einem Rechtsklick) das Kontextmenü für Ihre Gateway-VM und wählen Sie Einstellungen bearbeiten.
2. Öffnen Sie auf der Registerkarte Virtuelle Hardware im Dialogfeld Eigenschaften der virtuellen Maschine das Menü Neues Gerät hinzufügen und wählen Sie Netzwerkadapter aus, um einen neuen Netzwerkadapter hinzuzufügen.
3.
   a. Erweitern Sie die Details für das neue Netzwerk, um den neuen Adapter zu konfigurieren.
   b. Stellen Sie sicher, dass Bei Einschalten verbinden ausgewählt ist.
   c. Informationen zum Adaptertyp finden Sie unter Netzwerkadaptertypen in der ESXi- und vCenter-Server-Dokumentation.
4. Klicken Sie auf OK, um die neuen Netzwerkadaptereinstellungen zu speichern.

Die nächste Abfolge von Schritten zur Konfiguration eines zusätzlichen Adapters erfolgt in der AWS Backup Gateway-Konsole (beachten Sie, dass dies nicht dieselbe Oberfläche ist wie die AWS Management-Konsole, auf der Backups und andere Dienste verwaltet werden).

Sobald die neue Netzwerkkarte zur Gateway-VM hinzugefügt wurde, müssen Sie:

- Zu `Command Prompt` navigieren und die neuen Adapter anschalten
- Statische IPs für jede neue Netzwerkkarte konfigurieren
- Die bevorzugte NIC als Standard festlegen

So gehen Sie vor:

1. Wählen Sie im VMware vSphere-Client Ihre virtuelle Gateway-Maschine aus und starten Sie die Webkonsole, um auf die lokale Backup-Gateway-Konsole zuzugreifen.
   - Weitere Informationen zum Zugriff auf eine lokale Konsole finden Sie im Abschnitt zum Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi.

2. Verlassen Sie die Befehlszeile, gehen Sie zu „Netzwerkkonfiguration > Statische IP konfigurieren“ und folgen Sie den Setup-Anweisungen, um die Routing-Tabelle zu aktualisieren.
   a. Weisen Sie dem Subnetz des Netzwerkadapters eine statische IP zu.
   b. Richten Sie eine Netzwerkmaske ein.
   c. Geben Sie die IP-Adresse des Standard-Gateways ein. Dies ist das Netzwerk-Gateway, das eine Verbindung zum gesamten Datenverkehr außerhalb des lokalen Netzwerks herstellt.
3. Wählen Sie Standardadapter festlegen, um den Adapter, der mit der Cloud verbunden wird, als Standardgerät festzulegen.
4. Alle IP-Adressen für das Gateway können sowohl in der lokalen Konsole als auch auf der VM-Übersichtsseite in VMware vSphere angezeigt werden.

Hardwareanforderungen

Sie müssen in der Lage sein, die folgenden Mindestressourcen auf einem VM-Host für das Backup-Gateway zu reservieren:

- 4 Virtuelle Prozessoren
- 8 GiB reserviertes RAM

VMware-Berechtigungen

In diesem Abschnitt sind die Mindestberechtigungen von VMware aufgeführt, die für die Verwendung AWS Backup gateway erforderlich sind. Diese Berechtigungen sind erforderlich, damit das Backup-Gateway virtuelle Maschinen erkennen, sichern und wiederherstellen kann.

Um das Backup-Gateway mit aktivierter VMware Cloud™ AWS oder VMware Cloud™ zu verwenden AWS Outposts, müssen Sie den Standard-Admin-Benutzer verwenden `cloudadmin@vmc.local` oder die CloudAdmin Rolle Ihrem dedizierten Benutzer zuweisen.

Um das Backup-Gateway mit lokalen virtuellen VMware-Maschinen zu verwenden, erstellen Sie einen dedizierten Benutzer mit den unten aufgeführten Berechtigungen.

Global

- Deaktivieren von Methoden
- Aktivieren von Methoden

- Lizenzen
- Protokollereignis
- Managen benutzerdefinierter Attribute
- Festlegen benutzerdefinierter Attribute

vSphere-Tagging

- Zuweisen oder Zuweisung aufheben von vSphere-Tag

DataStore

- Zuweisen von Speicherplatz
- Durchsuchen des Datenspeichers
- Konfigurieren des Datenspeichers (für vSAN-Datenspeicher)
- Dateioperationen auf niedriger Ebene
- Aktualisieren von Dateien der virtuellen Maschine

Host

- Konfiguration
  - Erweiterte Einstellungen
  - Konfiguration der Speicherpartition

Ordner

- Erstellen von Ordnern

Network (Netzwerk)

- Zuweisen eines Netzwerks

dvPort-Gruppe

- Erstellen

- Löschen

Ressource

- Zuweisen einer virtuellen Maschine zum Ressourcenpool

Virtuelle Maschine

- Ändern der Konfiguration
  - Abrufen der Festplattenversion
  - Hinzufügen bestehender Festplatten
  - Hinzufügen einer neuen Festplatte
  - Erweiterte Konfiguration
  - Ändern der -Einstellungen
  - Konfigurieren eines unformatierten Geräts
  - Überprüfen der Geräteeinstellungen
  - Entfernen der Festplatte
  - Hinzufügen von Anmerkungen
  - Ändern der Nachverfolgung von Festplattenänderungen
- Bearbeiten des Inventars
  - Erstellen aus bestehenden
  - Neu erstellen
  - Registrieren
  - Remove
  - Aufheben der Registrierung
- Interaktionen
  - Ausschalten
  - Einschalten
- Bereitstellung
  - Zulassen von Festplattenzugriff
  - Zulassen von schreibgeschütztem Festplattenzugriff
  - Ermöglichen des Herunterladens der virtuellen Maschine

- Snapshot-Management
  - Snapshot erstellen
  - Entfernen des Snapshots
  - Zurückkehren zum Snapshot

Arbeiten mit Gateways

Um Ihre virtuellen Maschinen (VMs) mithilfe von zu sichern und wiederherzustellen AWS Backup, müssen Sie zunächst ein Backup-Gateway installieren. Ein Gateway ist eine Software in Form einer OVF-Vorlage (Open Virtualization Format), die Amazon Web Services Backup mit Ihrem Hypervisor verbindet, sodass dieser Ihre virtuellen Maschinen automatisch erkennt und Sie sie sichern und wiederherstellen können.

Ein einzelnes Gateway kann bis zu 4 Backup- oder Wiederherstellungsaufträge gleichzeitig ausführen. Um mehr als 4 Aufträge gleichzeitig auszuführen, erstellen Sie mehr Gateways und ordnen Sie sie Ihrem Hypervisor zu.

Erstellen eines Gateways

So erstellen Sie ein Gateway:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Gateways aus.
3. Wählen Sie Create gateway (Gateway erstellen).
4. Folgen Sie den Anweisungen im Abschnitt Gateway einrichten diesen Anweisungen, um die OVF-Vorlage herunterzuladen und bereitzustellen.

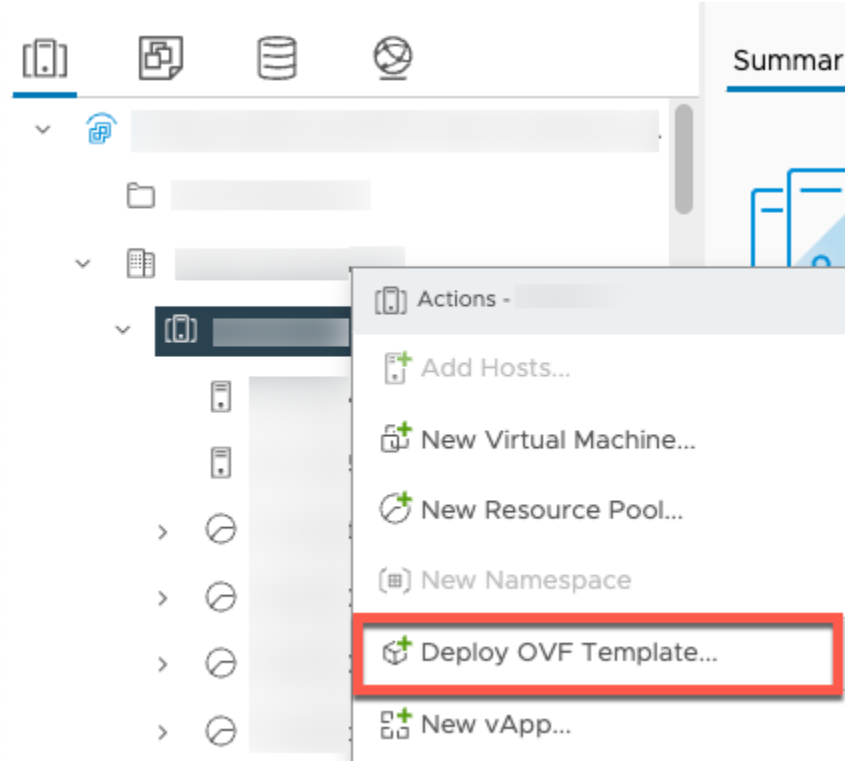
Herunterladen der VMware-Software

Verbinden des Hypervisors

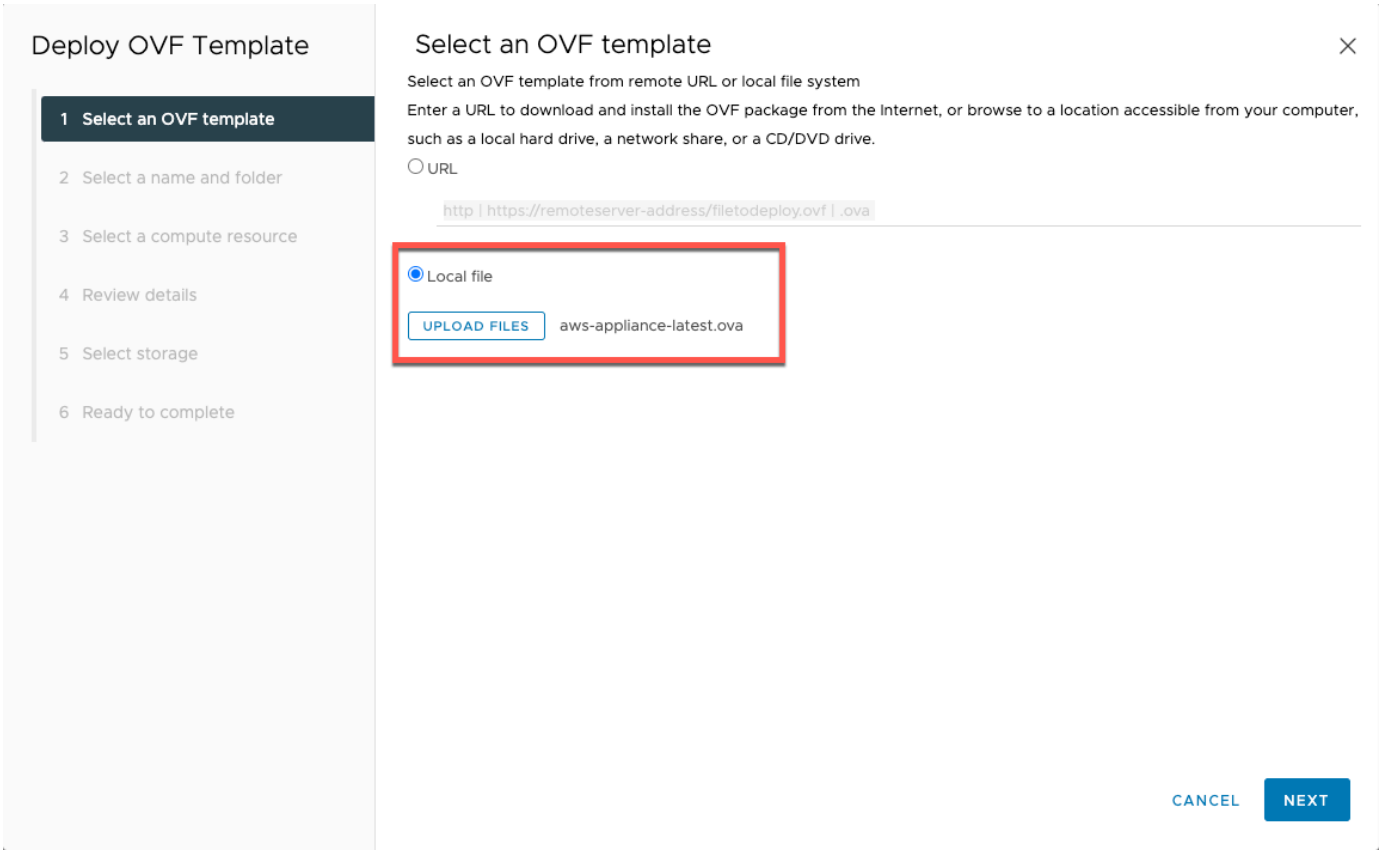
Gateways stellen eine Verbindung AWS Backup zu Ihrem Hypervisor her, sodass Sie Backups Ihrer virtuellen Maschinen erstellen und speichern können. Laden Sie die OVF-Vorlage herunter, um Ihr Gateway auf VMware ESXi einzurichten. Der Download kann ca. 10 Minuten dauern.

Wenn der Vorgang abgeschlossen ist, fahren Sie mit den folgenden Schritten fort:

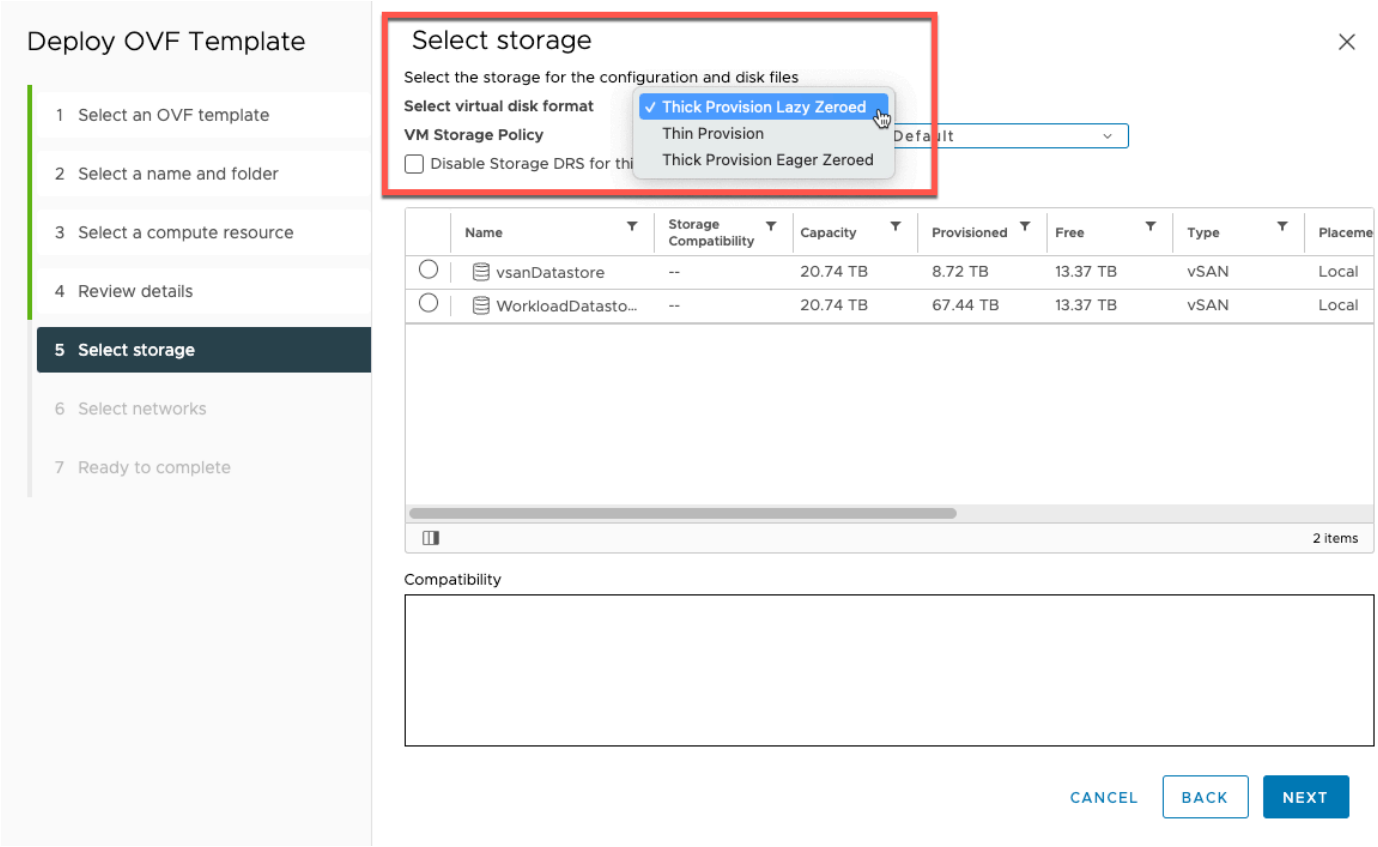
1. Stellen Sie mithilfe von VMware vSphere eine Verbindung zu Ihrem Hypervisor für virtuelle Maschinen her.
2. Klicken Sie mit der rechten Maustaste auf ein übergeordnetes Objekt einer virtuellen Maschine und wählen Sie OVF-Vorlage bereitstellen aus.



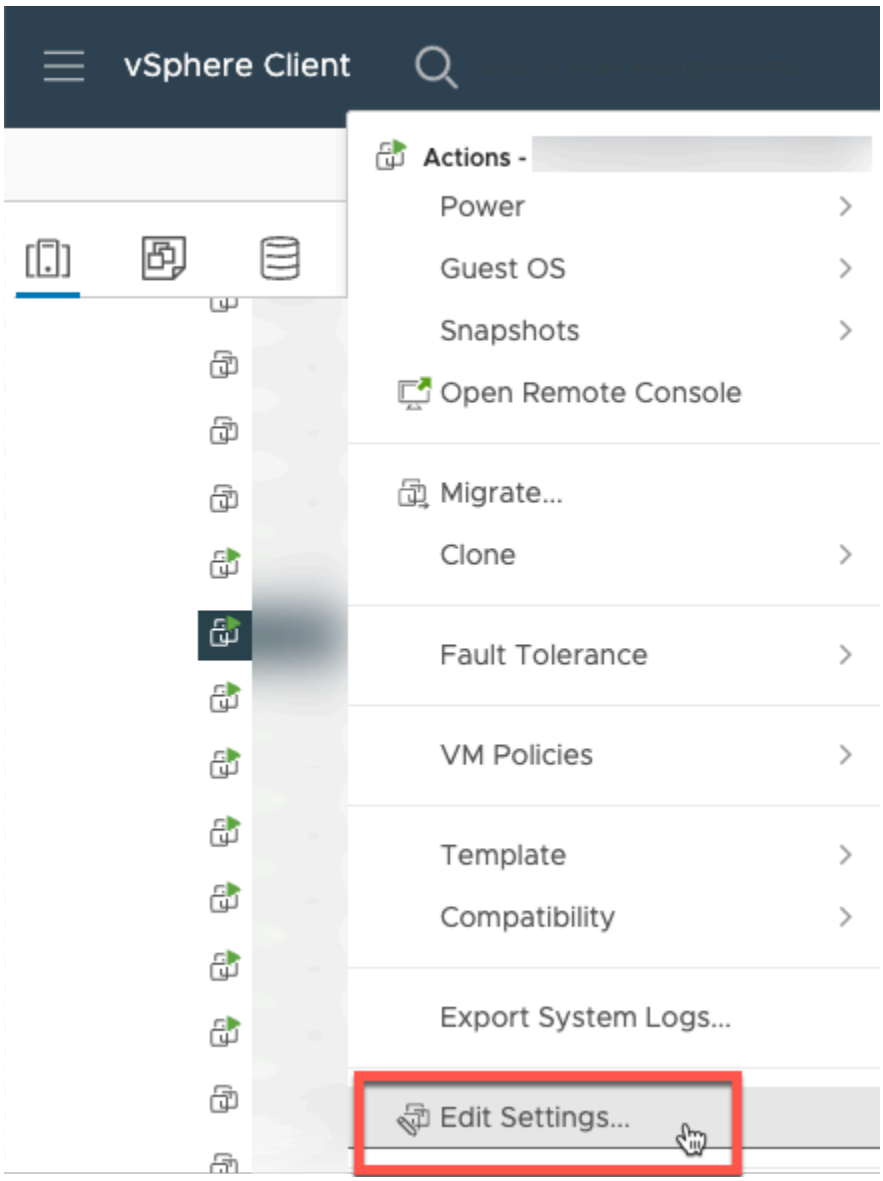
3. Wählen Sie Lokale Datei und laden Sie die heruntergeladene aws-appliance-latestOVA-Datei hoch.



4. Folgen Sie für die Bereitstellung den Anweisungen des Einrichtungsassistenten. Wählen Sie auf der Seite Speicher auswählen das virtuelle Festplattenformat Thick Provision Lazy Zeroed aus.

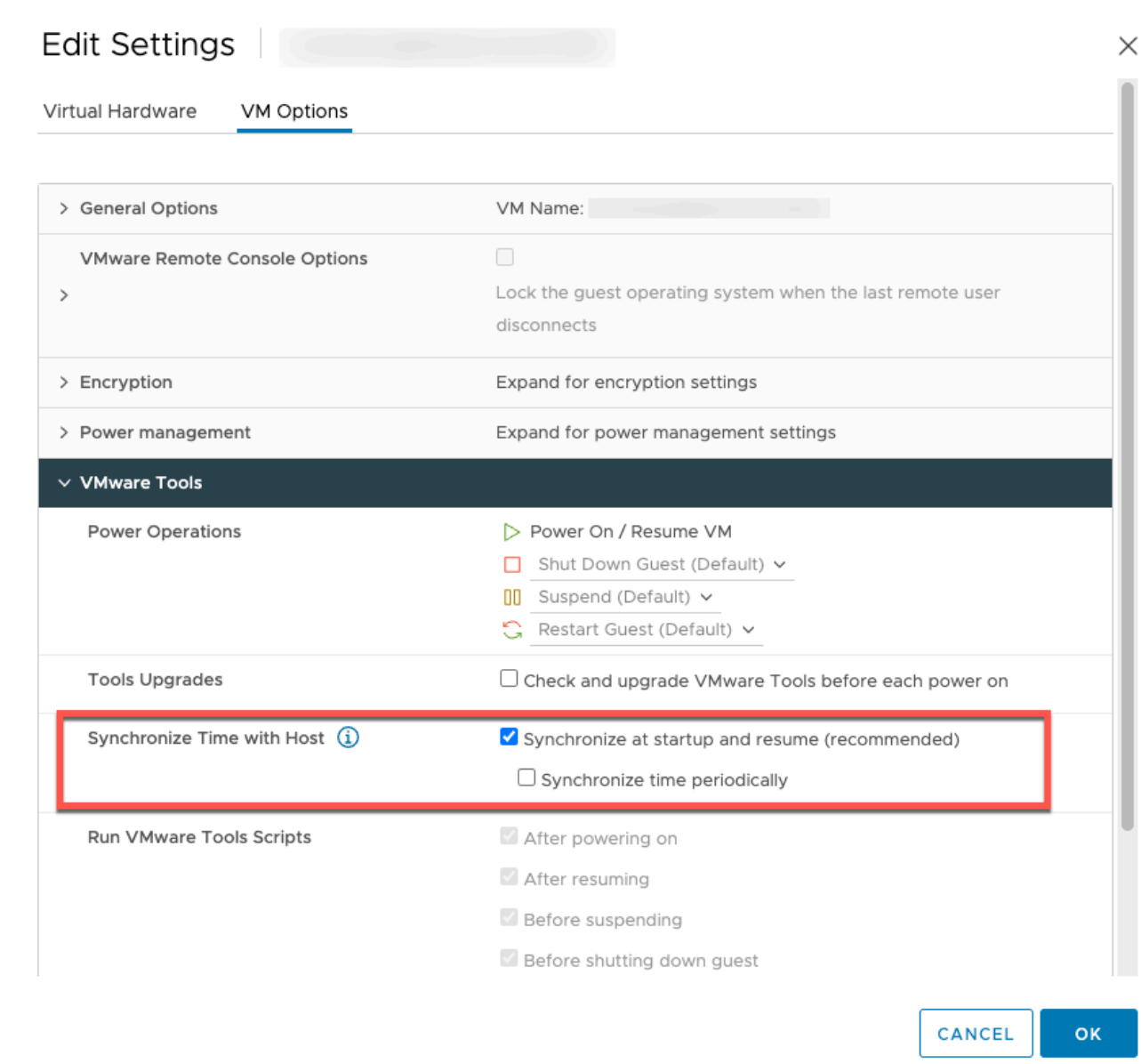


5. Klicken Sie nach der Bereitstellung von OVF mit der rechten Maustaste auf das Gateway und wählen Sie Einstellungen bearbeiten.

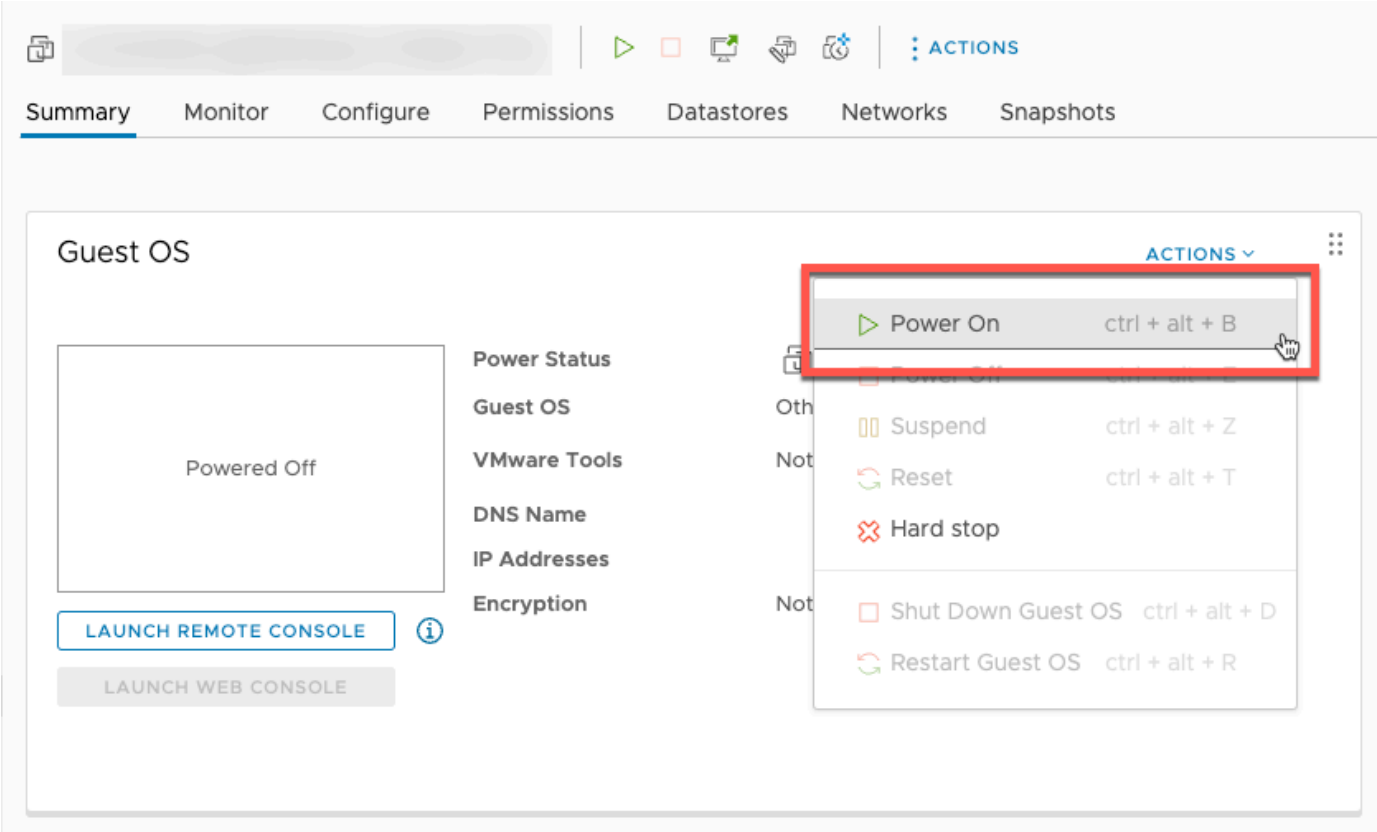


a. Gehen Sie unter VM-Optionen zu VM-Tools.

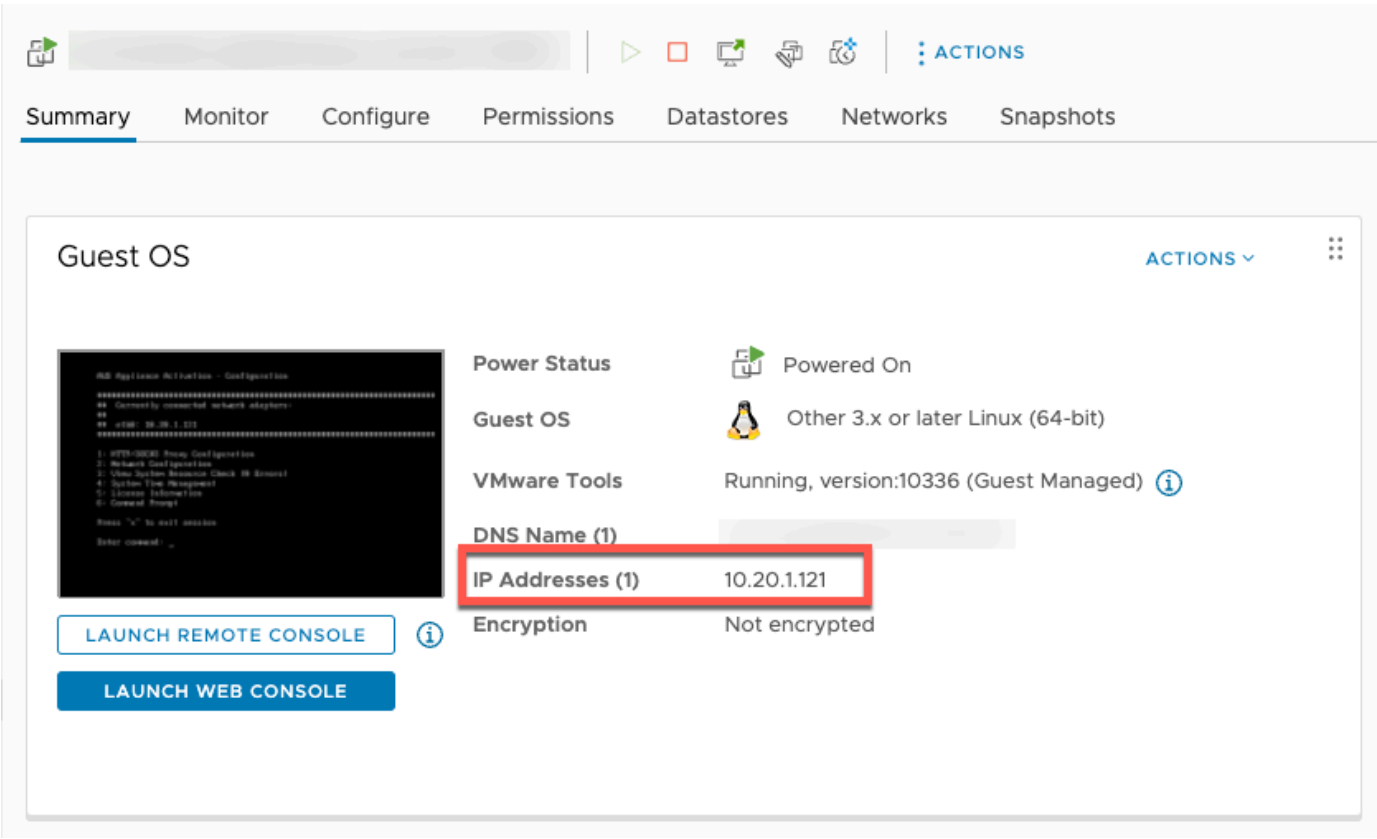
b. Stellen Sie sicher, dass für Zeit mit Host synchronisieren Beim Einschalten synchronisieren und wiederaufnehmen ausgewählt ist.



6. Schalten Sie die virtuelle Maschine ein, indem Sie im Menü Aktionen die Option „Einschalten“ auswählen.



7. Kopieren Sie die IP-Adresse aus der VM-Zusammenfassung und geben Sie sie unten ein.



Führen Sie nach dem Herunterladen der VMware-Software die folgenden Schritte aus:

1. Geben Sie im Abschnitt Gateway-Verbindung die IP-Adresse des Gateways ein.
   a. Gehen Sie zum vSphere Client, um diese IP-Adresse zu finden.
   b. Wählen Sie Ihr Gateway auf der Registerkarte Zusammenfassung aus.
   c. Kopieren Sie die IP-Adresse und fügen Sie sie in die Textleiste der AWS Backup Konsole ein.
2. Im Abschnitt Gateway-Einstellungen:
   a. Geben Sie einen Gateway-Namen ein.
   b. Überprüfen Sie die AWS Region.
   c. Wählen Sie aus, ob der Endpunkt öffentlich zugänglich ist oder in Ihrer Virtual Private Cloud (VPC) gehostet wird.
   d. Geben Sie je nach ausgewähltem Endpunkt den DNS-Namen des VPC-Endpunkts ein.

   Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts.
3. [Optional] Im Abschnitt Gateway-Tags können Sie Tags zuweisen, indem Sie den Schlüssel und den optionalen Wert eingeben. Um mehrere Tags hinzuzufügen, klicken Sie auf Ein weiteres Tag hinzufügen.
4. Um den Vorgang abzuschließen, klicken Sie auf Gateway erstellen, wodurch Sie zur Gateway-Detailseite weitergeleitet werden.

Bearbeiten oder Löschen eines Gateways

So bearbeiten oder löschen Sie ein Gateway:

1. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Gateways aus.
2. Wählen Sie im Abschnitt Gateways ein Gateway anhand seines Gateway-Namens aus.
3. Um den Gateway-Namen zu bearbeiten, wählen Sie Bearbeiten.
4. Um das Gateway zu löschen, wählen Sie Löschen und anschließend Gateway löschen.

   Sie können ein gelöschtes Gateway nicht reaktivieren. Wenn Sie sich erneut mit dem Hypervisor verbinden möchten, gehen Sie vor wie unter Erstellen eines Gateways beschrieben.
5. Um eine Verbindung zu einem Hypervisor herzustellen, wählen Sie im Abschnitt Verbundener Hypervisor die Option Verbinden.

Jedes Gateway ist mit einem einzelnen Hypervisor verbunden. Sie können jedoch mehrere Gateways mit demselben Hypervisor verbinden, um die Bandbreite zwischen ihnen über die des ersten Gateways hinaus zu erhöhen.

6. Um Tags zuzuweisen, zu bearbeiten oder zu verwalten, wählen Sie im Abschnitt Tags die Option Tags verwalten aus.

Bandbreitendrosselung des Backup-Gateways

> **Note**
>
> Dieses Feature wird auf neuen Gateways verfügbar sein, die nach dem 15. Dezember 2022 bereitgestellt werden. Für bestehende Gateways wird diese neue Funktion am oder vor dem 30. Januar 2023 über ein automatisches Softwareupdate verfügbar sein. Verwenden AWS CLI Sie den Befehl, um das Gateway manuell auf die neueste Version zu aktualisieren. `UpdateGatewaySoftwareNow`

Sie können den Upload-Durchsatz von Ihrem Gateway einschränken, AWS Backup um zu kontrollieren, wie viel Netzwerkbandbreite das Gateway verwendet. Standardmäßig gibt es bei einem aktivierten Gateway keine Ratenlimits.

Sie können einen Zeitplan für die Begrenzung der Bandbreitenrate mithilfe der AWS Backup Konsole oder mithilfe der API über AWS CLI () `PutBandwidthRateLimitSchedule`konfigurieren. Wenn Sie einen Zeitplan für Bandbreitenbegrenzungen verwenden, können Sie die Grenzwerte so konfigurieren, dass sie sich im Laufe des Tages oder der Woche automatisch ändern.

Bei der Bandbreitenbegrenzung wird der Durchsatz aller hochgeladenen Daten ausgeglichen, wobei der Durchschnitt über jede Sekunde berechnet wird. Es ist zwar möglich, dass Uploads die Bandbreitenratenbegrenzung für eine bestimmte Mikro- oder Millisekunde kurzzeitig überschreiten, dies führt jedoch in der Regel nicht zu großen Spitzen über längere Zeiträume.

Sie können bis zu 20 Intervalle hinzufügen. Der Höchstwert für die Upload-Rate beträgt 8.000.000 (Millionen) Megabyte pro Sekunde (Mbit/s).

In der Konsole können Sie den Zeitplan für die Bandbreitenbegrenzung für Ihr Gateway anzeigen und bearbeiten. AWS Backup

In diesem Abschnitt wird beschrieben, wie Sie den Zeitplan für die Bandbreitenratenlimit für Ihr Gateway anzeigen und bearbeiten.

So können Sie den Zeitplan für das Bandbreitenlimit anzeigen und bearbeiten:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Gateways aus. Im Bereich „Gateways“ werden Gateways nach Namen angezeigt. Klicken Sie auf das Optionsfeld neben dem Gateway-Namen, den Sie verwalten möchten.
3. Sobald Sie ein Optionsfeld ausgewählt haben, können Sie auf das Dropdownmenü Aktionen klicken. Klicken Sie auf Aktionen und dann auf Limit der Bandbreitenrate ändern. Der aktuelle Zeitplan wird angezeigt. Standardmäßig hat ein neues oder unbearbeitetes Gateway keine definierten Bandbreitenratenlimits.

   > **Note**
   >
   > Sie können auch auf der Seite mit den Gateway-Details auf Zeitplan verwalten klicken, um zur Seite „Bandbreite bearbeiten“ zu gelangen.

4. (Optional) Wählen Sie Intervall hinzufügen, um dem Zeitplan ein neues konfigurierbares Intervall hinzuzufügen. Geben Sie für jedes Intervall die folgenden Informationen ein:

   a. Wochentage – Wählen Sie den oder die wiederkehrenden Tage aus, für die das Intervall gelten soll. Wenn diese Option ausgewählt ist, werden die Tage unter dem Dropdown-Menü angezeigt. Sie können sie entfernen, indem Sie auf das X neben dem Tag klicken.

   b. Startzeit – Geben Sie die Startzeit für das Bandbreitenintervall im 24-Stunden-Format HH:MM ein. Die Uhrzeit wird in UTC (Universal Coordinated Time) gerendert.

      Hinweis: Ihr bandwidth-rate-limit Intervall beginnt am Anfang der angegebenen Minute.

   c. Endzeit – Geben Sie die Endzeit für das Bandbreitenintervall im 24-Stunden-Format HH:MM ein. Die Uhrzeit wird in UTC (Universal Coordinated Time) gerendert.

> **Important**
>
> Das bandwidth-rate-limit Intervall endet am Ende der angegebenen Minute. Um ein Intervall zu planen, das am Ende einer Stunde endet, geben Sie 59 ein. Um aufeinanderfolgende fortlaufende Intervalle zu planen, wobei der Übergang zu Beginn der Stunde ohne Unterbrechung zwischen den Intervallen erfolgt, geben Sie 59 für die Endminute des ersten Intervalls ein. Geben Sie `00` als Startminute des nachfolgenden Intervalls ein.

d. Upload-Rate – Geben Sie das Limit für die Upload-Rate in Megabit pro Sekunde (Mbit/s) ein. Der Mindestwert beträgt 102 Megabit pro Sekunde (Mbit/s).

5. (Optional) Wiederholen Sie den vorherigen Schritt wie gewünscht, bis Ihr Zeitplan für das Limit der Bandbreitenrate abgeschlossen ist. Wenn Sie ein Intervall aus Ihrem Zeitplan löschen müssen, wählen Sie Entfernen.

> **Important**
>
> Die Intervalle für das Bandbreitenlimit dürfen sich nicht überschneiden. Die Startzeit eines Intervalls muss nach der Endzeit eines vorherigen Intervalls und vor der Startzeit eines nachfolgenden Intervalls liegen. Die Endzeit muss vor der Startzeit des folgenden Intervalls liegen.

6. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Änderungen speichern.

In der AWS CLI können Sie den Zeitplan für die Bandbreitenbegrenzung für Ihr Gateway anzeigen und bearbeiten.

Die `GetBandwidthRateLimitSchedule`-Aktion kann verwendet werden, um den Zeitplan für die Bandbreitendrosselung für ein bestimmtes Gateway anzuzeigen. Wenn kein Zeitplan festgelegt ist, ist der Zeitplan eine leere Liste von Intervallen. Hier ist ein Beispiel für die Verwendung von AWS CLI , um den Bandbreitenplan eines Gateways abzurufen:

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

Um den Zeitplan für die Bandbreitendrosselung eines Gateways zu bearbeiten, können Sie die `PutBandwidthRateLimitSchedule`-Aktion verwenden. Beachten Sie, dass Sie den Zeitplan

eines Gateways nur als Ganzes aktualisieren können, anstatt einzelne Intervalle zu ändern, hinzuzufügen oder zu entfernen. Durch den Aufruf dieser Aktion wird der vorherige Zeitplan für die Bandbreitendrosselung des Gateways überschrieben.

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

Arbeiten mit Hypervisoren

Wenn Sie fertig sindErstellen eines Gateways, können Sie es mit einem Hypervisor verbinden, um mit den von diesem Hypervisor verwalteten virtuellen Maschinen arbeiten AWS Backup zu können. Der Hypervisor für VMware-VMs ist beispielsweise VMware vCenter Server. Stellen Sie sicher, dass Ihr Hypervisor mit den erforderlichen Berechtigungen für AWS Backup konfiguriert ist.

Hinzufügen eines Hypervisors

So fügen Sie einen Hypervisor hinzu:

1. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Hypervisors aus.
2. Wählen Sie Hypervisor hinzufügen aus.
3. Geben Sie im Abschnitt Hypervisor-Einstellungen einen Hypervisor-Namen ein.
4. Verwenden Sie für den vCenter-Server-Host das Dropdown-Menü, um entweder die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) auszuwählen. Geben Sie den entsprechenden Wert ein.
5. Geben Sie den AWS Backup Benutzernamen und das Passwort des Hypervisors ein, damit die virtuellen Maschinen auf dem Hypervisor erkannt werden können.
6. Verschlüsseln Sie Ihr Passwort. Sie können diese Verschlüsselung angeben, indem Sie im Dropdown-Menü einen bestimmten vom Dienst verwalteten KMS-Schlüssel oder einen vom Kunden verwalteten KMS-Schlüssel auswählen oder KMS-Schlüssel erstellen auswählen. Wenn Sie keinen bestimmten Schlüssel auswählen, verschlüsselt AWS Backup Ihr Passwort mit einem diensteigenen Schlüssel.
7. Geben Sie im Abschnitt Verbinden des Gateways mithilfe der Dropdown-Liste an, welches Gateway mit Ihrem Hypervisor verbunden werden soll.
8. Wählen Sie Gateway-Verbindung testen, um Ihre vorherigen Eingaben zu überprüfen.
9. Optional können Sie im Abschnitt Hypervisor-Tags dem Hypervisor Tags zuweisen, indem Sie Neues Tag hinzufügen wählen.

10. Optionale VMware-Tag-Zuordnung: Sie können bis zu 10 VMware-Tags hinzufügen, die Sie derzeit auf Ihren virtuellen Maschinen verwenden, um Tags zu generieren AWS .
11. Im Einstellungsbereich Protokollgruppe können Sie wählen, ob Sie Amazon CloudWatch Logs integrieren möchten, um die Protokolle Ihres Hypervisors zu verwalten (die Standardpreise für CloudWatch Logs gelten je nach Nutzung). Jeder Hypervisor kann zu einer Protokollgruppe gehören.

    a. Wenn Sie noch keine Protokollgruppe erstellt haben, wählen Sie das Optionsfeld Neue Protokollgruppe erstellen. Der Hypervisor, den Sie bearbeiten, wird dieser Protokollgruppe zugeordnet.

    b. Wenn Sie zuvor eine Protokollgruppe für einen anderen Hypervisor erstellt haben, können Sie diese Protokollgruppe für diesen Hypervisor verwenden. Wählen Sie Bestehende Protokollgruppe verwenden aus.

    c. Wenn Sie keine CloudWatch Protokollierung wünschen, wählen Sie Protokollierung deaktivieren.
12. Wählen Sie Hypervisor hinzufügen, um zu dessen Detailseite zu gelangen.

> **Tip**
>
> Sie können Amazon CloudWatch Logs (siehe Schritt 11 oben) verwenden, um Informationen über Ihren Hypervisor zu erhalten, einschließlich Fehlerüberwachung, Netzwerkverbindung zwischen dem Gateway und dem Hypervisor sowie Informationen zur Netzwerkkonfiguration. Informationen zu CloudWatch Protokollgruppen finden Sie unter Working with Log Groups and Log Streams im CloudWatch Amazon-Benutzerhandbuch.

Anzeigen virtueller Maschinen, die von einem Hypervisor verwaltet werden

So zeigen Sie virtuelle Maschinen auf einem Hypervisor an:

1. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Hypervisors aus.
2. Wählen Sie im Abschnitt Hypervisoren einen Hypervisor anhand seines Hypervisor-Namens aus, um zu seiner Detailseite zu gelangen.
3. Wählen Sie im Abschnitt unter Hypervisor-Zusammenfassung die Registerkarte Virtuelle Maschinen aus.

4. Im Abschnitt Verbundene virtuelle Maschinen wird automatisch eine Liste mit virtuellen Maschinen angezeigt.

Anzeigen von Gateways, die mit einem Hypervisor verbunden sind

So zeigen Sie Gateways an, die mit einem Hypervisor verbunden sind:

1. Wählen Sie die Registerkarte Gateways.
2. Im Abschnitt Verbundene Gateways wird automatisch eine Liste von Gateways angezeigt.

Verbinden eines Hypervisors mit weiteren Gateways

Ihre Backup- und Wiederherstellungsgeschwindigkeiten werden möglicherweise durch die Bandbreite der Verbindung zwischen Ihrem Gateway und dem Hypervisor begrenzt. Sie können diese Geschwindigkeiten erhöhen, indem Sie ein oder mehrere zusätzliche Gateways an Ihren Hypervisor anschließen. Sie können dies im Abschnitt Verbundene Gateways folgendermaßen tun:

1. Wählen Sie Verbinden aus.
2. Wählen Sie ein anderes Gateway aus dem Dropdown-Menü. Wählen Sie alternativ Gateway erstellen, um ein neues Gateway zu erstellen.
3. Wählen Sie Connect aus.

Bearbeiten einer Hypervisor-Konfiguration

Wenn Sie das Feature Gateway-Verbindung testen nicht verwenden, fügen Sie möglicherweise einen Hypervisor mit einem falschen Benutzernamen oder Passwort hinzu. In diesem Fall lautet der Verbindungsstatus des Hypervisors immer `Pending`. Alternativ können Sie den Benutzernamen oder das Passwort wechseln, um auf Ihren Hypervisor zuzugreifen. Aktualisieren Sie diese Informationen folgendermaßen:

So bearbeiten Sie einen bereits hinzugefügten Hypervisor:

1. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Hypervisors aus.
2. Wählen Sie im Abschnitt Hypervisoren einen Hypervisor anhand seines Hypervisor-Namens aus, um zu seiner Detailseite zu gelangen.
3. Wählen Sie Bearbeiten aus.
4. Der obere Bereich trägt den Namen Hypervisor-Einstellungen.

a. Unter vCenter-Server-Host können Sie auch den FQDN (Fully-Qualified Domain Name) oder die IP-Adresse bearbeiten.

b. Optional können Sie Benutzername und Passwort des Hypervisors eingeben.

5. Im Einstellungsbereich Protokollgruppe können Sie sich für eine Integration mit Amazon entscheiden, CloudWatch um die Protokolle Ihres Hypervisors zu verwalten (CloudWatch Standardpreise gelten je nach Nutzung). Jeder Hypervisor kann zu einer Protokollgruppe gehören.

   a. Wenn Sie noch keine Protokollgruppe erstellt haben, wählen Sie das Optionsfeld Neue Protokollgruppe erstellen. Der Hypervisor, den Sie bearbeiten, wird dieser Protokollgruppe zugeordnet.

   b. Wenn Sie zuvor eine Protokollgruppe für einen anderen Hypervisor erstellt haben, können Sie diese Protokollgruppe für diesen Hypervisor verwenden. Wählen Sie Bestehende Protokollgruppe verwenden aus.

   c. Wenn Sie keine CloudWatch Protokollierung wünschen, wählen Sie Protokollierung deaktivieren aus.

> **Tip**
>
> Sie können Amazon CloudWatch Logs (siehe Schritt 5 oben) verwenden, um Informationen über Ihren Hypervisor zu erhalten, einschließlich Fehlerüberwachung, Netzwerkverbindung zwischen dem Gateway und dem Hypervisor sowie Informationen zur Netzwerkkonfiguration. Informationen zu CloudWatch Protokollgruppen finden Sie unter Working with Log Groups and Log Streams im CloudWatch Amazon-Benutzerhandbuch.

Um einen Hypervisor programmgesteuert zu aktualisieren, verwenden Sie den CLI-Befehl update-hypervisor und den API-Aufruf. UpdateHypervisor

Löschen einer Hypervisor-Konfiguration

Wenn Sie einen bereits hinzugefügten Hypervisor entfernen müssen, entfernen Sie die Hypervisor-Konfiguration und fügen Sie eine weitere hinzu. Dieser Entfernungsvorgang bezieht sich auf die Konfiguration für die Verbindung mit dem Hypervisor. Der Hypervisor wird nicht gelöscht.

Gehen Sie wie folgt vor, um die Konfiguration für die Verbindung zu einem bereits hinzugefügten Hypervisor zu löschen:

1. Wählen Sie im linken Navigationsbereich im Abschnitt Externe Ressourcen Hypervisors aus.
2. Wählen Sie im Abschnitt Hypervisoren einen Hypervisor anhand seines Hypervisor-Namens aus, um zu seiner Detailseite zu gelangen.
3. Wählen Sie Entfernen und anschließend Hypervisor entfernen.
4. Optional: Ersetzen Sie die entfernte Hypervisor-Konfiguration mit dem Verfahren für Hinzufügen eines Hypervisors.

Grundlegendes zum Hypervisor-Status

Im Folgenden werden die einzelnen möglichen Hypervisor-Status und, falls zutreffend, die Schritte zur Behebung beschrieben. Der `ONLINE`-Status entspricht dem normalen Status des Hypervisors. Ein Hypervisor sollte diesen Status die ganze Zeit oder die meiste Zeit haben, wenn er für das Backup und die Wiederherstellung von vom Hypervisor verwalteten VMs verwendet wird.

Hypervisor-Status

Status	Bedeutung und Behebung
`ONLINE`	Sie haben einen Hypervisor hinzugefügt AWS Backup, ihm ein Gateway zugeordnet und können über Ihr Netzwerk eine Verbindung zu diesem Gateway herstellen, um die Sicherung und Wiederherstellung der vom Hypervisor verwalteten virtuellen Maschinen durchzufü hren. Sie können jederzeit On-Demand-Backups und geplante Backups dieser virtuellen Maschinen durchführen.
`PENDING`	Sie haben einen Hypervisor hinzugefügt, aber: AWS Backup • Er ist keinem Gateway zugeordnet, oder

Status	Bedeutung und Behebung
	• Er ist einem oder mehreren Gateways zugeordnet, aber all diese Gateways wurden gelöscht oder sind aus anderen Gründen nicht aktiv. Um den Status eines Hypervisors von `PENDING` zu `ONLINE` zu ändern, erstellen Sie ein Gateway und verbinden Sie Ihren Hypervisor mit diesem Gateway.
`OFFLINE`	Sie haben einen Hypervisor hinzugefügt AWS Backup und ihn einem Gateway zugeordne t, aber das Gateway kann über Ihr Netzwerk keine Verbindung zum Hypervisor herstellen. Um den Status eines Hypervisors von `OFFLINE` auf `ONLINE` zu ändern, überprüfen Sie die Richtigkeit Ihrer Netzwerkkonfiguration. Wenn das Problem weiterhin besteht, überprüfe n Sie, ob die IP-Adresse oder der FDQN Ihres Hypervisors korrekt sind. Wenn sie nicht korrekt sind, fügen Sie Ihren Hypervisor erneut mit den richtigen Informationen hinzu und testen Sie Ihre Gateway-Verbindung.
`ERROR`	Sie haben einen Hypervisor zu einem Gateway hinzugefügt AWS Backup und ihn einem Gateway zugeordnet, aber das Gateway kann nicht mit dem Hypervisor kommunizieren. Um den Status eines Hypervisors von `ERROR` zu `ONLINE` zu ändern, stellen Sie sicher, dass der Benutzername und das Passwort des Hypervisors korrekt sind. Wenn sie falsch sind, bearbeiten Sie Ihre Hypervisor-Konfiguration.

Nächste Schritte

Informationen zum Backup virtueller Maschinen auf Ihrem Hypervisor finden Sie unter Backup virtueller Maschinen.

Backup virtueller Maschinen

Nach Hinzufügen eines Hypervisors listet das Backup-Gateway Ihre virtuellen Maschinen automatisch auf. Sie können Ihre virtuellen Maschinen anzeigen, indem Sie im linken Navigationsbereich entweder Hypervisors oder Virtuelle Maschinen auswählen.

- Wählen Sie Hypervisoren, um nur die virtuellen Maschinen anzuzeigen, die von einem bestimmten Hypervisor verwaltet werden. In dieser Ansicht können Sie jeweils mit einer virtuellen Maschine arbeiten.
- Wählen Sie Virtuelle Maschinen aus, um alle virtuellen Maschinen auf allen Hypervisoren anzuzeigen, die Sie zu Ihrem hinzugefügt haben. AWS-Konto In dieser Ansicht können Sie mit einigen oder allen Ihren virtuellen Maschinen auf mehreren Hypervisoren arbeiten.

Unabhängig davon, für welche Ansicht Sie sich entscheiden: Um einen Backup-Vorgang auf einer bestimmten virtuellen Maschine durchzuführen, wählen Sie deren VM-Namen, um die entsprechende Detailseite zu öffnen. Die VM-Detailseite ist der Ausgangspunkt für die folgenden Verfahren.

Erstellen eines On-Demand-Backups einer virtuellen Maschine

Ein On-Demand-Backup ist ein einmaliges, vollständiges Backup, das Sie manuell initiieren. Sie können On-Demand-Backups verwenden, um die AWS Backup Sicherungs- und Wiederherstellungsfunktionen zu testen.

So erstellen Sie ein On-Demand-Backup einer virtuellen Maschine:

1. Wählen Sie On-Demand-Backup erstellen.
2. Konfigurieren Sie Ihr On-Demand-Backup.
3. Wählen Sie On-Demand-Backup erstellen.
4. Prüfen Sie, ob Ihr Backup-Auftrag den Status `Completed` hat. Wählen Sie im linken Navigationsmenü Aufträge aus.
5. Wählen Sie die Backup-Auftrags-ID, um Informationen zum Backup-Auftrag wie die Backup-Größe und die zwischen dem Erstellungs- und dem Abschlussdatum verstrichene Zeit anzuzeigen.

Inkrementelle VM-Backups

Neuere VMware-Versionen enthalten ein Feature namens Changed Block Tracking (CBT), mit der die Speicherblöcke virtueller Maschinen nachverfolgt werden, während sie sich im Laufe der Zeit ändern. Wenn Sie eine virtuelle Maschine sichern, AWS Backup versucht sie, die CBT-Daten zu verwenden, sofern sie verfügbar sind. AWS Backup AWS Backup verwendet CBT-Daten, um den Backup-Prozess zu beschleunigen. Ohne CBT-Daten sind Backup-Jobs oft langsamer und beanspruchen mehr Hypervisor-Ressourcen. Das Backup kann auch dann erfolgreich abgeschlossen werden, wenn die CBT-Daten nicht gültig oder verfügbar sind. Beispielsweise sind die CBT-Daten möglicherweise nicht gültig oder nicht verfügbar, wenn die virtuelle Maschine oder der ESXi-Host hart heruntergefahren wird.

In den Fällen, in denen CBT-Daten ungültig oder nicht verfügbar sind, wird der Backup-Status `Successful` mit einer Meldung angezeigt. In diesen Fällen weist die Meldung darauf hin, dass in Ermangelung von CBT-Daten anstelle der CBT-Daten von VMware ein eigener Mechanismus zur Erkennung von Änderungen AWS Backup verwendet wurde, um das Backup abzuschließen. Bei nachfolgenden Backups wird erneut versucht, CBT-Daten zu verwenden, und in den meisten Fällen sind die CBT-Daten erfolgreich gültig und verfügbar. Wenn das Problem weiterhin besteht, finden Sie unter VMware-Fehlerbehebung Schritte zur Behebung.

Damit CBT korrekt funktioniert, müssen folgende Bedingungen erfüllt sein:

- Der Host muss ESXi 4.0 oder höher sein
- Die VM, der die Festplatten gehören, muss die Hardwareversion 7 oder höher haben
- CBT muss für die virtuelle Maschine aktiviert sein (es ist standardmäßig aktiviert)

So überprüfen Sie, ob CBT für eine virtuelle Festplatte aktiviert ist:

1. Öffnen Sie den vSphere-Client und wählen Sie eine ausgeschaltete virtuelle Maschine aus.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und navigieren Sie zu Einstellungen bearbeiten > Optionen > Erweitert/Allgemein > Konfigurationsparameter.
3. Die Option `ctkEnabled` muss gleich `True` sein.

Automatisieren des Backups virtueller Maschinen durch Zuweisung von Ressourcen zu einem Backup-Plan

Ein Backup-Plan ist eine benutzerdefinierte Datenschutzrichtlinie, die den Datenschutz für viele AWS -Dienste und Drittanbieteranwendungen automatisiert. Sie erstellen zunächst Ihren Backup-Plan,

indem Sie dessen Backup-Häufigkeit, Aufbewahrungsdauer, Lebenszyklusrichtlinie und viele andere Optionen angeben. Informationen zum Erstellen eines Backup-Plans finden Sie im Tutorial „Erste Schritte“.

Nachdem Sie Ihren Backup-Plan erstellt haben, weisen Sie diesem AWS Backup Backup-Plan unterstützte Ressourcen, einschließlich virtueller Maschinen, zu. AWS Backup bietet viele Möglichkeiten, Ressourcen zuzuweisen, einschließlich der Zuweisung aller Ressourcen in Ihrem Konto, einschließlich oder Ausschließen einzelner bestimmter Ressourcen, oder des Hinzufügens von Ressourcen mit bestimmten Tags.

Zusätzlich zu den bestehenden Funktionen zur Ressourcenzuweisung bietet die AWS Backup Unterstützung für virtuelle Maschinen mehrere neue Funktionen, mit denen Sie virtuelle Maschinen schnell Backup-Plänen zuweisen können. Auf der Seite Virtuelle Maschinen können Sie mehreren virtuellen Maschinen Tags zuweisen oder das neue Feature Ressourcen dem Plan zuweisen verwenden. Verwenden Sie diese Funktionen, um Ihre virtuellen Maschinen zuzuweisen, die vom AWS Backup Gateway bereits erkannt wurden.

Wenn Sie davon ausgehen, dass in Zukunft weitere virtuelle Maschinen erkannt und zugewiesen werden, und Sie den Schritt der Ressourcenzuweisung automatisieren möchten, um diese zukünftigen virtuellen Maschinen einzubeziehen, verwenden Sie das neue Feature Gruppenzuweisung erstellen.

VMware-Tags

Tags sind Schlüssel-Wert-Paare, mit denen Sie Ihre Ressourcen verwalten, filtern und suchen können.

Ein VMware-Tag besteht aus einer Kategorie und einem Tag-Namen. VMware-Tags werden verwendet, um virtuelle Maschinen zu gruppieren. Ein Tag-Name ist eine Bezeichnung, die einer virtuellen Maschine zugewiesen wird. Eine Kategorie ist eine Sammlung von Tag-Namen.

In AWS Tags können Sie Zeichen aus UTF-8-Buchstaben, Zahlen, Leerzeichen und Sonderzeichen verwenden. `+ - = . _ : /`

Wenn Sie Tags auf Ihren virtuellen Maschinen verwenden, können Sie in AWS Backup bis zu 10 passende Tags hinzufügen, um die Organisation zu erleichtern. Sie können Tags bis zu 10 VMware-Tags zuordnen AWS . In der AWS Backup Konsole finden Sie diese unter Meine Organisation > Virtuelle Maschinen > AWS Tags oder VMware-Tags.

VMware-Tag-Zuweisung

Wenn Sie Tags auf Ihren virtuellen Maschinen verwenden, können Sie für mehr Übersichtlichkeit und Organisation in AWS Backup bis zu 10 passende Tags hinzufügen. Zuweisungen gelten für jede virtuelle Maschine auf dem Hypervisor.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Gehen Sie in der Konsole zu Hypervisor bearbeiten (klicken Sie auf Externe Ressourcen, dann auf Hypervisoren, dann auf den Hypervisor-Namen und dann auf Zuordnungen verwalten).
3. Der letzte Bereich, VMware-Tag-Mapping, enthält vier Textfelder, in die Sie Ihre vorhandenen VMware-Tag-Informationen in die entsprechenden AWS Tags eingeben können. Die vier Felder sind VMware-Tag-Kategorie, VMware-Tagname, AWS Tag-Schlüssel und AWS Tag-Wert (Beispiel: Kategorie = OS; Tagname = Windows; AWS Tag-Schlüssel = OS-Windows und AWS Tag-Wert = Windows).
4. Nachdem Sie Ihre bevorzugten Werte eingegeben haben, klicken Sie auf Zuweisung hinzufügen. Wenn Sie einen Fehler machen, können Sie auf Entfernen klicken, um die eingegebenen Informationen zu löschen.
5. Geben Sie nach dem Hinzufügen von Zuordnungen die IAM-Rolle an, die Sie verwenden möchten, um diese AWS -Tags auf die virtuellen VMware-Maschinen anzuwenden.

   Die Richtlinie `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` enthält die erforderlichen Berechtigungen. Sie können diese Richtlinie an die Rolle anhängen, die Sie verwenden (oder sie von einem Administrator anhängen lassen), oder Sie können eine benutzerdefinierte Richtlinie für die verwendete Rolle erstellen.
6. Klicken Sie abschließend auf Hypervisor hinzufügen oder auf Speichern.

Die Vertrauensstellung der IAM-Rolle sollte geändert werden, um die Dienste backup-gateway.amazonaws.com und backup.amazonaws.com hinzuzufügen. Ohne diesen Service wird beim Zuweisen von Tags wahrscheinlich ein Fehler auftreten. So bearbeiten Sie die Vertrauensstellung für eine vorhandene Rolle:

1. Melden Sie sich bei der IAM-Konsole an.
2. Wählen Sie im Navigationsbereich der Konsole Rollen aus.
3. Wählen Sie den Namen der Rolle aus, die Sie ändern möchten, und öffnen Sie die Registerkarte Vertrauensstellungen auf der Detailseite.

4. Fügen Sie unter Richtliniendokument Folgendes ein:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Wählen Sie Update Trust Policy (Trust Policy aktualisieren).

Weitere Informationen finden Sie unter Bearbeiten der Vertrauensstellung für eine bestehende Rolle im Administrationshandbuch zu AWS Directory Service.

VMware-Tag-Zuweisungen anzeigen

Klicken Sie in der AWS Backup -Konsole auf Externe Ressourcen, dann auf Hypervisoren und anschließend auf den Link Hypervisor-Name, um die Eigenschaften für den ausgewählten Hypervisor anzuzeigen. Unter dem Übersichtsbereich befinden sich vier Registerkarten, von denen die letzte die VMware-Tag-Zuweisung enthält. Falls Sie noch keine Zuweisungen haben, wird die Option „Keine VMware-Tag-Zuweisungen“ angezeigt.

Von hier aus können Sie die Metadaten der vom Hypervisor erkannten virtuellen Maschinen synchronisieren, Sie können Zuordnungen auf Ihre Hypervisoren kopieren, Sie können den AWS VMware-Tags zugeordnete Tags zur Backup-Auswahl eines Backup-Plans hinzufügen oder Zuordnungen verwalten.

Um zu sehen, welche Tags auf eine ausgewählte virtuelle Maschine angewendet wurden, klicken Sie in der Konsole auf Virtuelle Maschinen dann auf den Namen der virtuellen Maschine und dann auf AWS -Tags oder VMware-Tags. Sie können die mit dieser virtuellen Maschine verbundenen Tags anzeigen und diese Tags verwalten.

Zuweisen virtueller Maschinen zu einem Plan mithilfe von VMware-Tag-Zuweisungen

So können Sie virtuelle Maschinen mithilfe zugeordneter Tags einem Backup-Plan zuweisen:

1. Öffnen AWS Backup Sie die Konsole unter https://console.aws.amazon.com/backup.
2. Gehen Sie in der Konsole zu „VMware-Tag-Zuweisungen“ auf der Hypervisor-Detailseite (klicken Sie auf Externe Ressourcen, dann auf Hypervisoren, dann auf den Hypervisor-Namen).
3. Aktivieren Sie das Kontrollkästchen neben mehreren zugewiesenen Tags, um diese Tags demselben Backup-Plan zuzuweisen.
4. Klicken Sie auf Zur Ressourcenzuweisung hinzufügen.
5. Wählen Sie einen vorhandenen Backup-Plan aus der Dropdown-Liste aus. Alternativ können Sie einen neuen Backup-Plan erstellen über Backup-Plan erstellen.
6. Klicken Sie auf Bestätigen. Dadurch wird die Seite Ressourcen zuweisen mit dem Feld Auswahl mithilfe von Tags verfeinern mit vorausgefüllten Werten geöffnet.

VMware-Tags mit dem AWS CLI

AWS Backup verwendet den API-Aufruf `PutHypervisorPropertyMappings`, um die Eigenschaften von Hypervisor-Entitäten vor Ort den Eigenschaften in zuzuordnen. AWS

Verwenden Sie in AWS CLI der den Vorgang: `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
```

Ein Beispiel:

```
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
```

Sie können GetHypervisorPropertyMappings auch als Unterstützung bei der Bereitstellung von Informationen zur Eigenschaftszuweisung verwenden. Verwenden Sie im AWS CLI die Operation`get-hypervisor-property-mappings`. Hier ist ein Beispiel für eine Vorlage:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

Ein Beispiel:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Synchronisieren Sie Metadaten von virtuellen Maschinen, die vom Hypervisor AWS mithilfe von API, CLI oder SDK entdeckt wurden

Sie können die Metadaten virtueller Maschinen synchronisieren. Wenn Sie dies tun, werden die auf der virtuellen Maschine vorhandenen VMware-Tags, die Teil der Zuweisungen sind, synchronisiert. Außerdem werden AWS -Tags, die den auf der virtuellen Maschine vorhandenen VMware-Tags zugewiesen sind, auf die Ressource der virtuellen AWS -Maschine angewendet.

AWS Backup verwendet den API-Aufruf StartVirtualMachinesMetadataSync, um die Metadaten der vom Hypervisor erkannten virtuellen Maschinen zu synchronisieren. Verwenden Sie zum Synchronisieren von Metadaten auf virtuellen Maschinen, die vom Hypervisor über AWS CLI erkannt werden, den Vorgang `start-virtual-machines-metadata-sync`.

Beispielvorlage:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Beispiel:

```
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
```

Sie können ihn auch GetHypervisor zur Unterstützung mit Hypervisor-Informationen wie Host, Status und Status der letzten Metadatensynchronisierung verwenden und auch den Zeitpunkt der

letzten erfolgreichen Metadatensynchronisierung abrufen. Verwenden Sie in der AWS CLI den Vorgang`get-hypervisor`.

Beispielvorlage:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Beispiel:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Weitere Informationen finden Sie in der API-Dokumentation VmwareTagund VmwareToAwsTagMapping.

Dieses Feature wird auf neuen Gateways verfügbar sein, die nach dem 15. Dezember 2022 bereitgestellt werden. Für bestehende Gateways wird diese neue Funktion am oder vor dem 30. Januar 2023 über ein automatisches Softwareupdate verfügbar sein. Verwenden Sie den AWS CLI Befehl, um das Gateway manuell auf die neueste Version zu aktualisieren UpdateGatewaySoftwareNow.

Beispiel:

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Zuweisen virtueller Maschinen mithilfe von Tags

Sie können Ihren virtuellen Maschinen, die aktuell erkannt werden AWS Backup, zusammen mit anderen AWS Backup Ressourcen zuweisen, indem Sie ihnen ein Tag zuweisen, das Sie bereits einem Ihrer vorhandenen Backup-Pläne zugewiesen haben. Sie können auch einen neuen Backup-Plan und eine neue Tag-basierte Ressourcenzuweisung erstellen. Backup-Pläne suchen bei jeder Ausführung eines Backup-Auftrags nach neu zugewiesenen Ressourcen.

So markieren Sie mehrere virtuelle Maschinen mit demselben Tag:

1. Wählen Sie im linken Navigationsbereich die Option Virtuelle Maschinen aus.

2. Aktivieren Sie das Kontrollkästchen neben dem VM-Namen, um alle Ihre virtuellen Maschinen auszuwählen. Aktivieren Sie alternativ das Kontrollkästchen neben den VM-Namen, die Sie markieren möchten.
3. Wählen Sie Tags hinzufügen aus.
4. Geben Sie einen Tag-Schlüssel ein.
5. Empfehlung: Geben Sie einen Tag-Wert ein.
6. Wählen Sie Bestätigen aus.

Zuweisen virtueller Maschinen mithilfe des Features „Ressourcen dem Plan zuweisen“

Mithilfe der Funktion Ressourcen dem Plan zuweisen können Sie virtuelle Maschinen AWS Backup , die aktuell erkannt werden, einem vorhandenen oder neuen Backup-Plan zuweisen.

So weisen Sie virtuelle Maschinen mithilfe des Features „Ressourcen dem Plan zuweisen“ zu:

1. Wählen Sie im linken Navigationsbereich die Option Virtuelle Maschinen aus.
2. Aktivieren Sie das Kontrollkästchen neben dem VM-Namen, um alle Ihre virtuellen Maschinen auszuwählen. Sie können auch das Kontrollkästchen neben mehreren VM-Namen aktivieren, um sie demselben Backup-Plan zuzuweisen.
3. Wählen Sie Zuweisungen und anschließend Ressourcen dem Plan zuweisen aus.
4. Geben Sie unter Name der Ressourcenzuweisung einen Namen ein.
5. Wählen Sie eine IAM-Rolle für die Ressourcenzuweisung, um Backups zu erstellen und Wiederherstellungspunkte zu verwalten. Wenn Sie keine bestimmte IAM-Rolle verwenden können, empfehlen wir die Standardrolle, die über die richtigen Berechtigungen verfügt.
6. Wählen Sie im Abschnitt Backup-Plan einen vorhandenen Backup-Plan aus der Dropdown-Liste aus. Alternativ können Sie einen neuen Backup-Plan erstellen über Backup-Plan erstellen.
7. Wählen Sie Ressourcen zuweisen aus.
8. Optional: Vergewissern Sie sich, dass Ihre virtuellen Maschinen einem Backup-Plan zugewiesen sind, indem Sie Backup-Plan anzeigen wählen. Wählen Sie dann im Abschnitt Ressourcenzuweisungen den Namen der Ressourcenzuweisung aus.

Zuweisen virtueller Maschinen mithilfe des Features „Gruppenzuweisung erstellen“

Im Gegensatz zu den beiden vorherigen Funktionen zur Ressourcenzuweisung für virtuelle Maschinen weist die Funktion Gruppenzuweisung erstellen nicht nur virtuelle Maschinen zu, die

aktuell erkannt werden AWS Backup, sondern auch virtuelle Maschinen, die in future in einem von Ihnen definierten Ordner oder Hypervisor entdeckt werden.

Außerdem müssen Sie keine Kontrollkästchen aktivieren, um das Feature Gruppenzuweisung erstellen zu verwenden.

So weisen Sie virtuelle Maschinen mithilfe des Features „Ressourcen dem Plan zuweisen“ zu:

1. Wählen Sie im linken Navigationsbereich die Option Virtuelle Maschinen aus.
2. Wählen Sie Zuweisungen und anschließend Gruppenzuweisung erstellen.
3. Geben Sie unter Name der Ressourcenzuweisung einen Namen ein.
4. Wählen Sie eine IAM-Rolle für die Ressourcenzuweisung, um Backups zu erstellen und Wiederherstellungspunkte zu verwalten. Wenn Sie keine bestimmte IAM-Rolle verwenden können, empfehlen wir die Standardrolle, die über die richtigen Berechtigungen verfügt.
5. Wählen Sie im Abschnitt Ressourcengruppe das Dropdown-Menü Gruppentyp aus. Ihre Optionen sind Ordner oder Hypervisor.

    a. Wählen Sie Ordner, um alle virtuellen Maschinen in einem Ordner auf einem Hypervisor zuzuweisen. Wählen Sie über das Dropdown-Menü einen Gruppenname-Ordner aus, z. B. `datacenter/vm`. Sie können auch Unterordner miteinschließen.

    > **Note**
    >
    > Um ordnerbasierte Zuweisungen vorzunehmen, werden virtuelle Maschinen während des Erkennungsvorgangs mit dem Ordner versehen, AWS Backup in dem sie sich während des Erkennungsvorgangs befinden. Wenn Sie eine virtuelle Maschine später in einen anderen Ordner verschieben, AWS Backup kann das Tag aufgrund der bewährten Methoden AWS beim Tagging nicht für Sie aktualisiert werden. Diese Zuweisungsmethode kann dazu führen, dass weiterhin Backups von virtuellen Maschinen erstellt werden, die Sie aus Ihrem zugewiesenen Ordner verschoben haben.

    b. Wählen Sie Hypervisoren, um alle virtuellen Maschinen zuzuweisen, die von einem bestimmten Hypervisor verwaltet werden. Wählen Sie im Dropdown-Menü einen Hypervisor-ID-Gruppennamen aus.
6. Wählen Sie im Abschnitt Backup-Plan einen vorhandenen Backup-Plan aus der Dropdown-Liste aus. Alternativ können Sie einen neuen Backup-Plan erstellen über Backup-Plan erstellen.

7. Wählen Sie Gruppenzuweisung erstellen.
8. Optional: Vergewissern Sie sich, dass Ihre virtuellen Maschinen einem Backup-Plan zugewiesen sind, indem Sie Backup-Plan anzeigen wählen. Wählen Sie im Abschnitt Ressourcenzuweisungen den Namen der Ressourcenzuweisung aus.

Nächste Schritte

Informationen zum Wiederherstellen einer virtuellen Maschine finden Sie unter Wiederherstellen einer virtuellen Maschine mit AWS Backup.

Informationen über Drittanbieter-Quellkomponenten für Backup-Gateways

In diesem Abschnitt finden Sie Informationen zu Drittanbieter-Tools und Lizenzen, die erforderlich sind, um die Funktionalität von Backup-Gateways bereitzustellen.

Der Quellcode einiger der in der Backup-Gateway-Software enthaltenen Drittanbieter-Softwarekomponenten steht unter folgenden Links zum Download zur Verfügung:

- Laden Sie für Gateways, die auf VMware ESXi bereitgestellt werden, sources.tgz herunter.

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL Toolkit (https://www.openssl.org/) entwickelt wurde.

Dieses Produkt enthält Software, die vom VMware® vSphere Software Development Kit (https://www.vmware.com) entwickelt wurde.

Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unter Lizenzen von Drittanbietern.

Open-Source-Komponenten für die AWS -Appliance

Verschiedene Tools und Lizenzen von Drittanbietern werden verwendet, um Funktionen für das Backup-Gateway bereitzustellen.

Verwenden Sie die folgenden Links, um den Quellcode für bestimmte Open-Source-Softwarekomponenten herunterzuladen, die in der Appliance-Software enthalten sind: AWS

- Laden Sie für Gateways, die auf VMware ESXi bereitgestellt werden, sources.tar herunter.

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL Toolkit (https://www.openssl.org/) entwickelt wurde. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unter Lizenzen von Drittanbietern.

Beheben von VM-Problemen

Inkrementelle Backups/CBT-Probleme und Meldungen

Fehlernachricht: **"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."**

Wenn diese Meldung weiterhin angezeigt wird, setzen Sie CBT zurück, gemäß den Anweisungen von VMware.

In der Meldung wird darauf hingewiesen, dass CBT nicht aktiviert oder nicht verfügbar war: „VMware Change Block Tracking (CBT) war für diese virtuelle Maschine nicht verfügbar, aber das inkrementelle Backup wurde mit unserem proprietären Änderungsmechanismus erfolgreich abgeschlossen“.

Vergewissern Sie sich, dass CBT aktiviert ist. So überprüfen Sie, ob CBT für eine virtuelle Festplatte aktiviert ist:

1. Öffnen Sie den vSphere-Client und wählen Sie eine ausgeschaltete virtuelle Maschine aus.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und navigieren Sie zu Einstellungen bearbeiten > Optionen > Erweitert/Allgemein > Konfigurationsparameter.
3. Die Option `ctkEnabled` muss gleich `True` sein.

Wenn es aktiviert ist, stellen Sie sicher, dass Sie VMware-Funktionen verwenden up-to-date . Der Host muss ESXi 4.0 oder höher sein und die virtuelle Maschine, der die zu überwachenden Festplatten gehören, muss die Hardwareversion 7 oder höher haben.

Wenn CBT aktiviert ist und die Software und Hardware auf dem neuesten Stand sind, schalten Sie die virtuelle Maschine aus und dann wieder ein. Stellen Sie sicher, dass CBT aktiviert ist. Führen Sie das Backup dann erneut durch.

Erweitertes DynamoDB-Backup

AWS Backup unterstützt zusätzliche, erweiterte Funktionen für Ihre Amazon DynamoDB DynamoDB-Datenschutzanforderungen. Nachdem Sie die erweiterten Funktionen in Ihrem aktiviert AWS Backup

haben AWS-Region, entsperren Sie die folgenden Funktionen für alle neuen Tabellensicherungen für DynamoDB, die Sie erstellen:

- Kosteneinsparungen und Optimierung:
  - Tiering von Backups in Cold Storage zur Senkung der Speicherkosten
  - Kostenzuordnungskennzeichnung zur Verwendung mit Cost Explorer
- Geschäftskontinuität:
  - Regionsübergreifende Kopie
  - Regionsübergreifende Kopie
- Sicherheit:
  - Speichern Sie Backups in verschlüsselten AWS Backup -Tresoren, die Sie mit AWS Backup -Vault-Lock, AWS Backup -Richtlinien und Verschlüsselungsschlüsseln sichern können.
  - Backups erben Tags aus ihren DynamoDB-Quelltabellen, sodass Sie diese Tags verwenden können, um Berechtigungen und Service-Kontrollrichtlinien (SCPs) festzulegen.

Bei Neukunden, die AWS Backup nach November 2021 einsteigen, sind die erweiterten DynamoDB-Backup-Funktionen standardmäßig aktiviert. Genauer gesagt, erweiterte DynamoDB-Backup-Features sind standardmäßig für Kunden aktiviert, die vor dem 21. November 2021 keinen Backup-Tresor erstellt haben.

Wir empfehlen allen AWS Backup Bestandskunden, erweiterte Funktionen für DynamoDB zu aktivieren. Sobald Sie die erweiterten Features aktiviert haben, gibt es keinen Unterschied bei den Preisen für warmen Backup-Speicher. Sie können Geld sparen, indem Sie Backups auf Cold Storage verteilen und Ihre Kosten mithilfe von Tags zur Kostenzuweisung optimieren. Sie können auch damit beginnen, die Vorteile der AWS Backup Business Continuity- und Sicherheitsfunktionen zu nutzen.

> **Note**
>
> Wenn Sie anstelle der AWS Backup Standard-Servicerolle eine benutzerdefinierte Rolle oder Richtlinie verwenden, müssen Sie Ihrer benutzerdefinierten Rolle die folgenden Berechtigungsrichtlinien (oder die entsprechenden Berechtigungen) hinzufügen oder verwenden:
>
> - `AWSBackupServiceRolePolicyForBackup` für das Durchführen erweiterter DynamoDB-Backups.

- `AWSBackupServiceRolePolicyForRestores` für das Wiederherstellen erweiterter DynamoDB-Backups.

Weitere Informationen zu AWS-verwalteten Richtlinien und Beispiele für von Kunden verwaltete Richtlinien finden Sie unter. Verwaltete Richtlinien für AWS Backup

Themen

Aktivieren erweiterter DynamoDB-Backups über die Konsole

Sie können AWS Backup erweiterte Funktionen für DynamoDB-Backups entweder mit der AWS Backup oder der DynamoDB-Konsole aktivieren.

Gehen Sie wie folgt vor, um erweiterte DynamoDB-Backup-Funktionen von der AWS Backup Konsole aus zu aktivieren:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsmenü Einstellungen.
3. Vergewissern Sie sich im Abschnitt Unterstützte Dienste, dass DynamoDB aktiviert ist.

   Ist dies nicht der Fall, wählen Sie Opt-In und aktivieren Sie DynamoDB als AWS Backup -unterstützten Dienst.
4. Wählen Sie im Abschnitt Erweiterte Features für DynamoDB-Backups die Option Aktivieren aus.
5. Klicken Sie auf Enable features (Funktionen aktivieren).

Informationen zur Aktivierung AWS Backup erweiterter Funktionen mithilfe der DynamoDB-Konsole finden Sie unter AWS Backup Funktionen aktivieren im Amazon DynamoDB DynamoDB-Benutzerhandbuch.

Programmgesteuertes Aktivieren erweiterter DynamoDB-Backups

Sie können auch AWS Backup erweiterte Funktionen für DynamoDB-Backups mithilfe der AWS Command Line Interface (CLI) aktivieren. Sie aktivieren erweiterte DynamoDB-Backups, wenn Sie die beiden folgenden Werte auf `true` setzen:

So aktivieren Sie programmgesteuert AWS Backup erweiterte Funktionen für DynamoDB-Backups:

1. Prüfen Sie mit dem folgenden Befehl, ob Sie bereits AWS Backup erweiterte Funktionen für DynamoDB aktiviert haben:

   ```
   $ aws backup describe-region-settings
   ```

   Wenn `"DynamoDB":true` sowohl für `"ResourceTypeManagementPreference"` als auch für `"ResourceTypeOptInPreference"` zutrifft, haben Sie das erweiterte DynamoDB-Backup bereits aktiviert.

   Wenn – wie in der folgenden Ausgabe – mindestens eine `"DynamoDB":false`-Instance vorhanden, das erweiterte DynamoDB-Backup jedoch noch nicht aktiviert ist, fahren Sie mit dem nächsten Schritt fort.

   ```
   {
     "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. Verwenden Sie den folgenden UpdateRegionSettings-Vorgang, um sowohl für "ResourceTypeManagementPreference" als auch für "ResourceTypeOptInPreference" "DynamoDB":true festzulegen:

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

Bearbeiten eines erweiterten DynamoDB-Backups

Wenn Sie ein DynamoDB-Backup erstellen, nachdem Sie AWS Backup erweiterte Funktionen aktiviert haben, können Sie Folgendes verwenden AWS Backup :

- Regionsübergreifendes Kopieren eines Backups
- Kontoübergreifendes Kopieren eines Backups
- Ändern Sie, wann ein AWS Backup Backup dem Cold Storage zugewiesen wird
- Markieren des Backups

Informationen zur Verwendung dieser erweiterten Features für ein vorhandenes Backup finden Sie unter Ein Backup bearbeiten.

Wenn Sie später AWS Backup erweiterte Funktionen für DynamoDB deaktivieren, können Sie diese Operationen weiterhin für DynamoDB-Backups ausführen, die Sie in dem Zeitraum erstellt haben, in dem Sie die erweiterten Funktionen aktiviert haben.

Bearbeiten eines erweiterten DynamoDB-Backups

Sie können DynamoDB-Backups, die mit aktivierten AWS Backup erweiterten Funktionen erstellt wurden, genauso wiederherstellen wie DynamoDB-Backups, die vor der Aktivierung der erweiterten Funktionen erstellt wurden. AWS Backup Sie können eine Wiederherstellung entweder mit DynamoDB AWS Backup oder mit DynamoDB durchführen.

Sie können mit den folgenden Optionen angeben, wie Ihre neu wiederhergestellte Tabelle verschlüsselt werden soll:

- Wenn Sie in derselben Region wie Ihre Originaltabelle wiederherstellen, können Sie optional einen Verschlüsselungsschlüssel für Ihre wiederhergestellte Tabelle angeben. Wenn Sie keinen Verschlüsselungsschlüssel angeben, AWS Backup wird Ihre wiederhergestellte Tabelle automatisch mit demselben Schlüssel verschlüsselt, mit dem Ihre ursprüngliche Tabelle verschlüsselt wurde.
- Wenn Sie in einer anderen Region als Ihrer Originaltabelle wiederherstellen, müssen Sie einen Verschlüsselungsschlüssel angeben.

Informationen zur Wiederherstellung mit finden Sie AWS Backup unterWiederherstellen einer Amazon-DynamoDB-Tabelle.

Informationen zur Wiederherstellung mit DynamoDB finden Sie unter Wiederherstellen einer DynamoDB-Tabelle aus einem Backup im Amazon-DynamoDB-Benutzerhandbuch.

Löschen eines erweiterten DynamoDB-Backups

Sie können keine Backups löschen, die mit diesen erweiterten Features in DynamoDB erstellt wurden. Sie müssen AWS Backup zum Löschen von Backups verwenden, um die globale Konsistenz in Ihrer gesamten AWS -Umgebung aufrechtzuerhalten.

Informationen zum Löschen eines DynamoDB-Backups finden Sie unter Löschen eines Backups.

Weitere Vorteile der vollständigen AWS Backup -Verwaltung, wenn Sie das erweiterte DynamoDB-Backup aktivieren

Wenn Sie AWS Backup erweiterte Funktionen für DynamoDB aktivieren, übertragen Sie die vollständige Verwaltung Ihrer DynamoDB-Backups auf. AWS Backup Auf diese Weise erhalten Sie die folgenden zusätzlichen Vorteile:

Verschlüsselung

AWS Backup verschlüsselt die Backups automatisch mit dem KMS-Schlüssel Ihres Zieltresors. AWS Backup Zuvor wurden sie mit derselben Verschlüsselungsmethode wie Ihre DynamoDB-Quelltabelle verschlüsselt. Dadurch erhöht sich die Anzahl der Schutzmaßnahmen, die Sie zum Schutz Ihrer Daten einsetzen können. Weitere Informationen finden Sie unter Verschlüsselung für Backups in AWS Backup.

Amazon-Ressourcenname (ARN)

Der Dienst-Namespace jedes Backup-ARN lautet `awsbackup`. Zuvor war der Dienst-Namespace `dynamodb`. Anders ausgedrückt, der Anfang jedes ARN ändert sich von `arn:aws:dynamodb` auf `arn:aws:backup`. Weitere Informationen finden Sie unter ARNs für AWS Backup in der Service Authorization Reference.

Mit dieser Änderung können Sie oder Ihr Backup-Administrator mithilfe von `awsbackup`-Dienst-Namespace Zugriffsrichtlinien für Backups erstellen, die jetzt für DynamoDB-Backups gelten, die nach der Aktivierung erweiterter Features erstellt wurden. Mithilfe des `awsbackup`-Dienst-Namespace können Sie Richtlinien auch auf andere Backups anwenden, die von AWS Backup erstellt wurden. Weitere Informationen finden Sie unter Zugriffskontrolle.

Gebührenposten auf dem Rechnungsauszug

Gebühren für Backups (einschließlich Speicherung, Datenübertragungen, Wiederherstellungen und vorzeitiges Löschen) werden in Ihrer AWS Rechnung unter „Backup“ ausgewiesen. Bisher waren Gebühren in Ihrer Rechnung unter „DynamoDB“ aufgeführt.

Diese Änderung stellt sicher, dass Sie die AWS Backup Abrechnung verwenden können, um Ihre Backup-Kosten zentral zu überwachen. Weitere Informationen finden Sie unter Messung, Kosten und Abrechnung.

Amazon-Timestream-Backups

Amazon Timestream ist eine skalierbare Zeitreihendatenbank, die die Speicherung und Analyse von bis zu Billionen von Zeitreihendatenpunkten täglich ermöglicht. Timestream ist im Hinblick auf Kosten- und Zeiteinsparungen optimiert, indem aktuelle Daten im Arbeitsspeicher aufbewahrt und Verlaufsdaten gemäß Ihren Richtlinien auf einer kostenoptimierten Speicherebene gespeichert werden.

Eine Timestream-Datenbank enthält Tabellen. Diese Tabellen enthalten Datensätze, und jeder Datensatz ist ein einzelner Datenpunkt in einer Zeitreihe. Eine Zeitreihe ist eine Folge von Datensätzen, die über ein Zeitintervall aufgezeichnet wurden, z. B. ein Aktienkurs, die Speichernutzung einer Amazon EC2 EC2-Instance oder ein Temperaturmesswert. AWS Backup kann Timestream-Tabellen zentral sichern und wiederherstellen. Sie können diese Tabellensicherungen auf andere Konten und mehrere andere AWS-Regionen innerhalb derselben Organisation kopieren.

Timestream bietet derzeit keine systemeigenen Sicherungs- und Wiederherstellungsdienste AWS Backup an. Wenn Sie also sichere Kopien Ihrer Timestream-Tabellen erstellen, können Sie Ihren Ressourcen eine zusätzliche Sicherheits- und Ausfallsicherheit verleihen.

Backup von Timestream-Tabellen

Sie können Timestream-Tabellen entweder über die AWS Backup Konsole oder über die sichern. AWS CLI

Es gibt zwei Möglichkeiten, die AWS Backup Konsole zum Sichern einer Timestream-Tabelle zu verwenden: bei Bedarf oder als Teil eines Backup-Plans.

Erstellen von On-Demand-Timestream-Backups

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und anschließend On-Demand-Backup erstellen aus.
3. Wählen Sie auf der Seite On-Demand-Backup erstellen die Option Amazon Timestream aus.
4. Wählen Sie den Ressourcentyp Timestream und dann den Tabellennamen, den Sie sichern möchten.
5. Stellen Sie sicher, dass Backup jetzt erstellen ausgewählt ist. Dies löst sofort ein Backup aus und ermöglicht Ihnen, Ihr Cluster früher auf der Seite Geschützte Ressourcen zu sehen.
6. Im Dropdown-Menü Übergang zur Kühllagerung können Sie Ihre Übergangseinstellungen festlegen.
7. Unter Aufbewahrungszeitraum können Sie wählen, wie lange Ihr Backup aufbewahrt werden soll.
8. Wählen Sie einen vorhandenen Backup-Tresor aus oder erzeugen Sie einen neuen. Bei Auswahl von Create new backup vault (Neuen Sicherungstresor auswählen) wird eine neue Seite für die Erstellung des Tresors geöffnet; anschließend kehren Sie zur Seite Create on-demand backup (On-Demand-Sicherung erstellen) zurück.
9. Wählen Sie unter IAM-Rolle die Option Standardrolle aus (wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird sie mit den richtigen Berechtigungen für Sie erstellt).
10. Optional können Sie Tags zu Ihrem Wiederherstellungspunkt hinzufügen. Wenn Sie Ihrer On-Demand-Sicherung einen oder mehrere Tags zuweisen möchten, geben Sie einen key (Schlüssel) und optional einen value (Wert) ein und wählen Sie Add tag (Tag hinzufügen).
11. Wählen Sie On-Demand-Backup erstellen. Dadurch gelangen Sie zur Seite Jobs (Aufträge), die eine Liste von Aufträgen anzeigt.
12. Wählen Sie die Backup-Auftrags-ID für das Cluster, um die Details dieses Auftrags anzuzeigen. Es wird der Status `Completed`, `In Progress` oder `Failed` angezeigt. Sie können auf das Symbol „Aktualisieren“ klicken, um den Status zu aktualisieren.

Erstellen geplanter Timestream-Backups in einem Backup-Plan

Ihre geplanten Backups können Timestream-Tabellen enthalten, sofern es sich um eine geschützte Ressource handelt. So aktivieren Sie den Schutz von Amazon-Timestream-Tabellen:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Schalten Sie Amazon Timestream auf Ein.
4. Weitere Informationen zum Aufnehmen von Timestream-Tabellen in einen vorhandenen oder neuen Plan finden Sie unter Zuweisen von Ressourcen zu einer Konsole.

Unter Backup-Pläne verwalten können Sie wählen, ob Sie einen Backup-Plan erstellen und Timestream-Tabellen einbeziehen möchten, oder Sie können einen vorhandenen Plan so aktualisieren, dass er Timestream-Tabellen enthält. Wenn Sie den Ressourcentyp Timestream hinzufügen, können Sie wählen, ob Sie alle Timestream-Tabellen hinzufügen möchten, oder unter Bestimmte Ressourcentypen auswählen die Kästchen neben den Tabellen aktivieren, die Sie hinzufügen möchten.

Beim ersten Backup der Timestream-Tabellen handelt es sich um ein vollständiges Backup. Nachfolgende Backups werden inkrementelle Backups sein.

Sobald Sie Ihren Backup-Plan erstellt oder geändert haben, navigieren Sie in der linken Navigationsleiste zu Backup-Pläne. In dem von Ihnen angegebenen Backup-Plan sollten Ihre Cluster unter Ressourcenzuweisungen angezeigt werden.

Programmgesteuerte Backups

Sie können auch den Vorgangsnamen `start-backup-job` verwenden. Verwenden Sie die folgenden Parameter:

```
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-Region \
--endpoint-url URL
```

Anzeigen von Timestream-Tabellen-Backups

So können Sie Ihre Timestream-Tabellen-Backups in der Konsole anzeigen und ändern:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie Backup vaults (Sicherungstresore) aus. Klicken Sie dann auf den Namen des Backup-Tresors, der Ihre Timestream-Tabellen enthält.
3. Im Backup-Tresor werden eine Zusammenfassung und eine Liste der Backups angezeigt.

    a. Sie können auf den Link in der Spalte Wiederherstellungspunkt-ID klicken, oder

    b. Sie können das Kästchen links neben der Wiederherstellungspunkt-ID aktivieren und auf Aktionen klicken, um die Wiederherstellungspunkte zu löschen, die nicht mehr benötigt werden.

Wiederherstellen einer Timestream-Tabelle

Informationen zum Wiederherstellen einer Timestream-Tabelle

Backup von SAP-HANA-Datenbanken auf Amazon-EC2-Instances

> **Note**
>
> Unterstützte Dienste von AWS-Regionenthält die derzeit unterstützten Regionen, in denen SAP HANA-Datenbanksicherungen auf Amazon EC2 EC2-Instances verfügbar sind.

AWS Backup unterstützt Backups und Wiederherstellungen von SAP HANA-Datenbanken auf Amazon EC2 EC2-Instances.

Themen

- Überblick über SAP HANA-Datenbanken mit AWS Backup
- Voraussetzungen für die Sicherung von SAP HANA-Datenbanken über AWS Backup
- SAP HANA-Backup-Operationen in der Konsole AWS Backup
- SAP HANA-Datenbank-Backups anzeigen
- Verwenden Sie AWS CLI für SAP HANA-Datenbanken mit AWS Backup
- Fehlerbehebung bei Backups von SAP HANA-Datenbanken

- Glossar der SAP HANA-Begriffe bei der Verwendung AWS Backup
- AWS Backup Versionshinweise zur Unterstützung von SAP HANA-Datenbanken auf EC2-Instances

Überblick über SAP HANA-Datenbanken mit AWS Backup

Neben der Möglichkeit, Backups zu erstellen und Datenbanken wiederherzustellen, ermöglicht es die AWS Backup -Integration mit Amazon EC2 Systems Manager für SAP den Kunden, SAP-HANA-Datenbanken zu identifizieren und zu kennzeichnen.

AWS Backup ist in AWS Backint Agent integriert, um SAP HANA-Backups und Wiederherstellungen durchzuführen. Weitere Informationen finden Sie unter AWS -Backint.

Voraussetzungen für die Sicherung von SAP HANA-Datenbanken über AWS Backup

Bevor Backup- und Wiederherstellungsaktivitäten durchgeführt werden können, müssen mehrere Voraussetzungen erfüllt sein. Beachten Sie, dass Sie Administratorzugriff auf Ihre SAP HANA-Datenbank und Berechtigungen benötigen, um neue IAM-Rollen und -Richtlinien in Ihrem AWS Konto zu erstellen, um diese Schritte ausführen zu können.

Erfüllen Sie diese Voraussetzungen bei Amazon EC2 Systems Manager.

1. Richten Sie die erforderlichen Berechtigungen für die Amazon-EC2-Instance ein, auf der die SAP-HANA-Datenbank ausgeführt wird
2. Registrieren Sie Ihre Anmeldedaten in AWS Secrets Manager
3. Installieren Sie AWS Backint und AWS Systems Manager für SAP-Agenten
4. Überprüfen Sie den SSM-Agenten
5. Überprüfen Sie die Parameter
6. Registrieren Sie die SAP-HANA-Datenbank

Es hat sich bewährt, jede HANA-Instanz nur einmal zu registrieren. Mehrere Registrierungen können zu mehreren ARNs für dieselbe Datenbank führen. Die Verwaltung eines einzigen ARN und einer Registrierung vereinfacht die Erstellung und Wartung von Backup-Plänen und kann auch dazu beitragen, ungeplante Duplizierungen von Backups zu reduzieren.

SAP HANA-Backup-Operationen in der Konsole AWS Backup

Sobald die Voraussetzungen erfüllt und Setups von SSM für SAP abgeschlossen sind, können Sie Ihr SAP HANA auf EC2-Datenbanken sichern und wiederherstellen.

Aktivieren des Schutzes von SAP-HANA-Ressourcen

Um Ihre SAP HANA-Datenbanken AWS Backup zu schützen, muss SAP HANA als eine der geschützten Ressourcen aktiviert sein. So melden Sie sich an:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie unter Serviceanmeldung die Option Ressourcen konfigurieren aus.
4. Melden Sie sich für SAP HANA auf Amazon EC2 an.
5. Klicken Sie auf Bestätigen.

Die Serviceanmeldung für SAP HANA auf Amazon EC2 wird jetzt aktiviert.

Erstellen Sie ein geplantes Backup der SAP HANA-Datenbanken

Sie können einen vorhandenen Backup-Plan bearbeiten und ihm SAP-HANA-Ressourcen hinzufügen, oder Sie können einen neuen Backup-Plan nur für SAP-HANA-Ressourcen erstellen.

Wenn Sie sich dafür entscheiden, einen neuen Backup-Plan zu erstellen, haben Sie drei Optionen:

1. Option 1: Beginnen Sie mit einer Vorlage
    1. Wählen Sie eine Backup-Plan-Vorlage aus.
    2. Geben Sie einen Backup-Plan an.
    3. Klicken Sie auf Plan erstellen.
2. Option 2: Erstellen Sie einen neuen Plan
    1. Geben Sie einen Backup-Plan an.
    2. Geben Sie optional Tags an, die dem Backup-Plan hinzugefügt werden sollen.
    3. Geben Sie die Konfiguration der Backup-Regel an.
        a. Geben Sie einen Namen für die Backup-Regel an.

   b. Wählen Sie einen vorhandenen Backup-Tresor aus oder erstellen Sie einen neuen. Hier werden Ihre Backups gespeichert.
   c. Geben Sie eine Backup-Frequenz an.
   d. Geben Sie ein Backup-Fenster an.

      Beachten Sie, dass der Übergang zu Cold Storage derzeit nicht unterstützt wird.
   e. Geben Sie den Aufbewahrungszeitraum an.

      Das Kopieren an das Ziel wird derzeit nicht unterstützt
   f. (Optional) Geben Sie Tags an, die den Wiederherstellungspunkten hinzugefügt werden sollen.
4. Klicken Sie auf Plan erstellen.

3. Option 3: Definieren eines Plans mit JSON

   1. Geben Sie das JSON für Ihren Backup-Plan an, indem Sie entweder den JSON-Ausdruck eines vorhandenen Backup-Plans ändern oder einen neuen Ausdruck erstellen.
   2. Geben Sie einen Backup-Plan an.
   3. Klicken Sie auf JSON validieren.

   Sobald der Backup-Plan erfolgreich erstellt wurde, können Sie dem Backup-Plan im nächsten Schritt Ressourcen zuweisen.

Welchen Plan Sie auch verwenden, stellen Sie sicher, dass Sie Ressourcen zuweisen. Sie können wählen, welche SAP-HANA-Datenbanken zugewiesen werden sollen, einschließlich System- und Mandantendatenbanken. Sie haben auch die Möglichkeit, bestimmte Ressourcen-IDs auszuschließen.

Erstellen Sie ein On-Demand-Backup von SAP HANA-Datenbanken

Sie können ein vollständiges On-Demand-Backup erstellen, das unmittelbar nach der Erstellung ausgeführt wird. Beachten Sie, dass On-Demand-Backups von SAP-HANA-Datenbanken auf Amazon-EC2-Instances vollständige Backups sind; inkrementelle Backups werden nicht unterstützt.

Ihr On-Demand-Backup ist jetzt erstellt. Es beginnt mit dem Backup Ihrer angegebenen Ressourcen. Die Konsole leitet Sie zur Seite Backup-Aufträge weiter, auf der Sie den Fortschritt verfolgen können. Notieren Sie sich die Backup-Auftrags-ID auf dem blauen Banner oben auf Ihrem Bildschirm, da

Sie sie benötigen, um den Status Ihres Backup-Auftrags leicht zu ermitteln. Wenn das Backup abgeschlossen ist, wechselt der Status zu `Completed`. Backups können mehrere Stunden dauern.

Aktualisieren Sie die Liste der Backup-Aufträge, um die Statusänderung zu sehen. Sie können auch nach Ihrer Backup-Auftrags-ID suchen und darauf klicken, um den detaillierten Auftragsstatus zu sehen.

Kontinuierliche Backups von SAP-HANA-Datenbanken

Sie können fortlaufende Backups erstellen, die zusammen mit point-in-time Restore (PITR) verwendet werden können (beachten Sie, dass bei On-Demand-Backups Ressourcen in dem Zustand erhalten bleiben, in dem sie abgerufen wurden, wohingegen PITR kontinuierliche Backups verwendet, bei denen Änderungen über einen bestimmten Zeitraum aufgezeichnet werden).

Mit kontinuierlichen Backups können Sie Ihre SAP-HANA-Datenbank auf einer EC2-Instance bis zu einem bestimmten, von Ihnen gewählten, Zeitpunkt zurückspulen, bis auf 1 Sekunde genau (innerhalb der letzten 35 Tage). Bei kontinuierlichen Backups wird zunächst ein vollständiges Backup Ihrer Ressource erstellt und anschließend die Transaktionsprotokolle Ihrer Ressource kontinuierlich gesichert. Bei der PITR-Wiederherstellung wird auf Ihr vollständiges Backup zugegriffen und das Transaktionsprotokoll bis zu dem Zeitpunkt wiedergegeben, zu dem Sie für die Wiederherstellung angegeben haben. AWS Backup

Sie können sich für kontinuierliche Backups entscheiden, wenn Sie AWS Backup mithilfe der AWS Backup Konsole oder der API einen Backup-Plan erstellen.

Aktivieren des kontinuierlichen Backups mithilfe der Konsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie im Hauptnavigationsbereich auf Backup-Pläne und auf Backup-Plan erstellen.
3. Wählen Sie unter Backup-Regeln die Option Backup-Regel hinzufügen aus.
4. Wählen Sie im Abschnitt Konfiguration der Backup-Regeln die Option Fortlaufende Backups aktivieren für unterstützte Ressourcen aus.

Nachdem Sie PITR (point-in-timeWiederherstellung) für SAP HANA-Datenbanksicherungen deaktiviert haben, werden weiterhin Protokolle an gesendet, AWS Backup bis der Wiederherstellungspunkt abläuft (Status entsprichtEXPIRED). Um die Übertragung der Protokolle an AWS Backup zu beenden, können Sie in SAP HANA einen alternativen Protokoll-Backup-Speicherort festlegen.

Ein kontinuierlicher Wiederherstellungspunkt mit dem Status von `STOPPED` gibt an, dass ein kontinuierlicher Wiederherstellungspunkt unterbrochen wurde. Das heißt, die von SAP HANA an diese übermittelten Protokolle, die zeigen, AWS Backup dass die inkrementellen Änderungen an einer Datenbank zeigen, eine Lücke aufweisen. Die Wiederherstellungspunkte, die innerhalb dieser Zeitrahmenlücke auftreten, haben den Status `STOPPED`..

Informationen zu Problemen, die bei der Wiederherstellung kontinuierlicher Backups (Wiederherstellungspunkte) auftreten können, finden Sie im Abschnitt zur Problembehebung bei der Wiederherstellung von SAP HANA in diesem Handbuch.

SAP HANA-Datenbank-Backups anzeigen

Anzeigen des Status von Backup- und Wiederherstellungsaufträgen:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie Backup-, Wiederherstellungs- oder Kopieraufträge, um die Liste Ihrer Aufträge zu sehen.
4. Suchen Sie nach Ihrer Backup-Auftrags-ID und klicken Sie darauf, um den detaillierten Auftragsstatus zu sehen.

Alle Wiederherstellungspunkte in einem Tresor anzeigen:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Suchen Sie nach einem Backup-Tresor und klicken Sie darauf, um alle Wiederherstellungspunkte im Tresor anzuzeigen.

Anzeigen der Details geschützter Ressourcen:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Sie können auch nach Ressourcentyp filtern, um alle Backups dieses Ressourcentyps anzuzeigen.

Verwenden Sie AWS CLI für SAP HANA-Datenbanken mit AWS Backup

Jede Aktion in der Backup-Konsole hat einen entsprechenden API-Aufruf.

Verwenden Sie den API-Aufruf, um eine SAP HANA-Datenbank auf einer `StartBackupJob`EC2-Instance programmgesteuert zu konfigurieren AWS Backup und zu verwalten.

Verwenden Sie `start-backup-job` als CLI-Befehl.

Fehlerbehebung bei Backups von SAP HANA-Datenbanken

Wenn Sie während Ihres Workflows auf Fehler stoßen, sehen Sie sich die folgenden Beispielfehler und Lösungsvorschläge an:

Python-Voraussetzungen

- Fehler: Der Zypper-Fehler bezieht sich auf die Python-Version seit SSM für SAP und AWS Backup erfordert Python 3.6, aber SUSE 12 SP5 unterstützt standardmäßig Python 3.4.

  Lösung: Installieren Sie mehrere Versionen von Python auf SUSE12 SP5, indem Sie die folgenden Schritte ausführen:

  1. Führen Sie einen Befehl update-alternatives aus, um einen Symlink für Python 3 in '/usr/local/bin/' zu erstellen, anstatt '/usr/bin/python3' direkt zu verwenden. Mit diesen Befehlen wird Python 3.4 als Standardversion festgelegt. Der Befehl lautet: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. Fügen Sie Python 3.6 zur alternativen Konfiguration hinzu, indem Sie den folgenden Befehl ausführen: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. Ändern Sie die alternative Konfiguration zu Python 3.6, indem Sie den folgenden Befehl ausführen: `# sudo update-alternatives –config python3`

     Die folgende Ausgabe sollte angezeigt werden:

     ```
     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. Geben Sie die Zahl ein, die Python 3.6 entspricht.

5. Überprüfen Sie die Python-Version und stellen Sie sicher, dass Python 3.6 verwendet wird.
6. (Optional, aber empfohlen) Stellen Sie sicher, dass die Zypper-Befehle wie erwartet funktionieren.

Amazon EC2 Systems Manager für SAP-Erkennung und Registrierung

- Fehler: SSM für SAP konnte die Arbeitslast aufgrund eines blockierten Zugriffs auf öffentliche Endpunkte für AWS Secrets Manager und SSM nicht erkennen.

  Lösung: Testen Sie, ob Endpunkte von Ihrer SAP HANA-Datenbank aus erreichbar sind. Wenn sie nicht erreicht werden können, können Sie Amazon VPC-Endpunkte für AWS Secrets Manager und SSM für SAP erstellen.

  1. Testen Sie den Zugriff auf Secrets Manager vom Amazon EC2 EC2-Host für HANA DB aus, indem Sie den folgenden Befehl ausführen:`aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp`. Wenn der Befehl keinen Wert zurückgibt, blockiert die Firewall den Zugriff auf den Secrets Manager Manager-Dienstendpunkt. Das Protokoll wird bei dem Schritt „Geheimnisse aus Secrets Manager abrufen“ beendet.
  2. Testen Sie die Konnektivität zum SSM-Endpunkt für SAP, indem Sie den Befehl ausführen. `aws ssm-sap list-registration` Wenn der Befehl keinen Wert zurückgibt, blockiert die Firewall den Zugriff auf den SSM for SAP-Endpunkt.

     Beispiel für einen Fehler:`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`.

  Es gibt zwei Möglichkeiten, fortzufahren, wenn die Endpunkte nicht erreichbar sind.

  - Firewall-Ports öffnen, um den Zugriff auf öffentliche Dienstendpunkte für Secrets Manager und SSM für SAP zu ermöglichen; oder
  - Erstellen Sie VPC-Endpoints für Secrets Manager und SSM für SAP und gehen Sie dann wie folgt vor:
    - Stellen Sie sicher, dass Amazon VPC für DNSSupport und DNSHostName aktiviert ist.
    - Stellen Sie sicher, dass Ihr VPC-Endpunkt die Option Privaten DNS-Namen zulassen aktiviert hat.
    - Wenn die SSM for SAP-Erkennung erfolgreich abgeschlossen wurde, wird im Protokoll angezeigt, dass der Host erkannt wurde.

- Fehler: AWS Backup Und die Backint-Verbindung schlägt fehl, weil der Zugriff auf öffentliche AWS Backup Dienstendpunkte blockiert ist. `aws-backint-agent.log`kann ähnliche Fehler anzeigen: `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id"` oder. `level=fatal msg="Error performing backup missing backup data plane Id` Außerdem kann die AWS Backup Konsole Folgendes anzeigen `Fatal Error: An internal error occured.`

  Lösung: Es gibt zwei Möglichkeiten, fortzufahren, falls die Endpunkte nicht erreichbar sind:

  - Öffnen Sie Firewall-Ports, um den Zugriff auf Endpunkte des öffentlichen Dienstes (HTTPS) zu ermöglichen. Nachdem diese Option verwendet wurde, löst DNS Anfragen an AWS Dienste über öffentliche IP-Adressen auf.
  - Erstellen Sie VPC-Endpunkte, leiten Sie den Datenverkehr privat zu und von AWS Diensten weiter, für die erforderlich ist. AWS Backup Nachdem diese Option verwendet wurde, löst DNS Anfragen für diese Dienste über private IP-Adressen auf. Für diese Option sind möglicherweise Aktualisierungen des DNS-Servers erforderlich, um Regeln für die Weiterleitung von Anfragen an private Endpunkte hinzuzufügen.
- Fehler: Die SSM-Registrierung für SAP schlägt fehl, weil das HANA-Passwort Sonderzeichen enthält. Zu den Fehlern kann es sich beispielsweise um `Error connecting to database HBX/HBX when validating its credentials.` oder `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` nach dem Testen einer Verbindung handeln`tenantdb`, `hdbsql` bei der eine Amazon EC2 EC2-Instance der HANA-Datenbank verwendet wurde `systemdb` und die von dort aus getestet wurde.

  In der AWS Backup Konsole auf der Seite „Jobs“ können die Details des Backup-Jobs den Status „`FAILED`Mit dem Fehler`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`“ anzeigen.

  Lösung: Stellen Sie sicher, dass Ihr Passwort keine Sonderzeichen wie $ enthält.
- Fehler: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Lösung: Die Installation des AWS BackInt Agenten für SAP HANA wurde möglicherweise nicht erfolgreich abgeschlossen. Versuchen Sie erneut, den AWS Backint Agent und den Amazon EC2 Systems Manager Agent auf Ihrem SAP-Anwendungsserver bereitzustellen.
- Fehler: Die Konsole stimmt nach der Registrierung nicht mit den Protokolldateien überein.

Das Erkennungsprotokoll zeigt, dass die Registrierung beim Versuch, eine Verbindung zu HANA DB herzustellen, fehlgeschlagen ist, da das Passwort Sonderzeichen enthält. Die SSM-Konsole für SAP Application Manager für SAP zeigt jedoch eine erfolgreiche Registrierung an. Es bestätigt nicht, dass die Registrierung erfolgreich war. Wenn in der Konsole eine erfolgreiche Registrierung angezeigt wird, in den Protokollen jedoch nicht, schlagen Backups fehl.

Bestätigen Sie den Registrierungsstatus:

1. Loggen Sie sich in die SSM-Konsole ein
2. Wählen Sie in der linken Navigationsleiste Befehl ausführen aus.
3. Geben Sie im Textfeld Befehlsverlauf den Wert ein`Instance ID:Equal:`, der der Instanz entspricht, die Sie für die Registrierung verwendet haben. Dadurch wird der Befehlsverlauf gefiltert.
4. Verwenden Sie die Spalte mit der Befehls-ID, um Befehle mit Status zu finden`Failed`. Suchen Sie dann den Dokumentnamen AWSSystemsManagerSAP-Discovery.
5. Führen Sie im den AWS CLI Befehl `aws ssm-sap register-application status` aus. Wenn der zurückgegebene Wert angezeigt `Error` wird, war die Registrierung nicht erfolgreich.

Lösung: Stellen Sie sicher, dass Ihr HANA-Passwort keine Sonderzeichen (wie '$') enthält.

Erstellen einer Sicherungskopie einer SAP HANA-Datenbank

- Fehler: Die AWS Backup Konsole zeigt die Meldung „Schwerwiegender Fehler“ an, wenn ein On-Demand-Backup für SystemDB oder TenantDB erstellt wird. Dies liegt daran, dass auf den öffentlichen Endpunkt cell-1.prod.us-west-2.storage.cryo.aws.a2z.com nicht zugegriffen werden kann. Dies wird durch eine clientseitige Firewall verursacht, die den Zugriff auf diesen Endpunkt blockiert.

  `aws-backint-agent.log`kann Fehler wie `level=error msg="Storage configuration validation failed: missing backup data plane Id"` oder anzeigen `level=fatal msg="Error performing backup missing backup data plane Id."`

  Lösung: Öffnen Sie den Firewall-Zugriff auf den öffentlichen Endpunkt cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.
- **`Database cannot be backed up while it is stopped`**Fehler:.

Lösung: Stellen Sie sicher, dass die zu sichernde Datenbank aktiv ist. Datenbankdaten und -protokolle können nur gesichert werden, während die Datenbank online ist.

- Fehler: `Getting backup metadata failed. Check the SSM document execution for more details.`

  Lösung: Stellen Sie sicher, dass die zu sichernde Datenbank aktiv ist. Datenbankdaten und -protokolle können nur gesichert werden, während die Datenbank online ist.

Überwachung von Backup-Protokollen

- Fehler: `Encountered an issue with log backups, please check SAP HANA for details.`

  Lösung: Überprüfen Sie SAP HANA, um sicherzustellen, dass Protokollsicherungen AWS Backup von SAP HANA aus gesendet werden.
- Fehler: `One or more log backup attempts failed for recovery point.`

  Lösung: Überprüfen Sie SAP HANA auf Details. Stellen Sie sicher, dass Protokollsicherungen AWS Backup von SAP HANA aus gesendet werden.
- Fehler: `Unable to determine the status of log backups for recovery point.`

  Lösung: Überprüfen Sie SAP HANA auf Details. Stellen Sie sicher, dass Protokollsicherungen AWS Backup von SAP HANA aus gesendet werden.
- Fehler: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Lösung: Warten Sie, bis der Wiederherstellungsauftrag abgeschlossen ist. Die Protokoll-Backups sollten fortgesetzt werden.

Glossar der SAP HANA-Begriffe bei der Verwendung AWS Backup

Datensicherungstypen: SAP HANA unterstützt zwei Arten von Datensicherungen: Vollständige und INC-Datensicherungen (inkrementell). AWS Backup optimiert, welcher Typ bei jedem Backup-Vorgang verwendet wird.

Katalog-Backups: SAP HANA verwaltet ein eigenes Manifest, das als Katalog bezeichnet wird. AWS Backup interagiert mit diesem Katalog. Jedes neue Backup erstellt einen Eintrag im Katalog.

Kontinuierliche Protokoll-Backups (Transaktionsprotokolle): Für PITR-Features (zeitpunktbezogene Wiederherstellung) verfolgt SAP HANA alle Transaktionen seit dem letzten Backup.

Systemkopie: Ein Wiederherstellungsauftrag, bei dem sich die Zieldatenbank für die Wiederherstellung von der Quelldatenbank unterscheidet, aus der der Wiederherstellungspunkt erstellt wurde.

Destruktive Wiederherstellung: Eine destruktive Wiederherstellung ist eine Art von Wiederherstellungsauftrag, bei dem eine wiederhergestellte Datenbank die Quell- oder bestehende Datenbank löscht oder überschreibt.

VOLLSTÄNDIG: Eine vollständiges Backup ist das Backup einer vollständigen Datenbank.

INC: Ein inkrementelles Backup ist ein Backup aller Änderungen an einer SAP-HANA-Datenbank seit dem vorherigen Backup.

Weitere Details finden Sie im AWS -Glossar.

AWS Backup Versionshinweise zur Unterstützung von SAP HANA-Datenbanken auf EC2-Instances

Bestimmte Features werden derzeit nicht unterstützt:

- Regionsübergreifendes und kontoübergreifendes Kopieren wird nicht unterstützt.
- Backup Audit Manager und Reporting werden derzeit nicht unterstützt.
- Unterstützte Dienste von AWS-Regionenthält die derzeit unterstützten Regionen für SAP HANA-Datenbank-Backups auf Amazon EC2 EC2-Instances.

Amazon-Redshift-Backups

Amazon Redshift ist ein vollständig verwaltetes, skalierbares Cloud-Data-Warehouse, mit dem Sie mit schnellen, einfachen und sicheren Analysen schneller Erkenntnisse gewinnen können. Sie können AWS Backup damit Ihre Data Warehouses mit unveränderlichen Backups, separaten Zugriffsrichtlinien und zentraler organisatorischer Steuerung von Sicherungs- und Wiederherstellungsaufträgen schützen.

Ein Amazon Redshift Data Warehouse ist eine Sammlung von Rechenressourcen, die als Knoten bezeichnet werden und in einer Gruppe organisiert sind, die als Cluster bezeichnet wird. AWS Backup kann diese Cluster sichern.

Informationen zu Amazon Redshift finden Sie im Benutzerhandbuch zu ersten Schritten mit Amazon Redshift, im Datenbankentwicklerhandbuch für Amazon Redshift und im Cluster-Management-Handbuch für Amazon Redshift.

Backup für von Amazon Redshift bereitgestellte Cluster

Sie können Ihre Amazon Redshift Redshift-Cluster mithilfe der AWS Backup Konsole oder programmgesteuert mithilfe von API oder CLI schützen. Diese Cluster können im Rahmen eines Backup-Plans nach einem regelmäßigen Zeitplan gesichert werden, oder sie können nach Bedarf über ein On-Demand-Backup gesichert werden.

Sie können eine einzelne Tabelle (auch als Wiederherstellung auf Elementebene bezeichnet) oder ein ganzes Cluster wiederherstellen. Beachten Sie, dass Tabellen nicht eigenständig gesichert werden können. Tabellen werden als Teil eines Clusters gesichert, wenn der Cluster gesichert wird.

Durch die Verwendung AWS Backup können Sie Ihre Ressourcen zentral anzeigen. Wenn Amazon Redshift jedoch die einzige Ressource ist, die Sie verwenden, können Sie weiterhin den automatisierten Snapshot-Scheduler in Amazon Redshift verwenden. Beachten Sie, dass Sie manuelle Snapshot-Einstellungen nicht weiterhin mit Amazon Redshift verwalten können, wenn Sie diese über AWS Backup verwalten möchten.

Sie können Amazon Redshift Redshift-Cluster entweder über die AWS Backup Konsole oder mit dem AWS CLI sichern.

Es gibt zwei Möglichkeiten, die AWS Backup Konsole zum Sichern eines Amazon Redshift Redshift-Clusters zu verwenden: bei Bedarf oder als Teil eines Backup-Plans.

Erstellen von Amazon-Redshift-On-Demand-Backups

Weitere Informationen finden Sie auf der Seite Erstellen eines On-Demand-Backup-Typs.

Um einen manuellen Snapshot zu erstellen, lassen Sie das Kontrollkästchen „Kontinuierliches Backup“ deaktiviert, wenn Sie einen Backup-Plan erstellen, der Amazon-Redshift-Ressourcen umfasst.

Erstellen geplanter Amazon-Redshift-Backups in einem Backup-Plan

Ihre geplanten Backups können Amazon-Redshift-Cluster enthalten, sofern es sich um eine geschützte Ressource handelt. So aktivieren Sie den Schutz von Amazon-Redshift-Tabellen:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Schalten Sie Amazon Redshift auf Ein.
4. Weitere Informationen zum Aufnehmen von Amazon-Redshift-Clustern in einen vorhandenen oder neuen Plan finden Sie unter Zuweisen von Ressourcen zu einer Konsole.

Unter Backup-Pläne verwalten können Sie wählen, ob Sie einen Backup-Plan erstellen und Amazon-Redshift-Cluster einbeziehen möchten, oder Sie können einen vorhandenen Plan so aktualisieren, dass er Amazon-Redshift-Cluster enthält. Wenn Sie den Ressourcentyp Amazon Redshift hinzufügen, können Sie wählen, ob Sie Alle Amazon-Redshift-Cluster hinzufügen möchten, oder die Kästchen neben den Clustern aktivieren, die Sie

programmgesteuert sichern.

Sie können Ihren Backup-Plan auch in einem JSON-Dokument definieren und ihn über die AWS Backup Konsole oder bereitstellen AWS CLI. Informationen zum programmatischen Erstellen eines Backup-Plans finden Sie unter Erstellen von Backup-Plänen mithilfe eines JSON-Dokuments und der AWS Backup CLI.

Sie können die folgenden API-Vorgänge verwenden:

- Backup-Auftrag beginnen
- Backup-Auftrag beschreiben
- Metadaten für Wiederherstellungspunkt abrufen
- Wiederherstellungspunkte nach Ressourcen auflisten
- Tags für den Wiederherstellungspunkt auflisten

Anzeigen von Amazon-Redshift-Cluster-Backups

So können Sie Ihre Amazon-Redshift-Tabellen-Backups in der Konsole anzeigen und ändern:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie Backup vaults (Sicherungstresore) aus. Klicken Sie dann auf den Namen des Backup-Tresors, der Ihre Amazon-Redshift-Cluster enthält.
3. Im Backup-Tresor werden eine Zusammenfassung und eine Liste der Backups angezeigt. Sie können auf den Link in der Spalte Wiederherstellungspunkt-ID klicken.

4. Um einen oder mehrere Wiederherstellungspunkte zu löschen, aktivieren Sie die Kontrollkästchen der Punkte, die Sie löschen möchten. Unter der Schaltfläche Aktionen können Sie Löschen auswählen.

Wiederherstellen eines Amazon-Redshift-Clusters

Weitere Informationen finden Sie unter Wiederherstellen eines Amazon-Redshift-Clusters.

Backups von Amazon Relational Database Service

Amazon RDS und AWS Backup

Wenn Sie die Optionen zum Sichern Ihrer Amazon RDS-Instances und -Cluster in Betracht ziehen, müssen Sie unbedingt klären, welche Art von Backup Sie erstellen und verwenden möchten. Verschiedene AWS Ressourcen, darunter Amazon RDS, bieten ihre eigenen systemeigenen Backup-Lösungen an.

Amazon RDS bietet die Möglichkeit, automatische Backups und manuelle Backups zu erstellen. In der Amazon RDS-Terminologie erwägen alle Wiederherstellungspunkte AWS Backup, die von erstellt wurden, einschließlich der Wiederherstellungspunkte in einem Backup-Plan, manuelle Backups.

Wenn Sie AWS Backup zur Erstellung eines Backups (Wiederherstellungspunkts) einer Amazon RDS-Instance verwenden, wird AWS Backup geprüft, ob Sie Amazon RDS zuvor verwendet haben, um ein automatisiertes Backup zu erstellen. Wenn ein automatisiertes Backup vorhanden ist, AWS Backup erstellt eine Kopie dieses Snapshots (`copy-db-snapshot`Vorgang). Wenn kein vorhandenes Backup vorhanden ist, AWS Backup wird anstelle einer Kopie (`create-db-snapshot`Vorgang) ein Snapshot der von Ihnen angegebenen Instanz erstellt.

Der erste Snapshot AWS Backup, der von oder durch einen der Operationen erstellt wurde, führt zu einem vollständigen Snapshot. Bei allen nachfolgenden Kopien handelt es sich um inkrementelle Backups, solange die vollständige Sicherung existiert.

> **Important**
>
> Wenn ein AWS Backup Backup-Plan so geplant ist, dass mehrere tägliche Snapshots einer Amazon RDS-Instance erstellt werden, und wenn eines dieser geplanten AWS Backup Start-Backup-Fenster mit dem Amazon RDS-Backup-Fenster übereinstimmt, kann sich die Datenherkunft der Backups in nicht identische Backups verzweigen, wodurch ungeplante

und widersprüchliche Backups entstehen. Um dies zu verhindern, stellen Sie sicher, dass Ihr AWS Backup Backup-Plan oder Ihr Amazon RDS-Fenster nicht zeitlich übereinstimmen.

Kontinuierliche Amazon RDS-Backups und Point-in-Time-Wiederherstellung

Kontinuierliche Backups beinhalten AWS Backup die Erstellung einer vollständigen Sicherung Ihrer Amazon RDS-Ressource und die anschließende Erfassung aller Änderungen in einem Transaktionsprotokoll. Sie können eine größere Granularität erreichen, indem Sie zu dem Zeitpunkt zurückkehren, zu dem Sie wiederherstellen möchten, anstatt einen vorherigen Snapshot zu wählen, der in festen Zeitintervallen aufgenommen wurde.

Weitere Informationen finden Sie unter Kontinuierliche Backups und von PITR unterstützte Dienste und Verwaltung der Einstellungen für kontinuierliche Backups.

Amazon-RDS-Backup mit mehreren Availability Zones (AZ)

AWS Backup sichert und unterstützt die Bereitstellungsoptionen Amazon RDS for MySQL und PostgreSQL Multi-AZ (Availability Zone) mit einer primären und zwei lesbaren Standby-Datenbank-Instances.

Backups in mehreren Availability Zones sind in den folgenden Regionen verfügbar: Asien-Pazifik (Sydney), Asien-Pazifik (Tokio), Region Europa (Irland), Region USA Ost (Ohio), Region USA West (Oregon), Region Europa (Stockholm), Asien-Pazifik (Singapur), USA Ost (Nord-Virginia) und Europa (Frankfurt).

Die Multi-AZ-Bereitstellungsoption optimiert Schreibtransaktionen und ist ideal, wenn Ihre Workloads zusätzliche Lesekapazität, geringere Latenz bei Schreibtransaktionen, mehr Widerstandsfähigkeit gegen Netzwerk-Jitter (was sich auf die Konsistenz der Latenz von Schreibtransaktionen auswirkt) sowie hohe Verfügbarkeit und Haltbarkeit erfordern.

Um einen Multi-AZ-Cluster zu erstellen, können Sie entweder MySQL oder PostgreSQL als Engine-Typ wählen.

In der AWS Backup Konsole gibt es drei Bereitstellungsoptionen:

- Multi-AZ-DB-Cluster: Erstellt ein DB-Cluster mit einer primären DB-Instance und zwei lesbaren Standby-DB-Instances, wobei sich jede DB-Instance in einer anderen Availability Zone befindet. Bietet hohe Verfügbarkeit und Datenredundanz und erhöht die Kapazität für serverbereite Workloads.

- Multi-AZ-DB-Instance: Erstellt ein DB-Cluster mit einer primären DB-Instance und zwei lesbaren Standby-DB-Instances, wobei sich jede DB-Instance in einer anderen Availability Zone befindet. Dies bietet hohe Verfügbarkeit und Datenredundanz, aber die Standby-DB-Instance unterstützt keine Verbindungen für Lese-Workloads.
- Einzelne DB-Instance: Erstellt eine einzelne DB-Instance ohne Standby-DB-Instances.

Informationen zum Erstellen eines Backups für Amazon RDS finden Sie unter Erstellen eines Backups, um ein Backup als Teil Ihrer Backup-Pläne zu planen oder ein On-Demand-Backup zu erstellen.

> **Note**
>
> Zeitpunktbezogene Wiederherstellung (PITR) kann Instances unterstützen, aber keine Cluster.
> Das Kopieren eines Multi-AZ-DB-Cluster-Snapshots wird nicht unterstützt.

Unterschiede zwischen einem Multi-AZ-Cluster und einer RDS-Instance

Ein Backup in einer einzelnen Availability Zone oder in zwei Availability Zones ist eine RDS-Instance. Eine Bereitstellung und ein Backup mit drei oder mehr Instances ist ein Cluster, ähnlich wie Amazon-Aurora-, Amazon-Neptune- und Amazon-DocumentDB-Cluster.

Der ARN (Amazon-Ressourcenname) wird unterschiedlich gerendert, je nachdem, ob eine Instance oder ein Cluster verwendet wird:

Ein ARN für eine RDS-Instanz: `arn:aws:rds:`*`region`*`: `*`account`*`:db:`*`name`*

Ein RDS-Cluster mit mehreren Verfügbarkeiten: `arn:aws:rds:`*`region`*`:`*`account`*`:cluster:`*`name`*

Weitere Informationen finden Sie unter Multi-AZ-Custer-Bereitstellungen im Amazon-RDS-Benutzerhandbuch.

Weitere Informationen zum Erstellen eines Multi-AZ-Custer-Snapshots finden Sie im Amazon-RDS-Benutzerhandbuch.

AWS CloudFormation Backups stapeln

Ein CloudFormation Stack besteht aus mehreren statusbehafteten und zustandslosen Ressourcen, die Sie als eine einzige Einheit sichern können. Mit anderen Worten, Sie können eine Anwendung mit mehreren Ressourcen sichern und wiederherstellen, indem Sie einen Stack sichern und die darin enthaltenen Ressourcen wiederherstellen. Alle Ressourcen in einem Stack werden durch die AWS CloudFormation -Vorlage des Stacks definiert.

Wenn ein CloudFormation Stapel gesichert wird, werden Wiederherstellungspunkte für die CloudFormation Vorlage und für jede weitere Ressource erstellt, die von AWS Backup im Stapel unterstützt wird. Diese Wiederherstellungspunkte sind zu einem übergeordneten Wiederherstellungspunkt zusammengefasst, der als zusammengesetzt bezeichnet wird.

Dieser zusammengesetzte Wiederherstellungspunkt kann nicht wiederhergestellt werden, aber verschachtelte Wiederherstellungspunkte können wiederhergestellt werden. Sie können alle verschachtelten Backups innerhalb eines zusammengesetzten Backups mit der Konsole oder der AWS CLI wiederherstellen.

CloudFormation Terminologie des Anwendungsstapels

- Zusammengesetzter Wiederherstellungspunkt: Ein Wiederherstellungspunkt, der verwendet wird, um verschachtelte Wiederherstellungspunkte sowie andere Metadaten zu gruppieren.
- Verschachtelter Wiederherstellungspunkt: Ein Wiederherstellungspunkt einer Ressource, die Teil eines CloudFormation Stacks ist und als Teil des zusammengesetzten Wiederherstellungspunkts gesichert wird. Jeder verschachtelte Wiederherstellungspunkt gehört zum Stack eines zusammengesetzten Wiederherstellungspunkts.
- Zusammengesetzter Job: Ein Sicherungs-, Kopier- oder Wiederherstellungsauftrag für einen CloudFormation Stack, der andere Backup-Jobs für einzelne Ressourcen innerhalb des Stacks auslösen kann.
- Verschachtelter Job: Ein Sicherungs-, Kopier- oder Wiederherstellungsauftrag für eine Ressource innerhalb eines AWS CloudFormation Stacks.

CloudFormation Backup-Jobs stapeln

Der Vorgang der Backup-Erstellung wird als Backup-Auftrag bezeichnet. Ein CloudFormation Stack-Backup-Job hat einen Status. Wenn ein Backup-Auftrag abgeschlossen ist, hat er den Status `Completed`. Dies bedeutet, dass ein AWS CloudFormation Erholungspunkt (ein Backup) erstellt wurde.

CloudFormation Stapel können mit der Konsole oder programmatisch gesichert werden. Informationen zum Sichern beliebiger Ressourcen, einschließlich eines CloudFormation Stacks, finden Sie an anderer Stelle in diesem AWS Backup Entwicklerhandbuch unter Erstellen eines Backups.

CloudFormation Stacks können mit dem API-Befehl `StartBackupJob` gesichert werden. Beachten Sie, dass sich die Dokumentation und die Konsole auf zusammengesetzte und verschachtelte Wiederherstellungspunkte beziehen. In der API-Sprache wird die Terminologie „übergeordnete und untergeordnete Wiederherstellungspunkte“ in derselben kontextuellen Beziehung verwendet.

CloudFormation Stapel enthalten alle AWS Ressourcen, die in Ihrer CloudFormation Vorlage angegeben sind. Beachten Sie, dass Ihre Vorlage möglicherweise Ressourcen enthält, die noch nicht von AWS Backup unterstützt werden. Wenn Ihre Vorlage eine Kombination aus AWS unterstützten Ressourcen und nicht unterstützten Ressourcen enthält, AWS Backup wird die Vorlage trotzdem in einem zusammengesetzten Stack gesichert, Backup erstellt jedoch nur Wiederherstellungspunkte der von Backup unterstützten Dienste. Alle in der CloudFormation Vorlage enthaltenen Ressourcentypen werden in ein Backup aufgenommen, auch wenn Sie sich nicht für einen bestimmten Dienst entschieden haben (indem Sie einen Dienst in den Konsoleneinstellungen auf „Aktiviert“ setzen). Verschachtelte Backups (Wiederherstellungspunkte), die von AWS Backup unterstützt werden, können wiederhergestellt werden, verschachtelte Stacks können jedoch nicht gesichert oder wiederhergestellt werden.

AWS CloudFormation Erholungspunkt

Status des Wiederherstellungspunkts

Wenn der Backup-Auftrag eines Stacks abgeschlossen ist (der Auftragsstatus lautet `Completed`), wurde ein Backup des Stacks erstellt. Dieses Backup wird auch als zusammengesetzter Wiederherstellungspunkt bezeichnet. Ein zusammengesetzter Wiederherstellungspunkt kann einen der folgenden Status haben: `Completed`, `Failed` oder `Partial`. Beachten Sie, dass ein Backup-Auftrag einen Status hat und ein Recovery Point (auch Backup genannt) ebenfalls einen separaten Status hat.

Ein abgeschlossener Backup-Job bedeutet, dass Ihr gesamter Stack und die darin enthaltenen Ressourcen geschützt sind durch AWS Backup. Der Status „fehlgeschlagen“ bedeutet, dass der Backup-Auftrag nicht erfolgreich war. Sie sollten das Backup erneut erstellen, sobald das Problem, das den Fehler verursacht hat, behoben ist.

Ein `Partial`-Status bedeutet, dass nicht alle Ressourcen im Stack gesichert wurden. Dies kann passieren, wenn die CloudFormation Vorlage Ressourcen enthält, die derzeit nicht von unterstützt

werden AWS Backup, oder wenn einer oder mehrere der Backup-Jobs, die zu Ressourcen innerhalb des Stacks gehören (verschachtelte Ressourcen), einen anderen Status als haben. `Completed` Sie können manuell ein On-Demand-Backup erstellen, um alle Ressourcen erneut auszuführen, die zu einem anderen Status als `Completed` geführt haben. Wenn Sie erwartet haben, dass der Stack den Status `Completed` hat, der Status aber stattdessen `Partial` lautet, überprüfen Sie, welche der oben genannten Bedingungen für Ihren Stack zutreffen könnten.

Jede verschachtelte Ressource innerhalb des zusammengesetzten Wiederherstellungspunkts hat ihren eigenen individuellen Wiederherstellungspunkt mit jeweils eigenem Status (entweder `Completed` oder `Failed`). Verschachtelte Wiederherstellungspunkte mit dem Status `Completed` können wiederhergestellt werden.

Verwalten von Wiederherstellungspunkten

Zusammengesetzte Wiederherstellungspunkte (Backups) können kopiert werden. Verschachtelte Wiederherstellungspunkte können kopiert, gelöscht, getrennt oder wiederhergestellt werden. Ein zusammengesetzter Wiederherstellungspunkt, der verschachtelte Backups enthält, kann nicht gelöscht werden. Nachdem die verschachtelten Wiederherstellungspunkte innerhalb eines zusammengesetzten Wiederherstellungspunkts gelöscht oder die Zuweisung aufgehoben wurden, können Sie den zusammengesetzten Wiederherstellungspunkt manuell löschen oder ihn so lange bestehen lassen, bis er im Lebenszyklus des Backup-Plans gelöscht wird.

Löschen eines Wiederherstellungspunkts

Sie können einen Wiederherstellungspunkt mit der AWS Backup Konsole oder mit dem löschen. AWS CLI

Um Wiederherstellungspunkte mit der AWS Backup Konsole zu löschen,

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie in der linken Navigation auf Geschützte Ressourcen. Geben Sie in das Textfeld ein, `CloudFormation` um nur Ihre CloudFormation Stapel anzuzeigen.
3. Zusammengesetzte Wiederherstellungspunkte werden im Bereich Wiederherstellungspunkte angezeigt. Sie können auf das Pluszeichen (+) links neben jeder Wiederherstellungspunkt-ID klicken, um die einzelnen zusammengesetzten Wiederherstellungspunkte zu erweitern und alle verschachtelten Wiederherstellungspunkte anzuzeigen, die im zusammengesetzten Wiederherstellungspunkt enthalten sind. Sie können das Kästchen links neben einem beliebigen Wiederherstellungspunkt aktivieren, um ihn in die Auswahl der Wiederherstellungspunkte aufzunehmen, die Sie löschen möchten.

4. Klicken Sie auf die Schaltfläche Löschen.

Wenn Sie die Konsole verwenden, um einen oder mehrere zusammengesetzte Wiederherstellungspunkte zu löschen, wird ein Warnfeld angezeigt. In diesem Warnfeld müssen Sie bestätigen, dass Sie beabsichtigen, die zusammengesetzten Wiederherstellungspunkte zu löschen, einschließlich der verschachtelten Wiederherstellungspunkte in zusammengesetzten Stacks.

Verwenden Sie den `DeleteRecoveryPoint`-Befehl, um Wiederherstellungspunkte zu löschen.

Wenn Sie API mit dem verwenden, müssen AWS Command Line Interface Sie alle verschachtelten Wiederherstellungspunkte löschen, bevor Sie einen zusammengesetzten Punkt löschen. Wenn Sie eine API-Anfrage zum Löschen eines Composite-Stack-Backups (Wiederherstellungspunkts) senden, das noch verschachtelte Wiederherstellungspunkte enthält, gibt die Anfrage einen Fehler zurück.

Trennen der Zuweisung eines verschachtelten Wiederherstellungspunkts zu einem zusammengesetzten Wiederherstellungspunkt

Sie können die Zuweisung eines verschachtelten Wiederherstellungspunkts zu einem zusammengesetzten Wiederherstellungspunkt aufheben (Sie möchten beispielsweise den verschachtelten Wiederherstellungspunkt behalten, den zusammengesetzten Wiederherstellungspunkt aber löschen). Beide Wiederherstellungspunkte bleiben bestehen, aber sie sind nicht mehr miteinander verbunden. Das heißt, Aktionen, die auf dem zusammengesetzten Wiederherstellungspunkt ausgeführt werden, gelten nicht mehr für den verschachtelten Wiederherstellungspunkt, sobald er getrennt wurde.

Sie können die Verbindung des Wiederherstellungspunkts mithilfe der Konsole trennen oder die API `DisassociateRecoveryPointFromParent` aufrufen. [Beachten Sie, dass in den API-Aufrufen der Begriff „übergeordnetes Element“ verwendet wird, um sich auf zusammengesetzte Wiederherstellungspunkte zu beziehen.]

Kopieren eines Wiederherstellungspunkts

Sie können einen zusammengesetzten oder einen verschachtelten Wiederherstellungspunkt kopieren, wenn die Ressource konto- und regionsübergreifendes Kopieren unterstützt.

Gehen Sie wie folgt vor, um Wiederherstellungspunkte mit der Konsole zu kopieren: AWS Backup

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie in der linken Navigation auf Geschützte Ressourcen. Geben Sie in das Textfeld ein, `CloudFormation` um nur Ihre CloudFormation Stapel anzuzeigen.

3. Zusammengesetzte Wiederherstellungspunkte werden im Bereich Wiederherstellungspunkte angezeigt. Sie können auf das Pluszeichen (+) links neben jeder Wiederherstellungspunkt-ID klicken, um die einzelnen zusammengesetzten Wiederherstellungspunkte zu erweitern und alle verschachtelten Wiederherstellungspunkte anzuzeigen, die im zusammengesetzten Wiederherstellungspunkt enthalten sind. Sie können auf die kreisförmige Schaltfläche links neben einem beliebigen Wiederherstellungspunkt klicken, um ihn zu kopieren.
4. Sobald er ausgewählt ist, klicken Sie in der oberen rechten Ecke des Fensters auf Kopieren.

Beim Kopieren eines zusammengesetzten Wiederherstellungspunkts landen verschachtelte Wiederherstellungspunkte, die keine Kopierfunktion unterstützen, nicht im kopierten Stack. Der zusammengesetzte Wiederherstellungspunkt wird den Status `Partial` haben.

Häufig gestellte Fragen

1. „Was ist im Anwendungs-Backup enthalten?“

   Im Rahmen jeder Sicherung einer Anwendung, die mit definiert wurde CloudFormation, werden die Vorlage, der verarbeitete Wert jedes Parameters in der Vorlage und die verschachtelten Ressourcen, die von unterstützt AWS Backup werden, gesichert. Eine verschachtelte Ressource wird auf die gleiche Weise gesichert wie eine einzelne Ressource, die nicht Teil eines CloudFormation Stacks ist. Beachten Sie, dass Werte von Parametern, die als `no-echo` markiert sind, nicht gesichert werden.

2. „Kann ich meinen AWS CloudFormation Stack sichern, der verschachtelte Stapel enthält?“

   Ja. Ihre CloudFormation Stapel, die verschachtelte Stapel enthalten, können sich in Ihrem Backup befinden.

3. „Bedeutet ein *`Partial`*-Status, dass die Erstellung meines Backups fehlgeschlagen ist?“

   Nein. Ein unvollständiger Status weist darauf hin, dass einige der Wiederherstellungspunkte gesichert wurden, andere jedoch nicht. Es gibt drei Bedingungen, anhand derer Sie überprüfen können, ob Sie ein `Completed`-Backup-Ergebnis erwartet haben:

   a. Enthält Ihr CloudFormation Stack Ressourcen, die derzeit nicht unterstützt werden von? AWS Backup Eine Liste der unterstützten Ressourcen finden Sie in unserem Entwicklerhandbuch unter Unterstützte AWS Ressourcen und Anwendungen von Drittanbietern.

b. Einer oder mehrere der Backup-Aufträge, die zu Ressourcen innerhalb des Stacks gehören, waren nicht erfolgreich und der Auftrag muss erneut ausgeführt werden.

c. Ein verschachtelter Wiederherstellungspunkt wurde gelöscht oder vom zusammengesetzten Wiederherstellungspunkt getrennt.

4. „Wie schließe ich Ressourcen in meinem CloudFormation Stack-Backup aus?“

   Wenn Sie Ihren CloudFormation Stack sichern, können Sie Ressourcen davon ausschließen, Teil des Backups zu sein. In der Konsole gibt es während der Prozesse Einen Backup-Plan erstellen und Backup-Plan aktualisieren den Schritt Ressourcen zuweisen. In diesem Schritt gibt es einen Abschnitt zur Ressourcenauswahl. Wenn Sie bestimmte Ressourcentypen einbeziehen wählen und diese CloudFormation als Ressource in das Backup aufgenommen haben, können Sie bestimmte Ressourcen-IDs aus den ausgewählten Ressourcentypen ausschließen. Sie können Tags auch verwenden, um Ressourcen innerhalb des Stacks auszuschließen.

   Mit der CLI können Sie:

   - `NotResources`in Ihrem Backup-Plan, um eine bestimmte Ressource aus Ihren CloudFormation Stacks auszuschließen.
   - `StringNotLike` nutzen, um Elemente über Tags auszuschließen.

5. „Welche Arten von Backups werden für verschachtelte Ressourcen unterstützt?“

   Backups verschachtelter Ressourcen können entweder vollständige oder inkrementelle Backups sein, je nachdem, welche Art von Backup AWS Backup für diese Ressourcen unterstützt wird. Weitere Informationen finden Sie unter Funktionsweise von inkrementellen Backups. Beachten Sie jedoch, dass PITR (point-in-time Wiederherstellung) für verschachtelte Amazon S3- und Amazon RDS-Ressourcen nicht unterstützt wird.

6. „Werden Änderungssätze, die Teil des CloudFormation Stacks sind, gesichert?“

   Nein. Änderungssätze werden nicht als Teil des CloudFormation Stack-Backups gesichert.

7. „Wie wirkt sich der Status des AWS CloudFormation Stacks auf das Backup aus?“

   Der Status des CloudFormation Stacks kann sich auf das Backup auswirken. Ein Stack mit einem Status, der `COMPLETE` umfasst, kann gesichert werden, z. B. Status `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` oder `IMPORT_ROLLBACK_COMPLETE`.

Falls ein Upload einer neuen Vorlage fehlschlägt und der Stack den Status `ROLLBACK_COMPLETE` annimmt, wird die neue Vorlage gesichert, aber die Backups der verschachtelten Ressourcen basieren auf den zurückgerollten Ressourcen.

8. „Wie unterscheiden sich die Lebenszyklen von Anwendungs-Stacks von anderen Wiederherstellungspunkten?“

   Die Lebenszyklen verschachtelter Wiederherstellungspunkte werden durch den Backup-Plan bestimmt, zu dem sie gehören. Der zusammengesetzte Wiederherstellungspunkt wird durch den längsten Lebenszyklus aller verschachtelten Wiederherstellungspunkte bestimmt. Wenn der letzte verbleibende verschachtelte Wiederherstellungspunkt innerhalb eines zusammengesetzten Wiederherstellungspunkts gelöscht oder die Zuweisung aufgehoben wird, wird auch der zusammengesetzte Wiederherstellungspunkt gelöscht.

9. „Wie werden Tags eines Computers auf Wiederherstellungspunkte CloudFormation kopiert?“

   Ja. Diese Tags werden auf die jeweiligen verschachtelten Wiederherstellungspunkte kopiert.

10. „Gibt es eine Reihenfolge für das Löschen von zusammengesetzten und verschachtelten Wiederherstellungspunkten (Backups)?“

    Ja. Einige Backups müssen gelöscht werden, bevor andere gelöscht werden können. Zusammengesetzte Backups, die verschachtelte Wiederherstellungspunkte enthalten, können erst gelöscht werden, wenn alle Wiederherstellungspunkte innerhalb des zusammengesetzten Wiederherstellungspunkts gelöscht wurden. Sobald ein zusammengesetzter Wiederherstellungspunkt keine verschachtelten Wiederherstellungspunkte mehr enthält, können Sie ihn manuell löschen. Andernfalls wird er entsprechend dem Lebenszyklus seines Backup-Plans gelöscht.

Wiederherstellen von Anwendungen innerhalb eines Stacks

Weitere Informationen zum Wiederherstellen verschachtelter Wiederherstellungspunkte finden Sie unter So stellen Sie Anwendungs-Stack-Backups wieder her.

Erstellen von Windows-VSS-Backups

Mit AWS Backup können Sie VSS-fähige Windows-Anwendungen (Volume Shadow Copy Service) sichern und wiederherstellen, die auf Amazon EC2 EC2-Instances ausgeführt werden. Wenn für die

Anwendung der VSS Writer bei Windows VSS registriert ist, wird ein Snapshot AWS Backup erstellt, der für diese Anwendung konsistent ist.

Sie können konsistente Wiederherstellungen durchführen und dabei denselben verwalteten Backup-Service verwenden, der auch für den Schutz anderer AWS Ressourcen verwendet wird. Mit anwendungskonsistenten Windows-Backups auf EC2 erhalten Sie dieselben Konsistenzeinstellungen und dieselbe Anwendungsorientierung wie bei herkömmlichen Backup-Tools.

> **Note**
>
> AWS Backup unterstützt derzeit nur anwendungskonsistente Backups von Ressourcen, die auf Amazon EC2 laufen, insbesondere Backup-Szenarien, in denen Anwendungsdaten wiederhergestellt werden können, indem eine bestehende Instance durch eine neue Instance ersetzt wird, die aus dem Backup erstellt wurde. Nicht alle Instance-Typen oder Anwendungen werden für Windows-VSS-Backups unterstützt.

Weitere Informationen finden Sie unter Creating a VSS Application-Consistent Snapshot im Amazon EC2 EC2-Benutzerhandbuch.

Gehen Sie wie folgt vor, um VSS-fähige Windows-Ressourcen, auf denen Amazon EC2 ausgeführt wird, zu sichern und wiederherzustellen, um die erforderlichen Voraussetzungen zu erfüllen. Anweisungen finden Sie unter Bevor Sie beginnen im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

1. Laden Sie den SSM-Agenten unter herunter, installieren Sie ihn und konfigurieren Sie ihn. AWS Systems Manager Dieser Schritt ist erforderlich. Anweisungen finden Sie unter Arbeiten mit dem SSM-Agenten auf Amazon EC2 EC2-Instances für Windows Server im AWS Systems Manager Manager-Benutzerhandbuch.
2. Fügen Sie der IAM-Rolle eine IAM-Richtlinie hinzu und fügen Sie die Rolle der Amazon-EC2-Instance hinzu, bevor Sie das Windows-VSS-Backup (Volume Shadow Copy Service) durchführen. Anweisungen finden Sie unter Erstellen einer IAM-Rolle für VSS-fähige Snapshots im Amazon EC2 EC2-Benutzerhandbuch. Die IAM-Beispielrichtlinie finden Sie unter Verwaltete Richtlinien für AWS Backup.
3. Herunterladen und Installieren der VSS-Komponenten auf der Amazon-EC2-Windows-Instance
4. AWS Backup Aktivieren Sie VSS in:

    1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.

2. Wählen Sie im Dashboard den Backup-Typ aus, den Sie erstellen möchten, entweder On-Demand-Backup erstellen oder Backup-Pläne verwalten. Geben Sie die Informationen ein, die für Ihren Backup-Typ erforderlich sind.
3. Wenn Sie Ressourcen zuweisen, wählen Sie EC2. Windows VSS-Backup wird derzeit nur für EC2-Instances unterstützt.
4. Wählen Sie auf der Registerkarte Erweiterte Einstellungen die Option Windows VSS aus. Auf diese Weise können Sie anwendungskonsistente Windows-VSS-Backups erstellen.
5. Erstellen Sie Ihr Backup.

Ein Backup-Auftrag mit dem Status `Completed` garantiert nicht, dass der VSS-Teil erfolgreich ist. Die Aufnahme von VSS erfolgt auf Best-Effort-Basis. Fahren Sie mit den folgenden Schritten fort, um festzustellen, ob ein Backup anwendungskonsistent, absturzkonsistent oder fehlerhaft ist:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie im linken Navigationsbereich unter Mein Konto auf Aufträge.
3. Der Status `Completed` weist auf einen erfolgreichen Auftrag hin, der anwendungskonsistent (VSS) ist.

   Der Status `Completed with issues` gibt an, dass der VSS-Vorgang fehlgeschlagen ist, sodass nur ein absturzkonsistentes Backup erfolgreich war. Für diesen Status wird auch die Popover-Meldung "`Windows VSS Backup Job Error encountered, trying for regular backup`" angezeigt.

   Wenn das Backup nicht erfolgreich war, lautet der Status `Failed`.
4. Um weitere Details des Backup-Auftrags anzuzeigen, klicken Sie auf den einzelnen Auftrag. Die Details können beispielsweise `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation` lauten.

VSS-fähige Backups mit einem Ziel, bei dem es sich nicht um Windows oder um eine Windows-Komponente handelt, deren Aufgabe erfolgreich abgeschlossen wurde, sind ohne VSS absturzkonsistent.

Nicht unterstützte Amazon-EC2-Instances

Die folgenden Amazon-EC2-Instance-Typen werden für VSS-fähige Windows-Backups nicht unterstützt, da es sich um kleine Instances handelt, die das Backup möglicherweise nicht erfolgreich durchführen.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS und AWS Backup

Der Sicherungsvorgang für Amazon EBS-Ressourcen ähnelt den Schritten, die zum Sichern anderer Ressourcentypen verwendet werden:

- Erstellen eines On-Demand-Backups
- Erstellen eines geplanten Backups

Ressourcenspezifische Informationen werden in den folgenden Abschnitten vermerkt.

Amazon EBS Archive Tier für Cold Storage

EBS ist eine der Ressourcen, die die Übertragung von Backups zu Cold Storage unterstützt. Weitere Informationen finden Sie unter Lebenszyklus und Speicherstufen.

> **Note**
>
> Diese Funktion ist in den Regionen China (Peking), China (Ningxia), (USA-Ost) und AWS GovCloud AWS GovCloud (US-West) nicht verfügbar.

Absturzkonsistente Amazon-EBS-Backups mit Multi-Volume

AWS Backup Erstellt standardmäßig absturzsichere Backups von Amazon EBS-Volumes, die an eine Amazon EC2 EC2-Instance angehängt sind. Absturzkonsistenz bedeutet, dass die Snapshots für jedes Amazon-EBS-Volume, das an dieselbe Amazon-EC2-Instance angehängt ist, genau zum selben Zeitpunkt erstellt werden. Sie müssen Ihre Instances nicht mehr anhalten oder mehrere Amazon-EBS-Volumes koordinieren, um die Absturzkonsistenz Ihres Anwendungsstatus sicherzustellen.

Da es sich bei absturzsicheren Snapshots mit mehreren Volumes um eine AWS Backup Standardfunktion handelt, müssen Sie nichts anderes tun, um diese Funktion zu verwenden. Sie können Amazon-EBS-Volumes mit einem der folgenden Verfahren sichern:

Die Rolle, die zur Erstellung eines EBS-Snapshot-Wiederherstellungspunkts verwendet wurde, wird diesem Snapshot zugeordnet. Dieselbe Rolle muss verwendet werden, um die von ihr erstellten Wiederherstellungspunkte zu löschen oder um ihre Wiederherstellungspunkte auf eine Archivebene zu übertragen.

Amazon EBS Snapshot Lock und AWS Backup

AWS Backup verwaltete Amazon EBS-Snapshots und Snapshots, die mit einem AWS Backup verwalteten Amazon EC2 EC2-AMI verknüpft sind und auf die Amazon EBS Snapshot Lock angewendet wurde, dürfen nicht als Teil des Wiederherstellungspunkt-Lebenszyklus gelöscht werden, wenn die Dauer der Snapshot-Sperre den Backup-Lebenszyklus überschreitet. Stattdessen haben diese Wiederherstellungspunkte den Status `EXPIRED`. Diese Wiederherstellungspunkte können manuell gelöscht werden, wenn Sie zuerst das Amazon EBS Snapshot Lock entfernen.

Wiederherstellen von Amazon-EBS-Ressourcen

Um Ihre Amazon-EBS-Volumes wiederherzustellen, folgen Sie den Schritten unter Wiederherstellen eines Amazon-EBS-Volumes.

Kopieren von Tags in Backups

AWS Backup Kopiert im Allgemeinen Tags von den Ressourcen, die es schützt, auf Ihre Wiederherstellungspunkte. Weitere Informationen zum Kopieren von Tags während einer Wiederherstellung finden Sie unter Tags während einer Wiederherstellung kopieren.

Wenn Sie beispielsweise ein Amazon EC2 EC2-Volume sichern, AWS Backup kopiert es dessen Gruppen- und einzelne Ressourcen-Tags in den resultierenden Snapshot, wobei Folgendes gilt:

- Eine Liste der ressourcenspezifischen Berechtigungen, die zum Speichern von Metadaten-Tags auf Backups erforderlich sind, finden Sie unter Berechtigungen zum Zuweisen von Tags zu Backups.
- Tags, die ursprünglich einer Ressource zugeordnet waren, und Tags, die während des Backups zugewiesen wurden, werden Wiederherstellungspunkten zugewiesen, die in einem Backup-Tresor gespeichert sind, bis zu einem Maximum von 50 (dies ist eine AWS Einschränkung). Tags, die während des Backups zugewiesen werden, haben Priorität und beide Tagsätze werden in alphabetischer Reihenfolge kopiert.
- DynamoDB unterstützt das Zuweisen von Tags zu Backups nur, wenn Sie zuerst Erweitertes DynamoDB-Backup aktivieren.
- Amazon-EBS-Volumes, die an Amazon-EC2-Instances angehängt sind, sind verschachtelte Ressourcen. Tags auf den Amazon EBS-Volumes, die an Amazon EC2 EC2-Instances angehängt sind, sind verschachtelte Tags. AWS Backup unternimmt nach besten Kräften den Versuch, verschachtelte Tags zu kopieren. Wenn dies jedoch nicht gelingt, erstellt es ein Backup ohne sie und meldet den Status Abgeschlossen.
- Wenn ein Amazon EC2 EC2-Backup einen Image-Wiederherstellungspunkt und eine Reihe von Snapshots erstellt, werden Tags in das resultierende AMI AWS Backup kopiert. AWS Backup unternimmt außerdem nach besten Kräften den Versuch, die Tags von den Volumes, die der Amazon EC2 EC2-Instance zugeordnet sind, in die resultierenden Snapshots zu kopieren.

Wenn Sie Ihr Backup auf ein anderes kopieren AWS-Region, werden alle Tags des ursprünglichen Backups an das Ziel AWS Backup kopiert. AWS-Region

Anhalten eines Backup-Auftrags

Sie können einen Backup-Job beenden, AWS Backup nachdem er initiiert wurde. Wenn Sie dies tun, wird die Sicherung nicht erstellt und der Datensatz des Sicherungsauftrags wird mit dem Status aborted (abgebrochen) aufbewahrt.

Um einen Backup-Job mit der AWS Backup Konsole zu beenden

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich auf der linken Seite Jobs (Aufträge) aus.
3. Wählen Sie die Sicherung, die Sie anhalten möchten.
4. Wählen Sie im Detailfenster zu den Sicherungsaufträgen Stop (Anhalten).

Kopieren eines Backups

Für die meisten Ressourcentypen können Sie Backups AWS-Regionen auf mehrere AWS-Konten oder bei Bedarf oder automatisch als Teil eines geplanten Backup-Plans kopieren. Einzelheiten finden Sie unterthe section called “Verfügbarkeit von Features nach Ressource”.

Sie können auch eine Folge von konto- und regionsübergreifenden Kopien für die meisten unterstützten Ressourcen automatisieren, mit Ausnahme von Amazon RDS und Aurora. Unterstützt für Amazon RDS- und Aurora-Snapshots AWS Backup nur die Automatisierung von konto - oder regionsübergreifenden Kopien, da diese Dienste ihre Verschlüsselungsschlüssel erstellen (das Kopieren eines Multi-AZ-DB-Cluster-Snapshots wird nicht unterstützt).

Bei einigen Ressourcentypen sind sowohl kontinuierliche Backups als auch regions- und kontoübergreifende Kopien verfügbar. Wenn eine regionsübergreifende oder kontoübergreifende Kopie eines kontinuierlichen Backups erstellt wird, wird aus dem kopierten Recovery Point (Backup) ein Snapshot-Backup (regelmäßiges Backup). Je nach Ressourcentyp kann es sich bei den Snapshots um eine inkrementelle Kopie oder um eine vollständige Kopie handeln. Zeitpunktbezogene Wiederherstellung (Point-in-Time Restore, PITR) ist für diese Kopien nicht verfügbar.

Kopien behalten ihre Quellkonfiguration, einschließlich Erstellungsdatum und Aufbewahrungszeitraum. Das Erstellungsdatum bezieht sich auf den Zeitpunkt, an dem die Quelle erstellt wurde, nicht auf den Zeitpunkt, an dem die Kopie erstellt wurde.

HINWEIS: Die Quellkonfiguration überschreibt die Ablaufeinstellung der Kopie, auch wenn die Kopie so eingestellt ist, dass sie niemals abläuft. Eine Kopie, die niemals abläuft, behält trotzdem das Ablaufdatum ihrer Quelle.

Wenn Sie möchten, dass Ihr Backup nicht abläuft, legen Sie entweder fest, dass Ihre Quellbackups niemals ablaufen, oder geben Sie an, dass Ihre Kopie 100 Jahre nach ihrer Erstellung abläuft.

Inhalt

Erstellen von Sicherungskopien von AWS-Regionen

Mithilfe AWS Backup können Sie Backups AWS-Regionen bei Bedarf oder automatisch im Rahmen eines geplanten Sicherungsplans auf mehrere kopieren. Regionsübergreifende Replikation ist

besonders wertvoll, wenn Sie über Betriebskontinuität oder Compliance-Anforderungen verfügen, um Sicherungen in einem Mindestabstand von Ihren Produktionsdaten zu speichern. Ein Video-Tutorial finden Sie unter Regionsübergreifende Backup-Kopien verwalten.

Wenn Sie ein Backup zum ersten Mal auf ein neues AWS-Region kopieren, wird das Backup vollständig AWS Backup kopiert. Wenn ein Dienst inkrementelle Backups unterstützt, AWS-Region werden nachfolgende Kopien dieser Sicherung in derselben Regel inkrementell ausgeführt. AWS Backup verschlüsselt Ihre Kopie erneut mit dem vom Kunden verwalteten Schlüssel Ihres Ziel-Tresors.

Eine Ausnahme bildet Amazon EBS, das besagt, dass die Änderung des Verschlüsselungsstatus eines Snapshots während eines Kopiervorgangs zu einer vollständigen (nicht inkrementellen) Kopie führt.

Voraussetzungen

- Die meisten AWS Backup unterstützten Ressourcen unterstützen regionsübergreifende Backups. Weitere Einzelheiten finden Sie unter Verfügbarkeit von Features nach Ressource.
- Die meisten AWS Regionen unterstützen regionsübergreifendes Backup. Weitere Einzelheiten finden Sie unter Verfügbarkeit der Funktionen von AWS-Region.
- AWS Backup unterstützt keine regionsübergreifenden Kopien für die Speicherung auf kalten Speicherebenen.

Überlegungen zum regionsübergreifenden Kopieren mit bestimmten Ressourcen

Amazon RDS

Sie können eine Optionsgruppe nicht in eine andere AWS-Region kopieren. Wenn Sie das versuchen, erhalten Sie möglicherweise eine Fehlermeldung wie „Für den Snapshot ist eine Zieloptionsgruppe mit den folgenden Optionen erforderlich:...“

Sie müssen dieselben Optionsgruppen im Ziel eingeben, AWS-Region wenn Sie eine neue regionsübergreifende Kopie eines Amazon RDS-Snapshots erstellen.

Durchführen eines regionsübergreifenden On-Demand-Backups

So kopieren Sie ein vorhandenes Backup bei Bedarf

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.

2. Wählen Sie Backup vaults (Sicherungstresore) aus.
3. Wählen Sie den Tresor mit dem Wiederherstellungspunkt aus, den Sie kopieren möchten.
4. Wählen Sie im Abschnitt Backups einen zu kopierenden Wiederherstellungspunkt aus.
5. Wählen Sie mithilfe der Dropdown-Schaltfläche Aktionen die Option Kopieren aus.
6. Geben Sie die folgenden Werte ein:

   Kopieren auf das Ziel

   Wählen Sie das Ziel AWS-Region für die Kopie aus. Sie können einem neuen Ziel eine neue Kopierregel pro Kopie hinzufügen.

   Ziel-Backup-Tresor

   Wählen Sie den Zielsicherungstresor für die Kopie aus.

   Übergang auf Cold Storage

   Legen Sie fest, wann die Backup-Kopie in den Cold Storage übertragen werden soll. In den Archivspeicher übertragene Sicherungen müssen dort mindestens 90 Tage lang gespeichert werden. Dieser Wert kann nicht geändert werden, nachdem eine Kopie in den Cold Storage übergegangen ist.

   Eine Liste der Ressourcen, die Sie in den Cold Storage übertragen können, finden Sie unter „Lebenszyklus bis zu Cold Storage“ in der Tabelle.Verfügbarkeit von Features nach Ressource Der Cold-Storage-Ausdruck wird für andere Ressourcen ignoriert.

   Aufbewahrungszeitraum

   Wählen Sie die Anzahl der Tage nach der Erstellung, nach denen die Kopie gelöscht wird. Dieser Wert muss 90 Tage über dem Wert Übergang zu Cold Storage liegen. Mit der Aufbewahrungsfrist „Immer“ wird Ihre Kopie auf unbestimmte Zeit aufbewahrt.

   IAM-Rolle

   Wählen Sie die IAM-Rolle aus, die beim Erstellen der Kopie verwendet AWS Backup werden soll. Die Rolle muss außerdem als vertrauenswürdige Entität AWS Backup aufgeführt sein, sodass AWS Backup sie die Rolle übernehmen kann. Wenn Sie Standard wählen und die AWS Backup Standardrolle nicht in Ihrem Konto vorhanden ist, wird eine Rolle mit den richtigen Berechtigungen für Sie erstellt.
7. Wählen Sie die Option Kopieren aus.

Planen von regionsübergreifendem Backup

Sie können einen geplanten Backup-Plan verwenden, um Backups über AWS-Regionen hinweg zu kopieren.

So kopieren Sie ein Backup mit einem geplanten Backup-Plan:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie unter Mein Konto die Option Backup-Pläne und dann Backup-Plan erstellen aus.
3. Wählen Sie auf der Seite Backup-Plan erstellen die Option Neuen Plan erstellen aus.
4. Geben Sie für Name des Backup-Plans einen Namen für Ihren Backup-Plan ein.
5. Fügen Sie im Abschnitt Konfiguration der Backup-Regel eine Backup-Regel hinzu, die einen Backup-Zeitplan, ein Backup-Fenster und Lebenszyklusregeln definiert. Sie können später weitere Backup-Regeln hinzufügen.

    a. Geben Sie unter Name der Backup-Regel einen Namen für Ihre Regel ein.

    b. Wählen Sie für Backup-Tresor einen Tresor aus der Liste aus. Die Wiederherstellungspunkte für dieses Backup werden in diesem Tresor gespeichert. Sie können bei Bedarf auch einen neuen Backup-Tresor erstellen.

    c. Wählen Sie unter Backup-Frequenz aus, wie oft Sie Backups erstellen möchten.

    d. Wenn Sie für Dienste, die PITR unterstützen, diese Funktion nutzen möchten, wählen Sie Enable Continuous Backups for point-in-time Recovery (PITR). Eine Liste der Dienste, die PITR unterstützen, finden Sie in diesem Abschnitt der Tabelle.Verfügbarkeit von Features nach Ressource

    e. Wählen Sie für Backup-Fenster die Option Standardwerte für Backup-Fenster verwenden – empfohlen. Sie können das Backup-Fenster anpassen.

    f. Wählen Sie unter In das Ziel kopieren die Ziel- AWS-Region für Ihre Backup-Kopie aus. Ihr Backup wird in diese Region kopiert. Sie können einem neuen Ziel eine neue Kopierregel pro Kopie hinzufügen. Geben Sie dann die folgenden Werte ein:

        In den Tresor eines anderen Kontos kopieren

        > Schalten Sie diese Option nicht um. Weitere Informationen zu kontoübergreifenden Kopien finden Sie unter Erstellen von Sicherungskopien auf AWS-Konten

Ziel-Backup-Tresor

Wählen Sie den Backup-Tresor in der Zielregion aus, in den Ihr Backup kopiert AWS Backup werden soll.

Wenn Sie einen neuen Backup-Tresor für regionsübergreifendes Kopieren erstellen möchten, wählen Sie Neuen Backup-Tresor erstellen. Geben Sie die Informationen in den Assistenten ein. Wählen Sie Backup-Tresor erstellen aus.

6. Wählen Sie Plan erstellen aus.

Erstellen von Sicherungskopien auf AWS-Konten

Mithilfe AWS Backup können Sie bei Bedarf oder automatisch AWS-Konten im Rahmen eines geplanten Sicherungsplans mehrere sichern. Verwenden Sie ein kontoübergreifendes Backup, wenn Sie Ihre Backups aus betrieblichen oder Sicherheitsgründen sicher auf eines oder mehrere AWS-Konten in Ihrem Unternehmen kopieren möchten. Wenn Ihr ursprüngliches Backup versehentlich gelöscht wird, können Sie das Backup von seinem Zielkonto in das Quellkonto kopieren und dann die Wiederherstellung starten. Bevor Sie dies tun können, benötigen Sie zwei Konten, die zur selben Organisation im AWS Organizations -Dienst gehören. Weitere Informationen finden Sie unter Anleitung: Erstellen und Konfigurieren einer Organisation im Organisations-Benutzerhandbuch.

Sie müssen in Ihrem Zielkonto einen Backup-Tresor erstellen. Anschließend weisen Sie einen vom Kunden verwalteten Schlüssel zur Verschlüsselung von Backups im Zielkonto und eine ressourcenbasierte Zugriffsrichtlinie zu, die den Zugriff auf die Ressourcen ermöglicht AWS Backup , die Sie kopieren möchten. Wenn Ihre Ressourcen im Quellkonto mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind, müssen Sie diesen vom Kunden verwalteten Schlüssel mit dem Zielkonto teilen. Anschließend können Sie einen Backup-Plan erstellen und ein Zielkonto auswählen, das in AWS Organizations Teil Ihrer Organisationseinheit ist.

Wenn Sie ein Backup zum ersten Mal in ein Cross-Account-Konto kopieren, wird das Backup AWS Backup vollständig kopiert. Wenn ein Dienst inkrementelle Backups unterstützt, sind nachfolgende Kopien dieser Sicherung in demselben Konto im Allgemeinen inkrementell. AWS Backup verschlüsselt Ihre Kopie erneut mit dem vom Kunden verwalteten Schlüssel Ihres Zieltresors.

Voraussetzungen

- Bevor Sie Ressourcen für mehrere Benutzer AWS-Konten verwalten können AWS Backup, müssen Ihre Konten derselben Organisation im AWS Organizations Service angehören.

- Die meisten Ressourcen, die von unterstützt werden, AWS Backup unterstützen kontenübergreifendes Backup. Weitere Einzelheiten finden Sie unter Verfügbarkeit von Features nach Ressource.
- Die meisten AWS Regionen unterstützen kontenübergreifende Backups. Weitere Einzelheiten finden Sie unter Verfügbarkeit der Funktionen von AWS-Region.
- AWS Backup unterstützt keine kontoübergreifenden Kopien für die Speicherung in Cold-Tiers.

Einrichten kontenübergreifender Backups

Was benötigen Sie, um kontoübergreifende Backups zu erstellen?

- Ein Quellkonto

  Das Quellkonto ist das Konto, in dem sich Ihre AWS Produktionsressourcen und primären Backups befinden.

  Der Benutzer des Quellkontos initiiert den kontoübergreifenden Backup-Vorgang. Der Benutzer oder die Rolle des Quellkontos muss über die entsprechenden API-Berechtigungen verfügen, um den Vorgang zu initiieren. Geeignete Berechtigungen können die AWS verwaltete Richtlinie sein`AWSBackupFullAccess`, die vollen Zugriff auf den AWS Backup Betrieb ermöglicht, oder eine vom Kunden verwaltete Richtlinie, die Aktionen wie `ec2:ModifySnapshotAttribute` ermöglicht. Weitere Informationen zu Richtlinientypen finden Sie unter Von AWS Backup verwaltete Richtlinien.
- Ein Zielkonto

  Das Zielkonto ist das Konto, auf dem Sie eine Kopie Ihres Backups aufbewahren möchten. Sie können mehr als ein Zielkonto auswählen. Das Zielkonto muss sich in derselben Organisation befinden wie das Quellkonto in AWS Organizations.

  Sie müssen die Zugriffsrichtlinie `backup:CopyIntoBackupVault` für Ihren Ziel-Backup-Tresor „zulassen“. Wenn diese Richtlinie nicht vorhanden ist, werden Versuche, auf das Zielkonto zu kopieren, abgelehnt.
- Ein Verwaltungskonto in AWS Organizations

  Das Verwaltungskonto ist das primäre Konto in Ihrer Organisation, wie in AWS Organizations definiert, das Sie verwenden, um kontenübergreifende Backups in Ihrem AWS-Konten zu verwalten. Um kontoübergreifendes Backup verwenden zu können, müssen Sie außerdem Service Trust aktivieren. Nachdem Sie Service Trust aktiviert haben, können Sie jedes Konto in der

Organisation als Zielkonto verwenden. Von Ihrem Zielkonto aus können Sie auswählen, welche Tresore für kontoübergreifende Backups verwendet werden sollen.

- Aktivieren kontoübergreifender Backups in der AWS Backup -Konsole

Weitere Informationen zu Sicherheit finden Sie unter Sicherheitsüberlegungen für kontoübergreifende Backups.

Um das kontoübergreifende Backup verwenden zu können, müssen Sie das kontoübergreifende Backup-Feature aktivieren. Dann müssen Sie die Zugriffsrichtlinie `backup:CopyIntoBackupVault` für Ihren Ziel-Backup-Tresor „zulassen“.

Aktivieren Sie kontoübergreifendes Backup

1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Organizations Verwaltungskontos an. Kontoübergreifende Backups können nur mit diesen Anmeldeinformationen aktiviert oder deaktiviert werden.
2. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
3. Wählen Sie unter Mein Konto die Option Einstellungen aus.
4. Wählen Sie für kontoübergreifendes Backup die Option Aktivieren aus.
5. Wählen Sie unter Backup-Tresore Ihren Zieltresor aus.

   Beim kontoübergreifenden Kopieren befinden sich der Quelltresor und der Zieltresor in unterschiedlichen Konten. Wechseln Sie bei Bedarf zu dem Konto, dem das Zielkonto gehört.
6. Klicken Sie im Bereich Zugriffsrichtlinie auf `backup:CopyIntoBackupVault` „Zulassen“. Wählen Sie beispielsweise Berechtigungen hinzufügen und dann Zugriff auf einen Backup-Tresor aus der Organisation zulassen aus. Jede andere kontoübergreifende Aktion als `backup:CopyIntoBackupVault` wird abgelehnt.
7. Jetzt kann jedes Konto in Ihrer Organisation den Inhalt seines Backup-Tresors mit jedem anderen Konto in Ihrer Organisation teilen. Weitere Informationen finden Sie unter Freigeben eines Backup-Tresors für ein anderes AWS -Konto. Informationen zur Einschränkung, welche Konten den Inhalt der Backup-Tresore anderer Konten erhalten können, finden Sie unter Konfigurieren eines Kontos als Zielkonto.

Planen kontenübergreifender Backups

Sie können einen geplanten Backup-Plan verwenden, um Backups über AWS-Konten hinweg zu kopieren.

So kopieren Sie ein Backup mit einem geplanten Backup-Plan:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie unter Mein Konto die Option Backup-Pläne und dann Backup-Plan erstellen aus.
3. Wählen Sie auf der Seite Backup-Plan erstellen die Option Neuen Plan erstellen aus.
4. Geben Sie für Name des Backup-Plans einen Namen für Ihren Backup-Plan ein.
5. Fügen Sie im Abschnitt Konfiguration der Backup-Regel eine Backup-Regel hinzu, die einen Backup-Zeitplan, ein Backup-Fenster und Lebenszyklusregeln definiert. Sie können später weitere Backup-Regeln hinzufügen.

   Geben Sie unter Regelname einen Namen für Ihre Regel ein.
6. Wählen Sie im Abschnitt Zeitplan unter Häufigkeit aus, wie oft das Backup durchgeführt werden soll.
7. Wählen Sie für Backup-Fenster die Option Standardwerte für Backup-Fenster verwenden (empfohlen). Sie können das Backup-Fenster anpassen.
8. Wählen Sie für Backup-Tresor einen Tresor aus der Liste aus. Die Wiederherstellungspunkte für dieses Backup werden in diesem Tresor gespeichert. Sie können bei Bedarf auch einen neuen Backup-Tresor erstellen.
9. Geben Sie im Abschnitt Kopie generieren – optional die folgenden Werte ein:

   Zielregion

   Wählen Sie das Ziel AWS-Region für Ihre Sicherungskopie. Ihr Backup wird in diese Region kopiert. Sie können einem neuen Ziel eine neue Kopierregel pro Kopie hinzufügen.

   In den Tresor eines anderen Kontos kopieren

   Schalten Sie um, um diese Option auszuwählen. Die Option wird blau, wenn sie ausgewählt ist. Die Option Externer Tresor-ARN wird angezeigt.

   Externer Tresor-ARN

   Geben Sie den Amazon-Ressourcennamen (ARN) des Zielkontos ein. Der ARN ist eine Zeichenfolge, die die Konto-ID und ihre enthält AWS-Region. AWS Backup kopiert das

Backup in den Tresor des Zielkontos. Die Liste der Zielregionen wird automatisch mit der Region im externen Tresor-ARN aktualisiert.

Wählen Sie unter Zugriff auf Backup-Tresor zulassen die Option Zulassen aus. Wählen Sie dann im sich öffnenden Assistenten die Option Zulassen aus.

AWS Backup benötigt Zugriffsberechtigungen für das externe Konto, um das Backup auf den angegebenen Wert zu kopieren. Der Assistent zeigt die folgende Beispielrichtlinie, die diesen Zugriff ermöglicht.

```
{
  "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"
      }
    }
  ]
}
```

Übergang auf Cold Storage

Legen Sie fest, wann die Sicherungskopie in den Cold Storage übergestellt werden soll und wann die Kopie abläuft (gelöscht werden soll). In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Dieser Wert kann nicht geändert werden, nachdem eine Kopie in den Cold Storage übergegangen ist.

Eine Liste der Ressourcen, die Sie in den Cold Storage übertragen können, finden Sie unter „Lebenszyklus bis zu Cold Storage“ in der Tabelle.Verfügbarkeit von Features nach Ressource Der Cold-Storage-Ausdruck wird für andere Ressourcen ignoriert.

Expire (Ablaufdatum) gibt die Anzahl der Tage nach der Erstellung an, nach denen die Kopie gelöscht wird. Dieser Wert muss 90 Tage über dem Wert Übergang zu Cold Storage liegen.

> **Note**
>
> Wenn Backups ablaufen und im Rahmen Ihrer Lebenszyklus-Richtlinie zum Löschen markiert sind, werden die Backups zu einem zufällig ausgewählten Zeitpunkt innerhalb der folgenden 8 Stunden AWS Backup gelöscht. Dieses Zeitfenster trägt dazu bei, eine gleichbleibende Leistung zu ermöglichen.

10. Wählen Sie Zu Wiederherstellungspunkten hinzugefügte Tags, um Ihren Wiederherstellungspunkten Tags hinzuzufügen.
11. Wählen Sie unter Erweiterte Backup-Einstellungen Windows VSS aus, um anwendungsspezifische Snapshots für die ausgewählte Drittanbietersoftware zu aktivieren, die auf EC2 ausgeführt wird.
12. Wählen Sie Plan erstellen aus.

Durchführen eines kontoübergreifenden On-Demand-Backups

Sie können ein Backup bei Bedarf AWS-Konto auf ein anderes kopieren.

So kopieren Sie ein Backup nach Bedarf:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie unter Mein Konto die Option Backup-Tresor aus, um alle Ihre Backup-Tresore aufzulisten. Sie können nach dem Namen oder Tag des Backup-Tresors filtern.
3. Wählen Sie die Wiederherstellungspunkt-ID des Backups, das Sie kopieren möchten.
4. Wählen Sie die Option Kopieren aus.
5. Erweitern Sie die Backup-Details, um Informationen über den Wiederherstellungspunkt zu sehen, den Sie kopieren.
6. Wählen Sie im Abschnitt Konfiguration kopieren eine Option aus der Liste Zielregion aus.
7. Wählen Sie In den Tresor eines anderen Kontos kopieren. Die Option wird blau, wenn sie ausgewählt ist.
8. Geben Sie den Amazon-Ressourcennamen (ARN) des Zielkontos ein. Der ARN ist eine Zeichenfolge, die die Konto-ID und ihre enthält AWS-Region. AWS Backup kopiert das Backup in den Tresor des Zielkontos. Die Liste der Zielregionen wird automatisch mit der Region im externen Tresor-ARN aktualisiert.

9. Wählen Sie unter Zugriff auf Backup-Tresor zulassen die Option Zulassen aus. Wählen Sie dann im sich öffnenden Assistenten die Option Zulassen aus.

   Um die Kopie zu erstellen, AWS Backup sind Zugriffsberechtigungen für das Quellkonto erforderlich. Der Assistent zeigt die Beispielrichtlinie, die diesen Zugriff ermöglicht. Diese Richtlinie wird im Folgenden angezeigt.

```
{
  "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. Legen Sie unter Übergang in Cold Storage fest, wann die Backup-Kopie in den Cold Storage übertragen werden soll und wann die Kopie abläuft (gelöscht werden soll). In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Dieser Wert kann nicht geändert werden, nachdem eine Kopie in den Cold Storage übergegangen ist.

    Eine Liste der Ressourcen, die Sie in den Cold Storage übertragen können, finden Sie unter „Lebenszyklus bis zu Cold Storage“ in der Tabelle.Verfügbarkeit von Features nach Ressource Der Cold-Storage-Ausdruck wird für andere Ressourcen ignoriert.

    Expire (Ablaufdatum) gibt die Anzahl der Tage nach der Erstellung an, nach denen die Kopie gelöscht wird. Dieser Wert muss 90 Tage über dem Wert Übergang zu Cold Storage liegen.

11. Geben Sie unter IAM-Rolle die IAM-Rolle (z. B. die Standardrolle) an, die berechtigt ist, Ihr Backup zum Kopieren verfügbar zu machen. Der Vorgang des Kopierens wird von der serviceverknüpften Rolle Ihres Zielkontos ausgeführt.

12. Wählen Sie die Option Kopieren aus. Je nach Größe der Ressource, die Sie kopieren, kann dieser Vorgang bis zum Abschluss mehrere Stunden dauern. Wenn der Kopierauftrag

abgeschlossen ist, wird die Kopie auf der Registerkarte Aufträge kopieren im Menü Aufträge angezeigt.

Verschlüsselungsschlüssel und kontoübergreifende Kopien

Der Verschlüsselungsschlüssel für kontoübergreifende Kopien hängt vom Ressourcentyp ab. Ressourcen, die den Vollständige Verwaltung AWS Backup Verschlüsselungsschlüssel des Quell-Backup-Tresors verwendet haben. Vom Kunden verwaltete KMS-Schlüssel können für die kontoübergreifende Kopierverschlüsselung dieser Ressourcentypen verwendet werden.

Ressourcentypen, die nicht vollständig verwaltet werden, AWS Backup haben denselben KMS-Quellschlüssel und denselben Ressourcen-KMS-Schlüssel. Kontenübergreifendes Kopieren mit AWS verwalteten KMS-Schlüsseln wird für diese Ressourcentypen, die nicht vollständig verwaltet AWS Backup werden, nicht unterstützt.

Weitere Hilfe zur Behebung von Fehlern beim kontenübergreifenden Kopieren finden Sie im AWS Knowledge Center.

Bei einer kontoübergreifenden Kopie muss die KMS-Schlüsselrichtlinie für das Quellkonto das Zielkonto in der KMS-Schlüsselrichtlinie zulassen.

Wiederherstellung eines Backups von einem AWS-Konto auf ein anderes

AWS Backup unterstützt nicht die Wiederherstellung von Ressourcen von einem AWS-Konto zum anderen. Sie können jedoch ein Backup von einem Konto auf ein anderes Konto kopieren und es dann in diesem Konto wiederherstellen. Sie können beispielsweise kein Backup von Konto A auf Konto B wiederherstellen, aber Sie können ein Backup von Konto A auf Konto B kopieren und es dann in Konto B wiederherstellen.

Das Wiederherstellen eines Backups von einem Konto bei einem anderen ist ein zweistufiger Prozess.

So stellen Sie ein Backup von einem -Konto auf ein anderes wieder her:

1. Kopieren Sie das Backup von der Quelle AWS-Konto auf das Konto, für das Sie die Wiederherstellung durchführen möchten. Anweisungen finden Sie unter Kontoübergreifendes Backup einrichten.
2. Verwenden Sie die entsprechenden Anweisungen für Ihre Ressource, um das Backup wiederherzustellen.

Freigeben eines Backup-Tresors für ein anderes AWS -Konto

AWS Backup ermöglicht es Ihnen, einen Backup-Tresor mit einem oder mehreren Konten oder Ihrer gesamten Organisation gemeinsam zu nutzen AWS Organizations. Sie können einen Ziel-Backup-Tresor mit einem AWS -Quellkonto, einem Benutzer oder einer IAM-Rolle teilen.

So geben Sie einen Ziel-Backup-Tresor frei:

1. Wählen Sie AWS Backup und wählen Sie dann Backup-Tresore.
2. Wählen Sie den Namen des Backup-Tresors aus, den Sie freigeben möchten.
3. Wählen Sie im Bereich Zugriffsrichtlinie die Dropdown-Liste Berechtigungen hinzufügen aus.
4. Wählen Sie Zugriff auf Kontoebene auf einen Backup-Tresor zulassen. Sie können auch wählen, ob Sie Zugriff auf Organisations- oder Rollenebene zulassen möchten.
5. Geben Sie die KontoID des Kontos ein, das Sie für diesen Ziel-Backup-Tresor freigeben möchten.
6. Wählen Sie Richtlinie speichern.

Sie können IAM-Richtlinien verwenden, um Ihren Backup-Tresor freizugeben.

Freigeben eines Ziel-Backup-Tresors für ein AWS-Konto oder eine IAM-Rolle

Die folgende Richtlinie gibt einen Backup-Tresor mit der Kontonummer `4444555566666` und der IAM-Rolle `SomeRole` für die Kontonummer `111122223333` frei.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
```

```
}
```

Teilen Sie einen Ziel-Backup-Tresor mit einer Organisationseinheit, in der AWS Organizations

Die folgende Richtlinie gibt einen Backup-Tresor für Organisationseinheiten, die ihre `PrincipalOrgPaths` verwenden, frei.

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Teilen Sie einen Ziel-Backup-Tresor mit einer Organisation in AWS Organizations

Die folgende Richtlinie teilt gibt einen Backup-Tresor für die Organisation frei mit `PrincipalOrgID` „o-a1b2c3d4e5“.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
```

```
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Konfigurieren eines Kontos als Zielkonto

Wenn Sie zum ersten Mal kontenübergreifende Backups mit Ihrem AWS Organizations Verwaltungskonto aktivieren, kann jeder Benutzer eines Mitgliedskontos sein Konto als Zielkonto konfigurieren. Wir empfehlen, eine oder mehrere der folgenden Service-Kontrollrichtlinien (SCPs) in AWS Organizations festzulegen, um Ihre Zielkonten einzuschränken. Weitere Informationen zum Anhängen von Dienststeuerungsrichtlinien an AWS Organizations Knoten finden Sie unter Dienststeuerungsrichtlinien anhängen und trennen.

Beschränken von Zielkonten mithilfe von Tags

Wenn sie mit einem AWS Organizations Root-, OU- oder Einzelkonto verknüpft sind, beschränkt diese Richtlinie die Kopierziele von diesem Stammkonto, dieser Organisationseinheit oder diesem Konto nur auf die Konten mit Backup-Tresoren, die Sie markiert haben. `DestinationBackupVault` Die Berechtigung `"backup:CopyIntoBackupVault"` steuert, wie sich ein Backup-Tresor verhält und in diesem Fall, welche Ziel-Backup-Tresore gültig sind. Verwenden Sie diese Richtlinie zusammen mit dem entsprechenden Tag, das auf genehmigte Zieltresore angewendet wird, um die Ziele von kontenübergreifenden Kopien zu kontrollieren, die nur an genehmigte Konten und Backup-Tresore gesendet werden.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
```

```
    }
  ]
}
```

Beschränken der Zielkonten mithilfe von Kontonummern und Tresornamen

Wenn sie mit einem AWS Organizations Root-, OU- oder Einzelkonto verknüpft sind, beschränkt diese Richtlinie Kopien, die von diesem Root-, OU- oder Konto stammen, auf nur zwei Zielkonten. Die Berechtigung `"backup:CopyFromBackupVault"` steuert das Verhalten eines Wiederherstellungspunkts im Backup-Tresor und in diesem Fall die Ziele, an die Sie diesen Speicherort kopieren können. Der Quelltresor erlaubt nur Kopien auf das erste Zielkonto (112233445566), wenn ein oder mehrere Namen des Ziel-Backup-Tresors mit `cab-` beginnen. Der Quelltresor erlaubt nur Kopien auf das zweite Zielkonto (123456789012), wenn das Ziel der einzelne Backup-Tresor mit dem Namen `fort-knox` ist.

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Beschränken Sie Zielkonten mithilfe von Organisationseinheiten in AWS Organizations

Wenn sie an ein AWS Organizations Stammkonto oder eine Organisationseinheit angehängt sind, die Ihr Quellkonto enthält, oder wenn sie mit Ihrem Quellkonto verknüpft sind, beschränkt die folgende Richtlinie die Zielkonten auf die Konten innerhalb der beiden angegebenen Organisationseinheiten.

```
{
```

```
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Sicherheitsüberlegungen für kontoübergreifende Backups

Beachten Sie Folgendes, wenn Sie kontoübergreifende Backups in AWS Backup ausführen:

- Der Zieltresor kann nicht der Standardtresor sein. Das liegt daran, dass der Standardtresor mit einem Schlüssel verschlüsselt ist, der nicht mit anderen Konten geteilt werden kann.
- Kontoübergreifende Backups können nach dem Deaktivieren des kontoübergreifenden Backups noch bis zu 15 Minuten lang ausgeführt werden. Dies liegt an der eventuellen Konsistenz und kann dazu führen, dass einige kontoübergreifende Aufträge auch dann gestartet oder abgeschlossen werden, wenn Sie kontoübergreifende Backups deaktivieren.
- Wenn das Zielkonto die Organisation zu einem späteren Zeitpunkt verlässt, behält dieses Konto die Backups bei. Um mögliche Datenlecks zu vermeiden, sollten Sie der `organizations:LeaveOrganization`-Berechtigung in einer Service-Kontrollrichtlinie (SCP), die dem Zielkonto angehängt ist, die Berechtigung verweigern. Ausführliche Informationen zu SCPs finden Sie unter Entfernen eines Mitgliedskontos aus Ihrer Organisation im Benutzerhandbuch für Organisationen.
- Wenn Sie eine Kopierauftragsrolle während eines kontoübergreifenden Kopiervorgangs löschen, AWS Backup kann die Freigabe von Snapshots aus dem Quellkonto nicht rückgängig gemacht werden, wenn der Kopierauftrag abgeschlossen ist. In diesem Fall wird der Backup-Auftrag abgeschlossen, der Status des Kopierauftrags wird jedoch als Snapshot konnte nicht rückgängig gemacht werden angezeigt.

Löschen eines Backups

Wir empfehlen Ihnen, die Backups, die Sie nicht mehr benötigen, automatisch AWS Backup zu löschen, indem Sie Ihren Lebenszyklus bei der Erstellung Ihres Backup-Plans konfigurieren. Wenn Sie beispielsweise den Lebenszyklus Ihres Backup-Plans so einrichten, dass Ihre Wiederherstellungspunkte für ein Jahr aufbewahrt AWS Backup werden, werden die Wiederherstellungspunkte, die am oder innerhalb weniger Stunden nach dem 1. Januar 2021 erstellt wurden, automatisch am 1. Januar 2022 gelöscht. (sortiert AWS Backup die Löschungen innerhalb von 8 Stunden nach Ablauf des Wiederherstellungspunkts nach dem Zufallsprinzip, um die Leistung aufrechtzuerhalten.) Weitere Informationen zum Konfigurieren Ihrer Lebenszyklus-Aufbewahrungsrichtlinie finden Sie unter Erstellen eines Backup-Plans.

Möglicherweise möchten Sie jedoch einen oder mehrere Wiederherstellungspunkte manuell löschen. Beispielsweise:

- Sie haben `EXPIRED` Wiederherstellungspunkte. Diese Wiederherstellungspunkte AWS Backup konnten nicht automatisch gelöscht werden, da Sie die ursprüngliche IAM-Richtlinie, mit der Sie Ihren Backup-Plan erstellt haben, gelöscht oder geändert haben. Beim AWS Backup Versuch, sie zu löschen, fehlte die entsprechende Genehmigung.

  Abgelaufene Wiederherstellungspunkte können auch erstellt werden, wenn auf einen AWS verwalteten Amazon EBS- oder Amazon EC2-Wiederherstellungspunkt eine Amazon EBS Snapshot Lock angewendet wurde und AWS Backup der Lebenszyklusprozess, der normalerweise zur Löschung des Wiederherstellungspunkts führen würde, nicht abschließen kann. Beachten Sie, dass diese abgelaufenen Wiederherstellungspunkte über die Amazon-EC2-Konsole und die API oder die Amazon-EBS-Konsole und die API wiederhergestellt werden können.

  > **Warning**
  >
  > Sie werden weiterhin abgelaufene Wiederherstellungspunkte in Ihrem Konto speichern. Dies könnte Ihre Speicherkosten erhöhen.

  Nach dem 6. August 2021 AWS Backup wird der Ziel-Wiederherstellungspunkt in seinem Backup-Tresor als Abgelaufen angezeigt. Wenn Sie mit der Maus über den roten Status Abgelaufen fahren, wird eine Popover-Statusmeldung angezeigt, in der erklärt wird, warum das Backup nicht gelöscht werden konnte. Sie können auch Aktualisieren wählen, um die neuesten Informationen zu erhalten.

- Sie möchten nicht mehr, dass ein Backup-Plan so ausgeführt wird, wie Sie ihn konfiguriert haben. Die Aktualisierung des Backup-Plans wirkt sich auf zukünftige Wiederherstellungspunkte aus, die er erstellen wird, hat jedoch keine Auswirkungen auf bereits erstellte Wiederherstellungspunkte. Weitere Informationen finden Sie unter Aktualisieren eines Backup-Plans.
- Nach Abschluss eines Tests oder Tutorials sollte eine Bereinigung ausgeführt werden.

Manuelles Löschen von Backups

So löschen Sie Wiederherstellungspunkte manuell:

1. Wählen Sie in der AWS Backup Konsole im Navigationsbereich die Option Backup-Tresore aus.
2. Wählen Sie auf der Seite Backup vaults (Sicherungstresore) den Sicherungstresor, in dem Sie die Sicherungen gespeichert haben.
3. Wählen Sie einen Wiederherstellungspunkt aus, klicken Sie im Dropdown-Menü Aktionen auf Löschen.
4. 1. Wenn Ihre Liste ein kontinuierliches Backup enthält, wählen Sie eine der folgenden Optionen. Jedes kontinuierliche Backup hat einen einzigen Wiederherstellungspunkt.
   - Meine Backup-Daten dauerhaft löschen oder Wiederherstellungspunkt löschen. Wenn Sie eine dieser Optionen auswählen, beenden Sie zukünftige kontinuierliche Backups und löschen auch Ihre vorhandenen kontinuierlichen Backup-Daten.

     > **Note**
     >
     > Kontinuierliche Backups und point-in-time Wiederherstellung (PITR)Weitere Informationen zu den kontinuierlichen Backups von Amazon S3, Amazon RDS und Aurora finden Sie unter.

   - Behalten Sie meine kontinuierlichen Backup-Daten bei oder trennen Sie die Zuordnung des Wiederherstellungspunkts. Wenn Sie eine dieser Optionen auswählen, beenden Sie zukünftige kontinuierliche Backups, behalten aber Ihre vorhandenen kontinuierlichen Backup-Daten, bis sie gemäß Ihrer Aufbewahrungsfrist ablaufen.

     Ein getrennter Amazon S3 S3-Continuous Recovery Point (Backup) verbleibt in seinem Backup-Tresor, sein Status wird jedoch zu `STOPPED` wechseln.

   2. Um alle aufgelisteten Wiederherstellungspunkte zu löschen, geben Sie „Löschen“ ein und wählen Sie dann Wiederherstellungspunkte löschen aus.

3. AWS Backup beginnt, Ihre Wiederherstellungspunkte zum Löschen einzureichen und zeigt einen Fortschrittsbalken an. Lassen Sie Ihren Browser-Tab geöffnet und verlassen Sie diese Seite während des Übermittlungsvorgangs nicht.
4. Am Ende des Einreichungsvorgangs AWS Backup wird Ihnen im Banner ein Status angezeigt. Der Status kann folgendermaßen lauten:
   - Erfolgreich übermittelt. Unter Fortschritt anzeigen können Sie den Löschfortschritt zu jedem Wiederherstellungspunkt anzeigen.
   - Übermittlung ist fehlgeschlagen. Unter Fortschritt anzeigen können Sie den Löschfortschritt zu jedem Wiederherstellungspunkt anzeigen oder es unter Erneut versuchen noch einmal probieren.
   - Ein gemischtes Ergebnis: Einige Wiederherstellungspunkte wurden erfolgreich übermittelt, während andere Wiederherstellungspunkte nicht übermittelt werden konnten.
5. Wenn Sie Fortschritt anzeigen wählen, können Sie den Löschstatus der einzelnen Backups überprüfen. Wenn ein Löschstatus Fehlgeschlagen oder Abgelaufen lautet, können Sie auf diesen Status klicken, um den Grund dafür zu sehen. Sie können auch die Option Fehlgeschlagene Löschungen wiederholen auswählen.

Fehlerbehebung bei manuellen Löschungen

In seltenen Fällen AWS Backup kann Ihre Löschanfrage möglicherweise nicht abgeschlossen werden. AWS Backup verwendet die serviceverknüpfte Rolle`AWSServiceRoleForBackup`, um Löschungen durchzuführen.

Wenn Ihre Löschanfrage fehlschlägt, stellen Sie sicher, dass Ihre IAM-Rolle über die Berechtigung zum Erstellen von serviceverknüpften Rollen verfügt. Stellen Sie insbesondere sicher, dass Ihre IAM-Rolle über die entsprechende `iam:CreateServiceLinkedRole`-Aktion verfügt. Ist dies nicht der Fall, fügen Sie diese Berechtigung der Rolle hinzu, die zum Erstellen eines Backups verwendet wurde. Durch Hinzufügen dieser Berechtigung können manuelle AWS Backup Löschungen durchgeführt werden.

Wenn Sie bestätigt haben, dass die `iam:CreateServiceLinkedRole`-Aktion für Ihre Rolle aktiviert ist, aber Ihre Wiederherstellungspunkte immer noch im `DELETING`-Status hängen bleiben, werden wir Ihr Problem untersuchen. Schließen Sie Ihr manuelles Löschen mit den folgenden Schritten ab:

1. Richten Sie eine Erinnerung ein, um in 2–3 Tagen darauf zurückzukommen.

2. Suchen Sie nach 2–3 Tagen nach kürzlich `EXPIRED` gelöschten Punkten, die das Ergebnis Ihres ersten manuellen Löschvorgangs sind.
3. Löschen Sie diese `EXPIRED`-Wiederherstellungspunkte manuell.

Weitere Informationen zu Rollen finden Sie unter Serviceverknüpfte Rollen verwenden und Hinzufügen und Entfernen von IAM-Identitätsberechtigungen.

Bearbeiten eines Backups

Nachdem Sie ein Backup mit erstellt haben AWS Backup, können Sie den Lebenszyklus oder die Tags des Backups ändern. Der Lebenszyklus definiert, wann eine Sicherung in den Archivspeicher übertragen wird und wann sie abgelaufen ist. AWS Backup übermittelt Sicherungen automatisch gemäß dem von Ihnen definierten Lebenszyklus. Entsprechend laufen diese auch automatisch ab.

Eine Liste der Ressourcen, die Sie in den Cold Storage übertragen können, finden Sie unter „Lebenszyklus bis zu Cold Storage“ in der Tabelle.Verfügbarkeit von Features nach Ressource Der Cold-Storage-Ausdruck wird für andere Ressourcen ignoriert.

> **Note**
>
> Das Bearbeiten der Tags eines Backups mithilfe der AWS Backup Konsole wird nur für Backups von Amazon Elastic File System (Amazon EFS) -Dateisystemen und Advanced Amazon DynamoDB unterstützt.
> Tags, die bei der Erstellung für andere Ressourcen zum Wiederherstellungspunkt hinzugefügt wurden, werden weiterhin angezeigt, sind jedoch ausgegraut und können nicht bearbeitet werden. Auch wenn diese Tags in der AWS Backup Konsole nicht bearbeitet werden können, können Sie die Tags der Backups dieser anderen Services mithilfe der Konsole oder API des Services bearbeiten.

In den Archivspeicher übertragene Sicherungen müssen mindestens 90 Tage lang im Archivspeicher gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Wenn Sie die Einstellung für die Übertragung zum Archivspeicher in Tagen aktualisieren, muss der Wert mindestens dem Alter der Sicherung plus einen Tag entsprechen. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Im folgenden Beispiel wird gezeigt, wie Sie den Lebenszyklus einer Sicherung aktualisieren.

So bearbeiten Sie den Lebenszyklus einer Sicherung:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie im Abschnitt Backups (Sicherungen) eine Sicherung.
4. Wählen Sie auf der Seite mit den Details der Sicherung Edit (Bearbeiten) aus.
5. Konfigurieren Sie die Lebenszykluseinstellungen und wählen Sie dann Save (Speichern).

Wiederherstellen eines Backups

So führen Sie eine Wiederherstellung aus:

Anweisungen zur Konsolenwiederherstellung und Links zur Dokumentation für jeden AWS Backup unterstützten Ressourcentyp finden Sie unter den Links unten auf dieser Seite.

Verwenden Sie den StartRestoreJob-API-Vorgang, um ein Backup programmgesteuert wiederherzustellen.

Die Konfigurationswerte („Wiederherstellungsmetadaten“), die Sie für die Wiederherstellung Ihrer Ressource benötigen, variieren je nach der Ressource, die Sie wiederherstellen möchten. Um die Konfigurationsmetadaten abzurufen, mit denen Ihr Backup erstellt wurde, können Sie GetRecoveryPointRestoreMetadata aufrufen. Beispiele für die Wiederherstellung von Metadaten sind auch in den Links unten auf dieser Seite verfügbar.

Die Wiederherstellung aus Cold Storage dauert in der Regel 4 Stunden länger als die Wiederherstellung aus Warmspeicher.

Für jede Wiederherstellung wird ein Wiederherstellungsauftrag mit einer eindeutigen Auftrags-ID erstellt, z. B. `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

> **Note**
>
> AWS Backup bietet keine Service Level Agreements (SLAs) für die Dauer der Wiederherstellung an. Die Wiederherstellungszeiten können je nach Systemlast und Kapazität variieren, selbst bei Wiederherstellungen, die dieselben Ressourcen enthalten.

Zerstörungsfreie Wiederherstellungen

Wenn Sie AWS Backup ein Backup wiederherstellen, wird mit dem Backup, das Sie wiederherstellen, eine neue Ressource erstellt. Dies dient dazu, Ihre vorhandenen Ressourcen davor zu schützen, durch Ihre Wiederherstellungsaktivitäten zerstört zu werden.

Wiederherstellungstests

Sie können Tests an Ihren Ressourcen durchführen, um eine Wiederherstellung zu simulieren. Auf diese Weise können Sie feststellen, ob Sie Ihr organisatorisches Restore Time Objective (RTO) erreichen, und sich auf zukünftige Wiederherstellungsanforderungen vorbereiten.

Weitere Informationen finden Sie unter Wiederherstellungstests.

Kopieren von Tags während einer Wiederherstellung

> **Note**
>
> Bei Wiederherstellungen von Amazon DynamoDB, Amazon S3, SAP HANA auf Amazon-EC2-Instances, virtuellen Maschinen und Amazon-Timestream-Ressourcen ist dieses Feature derzeit nicht verfügbar.

Einführung

Sie können Tags bei der Wiederherstellung einer Ressource kopieren, wenn die Tags zum Zeitpunkt des Backups zur geschützten Ressource gehörten. Tags, die ein Schlüssel-Wert-Paar enthalten, können Ihnen helfen, Ressourcen zu identifizieren und nach ihnen zu suchen. Wenn Sie einen Wiederherstellungsauftrag starten, können Tags, die zu den ursprünglich gesicherten Ressourcen gehörten, der wiederherzustellenden Ressource hinzugefügt werden.

Wenn Sie sich dafür entscheiden, während eines Wiederherstellungsauftrags Tags einzubeziehen, kann dieser Schritt den Mehraufwand und die Arbeit ersetzen, die mit dem manuellen Anwenden von Tags auf Ressourcen nach Abschluss eines Wiederherstellungsauftrags verbunden ist. Beachten Sie, dass sich dies vom Hinzufügen neuer Tags zu wiederhergestellten Ressourcen unterscheidet.

Wenn Sie ein Backup im Konsolenablauf wiederherstellen, werden Ihre Quell-Tags standardmäßig kopiert. Deaktivieren Sie in der Konsole das Kontrollkästchen, wenn Sie das Kopieren von Tags auf eine wiederhergestellte Ressource deaktivieren möchten.

Bei der API-Operation `StartRestoreJob` ist der Parameter `CopySourceTagsToRestoredResource` standardmäßig auf `false` eingestellt, wodurch die ursprünglichen Quell-Tags von der Ressource ausgeschlossen werden, die Sie wiederherstellen. Wenn Sie Tags aus der Originalquelle einbeziehen möchten, setzen Sie diesen Wert auf `True`.

Überlegungen

- Eine Ressource kann einschließlich wiederhergestellter Ressourcen bis zu 50 Tags enthalten. Weitere Informationen zu Tag-Limits finden Sie unter AWS Ressourcen taggen.
- Stellen Sie sicher, dass die Rolle, die für Wiederherstellungen zum Kopieren von Tags verwendet wird, über die richtigen Berechtigungen verfügt. Die Standardrolle für Wiederherstellungen enthält die erforderlichen Berechtigungen. Eine benutzerdefinierte Rolle muss zusätzliche Berechtigungen zum Markieren von Ressourcen enthalten.
- Die folgenden Ressourcen werden derzeit nicht für die Aufnahme von Wiederherstellungs-Tags unterstützt: VMware Cloud™ on AWS, VMware Cloud™ on, lokale Systeme AWS Outposts, SAP HANA auf Amazon EC2 EC2-Instances, Timestream, DynamoDB, Advanced DynamoDB und Amazon S3.
- Bei kontinuierlichen Backups werden die Tags auf der ursprünglichen Ressource ab dem letzten Backup auf die wiederhergestellte Ressource kopiert.
- Tags werden bei Wiederherstellungen auf Elementebene nicht kopiert.
- Tags, die nach Abschluss des Backup-Auftrags zu einem Backup hinzugefügt wurden, aber vor dem Backup nicht auf der ursprünglichen Ressource vorhanden waren, werden nicht auf die wiederhergestellte Ressource kopiert. Nur Backups, die nach dem 22. Mai 2023 erstellt wurden, kommen für das Kopieren von Tags bei der Wiederherstellung in Frage.

Tag-Interaktion mit bestimmten Ressourcen

- Amazon EC2
  - Auf wiederhergestellte Amazon EC2 EC2-Instances angewendete Tags werden auch auf die angehängten wiederhergestellten Amazon EBS-Volumes angewendet.
  - Tags, die auf die EBS-Volumes angewendet wurden, die an Quell-Instances angehängt sind, werden nicht auf die Volumes kopiert, die den wiederhergestellten Instances zugeordnet sind. Wenn Sie über IAM-Richtlinien verfügen, die Benutzern den Zugriff auf EBS-Volumes anhand ihrer Tags gewähren oder verweigern, müssen Sie den wiederhergestellten Volumes die erforderlichen Tags manuell neu zuweisen, um sicherzustellen, dass Ihre Richtlinien in Kraft bleiben.

- Wenn Sie eine Amazon-EFS-Ressource wiederherstellen, muss sie in ein neues Dateisystem kopiert werden. Bei der Wiederherstellung eines vorhandenen Dateisystems können keine Tags darauf kopiert werden.
- Amazon RDS
  - Wenn das RDS-Cluster, das gesichert wurde, noch aktiv ist, werden Tags aus diesem Cluster kopiert.
  - Wenn das ursprüngliche Cluster nicht mehr aktiv ist, werden stattdessen Tags aus dem Snapshot des Clusters kopiert.
  - Tags, die zum Zeitpunkt des Backups auf der Ressource vorhanden waren, werden während der Wiederherstellung kopiert, unabhängig davon, ob der boolesche Parameter für auf `CopySourceTagsToRestoredResource`, `True` oder `False` gesetzt ist. Wenn der Snapshot jedoch keine Tags enthält, wird die obige boolesche Einstellung verwendet.
- Amazon-Redshift-Cluster enthalten standardmäßig während eines Wiederherstellungsauftrags immer Tags.

Kopieren von Tags über die Konsole

1. Öffnen Sie die AWS Backup -Konsole.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Amazon-S3-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Ressourcendetails wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. So stellen Sie eine Ressource wieder her:
   a. Wählen Sie im Bereich Backup die Wiederherstellungspunkt-ID der Ressource aus.
   b. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen aus (Sie können auch zum Backup-Tresor gehen, den Wiederherstellungspunkt suchen und dann auf Aktionen und dann auf Wiederherstellen klicken).
4. Suchen Sie auf der Seite Backup wiederherstellen den Bereich mit dem Namen „Wiederherstellen mit Tags“. Um alle Tags aus der ursprünglichen Ressource einzubeziehen, behalten Sie das Kontrollkästchen bei (beachten Sie, dass dieses Feld in der Konsole standardmäßig aktiviert ist).
5. Klicken Sie auf Backup wiederherstellen, nachdem Sie alle Ihre bevorzugten Einstellungen und Rollen ausgewählt haben.

So schließen Sie Tags programmgesteuert ein:

Verwenden Sie den API-Vorgang `StartRestoreJob`. Stellen Sie sicher, dass der folgende boolesche Parameter auf `True` gesetzt ist:

```
CopySourceTagsToRestoredResource = true
```

Wenn der boolesche Parameter `CopySourceTagsToRestoredResource` = `True` ist, kopiert der Wiederherstellungsauftrag die Tags von den Originalressourcen in das wiederhergestellte Material.

> **Important**
>
> Der Wiederherstellungsauftrag schlägt fehl, wenn dieser Parameter für eine nicht unterstützte Ressource (VMware, lokale Systeme AWS Outposts, SAP HANA auf EC2-Instances, Timestream, DynamoDB, Advanced DynamoDB und Amazon S3) enthalten ist.

```
{
    "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
}
```

Probleme mit der Tag-Wiederherstellung beheben

FEHLER: unzureichende Berechtigungen

ABHILFE: Stellen Sie sicher, dass Sie in Ihrer Wiederherstellungsrolle über die erforderlichen Berechtigungen verfügen, damit Sie Ihrer wiederhergestellten Ressource Tags hinzufügen können. Die standardmäßige Rollenrichtlinie für AWS verwaltete Dienste für Wiederherstellungen enthält die erforderlichen Berechtigungen für diese AWSBackupServiceRolePolicyForRestoresAufgabe.

Wenn Sie sich für die Verwendung einer benutzerdefinierten Rolle entscheiden, stellen Sie sicher, dass die folgenden Berechtigungen vorhanden sind:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Weitere Informationen finden Sie unter API-Berechtigungen.

Wiederherstellen von Auftragsstatus

Sie können den Status eines Wiederherstellungsauftrags auf der Seite Aufträge der AWS Backup -Konsole anzeigen. Wiederherstellungsauftragsstatus beinhalten Ausstehend, Wird ausgeführt, Abgebrochen, Abgeschlossen und Fehlgeschlagen.

Themen

- Wiederherstellen von S3-Daten
- Wiederherstellen einer virtuellen Maschine mit AWS Backup
- Wiederherstellen eines FSx-Dateisystems
- Wiederherstellen eines Amazon-EBS-Volumes
- Wiederherstellen eines Amazon-EFS-Dateisystems
- Wiederherstellen einer Amazon-DynamoDB-Tabelle
- Wiederherstellen einer RDS-Datenbank
- Wiederherstellung eines Amazon-Aurora-Clusters
- Wiederherstellen einer Amazon-EC2-Instance
- Wiederherstellen eines Storage-Gateway-Volumes
- Wiederherstellen einer Amazon-Timestream-Tabelle
- Wiederherstellen eines Amazon-Redshift-Clusters

- Wiederherstellen von SAP-HANA-Datenbanken auf Amazon-EC2-Instances
- Wiederherstellen eines DocumentDB-Clusters
- Wiederherstellen eines Neptun-Clusters
- Stack-Backups wiederherstellen CloudFormation

Wiederherstellen von S3-Daten

Sie können die S3-Daten, die Sie mit AWS Backup der Speicherklasse S3 Standard gesichert haben, wiederherstellen. Sie können alle Objekte in einem Bucket oder bestimmte Objekte wiederherstellen. Sie können sie in einem vorhandenen oder einem neuen Bucket wiederherstellen.

Amazon S3 S3-Wiederherstellungsberechtigungen

Bevor Sie mit der Wiederherstellung von Ressourcen beginnen, stellen Sie sicher, dass die Rolle, die Sie verwenden, über ausreichende Berechtigungen verfügt.

Weitere Informationen finden Sie in den folgenden Einträgen zu Richtlinien:

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. Verwaltete Richtlinien für AWS Backup

Überlegungen zur Amazon S3 S3-Wiederherstellung

- AWS Backup erstellt eine Sicherungskopie all Ihrer S3-Versionen, stellt jedoch zu einem beliebigen Zeitpunkt nur die neueste Version aus dem Versionsstapel wieder her.
- Access Control Lists (ACLs) müssen im Ziel-Bucket aktiviert sein, andernfalls schlägt der Auftrag fehl. Folgen Sie den Anweisungen auf der Seite ACLs konfigurieren, um ACLs zu aktivieren.
- Wiederherstellungen von Objekten werden übersprungen, wenn der Quell-Bucket ein Objekt mit demselben Namen oder derselben Versions-ID enthält.
- Wenn Sie bestimmte Objekte wiederherstellen, können Sie die aktuelle Version eines Objekts wiederherstellen.
- Wenn Sie den ursprünglichen S3-Bucket wiederherstellen,
  - AWS Backup führt keine destruktive Wiederherstellung durch, was bedeutet, dass unabhängig von der Version kein Objekt anstelle eines bereits vorhandenen Objekts in einen Bucket eingefügt AWS Backup wird.

  - Eine Löschmarkierung in der aktuellen Version wird so behandelt, als ob das Objekt nicht existiert, sodass eine Wiederherstellung erfolgen kann.
  - AWS Backup löscht während einer Wiederherstellung keine Objekte (ohne Löschmarkierungen) aus einem Bucket (Beispiel: Schlüssel, die sich derzeit im Bucket befinden und während der Sicherung nicht vorhanden waren, bleiben erhalten).
- Wiederherstellung regionsübergreifender Kopien
  - S3-Backups können zwar regionsübergreifend kopiert werden, Wiederherstellungsaufträge werden jedoch nur in derselben Region ausgeführt, in der sich das ursprüngliche Backup oder die Kopie befinden.

    Example

    Beispiel: Ein in der Region USA Ost (Nord-Virginia) erstellter S3-Bucket kann in die Region Kanada (Mitte) kopiert werden. Der Wiederherstellungsauftrag kann mithilfe des ursprünglichen Buckets in der Region USA Ost (Nord-Virginia) initiiert und in dieser Region wiederhergestellt werden, oder der Wiederherstellungsauftrag kann mithilfe der Kopie in der Region Kanada (Zentral) initiiert und in dieser Region wiederhergestellt werden.
  - Die ursprüngliche Verschlüsselungsmethode kann nicht zur Wiederherstellung eines Wiederherstellungspunkts (Backup) verwendet werden, der aus einer anderen Region kopiert wurde. Die regionsübergreifende AWS KMS Kopierverschlüsselung ist für Amazon S3 S3-Ressourcen nicht verfügbar. Verwenden Sie stattdessen einen anderen Verschlüsselungstyp für einen Wiederherstellungsauftrag.

Verwenden Sie die AWS Backup Konsole, um Amazon S3 S3-Wiederherstellungspunkte wiederherzustellen

So stellen Sie Ihre Amazon S3 S3-Daten mit der AWS Backup Konsole wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Amazon-S3-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Ressourcendetails wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. So stellen Sie eine Ressource wieder her:

   a. Wählen Sie im Bereich Backups die Wiederherstellungspunkt-ID der Ressource aus.

   b. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.

(Sie können auch zum Backup-Tresor gehen, den Wiederherstellungspunkt suchen und erst auf Aktionen und dann auf Wiederherstellen klicken.)

4. Wenn Sie ein kontinuierliches Backup wiederherstellen, wählen Sie im Bereich Wiederherstellungszeit eine der folgenden Optionen aus:

   a. Akzeptieren Sie die Standardeinstellung für die Wiederherstellung auf den letzten wiederherstellbaren Zeitpunkt.

   b. Geben Sie Datum und Uhrzeit für die Wiederherstellung an.

5. Geben Sie im Bereich Einstellungen an, ob Sie den Gesamten Bucket wiederherstellen oder eine Wiederherstellung auf Elementebene durchführen möchten.

   a. Wenn Sie die Wiederherstellung auf Elementebene wählen, stellen Sie bis zu 5 Elemente (Objekte oder Ordner in einem Bucket) pro Wiederherstellungsauftrag wieder her, indem Sie für jedes Element den S3-URI angeben, der dieses Objekt eindeutig identifiziert.

      (Weitere Informationen zu S3-Bucket-URIs finden Sie unter Zugriff auf einen Bucket im Benutzerhandbuch für Amazon Simple Storage Service.

   b. Wählen Sie Objekt hinzufügen, um ein anderes Element für die Wiederherstellung anzugeben.

6. Wählen Sie Ihr Wiederherstellungsziel. Sie können entweder Im Quell-Bucket wiederherstellen, Bestehenden Bucket verwenden oder Neuen Bucket erstellen wählen.

   > **Note**
   >
   > In Ihrem Ziel-Bucket für die Wiederherstellung muss die Versionierung aktiviert sein. AWS Backup benachrichtigt Sie, wenn der von Ihnen ausgewählte Bucket diese Anforderung nicht erfüllt.

   a. Wenn Sie „Bestehenden Bucket verwenden“ wählen, wählen Sie den S3-Ziel-Bucket aus dem Drop-down-Menü aus, in dem alle vorhandenen Buckets in Ihrer aktuellen Region angezeigt werden. AWS

   b. Wenn Sie Neuen Bucket erstellen wählen, geben Sie den neuen Bucket-Namen ein. Für den neuen Bucket ist standardmäßig die S3-Versionsverwaltung aktiviert. Die Einstellungen für Block Public Access (BPA) sind standardmäßig deaktiviert. Sie können diese Einstellungen ändern, nachdem Sie den Bucket in S3 erstellt haben.

7. Für die Verschlüsselung von Objekten in Ihrem S3-Bucket können Sie Ihre Verschlüsselung für wiederhergestellte Objekte auswählen. Verwenden Sie die ursprünglichen Verschlüsselungsschlüssel (Standard), Amazon-S3-Schlüssel (SSE-S3) oder AWS Key Management Service -Schlüssel (SSE-KMS).

   Diese Einstellungen gelten nur für die Verschlüsselung der Objekte im S3-Bucket. Dies hat keinen Einfluss auf die Verschlüsselung für den Bucket selbst.

   a. Ursprüngliche Verschlüsselungsschlüssel verwenden (Standard) stellt Objekte mit denselben Verschlüsselungsschlüsseln wieder her, die vom Quellobjekt verwendet wurden. Wenn ein Quellobjekt unverschlüsselt war, stellt diese Methode das Objekt ohne Verschlüsselung wieder her.

      Mit dieser Wiederherstellungsoption können Sie optional einen Ersatzverschlüsselungsschlüssel auswählen, um die Wiederherstellungsobjekte zu verschlüsseln, falls der Originalschlüssel nicht verfügbar ist.

   b. Wenn Sie Amazon-S3-Schlüssel (SSE-S3) wählen, müssen Sie keine anderen Optionen angeben.

   c. Wenn Sie AWS Key Management Service Schlüssel (SSE-KMS) wählen, können Sie die folgenden Optionen wählen: Von AWS verwalteter Schlüssel (aws/s3), Wählen Sie aus Ihren AWS KMS Schlüsseln oder Geben Sie den Schlüssel-ARN ein. AWS KMS

      i. Wenn Sie Von AWS verwalteter Schlüssel (aws/s3) wählen, müssen Sie keine anderen Optionen angeben.

      ii. Wenn Sie aus Ihren AWS KMS Schlüsseln wählen, wählen Sie einen AWS KMS Schlüssel aus dem Drop-down-Menü aus. Wählen Sie alternativ Schlüssel erstellen.

      iii. Wenn Sie den AWS KMS Schlüssel-ARN eingeben, geben Sie den ARN in das Textfeld ein. Wählen Sie alternativ Schlüssel erstellen.

8. Wählen Sie im Bereich Rolle wiederherstellen die IAM-Rolle aus, die AWS Backup für diese Wiederherstellung annimmt.

9. Wählen Sie Restore backup aus. Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon S3 S3-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie `StartRestoreJob`. Sie können bei Amazon-S3-Wiederherstellungen die folgenden Metadaten angeben:

```
// 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
```

Status des Wiederherstellungspunkts

Bei den Wiederherstellungspunkten wird der jeweilige Status angezeigt.

`PARTIAL`Der Status gibt an, dass der Wiederherstellungspunkt nicht erstellt werden AWS Backup konnte, bevor das Backup-Fenster geschlossen wurde. Informationen zur Verlängerung des Zeitfensters für Ihren Backup-Plan mithilfe der API finden Sie unter UpdateBackupPlan. Sie können das Fenster Ihres Backup-Plans auch mithilfe der Konsole vergrößern, indem Sie Ihren Backup-Plan auswählen und bearbeiten.

`EXPIRED`Der Status gibt an, dass der Wiederherstellungspunkt seine Aufbewahrungsfrist überschritten hat, aber nicht AWS Backup berechtigt ist oder er aus anderen Gründen nicht gelöscht werden kann. Informationen zum manuellen Löschen dieser Wiederherstellungspunkte finden Sie unter Schritt 3: Löschen der Wiederherstellungspunkte im Abschnitt Ressourcen bereinigen unter Erste Schritte.

Der Status `STOPPED` tritt bei einem kontinuierlichen Backup auf, bei dem ein Benutzer durch eine Aktion das kontinuierliche Backup deaktiviert hat. Dies kann durch das Entfernen von Berechtigungen, das Deaktivieren der Versionierung, das Deaktivieren von Ereignissen, die an

Amazon gesendet werden EventBridge, oder durch das Deaktivieren der EventBridge Regeln, die von eingerichtet wurden, verursacht werden. AWS Backup

Um den Status `STOPPED` zu lösen, stellen Sie sicher, dass alle angeforderten Berechtigungen vorhanden sind und dass die Versionierung für den S3-Bucket aktiviert ist. Sobald diese Bedingungen erfüllt sind, führt die nächste Ausführung einer Backup-Regel dazu, dass ein neuer kontinuierlicher Wiederherstellungspunkt erstellt wird. Die Wiederherstellungspunkte mit dem Status „ANGEHALTEN“ müssen nicht gelöscht werden.

Wiederherstellen einer virtuellen Maschine mit AWS Backup

Sie können eine virtuelle Maschine auf VMware, VMware Cloud on, VMware Cloud on AWS AWS Outposts, einem Amazon EBS-Volume oder auf einer Amazon EC2 EC2-Instance wiederherstellen. Für das Wiederherstellen (oder Migrieren) einer virtuellen Maschine auf EC2 ist eine Lizenz erforderlich. Standardmäßig ist eine Lizenz enthalten (es fallen Gebühren an). AWS Weitere Informationen finden Sie unter Lizenzierungsoptionen im VM Import/Export-Benutzerhandbuch.

Sie können eine virtuelle VMware-Maschine mithilfe der AWS Backup Konsole oder über die wiederherstellen. AWS CLI Wenn eine virtuelle Maschine wiederhergestellt wird, ist der Ordner VMware Tools nicht enthalten. Informationen zur Neuinstallation von VMware Tools finden Sie in der VMware-Dokumentation.

AWS Backup Wiederherstellungen virtueller Maschinen sind zerstörungsfrei, d. h., dass vorhandene virtuelle Maschinen während einer Wiederherstellung AWS Backup nicht überschrieben werden. Stattdessen stellt der Wiederherstellungsjob eine neue virtuelle Maschine bereit.

Aufgaben

- Überlegungen beim Wiederherstellen einer VM auf einer Amazon EC2 EC2-Instance
- Verwenden Sie die AWS Backup Konsole, um die Wiederherstellungspunkte der virtuellen Maschine wiederherzustellen
- Wird AWS CLI zum Wiederherstellen von Wiederherstellungspunkten für virtuelle Maschinen verwendet

Überlegungen beim Wiederherstellen einer VM auf einer Amazon EC2 EC2-Instance

- Für das Wiederherstellen (oder Migrieren) einer virtuellen Maschine auf EC2 ist eine Lizenz erforderlich. Standardmäßig beinhaltet AWS eine Lizenz (es fallen Gebühren an). Weitere Informationen finden Sie unter Lizenzierungsoptionen im VM Import/Export-Benutzerhandbuch.

- Es gibt ein maximales Limit von 5 TB (Terabyte) für jede Festplatte einer virtuellen Maschine.
- Sie können kein key pair angeben, wenn Sie die virtuelle Maschine auf einer Instanz wiederherstellen. Sie können `authorized_keys` während des Starts (über Instance-Benutzerdaten) oder nach dem Start (wie in diesem Abschnitt zur Fehlerbehebung im Amazon EC2 EC2-Benutzerhandbuch beschrieben) ein key pair hinzufügen.
- Vergewissern Sie sich im VM Import/Export User Guide, dass Ihr Betriebssystem für den Import in und Export aus Amazon EC2 unterstützt wird.
- Lesen Sie die Einschränkungen beim Import von VMs in Amazon EC2 im VM Import/Export User Guide.
- Wenn Sie mithilfe von eine Amazon EC2 EC2-Instance wiederherstellen AWS CLI, müssen Sie Folgendes angeben`"RestoreTo":"EC2Instance"`. Alle anderen Attribute haben Standardwerte.

Verwenden Sie die AWS Backup Konsole, um die Wiederherstellungspunkte der virtuellen Maschine wiederherzustellen

Im linken Navigationsbereich der AWS Backup Konsole können Sie eine virtuelle Maschine von mehreren Speicherorten aus wiederherstellen:

- Wählen Sie Hypervisoren, um die Wiederherstellungspunkte für virtuelle Maschinen anzuzeigen, die von einem Hypervisor verwaltet werden, der mit AWS Backup verbunden ist.
- Wählen Sie Virtuelle Maschinen aus, um die Wiederherstellungspunkte für virtuelle Maschinen auf all Ihren Hypervisoren anzuzeigen, die mit AWS Backup verbunden sind.
- Wählen Sie Backup-Tresore, um die in einem bestimmten AWS Backup Tresor gespeicherten Wiederherstellungspunkte anzuzeigen.
- Wählen Sie Geschützte Ressourcen, um die Wiederherstellungspunkte all Ihrer AWS Backup geschützten Ressourcen anzuzeigen.

Wenn Sie eine virtuelle Maschine wiederherstellen müssen, die keine Verbindung mehr mit dem Backup-Gateway hat, wählen Sie Backup-Tresore oder Geschützte Ressourcen, um Ihren Wiederherstellungspunkt zu finden.

Optionen

- Auf VMware wiederherstellen

- Auf einem Amazon EBS-Volume wiederherstellen
- Auf einer Amazon EC2 EC2-Instance wiederherstellen

Um eine virtuelle Maschine auf VMware, VMware Cloud on AWS und VMware Cloud on wiederherzustellen AWS Outposts

1. Wählen Sie in den Ansichten Hypervisoren oder Virtuelle Maschinen den Namen der wiederherzustellenden VM aus. Wählen Sie in der Ansicht Geschützte Ressourcen die Ressourcen-ID der virtuellen Maschine aus, die wiederhergestellt werden soll.
2. Wählen Sie die Radialtaste neben der Wiederherstellungspunkt-ID aus, die wiederhergestellt werden soll.
3. Wählen Sie Restore (Wiederherstellen) aus.
4. Wählen Sie den Wiederherstellungstyp.
    a. Bei der vollständigen Wiederherstellung werden alle Festplatten der virtuellen Maschine wiederhergestellt.
    b. Bei der Wiederherstellung auf Festplattenebene wird eine benutzerdefinierte Auswahl von einer oder mehreren Festplatten wiederhergestellt. Wählen Sie im Dropdown-Menü aus, welche Festplatten wiederhergestellt werden sollen.
5. Wählen Sie den Speicherort für die Wiederherstellung. Die Optionen sind VMware, VMware Cloud on AWS und VMware Cloud on AWS Outposts.
6. Wenn Sie eine vollständige Wiederherstellung durchführen, fahren Sie mit dem nächsten Schritt fort. Wenn Sie eine Wiederherstellung auf Festplattenebene durchführen, wird unter VM-Festplatten ein Dropdown-Menü angezeigt. Wählen Sie mindestens ein startfähiges Volume für die Wiederherstellung aus.
7. Wählen Sie im Dropdown-Menü einen Hypervisor aus, um die wiederhergestellte virtuelle Maschine zu verwalten.
8. Verwenden Sie für die wiederhergestellte virtuelle Maschine die Best Practices Ihrer Organisation, um Folgendes anzugeben:
    a. Name
    b. Pfad (z. B. `/datacenter/vm`)
    c. Name der Rechenressource (z. B. VMHost oder Cluster)

Wenn ein Host Teil eines Clusters ist, können Sie keine Wiederherstellung auf dem Host durchführen, sondern nur auf dem angegebenen Cluster.

d. Datenspeicher

9. Wählen Sie unter Rolle wiederherstellen entweder die Standardrolle aus (empfohlen), oder wählen Sie im Dropdown-Menü IAM-Rolle auswählen aus.
10. Wählen Sie Restore backup aus.
11. Optional: Prüfen Sie, ob Ihr Wiederherstellungsauftrag den Status `Completed` hat. Wählen Sie im linken Navigationsmenü Aufträge aus.

So stellen Sie eine virtuelle Maschine auf einem Amazon EBS-Volume wieder her

1. Wählen Sie in den Ansichten Hypervisoren oder Virtuelle Maschinen den Namen der wiederherzustellenden VM aus. Wählen Sie in der Ansicht Geschützte Ressourcen die Ressourcen-ID der virtuellen Maschine aus, die wiederhergestellt werden soll.
2. Wählen Sie die Radialtaste neben der Wiederherstellungspunkt-ID aus, die wiederhergestellt werden soll.
3. Wählen Sie Restore (Wiederherstellen) aus.
4. Wählen Sie den Wiederherstellungstyp.

   - Die Festplattenwiederherstellung stellt eine benutzerdefinierte Auswahl einer Festplatte wieder her. Wählen Sie im Dropdown-Menü aus, welche Festplatte wiederhergestellt werden soll.

5. Wählen Sie Amazon EBS als Speicherort für die Wiederherstellung aus.
6. Wählen Sie im Dropdown-Menü VM-Festplatte das bootfähige Volume für die Wiederherstellung aus.
7. Wählen Sie unter EBS-Volume-Typ den Volume-Typen aus.
8. Wählen Sie Ihre Availability Zone aus.
9. Verschlüsselung (optional). Markieren Sie das Kästchen, wenn Sie das EBS-Volume verschlüsseln möchten.
10. Wählen Sie Ihren KMS-Schlüssel aus dem Menü aus.
11. Wählen Sie für Rolle wiederherstellen entweder die Standardrolle (empfohlen) oder Wählen Sie eine IAM-Rolle aus.

12. Wählen Sie Restore backup aus.
13. Optional: Prüfen Sie, ob Ihr Wiederherstellungsauftrag den Status `Completed` hat. Wählen Sie im linken Navigationsmenü Aufträge aus.
14. Optional: Weitere Informationen wie Sie verwaltete Volumes bereitstellen und auf Daten auf dem wiederhergestellten Amazon EBS-Volume zugreifen können, finden Sie unter Wie erstelle ich ein logisches LVM-Volume auf einem gesamten Amazon-EBS-Volume?.

So stellen Sie eine virtuelle Maschine auf einer Amazon EC2 EC2-Instance wieder her

1. Wählen Sie in den Ansichten Hypervisoren oder Virtuelle Maschinen den Namen der wiederherzustellenden VM aus. Wählen Sie in der Ansicht Geschützte Ressourcen die Ressourcen-ID der virtuellen Maschine aus, die wiederhergestellt werden soll.
2. Wählen Sie die Radialtaste neben der Wiederherstellungspunkt-ID aus, die wiederhergestellt werden soll.
3. Wählen Sie Restore (Wiederherstellen) aus.
4. Wählen Sie den Wiederherstellungstyp.

    - Bei der vollständigen Wiederherstellung wird das Dateisystem vollständig wiederhergestellt, einschließlich des Ordners und der Dateien auf Stammebene.
5. Wählen Sie Amazon EC2 als Speicherort für die Wiederherstellung aus.
6. Wählen Sie unter Instanztyp die Kombination aus Rechenleistung und Arbeitsspeicher aus, die für die Ausführung Ihrer Anwendung auf Ihrer neuen Instance erforderlich ist.

    > **Tip**
    >
    > Wählen Sie einen Instanztyp, der den Spezifikationen der ursprünglichen virtuellen Maschine entspricht oder diese übertrifft. Weitere Informationen finden Sie im Amazon EC2 Instance Types Guide.

7. Wählen Sie für Virtual Private Cloud (VPC) eine Virtual Private Cloud (VPC) aus, die die Netzwerkumgebung für die Instanz definiert.
8. Wählen Sie für Subnet eines der Subnetze in der VPC aus. Ihre Instance erhält eine private IP-Adresse aus dem Subnetz-Adressbereich.
9. Wählen Sie für Sicherheitsgruppen eine Sicherheitsgruppe aus, die als Firewall für den Datenverkehr zu Ihrer Instance fungiert.

10. Wählen Sie für Wiederherstellungsrolle entweder die Standardrolle (empfohlen) oder Wählen Sie eine IAM-Rolle aus.
11. Optional: Um beim Start ein Skript auf Ihrer Instance auszuführen, erweitern Sie Erweiterte Einstellungen und geben Sie das Skript unter Benutzerdaten ein.
12. Wählen Sie Restore backup aus.
13. Optional: Prüfen Sie, ob Ihr Wiederherstellungsauftrag den Status `Completed` hat. Wählen Sie im linken Navigationsmenü Aufträge aus.

Wird AWS CLI zum Wiederherstellen von Wiederherstellungspunkten für virtuelle Maschinen verwendet

Verwenden Sie `StartRestoreJob`.

Sie können die folgenden Metadaten für die Wiederherstellung einer virtuellen Maschine in Amazon EC2 und Amazon EBS angeben:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Sie können die folgenden Metadaten für die Wiederherstellung einer virtuellen Maschine auf VMware, VMware Cloud on AWS und VMware Cloud on AWS Outpost angeben:

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

Dieses Beispiel veranschaulicht, wie eine vollständige Wiederherstellung auf VMware durchgeführt wird:

```
'{"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"}'
```

Wiederherstellen eines FSx-Dateisystems

Die Wiederherstellungsoptionen, die verfügbar sind, wenn Sie Amazon FSx-Dateisysteme wiederherstellen, sind dieselben wie bei der Verwendung des nativen Amazon FSx-Backups. AWS Backup Sie können den Wiederherstellungspunkt eines Backups verwenden, um ein neues Dateisystem zu erstellen und einen point-in-time Snapshot eines anderen Dateisystems wiederherzustellen.

AWS Backup Erstellt bei der Wiederherstellung von Amazon FSx-Dateisystemen ein neues Dateisystem und füllt es mit den Daten (Amazon FSx for NetApp ONTAP ermöglicht die Wiederherstellung eines Volumes in einem vorhandenen Dateisystem). Dies ähnelt der Art und Weise, wie natives Amazon FSx Dateisysteme sichert und wiederherstellt. Das Wiederherstellen eines Backups in einem neuen Dateisystem dauert genauso lange wie das Erstellen eines neuen Dateisystems. Die aus dem Backup wiederhergestellten Daten werden verzögert in das Dateisystem geladen. Daher kann es während des Vorgangs zu einer etwas höheren Latenz kommen.

> **Note**
>
> Sie können keine Wiederherstellung auf ein vorhandenes Amazon-FSx-Dateisystem durchführen, und Sie können keine einzelnen Dateien oder Ordner wiederherstellen.

FSx für ONTAP unterstützt das Backup von bestimmten Volume-Typen nicht, darunter DP-Volumes (Datenschutz), LS-Volumes (Load-Sharing), FlexGroup-Volumes, vollständige Volumes oder Volumes auf Dateisystemen, die voll sind. Weitere Informationen finden Sie unter Arbeiten mit FSx-für-ONTAP-Backups.
AWS Backup Tresore, die Wiederherstellungspunkte von Amazon FSx-Dateisystemen enthalten, sind außerhalb von sichtbar. AWS Backup Sie können die Wiederherstellungspunkte mit Amazon FSx wiederherstellen, aber Sie können sie nicht löschen.

Sie können Backups, die mit der integrierten automatischen Backup-Funktion von Amazon FSx erstellt wurden, von der AWS Backup Konsole aus sehen. Sie können diese Backups auch mithilfe von AWS Backup wiederherstellen. Sie können diese Backups jedoch nicht löschen oder die automatischen Backup-Zeitpläne Ihrer Amazon FSx-Dateisysteme mithilfe AWS Backup von ändern.

Sie können Backups wiederherstellen, die AWS Backup mit der AWS Backup Konsole, der API oder AWS CLI erstellt wurden. In diesem Abschnitt erfahren Sie, wie Sie die AWS Backup Konsole zur Wiederherstellung von Amazon FSx-Dateisystemen verwenden.

Verwenden Sie die AWS Backup Konsole, um Amazon FSx-Wiederherstellungspunkte wiederherzustellen

Wiederherstellen eines FSx-für-Windows-File-Server-Dateisystems

So stellen Sie ein FSx-für-Windows-File-Server-Dateisystem wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die Amazon-FSx-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Wählen Sie die Wiederherstellungspunkt-ID der Ressource aus.
4. Wählen Sie in der oberen rechten Ecke des Bereichs Wiederherstellen aus, um die Seite Backup wiederherstellen zu öffnen.
5. Im Abschnitt Dateisystemdetails wird die ID Ihres Backups unter Backup-ID und der Dateisystemtyp unter Dateisystemtyp angezeigt. Sie können FSx-für-Windows-File-Server- und FSx-für-Lustre-Dateisysteme wiederherstellen.

6. Akzeptieren Sie den Standardwert für den Bereitstellungstyp. Sie können den Bereitstellungstyp eines Dateisystems während der Wiederherstellung nicht ändern.
7. Wählen Sie den zu verwendenden Speichertyp aus. Wenn die Speicherkapazität Ihres Dateisystems weniger als 2.000 GiB beträgt, können Sie den Speichertyp HDD nicht verwenden.
8. Wählen Sie unter Durchsatzkapazität die Option Empfohlene Durchsatzkapazität, um die empfohlene Rate von 16 MB pro Sekunde (MBps) zu verwenden, oder wählen Sie Durchsatzkapazität angeben und geben Sie eine neue Rate ein.
9. Geben Sie im Abschnitt Netzwerk und Sicherheit die erforderlichen Informationen ein.
10. Wenn Sie ein FSx-für-Windows-File-Server-Dateisystem wiederherstellen, geben Sie die Windows-Authentifizierungsinformationen an, die für den Zugriff auf das Dateisystem verwendet wurden, oder Sie erstellen neue.

    > **Note**
    >
    > Beim Wiederherstellen eines Backups können Sie den Active-Directory-Typ im Dateisystem nicht ändern.

    Weitere Informationen zu Microsoft Active Directory finden Sie unter Arbeiten mit Active Directory in Amazon FSx für Windows File Server im Benutzerhandbuch zu Amazon FSx für Windows File Server.
11. (Optional) Geben Sie im Abschnitt Backup und Wartung die Informationen an, mit denen Sie Ihre Backup-Einstellungen festlegen können.
12. Wählen Sie im Abschnitt Wiederherstellungsrolle die IAM-Rolle aus, mit der AWS Backup Ihre Backups in Ihrem Namen erstellen und verwalten soll. Wir empfehlen Ihnen, die Standardrolle zu ändern. Wenn keine Standardrolle vorhanden ist, wird für Sie eine mit den korrekten Berechtigungen erstellt. Sie können auch Ihre eigene IAM-Rolle angeben.
13. Überprüfen Sie alle Ihre Eingaben und wählen Sie Backup wiederherstellen.

Wiederherstellen eines Amazon-für-Lustre-Dateisystems

AWS Backup unterstützt Amazon FSx for Lustre-Dateisysteme mit persistentem Speicherbereitstellungstyp, die nicht mit einem Daten-Repository wie Amazon S3 verknüpft sind.

So stellen Sie ein Amazon-FSx-für-Lustre-Dateisystem wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die Amazon-FSx-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Wählen Sie die Wiederherstellungspunkt-ID der Ressource aus.
4. Wählen Sie in der oberen rechten Ecke des Bereichs Wiederherstellen aus, um die Seite Backup in neuem Dateisystem wiederherstellen zu öffnen.
5. Im Abschnitt Einstellungen wird die ID Ihres Backup unter Backup-ID und der Dateisystemtyp unter Dateisystemtyp angezeigt. Der Dateisystemtyp sollte Lustre sein.
6. (Optional) Geben Sie einen Namen für das Dateisystem ein.
7. Wählen Sie einen Bereitstellungstyp aus. AWS Backup unterstützt nur den persistenten Bereitstellungstyp. Sie können den Bereitstellungstyp eines Dateisystems während der Wiederherstellung nicht ändern.

   Der persistente Bereitstellungstyp ist für die Langzeitspeicherung vorgesehen. Ausführliche Informationen zu den Bereitstellungsoptionen von FSx für Lustre finden Sie unter Verwenden verfügbarer Bereitstellungsoptionen für Amazon-FSx-für-Lustre-Dateisysteme im Benutzerhandbuch zu Amazon FSx für Lustre.
8. Wählen Sie den Durchsatz pro Speichereinheit, den Sie verwenden möchten.
9. Geben Sie die zu verwendende Speicherkapazität an. Geben Sie eine Kapazität zwischen 32 GiB und 64.436 GiB ein.
10. Geben Sie im Abschnitt Netzwerk und Sicherheit die erforderlichen Informationen ein.
11. (Optional) Geben Sie im Abschnitt Backup und Wartung die Informationen an, mit denen Sie Ihre Backup-Einstellungen festlegen können.
12. Wählen Sie im Abschnitt Wiederherstellungsrolle die IAM-Rolle aus, mit der AWS Backup Ihre Backups in Ihrem Namen erstellen und verwalten soll. Wir empfehlen Ihnen, die Standardrolle zu ändern. Wenn keine Standardrolle vorhanden ist, wird für Sie eine mit den korrekten Berechtigungen erstellt. Sie können auch Ihre IAM-Rolle angeben.
13. Überprüfen Sie alle Ihre Eingaben und wählen Sie Backup wiederherstellen.

Amazon FSx für NetApp ONTAP-Volumes wiederherstellen

So stellen Sie Amazon FSx for NetApp ONTAP-Volumes wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die Amazon-FSx-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Wählen Sie die Wiederherstellungspunkt-ID der Ressource aus.
4. Wählen Sie in der oberen rechten Ecke des Bereichs Wiederherstellen aus, um die Seite Wiederherstellen zu öffnen.

   Im ersten Abschnitt, Dateisystemdetails, werden die Wiederherstellungspunkt-ID, die Dateisystem-ID und der Dateisystemtyp angezeigt.
5. Unter Wiederherstellungsoptionen gibt es mehrere Auswahlmöglichkeiten. Wählen Sie zunächst das Dateisystem aus dem Dropdown-Menü aus.
6. Wählen Sie als Nächstes die bevorzugte virtuelle Speichermaschine aus dem Dropdown-Menü aus.
7. Geben Sie einen Namen für Ihr Volume ein.
8. Geben Sie den Junction Path an. Dabei handelt es sich um den Speicherort in Ihrem Dateisystem, an dem Ihr Volume bereitgestellt werden soll.
9. Geben Sie die Volume-Größe in Megabyte (MB) an, die Sie erstellen.
10. (Optional) Sie können wählen, ob Speichereffizienz aktiviert werden soll, indem Sie das Kästchen aktivieren. Dies ermöglicht Deduplizierung, Komprimierung und Verdichtung.
11. Wählen Sie im Dropdown-Menü Richtlinie für Kapazitätspool-Tiering die gewünschte Tiering-Präferenz aus.
12. Wählen Sie in den Wiederherstellungsberechtigungen die IAM-Rolle aus, die zum Wiederherstellen von Backups verwendet AWS Backup werden soll.
13. Überprüfen Sie alle Ihre Eingaben und wählen Sie Backup wiederherstellen.

Wiederherstellen eines Amazon-FSx-für-OpenZFS-Dateisystems

So stellen Sie ein Amazon-FSx-für-OpenZFS-Dateisystem wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die Amazon-FSx-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Wählen Sie die Wiederherstellungspunkt-ID der Ressource aus.
4. Wählen Sie in der oberen rechten Ecke des Bereichs Wiederherstellen aus, um die Seite Backup wiederherstellen zu öffnen.

   Im Abschnitt Dateisystemdetails wird die ID Ihres Backup unter Backup-ID und der Dateisystemtyp unter Dateisystemtyp angezeigt. Der Dateisystemtyp sollte FSx für OpenZFS sein.
5. Unter Wiederherstellungsoptionen können Sie Schnellwiederherstellung oder Standardwiederherstellung auswählen. Bei der Schnellwiederherstellung werden die Standardeinstellungen des Quelldateisystems verwendet. Wenn Sie eine Schnellwiederherstellung durchführen, fahren Sie mit Schritt 7 fort.

   Wenn Sie die Standardwiederherstellung wählen, geben Sie die folgenden zusätzlichen Konfigurationen an:

   a. Bereitgestellte SSD-IOPS: Sie können das Optionsfeld Automatisch oder, falls verfügbar, die Option Vom Benutzer bereitgestellt wählen.
   b. Durchsatzkapazität: Sie können die empfohlene Durchsatzkapazität von 64 MB/s oder die Option Durchsatzkapazität angeben wählen.
   c. (Optional) VPC-Sicherheitsgruppen: Sie können VPC-Sicherheitsgruppen angeben, die der Netzwerkschnittstelle Ihres Dateisystems zugeordnet werden sollen.
   d. Verschlüsselungsschlüssel: Geben Sie den AWS Key Management Service Schlüssel an, mit dem die wiederhergestellten Dateisystemdaten im Ruhezustand geschützt werden sollen.
   e. (Optional) Konfiguration des Root-Volumes: Diese Konfiguration ist standardmäßig ausgeblendet. Sie können sie erweitern, indem Sie auf das nach unten zeigende Karat (Pfeil) klicken. Wenn Sie ein Dateisystem aus einem Backup erstellen, wird ein neues Dateisystem erstellt. Die Volumes und Snapshots behalten ihre Quellkonfigurationen bei.

f. (Optional) Backup und Wartung: Um ein geplantes Backup einzurichten, klicken Sie auf das nach unten zeigende Karat (Pfeil), um den Abschnitt zu erweitern. Sie können das Backup-Fenster, Stunde und Minute, Aufbewahrungszeitraum und wöchentliches Wartungsfenster wählen.

6. (Optional) Sie können einen Namen für Ihr Volume eingeben.
7. Die SSD-Speicherkapazität zeigt die Speicherkapazität des Dateisystems an.
8. Wählen Sie die Virtual Private Cloud (VPC), von der aus auf Ihr Dateisystem zugegriffen werden kann.
9. Wählen Sie im Dropdown-Menü Subnetz das Subnetz aus, in dem sich die Netzwerkschnittstelle Ihres Dateisystems befindet.
10. Wählen Sie im Abschnitt Wiederherstellungsrolle die IAM-Rolle aus, mit der AWS Backup Sie Ihre Backups in Ihrem Namen erstellen und verwalten möchten. Wir empfehlen Ihnen, die Standardrolle zu ändern. Wenn keine Standardrolle vorhanden ist, wird für Sie eine mit den korrekten Berechtigungen erstellt. Sie haben auch die Möglichkeit, eine IAM-Rolle auszuwählen.
11. Überprüfen Sie alle Ihre Eingaben und wählen Sie Backup wiederherstellen.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon FSx-Wiederherstellungspunkte wiederherzustellen

Um Amazon FSx mithilfe der API oder CLI wiederherzustellen, verwenden Sie `StartRestoreJob`. Sie können bei Amazon-FSx-Wiederherstellungen die folgenden Metadaten angeben:

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
```

```
OpenZFSConfiguration
aws:backup:request-id
```

FSx für Windows File Server – Metadaten für die Wiederherstellung

Sie können bei FSx-für-Windows-File-Server-Wiederherstellungen die folgenden Metadaten angeben:

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx für Lustre – Metadaten für die Wiederherstellung

Sie können während einer FSx-für-Lustre-Wiederherstellung `PerUnitStorageThroughput` und `DriveCacheType` angeben.

FSx für ONTAP – Metadaten für die Wiederherstellung

Sie können bei FSx-für-ONTAP-Wiederherstellungen die folgenden Metadaten angeben:

- Name des zu erstellenden Volumes: #name
- OntapConfiguration: # Ontap-Konfiguration
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx für OpenZFS – Metadaten für die Wiederherstellung

Sie können bei FSx-für-OpenZFS-Wiederherstellungen die folgenden Metadaten angeben:

- `ThroughputCapacity`
- `DesklopsConfiguration`
- Wenn IOPS angegeben ist, müssen Sie einen Wert zwischen 0 und 160.000 angeben, den Modus jedoch nicht.

Beispiel für einen CLI-Wiederherstellungsbefehl:

```
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\"}"'
```

Beispiel für Metadaten für die Wiederherstellung:

```
"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\\\"]\"}"
```

Wiederherstellen eines Amazon-EBS-Volumes

Wenn Sie einen Amazon Elastic Block Store (Amazon EBS) -Snapshot wiederherstellen, AWS Backup wird ein neues Amazon EBS-Volume erstellt, das Sie an Ihre Amazon EC2 EC2-Instance anhängen können.

Sie können den Snapshot als EBS-Volume oder als AWS Storage Gateway -Volume wiederherstellen.

Verwenden Sie die AWS Backup Konsole, um Amazon EBS-Wiederherstellungspunkte wiederherzustellen

So stellen Sie Amazon-EBS-Volumes wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die EBS-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.

4. Geben Sie die Wiederherstellungsparameter für Ihre Ressource an. Die von Ihnen eingegebenen Wiederherstellungsparameter beziehen sich auf den ausgewählten Ressourcentyp.

   Wählen Sie unter Ressourcentyp die AWS Ressource aus, die bei der Wiederherstellung dieses Backups erstellt werden soll.

5. Wenn Sie EBS volume (EBS-Volume) auswählen, geben Sie die Werte für Volume type (Volume-Typ) und Size (Größe) (GiB) an und wählen Sie eine Availability Zone aus.

   - Nach dem Durchsatz erscheint das optionale Kontrollkästchen Dieses Volume verschlüsseln. Diese Option bleibt aktiv, wenn der EBS-Wiederherstellungspunkt verschlüsselt ist.

     Sie können einen KMS-Schlüssel angeben oder einen AWS KMS Schlüssel erstellen.

   Wenn Sie sich für ein Speicher-Gateway-Volume entscheiden, wählen Sie ein Gateway in einem erreichbaren Status. Wählen Sie auch Ihren iSCSI-Zielnamen.

   - Wählen Sie für Volume-Stored-Gateways eine Festplatten-ID aus.
   - Wählen Sie für Volume-Cached-Gateways eine Kapazität, die mindestens so groß ist wie Ihre geschützte Ressource.

6. Wählen Sie unter Wiederherstellungsrolle die IAM-Rolle aus, die für diese Wiederherstellung übernommen AWS Backup werden soll.

   > **Note**
   >
   > Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine Standardrolle mit den richtigen Berechtigungen für Sie erstellt. Sie können diese Standardrolle löschen oder unbrauchbar machen.

7. Wählen Sie Restore backup aus.

   Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Bei der Wiederherstellung eines archivierten EBS-Snapshots wird dieser vorübergehend von Cold zu Warm Storage verschoben, um ein neues EBS-Volume zu erstellen. Für diese Art der Wiederherstellung fällt eine einmalige Abrufgebühr an. Während dieses Wiederherstellungszeitraums

werden die Speicherkosten für Warm und Cold Storage in Rechnung gestellt. EBS-Volumes im Cold Storage können nicht auf einem Backup-Gateway-Volume wiederhergestellt werden.

Sie können einen archivierten EBS-Snapshot in Cold Storage mithilfe der AWS Backup -Konsole oder der Befehlszeile wiederherstellen. Eine Wiederherstellung aus Cold Storage kann bis zu 72 Stunden dauern. Weitere Informationen finden Sie unter Archivieren von Amazon EBS-Snapshots im Amazon EBS-Benutzerhandbuch.

Console

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Navigieren Sie zu Backup-Tresore > *Tresor* > Wiederherstellen eines archivierten EBS-Snapshots.
3. Geben Sie im Abschnitt Einstellungen einen Wert zwischen (einschließlich) 0 und 180 ein, der die Anzahl der Tage angibt, für die ein archivierter Snapshot vorübergehend wiederhergestellt werden soll.
4. Geben Sie weitere Einstellungen ein: Volume-Typ, Größe, IOPS, Availability Zone, Durchsatz und Verschlüsselung.
5. Wählen Sie Ihre Wiederherstellungsrolle.
6. Wählen Sie Backup wiederherstellen aus. Bestätigen Sie im Bestätigungs-Popup die Snapshots und den Wiederherstellungstyp. Wählen Sie dann Snapshot wiederherstellen aus.

AWS CLI

1. Verwenden von `start-restore-job`
2. Schließen Sie die Parameter ein.
3.
4.
5.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon EBS-Wiederherstellungspunkte wiederherzustellen

Um Amazon EBS mithilfe der API oder CLI wiederherzustellen, verwenden Sie `StartRestoreJob`. Sie können bei Amazon-EBS-Wiederherstellungen die folgenden Metadaten angeben:

```
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
```

Beispiel:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Wiederherstellen eines Amazon-EFS-Dateisystems

Wenn Sie eine Amazon-EFS-Instance (Amazon Elastic File System) wiederherstellen, können Sie eine vollständige Wiederherstellung oder Wiederherstellung auf Elementebene durchführen.

Vollständige Wiederherstellung

Wenn Sie die vollständige Wiederherstellung durchführen, wird das gesamte Dateisystem wiederhergestellt.

AWS Backup unterstützt keine destruktiven Wiederherstellungen mit Amazon EFS. Eine destruktive Wiederherstellung liegt vor, wenn ein wiederhergestelltes Dateisystem das Quelldateisystem oder das vorhandene Dateisystem löscht oder überschreibt. AWS Backup stellt Ihr Dateisystem stattdessen in einem Wiederherstellungsverzeichnis außerhalb des Stammverzeichnisses wieder her.

Wiederherstellung auf Elementebene

Wenn Sie eine Wiederherstellung auf Elementebene durchführen, wird eine bestimmte Datei oder ein bestimmtes Verzeichnis AWS Backup wiederhergestellt. Sie müssen den Pfad relativ zum Dateisystemstamm angeben. Wenn das Dateisystem beispielsweise in `/user/home/myname/efs` gemountet ist und der Dateipfad `user/home/myname/efs/file1` ist, geben Sie **`/file1`** ein. Bei Pfaden muss die Groß- und Kleinschreibung beachtet werden. Platzhalterzeichen und RegEx werden nicht unterstützt. Ihr Pfad kann sich von dem Pfad auf dem Host unterscheiden, wenn das Dateisystem über einen Zugriffspunkt gemountet wird.

Sie können bis zu 10 Elemente auswählen, wenn Sie mit der Konsole eine EFS-Wiederherstellung durchführen. Es gibt kein Elementlimit, wenn Sie CLI für die Wiederherstellung verwenden. Es gibt jedoch ein Limit von 200 KB für die Länge der Wiederherstellungsmetadaten, die übergeben werden können.

Sie können diese Elemente entweder in einem neuen oder einem vorhandenen Dateisystem wiederherstellen. In beiden Fällen erstellt AWS Backup ein neues Amazon-EFS-Verzeichnis (`aws-backup-restore_`*`datetime`*) aus dem Stammverzeichnis, das die Elemente enthält. Die vollständige Hierarchie der angegebenen Elemente bleibt im Wiederherstellungsverzeichnis erhalten. Wenn beispielsweise das Verzeichnis A die Unterverzeichnisse B, C und D enthält, behält AWS Backup die hierarchische Struktur bei, wenn A, B, C und D wiederhergestellt werden. Unabhängig davon, ob Sie eine Amazon-EFS-Wiederherstellung auf Elementebene in einem vorhandenen Dateisystem oder in einem neuen Dateisystem durchführen, wird bei jedem Wiederherstellungsversuch ein neues Wiederherstellungsverzeichnis aus dem Stammverzeichnis erstellt, das die wiederhergestellten Dateien enthält. Wenn Sie mehrere Wiederherstellungen für denselben Pfad versuchen, existieren möglicherweise mehrere Verzeichnisse, die die wiederhergestellten Elemente enthalten.

> **Note**
>
> Wenn Sie nur eine wöchentliche Sicherung beibehalten, können Sie den Status des Dateisystems nur zu dem Zeitpunkt wiederherstellen, an dem Sie die Sicherung erstellt haben. Sie können keine vorherigen inkrementellen Sicherungen wiederherstellen.

Verwenden Sie die AWS Backup Konsole, um einen Amazon EFS-Erholungspunkt wiederherzustellen

So stellen Sie ein Amazon-EFS-Dateisystem wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Ihr EFS-Backup-Tresor erhält die Zugriffsrichtlinie `Deny backup:StartRestoreJob` bei der Erstellung. Wenn Sie Ihren Backup-Tresor zum ersten Mal wiederherstellen, müssen Sie Ihre Zugriffsrichtlinie wie folgt ändern.

   a. Wählen Sie Backup vaults (Sicherungstresore) aus.

   b. Wählen Sie den Backup-Tresor aus, der den Wiederherstellungspunkt enthält, den Sie wiederherstellen möchten.

c. Scrollen Sie nach unten bis zur Richtlinie für den Tresor-Zugriff

d. Falls vorhanden, löschen Sie `backup:StartRestoreJob` aus dem `Statement`. Wählen Sie dazu Bearbeiten, `backup:StartRestoreJob` löschen und anschließend Richtlinie speichern aus.

3. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die EFS-Dateisystem-ID aus, die Sie wiederherstellen möchten.

4. Auf der Seite Ressourcendetails wird eine Liste der Wiederherstellungspunkte für die ausgewählte Dateisystem-ID angezeigt. Um ein Dateisystem wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID des Dateisystems aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.

5. Geben Sie die Wiederherstellungsparameter für Ihr Dateisystem an. Die von Ihnen eingegebenen Wiederherstellungsparameter beziehen sich auf den ausgewählten Ressourcentyp.

   Sie können eine Full restore (Vollständige Wiederherstellung) durchführen, die das gesamte Dateisystem wiederherstellt. Sie können auch bestimmte Dateien und Verzeichnisse mithilfe einer Item-level restore (Wiederherstellung auf Elementebene) wiederherstellen.

   - Wählen Sie die Option Vollständige Wiederherstellung aus, um das Dateisystem in seiner Gesamtheit wiederherzustellen, einschließlich aller Ordner und Dateien auf Stammebene.
   - Wählen Sie die Option Item-level restore (Wiederherstellungsoption auf Elementebene) aus, um eine bestimmte Datei oder ein bestimmtes Verzeichnis wiederherzustellen. Sie können bis zu fünf Elemente in Amazon EFS auswählen und wiederherstellen.

     Um eine bestimmte Datei oder ein bestimmtes Verzeichnis wiederherzustellen, müssen Sie den relativen Pfad für den Mountingpunkt angeben. Wenn das Dateisystem beispielsweise in `/user/home/myname/efs` gemountet und der Dateipfad „`user/home/myname/efs/file1`“ ist, geben Sie „**`/file1`**“ ein. Pfade beachten die Groß- und Kleinschreibung und dürfen keine Sonderzeichen, Platzhalter und RegEx-Zeichenfolgen enthalten.

     1. Geben Sie im Textfeld Item path (Elementpfad) den Pfad für die Datei oder den Ordner ein.
     2. Wählen Sie Add item (Element hinzufügen) aus, um weitere Dateien oder Verzeichnisse hinzuzufügen. Sie können bis zu fünf Elemente in Ihrem EFS-Dateisystem auswählen und wiederherstellen.

6. Für Restore location (Speicherort für Wiederherstellung)

- Wählen Sie In Verzeichnis im Quelldateisystem wiederherstellen aus, wenn Sie das Quelldateisystem wiederherstellen möchten.
- Wählen Sie In einem neuen Dateisystem wiederherstellen aus, wenn Sie in einem anderen Dateisystem wiederherstellen möchten.

7. Für Dateisystemtypen

   - (Empfohlen) Wählen Sie Regional, wenn Sie Ihr Dateisystem in mehreren AWS Availability Zones wiederherstellen möchten.
   - Wählen Sie Eine Zone, wenn Sie Ihr Dateisystem in einer einzigen Availability Zone wiederherstellen möchten. Wählen Sie dann in der Dropdown-Liste Availability Zone das Ziel für Ihre Wiederherstellung aus.

   Weitere Informationen finden Sie unter Amazon-EFS-Speicherklassen verwalten im Amazon-EFS-Benutzerhandbuch.

8. Für Leistung

   - Wenn Sie sich für eine regionale Wiederherstellung entschieden haben, wählen Sie entweder (Empfohlen) Allgemeine Zwecke oder Max. I/O aus.
   - Wenn Sie sich für eine One-Zone-Wiederherstellung entschieden haben, müssen Sie (Empfohlen) Allgemeine Zwecke wählen. One-Zone-Wiederherstellungen unterstützen Max. I/O nicht.

9. Für Verschlüsselung aktivieren

   - Wählen Sie Verschlüsselung aktivieren aus, wenn Sie Ihr Dateisystem verschlüsseln möchten. KMS-Schlüssel-IDs und Aliase werden in der Liste angezeigt, nachdem sie mit der Konsole AWS Key Management Service (AWS KMS) erstellt wurden.
   - Wählen Sie im Textfeld KMS-Schlüssel den zu verwendenden Schlüssel aus der Liste aus.

10. Wählen Sie unter Wiederherstellungsrolle die IAM-Rolle aus, die für diese Wiederherstellung verwendet AWS Backup werden soll.

> **Note**
>
> Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine Standardrolle mit den richtigen Berechtigungen für Sie erstellt. Sie können diese Standardrolle löschen oder unbrauchbar machen.

11. Wählen Sie Restore backup aus.

    Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

    > **Note**
    >
    > Wenn Sie nur eine wöchentliche Sicherung beibehalten, können Sie den Status des Dateisystems nur zu dem Zeitpunkt wiederherstellen, an dem Sie die Sicherung erstellt haben. Sie können keine vorherigen inkrementellen Sicherungen wiederherstellen.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon EFS-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie `StartRestoreJob`. Beim Wiederherstellen einer Amazon-EFS-Instance können Sie ein ganzes Dateisystem oder bestimmte Dateien oder Verzeichnisse wiederherstellen. Um Amazon-EFS-Ressourcen wiederherzustellen, benötigen Sie die folgenden Informationen:

- `file-system-id`— Die ID des Amazon EFS-Dateisystems, das von gesichert wird AWS Backup. Zurückgegeben in `GetRecoveryPointRestoreMetadata`. Dies ist nicht erforderlich, wenn ein neues Dateisystem wiederhergestellt wird (dieser Wert wird ignoriert, wenn der Parameter `newFileSystem` den Wert hat`True`).
- `Encrypted` – Ein boolescher Wert, der mit „True“ anzeigt, dass das Dateisystem verschlüsselt ist. Wenn `KmsKeyId` angegeben ist, muss `Encrypted` auf`true` gesetzt sein.
- `KmsKeyId`— Gibt den AWS KMS Schlüssel an, der zum Verschlüsseln des wiederhergestellten Dateisystems verwendet wird.
- `PerformanceMode` – Gibt den Durchsatzmodus für das Dateisystem an.
- `CreationToken` – Ein vom Benutzer bereitgestellter Wert, der die Eindeutigkeit (Idempotenz) der Anfrage sicherstellt.
- `newFileSystem` – Ein boolescher Wert, der, wenn „true“, angibt, dass der Wiederherstellungsort in einem neuen Amazon-EFS-Dateisystem wiederhergestellt wird.
- `ItemsToRestore` – Ein Array von bis zu fünf Zeichenketten, wobei jede Zeichenfolge ein Dateipfad ist. Verwenden Sie `ItemsToRestore`, um bestimmte Dateien oder Verzeichnisse anstelle des gesamten Dateisystems wiederherzustellen. Dieser Parameter ist optional.

Sie können auch `aws:backup:request-id` einschließen.

Eine Zonenwiederherstellung kann mit folgenden Parametern durchgeführt werden:

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Weitere Informationen zu Amazon EFS-Konfigurationswerten finden Sie unter create-file-system.

Deaktivieren automatischer Backups in Amazon EFS

Standardmäßig erstellt Amazon EFS automatisch Daten-Backups. Diese Backups werden in als Wiederherstellungspunkte dargestellt AWS Backup. Versuche, den Wiederherstellungspunkt zu entfernen, führen zu einer Fehlermeldung, die darauf hinweist, dass nicht genügend Rechte vorhanden sind, um die Aktion auszuführen.

Es empfiehlt sich, dieses automatische Backup aktiv zu lassen. Insbesondere bei versehentlichem Löschen von Daten ermöglicht dieses Backup die Wiederherstellung des Dateisysteminhalts bis zum Datum des letzten erstellten Wiederherstellungspunkts.

In dem unwahrscheinlichen Fall, dass Sie diese deaktivieren möchten, muss die Zugriffsrichtlinie von `"Effect": "Deny"` auf `"Effect": "Allow"` geändert werden. Weitere Informationen zum Ein- und Ausschalten von automatischen Backups finden Sie im Amazon-EFS-Benutzerhandbuch.

Wiederherstellen einer Amazon-DynamoDB-Tabelle

Verwenden Sie die AWS Backup Konsole, um DynamoDB-Wiederherstellungspunkte wiederherzustellen

So stellen Sie eine DynamoDB-Tabelle wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die DynamoDB-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.

4. Geben Sie unter Settings (Einstellungen) im Textfeld New table name (Neuer Tabellenname) einen neuen Tabellennamen ein.
5. Wählen Sie unter Wiederherstellungsrolle die IAM-Rolle aus, die für diese Wiederherstellung übernommen AWS Backup werden soll.
6. Für Verschlüsselungseinstellungen:

   a. Wenn Ihr Backup von DynamoDB verwaltet wird (sein ARN beginnt mit`arn:aws:dynamodb`), AWS Backup verschlüsselt es Ihre wiederhergestellte Tabelle mit einem AWS-eigenen Schlüssel.

      Um einen anderen Schlüssel für die Verschlüsselung Ihrer wiederhergestellten Tabelle auszuwählen, können Sie entweder den AWS Backup StartRestoreJobVorgang verwenden oder die Wiederherstellung von der DynamoDB-Konsole aus durchführen.

   b. Wenn Ihr Backup die vollständige AWS Backup Verwaltung unterstützt (sein ARN beginnt mit`arn:aws:backup`), können Sie eine der folgenden Verschlüsselungsoptionen wählen, um Ihre wiederhergestellte Tabelle zu schützen:

      - (Standard) DynamoDB-eigener KMS-Schlüssel (keine zusätzlichen Gebühren für Verschlüsselung)
      - Von DynamoDB verwalteter KMS-Schlüssel (es fallen KMS-Gebühren an)
      - Vom Kunden verwalteter KMS-Schlüssel (es fallen KMS-Gebühren an)

      „DynamoDB-eigene“ und „DynamoDB-verwaltete“ Schlüssel sind dieselben wie „AWS-eigene“ bzw. „AWS-verwaltete“ Schlüssel. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand: Funktionsweise im Entwicklerhandbuch zu Amazon DynamoDB.

      Weitere Informationen zur vollständigen AWS Backup Verwaltung finden Sie unterErweitertes DynamoDB-Backup.

> **Note**
>
> Die folgenden Hinweise gelten nur, wenn Sie ein kopiertes Backup wiederherstellen UND die wiederhergestellte Tabelle mit demselben Schlüssel verschlüsseln möchten, mit dem Sie Ihre ursprüngliche Tabelle verschlüsselt haben.

Wenn Sie ein regionsübergreifendes Backup wiederherstellen und Ihre wiederhergestellte Tabelle mit demselben Schlüssel verschlüsseln möchten, den Sie für die Verschlüsselung Ihrer Originaltabelle verwendet haben, muss es sich bei Ihrem Schlüssel um einen Schlüssel für mehrere Regionen handeln. AWS-eigene und AWS-verwaltete Schlüssel sind keine Schlüssel für mehrere Regionen. Weitere Informationen finden Sie unter Multiregionale Schlüssel im Entwicklerhandbuch für AWS Key Management Service .
Wenn Sie ein kontoübergreifendes Backup wiederherstellen und Ihre wiederhergestellte Tabelle mit demselben Schlüssel verschlüsseln möchten, den Sie für die Verschlüsselung Ihrer ursprünglichen Tabelle verwendet haben, müssen Sie den Schlüssel in Ihrem Quellkonto mit Ihrem Zielkonto teilen. AWS-eigene und AWS-verwaltete Schlüssel können nicht von mehreren Konten gemeinsam genutzt werden. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service - Entwicklerhandbuch.

7. Wählen Sie Restore backup aus.

   Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um DynamoDB-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie `StartRestoreJob`. Sie können bei DynamoDB-Wiederherstellungen die folgenden Metadaten angeben: Bei Metadaten wird die Groß- und Kleinschreibung nicht beachtet.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Das Folgende ist ein Beispiel für das `restoreMetadata`-Argument für einen `StartRestoreJob`-Vorgang in der CLI:

```
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
```

Im vorherigen Beispiel wird die wiederhergestellte Tabelle mit einem AWS Schlüssel verschlüsselt, der dem Benutzer gehört. Der Teil der Wiederherstellungsmetadaten, der die Verschlüsselung mit dem AWS eigenen Schlüssel spezifiziert, ist:. `\"encryptionType\":\"Default \",\"kmsMasterKeyArn\":\"Not Applicable\"`

Um Ihre wiederhergestellte Tabelle mit einem AWS verwalteten Schlüssel zu verschlüsseln, geben Sie die folgenden Wiederherstellungsmetadaten an:. `"encryptionType\":\"KMS\", \"kmsMasterKeyArn\":\"Not Applicable\"`

Um Ihre wiederhergestellte Tabelle mit einem vom Kunden verwalteten Schlüssel zu verschlüsseln, geben Sie die folgenden Wiederherstellungsmetadaten an: `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

Wiederherstellen einer RDS-Datenbank

Zum Wiederherstellen einer Amazon-RDS-Datenbank müssen mehrere Wiederherstellungsoptionen angegeben werden. Weitere Informationen zu diesen Optionen finden Sie unter Backup und Wiederherstellen einer Amazon RDS-DB-Instance im Benutzerhandbuch zu Amazon RDS.

Verwenden Sie die AWS Backup Konsole, um Amazon RDS-Wiederherstellungspunkte wiederherzustellen

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Amazon-RDS-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Übernehmen Sie im Bereich Instance specifications (Instance-Spezifikationen) die Standardeinstellungen oder geben Sie die Optionen für DB engine (DB-Engine), License Model

(Lizenzmodell), DB instance class (DB-Instance-Klasse), Multi AZ (Multi-AZ) und Storage type (Speichertyp) an. Wenn Sie beispielsweise eine Standby-Datenbank-Instance benötigen, geben Sie Multi AZ an.

5. Geben Sie im Bereich Einstellungen einen Namen an, der für alle DB-Instances und Cluster, die Ihnen gehören, AWS-Konto in der aktuellen Region eindeutig ist. Bei der DB-Instance-Kennung wird zwischen Groß- und Kleinschreibung unterschieden, sie wird jedoch komplett in Kleinbuchstaben gespeichert, wie in `mydbinstance`. Dies ist ein Pflichtfeld.
6. Akzeptieren Sie im Bereich Netzwerk und Sicherheit die Standardeinstellungen oder geben Sie die Optionen für die Einstellungen Virtual Private Cloud (VPC), Subnetzgruppe, Öffentliche Barrierefreiheit (normalerweise Ja) und Availability Zone an.
7. Übernehmen Sie im Bereich Database options (Datenbankoptionen) die Standardeinstellungen oder geben Sie die Optionen für Database port (Datenbankport), DB parameter group (DB-Parametergruppe), Option Group (Optionsgruppe), Copy tags to snapshots (Tags in Snapshots kopieren) und IAM DB Authentication Enabled (IAM-DB-Authentifizierung aktiviert) an.
8. Für Verschlüsselung verwenden Sie die Standardeinstellungen. Wenn die Datenbank-Instance für den Snapshot verschlüsselt wurde, wird die wiederhergestellte Datenbank-Instance ebenfalls verschlüsselt. Diese Verschlüsselung kann nicht entfernt werden.
9. Wählen Sie im Bereich Protokollexporte die Protokolltypen aus, die in Amazon CloudWatch Logs veröffentlicht werden sollen. Die IAM-Rolle ist bereits definiert.
10. Übernehmen Sie im Bereich Maintenance (Wartung) die Standardeinstellung oder geben Sie die Option für Auto minor version upgrade (Automatisches Unterversion-Upgrade) an.
11. Wählen Sie im Bereich Rolle wiederherstellen die IAM-Rolle aus, die AWS Backup für diese Wiederherstellung annimmt.
12. Nachdem alle Einstellungen festgelegt sind, wählen Sie Restore backup (Sicherung wiederherstellen) aus.

    Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon RDS-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie `StartRestoreJob`. Informationen zu akzeptierten Metadaten und Werten finden Sie unter `RestoreDBInstanceFromDBSnapshot` in der Amazon-RDS-API-Referenz. AWS Backup

Akzeptiert zusätzlich die folgenden reinen Informationsattribute. Ihre Aufnahme wirkt sich jedoch nicht auf die Wiederherstellung aus:

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Wiederherstellung eines Amazon-Aurora-Clusters

Verwenden Sie die AWS Backup Konsole, um Aurora-Wiederherstellungspunkte wiederherzustellen

AWS Backup stellt Ihren Aurora-Cluster wieder her; es wird keine Amazon RDS-Instance erstellt oder an Ihren Cluster angehängt. In den folgenden Schritten erstellen Sie mithilfe der CLI eine Amazon-RDS-Instance und fügen sie Ihrem wiederhergestellten Aurora-Cluster hinzu.

Zum Wiederherstellen eines Aurora-Clusters müssen Sie mehrere Wiederherstellungsoptionen angeben. Weitere Informationen zu diesen Optionen finden Sie unter Übersicht über Backup und Wiederherstellung eines Aurora-DB-Clusters im Amazon-Aurora-Benutzerhandbuch. Spezifikationen für die Wiederherstellungsoptionen finden Sie im API-Leitfaden für `RestoreDBClusterFromSnapshot`.

So stellen Sie ein Amazon-Aurora-Cluster wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Aurora-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Übernehmen Sie im Bereich Instance specifications (Instance-Spezifikationen die Standardeinstellungen oder geben Sie die Optionen für DB engine (DB-Engine), DB engine version (DB-Engine-Version) und Capacity type (Kapazitätstyp) an.

> **Note**
>
> Wenn der Kapazitätstyp Serverless (Serverlos) ausgewählt ist, wird ein Bereich Capacity settings (Kapazitätseinstellungen) angezeigt. Geben Sie die Optionen für Minimum Aurora capacity unit (Minimale Aurora Capacity Unit) und Maximum Aurora capacity unit (Maximale Aurora Capacity Unit) an oder wählen Sie andere Optionen im Abschnitt Additional scaling configuration (Zusätzliche Skalierungskonfiguration) aus.

5. Geben Sie im Bereich Einstellungen einen Namen an, der für alle DB-Cluster-Instances, die Ihnen gehören, AWS-Konto in der aktuellen Region eindeutig ist.
6. Übernehmen Sie im Bereich Netzwerk und Sicherheit die Standardeinstellungen oder geben Sie die Optionen für Virtual Private Cloud (VPC), Subnetzgruppe und Availability Zone an.
7. Übernehmen Sie im Bereich Database options (Datenbankoptionen) die Standardeinstellungen oder geben Sie die Optionen für Database port (Datenbankport), DB cluster parameter group (DB-Cluster-Parametergruppe) und IAM DB Authentication Enabled (IAM-DB-Authentifizierung aktiviert) an.
8. Übernehmen Sie im Bereich Backup (Sicherung) die Standardeinstellung oder geben Sie die Option für die Einstellung Copy tags to snapshots (Tags in Snapshots kopieren) an.
9. Übernehmen Sie im Bereich Backtrack (Rückverfolgung) die Standardeinstellung oder geben Sie die Optionen für Enable Backtrack (Rückspur aktivieren) oder Disable Backtrack (Rückspur deaktivieren) an.
10. Übernehmen Sie im Bereich Verschlüsselung die Standardeinstellung oder geben Sie die Optionen für Verschlüsselung aktivieren oder Verschlüsselung deaktivieren an.
11. Wählen Sie im Bereich Protokollexporte die Protokolltypen aus, die in Amazon CloudWatch Logs veröffentlicht werden sollen. Die IAM-Rolle ist bereits definiert.
12. Wählen Sie im Bereich Rolle wiederherstellen die IAM-Rolle aus, die AWS Backup für diese Wiederherstellung annimmt.
13. Nachdem Sie alle Einstellungen angegeben haben, wählen Sie Backup wiederherstellen aus.

    Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.
14. Nachdem Ihre Wiederherstellung abgeschlossen ist, hängen Sie Ihr wiederhergestelltes Aurora-Cluster an eine Amazon-RDS-Instance an.

    Verwenden der AWS CLI:

- Für Linux, macOS oder Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance \
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

- Für Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

Informationen zu kontinuierlichen Backups und zur point-in-time Wiederherstellung zu einem bestimmten Zeitpunkt finden Sie unter Kontinuierliche Backups und Wiederherstellung (PITR).

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Aurora-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie `StartRestoreJob`. Sie können bei Aurora-Wiederherstellungen die folgenden Metadaten angeben:

```
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;
```

Beispiel:

```
"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\":\"[]\"}"
```

Wiederherstellen einer Amazon-EC2-Instance

Wenn Sie eine EC2-Instance wiederherstellen, AWS Backup erstellt ein Amazon Machine Image (AMI), eine Instance, das Amazon EBS-Root-Volume, Amazon EBS-Datenvolumes (falls die geschützte Ressource Datenvolumen hatte) und Amazon EBS-Snapshots. Sie können einige Instance-Einstellungen mit der AWS Backup Konsole oder eine größere Anzahl von Einstellungen mit dem oder einem SDK anpassen. AWS CLI AWS

Die folgenden Überlegungen gelten für die Wiederherstellung von EC2-Instances:

- AWS Backup konfiguriert die wiederhergestellte Instanz so, dass sie dasselbe key pair verwendet, das die geschützte Ressource ursprünglich verwendet hat. Sie können während des Wiederherstellungsvorgangs kein anderes key pair für die wiederhergestellte Instanz angeben.
- AWS Backup sichert und stellt keine Benutzerdaten wieder her, die beim Starten einer Amazon EC2 EC2-Instance verwendet werden.
- Bei der Konfiguration der wiederhergestellten Instance können Sie wählen, ob Sie dasselbe Instance-Profil wie die ursprünglich verwendete geschützte Ressource verwenden oder ohne Instance-Profil starten möchten. Dadurch soll die Möglichkeit einer Eskalation von Rechten verhindert werden. Sie können das Instance-Profil für die wiederhergestellte Instance mithilfe der Amazon EC2 EC2-Konsole aktualisieren.

  Wenn Sie das ursprüngliche Instanzprofil verwenden, müssen Sie AWS Backup die folgenden Berechtigungen gewähren, wobei der Ressourcen-ARN der ARN der IAM-Rolle ist, die dem Instanzprofil zugeordnet ist.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
```

```
        "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

- Während einer Wiederherstellung gelten alle Amazon-EC2-Kontingente und Konfigurationseinschränkungen.
- Falls der Tresor mit Ihren Amazon EC2 EC2-Wiederherstellungspunkten über eine Tresorsperre verfügt, finden Sie Zusätzliche Sicherheitsüberlegungen weitere Informationen unter.

Verwenden Sie die AWS Backup Konsole, um Amazon EC2 EC2-Wiederherstellungspunkte wiederherzustellen

Sie können eine gesamte Amazon EC2 EC2-Instance von einem einzigen Wiederherstellungspunkt aus wiederherstellen, einschließlich des Root-Volumes, der Datenvolumes und einiger Instance-Konfigurationseinstellungen wie Instance-Typ und key pair.

So stellen Sie Amazon EC2 EC2-Ressourcen mithilfe der AWS Backup Konsole wieder her

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die ID der Amazon EC2 EC2-Ressource aus, um die Seite mit den Ressourcendetails zu öffnen.
3. Wählen Sie im Bereich Wiederherstellungspunkte das Optionsfeld neben der ID des wiederherzustellenden Wiederherstellungspunkts aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Im Bereich Netzwerkeinstellungen verwenden wir die Einstellungen der geschützten Instance, um die Standardwerte für den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die Instance-IAM-Rolle auszuwählen. Sie können diese Standardwerte verwenden oder sie nach Bedarf ändern.
5. Verwenden Sie im Bereich Rolle wiederherstellen die Standardrolle oder wählen Sie eine IAM-Rolle aus, um eine IAM-Rolle anzugeben, die die AWS Backup Berechtigung zum Wiederherstellen des Backups erteilt.
6. Im Bereich Geschützte Ressourcen-Tags wählen wir standardmäßig Tags von der geschützten Ressource in die wiederhergestellte Ressource kopieren aus. Wenn Sie diese Tags nicht kopieren möchten, deaktivieren Sie das Kontrollkästchen.
7. Akzeptieren Sie im Bereich Erweiterte Einstellungen die Standardwerte für die Instanzeinstellungen, oder ändern Sie sie nach Bedarf. Informationen zu diesen Einstellungen

erhalten Sie, wenn Sie für die Einstellung die Option Info auswählen, um den zugehörigen Hilfebereich zu öffnen.

8. Wenn Sie mit der Konfiguration der Instanz fertig sind, wählen Sie Backup wiederherstellen.

Stellen Sie Amazon EC2 wieder her mit AWS CLI

`start-restore-job`Ermöglicht in der Befehlszeilenschnittstelle die Wiederherstellung mit bis zu 32 Parametern (einschließlich einiger Parameter, die nicht über die AWS Backup Konsole anpassbar sind).

Die folgende Liste führt die akzeptierten Metadaten auf, die Sie zur Wiederherstellung eines Amazon-EC2-Wiederherstellungspunkts übergeben können.

```
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 akzeptiert die folgenden reinen Informationsattribute. Ihre Aufnahme wirkt sich jedoch nicht auf die Wiederherstellung aus:

```
vpcId
```

Sie können eine Amazon-EC2-Instance auch wiederherstellen, ohne gespeicherte Parameter einzubeziehen. Diese Option ist auf der Registerkarte Protected resource (Geschützte Ressource) in der AWS Backup -Konsole verfügbar.

Wiederherstellen eines Storage-Gateway-Volumes

Wenn Sie einen AWS Storage Gateway Volume-Snapshot wiederherstellen, können Sie wählen, ob Sie den Snapshot als Storage Gateway Gateway-Volume oder als Amazon EBS-Volume wiederherstellen möchten. Dies liegt daran, dass beide Services AWS Backup integriert sind und jeder Storage Gateway Gateway-Snapshot entweder auf einem Storage Gateway Gateway-Volume oder einem Amazon EBS-Volume wiederhergestellt werden kann.

Storage Gateway über die AWS Backup Konsole wiederherstellen

So stellen Sie Storage-Gateway-Volume wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Storage-Gateway-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Geben Sie die Wiederherstellungsparameter für Ihre Ressource an. Die von Ihnen eingegebenen Wiederherstellungsparameter beziehen sich auf den ausgewählten Ressourcentyp.

   Wählen Sie unter Ressourcentyp die AWS Ressource aus, die bei der Wiederherstellung dieses Backups erstellt werden soll.
5. Wenn Sie sich für ein Speicher-Gateway-Volume entscheiden, wählen Sie ein Gateway in einem erreichbaren Status. Wählen Sie auch Ihren iSCSI-Zielnamen.

   1. Wählen Sie für Volume-Stored-Gateways eine Festplatten-ID aus.

2. Wählen Sie für Volume-Cached-Gateways eine Kapazität, die mindestens so groß ist wie Ihre geschützte Ressource.

   Wenn Sie EBS volume (EBS-Volume) auswählen, geben Sie die Werte für Volume type (Volume-Typ) und Size (Größe) (GiB) an und wählen Sie eine Availability Zone aus.

6. Wählen Sie unter Wiederherstellungsrolle die IAM-Rolle aus, die für diese Wiederherstellung verwendet AWS Backup werden soll.

   > **Note**
   >
   > Wenn die AWS Backup Standardrolle in Ihrem Konto nicht vorhanden ist, wird eine Standardrolle mit den richtigen Berechtigungen für Sie erstellt. Sie können diese Standardrolle löschen oder unbrauchbar machen.

7. Wählen Sie Restore backup aus.

   Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Storage Gateway wiederherstellen mit AWS CLI

In der Befehlszeilenschnittstelle ermöglicht `start-restore-job`, ein Storage-Gateway-Volume wiederherzustellen.

Die folgende Liste enthält die akzeptierten Metadaten.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and AWS-Region.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Wiederherstellen einer Amazon-Timestream-Tabelle

Wenn Sie eine Amazon-Timestream-Tabelle wiederherstellen, müssen Sie mehrere Optionen konfigurieren, darunter den neuen Tabellennamen, die Zieldatenbank, Ihre

Speicherzuweisungseinstellungen (Arbeitsspeicher und Magnetspeicher) und die Rolle, die Sie zum Abschließen des Wiederherstellungsauftrags verwenden werden. Sie können auch einen Amazon-S3-Bucket auswählen, in dem Sie Fehlerprotokolle speichern möchten. Schreibvorgänge auf Magnetspeichern erfolgen asynchron, sodass Sie die Fehler möglicherweise protokollieren möchten.

Der Timestream-Datenspeicher besteht aus zwei Ebenen: einem Arbeitsspeicher und einem Magnetspeicher. Ein Arbeitsspeicher ist erforderlich, aber Sie haben die Möglichkeit, Ihre wiederhergestellte Tabelle nach Ablauf der angegebenen Speicherzeit in den Magnetspeicher zu übertragen. Der Speicherspeicher ist für Datenschreibvorgänge mit hohem Durchsatz und schnelle point-in-time Abfragen optimiert. Der Magnetspeicher ist für einen geringeren Durchsatz beim Schreiben spät eingehender Daten, für die Langzeitspeicherung von Daten und für schnelle analytische Abfragen optimiert.

Wenn Sie eine Timestream-Tabelle wiederherstellen, legen Sie fest, wie lange die Tabelle auf jeder Speicherebene verbleiben soll. Mithilfe der Konsole oder der API können Sie die Speicherzeit für beide festlegen. Beachten Sie, dass der Speicher linear und sequentiell ist. Timestream speichert Ihre wiederhergestellte Tabelle zuerst im Arbeitsspeicher und überträgt sie dann automatisch in den Magnetspeicher, wenn die Speicherzeit erreicht ist.

> **Note**
>
> Der Aufbewahrungszeitraum des Magnetspeichers muss mindestens dem ursprünglichen Aufbewahrungszeitraum entsprechen (wird oben rechts in der Konsole angezeigt). Andernfalls gehen Daten verloren.

Beispiel: Sie legen die Speicherzuweisung so fest, dass sie Daten für eine Woche und die Magnetspeicherzuweisung so konfiguriert, dass dieselben Daten ein Jahr lang gespeichert werden. Wenn die Daten im Speicher eine Woche alt werden, werden sie automatisch in den Magnetspeicher verschoben. Sie werden dann für ein Jahr im Magnetspeicher aufbewahrt. Nach Ablauf dieser Zeit wird es aus Timestream und von AWS Backup gelöscht.

So stellen Sie eine Amazon Timestream Timestream-Tabelle mithilfe der AWS Backup Konsole wieder her

Sie können Timestream-Tabellen in der AWS Backup Konsole wiederherstellen, die von erstellt wurden. AWS Backup

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.

2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Amazon-Timestream-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Geben Sie Ihre neuen Tabellenkonfigurationseinstellungen an, einschließlich:

   a. Neuer Tabellenname, bestehend aus 2 bis 256 Zeichen (Buchstaben, Zahlen, Bindestriche, Punkte und Unterstriche).

   b. Zieldatenbank, ausgewählt aus dem Dropdown-Menü.
5. Speicherzuweisung: Legen Sie fest, wie lange sich die wiederhergestellte Tabelle zunächst im Arbeitsspeicher befindet, und legen Sie fest, wie lange sich die wiederhergestellte Tabelle dann im Magnetspeicher befindet. Der Arbeitsspeicher kann auf Stunden, Tage, Wochen oder Monate festgelegt werden. Der Magnetspeicher kann auf Tage, Wochen, Monate oder Jahre eingestellt werden.
6. (Optional) Schreibvorgänge auf Magnetspeicher aktivieren: Sie haben die Möglichkeit, Schreibvorgänge auf Magnetspeicher zuzulassen. Wenn diese Option aktiviert ist, werden spät eintreffende Daten, d. h. Daten mit einem Zeitstempel, der außerhalb der Aufbewahrungszeit des Speichers liegt, direkt in den Magnetspeicher geschrieben.
7. (Optional) Speicherort der Amazon-S3-Fehlerprotokolle: Sie können einen S3-Speicherort angeben, an dem Ihre Fehlerprotokolle gespeichert werden. Durchsuchen Sie Ihre S3-Dateien oder kopieren Sie den S3-Dateipfad und fügen Sie ihn ein.

   > **Note**
   >
   > Wenn Sie sich dafür entscheiden, einen Speicherort für das S3-Fehlerprotokoll anzugeben, muss die Rolle, die Sie für diese Wiederherstellung verwenden, über die Berechtigung verfügen, in einen S3-Bucket zu schreiben, oder sie muss eine Richtlinie mit dieser Berechtigung enthalten.
8. Wählen Sie die IAM-Rolle aus, die für die Durchführung von Wiederherstellungen übergeben werden soll. Sie können die Standard-IAM-Rolle verwenden oder eine andere angeben.
9. Klicken Sie auf Backup wiederherstellen.

Ihre Wiederherstellungsaufträge werden unter „Geschützte Ressourcen“ angezeigt. Sie können den aktuellen Status Ihres Wiederherstellungsauftrags einsehen, indem Sie auf die Schaltfläche „Aktualisieren“ oder auf STRG-R klicken.

So stellen Sie eine Amazon-Timestream-Tabelle mithilfe von API, CLI oder SDK wieder her:

Verwenden Sie `StartRestoreJob`, um eine Timestream-Tabelle über die API wiederherzustellen.

Um einen Timestream mithilfe von wiederherzustellen AWS CLI, verwenden Sie den Vorgang `start-restore-job.` und geben Sie die folgenden Metadaten an:

```
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
```

Hier ist ein Beispiel für eine Vorlage:

```
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
```

Sie können `DescribeRestoreJob` auch als Unterstützung bei der Bereitstellung von Informationen zur Wiederherstellung verwenden.

Verwenden Sie in der AWS CLI den Vorgang `describe-restore-job` und verwenden Sie die folgenden Metadaten:

```
TableName: string;
```

```
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

Hier ist ein Beispiel für eine Vorlage:

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Wiederherstellen eines Amazon-Redshift-Clusters

Sie können automatische und manuelle Snapshots in der AWS Backup Konsole oder über die CLI wiederherstellen.

Wenn Sie ein Amazon-Redshift-Cluster wiederherstellen, werden die ursprünglichen Cluster-Einstellungen standardmäßig in die Konsole eingegeben. Sie können verschiedene Einstellungen für die folgenden Konfigurationen angeben. Beim Wiederherstellen einer Tabelle müssen Sie die Quell- und die Zieldatenbanken angeben. Weitere Informationen zu diesen Konfigurationen finden Sie unter Wiederherstellen eines Clusters aus einem Snapshot im Verwaltungshandbuch zu Amazon Redshift.

- Einzelne Tabelle oder Cluster: Sie können wählen, ob Sie einen gesamten Cluster oder eine einzelne Tabelle wiederherstellen möchten. Wenn Sie eine einzelne Tabelle wiederherstellen möchten, werden die Quelldatenbank, das Quellschema und der Name der Quelltabelle sowie der Zielcluster, das Schema und der neue Tabellenname benötigt.
- Knotentyp: Jedes Amazon-Redshift-Cluster besteht aus einem Leader-Knoten und mindestens einem Rechenknoten. Wenn Sie ein Cluster wiederherstellen, müssen Sie den Knotentyp angeben, der Ihren Anforderungen an CPU, RAM, Speicherkapazität und Laufwerkstyp entspricht.
- Anzahl der Knoten: Wenn Sie ein Cluster wiederherstellen, müssen Sie die Anzahl der benötigten Knoten angeben.
- Zusammenfassung der Konfiguration
- Cluster-Berechtigungen

So stellen Sie einen Amazon Redshift Redshift-Cluster oder eine Tabelle mithilfe der AWS Backup Konsole wieder her

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Eigenschaften und die Amazon-Redshift-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Wiederherstellungspunkte das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Wiederherstellungsoptionen
   a. Stellen Sie ein Cluster aus einem Snapshot wieder her oder
   b. stellen Sie eine einzelne Tabelle innerhalb eines Snapshots auf einem neuen Cluster wieder her. Wenn Sie diese Optionen wählen, müssen Sie Folgendes konfigurieren:
      i. Aktivieren oder deaktivieren Sie Namen, bei denen Groß- und Kleinschreibung beachtet wird.
      ii. Geben Sie die Werte der Quelltabelle ein, einschließlich der Datenbank, des Schemas und der Tabelle. Die Quelltabelleninformationen finden Sie in der Amazon-Redshift-Konsole.
      iii. Geben Sie die Werte der Zieltabelle ein, einschließlich der Datenbank, des Schemas und der neuen Tabelle.
5. Geben Sie Ihre neuen Cluster-Konfigurationseinstellungen an.
   a. Für die Cluster-Wiederherstellung: Wählen Sie Cluster-ID, Knotentyp und Anzahl der Knoten.
   b. Geben Sie die Availability Zone und die Wartungsfenster an.
   c. Sie können weitere Rollen zuordnen, indem Sie auf IAM-Rollen zuordnen klicken.
6. Optional: Zusätzliche Konfigurationen:
   a. Standardwerte verwenden ist standardmäßig aktiviert.
   b. Verwenden Sie die Dropdown-Menüs, um Einstellungen für Netzwerk und Sicherheit, VPC-Sicherheitsgruppen, Cluster-Subnetzgruppe und Availability Zone auszuwählen.

c. Schalten Sie Erweitertes VPC-Routing ein oder aus.

d. Stellen Sie fest, ob Sie Ihren Cluster-Endpunkt öffentlich zugänglich machen möchten. Ist dies der Fall, können Instances und Geräte außerhalb der VPC über den Cluster-Endpunkt eine Verbindung zu Ihrer Datenbank herstellen. Wenn diese Option aktiviert ist, geben Sie die elastische IP-Adresse ein.

7. Optional: Datenbankkonfiguration. Sie können Folgendes eingeben:

   a. Datenbankport (durch Eingabe in das Textfeld)

   b. Parametergruppen

8. Wartung: Sie können den

   a. Wartungsfenster

   b. Wartungstermin wählen: „Aktuell“, „Nachstehend“ oder „Vorschau“. So wird gesteuert, welche Clusterversion in einem Wartungszeitraum installiert wird.

9. Der automatische Snapshot ist auf die Standardeinstellung eingestellt.

   a. Automatisierter Snapshot-Aufbewahrungszeitraum. Die Aufbewahrungsfrist muss 0 bis 35 Tage betragen. Wählen Sie 0, um keine automatisierten Snapshots zu erstellen.

   b. Die Aufbewahrungsfrist für manuelle Snapshots beträgt 1 bis 3.653 Tage.

   c. Es gibt ein optionales Kontrollkästchen für die Cluster-Verschiebung. Wenn diese Option aktiviert ist, können Sie Ihr Cluster in eine andere Availability Zone verlagern. Nachdem Sie die Verlagerung aktiviert haben, können Sie den VPC-Endpunkt verwenden.

10. Überwachung: Nach der Wiederherstellung eines Clusters können Sie die Überwachung über CloudWatch oder Amazon Redshift einrichten.

11. Wählen Sie die IAM-Rolle aus, die für die Durchführung von Wiederherstellungen übergeben werden soll. Sie können die Standardrolle verwenden oder eine andere angeben.

Ihre Wiederherstellungsaufträge werden unter Aufträge angezeigt. Sie können den aktuellen Status Ihres Wiederherstellungsauftrags einsehen, indem Sie auf die Schaltfläche „Aktualisieren“ oder auf STRG-R klicken.

Wiederherstellen eines Amazon-Redshift-Clusters mithilfe von API, CLI oder SDK

Verwenden Sie `StartRestoreJob`, um einen Amazon-Redshift-Cluster wiederherzustellen.

Um Amazon Redshift mithilfe von wiederherzustellen AWS CLI, verwenden Sie den Befehl `start-restore-job` und geben Sie die folgenden Metadaten an:

```
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
```

Weitere Informationen finden Sie unter `RestoreFromClusterSnapshot` in der API-Referenz von Amazon Redshift und unter `restore-from-cluster-snapshot` im AWS CLI -Leitfaden.

Hier ist ein Beispiel für eine Vorlage:

```
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-Region
-\-endpoint-url URL
```

Ein Beispiel:

```
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 \
```

Sie können `DescribeRestoreJob` auch als Unterstützung bei der Bereitstellung von Informationen zur Wiederherstellung verwenden.

Verwenden Sie in der AWS CLI den Vorgang `describe-restore-job` und verwenden Sie die folgenden Metadaten:

```
Region
```

Hier ist ein Beispiel für eine Vorlage:

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region AWS-Region
```

Ein Beispiel:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Wiederherstellen von SAP-HANA-Datenbanken auf Amazon-EC2-Instances

SAP HANA-Datenbanken auf EC2-Instances können mithilfe der AWS Backup Konsole, mithilfe der API oder mithilfe AWS CLI von wiederhergestellt werden.

Themen

Stellen Sie mithilfe der Konsole eine SAP HANA on Amazon EC2 EC2-Instance-Datenbank wieder her AWS Backup

Beachten Sie, dass Backup- und Wiederherstellungsaufträge, die dieselbe Datenbank betreffen, nicht gleichzeitig ausgeführt werden können. Wenn ein Auftrag zur Wiederherstellung einer SAP-HANA-Datenbank ausgeführt wird, führen Versuche, dieselbe Datenbank zu sichern, wahrscheinlich zu einem Fehler: „Die Datenbank kann nicht gesichert werden, solange sie angehalten ist.“

1. Greifen Sie mit den Anmeldeinformationen aus den Voraussetzungen auf die AWS Backup Konsole zu.
2. Wählen Sie im Dropdown-Menü Ziel-Wiederherstellungsort eine Datenbank aus, die mit dem für die Wiederherstellung verwendeten Wiederherstellungspunkt überschrieben werden soll (beachten Sie, dass die Instance, die die Wiederherstellungszieldatenbank hostet, auch über die Berechtigungen aus den Voraussetzungen verfügen muss).

   > **Important**
   >
   > SAP-HANA-Datenbankwiederherstellungen sind destruktiv. Beim Wiederherstellen einer Datenbank wird die Datenbank am angegebenen Zielspeicherort für die Wiederherstellung überschrieben.

3. Führen Sie diesen Schritt nur aus, wenn Sie eine Systemkopie wiederherstellen. Fahren Sie andernfalls mit Schritt 4 fort.

Bei einer Systemkopie werden Aufträge auf eine Zieldatenbank wiederhergestellt, die sich von der Quelldatenbank unterscheidet, aus der der Wiederherstellungspunkt erstellt wurde. Beachten Sie bei der Wiederherstellung von Systemkopien den `aws ssm-sap put-resource-permission`-Befehl, der Ihnen auf der Konsole angezeigt wird. Dieser Befehl muss auf dem Computer, der die Voraussetzungen erfüllt hat, kopiert, eingefügt und ausgeführt werden. Verwenden Sie bei der Ausführung des Befehls die Anmeldeinformationen der Rolle in der Voraussetzung, in der Sie die erforderlichen Berechtigungen für die Registrierung von Anwendungen einrichten.

```
// 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. Sobald Sie den Speicherort für die Wiederherstellung ausgewählt haben, können Sie die Ressourcen-ID, den Anwendungsnamen, den Datenbanktyp und die EC2-Instance der Zieldatenbank sehen.
5. Optional können Sie die erweiterten Wiederherstellungseinstellungen öffnen, um Ihre Option für die Katalogwiederherstellung zu ändern. Die Standardauswahl besteht darin, den neuesten Katalog von AWS Backup wiederherzustellen.
6. Klicken Sie auf Backup wiederherstellen.
7. Der Zielort wird bei der Wiederherstellung überschrieben („Destruktive Wiederherstellung“). Sie müssen daher im nächsten Popup-Dialogfeld bestätigen, dass Sie dies zulassen.

   a. Um fortzufahren, müssen Sie sich darüber im Klaren sein, dass die bestehende Datenbank durch die Datenbank, die Sie wiederherstellen, überschrieben wird.

   b. Sobald Sie dies verstanden haben, müssen Sie bestätigen, dass die vorhandenen Daten überschrieben werden. Um dies zu bestätigen und fortzufahren, geben Sie überschreiben in das Texteingabefeld ein.
8. Klicken Sie auf Backup wiederherstellen.

Wenn der Vorgang erfolgreich war, erscheint oben in der Konsole ein blaues Banner. Dies bedeutet, dass der Wiederherstellungsauftrag gerade ausgeführt wird. Sie werden automatisch auf die Seite Aufträge weitergeleitet, auf der Ihr Wiederherstellungsauftrag in der Liste der

Wiederherstellungsaufträge erscheint. Dieser neueste Auftrag hat den Status `Pending`. Sie können nach der Wiederherstellungsauftrags-ID suchen und dann darauf klicken, um Details zu den einzelnen Wiederherstellungsaufträgen zu sehen. Sie können die Liste der Wiederherstellungsaufträge aktualisieren, indem Sie auf die Schaltfläche „Aktualisieren“ klicken, um die Änderungen am Status des Wiederherstellungsauftrags anzuzeigen.

StartRestoreJob API für SAP HANA auf EC2

Diese Aktion stellt die gespeicherte Ressource wieder her, die durch einen Amazon-Ressourcennamen (ARN) identifiziert wird.

Anforderungssyntax

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI-Anforderungsparameter: Die Anforderung verwendet keine URI-Parameter.

Anforderungstext: Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

IdempotencyTokenEine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen unterscheiden können. `StartRestoreJob` Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Metadaten

Eine Satz von Metadaten-Schlüssel-Wert-Paaren. Enthält Informationen, wie z. B. einen Ressourcennamen, die für die Wiederherstellung eines Wiederherstellungspunkts erforderlich sind.

Sie können Konfigurationsmetadaten zu einer Ressource zum Zeitpunkt des Backups abrufen, indem Sie `GetRecoveryPointRestoreMetadata` aufrufen. Für die Wiederherstellung einer Ressource sind jedoch möglicherweise zusätzlich zu den von `GetRecoveryPointRestoreMetadata` bereitgestellten Werten weitere Werte erforderlich. Sie müssen beispielsweise möglicherweise einen neuen Ressourcennamen angeben, wenn das Original bereits vorhanden ist.

Sie müssen spezifische Metadaten angeben, um eine SAP HANA auf Amazon-EC2-Instance wiederherzustellen. Informationen zu SAP HANA-spezifischen Elementen finden Sie in den StartRestoreJob Metadaten.

Um die relevanten Metadaten abzurufen, können Sie den Aufruf `GetRecoveryPointRestoreMetadata` verwenden.

Beispiel für einen standardmäßigen SAP-HANA-Datenbank-Wiederherstellungspunkt:

```
"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"
    }
```

Beispiel für einen kontinuierlichen SAP-HANA-Datenbank-Wiederherstellungspunkt:

```
"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"
    }
```

CLI für SAP HANA auf EC2

Der Befehl `start-restore-job` stellt die gespeicherte Ressource wieder her, die durch einen Amazon-Ressourcennamen (ARN) identifiziert wird. CLI folgt der obigen API-Richtlinie.

Syntax:

```
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]
```

Optionen

`--recovery-point-arn` (Zeichenfolge) ist eine Zeichenfolge in Form einer Amazon-Ressourcennummer (ARN), die einen Wiederherstellungspunkt eindeutig identifiziert; zum Beispiel `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata` (Zuweisung): Eine Satz von Metadaten-Schlüssel-Wert-Paaren. Enthält Informationen, wie z. B. einen Ressourcennamen, die für die Wiederherstellung eines Wiederherstellungspunkts erforderlich sind. Sie können Konfigurationsmetadaten zu einer Ressource zum Zeitpunkt des Backups abrufen, indem Sie `GetRecoveryPointRestoreMetadata` aufrufen. Für die Wiederherstellung einer Ressource sind jedoch möglicherweise zusätzlich zu den von `GetRecoveryPointRestoreMetadata` bereitgestellten Werten weitere Werte erforderlich. Sie müssen spezifische Metadaten angeben, um eine SAP HANA auf Amazon-EC2-Instance wiederherzustellen:

- `aws:backup:request-id`: Dies ist eine beliebige UUID-Zeichenfolge, die für Idempotenz verwendet wird. Ihr Wiederherstellungserlebnis wird dadurch in keiner Weise beeinträchtigt.
- `aws:backup:TargetDatabaseArn`: Geben Sie die Datenbank an, in der Sie wiederherstellen möchten. Dies ist der ARN für eine SAP-HANA-auf-Amazon-EC2-Datenbank.
- `CatalogRestoreOption`: Geben Sie an, von wo aus Ihr Katalog wiederhergestellt werden soll. Entweder `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, oder `CATALOG_FROM_LOCAL_PATH`
- `LocalCatalogPath`: Wenn der CatalogRestoreOption Metadatenwert lautet`CATALOG_FROM_LOCAL_PATH`, geben Sie den Pfad zum lokalen Katalog auf Ihrer EC2-Instance an. Dies sollte ein gültiger Dateipfad in Ihrer EC2-Instance sein.
- `RecoveryType`: Derzeit werden die Wiederherstellungstypen `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY`, und `MOST_RECENT_TIME_RECOVERY` unterstützt.

Schlüssel = (Zeichenfolge); Wert = (Zeichenfolge). Syntax-Kurznotation:

```
KeyName1=string,KeyName2=string
```

JSON-Syntax:

```
{"string": "string"
  ...}
```

`--idempotency-token` ist eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `StartRestoreJob` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

`--resource-type` ist eine Zeichenfolge, die einen Auftrag zur Wiederherstellung eines Wiederherstellungspunkts für eine der folgenden Ressourcen startet: `SAP HANA on Amazon EC2` für SAP HANA auf Amazon EC2. Optional können SAP-HANA-Ressourcen mit dem folgenden Befehl markiert werden: `aws ssm-sap tag-resource`.

Output: `RestoreJobId` ist eine Zeichenfolge, die den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig identifiziert.

Fehlerbehebung

Wenn beim Versuch eines Backup-Vorgangs einer der folgenden Fehler auftritt, finden Sie weitere Informationen zur entsprechenden Lösung.

- Fehler: Kontinuierlicher Backup-Protokollfehler

  Um die Wiederherstellungspunkte für kontinuierliche Backups aufrechtzuerhalten, werden von SAP HANA Protokolle für alle Änderungen erstellt. Wenn die Protokolle nicht verfügbar sind, lautet der Status jedes dieser kontinuierlichen Wiederherstellungspunkte `STOPPED`. Der letzte sichere wiederherstellbare Punkt, der für die Wiederherstellung verwendet werden kann, hat den Status `AVAILABLE`. Wenn die Protokolldaten für die Zeit zwischen Wiederherstellungspunkten mit einem `STOPPED`-Status und Punkten mit dem Status `AVAILABLE` fehlen, kann für diese Zeiten nicht garantiert werden, dass die Wiederherstellung erfolgreich ist. Wenn Sie ein Datum und eine Uhrzeit innerhalb dieses Bereichs eingeben, AWS Backup wird versucht, das Backup zu erstellen, wobei jedoch die nächstgelegene verfügbare wiederherstellbare Uhrzeit verwendet wird. Dieser Fehler wird in der Meldung angezeigt: `“Encountered an issue with log backups. Please check SAP HANA for details."`.

  Lösung: In der Konsole wird der letzte wiederherstellbare Zeitpunkt, der auf den Protokollen basiert, angezeigt. Sie können eine Uhrzeit eingeben, die jünger als die angezeigte ist. Wenn die Daten für diesen Zeitpunkt jedoch nicht in den Protokollen verfügbar sind, AWS Backup wird die letzte wiederherstellbare Uhrzeit verwendet.
- Fehler: `Internal error`

Lösung: Erstellen Sie von Ihrer Konsole aus eine Support-Anfrage oder kontaktieren Sie uns AWS Support mit den Einzelheiten Ihrer Wiederherstellung, z. B. der ID des Wiederherstellungsauftrags.

- Fehler: `The provided role arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Lösung: Stellen Sie sicher, dass die Rolle, die Sie beim Aufrufen der Wiederherstellung übernommen haben, über die erforderlichen Berechtigungen verfügt, um serviceverknüpfte Rollen zu erstellen.

- Fehler: `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:...`

  Lösung: Stellen Sie sicher, dass die Rolle, die beim Aufrufen der in den Voraussetzungen aufgeführten Wiederherstellungsberechtigungen übernommen wurde, korrekt eingegeben wurde.

- Fehler: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  Lösung: Stellen Sie sicher, dass der Backint-Agent ordnungsgemäß installiert wurde. Überprüfen Sie alle Voraussetzungen, insbesondere die Installation von AWS BackInt Agent und AWS Systems Manager für SAP auf Ihrem SAP-Anwendungsserver, und versuchen Sie dann erneut, den BackInt Agenten zu installieren.

- Fehler: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Lösung: Der Wiederherstellungsauftrag wurde durch den Service-Workflow abgebrochen. Wiederholen Sie den Wiederherstellungsauftrag.

- Fehler: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  Lösung: Auf der Instanz kommt es zu vorübergehender Netzwerkinstabilität. Wiederholen Sie den Wiederherstellungsauftrag. Wenn dieses Problem immer wieder auftritt, versuchen Sie, `ForceRetry: "true"` zur Agenten-Konfigurationsdatei hinzuzufügen unter `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`..

Weitere Probleme mit AWS Backint Agent finden Sie unter Troubleshooting AWS Backint Agent for SAP HANA.

Wiederherstellen eines DocumentDB-Clusters

Verwenden Sie die AWS Backup Konsole, um Amazon DocumentDB DocumentDB-Wiederherstellungspunkte wiederherzustellen

Zum Wiederherstellen eines Amazon-DocumentDB-Clusters müssen Sie mehrere Wiederherstellungsoptionen angeben. Informationen zu diesen Optionen finden Sie im Abschnitt zum Wiederherstellen aus einem Cluster-Snapshot im Entwicklerhandbuch zu Amazon DocumentDB.

So stellen Sie ein Amazon-DocumentDB-Cluster wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Amazon-DocumentDB-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Akzeptieren Sie im Konfigurationsbereich die Standardeinstellungen oder geben Sie die Optionen für die Cluster-ID, die Engine-Version, die Instance-Klasse und die Anzahl der Instances an.

   - HINWEIS: Wenn die Standard-VPC bei der Wiederherstellung nicht vorhanden ist, müssen Sie ein Subnetz in einer anderen VPC angeben.
5. Im Bereich Netzwerk und Sicherheit wird „Keine Einstellungen“ angezeigt.
6. Akzeptieren Sie im ncryption-at-restE-Bereich die Standardeinstellung, oder geben Sie die Optionen für die Einstellungen Verschlüsselung aktivieren oder Verschlüsselung deaktivieren an.
7. Geben Sie im Bereich Cluster-Optionen den Port ein und wählen Sie die Cluster-Parametergruppe aus.
8. Wählen Sie im Bereich Backup die Option Continuous Backup for point-in-time Recovery (PITR), geplante Snapshot-Backups oder beides.
9. Wählen Sie im Bereich Protokollexporte die Protokolltypen aus, die in Amazon CloudWatch Logs veröffentlicht werden sollen. Die IAM-Rolle ist bereits definiert.

10. Geben Sie im Bereich Wartung ein Wartungsfenster an oder wählen Sie Keine Präferenz.
11. Klicken Sie im Bereich Tags auf Tag hinzufügen.
12. Wählen Sie im Abschnitt Löschschutz Löschschutz aktivieren aus.
13. Nachdem Sie alle Einstellungen angegeben haben, wählen Sie Backup wiederherstellen aus.

    Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.
14. Nachdem Ihre Wiederherstellung abgeschlossen ist, hängen Sie Ihr wiederhergestelltes Amazon-DocumentDB-Cluster an eine Amazon-RDS-Instance an.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Amazon DocumentDB DocumentDB-Wiederherstellungspunkte wiederherzustellen

Stellen Sie zunächst Ihren Cluster wieder her. Verwenden Sie `StartRestoreJob`. Sie können bei Amazon-DocumentDB-Wiederherstellungen die folgenden Metadaten angeben:

```
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
```

Anschließend verbinden Sie Ihren wiederhergestellten Amazon-DocumentDB-Cluster mit `create-db-instance` anhand einer Amazon-RDS-Instance.

- Für Linux, macOS oder Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Für Windows:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Wiederherstellen eines Neptun-Clusters

Verwenden Sie die AWS Backup Konsole, um Amazon Neptune Neptune-Wiederherstellungspunkte wiederherzustellen

Zum Wiederherstellen einer Amazon-Neptune-Datenbank müssen mehrere Wiederherstellungsoptionen angegeben werden. Informationen zu diesen Optionen finden Sie im Abschnitt zum Wiederherstellen aus einem DB-Cluster-Snapshot im Neptune-Benutzerhandbuch.

So stellen Sie eine Neptune-Datenbank wieder her:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und die Neptune-Ressourcen-ID aus, die Sie wiederherstellen möchten.
3. Auf der Seite Resource details (Ressourcendetails) wird eine Liste der Wiederherstellungspunkte für die ausgewählte Ressourcen-ID angezeigt. Um eine Ressource wiederherzustellen, wählen Sie im Bereich Backups das Optionsfeld neben der Wiederherstellungspunkt-ID der Ressource aus. Wählen Sie in der oberen rechten Ecke des Bereichs die Option Wiederherstellen.
4. Akzeptieren Sie im Bereich Instance-Spezifikationen die Standardeinstellungen oder geben Sie die DB-Engine und Version an.
5. Geben Sie im Bereich Einstellungen einen Namen an, der für alle DB-Cluster-Instances, die Ihnen gehören, AWS-Konto in der aktuellen Region eindeutig ist. Bei der DB-Cluster-Kennung wird zwischen Groß- und Kleinschreibung unterschieden, sie wird jedoch komplett in Kleinbuchstaben gespeichert, wie in `mydbclusterinstance`. Dies ist ein Pflichtfeld.

6. Übernehmen Sie im Bereich Datenbankoptionen die Standardeinstellungen oder geben Sie die Optionen für Datenbankport, DB-Cluster-Parametergruppe an.
7. Übernehmen Sie im Bereich Verschlüsselung die Standardeinstellung oder geben Sie die Optionen für Verschlüsselung aktivieren oder Verschlüsselung deaktivieren an.
8. Wählen Sie im Bereich Protokollexporte die Protokolltypen aus, die in Amazon CloudWatch Logs veröffentlicht werden sollen. Die IAM-Rolle ist bereits definiert.
9. Wählen Sie im Bereich Rolle wiederherstellen die IAM-Rolle aus, die AWS Backup für diese Wiederherstellung annimmt.
10. Nachdem Sie alle Einstellungen angegeben haben, wählen Sie Backup wiederherstellen aus.

    Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.
11. Nachdem Ihre Wiederherstellung abgeschlossen ist, hängen Sie Ihr wiederhergestelltes Neptune-Cluster an eine Amazon-RDS-Instance an.

Verwenden Sie die AWS Backup API, CLI oder das SDK, um Neptune-Wiederherstellungspunkte wiederherzustellen

Stellen Sie zunächst Ihren Cluster wieder her. Verwenden Sie `StartRestoreJob`. Sie können bei Amazon-DocumentDB-Wiederherstellungen die folgenden Metadaten angeben:

```
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
```

Anschließend verbinden Sie Ihren wiederhergestellten Neptune-Cluster mit `create-db-instance` anhand einer Amazon-RDS-Instance.

- Für Linux, macOS oder Unix:

```
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
```

- Für Windows:

```
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
```

Weitere Informationen finden Sie unter `RestoreDBClusterFromSnapshot` in der Neptune-Management API-Referenz und unter `restore-db-cluster-from-snapshot` im Neptune-CLI-Leitfaden.

Stack-Backups wiederherstellen CloudFormation

Ein CloudFormation zusammengesetztes Backup ist eine Kombination aus einer CloudFormation Vorlage und allen zugehörigen verschachtelten Wiederherstellungspunkten. Es ist möglich, eine beliebige Anzahl von verschachtelten Wiederherstellungspunkten wiederherzustellen, aber der Verbundwiederherstellungspunkt (der der Wiederherstellungspunkt der obersten Ebene ist) kann nicht wiederhergestellt werden.

Wenn Sie einen CloudFormation Vorlagen-Wiederherstellungspunkt wiederherstellen, erstellen Sie einen neuen Stack mit einem Änderungssatz, der das Backup darstellt.

Wiederherstellung CloudFormation mit der AWS Backup Konsole;

Von der CloudFormation Konsole aus können Sie den neuen Stack und das Change-Set sehen. Weitere Informationen zu Änderungssätzen finden Sie unter Aktualisieren von Stacks mithilfe von Änderungssätzen im AWS CloudFormation -Benutzerhandbuch.

Ermitteln Sie, von welchen verschachtelten Wiederherstellungspunkten Sie mit Ihrem CloudFormation Stack wiederherstellen möchten, und stellen Sie sie dann mithilfe der AWS Backup Konsole wieder her.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Gehen Sie zu Backup-Tresore, wählen Sie den Backup-Tresor aus, der Ihren gewünschten Wiederherstellungspunkt enthält, und klicken Sie dann auf Wiederherstellungspunkte.
3. Stellen Sie den AWS CloudFormation Vorlagenwiederherstellungspunkt wieder her.

   a. Klicken Sie auf den Verbundwiederherstellungspunkt, der die verschachtelten Wiederherstellungspunkte enthält, die Sie wiederherstellen möchten, um die Detailseite für den Verbundwiederherstellungspunkt aufzurufen.

   b. Unter Verschachtelte Wiederherstellungspunkte werden die verschachtelten Wiederherstellungspunkte angezeigt. Jeder Wiederherstellungspunkt hat eine Wiederherstellungspunkt-ID, einen Status, eine Ressourcen-ID, einen Ressourcentyp, einen Backup-Typ und die Uhrzeit, zu der der Wiederherstellungspunkt erstellt wurde. Klicken Sie auf das Optionsfeld neben dem AWS CloudFormation Wiederherstellungspunkt und dann auf Wiederherstellen. Stellen Sie sicher, dass für den Wiederherstellungspunkt mit Ressourcentyp: AWS CloudFormation und Backup-Typ: Backup festgelegt ist.
4. Sobald der Wiederherstellungsauftrag für die CloudFormation Vorlage abgeschlossen ist, wird Ihre wiederhergestellte AWS CloudFormation Vorlage in der AWS CloudFormation Konsole unter Stacks angezeigt.
5. Unter Stack-Namen sollten Sie die wiederhergestellte Vorlage mit dem Status von `REVIEW_IN_PROGRESS` finden.
6. Klicken Sie auf den Stack-Namen, um die Stack-Details zu sehen.
7. Unter dem Stack-Namen befinden sich Tabs. Klicken Sie auf Änderungssatz.
8. Führen Sie den Änderungssatz aus.
9. Nach diesen Vorgängen werden die Ressourcen im ursprünglichen Stack im neuen Stack neu erstellt. Die statusbehafteten Ressourcen werden leer neu erstellt. Um die statusbehafteten Ressourcen wiederherzustellen, kehren Sie zur Liste der Wiederherstellungspunkte in der AWS Backup Konsole zurück, wählen Sie den gewünschten Wiederherstellungspunkt aus und starten Sie eine Wiederherstellung.

Wiederherstellung CloudFormation mit AWS CLI

`start-restore-job`Ermöglicht das Wiederherstellen eines CloudFormation Stacks in der Befehlszeilenschnittstelle.

Die folgende Liste enthält die akzeptierten Metadaten zum Wiederherstellen einer CloudFormation Ressource.

```
// 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
```

Wiederherstellungstests

Themen

Übersicht

Wiederherstellungstests, eine von angebotene Funktion AWS Backup, ermöglichen eine automatische und regelmäßige Bewertung der Durchführbarkeit einer Wiederherstellung sowie die Überwachung der Dauer von Wiederherstellungsaufträgen.

Zunächst erstellen Sie einen Wiederherstellungstestplan, wobei Sie einen Namen für Ihren Plan, die Häufigkeit der Wiederherstellungstests und die Zielstartzeit angeben. Dann weisen Sie die Ressourcen zu, die in Ihren Plan aufgenommen werden sollen. Anschließend entscheiden Sie, ob Sie bestimmte oder zufällige Wiederherstellungspunkte in Ihren Test einbeziehen möchten. AWS Backup backup leitet auf intelligente Weise die Metadaten ab, die für den Erfolg Ihres Wiederherstellungsauftrags benötigt werden.

Wenn der in Ihrem Plan festgelegte Zeitpunkt erreicht ist, werden die Wiederherstellungsaufträge auf der Grundlage Ihres Plans AWS Backup gestartet und die Zeit überwacht, die bis zum Abschluss der Wiederherstellung benötigt wird.

Nachdem der Wiederherstellungstestplan seine Ausführung abgeschlossen hat, können Sie anhand der Ergebnisse die Einhaltung organisatorischer oder behördlicher Anforderungen nachweisen, z. B. den erfolgreichen Abschluss von Wiederherstellungstestszenarien oder die Zeit für den Abschluss des Wiederherstellungsauftrags.

Optional können Sie es verwenden, Validierung des Wiederherstellungstests um die Ergebnisse des Wiederherstellungstests zu bestätigen.

Sobald die optionale Validierung abgeschlossen ist oder das Validierungsfenster geschlossen wird, werden die am Wiederherstellungstest beteiligten Ressourcen AWS Backup gelöscht, und die Ressourcen werden gemäß den Service-SLAs gelöscht.

Am Ende des Testvorgangs können Sie die Ergebnisse und die Abschlusszeit der Tests anzeigen.

Wiederherstellungstests im Vergleich zum Wiederherstellungsprozess

Beim Wiederherstellungstest werden Wiederherstellungsaufträge auf die gleiche Weise ausgeführt wie Wiederherstellungen auf Abruf. Dabei werden dieselben Wiederherstellungspunkte (Backups) wie bei einer Wiederherstellung auf Abruf verwendet. Für jeden Job, der mit dem `StartRestoreJob` CloudTrail Wiederherstellungstest gestartet wurde, werden Aufrufe von IN (falls aktiviert) angezeigt

Es gibt jedoch einige Unterschiede zwischen der Durchführung eines Tests zur Wiederherstellung nach Zeitplan und einer Wiederherstellung auf Abruf:

	Wiederherstellungstests	Wiederherstellung
Account	Es wird empfohlen, ein Konto festzulegen, das für Wiederher	Sie können Ressourcen von einem Konto aus wiederher stellen

	Wiederherstellungstests	Wiederherstellung
	stellungstests verwendet werden soll	
AWS Backup Audit Manager	Kann ein Steuerelement aktivieren, um zu bestätigen, ob ein Wiederherstellungstest die angegebenen Wiederher stellungsziele erfüllt	
Kadenz	Regelmäßig als Teil eines geplanten Plans.	On-Demand
Regionalität	Verfügbar in allen Handelsre gionen, in denen das AWS Backup Unternehmen tätig ist, mit Ausnahme von Israel (Tel Aviv) Nicht verfügbar AWS GovCloud (US-Ost), AWS GovCloud (US-West), China (Peking) und China (Ningxia).	Verfügbar in allen Handelsre gionen, in denen das Unternehmen tätig ist AWS Backup
Ressourcen	Zu den Ressourcentypen, die Sie Ihrem Testplan zuweisen können, gehören: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS und Amazon S3.	Alle Ressourcen können wiederhergestellt werden.

	Wiederherstellungstests	Wiederherstellung
Ergebnisse	Sobald der Wiederherstellungstestauftrag abgeschlossen ist, wird die wiederhergestellte Ressource nach Abschluss des Validierung des Wiederherstellungstests Fensters gelöscht.	Sobald der Wiederherstellungsauftrag abgeschlossen ist, bleibt die wiederhergestellte Version der Ressource erhalten.
Tags	Bei Ressourcentypen, die Tags bei der Wiederherstellung unterstützen, werden beim Testen Tags bei der Wiederherstellung angewendet.	Tags sind für unterstützte Ressourcen optional.

Verwaltung von Wiederherstellungstests

In der AWS Backup -Konsole können Sie einen Wiederherstellungtestplan erstellen, anzeigen, aktualisieren oder löschen.

Sie können AWS CLI verwenden, um Operationen für Wiederherstellungstestpläne programmgesteuert auszuführen. Jede CLI ist spezifisch für den AWS Dienst, aus dem sie stammt. Befehlen sollte das Präfix `aws backup` vorangestellt werden.

Löschen von Daten

Wenn ein Wiederherstellungstest abgeschlossen ist, AWS Backup beginnt das Löschen der am Test beteiligten Ressourcen. Dieses Löschen erfolgt nicht sofort. Jeder Ressource liegt eine Konfiguration zugrunde, die bestimmt, wie diese Ressourcen gespeichert und wie sie über ihren Lebenszyklus verteilt werden. Wenn beispielsweise Amazon-S3-Buckets Teil des Wiederherstellungstests sind, werden dem Bucket Lebenszyklusregeln hinzugefügt. Es kann bis zu mehreren Tagen dauern, bis die Regeln ausgeführt werden und der Bucket und seine Objekte vollständig gelöscht sind. Gebühren fallen für diese Ressourcen jedoch nur bis zu dem Tag an, an dem die Lebenszyklusregel initiiert wird (standardmäßig ist dies 1 Tag). Die Geschwindigkeit des Löschvorgangs hängt vom Ressourcentyp ab.

Ressourcen, die Teil eines Wiederherstellungstestplans sind, enthalten ein Tag mit dem Namen `awsbackup-restore-test`. Wenn ein Benutzer dieses Tag entfernt, AWS Backup kann die Ressource am Ende des Testzeitraums nicht gelöscht werden, und der Benutzer muss sie stattdessen manuell löschen.

Um zu überprüfen, warum Ressourcen möglicherweise nicht wie erwartet gelöscht wurden, können Sie in der Konsole nach fehlgeschlagenen Aufträgen suchen oder über die Befehlszeilenschnittstelle die API-Anfrage `DescribeRestoreJob` aufrufen, um Meldungen zum Löschstatus abzurufen.

Backup-Pläne (Testpläne ohne Wiederherstellung) ignorieren Ressourcen, die durch Wiederherstellungstests erstellt wurden (solche, deren Tag `awsbackup-restore-test` oder Name mit beginnt`awsbackup-restore-test`).

Kostenkontrolle

Bei Wiederherstellungstests fallen Kosten pro Wiederherstellungstest an. Je nachdem, welche Ressourcen in Ihrem Wiederherstellungstestplan enthalten sind, können für die Wiederherstellungsaufträge, die Teil des Plans sind, ebenso Kosten anfallen. Alle Einzelheiten finden Sie unter AWS Backup -Preise.

Wenn Sie zum ersten Mal einen Wiederherstellungstestplan einrichten, kann es für Sie von Vorteil sein, eine Mindestanzahl an Ressourcentypen und geschützten Ressourcen anzugeben, um sich mit dem Feature, dem Prozess und den damit verbundenen durchschnittlichen Kosten vertraut zu machen. Sie können einen Plan nach dessen Erstellung aktualisieren, um weitere Ressourcentypen und geschützte Ressourcen hinzuzufügen.

Erstellen eines Wiederherstellungstestplans

Ein Wiederherstellungstestplan besteht aus zwei Teilen: der Erstellung des Plans und der Zuweisung von Ressourcen.

Wenn Sie die Konsole verwenden, sind diese Teile sequenziell. Im ersten Teil legen Sie den Namen, die Frequenz und die Startzeiten fest. Im zweiten Teil weisen Sie Ihrem Testplan Ressourcen zu.

Wenn Sie eine API verwenden AWS CLI , verwenden Sie `create-restore-testing-plan`sie zuerst. Sobald Sie eine erfolgreiche Antwort erhalten haben und der Plan erstellt wurde, verwenden Sie `create-restore-testing-selection` für jeden Ressourcentyp, den Sie in Ihren Plan aufnehmen möchten.

Console

Teil I: Erstellen eines Wiederherstellungstestplans mithilfe der Konsole

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Suchen Sie im linken Navigationsbereich nach Wiederherstellungstests und wählen Sie dies aus.
3. Wählen Sie Wiederherstellungstestplan erstellen aus.
4. Allgemeines
    a. Name: Geben Sie einen Namen für Ihren neuen Wiederherstellungstestplan ein. Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name darf nur alphanumerische Zeichen und Unterstriche enthalten.
    b. Testfrequenz: Wählen Sie die Häufigkeit aus, mit der die Wiederherstellungstests ausgeführt werden.
    c. Startzeit: Stellen Sie die Uhrzeit (in Stunden und Minuten) ein, zu der der Test beginnen soll. Sie können auch die lokale Zeitzone festlegen, in der der Wiederherstellungstestplan ausgeführt werden soll.
    d. Start innerhalb: Dieser Wert (in Stunden) ist der Zeitraum, in dem der Wiederherstellungstest beginnen soll. AWS Backup bemüht sich nach besten Kräften, alle vorgesehenen Wiederherstellungsaufträge während des Startzeitraums zu starten, und ordnet die Startzeiten innerhalb dieses Zeitraums nach dem Zufallsprinzip an.
5. Auswahl des Wiederherstellungspunkts: Hier legen Sie die Quelltresore, den Wiederherstellungspunktbereich und die Auswahlkriterien dafür fest, welche Wiederherstellungspunkte (Backups) Teil des Plans sein sollen.
    a. Quelltresore: Wählen Sie aus, ob Sie alle verfügbaren Tresore oder nur bestimmte Tresore einbeziehen möchten, um zu filtern, welche Wiederherstellungspunkte in Ihrem Plan enthalten sein können. Wenn Sie sich für bestimmte Tresore entscheiden, wählen Sie aus dem Dropdown-Menü die Tresore aus, die Sie einbeziehen möchten.
    b. Berechtigte Wiederherstellungspunkte: Geben Sie den Zeitrahmen an, aus dem die Wiederherstellungspunkte ausgewählt werden. Sie können 1 bis 365 Tage, 1 bis 52 Wochen, 1 bis 12 Monate oder 1 Jahr wählen.
    c. Auswahlkriterien: Sobald Ihr Zeitraum für die Wiederherstellungspunkte festgelegt ist, können Sie wählen, ob Sie den neuesten oder einen zufälligen in Ihren Plan aufnehmen möchten. Möglicherweise möchten Sie einen zufälligen Wert auswählen, um den

allgemeinen Zustand der Wiederherstellungspunkte in regelmäßigeren Abständen zu überprüfen, falls eine Wiederherstellung auf eine ältere Version jemals erforderlich sein sollte.

d. P oint-in-time Wiederherstellungspunkte: Wenn Ihr Plan Ressourcen mit kontinuierlichen Sicherungspunkten (point-in-time-restore/PITR) umfasst, können Sie dieses Kontrollkästchen aktivieren, damit Ihr Testplan kontinuierliche Backups als geeignete Wiederherstellungspunkte umfasst (siehe Verfügbarkeit von Funktionen nach Ressourcen, für die Ressourcentypen über diese Funktion verfügen).

6. (optional) Dem Wiederherstellungstestplan hinzugefügte Tags: Sie können wählen, ob Sie Ihrem Wiederherstellungstestplan bis zu 50 Tags hinzufügen möchten. Alle Tags müssen separat hinzugefügt werden. Um einen neuen Tag hinzuzufügen, wählen Sie Neuen Tag hinzufügen.

Teil II: Dem Plan mithilfe der Konsole Ressourcen zuweisen

In diesem Abschnitt wählen Sie die Ressourcen aus, die Sie gesichert haben, um sie in Ihren Wiederherstellungstestplan aufzunehmen. Sie wählen den Namen der Ressourcenzuweisung und die Rolle, die Sie für den Wiederherstellungstest verwenden, aus und legen den Aufbewahrungszeitraum vor der Bereinigung fest. Anschließend wählen Sie den Ressourcentyp und den Umfang aus und verfeinern Ihre Auswahl optional mit Tags.

> **Tip**
>
> Um zu dem Wiederherstellungstestplan zurückzukehren, dem Sie Ressourcen hinzufügen möchten, können Sie in der AWS Backup -Konsole die Option Wiederherstellungstests auswählen, dann Ihren bevorzugten Testplan suchen und ihn auswählen.

1. Allgemeines

   a. Name der Ressourcenzuweisung: Geben Sie einen Namen für diese Ressourcenzuweisung ein. Verwenden Sie dazu eine Zeichenfolge aus alphanumerischen Zeichen und Unterstrichen ohne Leerzeichen.

   b. Wiederherstellen der IAM-Rolle: Der Test muss eine von Ihnen angegebene Identity-and-Access-Management (IAM)-Rolle verwenden. Sie können die AWS Backup Standardrolle oder eine andere Rolle wählen. Wenn die AWS Backup Standardeinstellung nach Abschluss dieses Vorgangs noch nicht vorhanden ist, AWS Backup wird sie automatisch

mit den erforderlichen Berechtigungen für Sie erstellt. Die IAM-Rolle, die Sie für den Wiederherstellungstest auswählen, muss die in AWSBackupServicePolicyForRestores enthaltenen Berechtigungen enthalten.

c. Aufbewahrungszeitraum vor der Bereinigung: Während eines Wiederherstellungstests werden Backup-Daten vorübergehend wiederhergestellt. Standardmäßig werden diese Daten nach Abschluss des Tests gelöscht. Sie haben die Möglichkeit, das Löschen dieser Daten zu verzögern, wenn Sie die Wiederherstellung validieren möchten.

   Wenn Sie die Validierung ausführen möchten, wählen Sie Für eine bestimmte Anzahl von Stunden aufbewahren und geben Sie einen Wert zwischen 1 und 168 Stunden (einschließlich) ein. Beachten Sie, dass die Validierung programmgesteuert, jedoch nicht von der AWS Backup -Konsole aus ausgeführt werden kann.

2. Geschützte Ressourcen:

   a. Ressourcentyp auswählen: Wählen Sie aus, welche Ressourcentypen und welcher Umfang von Backups dieser Typen in den Ressourcentestplan aufgenommen werden sollen. Jeder Plan kann mehrere Ressourcentypen enthalten, aber jeder Ressourcentyp muss dem Plan einzeln zugewiesen werden.

   b. Umfang der Ressourcenauswahl: Sobald der Typ ausgewählt ist, wählen Sie aus, ob Sie alle verfügbaren geschützten Ressourcen dieses Typs oder nur bestimmte geschützte Ressourcen einbeziehen möchten.

   c. (optional) Verfeinern der Ressourcenauswahl mithilfe von Tags: Wenn Ihre Backups Tags enthalten, können Sie nach Tags filtern, um bestimmte geschützte Ressourcen auszuwählen. Geben Sie den Tag-Schlüssel, die Bedingung, unter der dieser Schlüssel enthalten sein soll oder nicht, und den Wert für den Schlüssel ein. Wählen Sie dann die Schaltfläche Tags hinzufügen aus.

      Tags auf geschützten Ressourcen werden evaluiert, indem die Tags auf dem letzten Wiederherstellungspunkt im Backup-Tresor überprüft werden, der die geschützte Ressource enthält.

3. Wiederherstellungsparameter: Bei bestimmten Ressourcen müssen zur Vorbereitung eines Wiederherstellungsauftrags Parameter angegeben werden. In den meisten Fällen AWS Backup werden die Werte auf der Grundlage des gespeicherten Backups abgeleitet.

   In den meisten Fällen wird empfohlen, diese Parameter beizubehalten. Sie können die Werte jedoch ändern, indem Sie eine andere Auswahl aus dem Dropdown-Menü auswählen. Zu den Beispielen, bei denen eine Änderung der Werte optimal sein kann, gehören das

Überschreiben von Verschlüsselungsschlüsseln, Amazon-FSx-Einstellungen, bei denen keine Daten abgeleitet werden können, und die Erstellung von Subnetzen.

Wenn beispielsweise eine RDS-Datenbank zu den Ressourcentypen gehört, die Sie Ihrem Wiederherstellungstestplan zuweisen, werden Parameter wie Availability Zone, Datenbankname, Datenbank-Instance-Klasse und VPC-Sicherheitsgruppe mit abgeleiteten Werten angezeigt, die Sie gegebenenfalls ändern können.

AWS CLI

Der CLI-Befehl `CreateRestoreTestingPlan` wird verwendet, um einen Wiederherstellungstestplan zu erstellen.

Der Testplan muss Folgendes enthalten:

- `RestoreTestingPlan`, der einen eindeutigen `RestoreTestingPlanName` enthalten muss
- `ScheduleExpression`-Cron-Ausdruck
- `RecoveryPointSelection`

  Obwohl es ähnlich benannt ist, ist es NICHT dasselbe wie`RestoreTestingSelection`.

  `RecoveryPointSelection`hat fünf Parameter (drei erforderlich und zwei optional). Die von Ihnen angegebenen Werte bestimmen, welcher Erholungspunkt im Wiederherstellungstest enthalten ist. Sie müssen angeben, `Algorithm` ob Sie den neuesten `SelectionWindowDays` oder einen zufälligen Wiederherstellungspunkt verwenden möchten, und Sie müssen angeben, `IncludeVaults` aus welchen Tresoren die Wiederherstellungspunkte ausgewählt werden können.

Eine Auswahl kann einen oder mehrere ARNs für geschützte Ressourcen oder eine oder mehrere Bedingungen haben, aber sie kann nicht beide haben.

Sie können auch Folgendes einschließen:

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

Verwenden Sie den CLI-Befehl `create-restore-testing-plan`.

Sobald der Plan erfolgreich erstellt wurde, müssen Sie ihm mithilfe von `create-restore-testing-selection` Ressourcen zuweisen.

Dies besteht aus `RestoreTestingSelectionName`, `ProtectedResourceType` und einem der folgenden Elemente:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Jeder geschützte Ressourcentyp kann einen einzelnen Wert haben. Eine Auswahl für den Wiederherstellungstest kann einen Platzhalterwert („*“) für `ProtectedResourceArns` zusammen mit `ProtectedResourceConditions` enthalten. Alternativ können Sie bis zu 30 spezifische ARNs für geschützte Ressourcen in `ProtectedResourceArns` hinzufügen.

Bestimmung des Wiederherstellungspunkts

Jedes Mal, wenn ein Testplan ausgeführt wird (entsprechend der von Ihnen angegebenen Häufigkeit und Startzeit), wird ein geeigneter Wiederherstellungspunkt pro ausgewählter geschützter Ressource durch den Wiederherstellungstest wiederhergestellt. Wenn keine Wiederherstellungspunkte für eine Ressource die Auswahlkriterien für den Wiederherstellungspunkt erfüllen, wird diese Ressource nicht in den Test aufgenommen.

Ein Erholungspunkt für eine geschützte Ressource in einer Testauswahl kommt in Frage, wenn er die Kriterien für den angegebenen Zeitraum erfüllt und Tresore in den Wiederherstellungstestplan aufgenommen hat.

Eine geschützte Ressource wird ausgewählt, wenn die Auswahl des Ressourcentests den Ressourcentyp beinhaltet und wenn eine der folgenden Bedingungen zutrifft:

- Der Ressourcen-ARN ist in dieser Auswahl angegeben; oder
- Die Tag-Bedingungen für diese Auswahl stimmen mit den Tags auf dem letzten Recovery Point für die Ressource überein

Aktualisieren eines Wiederherstellungstestplans

Sie können Teile Ihres Wiederherstellungstestplans und die darin enthaltenen Ressourcenauswahlen über die Konsole oder AWS CLI aktualisieren.

Console

Aktualisieren von Wiederherstellungstestplänen und Auswahlen in der Konsole

Wenn Sie die Seite mit den Details zum Wiederherstellungstestplan in der Konsole aufrufen, können Sie viele Einstellungen Ihres Plans bearbeiten (aktualisieren). Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Suchen Sie im linken Navigationsbereich nach Wiederherstellungstests und wählen Sie dies aus.
3. Wählen Sie die Schaltfläche Bearbeiten aus.
4. Passen Sie die Häufigkeit, die Startzeit und die Zeit an, zu der der Test beginnen soll, innerhalb derer der Test nach der ausgewählten Startzeit beginnt.
5. Speichern Sie Ihre Änderungen.

AWS CLI

Aktualisieren Sie die Pläne und Auswahlen für die Wiederherstellung mithilfe von AWS CLI

Fordert an UpdateRestoreTestingPlanund UpdateRestoreTestingSelectionkann verwendet werden, um Teilaktualisierungen für einen bestimmten Plan oder eine Auswahl zu senden. Die Namen können nicht geändert werden, aber Sie können andere Parameter aktualisieren. Nehmen Sie in jede Anforderung nur Parameter auf, die Sie ändern möchten.

Verwenden Sie GetRestoreTestingPlanund, bevor Sie eine Aktualisierungsanfrage senden, GetRestoreTestingSelectionum festzustellen, ob Ihr RestoreTestingSelection Konto bestimmte ARNs enthält oder ob es den Platzhalter und die Bedingungen verwendet.

Wenn Ihre Wiederherstellungstest-Auswahl ARNs (anstelle von Platzhaltern) angegeben hat und Sie diese zu einem Platzhalter mit Bedingungen ändern möchten, muss die Aktualisierungsanforderung sowohl den ARN-Platzhalter als auch die Bedingungen enthalten. Eine Auswahl kann entweder ARNs für geschützte Ressourcen haben oder den Platzhalter mit Bedingungen verwenden, aber sie kann nicht beides haben.

- get-restore-testing-plan
- get-restore-testing-selection
- update-restore-testing-plan
- update-restore-testing-selection

Anzeigen bestehender Wiederherstellungstestpläne

Console

Anzeigen von Details zu einem vorhandenen Wiederherstellungstestplan und den zugewiesenen Ressourcen in der Konsole

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Wiederherstellungstests aus. Auf dem Display werden Ihre Wiederherstellungstestpläne angezeigt. Die Pläne werden standardmäßig nach der letzten Laufzeit angezeigt.
3. Wählen Sie den Link in einem Plan aus, um dessen Details anzuzeigen, einschließlich einer Zusammenfassung des Plans, seines Namens, seiner Häufigkeit, seiner Startzeit und seines „Start innerhalb von“-Werts.

Sie können auch die geschützten Ressourcen in diesem Plan, die Wiederherstellungstestaufträge der letzten 30 Tage, die in diesem Plan enthalten sind, und alle Tags, die Sie als Teil dieses Testplans erstellen können, einsehen.

AWS CLI

Abrufen von Details zu einem vorhandenen Wiederherstellungstestplan und zur Auswahl über die Befehlszeile

- list-restore-testing-plan
- list-restore-testing-selections
- get-restore-testing-plan
- get-restore-testing-selection

Anzeigen von Wiederherstellungstestaufträgen

Console

Anzeigen bestehender Wiederherstellungstestaufträge in der Konsole

Wiederherstellungstestaufträge sind auf der Seite mit Wiederherstellungsaufträgen enthalten.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Navigieren Sie zur Seite Aufträge.

   Alternativ können Sie Wiederherstellungstests und dann einen Wiederherstellungstestplan auswählen, um dessen Details und die mit dem Plan verknüpften Aufträge anzuzeigen.
3. Wählen Sie die Registerkarte Wiederherstellungsaufträge aus.

   Auf dieser Seite können Sie den Status, die Wiederherstellungszeit, den Wiederherstellungstyp, die Ressourcen-ID, den Ressourcentyp, den Wiederherstellungstestplan, zu dem der Auftrag gehört, die Erstellungszeit und die Wiederherstellungspunkt-ID des Wiederherstellungsauftrags anzeigen.

   Aufträge, die in einem Wiederherstellungstestplan enthalten sind, haben den Wiederherstellungstyp Test.

Wiederherstellungstestaufträge haben mehrere Statuskategorien:

- Ein Status-Typ, der Aufmerksamkeit erfordert, ist unterstrichen. Bewegen Sie den Mauszeiger über den Status, um weitere Details zu sehen, falls sie verfügbar sind.
- Es wird ein Validierungsstatus angezeigt, ob der Test initiiert Validierung des Wiederherstellungstests wurde (nicht in der Konsole verfügbar).
- Im Löschstatus wird der Status der durch den Wiederherstellungstest generierten Daten angegeben. Es gibt drei mögliche Löschstatus: Erfolgreich, Löschen und Fehlgeschlagen.

  Wenn das Löschen eines Wiederherstellungstestauftrags fehlgeschlagen ist, müssen Sie die Ressource manuell entfernen, da der Wiederherstellungstestablauf den Vorgang nicht automatisch abschließen konnte. Oft wird ein fehlgeschlagener Löschvorgang ausgelöst, wenn der Tag `awsbackup-restore-test` aus der Ressource entfernt wird.

AWS CLI

Anzeigen bestehender Wiederherstellungstestaufträge über die Befehlszeile

- `list-restore-jobs-by-protected-resource`

Löschen eines Wiederherstellungstestplans

Console

Löschen eines Wiederherstellungstestplans in der Konsole

1. Rufen Sie Anzeigen bestehender Wiederherstellungstestpläne auf, um Ihre aktuellen Wiederherstellungstestpläne anzuzeigen.
2. Löschen Sie auf der Seite mit den Details zum Wiederherstellungstestplan einen Plan, indem Sie Löschen auswählen.
3. Nachdem Sie „Löschen“ ausgewählt haben, wird ein Popup-Fenster zur Bestätigung angezeigt, dass Sie Ihren Plan löschen möchten. Auf diesem Bildschirm wird der Name Ihres spezifischen Wiederherstellungstestplans fett gedruckt angezeigt. Um fortzufahren, geben Sie den genauen Namen des Testplans unter Berücksichtigung der Groß- und Kleinschreibung ein, einschließlich aller Unterstriche, Bindestriche und Punkte.

   Wenn die Option Wiederherstellungstestplan löschen nicht ausgewählt werden kann, geben Sie den Namen erneut ein, bis er mit dem angezeigten Namen übereinstimmt. Sobald der Wert exakt übereinstimmt, kann die Option zum Löschen des Wiederherstellungstestplans ausgewählt werden.

AWS CLI

Löschen eines Wiederherstellungstestplans über die Befehlszeile

Der CLI-Befehl DeleteRestoreTestingSelectionkann verwendet werden, um eine Auswahl für Wiederherstellungstests zu löschen. Fügen Sie `RestoreTestingPlanName` und `RestoreTestingSelectionName` in die Anforderung ein.

Alle Testauswahlen, die mit einem Testplan verknüpft sind, müssen gelöscht werden, bevor der Testplan gelöscht werden kann. Sobald alle Testauswahlen gelöscht wurden, können Sie die API-

Anfrage verwenden, DeleteRestoreTestingPlanum einen Wiederherstellungstestplan zu löschen. Sie müssen `RestoreTestingPlanName` einschließen.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Prüfung eines Wiederherstellungstests

Stellen Sie Testintegrationen mit AWS Backup Audit Manager wieder her, damit Sie beurteilen können, ob eine wiederhergestellte Ressource innerhalb Ihrer Zielwiederherstellungszeit abgeschlossen wurde.

Weitere Informationen finden Sie unter Wiederherstellungszeit für Ressourcen, die dem Ziel entsprechen in AWS Backup Steuerelemente und Korrekturmaßnahmen in Audit Manager.

Kontingente und Parameter für Wiederherstellungstests

- 100 Wiederherstellungstestpläne
- Jedem Wiederherstellungstestplan können 50 Tags hinzugefügt werden
- 30 Auswahlen pro Plan
- 30 ARNs für geschützte Ressourcen pro Auswahl
- 30 Bedingungen für geschützte Ressourcen pro Auswahl (einschließlich der Bedingungen innerhalb von `StringEquals` und `StringNotEquals`)
- 30 Tresor-Selektoren pro Auswahl
- Maximales Auswahlzeitfenster in Tagen: 365 Tage
- Startzeitfenster in Stunden: Min.: 1 Stunde; Max.: 168 Stunden (7 Tage)
- Max. Länge des Plannamens: 50 Zeichen
- Max. Länge des Auswahlnamens: 50 Zeichen

Zusätzliche Informationen zu den Grenzwerten finden Sie unter AWS Backup Kontingente.

Wiederherstellung, Testfehler und Fehlerbehebung

Wenn Sie über Wiederherstellungstestaufträge mit dem Wiederherstellungsstatus von verfügen`Failed`, können Ihnen die folgenden Gründe dabei helfen, die Ursache zu ermitteln und Abhilfe zu schaffen.

Fehlermeldungen können in der AWS Backup Konsole auf der Seite mit den Auftragsstatusdetails oder mithilfe der CLI-Befehle `list-restore-jobs-by-protected-resource` oder angezeigt werden`list-restore-jobs`.

1. Fehler: *`No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.`*

   Lösung 1: Aktualisieren Sie Ihre Auswahl für den Wiederherstellungstest und überschreiben Sie den Parameter`SubnetId`. Die AWS Backup Konsole zeigt diesen Parameter als „Subnetz“ an.

   Lösung 2: Erstellen Sie die Standard-VPC neu.

   Betroffene Ressourcentypen: Amazon EC2

2. Fehler: *`No subnets found for the default VPC [vpc]. Please specify a subnet.`*

   Lösung 1: Aktualisieren Sie Ihre Auswahl für den Wiederherstellungstest und überschreiben Sie den `SubnetId` Wiederherstellungsparameter. Die AWS Backup Konsole zeigt diesen Parameter als „Subnetz“ an.

   Lösung 2: Erstellen Sie ein Standardsubnetz in der Standard-VPC.

   Betroffene Ressourcentypen: Amazon EC2

3. Fehler: *`No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.`*

   Lösung 1: Aktualisieren Sie Ihre Auswahl für den Wiederherstellungstest und überschreiben Sie den `DBSubnetGroupName` Wiederherstellungsparameter. Die AWS Backup Konsole zeigt diesen Parameter als Subnetzgruppe an.

   Lösung 2: Erstellen Sie ein Standardsubnetz in der Standard-VPC.

   Betroffene Ressourcentypen: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Fehler:. *`IAM Role cannot be assumed by AWS Backup`*

   Lösung: Die Wiederherstellungsrolle muss von AWS Backupübernommen werden. Aktualisieren Sie entweder die Vertrauensrichtlinie der Rolle in IAM, sodass sie von übernommen werden kann,

"backup.amazonaws.com" oder aktualisieren Sie Ihre Auswahl für den Wiederherstellungstest, sodass eine Rolle verwendet wird, die als angenommen werden kann. AWS Backup

Betroffene Ressourcentypen: alle

5. Fehler: *Access denied to KMS key.* oder *The specified AWS KMS key* ARN *does not exist, is not enabled or you do not have permissions to access it.*

   Lösung: Überprüfen Sie Folgendes:

   a. Die Wiederherstellungsrolle hat Zugriff auf den AWS KMS Schlüssel, der zum Verschlüsseln Ihrer Backups verwendet wurde, und gegebenenfalls auf den KMS-Schlüssel, mit dem die wiederhergestellte Ressource verschlüsselt wurde.

   b. Die Ressourcenrichtlinien für die oben genannten KMS-Schlüssel ermöglichen es der Wiederherstellungsrolle, auf sie zuzugreifen.

   Wenn die oben genannten Bedingungen noch nicht erfüllt sind, konfigurieren Sie die Wiederherstellungsrolle und die Ressourcenrichtlinien für den entsprechenden Zugriff. Führen Sie dann den Wiederherstellungstestjob erneut aus.

   Betroffene Ressourcentypen: alle

6. Fehler: *User ARN is not authorized to perform action on resource because no identity based policy allows the action.* oder*Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*.

   Lösung: Die Wiederherstellungsrolle verfügt nicht über die erforderlichen Berechtigungen. Aktualisieren Sie die Berechtigungen in IAM für die Wiederherstellungsrolle.

   Betroffene Ressourcentypen: alle

7. Fehler: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* oder *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   Lösung: Die Wiederherstellungsrolle hat keinen ausreichenden Zugriff auf die in der Nachricht angegebene Ressource. Aktualisieren Sie die Ressourcenrichtlinie für die erwähnte Ressource.

   Betroffene Ressourcentypen: alle

Abgeleitete Metadaten bei Wiederherstellungstests

Die Wiederherstellung eines Wiederherstellungspunkts erfordert Metadaten für die Wiederherstellung. Für die Durchführung von Wiederherstellungstests leitet AWS Backup automatisch Metadaten ab, die wahrscheinlich zu einer erfolgreichen Wiederherstellung führen. Der Befehl `get-restore-testing-inferred-metadata` kann verwendet werden, um eine Vorschau der AWS Backup Folgerungen anzuzeigen. Der Befehl `get-restore-job-metadata` gibt den Satz von Metadaten zurück, der von abgeleitet wurde. AWS Backup Beachten Sie, dass für einige Ressourcentypen (Amazon FSx) AWS Backup kein vollständiger Satz von Metadaten abgeleitet werden kann.

Die abgeleiteten Wiederherstellungsmetadaten werden während des Wiederherstellungstests ermittelt. Sie können bestimmte Schlüssel für Wiederherstellungsmetadaten überschreiben, indem Sie den Parameter `RestoreMetadataOverrides` in den Hauptteil von `RestoreTestingSelection` aufnehmen. Einige Metadaten-Overrides sind in der Konsole nicht verfügbar. AWS Backup

Jede unterstützte Ressource verfügt sowohl über abgeleitete Schlüssel und Werte für Wiederherstellungsmetadaten als auch über überschreibbare Schlüssel für Wiederherstellungsmetadaten. Es müssen nur `RestoreMetadataOverrides`-Schlüssel-/Wert-Paare oder verschachtelte Schlüssel-/Wert-Paare aufgenommen werden, die mit *`Für eine erfolgreiche Wiederherstellung erforderlich`* gekennzeichnet sind. Die anderen sind optional. Beachten Sie, dass Schlüsselwerte nicht zwischen Groß- und Kleinschreibung unterscheiden.

> **Important**
>
> AWS Backup kann daraus schließen, dass eine Ressource auf die Standardeinstellung zurückgesetzt werden sollte, z. B. eine Amazon EC2 EC2-Instance oder ein Amazon RDS-Cluster, der auf der Standard-VPC wiederhergestellt wurde. Wenn der Standard jedoch nicht vorhanden ist, z. B. die Standard-VPC oder das Standard-Subnetz gelöscht wurde und keine Metadaten-Override eingegeben wurde, ist die Wiederherstellung nicht erfolgreich.

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten

DynamoDB	`deletionProtection` , wobei der Wert auf `false` gesetzt ist
	
	`encryptionType` wird auf `Default` gesetzt
	
	`targetTableName` , wobei der Wert auf einen zufälligen Wert gesetzt wird, der mit `awsbackup-restore-test-` beginnt
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` , dessen Wert auf eine zufällige Availability Zone gesetzt ist
	
	`encrypted` , dessen Wert auf `true` gesetzt ist
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	Der `disableApiTermination` -Wert ist auf `false` gesetzt
	
	Der `instanceType` -Wert ist auf den InstanceType des wiederherzustellenden Wiederherstellungspunkts gesetzt
	
	Der `requiredImdsV2` -Wert ist auf `true` gesetzt
		`iamInstanceProfileName` der Wert kann Null sein oder `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`

Amazon EFS	Der `encrypted` -Wert ist auf `true` gesetzt	`kmsKeyId`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
	Der `file-system-id` -Wert ist auf die Dateisystem-ID des wiederherzustellenden Wiederherstellungspunkts gesetzt `kmsKeyId value` wird auf `alias/aws/elasticfilesystem` gesetzt Der `newFileSystem` -Wert ist auf `true` gesetzt Der `performanceMode` -Wert ist auf `generalPurpose` gesetzt	

Amazon FSx für Lustre	`lustreConfiguration` hat verschachtelte Schlüssel. Ein verschachtelter Schlüssel ist `automaticBackupRetentionDays` , dessen Wert auf `0` gesetzt ist	`kmsKeyId`
		
		`lustreConfiguration` hat den verschachtelten Schlüssel `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds` , *für eine erfolgreiche Wiederherstellung erforderlich*

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederher stellungsmetadaten	Überschreibbare Metadaten
Amazon FSx für ONTAP NetApp	`name` ist auf einen zufällige n Wert gesetzt, der mit `awsbackup_restore_ test_` beginnt `ontapConfiguration` hat verschachtelte Schlüssel, darunter: • `junctionPath` , wobei `/name` der Name des wiederherzustellenden Volumes ist • `sizeInMegabytes` , dessen Wert auf die Größe des wiederherzustellenden Wiederherstellungspunkts in Megabyte festgelegt ist • `snapshotPolicy` , wobei der Wert auf `none` gesetzt ist	`ontapConfiguration` hat bestimmte verschachtelte Schlüssel, die überschrieben werden können, darunter: • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyE nabled` • `storageVirtualMach ineId` , *für eine erfolgreiche Wiederherstellung erforderlich* • `tieringPolicy`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten

Amazon FSx für OpenZFS	`openZfzConfiguration`, das über verschachtelte Schlüssel verfügt, darunter:
	• `automaticBackupRetentionDays` mit dem Wert auf `0`
	• `deploymentType`, wobei der Wert auf den Bereitstellungstyp des wiederherzustellenden Wiederherstellungspunkts gesetzt ist
	• `throughputCapacity`, dessen Wert auf dem `deploymentType` basiert. Wenn `deploymentType` `SINGLE_AZ_1` ist, wird der Wert auf 64 gesetzt; wenn `deploymentType` `SINGLE_AZ_2 or MULTI_AZ_1` ist, wird der Wert auf `160` gesetzt
		`kmsKeyId`
		`openZfsConfiguration` hat bestimmte verschachtelte Schlüssel, die überschrieben werden können, darunter:
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten

Amazon FSx für Windows File Server	`windowsConfiguration`, die über verschachtelte Schlüssel verfügt, darunter:
	• `automaticBackupRetentionDays` mit dem Wert auf `0`
	• `deploymentType`, wobei der Wert auf den Bereitstellungstyp des wiederherzustellenden Wiederherstellungspunkts gesetzt ist
	• `throughputCapacity` mit dem Wert auf 8
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds` *für eine erfolgreiche Wiederherstellung erforderlich*
		`windowsConfiguration`, mit bestimmten verschachtelten Schlüsseln, die überschreibbar sind
		• `throughputCapacity`
		• `activeDirectoryId` *für eine erfolgreiche Wiederherstellung erforderlich, falls nicht selfManagedActiveDirectoryConfiguration enthalten*
		• `selfManagedActiveDirectoryConfiguration` *für eine erfolgreiche Wiederherstellung activeDirectoryId erforderlich, falls nicht enthalten*
		• `preferredSubnetId`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten

Amazon-RDS-, Aurora-, Amazon-DocumentDB- und Amazon-Neptune-Cluster	`availabilityZones` , wobei der Wert auf eine Liste von bis zu drei zufälligen Availability Zones gesetzt ist
	
	`dbClusterIdentifier` mit einem zufälligen Wert, der mit `awsbackup-restore-test` beginnt
	
	`engine`, wobei der Wert auf die Engine des wiederherzustellenden Wiederherstellungspunkts gesetzt ist
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten

Amazon-RDS-Instances	`dbInstanceIdentifier` mit einem zufälligen Wert, der mit `awsbackup-restore-test-` beginnt
	
	`deletionProtection` mit dem Wert auf `false`
	
	`multiAz` mit dem Wert auf `false`
	
	`publiclyAccessible`, wobei der Wert auf „false“ gesetzt ist
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
		`vpcSecurityGroupIds`

Amazon-Simple-Storage-Service (Amazon-S3)	`destinationBucketName` mit einem zufälligen Wert, der mit `awsbackup-restore-test-` beginnt
	
	`encrypted` mit dem Wert auf `true`
	
	`encryptionType` mit dem Wert auf `SSE-S3`
	
	`newBucket` mit dem Wert auf `true`
		`encryptionType`
		
		`kmsKey`

Validierung des Wiederherstellungstests

Sie haben die Möglichkeit, eine ereignisgesteuerte Validierung zu erstellen, die ausgeführt wird, wenn ein Wiederherstellungstestauftrag abgeschlossen ist.

Erstellen Sie zunächst einen Validierungs-Workflow mit einem beliebigen von Amazon unterstützten Ziel EventBridge, z. AWS Lambda B. Fügen Sie anschließend eine EventBridge Regel hinzu, die darauf wartet, dass der Wiederherstellungsauftrag den Status `COMPLETED` erreicht. Drittens erstellen Sie einen Testplan für die Wiederherstellung (oder lassen Sie einen vorhandenen Plan wie geplant ausführen). Überwachen Sie abschließend nach Abschluss des Wiederherstellungstests die Protokolle des Validierungs-Workflows, um sicherzustellen, dass er wie erwartet ausgeführt wurde (sobald die Validierung ausgeführt wurde, wird ein Validierungsstatus in der AWS Backup Konsole angezeigt).

1. Richten Sie den Validierungs-Workflow ein

   Sie können einen Validierungsworkflow mit Lambda oder einem anderen Ziel einrichten, das von EventBridge unterstützt wird. Wenn Sie beispielsweise einen Wiederherstellungstest

validieren, der eine Amazon EC2 EC2-Instance enthält, können Sie Code hinzufügen, der einen Healthcheck-Endpunkt anpingt.

Sie können anhand der Details des Ereignisses bestimmen, welche Ressource (n) validiert werden sollen.

Sie können eine benutzerdefinierte Lambda-Schicht verwenden, um das neueste SDK zu verwenden (da `PutRestoreValidationResult` es noch nicht über das Lambda-SDK verfügbar ist).

Hier ist ein Beispiel:

```
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. Fügen Sie eine EventBridge Regel hinzu

   Erstellen Sie eine EventBridge Regel, die auf das `COMPLETED`Ereignis des Wiederherstellungsauftrags wartet.

   Optional können Sie Ereignisse nach Ressourcentyp filtern oder den ARN des Testplans wiederherstellen. Legen Sie das Ziel dieser Regel fest, um den Validierungs-Workflow aufzurufen, den Sie in Schritt 1 definiert haben. Ein Beispiel:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Lassen Sie den Testplan für die Wiederherstellung laufen und schließen Sie ihn ab

   Der Testplan für die Wiederherstellung wird gemäß dem von Ihnen konfigurierten Zeitplan ausgeführt.

   Weitere Informationen finden Sie unter Erstellen eines Testplans für die Wiederherstellung, falls Sie noch keinen haben, oder Einen Testplan für die Wiederherstellung aktualisieren, wenn Sie die Einstellungen ändern möchten.

4. Überwachen Sie die Ergebnisse

   Sobald ein Wiederherstellungstestplan wie geplant ausgeführt wurde, können Sie die Protokolle Ihres Validierungsworkflows überprüfen, um sicherzustellen, dass er ordnungsgemäß ausgeführt wurde.

   Sie können die API aufrufen, `PutRestoreValidationResult` um die Ergebnisse zu veröffentlichen, die dann in der AWS Backup Konsole und über AWS Backup API-Aufrufe angezeigt werden, in denen Wiederherstellungsaufträge beschrieben und aufgelistet werden, z. B. `DescribeRestoreJob` oder`ListRestoreJob`.

   Sobald ein Validierungsstatus festgelegt ist, kann er nicht mehr geändert werden.

Anzeigen einer Liste von Backups

Sie können eine Liste Ihrer Backups über die AWS Backup Konsole oder programmgesteuert anzeigen.

Themen

Auflisten von Backups nach geschützter Ressource in der Konsole

Gehen Sie wie folgt vor, um eine Liste der Sicherungen einer bestimmten Ressource in der AWS Backup -Konsole anzuzeigen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Wählen Sie eine geschützte Ressource in der Liste aus, um die Liste der Sicherungen anzuzeigen. Nur Ressourcen, die von gesichert wurden, AWS Backup werden unter Geschützte Ressourcen aufgeführt.

Sie können die Backups für die Ressource anzeigen. Von dieser Ansicht aus können Sie auch eine Sicherung auswählen und wiederherstellen.

Auflisten von Backups nach Backup-Tresor in der Konsole

Gehen Sie wie folgt vor, um eine Liste der in einem Sicherungstresor organisierten Sicherungen anzuzeigen.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Zeigen Sie im Abschnitt Backups (Sicherungen) die Liste aller in diesem Sicherungstresor organisierten Sicherungen an. In dieser Ansicht können Sie Backups nach beliebigen Spaltenüberschriften (einschließlich Status) sortieren und ein Backup auswählen, um es wiederherzustellen, zu bearbeiten oder zu löschen.

Programmgesteuertes Auflisten von Backups

Mithilfe der folgenden `ListRecoveryPoint`-API-Vorgänge können Sie Backups programmgesteuert auflisten:

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

Der folgende Befehl AWS Command Line Interface (AWS CLI) listet beispielsweise alle Ihre Backups mit dem `EXPIRED` Status auf:

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Sie können AWS Backup Audit Manager verwenden, um die Einhaltung Ihrer AWS Backup Richtlinien anhand der von Ihnen definierten Kontrollen zu überprüfen. Eine Kontrolle ist ein Verfahren zur Überprüfung der Einhaltung einer Backup-Anforderung, wie z. B. der Backup-Frequenz oder des Aufbewahrungszeitraums von Backups.

AWS Backup Audit Manager hilft Ihnen bei der Beantwortung von Fragen wie:

- „Sichere ich alle meine Ressourcen?“
- „Sind alle meine Backups verschlüsselt?“
- „Werden meine Backups täglich ausgeführt?“

Sie können AWS Backup Audit Manager verwenden, um Backup-Aktivitäten und Ressourcen zu finden, die den von Ihnen definierten Kontrollen noch nicht entsprechen. Beachten Sie, dass nur aktive Ressourcen berücksichtigt werden, wenn Kontrollen Ressourcen auf ihre Compliance hin überprüfen. Beispielsweise wird eine Amazon-EC2-Instance, die gerade ausgeführt wird, ausgewertet. Eine EC2-Instance, die sich im angehaltenen Zustand befindet, wird nicht in die Auswertung der Compliance einbezogen.

Sie können damit auch automatisch einen Audit-Trail mit täglichen und On-Demand-Berichten für Ihre Backup-Governance-Zwecke generieren.

Die folgenden Schritte bieten einen Überblick über die Verwendung von AWS Backup Audit Manager. Detaillierte schrittweise Anleitungen erhalten Sie, indem Sie eines der Themen am Ende dieser Seite auswählen.

1. Erstellen Sie Frameworks, die eine oder mehrere Vorlagen für Governance-Kontrollen enthalten. Die obigen Fragen sind Beispiele für drei Vorlagen für Governance-Kontrollen. Sie können die Parameter einiger Governance-Kontrollvorlagen anpassen. Sie können beispielsweise die letzte Kontrolle so anpassen, dass gefragt wird „Werden meine Backups wöchentlich ausgeführt?“, anstelle von täglich.
2. Zeigen Sie Ihr Framework an, um zu sehen, wie viele Ihrer Ressourcen mit den Kontrollen, die Sie in diesem Framework definiert haben, konform (bzw. nicht konform) sind.
3. Erstellen Sie Berichte über den Backup- und Compliance-Status. Speichern Sie diese Berichte als Nachweise Ihrer Compliance-Verfahren oder um einzelne Backup-Aktivitäten und Ressourcen zu identifizieren, die noch nicht konform sind.

AWS Backup Audit Manager generiert automatisch alle 24 Stunden einen neuen Bericht für Sie und veröffentlicht ihn in Amazon S3. Sie können auch On-Demand-Berichte generieren.

> **Note**
>
> Bevor Sie das erste Compliance-Framework erstellen, müssen Sie die Ressourcennachverfolgung aktivieren. Auf diese Weise können AWS Config Sie Ihre AWS Backup Ressourcen verfolgen. Technische Dokumentation zur Verwaltung der Ressourcenverfolgung finden Sie im AWS Config Entwicklerhandbuch unter Einrichtung AWS Config mit der Konsole.
> Wenn Sie die Ressourcennachverfolgung aktivieren, fallen Gebühren an. Informationen zu Preisen und Fakturierung von Resource Tracking für AWS Backup Audit Manager finden Sie unter Erfassung, Kosten und Abrechnung.

Themen

Arbeiten mit Audit-Frameworks

Ein Framework ist eine Sammlung von Kontrollen, mit denen Sie Ihre Backup-Praktiken auswerten können. Sie können vorgefertigte, anpassbare Kontrollen verwenden, um Ihre Richtlinien zu definieren und zu bewerten, ob Ihre Backup-Methoden mit Ihren Richtlinien konform sind. Sie können auch automatische tägliche Berichte einrichten, um entsprechend Einblick in den Compliance-Status Ihrer Frameworks zu erhalten.

Jedes Framework gilt für ein einzelnes Konto und AWS-Region. Sie können maximal 15 Frameworks pro Konto und Region bereitstellen. Sie können keine doppelten Frameworks (Frameworks, die dieselben Kontrollen und Parameter enthalten) bereitstellen.

Es gibt zwei verschiedene Arten von Frameworks:

- Das AWS Backup -Framework (empfohlen): Verwenden Sie das AWS Backup -Framework, um alle verfügbaren Kontrollen bereitzustellen, um Ihre Backup-Aktivität, den Umfang und die Ressourcen anhand der von uns empfohlenen Best Practices zu überwachen.
- Ein benutzerdefiniertes Framework, das Sie definieren: Verwenden Sie ein benutzerdefiniertes Framework, um eine oder mehrere spezifische Kontrollen auszuwählen und die Kontrollparameter anzupassen.

Themen

Auswählen Ihrer Kontrollen

In der folgenden Tabelle sind die AWS Backup Audit Manager Manager-Steuerelemente, ihre anpassbaren Parameter und ihre AWS Config Aufzeichnungsressourcentypen aufgeführt. Für jede Kontrolle ist der Aufzeichnungsressourcentyp `AWS Config: resource compliance` erforderlich, da dieser Typ Ihren Compliance-Status aufzeichnet.

Verfügbare Kontrollen

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
Backup-Ressourcen sind durch einen Backup-Plan geschützt.	Prüft, ob Ressourcen durch einen Backup-Plan geschützt sind.	None	`AWS Backup: backup selection`

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
Backup-Plan hat eine Mindestfrequenz und einen Mindestaufbewahrungszeitraum.	Prüft, ob die Backup-Frequenz mindestens [1 Tag] und der Aufbewahrungszeitraum mindestens [35 Tage] beträgt.	Backup-Frequenz; Aufbewahrungszeitraum	`AWS Backup: backup plans`
Tresore verhindern das manuelle Löschen von Wiederherstellungspunkten.	Prüft, ob Backup-Tresore das manuelle Löschen von Wiederherstellungspunkten nur bei bestimmten AWS Identity and Access Management (IAM-) Rollen zulassen. Standardmäßig bestehen keine Ausnahmen für IAM-Rollen. Es gibt auch keine Ausnahmen für IAM-Rollen, wenn Sie dieses Steuerelement mit dem Framework bereitstellen. AWS Backup	Bis zu 5 IAM-Rollen, die das manuelle Löschen von Wiederherstellungspunkten ermöglichen	`AWS Backup: backup vaults`
Wiederherstellungspunkte sind verschlüsselt.	Prüft, ob die Wiederherstellungspunkte verschlüsselt sind.	None	`AWS Backup: recovery points`

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
Mindestaufbewahrungszeitraum ist für den Wiederherstellungspunkt festgelegt.	Prüft, ob der Aufbewahrungszeitraum für Wiederherstellungspunkte mindestens [35 Tage] beträgt.	Aufbewahrungszeitraum für Wiederherstellungspunkte	`AWS Backup: recovery points`
Regionsübergreifende Backup-Kopie ist geplant.	Prüft, ob eine Ressource so konfiguriert ist, dass Kopien ihrer Backups in einer anderen AWS-Region erstellt werden.	AWS-Region	`AWS Backup: backup selection`
Kontenübergreifende Backup-Kopie ist geplant.	Prüft, ob für eine Ressource eine kontenübergreifende Backup-Kopie konfiguriert ist.	AWS Konto-ID	`AWS Backup: backup selection`
Backups werden durch AWS Backup Vault Lock geschützt	Prüft, ob eine Ressource so konfiguriert ist, dass Backups in einem gesperrten Backup-Tresor gespeichert werden.	Min. Anzahl an Aufbewahrungstagen; max. Anzahl an Aufbewahrungstagen	`AWS Backup: backup selection`

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
Letzter Wiederherstellungspunkt wurde erstellt.	Prüft, ob innerhalb eines angegebenen Zeitraums ein Wiederherstellungspunkt erstellt wurde.	Wert in Stunden [1 bis 744] oder Tagen [1 bis 31]	`AWS Backup recovery points`
Wiederherstellungszeit für Ressourcen entspricht dem Ziel	Prüft, ob der Wiederherstellungstestauftrag innerhalb der Zielwiederherstellungszeit abgeschlossen wurde	Wert in Minuten	None

Detaillierte Informationen zu diesen Kontrollen finden Sie unter Steuerelemente und Abhilfemaßnahmen.

Eine Liste der AWS Backup unterstützten Ressourcen, die nicht alle Kontrollen unterstützen, finden Sie im Abschnitt AWS Backup Audit Manager der Verfügbarkeit von Features nach Ressource Tabelle.

> **Note**
>
> Wenn Sie keine der oben genannten Kontrollen verwenden möchten, können Sie AWS Backup Audit Manager trotzdem verwenden, um tägliche Berichte über Ihre Sicherungs-, Kopier- und Wiederherstellungsaufträge zu erstellen. Weitere Informationen finden Sie unter Arbeiten mit Auditberichten.

Aktivieren der Ressourcennachverfolgung

Bevor Sie das erste Compliance-Framework erstellen, müssen Sie die Ressourcennachverfolgung aktivieren. Auf diese Weise können AWS Config Sie Ihre AWS Backup Ressourcen verfolgen.

Technische Dokumentation zur Verwaltung der Ressourcenverfolgung finden Sie im AWS Config Entwicklerhandbuch unter Einrichtung AWS Config mit der Konsole.

Wenn Sie die Ressourcennachverfolgung aktivieren, fallen Gebühren an. Informationen zu Preisen und Fakturierung von Resource Tracking für AWS Backup Audit Manager finden Sie unter Erfassung, Kosten und Abrechnung.

Themen

- Aktivieren der Ressourcennachverfolgung mithilfe der Konsole
- Aktivieren der Ressourcennachverfolgung mit der AWS Command Line Interface (AWS CLI)
- Aktivieren der Ressourcennachverfolgung mithilfe einer AWS CloudFormation -Vorlage

Aktivieren der Ressourcennachverfolgung mithilfe der Konsole

So aktivieren Sie die Ressourcennachverfolgung über die Konsole

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich unter Audit Manager die Option Frameworks aus.
3. Aktivieren Sie die Ressourcennachverfolgung, indem Sie Ressourcennachverfolgung verwalten auswählen.
4. Wählen Sie Gehe zu AWS Config Einstellungen.
5. Wählen Sie Aufzeichnung aktivieren oder deaktivieren aus.
6. Wählen Sie Aufzeichnung aktivieren für alle der folgenden Ressourcentypen aus oder aktivieren Sie die Aufzeichnung für einige Ressourcentypen. Informationen darüber, welche Ressourcentypen für Ihre Kontrollen erforderlich sind, finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe.

    - `AWS Backup: backup plans`
    - `AWS Backup: backup vaults`
    - `AWS Backup: recovery points`
    - `AWS Backup: backup selection`

> **Note**
>
> AWS Backup Audit Manager benötigt `AWS Config: resource compliance` für jede Kontrolle.

7. Klicken Sie auf Schließen.
8. Warten Sie, bis aus dem blauen Banner mit dem Text Ressourcennachverfolgung wird aktiviert ein grüner Banner mit dem Text Ressourcennachverfolgung ist aktiviert wird.

Sie können an zwei Stellen in der AWS Backup Konsole überprüfen, ob Sie die Ressourcenverfolgung aktiviert haben und wenn ja, welche Ressourcentypen Sie aufzeichnen. Führen Sie im linken Navigationsbereich einen der folgenden Schritte aus:

- Wählen Sie Frameworks und dann den Text unter AWS Config -Recorder-Status aus.
- Wählen Sie Einstellungen und dann den Text unter AWS Config -Recorder-Status aus.

Aktivieren der Ressourcennachverfolgung mit der AWS Command Line Interface (AWS CLI)

Wenn Sie sich noch nicht angemeldet haben AWS Config, ist es möglicherweise schneller, das Onboarding mit dem durchzuführen. AWS CLI

So aktivieren Sie die Ressourcennachverfolgung mithilfe der AWS CLI

1. Geben Sie den folgenden Befehl ein, um festzustellen, ob Sie den AWS Config -Recorder bereits aktiviert haben.

```
$ aws configservice describe-configuration-recorders
```

   a. Überprüfen Sie, ob Ihre `ConfigurationRecorders`-Liste wie hier leer ist:

```
{
  "ConfigurationRecorders": []
}
```

In diesem Fall ist der Recorder nicht aktiviert. Fahren Sie mit Schritt 2 fort, um Ihren Recorder zu erstellen.

b. Wenn Sie die Aufzeichnung bereits für alle Ressourcen aktiviert haben, sieht die `ConfigurationRecorders`-Ausgabe wie folgt aus:

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

Da Sie alle Ressourcen aktiviert haben, haben Sie die Ressourcennachverfolgung bereits aktiviert. Sie müssen den Rest dieses Verfahrens nicht abschließen, um AWS Backup Audit Manager zu verwenden.

c. Wenn Ihre `ConfigurationRecorders`-Liste nicht leer ist, Sie aber die Aufzeichnung nicht für alle Ressourcen aktiviert haben, fügen Sie dem vorhandenen Recorder mithilfe des folgenden Befehls Backup-Ressourcen hinzu. Fahren Sie mit Schritt 3 fort.

```
$ 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. Erstellen Sie einen AWS Config Rekorder mit den AWS Backup Audit Manager Manager-Ressourcentypen

```
$ 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. Beschreiben Sie Ihren AWS Config Rekorder.

```
$ aws configservice describe-configuration-recorders
```

Stellen Sie sicher, dass es über die AWS Backup Audit Manager Manager-Ressourcentypen verfügt, indem Sie Ihre Ausgabe mit der folgenden erwarteten Ausgabe vergleichen.

```
{
  "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. Erstellen Sie einen Amazon S3 S3-Bucket als Ziel zum Speichern der AWS Config Konfigurationsdateien.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Verwenden Sie *policy.json*, um die AWS Config Erlaubnis für den Zugriff auf Ihren Bucket zu erteilen. Sehen Sie sich das folgende *policy.json*-Beispiel an.

```
$ 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. Konfigurieren Sie Ihren Bucket als Lieferkanal AWS Config

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Aktivieren Sie die AWS Config Aufnahme

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Stellen Sie sicher, dass `"FrameworkStatus":"ACTIVE"` in der letzten Zeile Ihrer `DescribeFramework`-Ausgabe wie folgt aussieht.

```
$ 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"
}
```

Aktivieren der Ressourcennachverfolgung mithilfe einer AWS CloudFormation -Vorlage

Eine AWS CloudFormation Vorlage, die die Ressourcenverfolgung aktiviert, finden Sie unter AWS Backup Audit Manager verwenden mit AWS CloudFormation.

Erstellen von Frameworks mithilfe der AWS Backup -Konsole

Nachdem Sie die Ressourcennachverfolgung aktiviert haben, erstellen Sie mithilfe der folgenden Schritte ein Framework.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Frameworks aus.
3. Wählen Sie Framework erstellen aus.
4. Geben Sie unter Name des Frameworks einen eindeutigen Namen ein. Der Framework-Name muss eine Länge von maximal 256 Zeichen haben, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstrichen (_) bestehen.
5. (Optional) Geben Sie eine Beschreibung des Frameworks ein.
6. In Steuerelemente werden Ihre aktiven Kontrollen angezeigt. Standardmäßig werden alle Kontrollen aufgeführt, die für eine Ressource in Frage kommen.

   Um zu ändern, welche Kontrollen aktiv sind, klicken Sie auf Steuerelemente bearbeiten.

   a. Das erste Kontrollkästchen gibt an, ob die Kontrolle aktiviert ist. Um eine Kontrolle auszuschalten, deaktivieren Sie das Kontrollkästchen.

   b. Unter Auszuwertende Ressourcen auswählen können Sie festlegen, wie Ressourcen ausgewählt werden sollen, entweder nach Typ, nach Tags oder nach einzelner Ressource.

   In der Liste der Kontrollen in AWS Backup Audit Manager werden die Anpassungsoptionen für jede Kontrolle beschrieben.

7. (Optional) Markieren Sie Ihr Framework, indem Sie Neues Tag hinzufügen auswählen. Mithilfe von Tags können Sie Ihre Frameworks suchen und filtern oder Ihre Kosten nachverfolgen.
8. Wählen Sie Framework erstellen aus.

AWS Backup Die Erstellung des Frameworks durch Audit Manager kann mehrere Minuten in Anspruch nehmen.

Wenn der Fehler `AlreadyExists` auftritt, ist bereits ein Framework mit denselben Kontrollen und Parametern vorhanden. Um erfolgreich ein neues Framework zu erstellen, muss sich mindestens eine Kontrolle oder ein Parameter von bestehenden Frameworks unterscheiden.

Frameworks mithilfe der AWS Backup API erstellen

Die folgende Tabelle enthält CreateFramework-API-Beispielanfragen für jede Kontrolle sowie API-Beispielantworten auf die entsprechenden DescribeFramework-Anfragen. Um programmgesteuert mit AWS Backup Audit Manager zu arbeiten, können Sie auf diese Codefragmente zurückgreifen.

Kontrolle	**`CreateFramework`** -Anfrage	**`DescribeFramework`** -Antwort
`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 }`	`{"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":[],`

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
	`} ], "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }`	`"ControlScope": {"Complia nceResourceTypes": ["RDS"] } } ], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }`

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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": {

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
	"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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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":

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
		<pre> {"key1": "foo"} }</pre>

Backup recovery points are encrypted	<pre>{"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"}
	}</pre>
		<pre>{"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"}
		}</pre>

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** -Antwort
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"} }

Kontrolle	**CreateFramework** -Anfrage	**DescribeFramework** - Antwort
	}	

Anzeigen des Framework-Compliance-Status

Sobald Sie ein Audit-Framework erstellt haben, wird es in der Tabelle Frameworks angezeigt. Sie können diese Tabelle anzeigen, indem Sie im linken Navigationsbereich der AWS Backup Konsole Frameworks auswählen. Um die Audit-Ergebnisse für das Framework anzuzeigen, wählen Sie den entsprechenden Namen unter Namen des Frameworks aus. Dadurch gelangen Sie zur Seite mit den Framework-Details, die aus zwei Abschnitten besteht: Zusammenfassung und Steuerelemente.

Im Abschnitt Zusammenfassung werden die folgenden Status von links nach rechts aufgeführt:

- Der Compliance-Status ist der allgemeine Compliance-Status Ihres Audit-Frameworks, der durch den Compliance-Status der einzelnen Kontrollen bestimmt wird. Der Compliance-Status jeder Kontrolle wird vom Compliance-Status jeder Ressource bestimmt, die sie auswertet.

  Der Status der Framework-Compliance ist nur `Compliant`, wenn alle Ressourcen im Umfang Ihrer Kontrollauswertungen diese Prüfungen bestanden haben. Wenn eine oder mehrere Ressourcen eine Kontrollauswertung nicht bestanden haben, ist der Compliance-Status `Non-Compliant`. Informationen darüber, wie Sie nicht konforme Ressourcen finden, erhalten Sie unter Auffinden nicht konformer Ressourcen. Informationen darüber, wie Sie die Compliance Ihrer Ressourcen sicherstellen, finden Sie im Abschnitt zum Thema Abhilfe im Artikel AWS Backup Audit Manager – Kontrollen und Abhilfe.
- Framework-Status bezieht sich darauf, ob Sie die Ressourcennachverfolgung für all Ihre Ressourcen aktiviert haben. Die folgenden Status sind möglich:
  - `Active`, wenn die Aufzeichnung für alle Ressourcen, die das Framework auswertet, aktiviert ist.
  - `Partially active`, wenn die Aufzeichnung für mindestens eine Ressource, die das Framework auswertet, deaktiviert ist.
  - `Inactive`, wenn die Aufzeichnung für alle Ressourcen, die das Framework auswertet, deaktiviert ist.
  - `Unavailable`wenn AWS Backup Audit Manager derzeit nicht in der Lage ist, den Aufzeichnungsstatus zu überprüfen.

So korrigieren Sie einen **`Inactive`**- oder **`Partially active`**-Status

1. Wählen Sie im linken Navigationsbereich die Option Frameworks aus.
2. Wählen Sie Ressourcennachverfolgung verwalten aus.
3. Folgen Sie den Anweisungen im Pop-up, um Aufzeichnungen, die zuvor für Ihre Ressourcentypen nicht aktiviert waren, zu aktivieren.

Weitere Informationen darüber, für welche Ressourcentypen eine Ressourcennachverfolgung auf Grundlage der Kontrollen erforderlich ist, die Sie in Ihre Frameworks integriert haben, finden Sie in den Informationen zu Ressourcen in AWS Backup Audit Manager – Kontrollen und Abhilfe.

- Der Bereitstellungsstatus bezieht sich auf den Bereitstellungsstatus des Frameworks. Dieser Status sollte in den meisten Fällen `Completed` sein, kann aber auch `Create in progress`, `Update in progress`, `Delete in progress` oder `Failed` sein.
  - Der Status `Failed` bedeutet, dass das Framework nicht ordnungsgemäß bereitgestellt wurde. Löschen Sie das Framework und erstellen Sie es anschließend über die AWS Backup -Konsole oder über die AWS Backup -API neu.
- Konforme Steuerelemente zeigt die Anzahl der Framework-Kontrollen an, bei denen alle Auswertungen bestanden wurden.
- Nicht konforme Steuerelemente zeigt eine Anzahl an Framework-Kontrollen an, bei denen mindestens eine Auswertung nicht bestanden wurde.

Der Abschnitt Steuerelemente stellt die folgenden Informationen bereit:

- Kontrollstatus bezieht sich auf den Compliance-Status der einzelnen Kontrollen. Eine Kontrolle kann folgende Status aufweisen: `Compliant`, was bedeutet, dass alle Ressourcen diese Auswertung bestehen; `Non-compliant`, was bedeutet, dass mindestens eine Ressource diese Auswertung nicht bestanden hat, oder `Insufficient data`, was bedeutet, dass die Kontrolle keine Ressourcen innerhalb des Auswertungsbereichs gefunden hat, die ausgewertet werden könnten.
- Auswertungsbereich beschränkt möglicherweise jede Kontrolle auf einen oder mehrere Ressourcentypen, eine Ressourcen-ID oder einen Tag-Schlüssel und Tag-Wert, je nachdem, wie Sie die Kontrolle bei der Erstellung des Audit-Frameworks angepasst haben. Wenn alle Felder leer sind (dargestellt durch einen Bindestrich: „-“), wertet die Kontrolle alle zutreffenden Ressourcen aus.

Suchen nicht konformer Ressourcen

AWS Backup Audit Manager hilft Ihnen auf zweierlei Weise dabei, herauszufinden, welche Ressourcen nicht konform sind.

- Wählen Sie, wenn Sie den Compliance-Status des Frameworks anzeigen, im Abschnitt Details den Namen der Kontrolle aus. Dadurch gelangen Sie zur AWS Config Konsole, in der Sie eine Liste Ihrer `Non-Compliant` Ressourcen einsehen können.
- Nachdem Sie einen Berichtsplan mit der Ressourcen-Compliance-Vorlage erstellt haben, der Ihr Framework enthält, können Sie Ihren Bericht anzeigen, um alle Ihre `Non-Compliant`-Ressourcen für alle Ihre Kontrollen zu identifizieren.

  Außerdem zeigt Ihnen `Resource compliance report` an, wann AWS Backup Audit Manager Ihre Kontrollen zum letzten Mal ausgewertet hat.

Aktualisieren von Audit-Frameworks

Sie können die Beschreibung, die Kontrollen und Parameter eines vorhandenen Audit-Frameworks aktualisieren.

So aktualisieren Sie ein vorhandenes Framework

1. Wählen Sie im linken Navigationsbereich der AWS Backup Konsole Frameworks aus.
2. Wählen Sie unter Name des Frameworks das Framework aus, das Sie bearbeiten möchten.
3. Wählen Sie Bearbeiten aus.

Löschen von Audit-Frameworks

So löschen Sie ein vorhandenes Framework

1. Wählen Sie im linken Navigationsbereich der AWS Backup Konsole Frameworks aus.
2. Wählen Sie unter Name des Frameworks das Framework aus, das Sie löschen möchten.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen Ihres Frameworks ein und wählen Sie Framework löschen aus.

Arbeiten mit Auditberichten

AWS Backup Audit Manager Manager-Berichte sind automatisch generierte Belege für Ihre AWS Backup Aktivitäten, z. B.:

- welche Backup-Jobs abgeschlossen wurden und wann
- welche Ressourcen Sie gesichert haben

Es gibt zwei Arten von Berichten. Wenn Sie einen Bericht erstellen, können Sie auswählen, welcher Typ erstellt werden soll.

Ein Typ ist ein Auftragsbericht, in dem die in den letzten 24 Stunden abgeschlossenen Aufträge und alle aktiven Aufträge angezeigt werden. Auftragsberichte zeigen nicht den Status `completed with issues` an. Um diesen Status zu finden, können Sie nach `Completed` Jobs mit einer oder mehreren Statusmeldungen filtern. AWS Backup nimmt nur dann eine Statusmeldung als Teil des `Completed` Auftragsstatus auf, wenn die Nachricht Aufmerksamkeit oder Maßnahmen erfordert.

Die zweite Art von Bericht ist ein Compliance-Bericht. Mit Compliance-Berichten können die Ressourcenebenen oder die verschiedenen gültigen Kontrollen überwacht werden.

AWS Backup Audit Manager übermittelt täglich einen Bericht in Ihren Amazon S3 S3-Bucket. Wenn sich der Bericht auf die aktuelle Region und das aktuelle Konto bezieht, können Sie wählen, ob Sie den Bericht im CSV- oder im JSON-Format erhalten möchten. Andernfalls steht der Bericht im CSV-Format zur Verfügung. Der Zeitpunkt des täglichen Berichts kann über mehrere Stunden schwanken, da AWS Backup Audit Manager eine Randomisierung durchführt, um seine Leistung aufrechtzuerhalten. Sie können auch jederzeit einen On-Demand-Bericht ausführen.

Alle Kontoinhaber können regionsübergreifende Berichte erstellen. Inhaber von Verwaltungskonten und Konten delegierter Administratoren können ebenfalls kontenübergreifende Berichte erstellen.

Sie können jeweils maximal 20 Berichtspläne haben. AWS-Konto

> **Note**
>
> Ressourcen wie RDS, die nicht in der Lage sind, inkrementelle Bytes an Daten eines bestimmten Backups anzuzeigen, zeigen für den Wert `backupSizeInBytes` 0 an.

Damit AWS Backup Audit Manager Tages- oder On-Demand-Berichte erstellen kann, müssen Sie zunächst einen Berichtsplan anhand einer Berichtsvorlage erstellen.

Themen

Auswählen Ihrer Berichtsvorlage

In einer Berichtsvorlage werden die Informationen definiert, die Ihr Berichtsplan in Ihrem Bericht einschließt. Wenn Sie Ihre Berichte mithilfe eines Berichtsplans automatisieren, stellt Ihnen AWS Backup Audit Manager Berichte für die letzten 24 Stunden zur Verfügung. AWS Backup Audit Manager erstellt diese Berichte zwischen 1 und 5 Uhr UTC. Folgende Berichtsvorlagen werden bereitgestellt:

Vorlagen für Backup-Berichte

Vorlagen für Backup-Berichte liefern Ihnen tägliche Updates über Ihre Backup-, Wiederherstellungs- oder Kopieraufträge. Sie können diese Berichte verwenden, um Ihre operative Situation zu überwachen und Fehler zu identifizieren, bei denen möglicherweise weitere Maßnahmen erforderlich sind. In der folgenden Tabelle finden Sie alle Namen von Backup-Berichtsvorlagen zusammen mit einer jeweiligen Beispielausgabe.

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
`BACKUP_JOB_REPORT`	`{ "reportItems": [ { "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566",`

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format


```
      "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-2:1122334455
66:backup-plan:349f2247-b48
9-4301-83ac-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-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format

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"
	    }

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
	<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>

Vorlagen für Compliance-Berichte

Vorlagen für Compliance-Berichte liefern Ihnen täglich Berichte über die Compliance Ihrer Backup-Aktivitäten und -Ressourcen anhand der von Ihnen in einem oder mehreren Frameworks definierten Kontrollen. Wenn der Compliance-Status eines Ihrer Frameworks `Non-compliant` ist, überprüfen Sie einen Compliance-Bericht, um die nicht konformen Ressourcen zu bestimmen.

Arten von Vorlagen für Compliance-Berichte

- `Control compliance report` hilft Ihnen dabei, den Compliance-Status der Kontrollen nachzuverfolgen, die Sie in Ihren Frameworks definiert haben.
- `Resource compliance report` hilft Ihnen dabei, den Compliance-Status Ihrer Ressourcen anhand der Kontrollen nachzuverfolgen, die Sie in Ihren Frameworks definiert haben. Diese Berichte enthalten detaillierte Auswertungsergebnisse, einschließlich Informationen zu nicht konformen Ressourcen, anhand derer Sie diese Ressourcen identifizieren und korrigieren können.

Die folgende Tabelle zeigt eine Beispielausgabe aus einem Compliance-Bericht.

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format
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",

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format


```
      "frameworkDescription": "A test
 framework",
      "controlName": "BACKUP_P
LAN_MIN_FREQUENCY_AND_MIN_R
ETENTION_CHECK",
      "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
\"}"
    }
  ]
}
```

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format

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"
	    }
	  ]
	}

Erstellen von Berichtsplänen mithilfe der AWS Backup -Konsole

Es gibt zwei Arten von Berichten. Ein Typ ist ein Auftragsbericht, in dem die in den letzten 24 Stunden abgeschlossenen Aufträge und alle aktiven Aufträge angezeigt werden. Die zweite Art von Bericht ist ein Compliance-Bericht. Mit Compliance-Berichten können die Ressourcenebenen oder die verschiedenen gültigen Kontrollen überwacht werden. Wenn Sie einen Bericht erstellen, können Sie auswählen, welcher Berichtstyp erstellt werden soll.

HINWEIS: Je nach Kontotyp kann die Anzeige der Konsole variieren. Die Funktion für mehrere Konten ist nur für Verwaltungskonten verfügbar.

Ähnlich wie bei einem Backup-Plan erstellen Sie einen Berichtsplan, um die Erstellung Ihrer Berichte zu automatisieren und deren Amazon-S3-Ziel-Bucket zu definieren. Ein Berichtsplan setzt voraus, dass Sie über einen S3-Bucket verfügen, um Berichte zu empfangen. Anweisungen zur Einrichtung eines neuen S3-Buckets finden Sie unter Schritt 1: Erstellen des ersten S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Um Ihren Berichtsplan in der AWS Backup Konsole zu erstellen

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie Berichtsplan erstellen aus.
4. Wählen Sie in der Dropdown-Liste eine der Berichtsvorlagen aus.
5. Geben Sie unter Name des Berichtsplans einen eindeutigen Namen ein. Der Name muss eine Länge von maximal 256 Zeichen haben, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.
6. (Optional) Geben Sie eine Beschreibung des Berichtsplans ein.
7. Vorlagen für Compliance-Berichte für nur ein Konto. Wählen Sie ein oder mehrere Frameworks aus, über die berichtet werden soll. Sie können einem Berichtsplan maximal 1 000 Frameworks hinzufügen.

    1. Wählen Sie mithilfe AWS der Dropdownliste Ihre Region aus.
    2. Wählen Sie in der Dropdown-Liste ein Framework aus dieser Region aus.
    3. Wählen Sie Framework hinzufügen aus.
8. (Optional) Um Ihrem Berichtsplan Tags hinzuzufügen, wählen Sie Tags zum Berichtsplan hinzufügen aus.

9. Wenn Sie ein Verwaltungskonto verwenden, können Sie angeben, welche Konten Sie in diesen Berichtsplan aufnehmen möchten. Sie können Nur mein Konto auswählen, wodurch Berichte nur für das Konto generiert werden, bei dem Sie derzeit angemeldet sind. Sie können auch ein oder mehrere Konten in meiner Organisation auswählen (verfügbar für Verwaltungs- und delegierte Administratorkonten).
10. (Überspringen Sie diesen Schritt, wenn Sie einen Compliance-Bericht nur für eine Region erstellen). Sie können auswählen, welche Regionen in den Bericht aufgenommen werden sollen. Klicken Sie auf das Dropdown-Menü, um die für Sie verfügbaren Regionen anzuzeigen. Wählen Sie Alle verfügbaren Regionen oder die Regionen aus, die Sie bevorzugen.

    - Wenn Sie das Kontrollkästchen Neue Regionen einschließen, wenn sie in Backup Audit Manager integriert sind aktivieren, werden neue Regionen in Ihre Berichte aufgenommen, sobald sie verfügbar sind.
11. Wählen Sie das Dateiformat Ihres Berichts aus. Alle Berichte können im CSV-Format exportiert werden. Darüber hinaus können Berichte für eine einzelne Region und eine einzelne Region im JSON-Format exportiert werden.
12. Wählen Sie in der Dropdown-Liste Ihren S3-Bucket-Namen aus.
13. (Optional) Geben Sie ein Bucket-Präfix ein.

    AWS Backup übermittelt Ihr Girokonto und Ihre aktuellen Regionsberichte an`s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name`.

    AWS Backup übermittelt Ihre kontenübergreifenden Berichte an `s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name`

    AWS Backup übermittelt Ihre regionsübergreifenden Berichte an `s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name`
14. Wählen Sie Berichtsplan erstellen aus.

Als Nächstes müssen Sie zulassen, dass Ihr S3-Bucket Berichte von AWS Backup empfängt. Nachdem Sie einen Berichtsplan erstellt haben, generiert AWS Backup Audit Manager automatisch eine S3-Bucket-Zugriffsrichtlinie, die Sie anwenden können.

Wenn Sie Ihren Bucket mit einem benutzerdefinierten KMS-Schlüssel verschlüsseln, muss die KMS-Schlüsselrichtlinie die folgenden Anforderungen erfüllen:

- Das `Principal` Attribut muss den `AWSServiceRolePolicyForBackupReports`ARN für die mit dem Service verknüpfte Rolle von Backup Audit Manager enthalten.

- Das `Action` Attribut muss `kms:Decrypt` mindestens Folgendes enthaltenkms:GenerateDataKey:

Die Richtlinie AWSServiceRolePolicyForBackupReportsverfügt über diese Berechtigungen.

So zeigen Sie diese Zugriffsrichtlinie an und wenden sie auf Ihren S3-Bucket an

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie unter Name des Berichtsplans einen Berichtsplan aus, indem Sie dessen Namen auswählen.
4. Wählen Sie Bearbeiten aus.
5. Wählen Sie Zugriffsrichtlinie für S3-Bucket anzeigen aus. Sie können die Richtlinie auch am Ende dieses Verfahrens verwenden.
6. Wählen Sie Berechtigungen kopieren aus.
7. Wählen Sie Bucket-Richtlinie bearbeiten aus. Beachten Sie, dass die serviceverknüpfte Rolle, auf die in der S3-Bucket-Richtlinie verwiesen wird, noch nicht existiert, bis der Backup-Bericht zum ersten Mal erstellt wird. Dies führt zu dem Fehler „Ungültiger Prinzipal“.
8. Kopieren Sie die Berechtigungen in die Richtlinie.

Bucket-Beispielrichtlinie

```
{
  "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"
        }
      }
    }
  ]
}
```

Wenn Sie Ihren Ziel-S3-Bucket AWS Key Management Service , in dem die Berichte gespeichert werden, mit einem benutzerdefinierten Code verschlüsseln, nehmen Sie die folgenden Aktionen in Ihre Richtlinie auf:

```
      "Action":[
        "kms:GenerateDataKey",
        "kms:Encrypt"
      ],
      "Resource":[
        "*"
      ],
```

Berichtspläne mithilfe der AWS Backup API erstellen

Sie können auch programmgesteuert mit Berichtsplänen arbeiten.

Es gibt zwei Arten von Berichten. Ein Typ ist ein Auftragsbericht, in dem die in den letzten 24 Stunden abgeschlossenen Aufträge und alle aktiven Aufträge angezeigt werden. Die zweite Art von Bericht ist ein Compliance-Bericht. Mit Compliance-Berichten können die Ressourcenebenen oder die verschiedenen gültigen Kontrollen überwacht werden. Wenn Sie einen Bericht erstellen, können Sie auswählen, welcher Berichtstyp erstellt werden soll.

Ähnlich wie bei einem Backup-Plan erstellen Sie einen Berichtsplan, um die Erstellung Ihrer Berichte zu automatisieren und deren Amazon-S3-Ziel-Bucket zu definieren. Ein Berichtsplan setzt voraus, dass Sie über einen S3-Bucket verfügen, um Berichte zu empfangen. Anweisungen zur Einrichtung eines neuen S3-Buckets finden Sie unter Schritt 1: Erstellen des ersten S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Wenn Sie Ihren Bucket mit einem benutzerdefinierten KMS-Schlüssel verschlüsseln, muss die KMS-Schlüsselrichtlinie die folgenden Anforderungen erfüllen:

- Das `Principal` Attribut muss den `AWSServiceRolePolicyForBackupReports`ARN für die mit dem Service verknüpfte Rolle von Backup Audit Manager enthalten.

- Das `Action` Attribut muss `kms:Decrypt` mindestens Folgendes enthaltenkms:GenerateDataKey:

Die Richtlinie AWSServiceRolePolicyForBackupReportsverfügt über diese Berechtigungen.

Verwenden Sie für Berichte mit einem einzigen Konto und einer Region die folgende Syntax, um CreateReportPlan aufzurufen.

```
{
   "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"
}
```

Wenn Sie DescribeReportPlan mit dem eindeutigen Namen eines Berichtsplans aufrufen, antwortet die AWS Backup -API mit den folgenden Informationen.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
```

```
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

Verwenden Sie für Berichte mit mehreren Konten und mehreren Regionen die folgende Syntax, um CreateReportPlan aufzurufen.

```
{
   "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"
   }
}
```

Wenn Sie DescribeReportPlan mit dem eindeutigen Namen eines Berichtsplans aufrufen, antwortet die AWS Backup -API mit den folgenden Informationen für Pläne mit mehreren Konten und mehreren Regionen:

```
{
   "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"
      }
   }
}
```

Erstellen von On-Demand-Berichten

Sie können nach Belieben neue Berichte erstellen, indem Sie mit den folgenden Schritten einen On-Demand-Bericht erstellen. AWS Backup Audit Manager übermittelt Ihren On-Demand-Bericht an den Amazon S3 S3-Bucket, den Sie in Ihrem Berichtsplan angegeben haben.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie unter Name des Berichtsplans einen Berichtsplan aus, indem Sie dessen Namen auswählen.
4. Wählen Sie On-Demand-Bericht erstellen aus.

Sie können einen On-Demand-Bericht für einen vorhandenen Berichtsplan generieren.

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.

3. Wählen Sie unter Berichtspläne einen Berichtsplan aus, indem Sie auf das Optionsfeld neben dem Namen des Berichtsplans klicken.
4. Klicken Sie auf Aktionen und dann auf On-Demand-Bericht erstellen.

Sie können dies für mehrere Berichte ausführen, auch während Berichte generiert werden.

Anzeigen von Auditberichten

Sie können AWS Backup Audit Manager Manager-Berichte mit den Programmen öffnen, anzeigen und analysieren, die Sie normalerweise für die Arbeit mit CSV- oder JSON-Dateien verwenden. Beachten Sie, dass Berichte für mehrere Regionen oder mehrere Konten nur im CSV-Format verfügbar sind.

Große Dateien werden in mehrere Berichte aufgeteilt, wenn die Gesamtdateigröße 50 MB überschreitet. Wenn die resultierenden Dateien mehr als 50 MB groß sind, erstellt AWS Backup Audit Manager zusätzliche CSV-Dateien mit dem Rest des Berichts.

So zeigen Sie einen Bericht an

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie unter Name des Berichtsplans einen Berichtsplan aus, indem Sie dessen Namen auswählen.
4. Klicken Sie unter Aufträge melden auf den Berichtslink, um den Bericht anzuzeigen.
5. Wenn der Berichtstatus Ihres Berichts eine gepunktete Unterstreichung zeigt, wählen Sie ihn aus, um Informationen zu Ihrem Bericht zu erhalten.
6. Wählen Sie anhand der Abschlusszeit aus, welcher Bericht angezeigt werden soll.
7. Wählen Sie den S3-Link aus. Dadurch wird Ihr S3-Ziel-Bucket geöffnet.
8. Wählen Sie unter Name den Namen des Berichts aus, den Sie anzeigen möchten.
9. Um den Bericht auf Ihrem Computer zu speichern, wählen Sie Herunterladen aus.

Aktualisieren von Berichtsplänen

Sie können die Beschreibung, das Bereitstellungsziel und das Format eines vorhandenen Berichtsplans aktualisieren. Falls zutreffend, können Sie auch Frameworks dem Berichtsplan hinzufügen oder sie daraus entfernen.

So aktualisieren Sie einen vorhandenen Berichtsplan

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie unter Name des Berichtsplans einen Berichtsplan aus, indem Sie dessen Namen auswählen.
4. Wählen Sie Bearbeiten aus.
5. Sie können die Details des Berichtsplans bearbeiten, einschließlich des Berichtsnamens und der Beschreibung sowie welche Konten und Regionen im Bericht enthalten sind.

Löschen von Berichtsplänen

Sie können einen vorhandenen Berichtsplan löschen. Wenn Sie einen Berichtsplan löschen, verbleiben alle Berichte, die bereits von diesem Berichtsplan erstellt wurden, in ihrem Amazon-S3-Ziel-Bucket.

So löschen Sie einen vorhandenen Berichtsplan

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich Berichte aus.
3. Wählen Sie unter Name des Berichtsplans einen Berichtsplan aus, indem Sie dessen Namen auswählen.
4. Wählen Sie Löschen aus.
5. Geben Sie den Namen des Berichtsplans ein und wählen Sie dann Berichtsplan löschen aus.

Verwenden von AWS Backup Audit Manager mit AWS CloudFormation

Wir stellen Ihnen die folgenden AWS CloudFormation Beispielvorlagen als Referenz zur Verfügung:

Themen

- Aktivieren der Ressourcennachverfolgung
- Bereitstellen von Standardkontrollen
- Ausschließen von IAM-Rollen aus der Kontrollauswertung

- Erstellen eines Berichtsplans

Aktivieren der Ressourcennachverfolgung

Mit der folgenden Vorlage wird die Ressourcennachverfolgung aktiviert, wie in Aktivieren der Ressourcennachverfolgung beschrieben.

```
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
```

Bereitstellen von Standardkontrollen

Die folgende Vorlage erstellt ein Framework mit den in AWS Backup Audit Manager – Kontrollen und Abhilfe beschriebenen Standardkontrollen.

```
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
```

Ausschließen von IAM-Rollen aus der Kontrollauswertung

Mit der Kontrolle BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED können bis zu fünf IAM-Rollen ausgenommen werden, die Wiederherstellungspunkte dennoch manuell löschen können. Die folgende Vorlage stellt diese Kontrolle bereit und schließt außerdem zwei IAM-Rollen aus.

```
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
```

Erstellen eines Berichtsplans

Die folgende Vorlage erstellt einen Berichtsplan.

```
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
```

Verwenden von AWS Backup Audit Manager mit AWS Audit Manager

AWS Backup Die Kontrollen von Audit Manager sind vorgefertigten Standardkontrollen zugeordnet AWS Audit Manager, sodass Sie die Compliance-Ergebnisse Ihres AWS Backup Audit Manager in Ihre AWS Audit Manager Berichte importieren können. Möglicherweise möchten Sie dies tun, um Compliance-Beauftragten, Prüfungsleitern oder anderen Kollegen zu helfen, die im Rahmen der allgemeinen Compliance-Situation Ihres Unternehmens über Backup-Aktivitäten berichten.

Sie können die Konformitätsergebnisse Ihrer AWS Backup Audit Manager Manager-Kontrollen in Ihre AWS Audit Manager Frameworks importieren. Um die automatische Erfassung von Daten aus Ihren AWS Backup Audit Manager Manager-Steuerelementen AWS Audit Manager zu ermöglichen, erstellen Sie ein benutzerdefiniertes Steuerelement, AWS Audit Manager indem Sie die Anweisungen zum Anpassen eines vorhandenen Steuerelements im AWS Audit Manager Benutzerhandbuch verwenden. Beachten Sie bei der Befolgung dieser Anweisungen, dass die Datenquelle für AWS Backup Steuerelemente wie folgt lautet AWS Config.

Eine Liste der AWS Backup Steuerelemente finden Sie unter Steuerelemente auswählen.

Steuerelemente und Abhilfemaßnahmen

Auf dieser Seite sind die verfügbaren Steuerelemente für AWS Backup Audit Manager aufgeführt. Sie können den rechten Informationsbereich auswählen, um eine Liste von Kontrollen anzuzeigen

und zu einer bestimmten Kontrolle zu springen. Informationen zum schnellen Vergleichen von Kontrollen finden Sie in der Tabelle im Artikel Auswählen Ihrer Kontrollen. Informationen zum programmgesteuerten Definieren von Kontrollen finden Sie in den Codefragmenten unter Erstellen von Frameworks mithilfe der AWS Backup -API.

Sie können bis zu 50 Kontrollen pro Konto und Region verwenden. Die Verwendung derselben Kontrolle in zwei verschiedenen Frameworks gilt als Verwendung von zwei Kontrollen aus den auf 50 beschränkten Kontrollen.

Auf dieser Seite werden alle Kontrollen mit den folgenden Informationen aufgeführt:

- Beschreibung. Die Werte in eckigen Klammern („[]“) sind die Standardparameterwerte.
- Die Ressource (n), die die Kontrolle auswertet.
- Die Parameter des Steuerelements.
- Anlass, bei dem die Steuerung ausgeführt wird.
- Der Umfang der Kontrolle ist wie folgt:
  - Sie können Ressourcen nach Typ angeben, indem Sie einen oder mehrere von AWS Backup unterstützte Services auswählen.
  - Sie geben einen Umfang Markierte Ressourcen mit einem einzigen Tag-Schlüssel und einem optionalen Wert an.
  - In der Dropdown-Liste Einzelne Ressource können Sie eine einzelne Ressource angeben.
- Schritte zur Abhilfe, um die Compliance der entsprechenden Ressourcen sicherzustellen.

Beachten Sie, dass nur aktive Ressourcen berücksichtigt werden, wenn Kontrollen Ressourcen auf ihre Compliance hin überprüfen. Beispielsweise wird eine Amazon-EC2-Instance, die gerade ausgeführt wird, durch die Kontrolle Letzter Wiederherstellungspunkt wurde erstellt ausgewertet. Eine EC2-Instance, die sich im angehaltenen Zustand befindet, wird nicht in die Auswertung der Compliance einbezogen.

Backup-Ressourcen sind durch einen Backup-Plan geschützt.

Beschreibung: Prüft, ob Ressourcen durch einen Backup-Plan geschützt sind.

Ressource: `AWS Backup: backup selection`

Parameter: Keine

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ (Standard)
- Einzelne Ressource

Abhilfe: Weisen Sie die Ressourcen einem Backup-Plan zu. AWS Backup schützt Ihre Ressourcen automatisch, nachdem Sie sie einem Backup-Plan zugewiesen haben. Weitere Informationen finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan.

Mindesthäufigkeit und Mindestspeicherung des Backup-Plans

Beschreibung: Prüft, ob Backup-Pläne mindestens eine Backup-Regel enthalten, für die die Backup-Frequenz mindestens [1 Tag] und der Aufbewahrungszeitraum mindestens [35 Tage] betragen.

Ressource: `AWS Backup: backup plans`

Parameter:

- Erforderliche Backup-Frequenz in Stunden oder Tagen
- Erforderlicher Aufbewahrungszeitraum in Tagen, Wochen, Monaten oder Jahren. Wir empfehlen eine Aufbewahrung im Warmspeicher für einen Zeitraum von mindestens einer Woche, damit AWS Backup nach Möglichkeit inkrementelle Backups erstellt werden können, wodurch zusätzliche Kosten vermieden werden.

Tritt auf: Konfigurationsänderungen

Umfang:

- Markierte Ressourcen
- Einzelne Ressource

Abhilfe: Aktualisieren Sie einen Backup-Plan, um entweder die Backup-Frequenz, den Aufbewahrungszeitraum oder beides zu ändern. Durch das Aktualisieren Ihres Backup-Plans wird der Aufbewahrungszeitraum für Wiederherstellungspunkte geändert, die der Plan nach der Aktualisierung erstellt.

Tresore verhindern das manuelle Löschen von Wiederherstellungspunkten.

Beschreibung: Prüft, ob Backup-Tresore das manuelle Löschen von Wiederherstellungspunkten nicht zulassen, mit Ausnahme bestimmter IAM- Rollen.

Ressource: `AWS Backup: backup vaults`

Parameter: Die Amazon-Ressourcennamen (ARNs) von bis zu fünf IAM-Rollen, die berechtigt sind, Wiederherstellungspunkte manuell zu löschen.

Tritt auf: Konfigurationsänderungen

Umfang:

- Markierte Ressourcen
- Einzelne Ressource

Abhilfe: Erstellen oder ändern Sie eine ressourcenbasierte Zugriffsrichtlinie für einen Backup-Tresor. Ein Beispiel für eine Richtlinie und Anweisungen zum Einrichten einer Zugriffsrichtlinie für Backup-Tresore finden Sie unter Verweigern des Zugriffs zum Löschen von Wiederherstellungspunkten in einem Backup-Tresor.

Wiederherstellungspunkte sind verschlüsselt.

Beschreibung: Prüft, ob Wiederherstellungspunkte verschlüsselt sind.

Ressource: `AWS Backup: recovery points`

Parameter: Keine

Tritt auf: Konfigurationsänderungen

Umfang:

- Markierte Ressourcen

Abhilfe: Konfigurieren Sie die Verschlüsselung für die Wiederherstellungspunkte. Die Art und Weise, wie Sie die Verschlüsselung für AWS Backup Wiederherstellungspunkte konfigurieren, ist je nach Ressourcentyp unterschiedlich.

Sie können die Verschlüsselung für Ressourcentypen konfigurieren, die eine vollständige AWS Backup Verwaltung bei der Verwendung unterstützen AWS Backup. Wenn der Ressourcentyp keine vollständige AWS Backup Verwaltung unterstützt, müssen Sie seine Backup-Verschlüsselung konfigurieren, indem Sie den Anweisungen dieses Dienstes folgen, z. B. Amazon EBS-Verschlüsselung im Amazon Elastic Compute Cloud-Benutzerhandbuch. Eine Liste der Ressourcentypen, die die vollständige AWS Backup Verwaltung unterstützen, finden Sie im Abschnitt „Vollständige AWS Backup Verwaltung“ der Verfügbarkeit von Features nach Ressource Tabelle.

Mindestaufbewahrungszeitraum ist für den Wiederherstellungspunkt festgelegt.

Beschreibung: Prüft, ob der Aufbewahrungszeitraum für den Wiederherstellungspunkt mindestens [35 Tage] beträgt.

Ressource: `AWS Backup: recovery points`

Parameter: Erforderlicher Aufbewahrungszeitraum für den Wiederherstellungspunkt in Tagen, Wochen, Monaten oder Jahren. Wir empfehlen eine Aufbewahrung im Warmspeicher für einen Zeitraum von mindestens einer Woche, damit AWS Backup nach Möglichkeit inkrementelle Backups erstellt werden können, wodurch zusätzliche Kosten vermieden werden.

Tritt auf: Konfigurationsänderungen

Umfang:

- Markierte Ressourcen

Abhilfe: Ändern Sie die Aufbewahrungszeiträume Ihrer Wiederherstellungspunkte. Weitere Informationen finden Sie unter Bearbeiten eines Backups.

Regionsübergreifende Backup-Kopie ist geplant.

Beschreibung: Prüft, ob eine Ressource so konfiguriert ist, dass Kopien ihrer Backups in eine andere AWS Region erstellt werden.

Ressource: `AWS Backup: backup selection`

Parameter:

- Wählen Sie die AWS-Region(n) aus, in denen die Sicherungskopie vorhanden sein soll (optional)

- Region

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ
- Einzelne Ressource

Behebung: Aktualisieren Sie einen Backup-Plan, um den AWS-Region Speicherort der Sicherungskopie zu ändern.

Kontenübergreifende Backup-Kopie ist geplant.

Beschreibung: Prüft, ob eine Ressource so konfiguriert ist, dass Kopien ihrer Backups in einem anderen Konto erstellt werden. Sie können bis zu 5 Konten hinzufügen, die von der Kontrolle ausgewertet werden. Das Zielkonto muss sich in derselben Organisation befinden wie das Quellkonto in AWS Organizations.

Ressource: `AWS Backup: backup selection`

Parameter:

- Wählen Sie die AWS Konto-ID (s) aus, unter denen die Sicherungskopie existieren soll (optional)
- Konto-ID

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ
- Einzelne Ressource

Behebung: Aktualisieren Sie einen Backup-Plan, um die AWS Konto-ID (s), unter denen die Kopie vorhanden sein soll, zu ändern oder hinzuzufügen.

Backups werden durch AWS Backup Vault Lock geschützt

Beschreibung: Prüft, ob für eine Ressource unveränderliche Backups in einem gesperrten Backup-Tresor gespeichert sind.

Ressource: `AWS Backup: backup selection`

Parameter:

- Geben Sie die Mindest- und Höchstdauer der Aufbewahrungsdauer für AWS Backup Vault Lock ein (optional)
- Minimale Anzahl von Aufbewahrungstagen
- Maximale Anzahl von Aufbewahrungstagen

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ
- Einzelne Ressource

Abhilfe: Sperren Sie einen Backup-Tresor, um seinen Namen festzulegen, entweder die Mindestanzahl von Aufbewahrungstagen, die maximale Anzahl von Aufbewahrungstagen oder beides zu ändern. Kann auch `ChangeableForDays` für eine Tresorsperre im Compliance-Modus umfassen.

Letzter Wiederherstellungspunkt wurde erstellt.

Beschreibung: Diese Kontrolle wertet aus, ob innerhalb des angegebenen Zeitraums (in Tagen oder Stunden) ein Wiederherstellungspunkt erstellt wurde.

Die Kontrolle ist konform, wenn für die Ressource innerhalb des angegebenen Zeitraums ein Wiederherstellungspunkt erstellt wurde. Die Kontrolle ist nicht konform, wenn innerhalb der angegebenen Anzahl von Tagen oder Stunden kein Wiederherstellungspunkt erstellt wurde.

Ressource: `AWS Backup: recovery points`

Parameter:

- Geben Sie den angegebenen Zeitraum in ganzen Zahlen ein, entweder in Stunden oder Tagen.

- Die Werte von `hours` können im Bereich von 1 bis 744 liegen.
- Der Wert von `days` kann im Bereich von 1 bis 31 liegen.

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ
- Einzelne Ressource

Abhilfe:

- Aktualisieren Sie einen Backup-Plan, um den angegebenen Zeitraum für die Erstellung des Wiederherstellungspunkts zu ändern.
- Darüber hinaus können Sie ein On-Demand-Backup erstellen.

Wiederherstellungszeit für Ressourcen entspricht dem Ziel

Beschreibung: Prüft, ob die Wiederherstellung geschützter Ressourcen innerhalb der angestrebten Wiederherstellungszeit abgeschlossen wurde.

Dieses Steuerelement prüft, ob die Wiederherstellungszeit einer bestimmten Ressource der Zieldauer entspricht. Die Regel ist NON_COMPLIANT, wenn die `LatestRestoreExecutionTimeMinutes` eines Ressourcentyps länger als `maxRestoreTime` Minuten ist.

Parameter:

- `maxRestoreTime` (in Minuten)

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Markierte Ressourcen
- Ressourcen nach Typ
- Einzelne Ressource

> **Note**
>
> AWS Backup bietet keine Service Level Agreements (SLAs) für eine Wiederherstellungszeit. Die Wiederherstellungszeiten können je nach Systemlast und Kapazität variieren, selbst bei Wiederherstellungen, die dieselben Ressourcen enthalten.

Verwaltung von AWS Backup Ressourcen über mehrere AWS-Konten

> **Note**
>
> Bevor Sie Ressourcen für mehrere AWS-Konten Benutzer verwalten können AWS Backup, müssen Ihre Konten derselben Organisation im AWS Organizations Service angehören.

Sie können die Funktion zur kontenübergreifenden Verwaltung verwenden, AWS Backup um Ihre Sicherungs-, Wiederherstellungs- und Kopieraufträge, mit AWS-Konten AWS Organizations denen Sie konfiguriert haben, zu verwalten und zu überwachen. AWS Organizationsist ein Dienst, der eine richtlinienbasierte Verwaltung für mehrere Benutzer AWS-Konten von einem einzigen Verwaltungskonto aus ermöglicht. Damit können Sie die Vorgehensweise zum Implementieren von Sicherungsrichtlinien standardisieren und so gleichzeitig manuelle Fehler und Aufwand minimieren. Von einer zentralen Ansicht aus können Sie problemlos Ressourcen in allen Konten ermitteln, die den für Sie relevanten Kriterien entsprechen.

Wenn Sie es einrichten AWS Organizations, können Sie es so konfigurieren, AWS Backup dass die Aktivitäten in all Ihren Konten von einem zentralen Ort aus überwacht werden. Sie können auch eine Backup-Richtlinie erstellen und diese auf ausgewählte Konten anwenden, die Teil Ihrer Organisation sind, und die gesamten Backup-Job-Aktivitäten direkt von der AWS Backup Konsole aus einsehen. Diese Funktionalität bietet Backup-Administratoren die Möglichkeit, über ein einziges Verwaltungskonto den Status von Backup-Aufträgen in Hunderten von Konten im gesamten Unternehmen effektiv zu überwachen. Hier gelten AWS Organizations -Kontingente.

Ein Beispiel: Sie definieren eine Sicherungsrichtlinie A, wonach tägliche Sicherungen bestimmter Ressourcen erstellt und 7 Tage aufbewahrt werden. Sie beschließen, Sicherungsrichtlinie A auf die gesamte Organisation anzuwenden. (Dies bedeutet, dass jedes Konto in der Organisation diese Backup-Richtlinie erhält, wodurch ein entsprechender Backup–Plan erstellt wird, der in diesem Konto sichtbar ist.) Anschließend erstellen Sie eine Organisationseinheit mit dem Namen Finance und entscheiden, deren Sicherungen nur für 30 Tage zu behalten. In diesem Fall definieren Sie eine Sicherungsrichtlinie B, die den Lebenszykluswert außer Kraft setzt, und fügen sie dieser Organisationseinheit Finance an. Folglich erhalten alle Konten unter der Organisationseinheit Finance einen neuen effektiven Sicherungsplan, nach dem tägliche Sicherungen aller angegebenen Ressourcen erstellt und 30 Tage aufbewahrt werden.

In diesem Beispiel wurden Backup-Richtlinie A und Backup-Richtlinie B zu einer einzigen Backup–Richtlinie zusammengeführt, die die Schutzstrategie für alle Konten unter der Organisationseinheit „Finance“ definiert. Alle anderen Konten in der Organisation bleiben durch die Backup-Richtlinie A geschützt. Die Zusammenführung erfolgt nur für Backup-Richtlinien mit demselben Backup-Plannamen. Sie können auch festlegen, dass Richtlinie A und Richtlinie B in diesem Konto koexistieren, ohne zusammengeführt zu werden. Erweiterte Zusammenführungsoperatoren können nur in der JSON-Ansicht der Konsole verwendet werden. Detaillierte Informationen zum Zusammenführen von Richtlinien finden Sie unter Definieren von Richtlinien, Richtliniensyntax und Richtlinienvererbung im AWS Organizations -Benutzerhandbuch. Weitere Referenzen und Anwendungsfälle finden Sie im Blog Managing Backups at your AWS Organizations using AWS Backup und im Videotutorial Managing Backups at your AWS Organizations use AWS Backup.

Unter Verfügbarkeit der Funktionen nach AWS Regionen finden Sie Informationen darüber, wo die kontoübergreifende Verwaltungsfunktion verfügbar ist.

Um die kontenübergreifende Verwaltung zu verwenden, müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie ein Verwaltungskonto in AWS Organizations und fügen Sie Konten unter dem Verwaltungskonto hinzu.
2. Aktivieren Sie die kontoübergreifende Verwaltungsfunktion in AWS Backup.
3. Erstellen Sie eine Backup-Richtlinie, die für alle Benutzer AWS-Konten Ihres Verwaltungskontos gilt.

   > **Note**
   >
   > Bei Backup-Plänen, die von Organizations verwaltet werden, überschreiben die Einstellungen für die Ressourcenanmeldung im Verwaltungskonto die Einstellungen in einem Mitgliedskonto, selbst dann, wenn ein oder mehrere delegierte Administratorkonten konfiguriert sind. Delegierte Administratorkonten sind Mitgliedskonten mit erweiterten Features und können Einstellungen nicht überschreiben, wie dies bei Verwaltungskonten möglich ist.

4. Verwalten Sie Sicherungs-, Wiederherstellungs- und Kopieraufträge in all Ihren AWS-Konten.

Themen

Erstellen eines Verwaltungskontos in Organizations

Zunächst müssen Sie Ihre Organisation erstellen und sie mit AWS Mitgliedskonten in konfigurieren AWS Organizations.

Um ein Verwaltungskonto in zu erstellen AWS Organizations und Konten hinzuzufügen

- Anweisungen finden Sie unter Praktische Anleitung: Erstellen und Konfigurieren einer Organisation im AWS Organizations -Benutzerhandbuch.

Aktivieren der kontenübergreifenden Verwaltung

Bevor Sie die kontenübergreifende Verwaltung in verwenden können AWS Backup, müssen Sie die Funktion aktivieren (d. h. sich dafür anmelden). Nach Aktivierung der Funktion können Sie Sicherungsrichtlinien erstellen, mit denen Sie die gleichzeitige Verwaltung mehrerer Konten automatisieren können.

So aktivieren Sie die kontenübergreifende Verwaltung

1. Öffnen Sie die AWS-Backup-Konsole unter https://console.aws.amazon.com/backup/. Melden Sie sich mit den Anmeldeinformationen Ihres Verwaltungskontos an.
2. Wählen Sie im linken Navigationsbereich Settings (Einstellungen) aus, um die Seite für die kontenübergreifende Verwaltung zu öffnen.
3. Wählen Sie im Abschnitt Backup policies (Sicherungsrichtlinien) die Option Enable (Aktivieren) aus.

Auf diese Weise erhalten Sie Zugriff auf alle Konten und können Richtlinien erstellen, die die gleichzeitige Verwaltung mehrerer Konten in Ihrer Organisation automatisieren.

4. Wählen Sie im Abschnitt Cross-account monitoring (Kontenübergreifende Überwachung) die Option Enable (Aktivieren) aus.

   Auf diese Weise können Sie die Backup-, Kopier- und Wiederherstellungsaktivitäten aller Konten in Ihrer Organisation von Ihrem Verwaltungskonto aus überwachen.

Delegierter Administrator

Delegierte Administration bietet zugewiesenen Benutzern in einem registrierten Mitgliedskonto eine bequeme Möglichkeit, die meisten AWS Backup administrativen Aufgaben auszuführen. Sie können sich dafür entscheiden, die Verwaltung AWS Backup an ein Mitgliedskonto in zu delegieren AWS Organizations, wodurch die Möglichkeit der Verwaltung AWS Backup von außerhalb des Verwaltungskontos und auf die gesamte Organisation ausgedehnt wird.

Das Verwaltungskonto ist standardmäßig das Konto, das zur Bearbeitung und Verwaltung von Richtlinien verwendet wird. Mithilfe der Funktion für die delegierte Verwaltung können Sie diese Verwaltungsaufgaben an von Ihnen festgelegte Mitgliedskonten delegieren. Im Gegenzug können diese Konten zusätzlich zum Verwaltungskonto Richtlinien verwalten.

Nachdem ein Mitgliedskonto erfolgreich für die delegierte Verwaltung registriert wurde, ist es ein delegiertes Administratorkonto. Beachten Sie, dass Konten, nicht Benutzer, als delegierte Administratoren benannt werden.

Das Aktivieren delegierter Administratorkonten ermöglicht das Verwalten von Backup-Richtlinien, reduziert die Anzahl der Benutzer mit Zugriff auf das Verwaltungskonto und lässt die kontenübergreifende Überwachung von Aufträgen zu.

Im Folgenden finden Sie eine Tabelle mit den Funktionen des Verwaltungskontos, der Konten, die als Backup-Administratoren delegiert wurden, und der Konten, die Mitglieder der AWS Organisation sind.

> **Note**
>
> Delegierte Administratorkonten sind Mitgliedskonten mit erweiterten Features, die jedoch Einstellungen für die Serviceanmeldung nicht überschreiben können, wie dies bei Verwaltungskonten möglich ist.

PRIVILEGES	VERWALTUNGSKONTO	DELEGIERTER ADMINISTRATOR	MITGLIEDSKONTO
Registrieren/Aufheben der Registrierung delegierter Administratorkonten	Ja	Nein	Nein
Verwalten Sie Backup-Richtlinien für alle Konten in AWS Organizations	Ja	Ja	Nein
Überwachen kontenübergreifender Aufträge	Ja	Ja	Nein

Voraussetzungen

Bevor Sie die Backup-Verwaltung delegieren können, müssen Sie zunächst mindestens ein Mitgliedskonto in Ihrer AWS Organisation als delegierten Administrator registrieren. Bevor Sie ein Konto als delegierten Administrator registrieren können, müssen Sie zuerst folgende Einstellungen konfigurieren:

- AWS Organizations muss zusätzlich zu Ihrem Standard-Verwaltungskonto mit mindestens einem Mitgliedskonto aktiviert und konfiguriert sein.
- Stellen Sie sicher, dass in der AWS Backup Konsole die Backup-Richtlinien, die kontoübergreifende Überwachung und die Funktionen für kontoübergreifende Backups aktiviert sind. Diese befinden sich in der Konsole unter dem Bereich Delegierte Administratoren. AWS Backup
  - Kontenübergreifende Überwachung gibt Ihnen die Möglichkeit, die Backup-Aktivitäten über alle Konten in Ihrer Organisation hinweg sowohl vom Verwaltungskonto als auch von delegierten Administratorkonten aus zu überwachen.
  - Optional: Kontoübergreifende Sicherung, die es Konten in Ihrer Organisation ermöglicht, Backups auf andere Konten zu kopieren (für von Backup unterstützte kontenübergreifende Ressourcen).

- Aktivieren Sie den Servicezugriff mit. AWS Backup

Die Einrichtung der delegierten Verwaltung umfasst zwei Schritte. Der erste Schritt besteht darin, die kontenübergreifende Überwachung von Aufträgen zu delegieren. Im zweiten Schritt wird die Verwaltung der Backup-Richtlinien delegiert.

Registrieren eines Mitgliedskontos als delegiertes Administratorkonto

Dies ist der erste Abschnitt: Verwenden der AWS Backup Konsole zur Registrierung eines delegierten Administratorkontos zur Überwachung kontenübergreifender Jobs. Um AWS Backup Richtlinien zu delegieren, verwenden Sie im nächsten Abschnitt die Organisationskonsole.

So registrieren Sie ein Mitgliedskonto über die AWS Backup Konsole:

1. Öffnen Sie das AWS-Backup-Konsole unter https://console.aws.amazon.com/backup/. Melden Sie sich mit den Anmeldeinformationen Ihres Verwaltungskontos an.
2. Wählen Sie in der linken Navigationsleiste der Konsole unter Mein Konto die Option Einstellungen aus.
3. Klicken Sie im Bereich Delegierter Administrator auf Delegierten Administrator registrieren oder auf Delegierten Administrator hinzufügen.
4. Wählen Sie auf der Seite Delegierten Administrator registrieren das Konto, das Sie registrieren möchten, und dann Konto registrieren aus.

Dieses designierte Konto wird nun als delegierter Administrator registriert. Es verfügt dadurch über Administratorrechte zur Überwachung von Aufträgen über alle Konten innerhalb der Organisation hinweg und kann Richtlinien einsehen und bearbeiten (Richtliniendelegierung). Dieses Mitgliedskonto kann keine anderen delegierten Administratorkonten registrieren oder deren Registrierung aufheben. Sie können über die Konsole bis zu 5 Konten als delegierte Administratoren registrieren.

So registrieren Sie ein Mitgliedskonto programmgesteuert

Verwenden Sie den `register-delegated-administrator`-CLI-Befehl. Sie können die folgenden Parameter in Ihrer CLI-Anfrage angeben:

- `service-principal`
- `account-id`

Im Folgenden finden Sie ein Beispiel für eine CLI-Anfrage für die programmgesteuerte Registrierung eines Mitgliedskontos:

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Aufheben der Registrierung eines Mitgliedskontos

Gehen Sie wie folgt vor, um den Administratorzugriff zu entfernen, AWS Backup indem Sie ein Mitgliedskonto in Ihrer AWS Organisation abmelden, das zuvor als delegierter Administrator festgelegt wurde.

So heben Sie die Registrierung eines Mitgliedskontos in der Konsole auf

1. Öffnen Sie das unter https://console.aws.amazon.com/backup/ AWS-Backup-Konsole . Melden Sie sich mit den Anmeldeinformationen Ihres Verwaltungskontos an.
2. Wählen Sie in der linken Navigationsleiste der Konsole unter Mein Konto die Option Einstellungen aus.
3. Klicken Sie im Bereich Delegierter Administrator auf Registrierung des Kontos aufheben.
4. Wählen Sie das Konto oder die Konten aus, dessen bzw. deren Registrierung Sie aufheben möchten.
5. Überprüfen Sie im Dialogfeld Registrierung des Kontos aufheben die Sicherheitsauswirkungen und geben Sie dann `confirm` ein, um das Aufheben der Registrierung abzuschließen.
6. Wählen Sie `Deregister account`.

So heben Sie die Registrierung eines Mitgliedskontos programmgesteuert auf

Verwenden Sie den CLI-Befehl `deregister-delegated-administrator`, um die Registrierung eines delegierten Administratorkontos aufzuheben. Sie können die folgenden Parameter in Ihrer API-Anfrage angeben:

- `service-principal`
- `account-id`

Im Folgenden finden Sie ein Beispiel für eine CLI-Anfrage zur programmgesteuerten Aufhebung der Registrierung eines Mitgliedskontos:

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Delegieren Sie AWS Backup Richtlinien über AWS Organizations

In der AWS Organizations Konsole können Sie die Verwaltung mehrerer Richtlinien, einschließlich Backup-Richtlinien, delegieren.

Sie können vom Verwaltungskonto aus, das bei der AWS Organizations -Konsole angemeldet ist, eine ressourcenbasierte Delegierungsrichtlinie für Ihre Organisation erstellen, anzeigen oder löschen. Schritte zum Delegieren von Richtlinien finden Sie unter Erstellen oder Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie im AWS Organizations -Benutzerhandbuch.

Erstellen einer Backup-Richtlinie

Nachdem Sie die kontenübergreifende Verwaltung aktiviert haben, erstellen Sie von Ihrem Verwaltungskonto aus eine kontenübergreifende Backup-Richtlinie.

> **Warning**
>
> Wenn Sie eine Richtlinie mit JSON erstellen, werden doppelte Schlüsselnamen zurückgewiesen. Der Name jedes Schlüssels muss eindeutig sein, wenn mehrere Pläne, Regeln oder Auswahlen in einer einzigen Richtlinie enthalten sind.

Erstellen Sie über die Konsole eine Backup-Richtlinie AWS Backup

1. Wählen Sie im linken Navigationsbereich Backup policies (Sicherungsrichtlinien) aus. Wählen Sie auf der Seite Backup policies (Sicherungsrichtlinien) die Option Create backup policies (Sicherungsrichtlinien erstellen) aus.
2. Geben Sie im Abschnitt Details einen Namen für die Sicherungsrichtlinie ein und geben Sie eine Beschreibung an.
3. Wählen Sie im Abschnitt Backup plans details (Details zu Sicherungsplänen) die Registerkarte „Visual Editor (Visueller Editor)“ aus und führen Sie die folgenden Schritte aus:

    a. Geben Sie für Backup plan name (Name des Sicherungsplans einen Namen ein.

    b. Wählen Sie für Region eine Region aus der Liste aus.

4. Wählen Sie im Abschnitt Backup rule configuration (Konfiguration der Sicherungsregel) die Option Add backup rule (Sicherungsregel hinzufügen) aus.

   Die maximale Anzahl von Regeln pro Backup-Plan beträgt 10. Wenn ein Plan mehr als 10 Regeln enthält, wird der Backup-Plan ignoriert und es werden keine Backups daraus erstellt.

   a. Geben Sie für Rule name (Regelname) einen Namen für die Regel ein. Bei dem Regelnamen wird zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nur alphanumerische Zeichen oder Bindestriche enthalten.

   b. Wählen Sie unter Schedule (Zeitplan) eine Sicherungshäufigkeit in der Liste Frequency (Häufigkeit) aus und wählen Sie dann eine der Optionen unter Backup window (Sicherungsfenster) aus. Wir empfehlen Ihnen, die Option Standardwerte für das Backup-Fenster verwenden – empfohlen auszuwählen.

5. Wählen Sie unter Lifecycle (Lebenszyklus) die gewünschten Lebenszykluseinstellungen aus.

6. Geben Sie für Backup vault name (Name des Sicherungstresors) einen Namen ein. Dies ist der Sicherungstresor, in dem Wiederherstellungspunkte gespeichert werden, die von Ihren Sicherungen erstellt wurden.

   Stellen Sie sicher, dass der Backup-Tresor in all Ihren Konten vorhanden ist. AWS Backup prüft das nicht.

7. (optional) Wählen Sie eine Zielregion aus der Liste aus, wenn Sie möchten, dass Ihre Backups in eine andere kopiert werden AWS-Region, und fügen Sie Tags hinzu. Sie können Tags für die erstellten Wiederherstellungspunkte auswählen, unabhängig von den regionsübergreifenden Kopiereinstellungen. Sie können auch weitere Regeln hinzufügen.

8. Geben Sie im Abschnitt Ressourcenzuweisung den Namen der AWS Identity and Access Management (IAM-) Rolle ein. Um die AWS Backup Servicerolle zu verwenden, geben Sie `service-role/AWSBackupDefaultServiceRole` an.

   AWS Backup nimmt diese Rolle in jedem Konto an, um die Berechtigungen zur Ausführung von Sicherungs- und Kopieraufträgen zu erhalten, einschließlich der Berechtigungen für Verschlüsselungsschlüssel, falls zutreffend. AWS Backup verwendet diese Rolle auch, um Lebenszyklus-Löschungen durchzuführen.

   > **Note**
   >
   > AWS Backup überprüft nicht, ob die Rolle existiert oder ob die Rolle übernommen werden kann.

Bei Backup-Plänen, die im Rahmen der kontoübergreifenden Verwaltung erstellt wurden, AWS Backup werden die Opt-in-Einstellungen des Verwaltungskontos verwendet und die Einstellungen bestimmter Konten außer Kraft gesetzt.
Für jedes Konto, dem Sie Backup-Richtlinien hinzufügen möchten, müssen Sie die Tresore und IAM-Rollen selbst erstellen.

9. Fügen Sie Tags hinzu, um die Ressourcen auszuwählen, die Sie sichern möchten. Die maximal zulässige Anzahl von Tags ist 30.

   AWS Organizations Die Richtlinie ermöglicht die Angabe von maximal 30 Tags, wenn ein Backup-Plan über die Organisationsrichtlinie erstellt wird. Zusätzliche Tags können hinzugefügt werden, indem mehrere Ressourcenzuweisungen oder mehrere Backup-Pläne verwendet werden.

   Wenn die Anzahl der Tags in derselben Backup-Auswahl 30 überschreitet, entweder durch Änderung der vorhandenen Auswahl oder durch Verwendung`@@append`, wird der Backup-Plan ungültig und aus dem lokalen Konto entfernt.

10. Wählen Sie im Abschnitt Erweiterte Einstellungen die Option Windows VSS aus, wenn auf der Ressource, die Sie sichern, Microsoft Windows auf einer Amazon-EC2-Instance ausgeführt wird. Auf diese Weise können Sie anwendungskonsistente Windows-VSS-Backups erstellen.

    > **Note**
    >
    > AWS Backup unterstützt derzeit nur anwendungskonsistente Backups von Ressourcen, die auf Amazon EC2 ausgeführt werden. Nicht alle Instance-Typen oder Anwendungen werden für Windows-VSS-Backups unterstützt. Weitere Informationen finden Sie unter Erstellen von Windows-VSS-Backups.

11. Wählen Sie Add backup plan (Sicherungsplan hinzufügen), um ihn der Richtlinie hinzuzufügen, und wählen Sie dann Create backup policy (Sicherungsrichtlinie erstellen).

    Durch das Erstellen einer Sicherungsrichtlinie werden Ihre Ressourcen erst geschützt, wenn Sie sie an die Konten anfügen. Sie können Ihren Richtliniennamen wählen und die Details anzeigen.

    Im Folgenden finden Sie ein Beispiel AWS Organizations für eine Richtlinie, mit der ein Backup-Plan erstellt wird. Wenn Sie Windows VSS-Backup aktivieren, müssen Sie Berechtigungen hinzufügen, die es Ihnen ermöglichen, anwendungskonsistente Backups zu erstellen, wie im Abschnitt `advanced_backup_settings` der Richtlinie beschrieben.

```
{
  "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. Wählen Sie im Abschnitt Targets (Ziele) die Organisationseinheit oder das Konto, an das Sie die Richtlinie anfügen möchten, und wählen Sie Attach (Anfügen). Die Richtlinie kann auch einzelnen Organisationseinheiten oder Konten hinzugefügt werden.

> **Note**
>
> Stellen Sie sicher, dass Sie die Richtlinie validieren und dass alle erforderlichen Felder in der Richtlinie enthalten sind. Wenn Teile der Richtlinie ungültig sind, ignoriert AWS Backup diese Teile. Die gültigen Teile der Richtlinie funktionieren jedoch wie erwartet. Überprüft AWS Organizations Richtlinien derzeit AWS Backup nicht auf ihre Richtigkeit. Wenn Sie eine Richtlinie auf das Verwaltungskonto und eine andere Richtlinie auf ein Mitgliedskonto anwenden und diese miteinander in Konflikt stehen (weil sie z. B. unterschiedliche Aufbewahrungsfristen für Backups aufweisen), können beide Richtlinien problemlos ausgeführt werden (d. h., die Richtlinien werden für jedes Konto unabhängig ausgeführt). Wenn die Verwaltungskontorichtlinie beispielsweise einmal täglich ein Amazon-EBS-Volume sichert und die lokale Richtlinie ein EBS-Volume einmal pro Woche sichert, werden beide Richtlinien ausgeführt.
> Wenn Pflichtfelder in der effektiven Richtlinie fehlen, die auf ein Konto angewendet wird (wahrscheinlich aufgrund der Zusammenführung zwischen verschiedenen Richtlinien), wendet AWS Backup die Richtlinie überhaupt nicht auf das Konto an. Wenn einige Einstellungen nicht gültig sind, werden sie AWS Backup angepasst.

Unabhängig von den Opt-In-Einstellungen in einem Mitgliedskonto werden in einem Backup-Plan, der anhand einer Backup-Richtlinie erstellt AWS Backup wird, die im Verwaltungskonto der Organisation angegebenen Opt-in-Einstellungen verwendet.

Wenn Sie eine Richtlinie an eine Organisationseinheit anfügen, erhält jedes Konto, das dieser Organisationseinheit beitritt, diese Richtlinie automatisch, und jedes Konto, das aus der Organisationseinheit entfernt wird, verliert diese Richtlinie. Die entsprechenden Sicherungspläne werden automatisch aus diesem Konto gelöscht.

Überwachen von Aktivitäten in mehreren AWS-Konten

Um Sicherungs-, Kopier- und Wiederherstellungsaufträge kontenübergreifend überwachen zu können, müssen Sie die kontenübergreifende Überwachung aktivieren. Auf diese Weise können Sie Backup-Aktivitäten in allen Konten über das Verwaltungskonto Ihrer Organisation überwachen. Nachdem Sie sich angemeldet haben, können Sie alle Aufträge in Ihrer Organisation sehen, die nach dem Opt-In erstellt wurden. Wenn Sie sich abmelden, werden die Aufträge 30 Tage lang (ab Erreichen des Beendigungsstatus) in der aggregierten Ansicht von AWS Backup aufbewahrt. Nach der Abmeldung erstellte Aufträge und neu erstellte Sicherungsaufträge können Sie nicht sehen. Anweisungen zur Abmeldung finden Sie unter Aktivieren der kontenübergreifenden Verwaltung.

So überwachen Sie mehrere Konten

1. Öffnen Sie das AWS-Backup-Konsole unter https://console.aws.amazon.com/backup/. Melden Sie sich mit den Anmeldeinformationen Ihres Verwaltungskontos an.
2. Wählen Sie im linken Navigationsbereich Settings (Einstellungen) aus, um die Seite für die kontenübergreifende Verwaltung zu öffnen.
3. Wählen Sie im Abschnitt Cross-account monitoring (Kontenübergreifende Überwachung) die Option Enable (Aktivieren) aus.

   Auf diese Weise können Sie die Backup- und Wiederherstellungsaktivitäten aller Konten in Ihrer Organisation von Ihrem Verwaltungskonto aus überwachen.
4. Wählen Sie im linken Navigationsbereich Cross-account monitoring (Kontenübergreifende Überwachung) aus.

5. Wählen Sie auf der Seite Cross-account monitoring (Kontenübergreifende Überwachung) die Registerkarte Backup jobs (Sicherungsaufträge), Restore jobs (Wiederherstellungsaufträge) oder Copy jobs (Kopieraufträge), um alle in allen Konten erstellten Aufträge anzuzeigen. Sie können jeden dieser Jobs anhand der AWS-Konto ID sehen, und Sie können alle Jobs in einem bestimmten Konto sehen.
6. Im Suchfeld können Sie die Aufträge nach Account ID (Konto-ID), Status oder Job-ID (Auftrags-ID) filtern.

   Sie können beispielsweise die Registerkarte Backup jobs (Sicherungsaufträge) auswählen und alle Sicherungsaufträge anzeigen, die in allen Konten erstellt wurden. Sie können die Liste nach Account ID (Konto-ID) filtern und alle Sicherungsaufträge anzeigen, die in diesem Konto erstellt wurden.

Opt-In-Regeln für Ressourcen

Wenn der Backup-Plan eines Mitgliedskontos durch eine Backup-Richtlinie auf Organisationsebene erstellt wurde, überschreiben die AWS Backup Opt-in-Einstellungen für das Organisationsverwaltungskonto die Opt-in-Einstellungen in diesem Mitgliedskonto, jedoch nur für diesen Backup-Plan.

Wenn das Mitgliedskonto auch Backup-Pläne auf lokaler Ebene hat, die von Benutzern erstellt wurden, folgen diese Backup-Pläne den Opt-In-Einstellungen im Mitgliedskonto, ohne Verweis auf die Opt-In-Einstellungen des Organizations-Verwaltungskontos.

Definieren von Richtlinien, Richtliniensyntax und Richtlinienvererbung

Die folgenden Themen sind im Benutzerhandbuch dokumentiert. AWS Organizations

- Backup-Richtlinien – Siehe Backup-Richtlinien.
- Richtliniensyntax – Siehe Syntax und Beispiele für Backup-Richtlinien.
- Vererbung für Verwaltungsrichtlinientypen – Siehe Vererbung von Verwaltungsrichtlinien verstehen.

AWS Backup und AWS CloudFormation

Allgemeines

Mit AWS CloudFormation können Sie Ihre AWS-Ressourcen mithilfe von Vorlagen, die Sie erstellen, auf sichere und wiederholbare Weise bereitstellen und verwalten. Sie können AWS CloudFormation-Vorlagen und -StackSets verwenden, um Ihre Backup-Pläne, Backup-Ressourcenauswahl und Backup-Tresore zu verwalten. Weitere Informationen zur Verwendung von AWS CloudFormation finden Sie unter Wie funktioniert AWS CloudFormation? im AWS CloudFormation-Benutzerhandbuch .

Berücksichtigen Sie Folgendes, bevor Sie die AWS CloudFormation-Vorlage bzw. das StackSet erstellen:

- Erstellen Sie separate Vorlagen für Ihre Backup-Pläne und Ihre Backup-Tresore. Sie können nur leere Backup-Tresore löschen. Sie können einen Stack, der Backup-Tresore enthält, nicht löschen, wenn diese Wiederherstellungspunkte enthalten.
- Überprüfen Sie, ob Sie eine Servicerolle zur Verfügung haben, bevor Sie den Stack erstellen. Die AWS Backup-Standard-Servicerolle wird für Sie erstellt, wenn Sie einem Sicherungsplan zum ersten Mal Ressourcen zuweisen. Wenn Sie Ihrem Backup-Plan keine Ressourcen zugewiesen haben, tun Sie dies, bevor Sie den Stack erstellen. Sie können auch eine benutzerdefinierte Rolle angeben, die Sie erstellen. Weitere Informationen zu Rollen finden Sie unter IAM-Servicerollen.

Bereitstellen eines Backup-Tresors, eines Backup-Plans und einer Ressourcenzuweisung mithilfe von AWS CloudFormation

AWS CloudFormation-Beispielvorlagen für die Bereitstellung eines Backup-Tresors, von Backup-Plänen und einer Ressourcenweisung finden Sie unter Zuweisen von Ressourcen mit AWS CloudFormation.

Bereitstellen von Backup-Plänen mithilfe von AWS CloudFormation

AWS CloudFormation-Beispielvorlagen für die Bereitstellung von Backup-Plänen finden Sie unter AWS CloudFormation-Vorlagen für Backup-Pläne.

Bereitstellen von AWS Backup-Audit-Manager-Frameworks und -Berichtsplänen mithilfe von AWS CloudFormation

AWS CloudFormation-Beispielvorlagen, die AWS Backup-Audit-Manager-Frameworks und -Berichtspläne bereitstellen, finden Sie unter AWS CloudFormation-Vorlagen für Backup-Pläne.

Kontenübergreifendes Bereitstellen von Backup-Plänen mithilfe von AWS CloudFormation

Sie können AWS CloudFormation-StackSets für mehrere Konten in einer AWS-Organisation verwenden. Beispielvorlagen stehen im AWS CloudFormation-Benutzerhandbuch zur Verfügung.

Ein hervorragender Ausgangspunkt und eine großartige Referenz ist die Veröffentlichung Automate centralized backup at scale across AWS services using AWS Backup. Mit Ibukun Oyewumi und Sabith Venkitachalapathy (Juli 2021).

Weitere Informationen zu AWS CloudFormation

Informationen zur Verwendung von AWS CloudFormation mit AWS Backup finden Sie unter Ressourcentypenreferenz für AWS Backup im AWS CloudFormation-Benutzerhandbuch.

Informationen zum Steuern des Zugriffs auf AWS-Serviceressourcen bei Verwendung von AWS CloudFormation finden Sie unter Zugriffssteuerung mit AWS Identity and Access Management im AWS CloudFormation-Benutzerhandbuch.

Sicherheit in AWS Backup

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Backup, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud – Ihre Verantwortung AWS Backup umfasst unter anderem Folgendes. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.
  - Beantwortung von Mitteilungen, die Sie erhalten von AWS.
  - Verwaltung der Anmeldeinformationen, die Sie und Ihr Team verwenden. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung in AWS Backup.
  - Die Backup-Pläne und Ressourcenzuweisungen sollten den Datenschutzrichtlinien Ihrer Organisation entsprechen. Weitere Informationen finden Sie unter Verwalten von Sicherungsplänen.
  - Testen Sie regelmäßig Ihre Fähigkeit, bestimmte Wiederherstellungspunkte zu finden und wiederherzustellen. Weitere Informationen finden Sie unter Arbeiten mit Sicherungen.
  - Aufnahme von AWS Backup Verfahren in die schriftlichen Verfahren für Notfallwiederherstellung und Geschäftskontinuität Ihres Unternehmens. Einen Ausgangspunkt finden Sie unter Erste Schritte mit AWS Backup.
  - Stellen Sie sicher, dass Ihre Mitarbeiter mit Ihren organisatorischen Abläufen im Notfall vertraut sind und diese geübt haben. AWS Backup Weitere Informationen finden Sie unter AWS Well-Architected Framework.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Backup. In den folgenden Themen erfahren Sie, wie Sie

die Konfiguration vornehmen AWS Backup , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Außerdem erfahren Sie, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Backup Ressourcen unterstützen.

Themen

Überprüfung der Einhaltung von Vorschriften für AWS Backup

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen entwickeln AWS können.

> **Note**
>
> Nicht AWS-Services alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Datenschutz in AWS Backup

AWS Backup entspricht dem Modell der AWS gemeinsamen Verantwortung, das Vorschriften und Richtlinien für den Datenschutz beinhaltet. AWS ist verantwortlich für den Schutz der globalen Infrastruktur, die alle AWS Dienste betreibt. AWS behält die Kontrolle über die auf dieser Infrastruktur

gehosteten Daten, einschließlich der Sicherheitskonfigurationskontrollen für den Umgang mit Kundeninhalten und personenbezogenen Daten. AWS Kunden und AWS Partner Network (APN), die entweder als Datenverantwortliche oder als Datenverarbeiter agieren, sind für alle personenbezogenen Daten verantwortlich, die AWS Cloud sie eingeben.

Aus Datenschutzgründen empfehlen wir Ihnen, Ihre AWS-Konto Anmeldeinformationen zu schützen und individuelle Benutzerkonten bei AWS Identity and Access Management (IAM) einzurichten. Auf diese Weise erhält jeder Benutzer nur die Berechtigungen, die zum Erledigen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie Secure Sockets Layer (SSL)/Transport Layer Security (TLS) für die Kommunikation mit AWS -Ressourcen.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS Backup oder anderen AWS Diensten arbeiten, die Konsole AWS CLI, API oder AWS SDKs verwenden. Alle Daten, die Sie in AWS Backup oder andere Services eingeben, werden möglicherweise in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag AWS Shared Responsibility Model and GDPR im AWS -Sicherheitsblog.

Verschlüsselung für Backups in AWS Backup

> **Note**
>
> AWS Backup Audit Manager hilft Ihnen dabei, unverschlüsselte Backups automatisch zu erkennen.

Sie können die Verschlüsselung für Ressourcentypen konfigurieren, die eine vollständige AWS Backup Verwaltung bei der Verwendung AWS Backup unterstützen. Wenn der Ressourcentyp

keine vollständige AWS Backup Verwaltung unterstützt, müssen Sie seine Backup-Verschlüsselung konfigurieren, indem Sie den Anweisungen dieses Dienstes folgen, z. B. Amazon EBS-Verschlüsselung im Amazon Elastic Compute Cloud-Benutzerhandbuch. Eine Liste der Ressourcentypen, die die vollständige AWS Backup Verwaltung unterstützen, finden Sie im Abschnitt „Vollständige AWS Backup Verwaltung“ der Verfügbarkeit von Features nach Ressource Tabelle.

Die folgende Tabelle führt alle unterstützten Ressourcentypen und die Konfiguration der Verschlüsselung für Sicherungen auf und gibt an, ob die unabhängige Verschlüsselung für Sicherungen unterstützt wird. Wenn AWS Backup eine Sicherung unabhängig verschlüsselt, wird der branchenübliche AES-256-Verschlüsselungsalgorithmus verwendet.

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon-Simple-Storage-Service (Amazon-S3)	Amazon S3 S3-Backups werden mit einem AWS KMS (AWS Key Management Service) -Schlüssel verschlüsselt, der dem Backup-Tresor zugeordnet ist. Bei dem AWS KMS-Schlüssel kann es sich entweder um einen vom Kunden verwalteten CMK oder um einen mit dem AWS Service verknüpften CMK handeln. AWS Backup AWS Backup verschlüsselt alle Backups, auch wenn die Amazon S3 S3-Quell-Buckets nicht verschlüsselt sind.	Unterstützt
Virtuelle VMware-Maschinen	VM-Backups sind immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für Backups virtueller Maschinen wird in dem AWS Backup Tresor konfiguriert, in dem	Unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
	die Backups der virtuellen Maschinen gespeichert sind.	
Amazon DynamoDB nach der Aktivierung von Erweitertes DynamoDB-Backup	DynamoDB-Sicherungen werden immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für DynamoDB-Backups wird in dem AWS Backup Tresor konfiguriert, in dem die DynamoDB-Backups gespeichert sind.	Unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon DynamoDB ohne Aktivierung von Erweitertes DynamoDB-Backup	DynamoDB-Sicherungen werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung der DynamoDB-Tabelle verwendet wurde. Snapshots unverschlüsselter DynamoDB-Tabellen sind ebenfalls unverschlüsselt. **Note** Um eine Sicherungskopie einer verschlüsselten DynamoDB-Tabelle AWS Backup zu erstellen, müssen Sie die Berechtigungen `kms:Decrypt` und `kms:GenerateDataKey` zur IAM-Rolle hinzufügen, die für die Sicherung verwendet wird. Alternativ können Sie die Standard-Servicerolle verwenden. AWS Backup	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon Elastic File System (Amazon EFS)	Amazon EFS-Sicherungen werden immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für Amazon EFS-Backups wird in dem AWS Backup Tresor konfiguriert, in dem die Amazon EFS-Backups gespeichert sind.	Unterstützt
Amazon Elastic Block Store (Amazon EBS)	Standardmäßig werden Amazon EBS-Sicherungen entweder mit dem Schlüssel verschlüsselt, der zur Verschlüsselung des Quell-Volumes verwendet wurde, oder sie sind unverschlüsselt. Während der Wiederherstellung können Sie die Standardverschlüsselungsmethode überschreiben, indem Sie einen KMS-Schlüssel angeben.	Nicht unterstützt
Amazon Elastic Compute Cloud (Amazon EC2) AMIs	AMIs sind unverschlüsselt. EBS-Snapshots werden nach den Standardverschlüsselungsregeln für EBS-Backups verschlüsselt (siehe Eintrag für EBS). EBS-Snapshots von Daten und Root-Volumes können verschlüsselt und an ein AMI angehängt werden.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon Relational Database Service (Amazon RDS)	Amazon RDS-Snapshots werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung der Amazon RDS-Quell-Datenbank verwendet wurde. Snapshots unverschlüsselter Amazon RDS-Datenbanken sind ebenfalls unverschlüsselt. **Note** AWS Backup unterstützt derzeit alle Amazon RDS-Datenbank-Engines, einschließlich Amazon Aurora.	Nicht unterstützt
Amazon Aurora	Aurora-Cluster-Snapshots werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung des Amazon Aurora-Quell-Clusters verwendet wurde. Snapshots unverschlüsselter Aurora-Cluster sind ebenfalls unverschlüsselt.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
AWS Storage Gateway	Storage Gateway-Snapshots werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung des Storage Gateway-Quell-Volumes verwendet wurde. Snapshots unverschlüsselter Storage Gateway-Volumes sind ebenfalls unverschlüsselt. **Note** Sie müssen nicht für alle Services einen Customer Managed Key verwenden, um Storage Gateway zu aktivieren. Sie müssen die Storage Gateway-Sicherung nur in einen Tresor kopieren, für den ein KMS-Schlüssel konfiguriert ist. Das liegt daran, dass Storage Gateway keinen dienstspezifischen AWS KMS verwalteten Schlüssel hat.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon FSx	Die Verschlüsselungsfunktionen für Amazon FSx-Dateisysteme unterscheiden sich je nach dem zugrunde liegenden Dateisystem. Weitere Informationen zu Ihrem speziellen Amazon FSx-Dateisystem finden Sie im entsprechenden FSx-Benutzerhandbuch.	Nicht unterstützt
Amazon DocumentDB	Amazon DocumentDB-Cluster-Snapshots werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung des Amazon DocumentDB-Quell-Clusters verwendet wurde. Snapshots unverschlüsselter Amazon DocumentDB-Cluster sind ebenfalls unverschlüsselt.	Nicht unterstützt
Amazon Neptune	Neptune-Cluster-Snapshots werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung des Neptune-Quell-Clusters verwendet wurde. Snapshots unverschlüsselter Neptune-Cluster sind ebenfalls unverschlüsselt.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
Amazon Timestream	Sicherungen von Timestream-Tabellen-Snapshots sind immer verschlüsselt. Der AWS KMS -Verschlüsselungsschlüssel für Timestream-Sicherungen ist im Backup-Tresor konfiguriert, in dem die Timestream-Sicherungen gespeichert sind.	Unterstützt
Amazon-Redshift	Amazon Redshift-Cluster werden automatisch mit demselben Schlüssel verschlüsselt, der zur Verschlüsselung des Amazon Redshift-Quell-Clusters verwendet wurde. Snapshots unverschlüsselter Amazon Redshift-Cluster sind ebenfalls unverschlüsselt.	Nicht unterstützt
AWS CloudFormation	CloudFormation Backups werden immer verschlüsselt. Der CloudFormation Verschlüsselungsschlüssel für CloudFormation Backups wird in dem CloudFormation Tresor konfiguriert, in dem die CloudFormation Backups gespeichert werden.	Unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige AWS Backup Verschlüsselung
SAP HANA-Datenbanken auf Amazon EC2-Instances	SAP HANA-Datenbank-Sicherungen sind immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für SAP HANA-Datenbanksicherungen wird in dem AWS Backup Tresor konfiguriert, in dem die Datenbanksicherungen gespeichert sind.	Unterstützt

Verschlüsselung für Sicherungskopien

Wenn Sie AWS Backup Ihre Backups konto- oder regionsübergreifend kopieren, AWS Backup werden diese Kopien für die meisten Ressourcentypen automatisch verschlüsselt, auch wenn das ursprüngliche Backup unverschlüsselt ist. AWS Backup verschlüsselt Ihre Kopie mit dem KMS-Schlüssel des Ziel-Tresors. Snapshots von unverschlüsselten Aurora-, Amazon DocumentDB- und Neptune-Clustern sind jedoch ebenfalls unverschlüsselt.

Verschlüsselung und Sicherungskopien

Kontoübergreifende Kopien mit AWS verwalteten KMS-Schlüsseln werden für Ressourcen, die nicht vollständig von AWS Backup verwaltet werden, nicht unterstützt. Weitere Informationen Vollständige Verwaltung AWS Backup dazu, welche Ressourcen vollständig verwaltet werden, finden Sie unter.

Bei den Ressourcen, die vollständig verwaltet werden AWS Backup, werden die Backups mit dem Verschlüsselungsschlüssel des Backup-Tresors verschlüsselt. Für Ressourcen, die nicht vollständig verwaltet werden AWS Backup, verwenden kontenübergreifende Kopien denselben KMS-Schlüssel wie die Quellressource. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel und kontoübergreifende Kopien.

Verschlüsselung der Hypervisor-Anmeldeinformationen für virtuelle Maschinen

Virtuelle Maschinen, die von einem Hypervisor verwaltet werden, verwenden AWS Backup Gateway, um lokale Systeme mit AWS Backup zu verbinden. Es ist wichtig, dass Hypervisoren über dieselbe

robuste und zuverlässige Sicherheit verfügen. Diese Sicherheit kann erreicht werden, indem der Hypervisor entweder mit eigenen Schlüsseln oder mit vom Kunden AWS verwalteten Schlüsseln verschlüsselt wird.

AWS eigene und vom Kunden verwaltete Schlüssel

AWS Backup bietet Verschlüsselung für Hypervisor-Anmeldeinformationen, um vertrauliche Kunden-Anmeldeinformationen mithilfe AWS eigener Verschlüsselungsschlüssel zu schützen. Sie haben die Möglichkeit, stattdessen vom Kunden verwaltete Schlüssel zu verwenden.

Standardmäßig handelt es sich bei den Schlüsseln, die zum Verschlüsseln von Anmeldeinformationen in Ihrem Hypervisor verwendet werden AWS , um eigene Schlüssel. AWS Backup verwendet diese Schlüssel, um Hypervisor-Anmeldeinformationen automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel weder anzeigen, verwalten oder verwenden, noch können Sie deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie AWS im AWS KMS Entwicklerhandbuch unter Eigene Schlüssel.

Alternativ können Anmeldeinformationen mit von Kunden verwalteten Schlüsseln verschlüsselt werden. AWS Backup unterstützt die Verwendung von symmetrischen kundenverwalteten Schlüsseln, die Sie erstellen, besitzen und verwalten, um Ihre Verschlüsselung durchzuführen. Da Sie die volle Kontrolle über diese Verschlüsselung haben, können Sie Aufgaben wie die folgenden ausführen:

- Festlegung und Pflege von Schlüsselrichtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, wird AWS Backup überprüft, ob Ihre Rolle berechtigt ist, mithilfe dieses Schlüssels zu entschlüsseln (bevor ein Sicherungs- oder Wiederherstellungsauftrag ausgeführt wird). Sie müssen die `kms:Decrypt`-Aktion der Rolle hinzufügen, die zum Starten eines Sicherungs- oder Wiederherstellungsauftrags verwendet wurde.

Da die `kms:Decrypt`-Aktion nicht zur Standard-Sicherungsrolle hinzugefügt werden kann, müssen Sie eine andere Rolle als die Standard-Sicherungsrolle verwenden, um vom Kunden verwaltete Schlüssel zu verwenden.

Weitere Informationen finden Sie unter von Kunden verwaltete Schlüssel im AWS Key Management Service -Entwicklerhandbuch.

Bei Verwendung kundenverwalteter Schlüssel erforderliche Erteilung

AWS KMS erfordert eine Genehmigung zur Nutzung Ihres vom Kunden verwalteten Schlüssels. Wenn Sie eine Hypervisor-Konfiguration importieren, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, AWS Backup erstellt in Ihrem Namen einen Zuschuss, indem es eine `CreateGrant`Anfrage an AWS KMS sendet. AWS Backup verwendet Zuschüsse, um auf einen KMS-Schlüssel in einem Kundenkonto zuzugreifen.

Sie können den Zugriff auf den Grant jederzeit widerrufen oder ihm den Zugriff auf den vom Kunden verwalteten Schlüssel entziehen AWS Backup. Wenn Sie dies tun, können all Ihre mit Ihrem Hypervisor verknüpften Gateways nicht mehr auf den Benutzernamen und das Passwort des Hypervisors zugreifen, die mit dem vom Kunden verwalteten Schlüssel verschlüsselt wurden, was sich auf Ihre Sicherungs- und Wiederherstellungsaufträge auswirkt. Insbesondere Sicherungs- und Wiederherstellungsaufträge, die Sie auf den virtuellen Maschinen in diesem Hypervisor ausführen, schlagen fehl.

Das Backup-Gateway verwendet den `RetireGrant`-Vorgang, um einen Zuschuss zu entfernen, wenn Sie einen Hypervisor löschen.

Überwachen von Verschlüsselungsschlüsseln

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel mit Ihren AWS Backup Ressourcen verwenden, können Sie Amazon CloudWatch Logs verwenden AWS CloudTrail, um Anfragen zu verfolgen, die AWS Backup an gesendet AWS KMS werden.

Suchen Sie nach AWS CloudTrail Ereignissen mit den folgenden `"eventName"` Feldern zur Überwachung von AWS KMS Vorgängen, die aufgerufen werden AWS Backup , um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`

- `"eventName": "DescribeKey"`

Identitäts- und Zugriffsmanagement in AWS Backup

Für den Zugriff auf AWS Backup sind Anmeldeinformationen erforderlich. Diese Anmeldeinformationen müssen Berechtigungen für den Zugriff auf AWS -Ressourcen wie etwa eine Amazon DynamoDB-Datenbank oder ein Amazon EFS-Dateisystem haben. Darüber hinaus können Wiederherstellungspunkte, die von AWS Backup einigen AWS Backup unterstützten Diensten erstellt wurden, nicht mithilfe des Quelldienstes (wie Amazon EFS) gelöscht werden. Sie können diese Wiederherstellungspunkte mithilfe von AWS Backup löschen.

In den folgenden Abschnitten erfahren Sie, wie Sie AWS Identity and Access Management (IAM) verwenden können und wie Sie AWS Backup den Zugriff auf Ihre Ressourcen sichern können.

> **Warning**
>
> AWS Backup verwendet dieselbe IAM-Rolle, die Sie bei der Zuweisung von Ressourcen für die Verwaltung Ihres Wiederherstellungspunkt-Lebenszyklus ausgewählt haben. Wenn Sie diese Rolle löschen oder ändern, kann Ihr Wiederherstellungspunkt-Lebenszyklus AWS Backup nicht verwaltet werden. In diesem Fall wird versucht, eine serviceverknüpfte Rolle zu verwenden, um Ihren Lebenszyklus zu verwalten. In einem kleinen Prozentsatz der Fälle funktioniert dies möglicherweise auch nicht, sodass `EXPIRED`-Wiederherstellungspunkte auf Ihrem Speicher verbleiben, was zu unerwünschten Kosten führen kann. Um `EXPIRED`-Wiederherstellungspunkte zu löschen, löschen Sie sie manuell. Gehen Sie dabei wie unter Löschen von Sicherungen beschrieben vor.

Themen

Authentifizierung

Für den Zugriff auf AWS Backup oder die AWS Dienste, die Sie sichern, sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Sie können mit einer der folgenden Arten von Identitäten darauf zugreifen AWS :

- AWS-Konto Root-Benutzer — Wenn Sie sich für registrieren AWS, geben Sie eine E-Mail-Adresse und ein Passwort an, die mit Ihrem AWS Konto verknüpft sind. Dies ist Ihr AWS-Konto -Root-Benutzer Seine Anmeldeinformationen bieten vollständigen Zugriff auf alle Ihre AWS Ressourcen.

  > **Important**
  >
  > Aus Sicherheitsgründen empfehlen wir, den Root-Benutzer nur zum Erstellen eines Administrators zu verwenden. Der Administrator ist ein IAM-Benutzer mit vollständigen Berechtigungen für Ihr AWS-Konto. Anschließend können Sie mit diesem Administratorbenutzer andere IAM-Benutzer und IAM-Rollen mit eingeschränkten Berechtigungen erstellen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM und Erstellen Ihres ersten IAM-Administrator-Benutzers und Ihrer ersten Administratorgruppe im IAM-Benutzerhandbuch.

- IAM-Benutzer - Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten benutzerdefinierten Berechtigungen (z. B. Berechtigungen zum Erstellen eines Sicherungstresors für die Speicherung Ihrer Sicherungen). Sie können einen IAM-Benutzernamen und ein Passwort verwenden, um sich auf sicheren AWS Webseiten wie den AWS Management ConsoleAWSDiskussionsforen oder dem AWS Support Center anzumelden.

  Zusätzlich zu einem Benutzernamen und Passwort können Sie Zugriffsschlüssel für jeden Benutzer erstellen. Sie können diese Schlüssel verwenden, wenn Sie programmgesteuert auf AWS Dienste zugreifen, entweder über eines der verschiedenen SDKs oder mithilfe der AWS Command Line Interface (AWSCLI). Das SDK und die AWS CLI -Tools verwenden die Zugriffsschlüssel, um Ihre Anfrage verschlüsselt zu signieren. Wenn Sie die AWS -Tools nicht nutzen, müssen Sie die Anforderung selbst signieren. Weitere Informationen zur Authentifizierung von Anfragen finden Sie unter Signature Version 4-Signaturprozess im Allgemeine AWS-Referenz.
- IAM-Rolle – Eine IAM-Rolle ist eine weitere IAM-Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Sie ähnelt einem IAM-Benutzer, ist aber nicht mit einer bestimmten Person verknüpft. Mit einer IAM-Rolle können Sie temporäre Zugriffsschlüssel abrufen, die für den Zugriff auf Dienste und Ressourcen verwendet werden können. AWS IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Föderierter Benutzerzugriff — Anstatt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Benutzeridentitäten aus AWS Directory Service Ihrem Unternehmensbenutzerverzeichnis oder einem Web-Identitätsanbieter verwenden. Diese werden als Verbundbenutzer bezeichnet. AWS weist einem Verbundbenutzer eine Rolle zu, wenn Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu Verbundbenutzern finden Sie unter Verbundbenutzer und Rollen im IAM-Leitfaden.
- Kontoübergreifende Verwaltung — Sie können eine IAM-Rolle in Ihrem Konto verwenden, um anderen AWS-Konto Berechtigungen zur Verwaltung der Ressourcen Ihres Kontos zu gewähren. Ein Beispiel finden Sie unter Tutorial: Delegate Access Across AWS-Konten Using IAM Roles im IAM-Benutzerhandbuch.
- AWS Servicezugriff — Sie können eine IAM-Rolle in Ihrem Konto verwenden, um einem AWS Dienst Berechtigungen für den Zugriff auf die Ressourcen Ihres Kontos zu erteilen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.
- Anwendungen, die auf Amazon Elastic Compute Cloud (Amazon EC2) ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2 EC2-Instance ausgeführt werden und API-Anfragen stellen AWS . Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2 Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen zu authentifizieren. Wenn Sie jedoch nicht über die entsprechenden Berechtigungen verfügen, können Sie nicht auf AWS Backup Ressourcen wie Backup-Tresore zugreifen. Sie können auch keine AWS Ressourcen wie Amazon Elastic Block Store (Amazon EBS) -Volumes sichern.

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf eine Ressource werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann AWS Identity and Access Management (IAM-) Identitäten (d. h. Benutzern, Gruppen und

Rollen) Berechtigungsrichtlinien zuordnen. Einige Services unterstützen auch das Anfügen von Berechtigungsrichtlinien an Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorberechtigungen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Beim Erteilen von Berechtigungen entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen die Berechtigungen gelten und welche Aktionen an diesen Ressourcen gestattet werden sollen.

In den folgenden Themen erfahren Sie, wie Zugriffsrichtlinien funktionieren und wie Sie sie verwenden, um Ihre Sicherungen zu schützen.

Themen

- Ressourcen und Operationen
- Ressourceneigentümerschaft
- Festlegen der Richtlinienelemente: Aktionen, Effekte und Prinzipale
- Angeben von Bedingungen in einer Richtlinie
- API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen
- Berechtigungen zum Kopieren von Tags
- Zugriffsrichtlinien

Ressourcen und Operationen

Eine Ressource ist ein Objekt, das innerhalb eines Dienstes existiert. AWS Backup Zu den Ressourcen gehören Backup-Pläne, Backup-Tresore und Backups. Backup ist ein allgemeiner Begriff, der sich auf die verschiedenen Arten von Backup-Ressourcen bezieht, die in existieren AWS. Beispielsweise sind Amazon EBS-Snapshots, Amazon Relational Database Service (Amazon RDS)-Snapshots und Amazon DynamoDB-Sicherungen alle Arten von Backup-Ressourcen.

AWS Backup In werden Backups auch als Wiederherstellungspunkte bezeichnet. Bei der Verwendung AWS Backup arbeiten Sie auch mit den Ressourcen anderer AWS Dienste, die Sie

schützen möchten, wie Amazon EBS-Volumes oder DynamoDB-Tabellen. Diesen Ressourcen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet. ARNs identifizieren Ressourcen eindeutig. AWS Ein ARN ist erforderlich, um eine Ressource im gesamten AWS-System eindeutig anzugeben, z. B. in IAM-Richtlinien oder API-Aufrufen.

In der folgenden Tabelle sind die Ressourcen, Subressourcen, ARN-Format und ein Beispiel für eine eindeutige ID aufgeführt.

AWS Backup Ressourcen-ARNs

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Sicherungsplan	`arn:aws:backup:region:account-id:backup-plan:*`	
Sicherungstresor	`arn:aws:backup:region:account-id:backup-vault:*`	
Wiederherstellungspunkt für Amazon EBS	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Wiederherstellungspunkt für Amazon EC2 EC2-Images	`arn:aws:ec2:region::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Wiederherstellungspunkt für Amazon RDS	`arn:aws:rds:region:account-id:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Wiederherstellungspunkt für Aurora	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Wiederherstellungspunkt für Storage Gateway	`arn:aws:ec2:` *region* `::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
Wiederherstellungspunkt für DynamoDB ohne Erweitertes DynamoDB-Backup	`arn:aws:dynamodb:` *region* `:` *account-id* `:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
Wiederherstellungspunkt für DynamoDB mit aktiviertem Erweitertes DynamoDB-Backup	`arn:aws:backup:` *region* `:` *account-id* `:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`
Wiederherstellungspunkt für Amazon EFS	`arn:aws:backup:` *region* `:` *account-id* `:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Wiederherstellungspunkt für Amazon FSx	`arn:aws:fsx:` *region* `:` *account-id* `:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Wiederherstellungspunkt für virtuelle Maschinen	`arn:aws:backup:` *region* `:` *account-id* `:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`
Wiederherstellungspunkt für kontinuierliche Amazon S3-Sicherung	`arn:aws:backup:` *region* `:` *account-id* `:recovery-point:*`	*my-bucket* `-5ec207d0`
Wiederherstellungspunkt für regelmäßige S3-Sicherung	`arn:aws:backup:` *region* `:` *account-id* `:recovery-point:*`	*my-bucket* `-20211231900000-5ec207d0`

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Erholungspunkt für Amazon DocumentDB	`arn:aws:rds: region:account-id :cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Erholungspunkt für Neptune	`arn:aws:rds: region:account-id :cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Erholungspunkt für Amazon Redshift	`arn:aws:redshift: region:account-id :snapshot : resource/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Erholungspunkt für Amazon Timestream	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
Erholungspunkt für die Vorlage AWS CloudFormation	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Erholungspunkt für die SAP HANA-Datenbank auf einer Amazon EC2 EC2-Instance	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, haben alle Wiederherstellungspunkte in diesem Format, sodass Sie leichter Berechtigungsrichtlinien anwenden können, um diese Wiederherstellungspunkte zu schützen`arn:aws:backup:region:account-id:recovery-point:*`. Informationen zu den Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, finden Sie in diesem Abschnitt der Verfügbarkeit von Features nach Ressource Tabelle.

AWS Backup bietet eine Reihe von Vorgängen für die Arbeit mit AWS Backup Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter AWS Backup Aktionen.

Ressourceneigentümerschaft

Der AWS-Konto besitzt die Ressourcen, die im Konto erstellt wurden, unabhängig davon, wer die Ressourcen erstellt hat. Insbesondere ist der Ressourcenbesitzer derjenige AWS-Konto der Prinzipalentität (d. h. der AWS-Konto Root-Benutzer, ein IAM-Benutzer oder eine IAM-Rolle), die die Anfrage zur Ressourcenerstellung authentifiziert. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie Ihre AWS-Konto Root-Benutzeranmeldedaten verwenden, AWS-Konto um einen Backup-Tresor zu erstellen, sind Sie AWS-Konto der Eigentümer des Tresors.
- Wenn Sie in Ihrem einen IAM-Benutzer erstellen AWS-Konto und diesem Benutzer die Berechtigung zum Erstellen eines Backup-Tresors erteilen, kann der Benutzer einen Backup-Tresor erstellen. Eigentümer der Ressource der Sicherungstresorressource ist jedoch Ihr AWS -Konto, zu dem der Benutzer gehört.
- Wenn Sie in Ihrem System eine IAM-Rolle AWS-Konto mit den Berechtigungen zum Erstellen eines Backup-Tresors erstellen, kann jeder, der diese Rolle übernehmen kann, einen Tresor erstellen. Ihre AWS-Konto, zu der die Rolle gehört, besitzt die Backup-Vault-Ressource.

Festlegen der Richtlinienelemente: Aktionen, Effekte und Prinzipale

Für jede AWS Backup Ressource (siehe Ressourcen und Operationen) definiert der Dienst eine Reihe von API-Operationen (siehe Aktionen). AWS Backup Definiert eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können, um Berechtigungen für diese API-Operationen zu gewähren. Für das Durchführen einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Weitere Informationen finden Sie unter Ressourcen und Operationen.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten.
- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den

Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.

- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien).

Weitere Informationen zur Syntax sowie Beschreibungen von IAM-Richtlinien finden Sie in der -IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine Tabelle mit allen AWS Backup API-Aktionen finden Sie unterAPI-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

AWS Backup definiert seinen eigenen Satz von Bedingungsschlüsseln. Eine Liste der AWS Backup Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Backup in der Service Authorization Reference.

API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

Wenn Sie die Zugriffskontrolle einrichten und eine Berechtigungsrichtlinie für eine IAM-Identität (identitätsbasierte Richtlinie) verfassen, können Sie die folgende Liste als Referenz verwenden. Die enthält die einzelnen AWS Backup API-Operationen, die entsprechenden Aktionen, für die Sie Berechtigungen zur Ausführung der Aktion erteilen können, und die AWS Ressource, für die Sie die Berechtigungen erteilen können. Die Aktionen geben Sie im Feld `Action` und den Wert für die Ressource im Feld `Resource` der Richtlinie an. Wenn das `Resource`-Feld leer ist, können Sie den Platzhalter (`*`) verwenden, um alle Ressourcen einzubeziehen.

Sie können in Ihren AWS Backup Richtlinien AWS allgemeine Bedingungsschlüssel verwenden, um Bedingungen auszudrücken. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter Verfügbare Schlüssel im IAM-Benutzerhandbuch.

[1] Verwendet die bestehende Tresorzugriffsrichtlinie.

[2] Informationen AWS Backup Ressourcen-ARNs zu ressourcenspezifischen Wiederherstellungspunkt-ARNs finden Sie unter.

[3] `StartRestoreJob` muss das Schlüssel-Wert-Paar in den Metadaten für die Ressource enthalten. Rufen Sie die `GetRecoveryPointRestoreMetadata`-API auf, um die Metadaten der Ressource abzurufen.

[4] Bei bestimmten Ressourcentypen muss die Rolle, die das Backup durchführt, über eine bestimmte Tagging-Berechtigung verfügen, `backup:TagResource` wenn Sie entweder ursprüngliche Ressourcen-Tags in Ihr Backup aufnehmen oder einem Backup zusätzliche Tags hinzufügen möchten. Für alle Backups, bei denen ein ARN mit beginnt, `arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:` oder für Backups, die kontinuierlich sind, ist diese Genehmigung erforderlich. `backup:TagResource`Die Genehmigung muss beantragt werden für `"`*`resourcetype`*`": "arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*"`

Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup in der Service-Autorisierungs-Referenz.

Berechtigungen zum Kopieren von Tags

Bei AWS Backup der Ausführung eines Sicherungs- oder Kopierauftrags wird versucht, die Tags von Ihrer Quellressource (oder von Ihrem Wiederherstellungspunkt im Fall einer Kopie) auf Ihren Wiederherstellungspunkt zu kopieren.

> **Note**
>
> AWS Backup kopiert Tags bei Wiederherstellungsaufträgen nicht nativ. Eine ereignisgesteuerte Architektur, die Tags bei Wiederherstellungsaufträgen kopiert, finden Sie unter So behalten Sie Ressourcen-Tags in AWS Backup Wiederherstellungsaufträgen bei.

AWS Backup Aggregiert während eines Sicherungs- oder Kopierauftrags die Tags, die Sie in Ihrem Backup-Plan (oder Kopierplan oder On-Demand-Backup) angeben, mit den Tags aus Ihrer

Quellressource. AWS Erzwingt jedoch ein Limit von 50 Tags pro Ressource, das AWS Backup nicht überschritten werden darf. Wenn ein Sicherungs- oder Kopierauftrag Tags aus dem Plan und der Quellressource zusammenfasst, werden möglicherweise insgesamt mehr als 50 Tags erkannt, der Job kann nicht abgeschlossen werden und der Job schlägt fehl. Dies steht im Einklang mit den bewährten Methoden für AWS das Tagging in allen Bereichen. Weitere Informationen finden Sie unter Tag-Limits im AWS Allgemeinen Referenzhandbuch.

- Ihre Ressource hat mehr als 50 Tags, nachdem Sie Ihre Backup-Job-Tags mit Ihren Quellressourcen-Tags zusammengefasst haben. AWS unterstützt bis zu 50 Tags pro Ressource. Weitere Informationen finden Sie unter Tag-Limits.
- Der IAM-Rolle, der Sie zur Verfügung stellen, AWS Backup sind nicht berechtigt, die Quell-Tags zu lesen oder die Ziel-Tags festzulegen. Weitere Informationen und Beispiele zu IAM-Rollenrichtlinien finden Sie unter Managed Policies.

Sie können Ihren Sicherungsplan verwenden, um Tags zu erstellen, die Ihren Quellressourcen-Tags widersprechen. Wenn die beiden in Konflikt geraten, haben die Tags aus Ihrem Sicherungsplan Vorrang. Verwenden Sie diese Technik, wenn Sie es vorziehen, keinen Tag-Wert aus Ihrer Quellressource zu kopieren. Geben Sie mithilfe Ihres Sicherungsplans denselben Tag-Schlüssel, aber einen anderen oder leeren Wert an.

Erforderliche Berechtigungen zum Zuweisen von Tags zu Sicherungen

Ressourcentyp	Erforderliche Berechtigung
Amazon-EFS-Dateisystem	`elasticfilesystem:DescribeTags`
Amazon FSx-Dateisystem	`fsx:ListTagsForResource`
Amazon RDS-Datenbank und Amazon Aurora-Cluster	`rds:AddTagsToResource` `rds:ListTagsForResource`
Storage Gateway-Volume	`storagegateway:ListTagsForResource`
Amazon EC2-Instance und Amazon EBS-Volume	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB unterstützt das Zuweisen von Tags zu Sicherungen nur, wenn Sie zuerst Erweitertes DynamoDB-Backup aktivieren.

Wenn ein Amazon EC2 EC2-Backup einen Image Recovery Point und eine Reihe von Snapshots erstellt, werden Tags in das resultierende AMI AWS Backup kopiert. AWS Backup kopiert auch die Tags von den Volumes, die der Amazon EC2 EC2-Instance zugeordnet sind, in die resultierenden Snapshots.

Zugriffsrichtlinien

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. An eine IAM-Identität angefügte Richtlinien werden als identitätsbasierte Richtlinien (oder IAM-Richtlinien) bezeichnet. Mit einer Ressource verknüpfte Richtlinien werden als ressourcenbasierte Richtlinien bezeichnet. AWS Backup unterstützt sowohl identitätsbasierte Richtlinien als auch ressourcenbasierte Richtlinien.

> **Note**
>
> In diesem Abschnitt wird die Verwendung von IAM im Kontext von beschrieben. AWS Backup Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Informationen zur IAM-Richtliniensyntax und Beschreibungen finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Identitätsbasierte Richtlinien sind Richtlinien, die Sie IAM-Identitäten anfügen können, etwa Benutzern oder Rollen. Sie können beispielsweise eine Richtlinie definieren, die es einem Benutzer ermöglicht, AWS Ressourcen einzusehen und zu sichern, ihn aber daran hindert, Backups wiederherzustellen.

Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie im Thema Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Informationen zur Verwendung von IAM-Richtlinien für die Steuerung des Zugriffs auf Sicherungen finden Sie unter .

Ressourcenbasierte Richtlinien

AWS Backup unterstützt ressourcenbasierte Zugriffsrichtlinien für Backup-Tresore. Damit können Sie eine Zugriffsrichtlinie definieren, die steuern kann, welche Benutzer welche Art von Zugriff

auf eine der in einem Sicherungstresor organisierten Sicherungen haben. Ressourcenbasierte Zugriffsrichtlinien für Sicherungstresore bieten eine einfache Möglichkeit zur Steuerung des Zugriffs auf Ihre Sicherungen.

Zugriffsrichtlinien für Backup-Tresore steuern den Benutzerzugriff, wenn Sie AWS Backup APIs verwenden. Auf einige Sicherungstypen, z. B. Amazon Elastic Block Store (Amazon EBS) und Amazon Relational Database Service (Amazon RDS), kann auch über die APIs dieser Services zugegriffen werden. Sie können separate Zugriffsrichtlinien in IAM einrichten, die den Zugriff auf diese APIs steuern, um den Zugriff auf Sicherungen vollständig kontrollieren zu können.

Informationen zur Erstellung einer Zugriffsrichtlinie für Sicherungstresore finden Sie unter Festlegen von Zugriffsrichtlinien für Backup-Tresore.

IAM-Servicerollen

Eine AWS Identity and Access Management (IAM-) Rolle ähnelt einem Benutzer insofern, als es sich um eine AWS Identität mit Berechtigungsrichtlinien handelt, die festlegen, wofür die Identität zuständig ist und was nicht. AWS Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen. Eine Servicerolle ist eine Rolle, die ein AWS Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Als Service, der für Sie Sicherungsoperationen durchführt, erfordert AWS Backup die Übergabe einer Rolle, die es annehmen soll, wenn es für Sie Sicherungsoperationen durchführt. Weitere Informationen zu IAM-Rollen finden Sie unter IAM-Rollen im IAM-Benutzerhandbuch.

Die Rolle, zu der Sie übergehen, AWS Backup muss über eine IAM-Richtlinie mit den Berechtigungen verfügen, die es ermöglichen AWS Backup , Aktionen im Zusammenhang mit Backup-Vorgängen durchzuführen, wie z. B. das Erstellen, Wiederherstellen oder Ablaufen von Backups. Für jeden der unterstützten AWS Dienste sind unterschiedliche Berechtigungen erforderlich. AWS Backup Die Rolle muss außerdem als vertrauenswürdige Entität AWS Backup aufgeführt sein, sodass AWS Backup die Rolle übernommen werden kann.

Wenn Sie einem Backup-Plan Ressourcen zuweisen oder wenn Sie bei Bedarf eine Sicherung, Kopie oder Wiederherstellung durchführen, müssen Sie eine Servicerolle übergeben, die Zugriff auf die Ausführung der zugrunde liegenden Operationen auf den angegebenen Ressourcen hat. AWS Backup verwendet diese Rolle, um Ressourcen in Ihrem Konto zu erstellen, zu kennzeichnen und zu löschen.

Verwendung von AWS Rollen zur Steuerung des Zugriffs auf Backups

Sie können Rollen verwenden, um den Zugriff auf Ihre Sicherungen zu steuern, indem Sie eng gefasste Rollen definieren und angeben, wer diese Rolle an AWS Backupübergeben kann. Sie könnten beispielsweise eine Rolle erstellen, die nur Berechtigungen zum Sichern von Amazon Relational Database Service (Amazon RDS) -Datenbanken gewährt und nur Besitzern von Amazon RDS-Datenbanken die Erlaubnis erteilt, diese Rolle weiterzugeben. AWS Backup AWS Backup bietet mehrere vordefinierte verwaltete Richtlinien für jeden der unterstützten Dienste. Sie können diese verwalteten Richtlinien an Rollen anfügen, die Sie erstellen. Dies macht es einfacher, dienstspezifische Rollen zu erstellen, die über die richtigen Berechtigungen verfügen, die AWS Backup benötigt werden.

Weitere Informationen zu AWS verwalteten Richtlinien für finden Sie AWS Backup unterVerwaltete Richtlinien für AWS Backup.

Standard-Servicerolle für AWS Backup

Wenn Sie die AWS Backup Konsole zum ersten Mal verwenden, können Sie wählen, ob Sie eine Standard-Servicerolle für Sie AWS Backup erstellen möchten. Diese Rolle verfügt über die erforderlichen AWS Backup Berechtigungen, um in Ihrem Namen Backups zu erstellen und wiederherzustellen.

> **Note**
>
> Die Standardrolle wird automatisch erstellt, wenn Sie AWS Management Console verwenden. Sie können die Standardrolle mit AWS Command Line Interface (AWS CLI) erstellen, dies muss jedoch manuell erfolgen.

Wenn Sie lieber benutzerdefinierte Rollen verwenden möchten, z. B. separate Rollen für verschiedene Ressourcentypen, können Sie dies auch tun und Ihre benutzerdefinierten Rollen an AWS Backupübergeben. Beispiele für Rollen, die Sicherung und Wiederherstellung für einzelne Ressourcentypen ermöglichen, finden Sie in der Kundenverwaltete Richtlinien-Tabelle.

Die Standarddienstrolle ist benannt`AWSBackupDefaultServiceRole`. Diese Servicerolle enthält zwei verwaltete Richtlinien AWSBackupServiceRolePolicyForBackupund AWSBackupServiceRolePolicyForRestores.

`AWSBackupServiceRolePolicyForBackup`beinhaltet eine IAM-Richtlinie, die AWS Backup Berechtigungen zur Beschreibung der zu sichernden Ressource gewährt und die Möglichkeit bietet,

ein Backup unabhängig vom AWS KMS Schlüssel, mit dem es verschlüsselt wurde, zu erstellen, zu löschen, zu beschreiben oder Tags hinzuzufügen.

`AWSBackupServiceRolePolicyForRestores`beinhaltet eine IAM-Richtlinie, die AWS Backup Berechtigungen zum Erstellen, Löschen oder Beschreiben der neuen Ressource, die aus einem Backup erstellt wird, gewährt, unabhängig vom AWS KMS Schlüssel, mit dem sie verschlüsselt wurde. Dazu kommen die Berechtigungen zum Markieren der neu erstellten Ressource mit Tags.

Um eine Amazon EC2-Instance wiederherzustellen, müssen Sie eine neue Instance starten.

Erstellen der Standardservicerolle mithilfe der Konsole

Durch bestimmte Aktionen, die Sie in der AWS Backup Konsole ausführen, wird die AWS Backup Standard-Servicerolle erstellt.

Um die AWS Backup Standard-Servicerolle in Ihrem AWS Konto zu erstellen

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Um die Rolle für Ihr Konto zu erstellen, weisen Sie entweder Ressourcen einem Sicherungsplan zu oder erstellen Sie ein On-Demand-Backup.

    a. Erstellen Sie einen Sicherungsplan und weisen Sie der Sicherung Ressourcen zu. Siehe Eine geplante Sicherung erstellen.

    b. Sie können aber auch eine On-Demand-Sicherung erstellen. Siehe So erstellen Sie eine On-Demand-Sicherung.
3. Stellen Sie sicher, dass Sie das `AWSBackupDefaultServiceRole` in Ihrem Konto anhand der folgenden Schritte erstellt haben:

    a. Warten Sie ein paar Minuten. Weitere Informationen finden Sie unter Meine Änderungen sind nicht immer sofort sichtbar im AWS Identity and Access Management-Benutzerhandbuch.

    b. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

    c. Klicken Sie im linken Navigationsmenü auf Roles (Rollen).

    d. Geben Sie in das Suchfeld `AWSBackupDefaultServiceRole` ein. Wenn diese Auswahl vorhanden ist, haben Sie die AWS Backup Standardrolle erstellt und dieses Verfahren abgeschlossen.

e. Falls `AWSBackupDefaultServiceRole` immer noch nicht angezeigt wird, fügen Sie entweder dem IAM-Benutzer oder der IAM-Rolle, die Sie für den Zugriff auf die Konsole verwenden, die folgenden Berechtigungen hinzu.

```
{
  "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":"*"
    }
  ]
}
```

Für chinesische Regionen ersetzen Sie *aws* durch *aws-cn*. Ersetzen Sie *aws* für AWS GovCloud (US) Regionen durch *aws-us-gov*.

f. Wenn Sie Ihrem IAM-Benutzer oder Ihrer IAM-Rolle keine Berechtigungen hinzufügen können, bitten Sie Ihren Administrator, manuell eine Rolle mit einem anderen Namen als `AWSBackupDefaultServiceRole` zu erstellen und diese Rolle diesen verwalteten Richtlinien zuzuweisen:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Verwaltete Richtlinien für AWS Backup

Verwaltete Richtlinien sind eigenständige identitätsbasierte Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Wenn Sie eine Richtlinie an eine Auftraggeber-Entität anfügen, gewähren Sie ihr die in der Richtlinie festgelegten Berechtigungen.

AWS verwaltete Richtlinien werden von erstellt und verwaltet. AWS Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist.

Mit vom Kunden verwalteten Richtlinien können Sie den Zugriff auf Backups genau festlegen. AWS Backup Sie können sie beispielsweise verwenden, um Ihrem Datenbank-Backup-Administrator Zugriff auf Amazon RDS-Sicherungen zu gewähren, aber nicht auf Amazon EFS-Sicherungen.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwaltete Richtlinien.

AWS verwaltete Richtlinien

AWS Backup bietet die folgenden AWS verwalteten Richtlinien für allgemeine Anwendungsfälle. Diese Richtlinien erleichtern die Definition der erforderlichen Berechtigungen und die Steuerung des Zugriffs auf Ihre Sicherungen. Es gibt zwei Typen von verwalteten Richtlinien. Ein Typ ist so konzipiert, dass er Benutzer zugewiesen wird, um deren Zugriff auf AWS Backup zu steuern. Der andere Typ verwalteter Richtlinien wird Rollen zugewiesen, die Sie an AWS Backupübergeben. In der folgenden Tabelle sind alle verwalteten Richtlinien und ihre Definitionen aufgeführt, die AWS Backup bereitstellt. Sie finden diese verwalteten Richtlinien im Abschnitt Policies (Richtlinien) der -Konsole.

Richtlinien

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup

- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Diese Richtlinie gewährt Benutzern die Erlaubnis, Kontrollen und Frameworks zu erstellen, die ihre Erwartungen an AWS Backup Ressourcen und Aktivitäten definieren, und AWS Backup Ressourcen und Aktivitäten anhand ihrer definierten Kontrollen und Frameworks zu überprüfen. Diese Richtlinie gewährt Benutzern AWS Config und ähnlichen Diensten die Erlaubnis, die Erwartungen der Benutzer zu beschreiben und die Prüfungen durchzuführen.

Diese Richtlinie gewährt auch Berechtigungen zur Übermittlung von Auditberichten an Amazon S3 und ähnliche Dienste und ermöglicht es Benutzern, ihre Auditberichte zu finden und zu öffnen.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupAuditAccessin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupDataTransferAccess

Diese Richtlinie bietet Berechtigungen für die Datenübertragungs-APIs der AWS Backup Speicherebene, sodass der AWS Backint-Agent die Backup-Datenübertragung mit der AWS Backup Speicherebene abschließen kann. Sie können diese Richtlinie an Rollen anhängen, die von Amazon EC2 EC2-Instances übernommen werden, auf denen SAP HANA mit dem Backint-Agenten ausgeführt wird.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupDataTransferAccessin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupFullAccess

Der Backup-Administrator hat vollen Zugriff auf alle AWS Backup Vorgänge wie das Erstellen oder Bearbeiten von Backup-Plänen, das Zuweisen von AWS Ressourcen zu Backup-Plänen und das Wiederherstellen von Backups. Sicherungsadministratoren sind verantwortlich für die Festlegung

und Durchsetzung der Sicherungs-Compliance durch die Definition von Sicherungsplänen, die den geschäftlichen und regulatorischen Anforderungen ihrer Organisation entsprechen. Backup-Administratoren stellen außerdem sicher, dass die AWS Ressourcen ihrer Organisation dem entsprechenden Plan zugewiesen sind.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupFullAccessin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Die Berechtigungen für diese Richtlinie finden Sie in der Referenz zu AWS verwalteten Richtlinien.

AWSBackupOperatorAccess

Sicherungsoperatoren sind Benutzer, die dafür verantwortlich sind, sicherzustellen, dass die unter ihrer Verantwortung stehenden Ressourcen korrekt gesichert werden. Backup-Operatoren sind berechtigt, den Backup-Plänen, die der Backup-Administrator erstellt, AWS Ressourcen zuzuweisen. Sie sind auch berechtigt, On-Demand-Backups ihrer AWS Ressourcen zu erstellen und die Aufbewahrungsdauer von On-Demand-Backups zu konfigurieren. Sicherungsoperatoren sind nicht berechtigt, Sicherungspläne zu erstellen oder zu bearbeiten oder geplante Sicherungen nach ihrer Erstellung zu löschen. Sicherungsoperatoren können Sicherungen wiederherstellen. Sie können die Ressourcentypen einschränken, die ein Sicherungsoperator einem Sicherungsplan oder einer Wiederherstellung aus einer Sicherung zuweisen kann. Sie tun dies, indem Sie zulassen, dass nur bestimmte Servicerollen übergeben werden AWS Backup , die über Berechtigungen für einen bestimmten Ressourcentyp verfügen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSBackupOperatorAccessin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupOrganizationAdminAccess

Der Organisationsadministrator hat vollen Zugriff auf alle AWS Organizations Vorgänge, darunter das Erstellen, Bearbeiten oder Löschen von Backup-Richtlinien, das Zuweisen von Backup-Richtlinien zu Konten und Organisationseinheiten und das Überwachen der Backup-Aktivitäten innerhalb der Organisation. Es ist Aufgabe der Organisationsadministratoren, die Konten in ihrer Organisation zu schützen, indem sie Sicherungsrichtlinien definieren und zuweisen, die die geschäftlichen und behördlichen Anforderungen ihrer Organisation erfüllen.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupOrganizationAdminAccessin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupRestoreAccessForSAPHANA

Diese Richtlinie gewährt die AWS Backup Erlaubnis, ein Backup von SAP HANA auf Amazon EC2 wiederherzustellen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSBackupRestoreAccessForSAPHANAin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupServiceLinkedRolePolicyForBackup

Diese Richtlinie ist der dienstbezogenen Rolle mit dem Namen zugeordnetAWSServiceRoleforBackup, sodass Sie in Ihrem Namen AWS Dienste aufrufen können, AWS Backup um Ihre Backups zu verwalten. Weitere Informationen finden Sie unter the section called “Sichern und Kopieren”.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceLinkedRolePolicyforBackupin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupServiceLinkedRolePolicyForBackupTest

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceLinkedRolePolicyForBackupTestin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupServiceRolePolicyForBackup

Bietet AWS Backup Berechtigungen zum Erstellen von Backups aller unterstützten Ressourcentypen in Ihrem Namen.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceRolePolicyForBackupin der Referenz zu AWS verwalteten Richtlinien.

AWSBackupServiceRolePolicyForRestores

Bietet AWS Backup Berechtigungen zum Wiederherstellen von Backups aller unterstützten Ressourcentypen in Ihrem Namen.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceRolePolicyForRestoresin der Referenz zu AWS verwalteten Richtlinien.

Für EC2-Instance-Wiederherstellungen müssen Sie außerdem die folgenden Berechtigungen angeben, um die EC2-Instance zu starten:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

Diese Richtlinie enthält die Berechtigungen, die für AWS Backup die Sicherung eines beliebigen S3-Buckets erforderlich sind. Dies beinhaltet den Zugriff auf alle Objekte in einem Bucket und alle zugehörigen AWS KMS Schlüssel.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceRolePolicyForS3Backupin der Referenz für AWS verwaltete Richtlinien.

AWSBackupServiceRolePolicyForS3Restore

Diese Richtlinie enthält Berechtigungen, die für die AWS Backup Wiederherstellung eines S3-Backups in einem Bucket erforderlich sind. Dazu gehören Lese- und Schreibberechtigungen für die Buckets sowie die Verwendung beliebiger AWS KMS Schlüssel für S3-Operationen.

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceRolePolicyForS3Restorein der Referenz zu AWS verwalteten Richtlinien.

AWSServiceRolePolicyForBackupReports

AWS Backup verwendet diese Richtlinie für die AWSServiceRoleForBackupReportsdienstbezogene Rolle. Diese dienstbezogene Rolle gibt Ihnen AWS Backup die Möglichkeit, die Übereinstimmung Ihrer Backup-Einstellungen, Jobs und Ressourcen mit Ihren Frameworks zu überwachen und darüber zu berichten.

Die Berechtigungen für diese Richtlinie finden Sie AWSServiceRolePolicyForBackupReportsin der Referenz zu AWS verwalteten Richtlinien.

AWSServiceRolePolicyForBackupRestoreTesting

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSServiceRolePolicyForBackupRestoreTestingin der Referenz zu AWS verwalteten Richtlinien.

Kundenverwaltete Richtlinien

In den folgenden Abschnitten werden die empfohlenen Sicherungs- und Wiederherstellungsberechtigungen für die Anwendung AWS-Services und Drittanbieteranwendung beschrieben, die von unterstützt wird AWS Backup. Sie können bei der Erstellung Ihrer eigenen Richtliniendokumente die vorhandenen AWS verwalteten Richtlinien als Modell verwenden und diese dann anpassen, um den Zugriff auf Ihre AWS Ressourcen weiter einzuschränken.

Amazon Aurora

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Wiederherstellung

Beginnen Sie mit der `RDSPermissions` Aussage von AWSBackupServiceRolePolicyForRestores.

Amazon-DynamoDB

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Wiederherstellung

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForRestores:

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamoDBRestorePermissions
- KMSPermissions

Amazon EBS

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- EBSResourcePermissions
- EBSTagAndDeletePermissions
- EBSCopyPermissions
- EBSSnapshotTierPermissions
- GetResourcesPermissions
- BackupVaultPermissions

Wiederherstellung

Beginnen Sie mit der EBSPermissions Aussage von AWSBackupServiceRolePolicyForRestores.

Fügen Sie die folgende Anweisung hinzu.

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

Wiederherstellung

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForRestores:

- EBSPermissions
- EC2DescribePermissions
- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

Fügen Sie die folgende Anweisung hinzu.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- EFSPermissions
- GetResourcesPermissions

- `BackupVaultPermissions`

Wiederherstellung

Beginnen Sie mit der `EFSPermissions` Aussage von AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Wiederherstellung

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`
- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Wiederherstellung

Beginnen Sie mit der `RDSPermissions` Aussage von AWSBackupServiceRolePolicyForRestores.

Amazon S3

Backup

Beginnen Sie mit AWSBackupServiceRolePolicyForS3Backup.

Fügen Sie die `BackupVaultCopyPermissions` Anweisungen `BackupVaultPermissions` und hinzu, wenn Sie Backups auf ein anderes Konto kopieren müssen.

Wiederherstellung

Beginnen Sie mit AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Backup

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Fügen Sie die folgende Anweisung hinzu.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Wiederherstellung

Beginnen Sie mit den folgenden Aussagen von AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Virtuelle Maschine

Backup

Beginnen Sie mit der `BackupGatewayBackupPermissions` Aussage von AWSBackupServiceRolePolicyForBackup.

Wiederherstellung

Beginnen Sie mit der `GatewayRestorePermissions` Aussage von AWSBackupServiceRolePolicyForRestores.

Verschlüsseltes Backup

Um eine verschlüsselte Sicherung wiederherzustellen, führen Sie einen der folgenden Schritte aus:

- Fügen Sie Ihre Rolle der Zulassungsliste für die AWS KMS Schlüsselrichtlinie hinzu
- Fügen Sie Ihrer IAM-Rolle für AWSBackupServiceRolePolicyForRestoresWiederherstellungen die folgenden Anweisungen von hinzu:
  - `KMSDescribePermissions`
  - `KMSPermissions`

- `KMSCreateGrantPermissions`

Richtlinien-Updates für AWS Backup

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien, die AWS Backup seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden.

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie `backup:TagResource` eine Berechtigung hinzugefügt. Die Genehmigung ist erforderlich, um bei der Erstellung eines Wiederherstellungspunkts Tagging-Berechtigungen zu erhalten.	17. Mai 2024
AWSBackupServiceRolePolicyForS3Backup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Dieser Richtlinie wurde `backup:TagResource` eine Genehmigung hinzugefügt. Die Genehmigung ist erforderlich, um bei der Erstellung eines Wiederherstellungspunkts Tagging-Berechtigungen zu erhalten.	17. Mai 2024
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Dieser Richtlinie wurde `backup:TagResource` eine Genehmigung hinzugefügt. Die Genehmigung ist erforderlich, um bei der Erstellung	17. Mai 2024

Änderung	Beschreibung	Datum
	eines Wiederherstellungspunkts Tagging-Berechtigungen zu erhalten.	
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die Erlaubnis wurde hinzugefügt `rds:DeleteDBInstanceAutomatedBackups` . Diese Genehmigung ist erforderlich AWS Backup , um kontinuierliche Backups und point-in-time-restore Amazon RDS-Instances zu unterstützen.	1. Mai 2024
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat den Amazon-Ressourcennamen (ARN) mit Genehmigung `storagegateway:ListVolumes` von bis aktualisiert `arn:aws:storagegateway:*:*:gateway/*` , * um einer Änderung des Storage Gateway Gateway-API-Modells Rechnung zu tragen.	1. Mai 2024

Änderung	Beschreibung	Datum
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat den Amazon-Ressourcennamen (ARN) mit Genehmigung `storagegateway:ListVolumes` von bis aktualisiert `arn:aws:storagegateway:*:*:gateway/*` , * um einer Änderung des Storage Gateway Gateway-API-Modells Rechnung zu tragen.	1. Mai 2024

Änderung	Beschreibung	Datum
AWSServiceRolePolicyForBackupRestoreTesting – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen hinzugefügt, um Wiederherstellungspunkte und geschützte Ressourcen zu beschreiben und aufzulisten, um Wiederherstellungstestpläne durchzuführen: `backup:DescribeRecoveryPoint` `backup:DescribeProtectedResource` ,`backup:ListProtectedResources` , und`backup:ListRecoveryPointsByResource` . Die Berechtigung `ec2:DescribeSnapshotTierStatus` zur Unterstützung von Amazon EBS-Archiv-Tier-Speicher wurde hinzugefügt. Die Erlaubnis `rds:DescribeDBClusterAutomatedBackups` zur Unterstützung kontinuierlicher Amazon Aurora Aurora-Backups wurde hinzugefügt. Die folgenden Berechtigungen wurden hinzugefügt, um Wiederherstellungstests von Amazon Redshift Redshift-Backups zu unterstützen: `redshift:DescribeC`	14. Februar 2024

Änderung	Beschreibung	Datum
	`lusters undredshift: DeleteCluster` . Es wurde die Erlaubnis `timestream:DeleteT able` hinzugefügt, Wiederher stellungstests von Amazon Timestream-Backups zu unterstützen.	
AWSBackupServiceRo lePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigungen `ec2:DescribeSnapsh otTierStatus` und wurden hinzugefü gt`ec2:RestoreSnapsho tTier` . Diese Berechtigungen sind erforderlich, damit Benutzer die Möglichkeit haben, Amazon EBS-Ressourcen, die mit gespeichert wurden, AWS Backup aus dem Archivspe icher wiederherzustellen. Für EC2-Instance-Wiede rherstellungen müssen Sie außerdem die in der folgenden Richtlinienanweisu ng gezeigten Berechtigungen angeben, um die EC2-Insta nce zu starten:	8. November 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die Berechtigungen `ec2:DescribeSnapshotTierStatus` und `ec2:ModifySnapshotTier` die Unterstützung einer zusätzlichen Speicheroption für gesicherte Amazon EBS-Ressourcen hinzugefügt, die auf die Archivspeicherebene übertragen werden sollen. Diese Berechtigungen sind erforderlich, damit Benutzer die Möglichkeit haben, Amazon EBS-Ressourcen, die zusammen gespeichert sind, AWS Backup auf Archivspeicher umzustellen.	8. November 2023

Änderung	Beschreibung	Datum
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die Berechtigungen `ec2:DescribeSnapshotTierStatus` und `ec2:ModifySnapshotTier` die Unterstützung einer zusätzlichen Speicheroption für gesicherte Amazon EBS-Ressourcen hinzugefügt, die auf die Archivspeicherebene übertragen werden sollen. Diese Berechtigungen sind erforderlich, damit Benutzer die Möglichkeit haben, Amazon EBS-Ressourcen, die zusammen gespeichert sind, AWS Backup auf Archivspeicher umzustellen. Die Berechtigungen `rds:DescribeDBClusterSnapshots` und wurden hinzugefügt`rds:RestoreDBClusterToPointInTime` , was für PITR (point-in-time Wiederherstellungen) von Aurora-Clustern erforderlich ist.	

Änderung	Beschreibung	Datum
AWSServiceRolePolicyForBackupRestoreTesting – Neue Richtlinie.	Stellt die für die Durchführung von Wiederherstellungstests erforderlichen Berechtigungen bereit. Die Berechtigungen umfassen die Aktionen `list, read, and write` für die folgenden Services, die in Wiederherstellungstests aufgenommen werden sollen: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx für ONTAP, FSx für OpenZFS, Amazon Neptune, Amazon RDS und Amazon S3.	8. November 2023
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	`restore-testing.backup.amazonaws.com` wurde `IamPassRolePermissions` und `IamCreateServiceLinkedRolePermissions` hinzugefügt. Dieser Zusatz ist erforderlich AWS Backup , um Wiederherstellungstests im Auftrag von Kunden durchzuführen.	8. November 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigungen `rds:DescribeDBClusterSnapshots` und wurden hinzugefügt `rds:RestoreDBClusterToPointInTime` , was für PITR (point-in-time Wiederherstellungen) von Aurora-Clustern erforderlich ist.	6. September 2023
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung wurde hinzugefügt `rds:DescribeDBClusterAutomatedBackups` , die für die kontinuierliche Sicherung und point-in-time Wiederherstellung von Aurora-Clustern erforderlich ist.	6. September 2023
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigung wurde hinzugefügt `rds:DescribeDBClusterAutomatedBackups` , die für die kontinuierliche Sicherung und point-in-time Wiederherstellung von Aurora-Clustern erforderlich ist.	6. September 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die Erlaubnis wurde hinzugefügt `rds:DescribeDBClusterAutomatedBackups` . Diese Genehmigung ist für die AWS Backup Unterstützung der kontinuierlichen Sicherung und point-in-time Wiederherstellung von Aurora-Clustern erforderlich. Es wurde die Erlaubnis `rds:DeleteDBClusterAutomatedBackups` hinzugefügt, AWS Backup Lifecycle das Löschen und Trennen von kontinuierlichen Amazon Aurora Aurora-Wiederherstellungspunkten zu gestatten, wenn ein Aufbewahrungszeitraum abgelaufen ist. Diese Genehmigung ist für den Aurora-Wiederherstellungspunkt erforderlich, um einen Übergang in einen `EXIPIRED`-Status zu verhindern. Die Erlaubnis `rds:ModifyDBCluster` , mit Aurora-Clustern AWS Backup zu interagieren, wurde hinzugefügt. Dieser Zusatz ermöglicht es Benutzern, kontinuierliche Sicherungen auf der Grundlage der gewünschten	6. September 2023

Änderung	Beschreibung	Datum
	Konfigurationen zu aktivieren oder zu deaktivieren.	
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde die Aktion hinzugefügt `tram:GetResourceShareAssociations` , um dem Benutzer die Erlaubnis zu erteilen, Ressourcenfreigabe zuordnungen für einen neuen Tresortyp abzurufen.	08. August 2023
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde die Aktion hinzugefügt `tram:GetResourceShareAssociations` , um dem Benutzer die Erlaubnis zu erteilen, Ressourcenfreigabe zuordnungen für einen neuen Tresortyp abzurufen.	08. August 2023
AWSBackupServiceRolePolicyForS3Backup – Aktualisierung auf eine bestehende Richtlinie	Es wurde die Erlaubnis `s3:PutInventoryConfiguration` hinzugefügt, die Geschwindigkeit der Backup-Leistung mithilfe eines Bucket-Inventars zu erhöhen.	1. August 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Aktionen hinzugefügt, um dem Benutzer Berechtigungen zum Hinzufügen von Tags zur Wiederherstellung von Ressourcen zu gewähren: `storagegateway:AddTagsToResource elasticfilesystem:TagResource` ,, nur `ec2:CreateTags` für `ec2:CreateAction` das, was entweder `RunInstances` oder `CreateVolume fsx:TagResource` , und beinhalte `tcloudformation:TagResource` .	22. Mai 2023
AWSBackupAuditAccess – Aktualisierung auf eine bestehende Richtlinie	Die Ressourcenauswahl innerhalb der API wurde `config:DescribeCompliancebyConfigRule` durch eine Platzhalterressource ersetzt, um Benutzern die Auswahl von Ressourcen zu erleichtern.	11. April 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Wiederherstellung von Amazon EFS mithilfe eines vom Kunden verwalteten Schlüssels wurde hinzugefügt:`kms:GenerateDataKeyWithoutPlaintext` . Dadurch wird sichergestellt, dass Benutzer über die erforderlichen Berechtigungen zur Wiederherstellung von Amazon EFS-Ressourcen verfügen.	27. März 2023
AWSServiceRolePolicyForBackupReports – Aktualisierung auf eine bestehende Richtlinie	Die `config:DescribeConfigRuleEvaluationStatus` Aktionen `config:DescribeConfigRules` und wurden aktualisiert, sodass AWS Backup Audit Manager auf von AWS Backup Audit Manager verwaltete Regeln zugreifen kann AWS Config .	9. März 2023

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForS3Restore – Aktualisierung auf eine bestehende Richtlinie	Der Richtlinie wurden die folgenden Berechtigungen hinzugefügt: `kms:Decrypt` `s3:PutBucketOwnershipControls` ,`s3:GetBucketOwnershipControls` , und. `AWSBackupServiceRolePolicyForS3Restore` Diese Berechtigungen sind erforderlich, um die Wiederherstellung von Objekten zu unterstützen, wenn die KMS-Verschlüsselung in der ursprünglichen Sicherung verwendet wird, und für die Wiederherstellung von Objekten, wenn der Objekteigentum im ursprünglichen Bucket statt in ACL konfiguriert ist.	13. Februar 2023

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen hinzugefügt, um Backups mithilfe von VMware-Tags virtueller Maschinen zu planen und die zeitplanbasierte Bandbreitendrosselung zu unterstützen:`backup-gateway:GetHypervisorPropertyMappings` ,,,`backup-gateway:GetVirtualMachine` , `backup-gateway:PutHypervisorPropertyMappings` `backup-gateway:GetHypervisor` , `backup-gateway:StartVirtualMachinesMetadataSync` und. `backup-gateway:GetBandwidthRateLimitSchedule` `backup-gateway:PutBandwidthRateLimitSchedule`	15. Dezember 2022

Änderung	Beschreibung	Datum
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen hinzugefügt, um Backups mithilfe von VMware-Tags virtueller Maschinen zu planen und die zeitplanbasierte Bandbreitendrosselung zu unterstützen:,, und. `backup-gateway:GetHypervisorPropertyMappings` `backup-gateway:GetVirtualMachine` `backup-gateway:GetHypervisor` `backup-gateway:GetBandwidthRateLimitSchedule`	15. Dezember 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync – Neue Richtlinie.	Ermöglicht AWS Backup Gateway, die Metadaten virtueller Maschinen in lokalen Netzwerken mit Backup Gateway zu synchronisieren.	15. Dezember 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen zur Unterstützung von Timestream-Backup-Jobs hinzugefügt: `timestream:StartAwsBackupJob` `timestream:GetAwsBackupStatus` `timestream:ListTables` ,,`timestream:ListDatabases` ,`timestream:ListTagsForResource` , `timestream:DescribeTable` `timestream:DescribeDatabase` , und. `timestream:DescribeEndpoints`	13. Dezember 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Wiederherstellungsaufträgen wurden hinzugefügt: `timestream:StartAwsRestoreJob` `timestream:GetAwsRestoreStatus` ,`timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:ListDatabases` ,`timestream:DescribeTable` , `timestream:DescribeDatabase` `s3:GetBucketAcl` , und. `timestream:DescribeEndpoints`	13. Dezember 2022
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt:`timestream:ListTables` ,`timestream:ListDatabases` , `s3:ListAllMyBuckets` und. `timestream:DescribeEndpoints`	13. Dezember 2022

Änderung	Beschreibung	Datum
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt:`timestream:ListDatabases` , `timestream:ListTables` `s3:ListAllMyBuckets` , und. `timestream:DescribeEndpoints`	13. Dezember 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt: `timestream:ListDatabases` `timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:DescribeDatabase` ,`timestream:DescribeTable` , `timestream:GetAwsBackupStatus` `timestream:GetAwsRestoreStatus` , und. `timestream:DescribeEndpoints`	13. Dezember 2022

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Ressourcen wurden hinzugefügt: `redshift:DescribeClusters` `redshift:DescribeClusterSubnetGroups` `redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups` ,`redshift:DescribeClusterTracks` ,`redshift:DescribeSnapshotSchedules` , `undec2:DescribeAddresses` .	27. November 2022

Änderung	Beschreibung	Datum
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Ressourcen wurden hinzugefügt:`redshift:DescribeClusters` ,`redshift:DescribeClusterSubnetGroups` ,`redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups`, ,`redshift:DescribeClusterTracks` . `redshift:DescribeSnapshotSchedules` , und. `ec2:DescribeAddresses`	27. November 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Wiederherstellungsaufträgen wurden hinzugefügt: `redshift:RestoreFromClusterSnapshot` `redshift:RestoreTableFromClusterSnapshot` ,`redshift:DescribeClusters` ,`redshift:DescribeTableRestoreStatus` .	27. November 2022
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Backup-Jobs wurden hinzugefügt: `redshift:CreateClusterSnapshot` `redshift:DescribeClusterSnapshots` ,`redshift:DescribeTags` ,`redshift:DeleteClusterSnapshot` ,`redshift:DescribeClusters` ,`redshift:CreateTags` .	27. November 2022

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von CloudFormation Ressourcen wurde hinzugefügt:`cloudformation:ListStacks` .	27. November 2022
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von CloudFormation Ressourcen wurde hinzugefügt:`cloudformation:ListStacks` .	27. November 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von CloudFormation Ressourcen wurden hinzugefügt: `redshift:DescribeClusterSnapshots` `redshift:DescribeTags` ,`redshift:DeleteClusterSnapshot` , und`redshift:DescribeClusters` .	27. November 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um Backup-Jobs für den AWS CloudFormation Anwendungsstapel zu unterstützen: `cloudformation:GetTemplate cloudformation:DescribeStacks` , und`cloudformation:ListStackResources` .	16. November 2022
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um Backup-Jobs für den AWS CloudFormation Anwendungsstapel zu unterstützen: `cloudformation:CreateChangeSet` und `cloudformation:DescribeChangeSet`	16. November 2022

Änderung	Beschreibung	Datum
AWSBackupOrganizationAdminAccess – Aktualisierung auf eine bestehende Richtlinie	Dieser Richtlinie wurden die folgenden Berechtigungen hinzugefügt, damit Organisationsadministratoren die Funktion „Delegierter Administrator“ verwenden können:`organizations:ListDelegatedAdministrator` , und `organizations:RegisterDelegatedAdministrator` `organizations:DeregisterDelegatedAdministrator`	27. November 2022
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf Amazon EC2 EC2-Instances wurden hinzugefügt: `ssm-sap:GetOperation` `ssm-sap:ListDatabases` ,`ssm-sap:BackupDatabase` ,`ssm-sap:UpdateHanaBackupSettings` ,`ssm-sap:GetDatabase` , und`ssm-sap:ListTagsForResource` .	20. November 2022

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf Amazon EC2 EC2-Instances wurden hinzugefügt: `ssm-sap:GetOperation` `ssm-sap:ListDatabases` ,`ssm-sap:GetDatabase` , und`ssm-sap:ListTagsForResource` .	20. November 2022
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf Amazon EC2 EC2-Instances wurden hinzugefügt: `ssm-sap:GetOperation` `ssm-sap:ListDatabases` ,`ssm-sap:GetDatabase` , und`ssm-sap:ListTagsForResource` .	20. November 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von SAP HANA auf Amazon EC2 EC2-Instances wurde hinzugefügt:`ssm-sap:GetOperation` .	20. November 2022
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von Backup-Gateway-Wiederherstellungsaufträgen für eine EC2-Instance wurde hinzugefügt:`ec2:CreateTags` .	20. November 2022

Änderung	Beschreibung	Datum
AWSBackupDataTransferAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um die sichere Speicherdatenübertragung für SAP HANA On Amazon EC2 EC2-Ressourcen zu unterstützen: `backup-storage:StartObject backup-storage:PutChunk ,backup-storage:GetChunk ,backup-storage:ListChunks ,backup-storage:ListObjects ,backup-storage:GetObjectMetadata , undbackup-storage:NotifyObjectComplete .`	20. November 2022

Änderung	Beschreibung	Datum
AWSBackupRestoreAccessForSAPHANA – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen für Ressourcenbesitzer hinzugefügt, um die Wiederherstellung von SAP HANA On Amazon EC2 EC2-Ressourcen durchzuführen: `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 ,` und`ssm-sap:ListTagsForResource .`	20. November 2022
AWSBackupServiceRolePolicyForS3Backup – Aktualisierung auf eine bestehende Richtlinie	Die Erlaubnis `s3:GetBucketAcl` zur Unterstützung von Backup-Vorgängen von AWS Backup für Amazon S3 wurde hinzugefügt.	24. August 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Zugriff auf die Erstellung einer Datenbank-Instance zur Unterstützung der Multi-Availability Zone (Multi-AZ) - Funktionalität zu gewähren:. `rds:CreateDBInstance`	20. Juli 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde die `s3:GetBucketTagging` Berechtigung hinzugefügt, dem Benutzer die Erlaubnis zu erteilen, Buckets für die Sicherung mit einem Ressourcen-Platzhalter auszuwählen. Ohne diese Berechtigung sind Benutzer, die auswählen, welche Buckets mit einem Ressourcen-Platzhalter gesichert werden sollen, erfolglos.	6. Mai 2022
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Volume-Ressourcen wurden im Rahmen vorhandener `fsx:CreateBackup` und `fsx:ListTagsForResource` Aktionen hinzugefügt, und es wurde eine neue Aktion `fsx:DescribeVolumes` zur Unterstützung von FSx for ONTAP Backups auf Volume-Ebene hinzugefügt.	27. April 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um den Benutzern Berechtigungen zur Wiederherstellung von FSx for ONTAP-Volumes`fsx:DescribeVolumes` , `fsx:CreateVolumeFromBackup` `fsx:DeleteVolume` , und zu gewähren. `fsx:UntagResource`	27. April 2022
AWSBackupServiceRolePolicyForS3Backup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zu erteilen, Benachrichtigungen über Änderungen an ihren Amazon S3 S3-Buckets während Backup-Vorgängen zu erhalten: `s3:GetBucketNotification` und`s3:PutBucketNotification` .	25. Februar 2022

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForS3Backup – Neue Richtlinie.	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zum Sichern ihrer Amazon S3 S3-Buckets zu gewähren: `s3:GetInventoryConfiguration` ,,,`s3:PutInventoryConfiguration` ,,`s3:ListBucketVersions` ,`s3:ListBucket` ,`s3:GetBucketTagging` ,`s3:GetBucketVersioning` ,, `s3:GetBucketNotification` `s3:GetBucketLocation` , und `s3:ListAllMyBuckets` Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zum Sichern ihrer Amazon S3 S3-Objekte zu gewähren: `s3:GetObject` `s3GetObjectAcl` ,`s3:GetObjectVersionTagging` ,`s3:GetObjectVersionAcl` ,`s3:GetObjectTagging` , unds`3:GetObjectVersion` . Die folgenden Aktionen wurden hinzugefügt, um	17. Februar 2022

Änderung	Beschreibung	Datum
	Benutzern Berechtigungen zum Sichern ihrer verschlüsselten Amazon S3 S3-Daten zu gewähren: `kms:Decrypt` und`kms:DescribeKey` . Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zum Erstellen inkrementeller Backups ihrer Amazon S3 S3-Daten unter Verwendung von EventBridge Amazon-Regeln zu gewähren: `events:DescribeRule` `events:EnableRule` ,`events:PutRule` ,`events:DeleteRule` ,`events:PutTargets` ,,`events:RemoveTargets` ,`events:ListTargetsByRule` ,`events:DisableRule` ,`cloudwatch:GetMetricData` , und`events:ListRules` .	

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForS3Restore – Neue Richtlinie.	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Wiederherstellung ihrer Amazon S3 S3-Buckets zu gewähren: `s3:CreateBucket s3:ListBucketVersions ,s3:ListBucket ,, s3:GetBucketVersioning s3:GetBucketLocation , unds3:PutBucketVersioning .` Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Wiederherstellung ihrer Amazon S3 S3-Buckets zu gewähren: `s3:GetObject s3:GetObjectVersion ,s3:DeleteObject ,s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging ,s3:PutObjectTagging ,,s3:GetObjectAcl , s3:PutObjectAcl s3:PutObject , unds3:ListMultipartUploadParts .`	17. Februar 2022

Änderung	Beschreibung	Datum
	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Verschlüsselung ihrer wiederhergestellten Amazon S3 S3-Daten zu gewähren: `kms:Decrypt kms:DescribeKey` , und`kms:GenerateDataKey` .	
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde hinzugefügt`s3:ListAllMyBuckets` , um Benutzern die Möglichkeit zu geben, eine Liste ihrer Buckets einzusehen und auszuwählen, welche Buckets einem Backup-Plan zugewiesen werden sollen.	14. Februar 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Wurde hinzugefügt`backup-gateway:ListVirtualMachines` , um Benutzern die Möglichkeit zu geben, eine Liste ihrer virtuellen Maschinen einzusehen und auszuwählen, welche sie einem Backup-Plan zuweisen möchten. Wurde hinzugefügt`backup-gateway:ListTagsForResource` , um Benutzern das Recht zu gewähren, die Tags für ihre virtuellen Maschinen aufzulisten.	30. November 2021

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt`backup-gateway:Backup` , um Benutzern Rechte für die Wiederherstellung ihrer virtuellen Maschinen-Backups zu gewähren. AWS Backup wurde auch hinzugefügt`backup-gateway:ListTagsForResource` , um Benutzern die Möglichkeit zu geben, die Tags aufzulisten, die ihren Backups virtueller Maschinen zugewiesen sind.	30. November 2021
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Wurde hinzugefügt`backup-gateway:Restore` , um Benutzern Rechte für die Wiederherstellung ihrer virtuellen Maschinen-Backups zu gewähren.	30. November 2021

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Verwendung von AWS Backup Gateway zum Sichern, Wiederherstellen und Verwalten ihrer virtuelle n Maschinen zu gewähren: ,backup-gateway:Ass ociateGatewayToSer ver ,,,,,backup-ga teway:CreateGatewa y ,backup-gateway:Del eteGateway ,,backup-ga teway:DeleteHyperv isor ,backup-gateway:Dis associateGatewayFr omServer ,backup-gateway:Imp ortHypervisorConfi guration ,backup-ga teway:ListGateways ,,backup-gateway:Lis tHypervisors ,backup-gateway:ListTagsForR esource ,backup-ga teway:ListVirtualM achines ,backup-ga teway:PutMaintenan ceStartTime ,,backup-gateway:Tag Resource ,backup-gateway:Tes	30. November 2021

Änderung	Beschreibung	Datum
	`tHypervisorConfigu ration` ,`backup-ga teway:UntagResourc e` ,`backup-gateway:Upd ateGatewayInformat ion` ,, und`backup-ga teway:UpdateHyperv isor` .	
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtig ungen zum Sichern ihrer virtuellen Maschinen zu gewähren: `backup-ga teway:ListGateways` `backup-gateway:Lis tHypervisors` ,`backup-gateway:ListTagsForR esource` , und`backup-ga teway:ListVirtualM achines` .	30. November 2021
AWSBackupServiceLi nkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Es wurde hinzugefügt`dynamodb: ListTagsOfResource` , um Benutzern die Rechte zu gewähren, Tags ihrer DynamoDB-Tabellen aufzulist en, um sie mithilfe der erweiterten DynamoDB-Backup-Funktionen zu sichern.	23. November 2021

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt`dynamodb:StartAwsBackupJob`, um Benutzern Berechtigungen zum Sichern ihrer DynamoDB-Tabellen mithilfe erweiterter Backup-Funktionen zu gewähren. Hinzugefügt`dynamodb:ListTagsOfResource`, um Benutzern Berechtigungen zum Kopieren von Tags aus ihren DynamoDB-Quelltabellen in ihre Backups zu gewähren.	23. November 2021
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Es wurde hinzugefügt`dynamodb:RestoreTableFromAwsBackup`, um Benutzern Rechte zur Wiederherstellung ihrer DynamoDB-Tabellen zu gewähren, die mit den erweiterten DynamoDB-Backup-Funktionen gesichert wurden.	23. November 2021

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Es wurde hinzugefügt`dynamodb:RestoreTableFromAwsBackup` , um Benutzern Rechte zur Wiederherstellung ihrer DynamoDB-Tabellen zu gewähren, die mit den erweiterten DynamoDB-Backup-Funktionen gesichert wurden.	23. November 2021
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die Aktionen wurden entfernt, `rds:DescribeDBSnapshots` weil sie `backup:GetRecoveryPointRestoreMetadata` überflüssig waren. AWS Backup brauchte nicht beides `backup:GetRecoveryPointRestoreMetadata` und `backup:Get*` als Teil von`AWSBackupOperatorAccess` . Ich AWS Backup brauchte auch nicht beides `rds:DescribeDBSnapshots` und `rds:describeDBSnapshots` als Teil von`AWSBackupOperatorAccess` .	23. November 2021

Änderung	Beschreibung	Datum
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neuen Aktionen`elasticfilesystem:DescribeFileSystems` ,,,`dynamodb:ListTables` ,`storagegateway:ListVolumes` , `ec2:DescribeVolumes` `ec2:DescribeInstances` , und wurden hinzugefügt `rds:DescribeDBInstances` `rds:DescribeDBClusters` , `fsx:DescribeFileSystems` damit Kunden bei der Auswahl der Ressourcen, die sie einem AWS Backup Backup-Plan zuweisen möchten, eine Liste der von ihnen unterstützten Ressourcen einsehen und auswählen können.	10. November 2021
AWSBackupAuditAccess – Neue Richtlinie.	Hinzugefügt`AWSBackupAuditAccess` , um dem Benutzer Berechtigungen zur Verwendung von AWS Backup Audit Manager zu gewähren. Zu den Berechtigungen gehört die Möglichkeit, Compliance-Frameworks zu konfigurieren und Berichte zu erstellen.	24. August 2021

Änderung	Beschreibung	Datum
AWSServiceRolePolicyForBackupReports – Neue Richtlinie.	Es wurde hinzugefügt `AWSServiceRolePolicyForBackupReports`, um Berechtigungen für eine dienstbezogene Rolle zu gewähren, um die Überwachung von Backup-Einstellungen, Jobs und Ressourcen im Hinblick auf die Einhaltung der vom Benutzer konfigurierten Frameworks zu automatisieren.	24. August 2021
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt `iam:CreateServiceLinkedRole`, um eine dienstbezogene Rolle (nach bestem Wissen) zu erstellen, um das Löschen abgelaufener Wiederherstellungspunkte für Sie zu automatisieren. Ohne diese serviceverknüpfte Rolle können abgelaufene Wiederherstellungspunkte AWS Backup nicht gelöscht werden, nachdem Kunden die ursprüngliche IAM-Rolle gelöscht haben, mit der sie ihre Wiederherstellungspunkte erstellt haben.	5. Juli 2021

Änderung	Beschreibung	Datum
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde die neue Aktion hinzugefügt`dynamodb:DeleteBackup` , um die `DeleteRecoveryPoint` Erlaubnis zu erteilen, das Löschen abgelaufener DynamoDB-Wiederherstellungspunkte auf der Grundlage der Lebenszykluseinstellungen Ihres Backupplans zu automatisieren.	5. Juli 2021
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die Aktionen `backup:GetRecoveryPointRestoreMetadata` wurden entfernt`rds:DescribeDBSnapshots` , weil sie überflüssig waren. AWS Backup brauchte nicht beide `backup:GetRecoveryPointRestoreMetadata` und `backup:Get*` als Teil von `AWSBackupOperatorAccess` Also AWS Backup brauchte ich nicht beides `rds:DescribeDBSnapshots` und `rds:describeDBSnapshots` als Teil von `AWSBackupOperatorAccess`	25. Mai 2021

Änderung	Beschreibung	Datum
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die Aktionen `backup:GetRecoveryPointRestoreMetadata` wurden entfernt`rds:DescribeDBSnapshots`, weil sie überflüssig waren. AWS Backup brauchte nicht beides `backup:GetRecoveryPointRestoreMetadata` und `backup:Get*` als Teil von`AWSBackupOperatorAccess`. Ich AWS Backup brauchte auch nicht beides `rds:DescribeDBSnapshots` und `rds:describeDBSnapshots` als Teil von`AWSBackupOperatorAccess`.	25. Mai 2021
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt`fsx:TagResource`, um Ihnen die `StartRestoreJob` Erlaubnis zu erteilen, während des Wiederherstellungsvorgangs Tags auf Amazon FSx-Dateisysteme anzuwenden.	24. Mai 2021

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Es wurden die neuen Aktionen `ec2:DescribeImages` und `ec2:DescribeInstances` die Erteilung von `StartRestoreJob` Berechtigungen hinzugefügt, mit denen Sie Amazon EC2 EC2-Instances von Wiederherstellungspunkten wiederherstellen können.	24. Mai 2021
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt`fsx:CopyBackup` , um Ihnen die `StartCopyJob` Erlaubnis zu erteilen, Amazon FSx-Wiederherstellungspunkte zwischen Regionen und Konten zu kopieren.	12. April 2021
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt`fsx:CopyBackup` , um Ihnen die `StartCopyJob` Erlaubnis zu erteilen, Amazon FSx-Wiederherstellungspunkte zwischen Regionen und Konten zu kopieren.	12. April 2021

Änderung	Beschreibung	Datum
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde aktualisiert, um die folgenden Anforderungen zu erfüllen: AWS Backup Um ein Backup einer verschlüsselten DynamoDB-Tabelle zu erstellen, müssen Sie die Berechtigungen `kms:Decrypt` und `kms:GenerateDataKey` zur IAM-Rolle hinzufügen, die für die Sicherung verwendet wird.	10. März 2021

Änderung	Beschreibung	Datum
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde aktualisiert, um die folgenden Anforderungen zu erfüllen: Um kontinuierliche Backups für Ihre Amazon RDS-Datenbank AWS Backup zu konfigurieren, stellen Sie sicher, dass die API-Berechtigung in der IAM-Rolle `rds:ModifyDBInstance` vorhanden ist, die in Ihrer Backup-Plan-Konfiguration definiert ist. Um kontinuierliche Amazon RDS-Sicherungen wiederherzustellen, müssen Sie die Berechtigung `rds:RestoreDBInstanceToPointInTime` zu der IAM-Rolle hinzufügen, die Sie für den Wiederherstellungsauftrag eingereicht haben. Um in der AWS Backup Konsole den Zeitraum zu beschreiben, der für die point-in-time Wiederherstellung zur Verfügung steht, müssen Sie die `rds:DescribeDBInstanceAutomatedBackups` API-Berechtigung in Ihre von IAM verwaltete Richtlinie aufnehmen.	10. März 2021

Änderung	Beschreibung	Datum
AWS Backup hat begonnen, Änderungen zu verfolgen	AWS Backup hat begonnen, Änderungen für die von AWS ihm verwalteten Richtlinien zu verfolgen.	10. März 2021

Verwenden von serviceverknüpften Rollen für AWS Backup

AWS Backup verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Backup Mit Diensten verknüpfte Rollen sind vordefiniert AWS Backup und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Themen

- Rollen zum Sichern und Kopieren verwenden
- Rollen für AWS Backup Audit Manager verwenden
- Rollen für Wiederherstellungstests verwenden

Rollen zum Sichern und Kopieren verwenden

AWS Backup verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Backup Mit Diensten verknüpfte Rollen sind vordefiniert AWS Backup und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Backup erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Backup definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Backup kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS Backup Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Backup

AWS Backup verwendet die dienstbezogene Rolle mit dem Namen AWSServiceRoleForBackup—Ermöglicht AWS Backup das Auflisten von Ressourcen, die Sie sichern können, und das Kopieren von Backups.

AWS Backup verwendet die Rolle auch, um alle Backups für alle Ressourcentypen außer Amazon EC2 zu löschen.

Die AWSServiceRoleForBackup serviceverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `backup.amazonaws.com`

Die Berechtigungen für diese Richtlinie finden Sie AWSBackupServiceLinkedRolePolicyforBackupin der Referenz für AWS verwaltete Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS Backup

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die zu sichernden Ressourcen auflisten, kontenübergreifende Backups einrichten oder Backups in der AWS Management Console, der oder der AWS CLI AWS API durchführen, AWS Backup wird die dienstbezogene Rolle für Sie erstellt.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie zu sichernde Ressourcen auflisten, kontenübergreifende Backups einrichten oder Backups durchführen, AWS Backup wird die dienstbezogene Rolle erneut für Sie erstellt.

Bearbeiten einer serviceverknüpften Rolle für AWS Backup

AWS Backup erlaubt es Ihnen nicht, die AWSServiceRoleForBackup dienstverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Backup

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen. Zunächst müssen Sie alle Ihre Wiederherstellungspunkte löschen. Dann müssen Sie alle Ihre Backup-Tresore löschen.

> **Note**
>
> Wenn der AWS Backup Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRoleForBackup (Konsole) verwendet werden

1. Gehen Sie wie unter Löschen eines Backup-Tresors beschrieben vor, um alle Ihre Wiederherstellungspunkte und Backup-Tresore (mit Ausnahme Ihres Standard-Tresors) zu löschen.
2. Um Ihren Standard-Tresor zu löschen, verwenden Sie den folgenden Befehl in der AWS CLI:

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

Um AWS Backup Ressourcen zu löschen, die von AWSServiceRoleForBackup (AWS CLI) verwendet werden

1. Um all Ihre Wiederherstellungspunkte zu löschen, verwenden Sie delete-recovery-point.
2. Um all Ihre Backup-Tresore zu löschen, verwenden Sie `delete-backup-vault`.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRoleForBackup (API) verwendet werden

1. Um alle Ihre Wiederherstellungspunkte zu löschen, verwenden Sie `DeleteRecoveryPoint`.
2. Um all Ihre Backup-Tresore zu löschen, verwenden Sie `DeleteBackupVault`.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForBackup serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte AWS Backup -Rollen

AWS Backup unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Backup Unterstützte Features und Regionen.

Rollen für AWS Backup Audit Manager verwenden

AWS Backup verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Backup Mit Diensten verknüpfte Rollen sind vordefiniert AWS Backup und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Backup erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Backup definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Backup kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die

Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS Backup Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Backup

AWS Backup verwendet die dienstbezogene Rolle mit dem Namen AWSServiceRoleForBackupReports— Erlaubt AWS Backup die Berechtigung zum Erstellen von Steuerelementen, Frameworks und Berichten.

Die AWSServiceRoleForBackupReports dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `backup.amazonaws.com`

Die Berechtigungen für diese Richtlinie finden Sie AWSServiceRolePolicyForBackupReportsin der Referenz für AWS verwaltete Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS Backup

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Framework oder einen Berichtsplan in der AWS Management Console, der oder der AWS CLI AWS API erstellen, AWS Backup wird die dienstbezogene Rolle für Sie erstellt.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten

Features verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Framework oder einen Berichtsplan erstellen, AWS Backup wird die dienstbezogene Rolle erneut für Sie erstellt.

Bearbeiten einer serviceverknüpften Rolle für AWS Backup

AWS Backup ermöglicht es Ihnen nicht, die AWSServiceRoleForBackupReports dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Backup

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen. Sie müssen alle Frameworks und Berichtspläne löschen.

> **Note**
>
> Wenn der AWS Backup Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRoleForBackupReports (Konsole) verwendet werden

1. Informationen zum Löschen aller Frameworks finden Sie unter Löschen von Frameworks.

2. Informationen zum Löschen aller Berichtspläne finden Sie unter Löschen von Berichtsplänen.

Um AWS Backup Ressourcen zu löschen, die von AWSServiceRoleForBackupReports (AWS CLI) verwendet werden

1. Verwenden Sie zum Löschen aller Frameworks delete-framework.
2. Um alle Berichtspläne zu löschen, verwenden Sie delete-report-plan.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRoleForBackupReports (API) verwendet werden

1. Um alle Frameworks zu löschen, verwenden Sie DeleteFramework.
2. Um alle Berichtspläne zu löschen, verwenden Sie DeleteReportPlan.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForBackupReports serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte AWS Backup -Rollen

AWS Backup unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Backup Unterstützte Features und Regionen.

Rollen für Wiederherstellungstests verwenden

AWS Backup verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Backup Mit Diensten verknüpfte Rollen sind vordefiniert AWS Backup und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Backup erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Backup definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Backup kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die

Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS Backup Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Backup

AWS Backup verwendet die dienstbezogene Rolle mit dem Namen AWSServiceRolePolicyForBackupRestoreTesting— Stellt Backup-Berechtigungen für die Durchführung von Wiederherstellungstests bereit.

Die AWSServiceRolePolicyForBackupRestoreTesting dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `backup.amazonaws.com`

Die Berechtigungen für diese Richtlinie finden Sie AWSServiceRolePolicyForBackupRestoreTestingin der Referenz für AWS verwaltete Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS Backup

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Wiederherstellungstests in der AWS Management Console AWS CLI, der oder der AWS API durchführen, AWS Backup wird die dienstbezogene Rolle für Sie erstellt.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten

Features verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie Wiederherstellungstests durchführen, AWS Backup erstellt die dienstbezogene Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für AWS Backup

AWS Backup erlaubt Ihnen nicht, die AWSServiceRolePolicyForBackupRestoreTesting dienstverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Backup

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen. Sie müssen alle Wiederherstellungstestpläne löschen.

> **Note**
>
> Wenn der AWS Backup Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRolePolicyForBackupRestoreTesting (Konsole) verwendet werden

- Informationen zum Löschen aller Wiederherstellungstestpläne finden Sie unter Wiederherstellungstests.

Um AWS Backup Ressourcen zu löschen, die von AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI) verwendet werden

- Um Wiederherstellungstestpläne zu löschen, verwenden Sie `delete-restore-testing-plan`.

Um AWS Backup Ressourcen zu löschen, die von der AWSServiceRolePolicyForBackupRestoreTesting (API) verwendet werden

- Um Wiederherstellungstestpläne zu löschen, verwenden Sie `DeleteRestoreTestingPlan`.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRolePolicyForBackupRestoreTesting serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte AWS Backup -Rollen

AWS Backup unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Backup Unterstützte Features und Regionen.

Dienstübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die AWS Backup einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert

und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der Wert von `aws:SourceArn` muss ein AWS Backup-Tresor sein, wenn Sie AWS Backup verwenden, um Amazon-SNS-Themen in Ihrem Namen veröffentlichen.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontextschlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel mit Platzhaltern (`aws:SourceArn`) `*` für die unbekannten Teile des ARN. Beispiel: `arn:aws::servicename::123456789012:*`.

Sicherheit der Infrastruktur in AWS Backup

Als verwalteter Dienst AWS Backup ist er durch AWS globale Netzwerksicherheit geschützt. Weitere Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Backup über das Netzwerk. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Integrität der Daten in AWS Backup

AWS Backup Ziel der Datenintegrität

AWS Backup versucht, die Integrität bei der Übertragung, Speicherung und Verarbeitung Ihrer Daten aufrechtzuerhalten. AWS Backup behandelt gespeicherte Ressourcendaten als inhaltsunabhängige

kritische Informationen, da wir unseren Kunden unabhängig von der Art der Daten, die Sie speichern, dasselbe hohe Sicherheitsniveau bieten. Wir achten auf die Sicherheit unserer Kunden und haben ausgefeilte technische und physische Maßnahmen gegen unbefugten Zugriff getroffen. Sie behalten die vollständige Kontrolle darüber, wie Ihre Daten klassifiziert werden, in welchen Regionen Sie Ihre Daten speichern und wie Sie Ihre Daten kontrollieren, archivieren und vor Offenlegung schützen.

AWS Backup Implementierung der Datenintegrität

AWS Backup arbeitet mit anderen Diensten AWS und Amazon-Diensten zusammen, um die Integrität der Daten zu wahren, die sie speichern und mit denen sie interagieren. Die verwendeten Tools können variieren und können Folgendes beinhalten (sind aber nicht darauf beschränkt):

- Kontinuierliche Objektvalidierung anhand ihrer Prüfsumme, um Objektbeschädigungen zu verhindern
- Interne Prüfsummen zur Bestätigung der Integrität von Daten während der Übertragung und im Ruhezustand
- Prüfsummen, die anhand von Daten in Sicherungen berechnet wurden, die im Primärspeicher erstellt wurden
- Automatischer Versuch, das normale Maß an Objektspeicher-Redundanz wiederherzustellen, falls eine Festplatte beschädigt wird oder ein Geräteausfall erkannt wird
- Redundante Speicherung von Daten an mehreren physischen Standorten
- Verbesserung der Objektbeständigkeit in mehreren Availability Zones während des ersten Schreibvorgangs, kombiniert mit weiterer Replikation für den Fall, dass das Gerät nicht verfügbar ist oder Bit-Rot erkannt wird
- Prüfsummen für den gesamten Netzwerkverkehr, um Beschädigungen von Datenpaketen beim Speichern oder Abrufen von Daten zu erkennen

AWS Backup Speichert nativ Daten für Amazon DynamoDB mit erweiterten Funktionen, Amazon EFS, Amazon S3, Amazon Timestream und virtuelle Maschinen, die mit VMware laufen und über das Backup-Gateway verbunden sind. AWS Backup ermöglicht Backups von Daten, die mit anderen Diensten gespeichert wurden, darunter Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon FSx für OpenZFS, Amazon FSx für ONTAP, Amazon Neptune, Amazon RDS und Amazon Redshift. NetApp

Objektive Bestätigung und Prüfung der AWS Backup -Datenintegrität

Die Daten, die direkt von anderen Diensten, mit denen AWS Backup interagiert, gespeichert werden, AWS Backup und die Daten, die in Partnerschaft mit anderen AWS Diensten gespeichert werden, unterliegen dem strengen Verfahren von Amazon Simple Storage Service (Amazon S3), das diese Datenintegrität untermauert. Diese Integrität wird von einem unabhängigen externen Prüfer anhand eines jährlichen SOC-Prüfberichts bestätigt, der über AWS Artifact in dem AWS Management Console verfügbar ist.

Rechtliche Aufbewahrungsfristen und AWS Backup

Eine gesetzliche Aufbewahrungsfrist ist ein administratives Tool, mit dem verhindert werden kann, dass Sicherungen gelöscht werden, während sie sich noch im Sperrmodus befinden. Solange die Sperre aktiv ist, können Sicherungen, die sich in einer Sperre befinden, nicht gelöscht werden, und Lebenszyklusrichtlinien, die den Backup-Status ändern würden (z. B. der Übergang in einen `Deleted`-Status), werden verzögert, bis die gesetzliche Sperre aufgehoben wird. Eine Sicherung kann mehrere gesetzliche Aufbewahrungsfristen haben.

Gesetzliche Aufbewahrungsfristen können auf ein oder mehrere Backups (auch als Wiederherstellungspunkte bezeichnet) angewendet werden, die von erstellt wurden, AWS Backup sofern deren Lebenszyklen dies zulassen. Ein Sicherungstyp, der als kontinuierliches Backup bezeichnet wird, hat einen maximalen Lebenszyklus von 35 Tagen. Gesetzliche Aufbewahrungsfristen verlängern einen kontinuierlichen Backup-Lebenszyklus nicht.

Wenn eine gesetzliche Aufbewahrungsfrist eingerichtet wird, können dabei bestimmte Filterkriterien wie Ressourcentypen und Ressourcen-IDs berücksichtigt werden. Darüber hinaus können Sie den Zeitraum für das Erstellungsdatum der Sicherungen definieren, die Sie in eine gesetzliche Aufbewahrungsfrist aufnehmen möchten. Rechtliche Aufbewahrungsfristen und Sicherungen stehen in einer Viele:Viele-Beziehung, was bedeutet, dass ein Backup mehr als ein Legal Hold haben kann und ein Legal Hold mehr als ein Backup umfassen kann. Für jedes Konto können maximal 50 aktive Aufbewahrungsfristen gleichzeitig bestehen.

Gesetzliche Aufbewahrungsfristen gelten nur für das ursprüngliche Backup, auf dem sie gespeichert sind. Wenn ein Backup zwischen Regionen oder Konten kopiert wird (sofern die Ressource dies unterstützt), behält es seine gesetzlichen Aufbewahrungsfristen nicht bei. Einer rechtlichen Aufbewahrungsfrist ist, wie jeder anderen Ressource, ein eindeutiger Amazon-Ressourcenname (ARN) zugeordnet. Nur Wiederherstellungspunkte, die von erstellt wurden, AWS Backup können Teil einer gesetzlichen Aufbewahrungsfrist sein.

Beachten Sie, dass AWS Backup Vault Lock zwar zusätzlichen Schutz und die Unveränderlichkeit eines Tresors bietet, ein gesetzlicher Aufbewahrungszeitraum jedoch zusätzlichen Schutz vor dem Löschen einzelner Sicherungen (Wiederherstellungspunkte) bietet. Die gesetzliche Aufbewahrungsfrist läuft nicht ab und die Daten im Backup werden auf unbestimmte Zeit aufbewahrt. Die Sperre bleibt aktiv, bis sie von einem Benutzer mit ausreichenden Berechtigungen freigegeben wird.

Erstellen einer gesetzlichen Aufbewahrungsfrist

Wenn ein gesetzlicher Aufbewahrungszeitraum erstellt wird, enthält er nur Wiederherstellungspunkte, die bereits erstellt wurden. Sicherungen (Wiederherstellungspunkte) mit dem Status `EXPIRED` oder `DELETING` werden nicht in den gesetzlichen Aufbewahrungszeitraum aufgenommen. Wiederherstellungspunkte (Backups) mit dem Status `CREATING` von werden je nach dem Zeitpunkt der Fertigstellung möglicherweise nicht in die gesetzliche Aufbewahrungsfrist einbezogen.

Rechtliche Sperren können von Benutzern hinzugefügt werden, die über die erforderlichen IAM-Berechtigungen verfügen.

Erstellen Sie mithilfe der -Konsole eine gesetzliche Aufbewahrungsfrist

Um eine gesetzliche Sperre zu erstellen

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Suchen Sie im Dashboard auf der linken Seite der Konsole nach My Account (Mein Konto). Wählen Sie „Rechtliche Aufbewahrungsfristen“.
3. Wählen Sie „Rechtliche Sperre hinzufügen“.
4. Es werden drei Bereiche angezeigt: Details zur gesetzlichen Aufbewahrung, Geltungsbereich der gesetzlichen Aufbewahrung und Tags zur gesetzlichen Aufbewahrung.

    a. Geben Sie unter Detials zur gesetzlichen Aufbewahrungsfrist einen Titel und eine Beschreibung der Sperre in die dafür vorgesehenen Textfelder ein.

    b. Wählen Sie im Bereich Gesetzliche Aufbewahrungsfrist aus, wie Sie die Ressource auswählen möchten, die in die Sperre aufgenommen werden soll. Wenn Sie einen Aufbewahrungszeitraum erstellen, wählen Sie die Methode aus, mit der die Ressourcen ausgewählt werden, die sich innerhalb des gesetzlichen Aufbewahrungszeitraums befinden. Sie können den Einschluss einer der folgenden Optionen auswählen:

        - Spezifische Ressourcentypen und IDs

- Wählen Sie Backup-Tresore aus
- Alle Ressourcentypen oder alle Backup-Tresore in Ihrem Konto

c. Geben Sie den Zeitraum an, für den Ihre gesetzliche Aufbewahrung gilt. Geben Sie die Daten im Format YYYY:MM:DD ein (Datumsangaben sind inklusive).

d. Optional können Sie unter Rechtliche Aufbewahrungstags Stichwörter für den Aufbewahrungszeitraum hinzufügen. Mithilfe von Stichwörtern können Sie die Sperre kategorisieren, sodass Sie future zurückgreifen und sie organisieren können. Sie können insgesamt bis zu 50 Tags hinzufügen.

5. Wenn Sie mit der Konfiguration Ihrer neuen gesetzlichen Sperre zufrieden sind, klicken Sie auf die Schaltfläche Neue Sperre hinzufügen.

Erstellen Sie einen gesetzlichen Aufbewahrungszeitraum mit dem AWS CLI

Sie können eine gesetzliche Sperre mit dem create-legal-holdBefehl erstellen.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Sehen von rechtlichen Aufbewahrungsfristen

Sie können Details zur gesetzlichen Sperre in der AWS Backup Konsole oder programmgesteuert anzeigen.

In der Konsole können Sie sich gesetzliche Aufbewahrungsfristen anzeigen lassen

Um alle gesetzlichen Aufbewahrungsfristen innerhalb eines Kontos mit der Backup-Konsole einzusehen,

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Klicken Sie im linken Teil des Dashboards unter Mein Konto auf Gesetzliche Aufbewahrungsfristen.
3. In der Tabelle mit den gesetzlichen Aufbewahrungsfristen werden Titel, Status, Beschreibung, ID und Erstellungsdatum vorhandener Sperren angezeigt. Klicken Sie auf das Karat (Abwärtspfeil) neben der Tabellenüberschrift, um die Tabelle nach der ausgewählten Spalte zu filtern.

Rechtliche Beschränkungen programmatisch anzeigen

Um alle gesetzlichen Aufbewahrungsfristen programmgesteuert anzuzeigen, können Sie die folgenden API-Aufrufe verwenden: ListLegalHoldsund. GetLegalHold

Die folgende JSON-Vorlage kann für verwendet werden. `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
        }
   }
}
```

Die folgende JSON-Vorlage kann für verwendet werden`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,
  ]

}
```

Im Folgenden sind die möglichen Statuswerte aufgeführt.

Status	Description
WIRD ERSTELLT	Angeforderte Wiederherstellungspunkte werden gerade zurückgehalten, und Löschanfragen dieser Wiederherstellungspunkte können erfolgreich sein, da die Erstellung des Holds noch nicht abgeschlossen ist.
ACTIVE	Der gesetzliche Aufbewahrungszeitraum wurde eingerichtet. Alle Wiederherstellungspunkte, die

Status	Description
	unter diesem gesetzlichen Aufbewahrungszeitraum aufgeführt sind, werden gespeichert.
CANCELLING	Rechtliche Sperren werden gerade aufgehoben und Anfragen zum Löschen von Wiederherstellungspunkten, die sich unter dieser Sperre befinden, sind möglicherweise erfolgreich.
CANCELED	Die gesetzliche Sperre ist vollständig aufgehoben und hat keine Wirkung mehr. Wiederherstellungspunkte können gelöscht werden.

Erstellen einer gesetzlichen Aufbewahrungsfrist

Gesetzliche Sperren bleiben in Kraft, bis sie von einem Benutzer mit ausreichenden Berechtigungen entfernt werden. Das Entfernen einer gesetzlichen Sperre wird auch als Aufheben, Löschen oder Aufheben einer gesetzlichen Sperre bezeichnet. Durch das Entfernen einer gesetzlichen Aufbewahrungsfrist wird sie aus allen Sicherungen entfernt, an die sie angehängt wurde. Alle Backups, die während des gesetzlichen Aufbewahrungszeitraums abgelaufen sind, werden innerhalb von 24 Stunden nach Aufhebung des gesetzlichen Aufbewahrungszeitraums gelöscht.

Heben Sie mithilfe der -Konsole eine gesetzliche Aufbewahrungsfrist auf

Um eine Sperre mithilfe der Konsole aufzuheben

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Geben Sie die Beschreibung ein, die Sie der Veröffentlichung zuordnen möchten.
3. Überprüfen Sie die Details und klicken Sie dann auf Sperre aufheben.
4. Wenn das Dialogfeld „Sperre aufheben“ (Release hold) angezeigt wird, bestätigen Sie, dass Sie beabsichtigen, die Sperre aufzuheben, indem Sie `confirm` in das Textfeld eingeben.

    - Markieren Sie das Kästchen, das bestätigt, dass Sie die Sperre aufheben.

Auf der Seite Gestzliche Aufbewahrungsfristen (Legal holds) können Sie alle Ihre Sperren einsehen. Wenn die Freigabe erfolgreich war, wird der Status dieser Sperre als angezeigt`Released`.

Eine gesetzliche Sperre programmgesteuert aufheben

Verwenden Sie den API-Aufruf, um eine Sperre programmgesteuert zu entfernen. CancelLegalHold

Verwenden Sie die folgende JSON-Vorlage.

```
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 ermöglicht es Ihnen, eine private Verbindung zwischen Ihrer Virtual Private Cloud („VPC“) und AWS Backup Endpunkten herzustellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, die es Ihnen ermöglicht, privat auf AWS Backup APIs zuzugreifen, indem der gesamte Netzwerkverkehr zwischen Ihrer VPC und AWS Backup dem Amazon-Netzwerk eingeschränkt wird.

AWS PrivateLink ermöglicht Ihnen den privaten Zugriff auf AWS Backup Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder Verbindung. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit AWS Backup API-Endpunkten zu kommunizieren. Ihre Instances benötigen auch keine öffentlichen IP-Adressen, um die verfügbaren AWS Backup API- und Backup-Gateway-API-Operationen zu verwenden. Datenverkehr zwischen Ihrer VPC und dem, der das Amazon-Netzwerk AWS Backup nicht verlässt.

Weitere Informationen zu VPC-Endpunkten finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon VPC Benutzerhandbuch.

Überlegungen zu Amazon VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für AWS Backup Endpoints einrichten, lesen Sie die Eigenschaften und Einschränkungen der Schnittstellen-Endpunkte im Amazon VPC-Benutzerhandbuch.

Alle für die Verwaltung von Amazon Backup-Ressourcen relevanten AWS Backup Vorgänge sind über Ihre VPC verfügbar unter AWS PrivateLink.

VPC-Endpunktrichtlinien werden für Sicherungsendpunkte unterstützt. Standardmäßig ist der vollständige Zugriff auf Sicherungsoperationen über den Endpunkt zulässig. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Einen AWS Backup VPC-Endpunkt erstellen

Sie können einen VPC-Endpunkt für die AWS Backup Verwendung entweder der Amazon VPC-Konsole oder der AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Amazon VPC Benutzerhandbuch.

Erstellen Sie einen VPC-Endpunkt für die AWS Backup Verwendung des Dienstnamens`com.amazonaws.`*`region`*`.backup`.

In den Regionen China (Peking) und China (Ningxia) sollte der Servicename `cn.com.amazonaws.`*`region`*`.backup` lauten.

Verwenden Sie `com.amazonaws.`*`region`*`.backup-gateway` für Backup-Gateway-Endpunkte.

Die folgenden TCP-Ports müssen in der Sicherheitsgruppe zulässig sein, wenn ein VPC-Endpunkt für das Backup-Gateway erstellt wird:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
TCP	443 (HTTPS)	Ausgehend	Backup-Gateway	AWS	Für die Kommunikation vom Backup Gateway zum AWS Service-Endpunkt

Verwenden eines VPC-Endpunkts

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an AWS Backup den VPC-Endpunkt stellen, indem Sie beispielsweise `backup.us-east-1.amazonaws.com` dessen Standard-DNS-Namen für die AWS Region verwenden.

Für die Regionen China (Peking) und China (Ningxia) sollten API-Anfragen jedoch mit dem VPC-Endpunkt unter Verwendung von `backup.cn-north-1.amazonaws.com.cn` und `backup.cn-northwest-1.amazonaws.com.cn` gestellt werden. AWS-Regionen

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf die Amazon Backup-API steuert. Die Richtlinie legt Folgendes fest:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

> **Important**
>
> Wenn eine nicht standardmäßige Richtlinie auf einen VPC-Schnittstellen-Endpunkt für angewendet wird AWS Backup, werden bestimmte fehlgeschlagene API-Anfragen, z. B. solche, die von fehlschlagen`RequestLimitExceeded`, möglicherweise nicht bei Amazon AWS CloudTrail oder Amazon protokolliert. CloudWatch

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS Backup

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für AWS Backup. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie Zugriff auf die aufgelisteten AWS Backup Aktionen für alle Prinzipien auf allen Ressourcen.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Beispiel: VPC-Endpunkt-Richtlinie, die den gesamten Zugriff über ein angegebenes AWS -Konto verweigert

Die folgende VPC-Endpunktrichtlinie verweigert dem AWS Konto `123456789012` jeglichen Zugriff auf Ressourcen, die den Endpunkt verwenden. Die Richtlinie erlaubt alle Aktionen von anderen Konten.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Weitere Informationen zu verfügbaren API-Antworten finden Sie im API-Leitfaden.

Availability unterstützt AWS Backup derzeit VPC-Endpunkte in den folgenden Regionen: AWS

- Region USA Ost (Ohio)
- Region USA Ost (Nord-Virginia)
- Region USA West (Oregon)
- Region US West (N. California)
- Region Afrika (Kapstadt)
- Region Asien-Pazifik (Hongkong)
- Region Asien-Pazifik (Mumbai)
- Region Asien-Pazifik (Osaka)
- Asia Pacific (Seoul) Region
- Region Asien-Pazifik (Singapur)
- Region Asien-Pazifik (Sydney)
- Region Asien-Pazifik (Tokio)
- Region Kanada (Zentral)

- Region Europa (Frankfurt)
- Region Europa (Irland)
- Region Europa (London)
- Region Europa (Paris)
- Region Europa (Stockholm)
- Region Europa (Mailand)
- Region Naher Osten (Bahrain)
- Region Südamerika (São Paulo)
- Region Asien-Pazifik (Jakarta)
- Region Asien-Pazifik (Osaka)
- Region China (Peking)
- Region China (Ningxia)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

> **Note**
>
> AWS Backup für VMware ist in den Regionen China (Region China (Peking) und Region China (Ningxia)) oder Asien-Pazifik (Jakarta) nicht verfügbar.

Resilienz in AWS Backup

AWS Backup nimmt ihre Widerstandsfähigkeit — und Ihre Datensicherheit — sehr ernst.

AWS Backup speichert Ihre Backups mit mindestens der Stabilität und Haltbarkeit, die Ihnen der ursprüngliche AWS Service Ihrer Ressource bieten würde, wenn Sie sie dort sichern würden.

AWS Backup ist so konzipiert, dass es die AWS globale Infrastruktur nutzt, um Ihre Backups über mehrere Availability Zones hinweg zu replizieren und so eine Haltbarkeit von 99,999999999% (11 Neunen) pro Jahr zu erreichen, vorausgesetzt, Sie halten sich an die aktuelle Dokumentation. AWS Backup

AWS Backup verschlüsselt Ihre Backup-Pläne im Ruhezustand und sichert sie kontinuierlich. Sie können den Zugriff auf Ihre Backup-Pläne auch mithilfe von AWS Identity and Access Management

(IAM-) Anmeldeinformationen und -Richtlinien einschränken. Weitere Informationen finden Sie unter Authentication, Access Control und Security Best Practices in IAM.

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. AWS Backup speichert Ihre Backups in verschiedenen Availability Zones. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren. Weitere Informationen finden Sie unter AWS Backup Service Level Agreement (SLA).

Darüber hinaus können AWS Backup Sie Ihre Backups regionsübergreifend kopieren, um die Ausfallsicherheit zu erhöhen. Weitere Informationen zur Funktion für AWS Backup regionsübergreifendes Kopieren finden Sie unter Erstellen einer Backup.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

AWS Backup Kontingente

Die folgenden Kontingente gelten für die Arbeit mit AWS Backup. Viele AWS Backup Kontingente sind anpassbar, sofern der Ressourcentyp Service dies zulässt. Um eine Kontingentanpassung anzufordern, beschreiben Sie Ihren Anwendungsfall dem AWS Support.

AWS Backup Kontingente

Ressource	Kontingent	Hinweise
Anzahl der Backup-Tresore pro Region und Konto	300	Sie können eine Anpassung anfordern.
Anzahl der Wiederherstellungspunkte pro Sicherungstresor	1 000 000	Sie können eine Anpassung anfordern.
Anzahl der Backup-Pläne pro Region und Konto	300	Sie können eine Anpassung anfordern.
Anzahl der Versionen pro Sicherungsplan	2.000	Sie können eine Anpassung anfordern.
Anzahl der Ressourcenzuweisungen pro Sicherungsplan	100	Nicht anpassbar
Anzahl der aktiven Backup-Aufträge pro Konto	Unbegrenzt	
Anzahl gleichzeitiger Sicherungskopien pro Konto ausgehend in eine Zielregion	100	Sie können eine Anpassung für bestimmte Ressourcen beantragen (derzeit virtuelle Maschinen, Advanced DynamoDB, Timestream, Amazon EFS und SAP HANA-Datenbanken auf Amazon-EC 2-Instances).

Ressource	Kontingent	Hinweise
Anzahl gleichzeitiger Kopien pro Ziel-Backup-Tresor im Konto, nachdem das Limit (Eintrag oben) erreicht wurde	5	Nicht anpassbar
Anzahl der gleichzeitigen kontenübergreifenden Kopien, die von derselben Ressource in dieselbe Zielregion erstellt werden können	30	Nicht anpassbar.
Anzahl der gleichzeitigen Backup- und Kopieraufträge pro Ressource	1	Nicht anpassbar. Dieses Kontingent hilft Ihnen, die Leistung Ihrer Workloads aufrechtzuerhalten.
Anzahl der Metadaten-Tags pro Sicherung	50	Sie können keine Anpassung beantragen. AWS legt dieses Kontingent für alle Ressourcen fest. Weitere Informationen finden Sie unter Einschränkungen und Anforderungen für die Benennung von Tags im Referenzhandbuch für AWS .
Anzahl der Tags pro Ressourcenauswahl in einer kontoübergreifenden Backup-Richtlinie	30	Nicht anpassbar. Zusätzliche Tags können hinzugefügt werden, indem mehrere Ressourcenzuweisungen oder Backup-Pläne verwendet werden.
Anzahl der Hypervisoren	10	Nicht anpassbar
Anzahl der gesetzlichen Aufbewahrungsfristen	50 pro Konto	Nicht anpassbar

Ressource	Kontingent	Hinweise
Maximale Anzahl verschachtelter Backup-Layer von Anwendungs-Stacks	10	Nicht anpassbar

AWS Backup der Amazon Timestream Timestream-Ressourcenkontingente

Ressource	Kontingent	Hinweise
Anzahl gleichzeitiger Timestream-Backup-Aufträge pro Konto	4	Sie können eine Anpassung anfordern.
Anzahl gleichzeitiger Timestream-Wiederherstellungsaufträge pro Konto	1	Sie können eine Anpassung anfordern.

Es gibt Kontingente für eine einzelne Ressourcenzuweisung in einer einzigen Backup-Regel. Sie können einen Backup-Plan mit mehreren Backup-Regeln erstellen.

AWS Backup Quoten für Audit Manager

Ressource	Kontingent	Hinweise
Anzahl der Frameworks pro Konto und Region	15	Sie können eine Anpassung anfordern.
Anzahl an der Steuerelemente pro Konto und Region	50	Sie können eine Anpassung anfordern.
Anzahl der Reaktionspläne pro Konto	20	Sie können eine Anpassung anfordern.
Anzahl von Frameworks pro Berichtsplan	1.000	Nicht anpassbar

Ressource	Kontingent	Hinweise
Maximale Anzahl von Konten multipliziert mit Regionen in einem Reaktionsplan	300	Nicht anpassbar

Wiederherstellungstestplan-Kontingente

Ressource	Kontingent	Hinweise
Wiederherstellungstestpläne	100	Nicht anpassbar
Anzahl der Tags in jedem Plan	50	Nicht anpassbar
Auswahl pro Plan	30	Nicht anpassbar
ARNs pro Wiederherstellungstest-Auswahl	30	Nicht anpassbar
Bedingungen pro Auswahl	30	Schließt diejenigen ein, die sowohl in `StringEquals` als auch in `StringNotEquals` enthalten sind.
Tresorauswahlen pro Wiederherstellungstest-Auswahl	30	Nicht anpassbar
Maximalwert (in Tagen) des Auswahlfensters	365 Tage	
Grenzen für Startfensterstunden	Minimum: 1 Stunde; Maximum: 168 Stunden	
Maximale Zeichenlänge des Namens des Wiederherstellungstestplans	50 Zeichen	Alphanumerische Zeichen und Unterstriche, keine Leerzeichen

Ressource	Kontingent	Hinweise
Maximale Zeichenlänge des Namens der Wiederherstellungstest-Auswahl	50 Zeichen	Alphanumerische Zeichen und Unterstriche, keine Leerzeichen

AWS Backup gateway Kontingente

Ressource	Kontingent	Hinweise
Backup- oder Wiederherstellungsaufträge pro Gateway	4	Sie können keine Anpassung anfordern. Erstellen Sie stattdessen mehr Gateways und verbinden Sie sie mit Ihrem Hypervisor.

Wenn Sie Backups für mehrere Konten mithilfe von verwalten AWS Organizations, stoßen Sie möglicherweise auf Kontingente, die AWS Organizations vorgegeben werden. Informationen zu diesen Kontingenten finden Sie unter Kontingente für AWS Organizations im AWS Organizations - Benutzerhandbuch.

Möglicherweise stoßen Sie auch auf Kontingente, die Ihnen von einem AWS Backup unterstützten Dienst auferlegt werden, darunter:

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon-DynamoDB
- Amazon FSx für Lustre
- Amazon FSx für Windows File Server
- Amazon DocumentDB

- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

Überwachen

AWS Backup arbeitet mit anderen AWS Tools zusammen, sodass Sie die Workloads überwachen können. Diese Tools umfassen u. a. folgende:

- AWS Backup Konsolen-Dashboards
  - Das Auftrags-Dashboard ermöglicht die Überwachung des Auftragsstatus. Hier können Sie Kennzahlen zu erfolgreichen und fehlgeschlagenen Aufträgen einsehen, gefiltert nach Gründen, Konten, Region und Ressourcentyp.
  - Das Job-Dashboard ist in Regionen verfügbar, in denen AWS Backup Audit Manager unterstützt wird. Informationen zu diesen Regionen finden Sie unter Verfügbarkeit der Funktionen von AWS-Region. Alle anderen Regionen können auf das CloudWatch Dashboard zugreifen.
- Amazon CloudWatch und Amazon EventBridge zur Überwachung von AWS Backup Prozessen.
  - Sie können CloudWatch damit Kennzahlen verfolgen, Alarme erstellen und Dashboards anzeigen.
  - Sie können es verwenden EventBridge , um AWS Backup Ereignisse anzuzeigen und zu überwachen.

  Weitere Informationen finden Sie unter AWS Backup Ereignisse mit Amazon überwachen EventBridge.
- AWS CloudTrailum AWS Backup API-Aufrufe zu überwachen. Sie können die Uhrzeit, die Quell-IP, die Benutzer und die Konten identifizieren, die diese Aufrufe tätigen. Weitere Informationen finden Sie unter AWS Backup API-Aufrufe protokollieren mit CloudTrail.
- Amazon Simple Notification Service (Amazon SNS), um verwandte Themen wie Sicherungs-, Wiederherstellungs- und Kopierereignisse zu AWS Backup abonnieren. Weitere Informationen finden Sie unter Benachrichtigungsoptionen mit AWS Backup.

AWS Backup Konsolen-Dashboards

> **Note**
>
> Das Job-Dashboard ist in allen Regionen verfügbar, in denen AWS Backup Audit Manager unterstützt wird. Informationen zu diesen Regionen finden Sie unter Verfügbarkeit der

Funktionen von AWS-Region. Alle anderen Regionen können auf das CloudWatch Dashboard zugreifen.

Themen

Übersicht über Backup-Dashboards

AWS Backup bietet in der Konsole ein Job-Dashboard, mit dem Sie den Zustand Ihrer Sicherungs-, Kopier- und Wiederherstellungsaufträge überwachen können. Dieselben Daten, die in der Konsole visuell angezeigt werden, können über die Befehlszeile abgerufen werden AWS CLI.

Das Auftrags-Dashboard kann verwendet werden, um Probleme mit Backup-, Kopier- und Wiederherstellungsaufträgen durch Überwachung auf Organisationsebene oder Mitgliedskonten zu identifizieren. Anhand dieser Informationen können Sie Ereignisse und mögliche Probleme identifizieren und diagnostizieren, um sicherzustellen, dass Ihre Aktivitäten korrekt ablaufen.

Das Auftrags-Dashboard kann zwei Zeitrahmen anzeigen. Standardmäßig werden Daten der letzten 14 Tage angezeigt, Sie können die Ansicht jedoch so ändern, dass sie die letzten 7 Tage anzeigt. Wenn Sie den Zeitrahmen ändern, werden die Daten entsprechend dem neuen Zeitintervall aktualisiert.

Beachten Sie, dass im Dashboard Daten bis zum letzten Tag um 0:00 Uhr UTC angezeigt werden. Das heißt, die Daten des aktuellen Tages sind nicht enthalten. Das Dashboard wird täglich zwischen ca. 1:30 und 2:30 Uhr UTC aktualisiert.

Anzeigen des Auftrags-Dashboards

Um das Job-Dashboard aufzurufen, melden Sie sich bei der AWS Backup Konsole an und wählen Sie in der linken Navigationsleiste Jobs-Dashboards aus.

Auf der Auftrags-Dashboard-Seite können Sie zwischen den Registerkarten für Backup-, Kopier- oder Wiederherstellungsaufträge wählen.

In der Übersicht über das Auftrags-Dashboard wird eine aggregierte Ansicht der Auftragsaktivitäten über den angegebenen Zeitraum angezeigt, einschließlich abgeschlossener Aufträge, abgeschlossener Aufträge mit Problemen, abgelaufener und fehlgeschlagener Aufträge. Standardmäßig werden Daten der letzten 14 Tage angezeigt, Sie können die Ansicht jedoch so ändern, dass sie 7 Tage anzeigt.

> **Note**
>
> `Completed with issues` ist der Status eines Auftrags, der in der Konsole angezeigt wird und einen abgeschlossenen Auftrag mit einer Statusmeldung kennzeichnet.

Auftragszustand

Das Liniendiagramm zeigt die Raten für erfolgreiche und erfolglose Aufträge im Zeitverlauf an. Die Linie mit der Erfolgsquote zeigt eine Zusammenfassung der abgeschlossenen und abgeschlossenen Aufträge mit Problemen. Die Linie mit der Rate fehlgeschlagener Aufträge zeigt die Summe der fehlgeschlagenen und abgelaufenen Aufträge gemäß dem angegebenen Zeitraum.

Aufträge mit dem Status „Nicht abgeschlossen“ oder „Nicht fehlgeschlagen“ (Aufträge mit dem Status „Erstellt“, „Ausstehend“, „Wird ausgeführt“, „Abgebrochen“ oder „Teilweise“) sind nicht enthalten. Die Gesamtwerte in Prozent entsprechen möglicherweise nicht 100 %.

Auftragsstatus im Zeitverlauf

Mit dem Balkendiagramm können Sie ein benutzerdefiniertes Balkendiagramm erstellen, das die Anzahl der Aufträge in jeder Kategorie (Abgeschlossen, Mit Problemen abgeschlossen, Fehlgeschlagen und Abgelaufen), verteilt nach Tagen, anzeigt.

Wählen Sie in den Dropdownmenüs die Status (e), Ressourcentypen und AWS Regionen aus, die Sie im Diagramm sehen möchten. Wenn Sie Ihre Auswahl genauer untersuchen möchten, wählen Sie Aufträge anzeigen aus, um einen vorgefilterten Teil der Seite für die Aufträge/kontoübergreifende Überwachung zu sehen.

Sie können den Mauszeiger über einen Balken bewegen, um ein Popover mit detaillierten Auftragsdaten für das ausgewählte Datum anzuzeigen.

Problematische Aufträge

Ein problematischer Auftrag ist ein Auftrag mit dem Status „Fehlgeschlagen“, „Abgelaufen“ oder „Abgeschlossen mit Problemen“. In jedem Diagramm wird die entsprechende Metrik angezeigt, die entweder die Konten, Ressourcentypen oder die wichtigsten Gründe für die meisten problematischen Aufträge enthält.

In der Standardanzeige wird das Dashboard-Widget nach der angegebenen Metrik in absteigender Reihenfolge sortiert, beginnend mit der Metrik mit der höchsten Anzahl problematischer Aufträge, die zur Metrik gehören.

Die Anzeige der Konten mit den häufigsten Problemen ist nur bei Konten sichtbar, die über Organizations Zugriff haben, z. B. bei Administratorkonten und delegierten Administratorkonten. Falls sichtbar, können Sie den Mauszeiger über ein Konto bewegen, um die Anzahl der problematischen Aufträge anzuzeigen, die zu dem ausgewählten Konto gehören.

Sie können einen Balken im Diagramm auswählen, um ein Popup-Fenster zu öffnen. In diesem Fenster können Sie einen Auftragsstatus auswählen, um eine nach dem ausgewählten Status gefilterte Tabelle zur Überwachung von Aufträgen und Konten zu öffnen.

Gründe für problematische Aufträge

Das Widget Häufigste Gründe für Probleme zeigt die Nachrichtencode-Kategorie an, zu der die Fehlermeldungen gehören. Die Kategorie erläutert jedoch möglicherweise nicht die Probleme, auf die ein Auftrag stößt. Erweitern Sie die folgenden Nachrichtencode-Kategorien, um weitere Informationen zu den spezifischen Meldungen oder Fehlern zu erhalten, auf die Ihre Aufträge stoßen könnten.

„VSS_ERROR“

- „Der Windows-VSS-Backup-Versuch ist fehlgeschlagen, weil entweder die Instance oder der SSM-Agent einen ungültigen Status oder unzureichende Berechtigungen hat.“
- „Der Windows-VSS-Backup-Versuch ist fehlgeschlagen, da die Berechtigungen zum Ausführen dieses Vorgangs nicht ausreichen“
- „Der Windows-VSS-Backup-Versuch ist fehlgeschlagen, weil ec2-vss-agent.exe nicht in der Instance installiert ist“
- „Beim Versuch, ein reguläres Backup durchzuführen, ist ein Fehler beim Windows-VSS-Backup-Auftrag aufgetreten“
- „Der Windows-VSS-Backup-Versuch ist aufgrund eines Timeouts bei der Erstellung von VSS-aktivierten Snapshots fehlgeschlagen“

- „Der Windows-VSS-Backup-Versuch ist aufgrund einer nicht unterstützten Windows-Server-Version fehlgeschlagen. Unterstützte Versionen sind Windows Server 2012 oder höher.“
- „Der Windows-VSS-Backup-Versuch ist aufgrund eines Timeouts bei der Erstellung von VSS-aktivierten Snapshots fehlgeschlagen“

„LIMIT_EXCEEDED“

- „Subscriber-Limit überschritten: Sie haben die maximale Anzahl gleichzeitiger Backups erreicht, die 300 beträgt. Warten Sie, bis andere Aufträge abgeschlossen sind, und versuchen Sie es dann erneut. Sie können sich auch an uns wenden, AWS Support um eine Erhöhung des Kontingents zu beantragen.“
- „Die maximal zulässige Anzahl laufender Snapshots für ein einzelnes Volume wurde überschritten.“
- „Die maximal zulässige Obergrenze für aktive Snapshots wurde überschritten.“
- „Es können nicht mehr als 20 Benutzer-Snapshots erstellt werden“
- „Das resultierende Tag-Set darf nicht mehr als 50 Benutzer-Tags enthalten.“
- „Sie haben die maximale Anzahl unterstützter Backups für Ihr Konto/Ihre Datenbank erreicht. Weitere Informationen finden Sie unter „Kontingente“ im Timestream-Entwicklerhandbuch.“
- „Sie haben Ihr Kontingent von 50 000 für die Anzahl der in dieser Region zulässigen öffentlichen und privaten Bilder erreicht. Melden Sie ungenutzte Bilder ab oder fordern Sie eine Erhöhung Ihres AMI-Kontingents an.“
- „Ihr Backup war erfolgreich, aber wir konnten die NetworkInterfaces Metadaten nicht speichern, da ihre Größe unsere internen Grenzwerte überschritten hat.“
- „REGEX#Subscriber-Limit überschritten“
- „REGEX#Mehr als 50 Tags angegeben“
- „REGEX#Obergrenze ist“

"ACCESS_DENIED"

- „Sie sind zur Ausführung dieser Operation nicht autorisiert.“
- „Beim Versuch, den AWS Backup Service anzurufen, wurde der Zugriff verweigert“
- „Bilder von AWS Marketplace können nicht auf ein anderes AWS Konto kopiert werden.“
- „Der Kopierauftrag ist fehlgeschlagen, weil der Backup-Ziel-Tresor mit dem standardmäßigen verwalteten Schlüssel des Backup-Service verschlüsselt ist. Der Inhalt dieses Tresors kann nicht

kopiert werden. Nur der Inhalt eines mit einem AWS KMS Schlüssel verschlüsselten Backup-Tresors darf kopiert werden.

- Mit dem verschlüsselte Schnappschüsse Von AWS verwalteter Schlüssel können nicht geteilt werden. Geben Sie einen anderen Snapshot an.
- „Verschlüsselte Snapshots mit dem Amazon-EBS-Standardschlüssel können nicht weitergegeben werden
- „Kopierauftrag fehlgeschlagen. Quell- und Ziel-Konto müssen zur selben Organisation gehören.“
- „REGEX#Zugriff verweigert“
- „REGEX#nicht autorisiert für“
- „REGEX #cannot wird angenommen von AWS Backup
- „REGEX#hat nicht die Berechtigung“
- „REGEX#Berechtigung fehlt“

„CONCURRENT_JOB“

- „Der Backup-Auftrag ist fehlgeschlagen, weil ein Auftrag für dieselbe Ressource ausgeführt wurde.“

„FEATURE_NOT_ENABLED“

- „Kopierauftrag fehlgeschlagen. Das Feature zum kontoübergreifenden Kopieren ist für die aktuelle Organisation nicht aktiviert.“

„JOB_EXPIRED“

- „Der Backup-Auftrag ist vor Abschluss abgelaufen.“

„INVALID_LIFECYCLE“

- „Kopierauftrag fehlgeschlagen. Die im Auftrag angegebene Aufbewahrung liegt nicht innerhalb des für den Ziel-Backup-Tresor angegebenen Bereichs.“
- „REGEX#konnte nicht gestartet werden, weil es entweder innerhalb oder zu nahe am konfigurierten wöchentlichen Wartungszeitfenster liegt“
- „REGEX#konnte nicht gestartet werden, weil es entweder innerhalb oder zu nahe am konfigurierten automatisierten Backup-Zeitfenster liegt“

„INVALID_STATE“

- „REGEX#Instance ist nicht im Status“
- „REGEX#nicht im verfügbaren Status“
- „REGEX#nicht im verfügbaren Status“
- „REGEX#Snapshot von Volume nicht möglich“

„KMS_KEY_ERROR“

- „Der KMS-Schlüssel ist entweder deaktiviert oder das Löschen steht noch aus oder der Zugriff auf den KMS-Schlüssel wurde verweigert“
- „Auf die angegebene Schlüssel-ID kann nicht zugegriffen werden“
- „Das Kopieren des AMI-Snapshots ist mit dem folgenden Fehler fehlgeschlagen: Auf die angegebene Schlüssel-ID kann nicht zugegriffen werden. Sie müssen über DescribeKey Berechtigungen für das Standard-CMK verfügen“
- „REGEX#kms-Schlüssel“

„ACCESS_KEY_ERROR“

- „Die AWS Access Key-ID benötigt ein Abonnement für den Dienst“

„HYPERVISOR_OFFLINE“

- „Dieser Vorgang ist für den angegebenen Hypervisor nicht gültig, da er nicht online ist“

„RESOURCE_NOT_FOUND“

- „Das angegebene Volume wurde nicht gefunden.“
- „Die virtuelle Maschine wurde nicht gefunden.“
- „Die angegebene Schlüssel-ID ist nicht vorhanden“
- „REGEX#ist nicht vorhanden“
- „REGEX#Ressource nicht gefunden“
- „REGEX#Cryopod nicht gefunden“
- „REGEX#Wiederherstellungspunkt nicht gefunden“

- „REGEX#Ressource nicht gefunden“
- „REGEX#nicht mehr verfügbar“
- „REGEX#ist ungültig“

„RESOURCE_NOT_SUPPORTED“

- „REGEX#nicht unterstützter Ressourcentyp“
- „REGEX#Nicht unterstützter Ressourcentyp“

„TAG_COPY_ERROR“

- „Aufgrund eines internen Fehlers können wir keine Ressourcen-Tags in Ihr Backup kopieren.“
- „Wir können keine Ressourcen-Tags in Ihr Backup kopieren, da der Quell- oder Zielwiederherstellungspunkt nicht verfügbar ist“

„TOKEN_EXPIRED“

- „Token abgelaufen. Bitte versuchen Sie es erneut.“

„UNSUPPORTED_OPERATION“

- CreateSnapshot Die Methode "wird auf dem Hypervisor während der Snapshot-Erstellung nicht unterstützt. Backup-Auftrag abgebrochen“
- „UnsupportedOperation : Für Storage Gateway Gateway-Backup-Kopien sind ein vom Benutzer erstellter Backup-Tresor und CMK am Ziel erforderlich.“
- „REGEX#Feature wird für den angegebenen Ressourcentyp nicht unterstützt.“

„FATAL_ERROR“

- „Es ist ein interner Fehler aufgetreten.“
- „Beim Kopierauftrag ist ein schwerwiegender Fehler aufgetreten. Bitte kontaktieren Sie den AWS Support für weitere Unterstützung.“
- „Beim Kopierauftrag ist ein schwerwiegender Fehler aufgetreten.“
- „REGEX#Beim Backup-Auftrag ist ein schwerwiegender Fehler aufgetreten“

Abrufen von Dashboard-Daten über AWS CLI

Sie können die Befehlszeilenschnittstelle verwenden, um die Daten abzurufen, die in der Konsole angezeigt werden. Verwenden Sie einen der folgenden CLI-Befehle:

- list-backup-job-summaries
- list-copy-job-summaries
- list-restore-job-summaries

Es gibt gültige Parameter, die Sie in jeden Befehl aufnehmen können:

```
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)
```

Dieses Beispiel zeigt eine Beispielanforderung, bei der ein Benutzer die Eingabe `list-backup-job-summaries` macht, bei der die Anforderung dazu auffordert, alle verfügbaren Konten zurückzugeben, deren Status in den letzten 14 Tagen `FAILED` war:

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Um eine Auftragsanzahl für Aufträge mit dem Status `completed with issues` zu erhalten, subtrahieren Sie die Anzahl der `COMPLETED`-Aufträge mit der `MessageCategory` `SUCCESS` von der Gesamtzahl von `COMPLETED`.

AWS Backup Ereignisse mit Amazon überwachen EventBridge

AWS Backup sendet Ereignisse an Amazon, EventBridge wenn sich der Status eines Sicherungs- oder Kopierauftrags ändert. Sie können es verwenden EventBridge , um AWS Backup Ereignisse zu überwachen. Sie können beispielsweise einen Alarm erhalten, wenn ein Backup-Job fehlschlägt. AWS Backup sendet nach EventBridge bestem Wissen und Gewissen alle 5 Minuten Ereignisse aus.

Informationen zum Verfolgen von Ereignissen mithilfe von EventBridge:

- Eine Regel erstellen, die auf Ereignisse reagiert (EventBridge Amazon-Benutzerhandbuch)
- CloudWatch Amazon-Ereignisse und -Metriken für AWS Backup (Blog — siehe AWS Backup Ereignisse für das Senden an Amazon konfigurieren EventBridge)

Einige Ereignisse melden `status: COMPLETED`, während andere Ereignisse `state: COMPLETED` melden. Dies steht im Einklang mit der AWS Backup API. Einige Status sind AWS Backup konsolenspezifisch: Der `Completed with issues` Statusstatus ist eine Darstellung von `Completed` Jobs mit Statusmeldungen. Um `Completed with issues`-Ereignisse zu überwachen, überwachen Sie `COMPLETED`-Aufträge, für die eine Statusmeldung angezeigt wird.

Sie können alternativ die AWS Backup Benachrichtigungs-API verwenden, um AWS Backup Ereignisse mit Amazon Simple Notification Service (Amazon SNS) zu verfolgen. EventBridge Verfolgt jedoch mehr Änderungen als die Benachrichtigungs-API, einschließlich Änderungen an den Backup-Tresoren, dem Status des Kopierauftrags, den Regionseinstellungen und der Anzahl der kalten oder warmen Wiederherstellungspunkte.

Ereignisse

Backup-Job-Ereignisse

Im Folgenden sind Beispielereignisse aufgeführt.

Status

Status: FEHLGESCHLAGEN


```
{
  "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
  }
}
```

Status: ABGESCHLOSSEN

```
{
  "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
  }
}
```

Status: LÄUFT

```
{
  "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"
    }
  }
}
```

Zustand: ABGEBROCHEN


```
{
  "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
  }
}
```


Status: ABGELAUFEN


```
{
  "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"
    }
  }
}
```

Status: AUSSTEHEND

```
{
  "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
  }
}
```

Bundesstaat: ERSTELLT

```
{
  "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"
  }
}
```

Ereignisse im Backup-Plan

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- Status: GEÄNDERT
- Zustand: GELÖSCHT
- Status: ERSTELLT

Status: GEÄNDERT

```
{
  "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"
  }
}
```

Zustand: GELÖSCHT

```
{
  "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"
  }
}
```

Status: ERSTELLT

```
{
```

```
  "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-Ereignisse

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- Status: ERSTELLT
- Zustand: GEÄNDERT
- Zustand: GELÖSCHT

Status: ERSTELLT

```
{
  "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"
  }
}
```

Zustand: GEÄNDERT

```
{
  "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"
  }
}
```

Zustand: GELÖSCHT

```
{
  "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"
  }
}
```

Job-Ereignisse kopieren

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- Status: FEHLGESCHLAGEN
- Status: LÄUFT
- Status: ABGESCHLOSSEN
- Status: ERSTELLT

Status: FEHLGESCHLAGEN

```
{
  "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": {}
  }
}
```

Status: LÄUFT

```
{
  "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"
    }
  }
}
```

Status: ABGESCHLOSSEN


```
{
  "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"
    }
  }
}
```


Status: ERSTELLT


```
{
  "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"
  }
}
```

Recovery Point-Ereignisse

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- Status: ABGESCHLOSSEN
- Status: GELÖSCHT
- Zustand: GEÄNDERT

Status: ABGESCHLOSSEN

```
{
    "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"
        }
    }
}
```

Status: GELÖSCHT

```
{
  "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"
    }
  }
}
```

Zustand: GEÄNDERT

```
{
  "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"
  }
}
```

Ereignisse in den Regionseinstellungen

Es folgt ein Beispielereignis.

```
{
  "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"
  }
}
```

Job-Ereignisse wiederherstellen

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- Status: FEHLGESCHLAGEN
- Status: LÄUFT
- Status: ABGESCHLOSSEN
- Zustand: AUSSTEHEND
- Bundesstaat: ERSTELLT

Status: FEHLGESCHLAGEN

```
{
  "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."
  }
}
```

Status: LÄUFT

```
{
  "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"
  }
}
```

Status: ABGESCHLOSSEN

```
{
  "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"
  }
}
```

Zustand: AUSSTEHEND

```
{
  "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"
  }
}
```

Bundesstaat: ERSTELLT

```
{
  "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 Metriken mit Amazon CloudWatch

Themen

CloudWatch Dashboard

> **Note**
>
> Das Konsolen-Dashboard hängt davon ab, welche Region auf die Konsole zugreift. Unter Verfügbarkeit der Funktionen von AWS-Region erfahren Sie, welche Regionen Zugriff auf das Auftrags-Dashboard haben. Regionen, die nicht aufgeführt sind, können auf das CloudWatch Dashboard zugreifen.

Ihre AWS Backup Konsole enthält ein Dashboard, in dem Sie Kennzahlen zu abgeschlossenen oder fehlgeschlagenen Sicherungs-, Kopier- und Wiederherstellungsaufträgen einsehen können. In diesem Dashboard können Sie den Auftragsstatus nach Zeitraum sortiert und an den von Ihnen gewünschten Zeitraum angepasst anzeigen.

SO GREIFEN SIE AUF DAS DASHBOARD ZU

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im linken Navigationsbereich die Option Dashboard aus.

DAS DASHBOARD BETRACHTEN UND VERSTEHEN

Das CloudWatch Dashboard zeigt mehrere Widgets an. Jedes Widget zeigt Auftragsmetriken nach Anzahl an. Jedes Widget zeigt mehrere Liniendiagramme. Jede Zeile entspricht einer geschützten Ressource (wenn eine erwartete Ressource nicht angezeigt wird, stellen Sie sicher, dass die Ressource in den Einstellungen aktiviert ist). Auf den Displays werden keine laufenden Aufträge angezeigt.

Die Y-Achse (vertikale Werte) zeigt die Anzahl. Die X-Achse (horizontale Werte) zeigt Zeitpunkte. Wenn im ausgewählten Auftragsstatus keine Datenpunkte zur Visualisierung vorhanden sind, wird

der Wert auf 0 gesetzt. Es wird eine horizontale Linie auf der X-Achse angezeigt. Die Legende mit den Ressourcen ist weiterhin sichtbar.

Die Metriken zeigen konto- und regionsspezifische Informationen zum aktuellen Login an. Um andere Konten oder Regionen anzuzeigen, müssen Sie sich unter dem ausgewählten Konto anmelden.

DAS DASHBOARD ANPASSEN

Standardmäßig ist der angezeigte Zeitrahmen eine Woche. Im oberen Menü gibt es Optionen zur Neudefinition des angezeigten Zeitrahmens. Sie können zwischen 1 Stunde, 3 Stunden, 12 Stunden, 1 Tag, 3 Tagen und 1 Woche auswählen. Darüber hinaus können Sie Benutzerdefiniert auswählen, um einen anderen Wert anzugeben. Durch die Anpassung wird die aktuelle Ansicht vorübergehend an Ihre Spezifikationen angepasst.

Sie können den Mauszeiger über ein Widget bewegen, wodurch oben rechts im Widget eine Schaltfläche Vergrößern angezeigt wird. Klicken Sie auf Vergrößern, um das Widget in der Vollbildansicht zu öffnen. Im Vollbildmodus gibt es weitere Optionen zum Anpassen der Diagrammanzeige, z. B. zum Ändern des Zeitraums (die Zeit zwischen den einzelnen Datenpunkten). Änderungen werden nicht beibehalten, sobald die Vollbildansicht geschlossen wird.

Um jeweils nur einen Ressourcentyp anzuzeigen, klicken Sie in der Diagrammlegende auf den Beschriftungstext des Ressourcentyps, den Sie anzeigen möchten. Dadurch wird die Auswahl aller Ressourcentypen aufgehoben. Um dies rückgängig zu machen, klicken Sie in der Legende auf ein Farbfeld für den Ressourcentyp. Klicken Sie erneut auf den Beschriftungstext eines beliebigen ausgewählten Ressourcentyps, um zur Standardansicht aller Ressourcentypen mit allen ausgewählten Beschriftungen zurückzukehren.

Wenn Sie auf die drei vertikalen Punkte in der oberen rechten Ecke eines Widgets klicken, wird ein Dropdown-Menü mit Optionen zum Aktualisieren, Vergrößern, Anzeigen in Metriken und Anzeigen in Protokollen geöffnet. „In Metriken anzeigen“ öffnet sich die Metrik, die im Widget verwendet wird, in der CloudWatch Konsole. Sie können dort alle Änderungen am Widget vornehmen und das Widget zu einem benutzerdefinierten Dashboard im CloudWatch Dashboard hinzufügen. Alle Änderungen, die Sie im CloudWatch Dashboard vornehmen, werden nicht auf dem Dashboard in der AWS Backup Konsole widergespiegelt. „Als Protokolle anzeigen“ öffnet sich die Seite mit der Protokollansicht in der CloudWatch Konsole.

Um Ihrem eigenen benutzerdefinierten CloudWatch Dashboard angezeigte Widgets hinzuzufügen, klicken Sie oben rechts im Dashboard auf die Schaltfläche Zum Dashboard hinzufügen. Dadurch wird die CloudWatch Konsole geöffnet, in der Sie auswählen können, in welchem benutzerdefinierten Dashboard alle sechs Widgets hinzugefügt werden sollen.

Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Metriken.

Metriken mit CloudWatch

Sie können es verwenden CloudWatch , um AWS Backup Metriken zu überwachen. Der `AWS/Backup` Namespace ermöglicht es Ihnen, die folgenden Metriken zu verfolgen. AWS Backup sendet CloudWatch alle 5 Minuten aktualisierte Metriken aus.

Der Zweck dieser Dokumentationsseite besteht darin, Ihnen Referenzmaterialien zur Verfügung zu stellen, die Sie CloudWatch zur Überwachung AWS Backup verwenden können. Informationen zur Überwachung einer Metrik mithilfe von CloudWatch Amazon CloudWatch Events and Metrics for AWS Backup oder Focus on Metrics and Alarms in a Single AWS Service im CloudWatch Benutzerhandbuch finden Sie im Blog. Informationen zum Einstellen von Alarmen finden Sie unter Verwenden von Amazon CloudWatch Alarms im CloudWatch Benutzerhandbuch.

Kategorie	Metriken	Beispiel-Dimensionen	Beispielanwendungsfall
Aufträge	Anzahl der Backup-, Wiederherstellungs- und Kopieraufträge über jeden Status hinweg, einschließlich `CREATED`, `PENDING`, `RUNNING`, `ABORTED`, `COMPLETED` , `FAILED` und `EXPIRED`. Verschiedene Auftragstypen haben unterschiedliche verfügbare Status.	Ressourcentyp, Tresorname. Der Tresorname von Kopieraufträgen entspricht dem ihres Zieltresores.	Überwachen Sie die Anzahl der fehlgeschlagenen Backup-Aufträge in einem oder mehreren bestimmten Backup-Tresoren. Wenn innerhalb einer Stunde mehr als fünf fehlgeschlagene Aufträge vorliegen , senden Sie eine E-Mail oder SMS über Amazon SNS oder eröffnen Sie ein Ticket damit das Entwicklungsteam dies untersuchen kann.

Kategorie	Metriken	Beispiel-Dimensionen	Beispielanwendungsfall
			Berichtkriterien: Ein Wert ungleich Null
Wiederherstellungspunkte	Anzahl der warmen und kalten Wiederherstellungspunkte über jeden Status hinweg: `MODIFIED`, `COMPLETED` , `PARTIAL`, `EXPIRED`, `DELETED`.	Ressourcentyp, Tresorname.	Verfolgen Sie die Anzahl der gelöschten Wiederherstellungspunkte für Ihre Amazon-EBS-Volumes und verfolgen Sie separat die Anzahl der warmen und kalten Wiederherstellungspunkte in jedem Backup-Tresor. Berichtkriterien: Ein Wert ungleich Null

> **Note**
>
> Der Auftragsstatus von `Completed with issues` ist nur AWS Backup konsolenspezifisch und kann nicht nachverfolgt werden CloudWatch.

Die folgende Tabelle listet alle Metriken auf, die verfügbar sind.

Metrik	Beschreibung
`NumberOfBackupJobsCreated`	Die Anzahl der AWS Backup erstellten Backup-Jobs.
`NumberOfBackupJobsPending`	Die Anzahl der Backup-Aufträge, die gleich in AWS Backup ausgeführt werden.

Metrik	Beschreibung
`NumberOfBackupJobsRunning`	Die Anzahl der Backup-Jobs, die derzeit ausgeführt werden AWS Backup.
`NumberOfBackupJobsAborted`	Die Anzahl der vom Benutzer stornierten Backup-Aufträge.
`NumberOfBackupJobsCompleted`	Die Anzahl der AWS Backup abgeschlossenen Backup-Jobs.
`NumberOfBackupJobsFailed`	Die Anzahl der Backup-Aufträge mit dem Status `Failed`. Wird häufig dadurch verursacht, dass ein Backup-Job während oder 1 Stunde vor einer Datenbankressource oder 4 Stunden vor oder während eines Amazon FSx-Wartu ngsfensters oder eines automatisierten Backup-Fensters geplant und nicht AWS Backup zur Durchführung kontinuierlicher Backups für point-in-time Wiederherstellungen verwendet wird. Unter Point-in-Time Recovery finden Sie eine Liste der unterstützten Services und Anleitungen zur Erstellung kontinuierlicher Backups oder AWS Backup zur Neuplanung Ihrer Backup-Jobs.
`NumberOfBackupJobsExpired`	Die Anzahl der Backup-Jobs mit dem Status. `EXPIRED` Ein Backup-Job wechselt vom Status `CREATED` in „`EXPIRED`Wenn ein Backup nicht innerhalb des Startfensters beginnen kann“.
`NumberOfCopyJobsCreated`	Die Anzahl der konto- und regionsübergreifen den Kopieraufträge, die AWS Backup erstellt hat.

Metrik	Beschreibung
NumberOfCopyJobsRunning	Die Anzahl der konto- und regionsübergreifen den Kopieraufträge, die derzeit in AWS Backup ausgeführt werden.
NumberOfCopyJobsCompleted	Die Anzahl der konto- und regionsübergreifen den Kopieraufträge, die AWS Backup ab geschlossen hat.
NumberOfCopyJobsFailed	Die Anzahl der konto- und regionsübergreifen den Kopieraufträge, die AWS Backup versucht wurden, aber nicht abgeschlossen werden konnten.
NumberOfRestoreJobsPending	Die Anzahl der Wiederherstellungsaufträge, die gleich in AWS Backup ausgeführt werden.
NumberOfRestoreJobsRunning	Die Anzahl der Wiederherstellungsaufträge, die derzeit ausgeführt werden. AWS Backup
NumberOfRestoreJobsCompleted	Die Anzahl der AWS Backup abgeschlossenen Wiederherstellungsaufträge.
NumberOfRestoreJobsFailed	Die Anzahl der Wiederherstellungsaufträge, die AWS Backup versucht wurden, aber nicht abgeschlossen werden konnten.
NumberOfRecoveryPointsCompleted	Die Anzahl der Wiederherstellungspunkte, die AWS Backup erstellt wurden.
NumberOfRecoveryPointsPartial	Die Anzahl der Wiederherstellungspunkte, deren Erstellung AWS Backup begonnen, aber nicht abgeschlossen werden konnte. AWS versucht den Vorgang zu einem späteren Zeitpunkt erneut. Da die Wiederholung jedoch zu einem späteren Zeitpunkt erfolgt, wird der teilweise wiederhergestellte Punkt beibehalten.

Metrik	Beschreibung
`NumberOfRecoveryPointsExpired`	Die Anzahl der Wiederherstellungspunkte, die AWS Backup versucht haben zu löschen, basierend auf Ihrem Aufbewahrungszyklus für Backups, aber nicht gelöscht werden konnten. Ihnen wird der Speicherplatz in Rechnung gestellt, den abgelaufene Backups belegen. Sie sollten diese manuell löschen.
`NumberOfRecoveryPointsDeleting`	Die Anzahl der Wiederherstellungspunkte, AWS Backup die gelöscht werden.
`NumberOfRecoveryPointsCold`	Die Anzahl der Wiederherstellungspunkte, die der AWS Backup Kategorie Cold Storage zugeordnet wurden.

Neben den in der Tabelle aufgeführten Dimensionen sind weitere Dimensionen verfügbar. Um alle Dimensionen einer Metrik anzuzeigen, geben Sie den Namen dieser Metrik in den `AWS/Backup` Namespace des Abschnitts Metriken der CloudWatch Konsole ein.

AWS Backup API-Aufrufe protokollieren mit CloudTrail

AWS Backup ist in AWS CloudTraileinen Dienst integriert, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe AWS Backup als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Backup Konsole und Codeaufrufen für die AWS Backup API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde AWS Backup, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Ob die Anfrage im Namen eines IAM Identity Center-Benutzers gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können einen Pfad mit einer oder mehreren Regionen erstellen, indem Sie den verwenden. AWS CLI Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten in Ihrem Konto AWS-Regionen erfassen. Wenn du einen Trail mit nur einer Region erstellst, kannst du dir nur die Ereignisse ansehen, die in den Trails protokolliert wurden. AWS-Region Weitere Informationen zu Trails finden Sie unter Einen Trail für Sie erstellen AWS-Konto und Einen Trail für eine Organisation erstellen im AWS CloudTrail Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3-Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur

Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung.

AWS Backup Ereignisse in CloudTrail

AWS Backup generiert diese CloudTrail Ereignisse, wenn es Backups, Wiederherstellungen, Kopien oder Benachrichtigungen durchführt. Diese Ereignisse werden nicht unbedingt durch die Verwendung der AWS Backup öffentlichen APIs generiert. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter AWS-Service Ereignisse.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Grundlegendes zu AWS Backup Einträgen in Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen

Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DeleteRecoveryPoint` Aktionen `StartBackupJobStartRestoreJob`, und auch das `BackupJobCompleted` Ereignis demonstriert.


```
{
    "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"
    }
}
```


Protokollieren von Ereignissen der kontenübergreifenden Verwaltung

Mit AWS Backup können Sie Ihre Backups AWS-Konten innerhalb Ihrer gesamten AWS OrganizationsStruktur verwalten. AWS Backup generiert diese CloudTrail Ereignisse, wenn Sie eine AWS Organizations Backup-Richtlinie erstellen, aktualisieren oder löschen (die Backup-Pläne auf Ihre Mitgliedskonten anwendet) oder wenn es einen ungültigen organisatorischen Backup-Plan gibt:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`

- `InvalidOrganizationalBackupPlan`

Beispiel: AWS Backup Protokolldateieinträge für die kontoübergreifende Verwaltung

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateOrganizationalBackupPlan` Aktion demonstriert.


```
{
    "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"
    }
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DeleteOrganizationalBackupPlan` Aktion demonstriert.

```
{
    "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"
    }
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis veranschaulicht. Es wird gesendet`InvalidOrganizationBackupPlan`, wenn ein ungültiger Backup-Plan von Organizations AWS Backup empfangen wird.

```
{
    "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"
}
```

Benachrichtigungsoptionen mit AWS Backup

Es gibt zwei Möglichkeiten, Benachrichtigungen zu erhalten über AWS Backup:

- AWS Benutzerbenachrichtigungen können Benachrichtigungen, einschließlich CloudWatch Amazon-Alarmen AWS Support, und Benachrichtigungen anderer Dienste senden.

- Amazon Simple Notification Service kann Sie über AWS Backup Ereignisse informieren.

AWS Benutzerbenachrichtigungen und AWS Backup

AWS Backup unterstützt die Verwaltung Ihrer Backup-Benachrichtigungen über die AWS Benutzerbenachrichtigungskonsole. Mit AWS -Benutzerbenachrichtigungen können Sie den Status Ihrer Backup-, Kopier- und Wiederherstellungsaufträge sowie Änderungen an Ihren Backup-Richtlinien, Tresoren, Wiederherstellungspunkten und Einstellungen im Benachrichtigungscenter für Benutzerbenachrichtigungen verfolgen.

Amazon CloudWatch, EventBridge Amazon-Alarme und AWS Support Fallaktualisierungen gehören zu den anderen Arten von Benachrichtigungen, die Sie von der Konsole aus verwalten können. Darüber hinaus können Sie verschiedene Versandoptionen einrichten, darunter E-Mail, AWS Chatbot Benachrichtigungen und AWS Console Mobile Application Push-Benachrichtigungen.

Amazon SNS und Ereignisse AWS Backup

AWS Backup nutzt die robusten Benachrichtigungen von Amazon Simple Notification Service (Amazon SNS). Sie können Amazon SNS so konfigurieren, dass Sie von der Amazon SNS SNS-Konsole aus über AWS Backup Ereignisse informiert werden.

Einschränkungen

- Der Amazon SNS SNS-Service ermöglicht zwar kontoübergreifende Benachrichtigungen, AWS Backup unterstützt diese Funktion jedoch derzeit nicht. Sie müssen Ihre eigene AWS Konto-ID und den Ressourcen-ARN Ihres Themas angeben.
- AWS Backup unterstützt Standardthemen für SNS-Best-Effort-Deduplizierung, unterstützt derzeit jedoch AWS Backup keine SNS-FIFO-Themen für Strict-Deduplizierung.

Häufige Anwendungsfälle

- Richten Sie Benachrichtigungen für fehlgeschlagene Backup-Jobs ein, indem Sie die Schritte unter Wie erhalte ich Benachrichtigungen für fehlgeschlagene Backup-Jobs? befolgen. AWS Backup vom AWS Premium Support.
- Sehen Sie sich Beispiele für Amazon-SNS-Benachrichtigungs-JSONs für abgeschlossene, fehlgeschlagene und abgelaufene Backup-Aufträge in der Tabelle mit den Beispielen für Ereignisse unten an.

Weitere allgemeine Informationen zu Amazon SNS finden Sie unter Erste Schritte mit Amazon SNS im Benutzerhandbuch für Amazon Simple Notification Service.

AWS Backup Benachrichtigungs-APIs

Nachdem Sie Ihre Themen mit der Amazon SNS SNS-Konsole oder AWS Command Line Interface (AWS CLI) erstellt haben, können Sie die folgenden AWS Backup API-Operationen verwenden, um Ihre Backup-Benachrichtigungen zu verwalten.

- DeleteBackupVaultNotifications: löscht Ereignisbenachrichtigungen für den angegebenen Sicherungstresor
- GetBackupVaultNotifications listet die Ereignisbenachrichtigungen für den angegebenen Sicherungstresor auf
- PutBackupVaultNotifications aktiviert Benachrichtigungen für das angegebene Thema und die angegebenen Ereignisse

AWS Backup unterstützt die folgenden Ereignisse:

Job type	Ereignis
Backup-Auftrag	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Kopierauftrag	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Wiederherstellungsauftrag	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Wiederherstellungspunkt	`RECOVERY_POINT_MODIFIED`

AWS Backup für S3 unterstützt zwei zusätzliche Ereignisse:

- `S3_BACKUP_OBJECT_FAILED` benachrichtigt Sie über jedes S3-Objekt, das AWS Backup während eines Backup-Auftrags nicht sichern konnte.

- `S3_RESTORE_OBJECT_FAILED` benachrichtigt Sie über jedes S3-Objekt, das AWS Backup während eines Wiederherstellungsauftrags nicht wiederherstellen konnte.

Beispiel für Ereignisse

Example Beispiel: Backup-Job abgeschlossen

```
{
    "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 Beispiel: Backup-Job ist fehlgeschlagen

```
{
    "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 Beispiel: Der Backup-Job konnte während des Backup-Fensters nicht abgeschlossen werden

```
{
    "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 Beispiele für Benachrichtigungsbefehle

Sie können AWS CLI Befehle verwenden, um Amazon SNS SNS-Benachrichtigungen für Ihre AWS Backup Ereignisse zu abonnieren, aufzulisten und zu löschen.

Beispiel für eine Put-Benachrichtigung zum Backup-Tresor

Mit dem folgenden Befehl wird ein Amazon-SNS-Thema für den angegebenen Backup-Tresor abonniert, das Sie benachrichtigt, wenn ein Wiederherstellungsauftrag gestartet oder abgeschlossen oder wenn ein Wiederherstellungspunkt geändert wird.

```
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
```

Beispiel für eine Get-Benachrichtigung zum Backup-Tresor

Der folgende Befehl listet alle Ereignisse auf, die derzeit ein Amazon-SNS-Thema für den angegebenen Backup-Tresor abonniert haben.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

Die Beispielausgabe lautet wie folgt:

```
{
    "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"
}
```

Beispiel für eine Löschbenachrichtigung zum Backup-Tresor

Mit dem folgenden Befehl wird das Abonnement eines Amazon-SNS-Themas für den angegebenen Backup-Tresor aufgehoben.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

AWS Backup Als Service Principal angeben

> **Note**
>
> Um SNS-Themen in Ihrem Namen veröffentlichen AWS Backup zu können, müssen Sie dies AWS Backup als Service Principal angeben.

Nehmen Sie den folgenden JSON-Code in die Zugriffsrichtlinie des Amazon SNS SNS-Themas auf, das Sie zur Nachverfolgung von AWS Backup Ereignissen verwenden. Sie müssen den Amazon-Ressourcennamen (ARN) Ihres Themas angeben.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Weitere Informationen zur Angabe eines Service Principals in einer Amazon SNS SNS-Zugriffsrichtlinie finden Sie unter Zulassen, dass jede AWS Ressource zu einem Thema veröffentlicht wird im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Wenn Ihr Thema verschlüsselt ist, müssen Sie zusätzliche Berechtigungen in Ihre Richtlinie aufnehmen, AWS Backup damit es veröffentlicht werden kann. Weitere Informationen darüber, wie Services das Veröffentlichen unter verschlüsselten Themen aktivieren können, finden Sie unter Enable Compatibility between Event Sources from AWS Services and Encrypted Topics im Amazon Simple Notification Service Developer Guide.

Problembehebung AWS Backup

Bei der Verwendung AWS Backup können Probleme auftreten. Die folgenden Abschnitte können zum Beheben von häufig auftretenden Problemen helfen.

Allgemeine Fragen AWS Backup zu finden Sie in den AWS Backup häufig gestellten Fragen. Sie können auch im AWS Backup -Forum nach Antworten suchen und Fragen posten.

Themen

Fehlerbehebung bei allgemeinen Problemen

Wenn Sie Ressourcen sichern und wiederherstellen, benötigen Sie eine Nutzungs AWS Backup - und Zugriffsberechtigung für die Ressourcen, die Sie schützen möchten. Der einfachste Weg, über die richtigen Berechtigungen zu verfügen, besteht darin, die Standardrolle zu wählen, wenn Sie Ressourcen einem Backup-Plan zuweisen. Weitere Informationen zur Zugriffssteuerung mit AWS Identity and Access Management (IAM) finden Sie AWS Backup unterZugriffskontrolle.

Wenn Sie versuchen, auf eine AWS Backup Ressource zuzugreifen, z. B. auf einen Backup-Tresor, eine `AccessDenied` Fehlermeldung erhalten, ist die Ressource entweder nicht vorhanden oder Sie haben keine Zugriffsberechtigungen für die Ressource.

Wenn beim Sichern und Wiederherstellen eines bestimmten Ressourcentyps Probleme auftreten, kann es hilfreich sein, das Thema zur Fehlerbehebung bei Backups und Wiederherstellungen für diese Ressource zu konsultieren. Weitere Informationen finden Sie unter den Links unter So AWS Backup funktioniert es mit unterstützten AWS Diensten.

Wenn AWS Backup eine Ressource nicht erstellt oder gelöscht werden kann, können Sie mehr über das Problem erfahren, indem Sie die Option AWS CloudTrail zum Anzeigen von Fehlermeldungen oder Protokollen verwenden. Weitere Informationen zur Verwendung von CloudTrail mit AWS Backup finden Sie unterAWS Backup API-Aufrufe protokollieren mit CloudTrail.

Fehlerbehebung beim Erstellen von Ressourcen

Die folgenden Informationen können Ihnen bei der Fehlerbehebung beim Erstellen von Sicherungen behilflich sein.

- Im Allgemeinen können AWS -Datenbankservices eine Stunde vor oder während ihres Wartungsfensters oder automatischen Backup-Fensters keine Backups starten. Amazon FSx kann vier Stunden vor oder während des Wartungsfensters oder des automatischen Backup-Fensters keine Backups starten (Amazon Aurora ist von dieser Einschränkung durch das Wartungsfenster ausgenommen). Zu diesen Zeiten geplante Snapshot-Backups schlagen fehl. Eine Ausnahme: Wenn Sie sich für einen unterstützten Dienst sowohl AWS Backup für Snapshot- als auch für kontinuierliche Backups entscheiden, müssen Sie sich keine Gedanken mehr über diese Fenster machen, da ich sie für Sie einplanen AWS Backup werde. Eine Liste der unterstützten Dienste und Anleitungen zur Erstellung kontinuierlicher Backups finden Sie AWS Backup unter Point-in-Time Recovery.
- Das Erstellen von Backups für DynamoDB-Tabellen schlägt fehl, während Tabellen erstellt werden. Das Erstellen einer DynamoDB-Tabelle dauert in der Regel einige Minuten.
- Das Sichern von Amazon-EFS-Dateisystemen kann bis zu sieben Tage dauern, wenn die Dateisysteme sehr groß sind. Für ein Amazon-EFS-Dateisystem kann jeweils nur ein gleichzeitiges Backup in die Warteschlange gestellt werden. Wenn eine nachfolgende Sicherung in die Warteschlange gestellt wird, während eine vorherige Sicherung noch ausgeführt wird, kann das Sicherungszeitfenster ablaufen, und es wird keine Sicherung erstellt.
- Amazon EBS hat ein Soft-Kontingent von 100.000 Backups AWS-Region pro Konto. Zusätzliche Backups schlagen fehl, wenn dieses Kontingent erreicht ist. Wenn Sie dieses Kontingent erreichen, können Sie überschüssige Sicherungen löschen oder eine Kontingenterhöhung beantragen. Weitere Informationen zum Anfordern einer Kontingenterhöhung finden Sie im AWS -Servicekontingente.
- Beachten beim Erstellen von RDS-Backups (Amazon Relational Database Service) Folgendes:
  - Wenn Sie AWS Backup nicht sowohl Amazon RDS-Snapshots als auch kontinuierliche Backups mit point-in-time Wiederherstellung verwalten, schlagen Ihre Backups fehl, wenn sie während des täglichen, vom Benutzer konfigurierbaren 30-minütigen Backup-Fensters initiiert oder nach Bedarf erstellt werden. Weitere Informationen zu automatisierten Amazon-RDS-Backups finden Sie unter Arbeiten mit Backups im Amazon-RDS-Benutzerhandbuch. Sie können diese Einschränkung umgehen, indem AWS Backup Sie sowohl Amazon RDS-Snapshots als auch kontinuierliche Backups mit point-in-time Wiederherstellung verwalten.

- Wenn Sie eine Backup-Aufgabe von der Amazon-RDS-Konsole aus initiieren, kann dies zu einem Konflikt mit einem Aurora-Cluster-Backup-Auftrag führen, was den Fehler `Backup job expired before completion.` verursacht. Wenn dieser Fall auftritt, konfigurieren Sie in AWS Backup ein längeres Backup-Fenster.
- AWS Backup gibt die TDE-Optionsgruppe derzeit nicht weiter, wenn ein Kopierauftrag erstellt wird. Wenn Sie beabsichtigen, diese Optionsgruppe für die Erstellung von Kopieraufträgen zu verwenden, müssen Sie die Amazon-RDS-Konsole oder die Amazon-RDS-API anstelle von AWS Backup -Tools verwenden. Weitere Informationen finden Sie unter Kopieren einer Optionsgruppe im Benutzerhandbuch zu Amazon Relational Database Service.
- FEHLER: On-Demand-Backups werden abgeschlossen, aber geplante Backups schlagen fehl mit der Fehlermeldung, dass der KMS-Quell-Snapshot-Schlüssel nicht existiert, nicht aktiviert ist oder Sie keine Zugriffsrechte haben. Der On-Demand-Auftrag wird abgeschlossen, weil er den API-Aufruf `CopyDBSnapshot` verwendet, für den kein KMS-Zugriff erforderlich ist.

  ABHILFE: Fügen Sie Ihrem KMS-Schlüssel die IAM-Rolle hinzu. Dazu können Sie die Rolle in Ihrer KMS-Schlüsselrichtlinie zulassen.

  Um Ihre Richtlinie zu bearbeiten,

  1. Öffnen Sie die KMS-Konsole.
  2. Klicken Sie in linken Navigationsleiste auf Vom Kunden verwaltete Schlüssel.
  3. Klicken Sie auf den vom Kunden verwalteten Schlüssel, den Sie bearbeiten möchten.
  4. Wählen Sie unter Schlüsselrichtlinie die Option Zur Richtlinienansicht wechseln aus.
  5. Klicken Sie auf Bearbeiten.
  6. Fügen Sie die Rolle hinzu.

Fehlerbehebung beim Löschen von Ressourcen

Wiederherstellungspunkte, die von erstellt wurden, AWS Backup können nicht im Konsolenfenster der geschützten Ressource gelöscht werden. Sie können sie auf der AWS Backup Konsole löschen, indem Sie sie im Tresor auswählen, in dem sie gespeichert sind, und dann Löschen wählen.

Um einen Wiederherstellungspunkt oder einen Sicherungstresor zu löschen, benötigen Sie die entsprechenden Berechtigungen. Weitere Informationen zur Zugriffskontrolle mithilfe von IAM with finden Sie AWS Backup unterZugriffskontrolle.

Fehlerbehebung beim Wiederherstellen von Ressourcen

Wiederherstellung mithilfe der API

Verwenden Sie den StartRestoreJob-API-Vorgang, um ein Backup programmgesteuert wiederherzustellen.

Um die Konfigurationsmetadaten abzurufen, mit denen Ihr Backup erstellt wurde, können Sie GetRecoveryPointRestoreMetadata aufrufen.

Weitere Informationen finden Sie unter Wiederherstellen eines Backups.

Wiederherstellen mit der Konsole

- Wiederherstellen von Amazon-S3-Daten
- Wiederherstellen einer virtuellen Maschine
- Wiederherstellen eines Amazon-FSx-Dateisystems
- Wiederherstellen eines Amazon-EBS-Volumes
- Wiederherstellen eines Amazon-EFS-Dateisystems
- Wiederherstellen einer Amazon-DynamoDB-Tabelle
- Wiederherstellen einer Amazon-RDS-Datenbank
- Wiederherstellung eines Aurora-Clusters
- Wiederherstellen einer Amazon-EC2-Instance
- Wiederherstellen eines Storage-Gateway-Volumes
- Wiederherstellen eines Amazon-DocumentDB-Clusters
- Wiederherstellen eines Neptun-Clusters

Behebung von Formatierungsfehlern

Wenn ein Platzhalter (*) für den Wert in einem Parameter verwendet wird, wird der Platzhalter so verarbeitet, dass er andere Werte als Leerzeichen enthält. Werte in einem Schlüssel-Wert-Paar, die Leerzeichen enthalten, werden nicht in den Platzhalter aufgenommen.

AWS Backup-API

Zusätzlich zur Verwendung der Konsole können Sie die AWS Backup-API-Aktionen und -Datentypen verwenden, um AWS Backup und die entsprechenden Ressourcen programmgesteuert zu konfigurieren und zu verwalten. In diesem Abschnitt werden AWS Backup-Aktionen und -Datentypen beschrieben. Er enthält die API-Referenz für AWS Backup.

AWS Backup-API

- AWS Backup-Aktionen
- AWS Backup-Datentypen

Aktionen

Folgende Aktionen werden von AWS Backup unterstützt:

- 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

Folgende Aktionen werden von AWS Backup gateway unterstützt:

- 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

Folgende Aktionen werden von AWS Backup unterstützt:

- 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

Service: AWS Backup

Hebt die angegebene gesetzliche Sperre für einen Wiederherstellungspunkt auf. Diese Aktion kann nur von einem Benutzer mit ausreichenden Berechtigungen durchgeführt werden.

Anforderungssyntax

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

[CancelDescription](#)

Eine Zeichenfolge, die den Grund für die Aufhebung der gesetzlichen Sperre beschreibt.

Erforderlich: Ja

[legalHoldId](#)

Die ID der gesetzlichen Sperre.

Erforderlich: Ja

[RetainRecordInDays](#)

Der ganzzahlige Betrag in Tagen, nach dessen Ablauf die gesetzliche Sperre aufgehoben werden soll.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 201
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-201-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidResourceStateException

AWS Backup führt bereits eine Aktion an diesem Wiederherstellungspunkt durch. Die von Ihnen angeforderte Aktion kann erst ausgeführt werden, wenn die erste Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateBackupPlan

Service: AWS Backup

Erstellt einen Backup-Plan unter Verwendung eines Backup-Plannamens und der Backup-Regeln. Ein Sicherungsplan ist ein Dokument, das Informationen enthält, AWS Backup anhand derer Aufgaben geplant werden, mit denen Wiederherstellungspunkte für Ressourcen erstellt werden.

Wenn Sie `CreateBackupPlan` mit einem Plan aufrufen, der bereits existiert, erhalten Sie ein `AlreadyExistsException`-Beispiel.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupPlan

Der Hauptteil eines Backup-Plans. Beinhaltet einen `BackupPlanName` und einen oder mehrere Sätze von `Rules`.

Typ: BackupPlanInput Objekt

Erforderlich: Ja

BackupPlanTags

Die Tags, die dem Backup-Plan zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

CreatorRequestId

Identifiziert die Anforderung und ermöglicht die Wiederholung fehlgeschlagener Anforderungen, ohne dass das Risiko besteht, dass der Vorgang zweimal ausgeführt wird. Wenn die Anforderung eine `CreatorRequestId` enthält, der einem vorhandenen Backup-Plan entspricht, wird dieser Plan zurückgegeben. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AdvancedBackupSettings

Die Einstellungen für einen Ressourcentyp. Diese Option ist nur für Windows-VSS-Backup-Aufträge (Volume Shadow Copy Service) verfügbar.

Typ: Array von AdvancedBackupSetting-Objekten

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

BackupPlanId

Die ID des Backup-Plans.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung der Domainliste im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Sie können nicht bearbeitet werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python

- AWS SDK for Ruby V3

CreateBackupSelection

Service: AWS Backup

Erstellt ein JSON-Dokument, das eine Gruppe von Ressourcen zum Zuweisen zu einem Backup-Plan angibt. Beispiele finden Sie unter Programmgesteuertes Zuweisen von Ressourcen.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Die ID des Backup-Plans.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupSelection

Der Hauptteil einer Anfrage, einem Backup-Plan eine Reihe von Ressourcen zuzuweisen.

Typ: BackupSelection Objekt

Erforderlich: Ja

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanId

Die ID des Backup-Plans.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung einer Backup-Auswahl im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

SelectionId

Identifiziert den Text einer Anforderung zum Zuweisen einer Gruppe von Ressourcen zu einem Backup-Plan eindeutig.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateBackupVault

Service: AWS Backup

Erzeugt einen logischen Container, in dem Backups gespeichert werden. Eine `CreateBackupVault`-Anforderung enthält einen Namen, optional ein oder mehrere Ressourcen-Tags, einen Verschlüsselungsschlüssel und eine Anforderungs-ID.

> **Note**
>
> Fügen Sie keine sensiblen Daten wie Passnummern in den Namen eines Backup-Tresors ein.

Anforderungssyntax

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind. Sie bestehen aus Kleinbuchstaben, Zahlen und Bindestrichen.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupVaultTags

Die Tags, die dem Backup-Tresor zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

EncryptionKeyArn

Die serverseitige Verschlüsselung zum Schutz Ihrer Backups, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind. Sie bestehen aus Kleinbuchstaben, Zahlen und Bindestrichen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Tresors im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python

- AWS SDK for Ruby V3

CreateFramework

Service: AWS Backup

Erstellt ein Framework mit einem oder mehreren Steuerelementen. Ein Framework ist eine Sammlung von Steuerelementen, mit denen Sie Ihre Backup-Praktiken auswerten können. Durch die Verwendung vorgefertigter, anpassbarer Steuerelemente zur Definition Ihrer Richtlinien können Sie bewerten, ob Ihre Backup-Praktiken Ihren Richtlinien entsprechen und welche Ressourcen noch nicht konform sind.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

FrameworkControls

Die Kontrollen, aus denen das Framework besteht. Jedes Steuerelement in der Liste hat einen Namen, Eingabeparameter und einen Bereich.

Typ: Array von FrameworkControl-Objekten

Erforderlich: Ja

FrameworkDescription

Eine optionale Beschreibung des Frameworks mit einer Länge von maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

FrameworkName

Der eindeutige Name des Frameworks. Der Name muss eine Länge von maximal 256 Zeichen haben, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

FrameworkTags

Die Tags, die dem Framework zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `CreateFrameworkInput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

FrameworkArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

FrameworkName

Der eindeutige Name des Frameworks. Der Name muss eine Länge von maximal 256 Zeichen haben, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateLegalHold

Service: AWS Backup

Erzeugt eine gesetzliche Sperre für einen Wiederherstellungspunkt (Backup). Eine gesetzliche Aufbewahrungsfrist ist ein Verbot, ein Backup zu ändern oder zu löschen, bis ein autorisierter Benutzer die Sperrung aufhebt. Alle Aktionen zum Löschen oder Aufheben der Zuordnung eines Wiederherstellungspunkts schlagen mit einem Fehler fehl, wenn der Wiederherstellungspunkt mit einer oder mehreren aktiven gesetzlichen Aufbewahrungsfristen belegt ist.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Description

Die Beschreibung der gesetzlichen Sperre.

Typ: Zeichenfolge

Erforderlich: Ja

IdempotencyToken

Dies ist eine vom Benutzer gewählte Zeichenfolge, mit der zwischen ansonsten identischen Aufrufen unterschieden wird. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointSelection

Die Kriterien für die Zuweisung einer Gruppe von Ressourcen, z. B. Ressourcentypen oder Backup-Tresore.

Typ: RecoveryPointSelection Objekt

Erforderlich: Nein

Tags

Optionale Tags, die hinzugefügt werden sollen. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen verwalten, filtern und suchen können. Erlaubte Zeichen sind: UTF-8-Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: + - = . _ : /.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Title

Der Titel der gesetzlichen Sperre.

Typ: Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationDate

Der Zeitpunkt, zu dem der gesetzliche Aufbewahrungsort erstellt wurde.

Typ: Zeitstempel

Description

Die Beschreibung der gesetzlichen Sperre.

Typ: Zeichenfolge

LegalHoldArn

Der Amazon-Ressourcenname (ARN) der gesetzlichen Aufbewahrungsfrist.

Typ: Zeichenfolge

LegalHoldId

Die ID der gesetzlichen Aufbewahrungsfrist.

Typ: Zeichenfolge

RecoveryPointSelection

Die Kriterien, die einer Gruppe von Ressourcen zugewiesen werden sollen, z. B. Ressourcentypen oder Backup-Tresore.

Typ: RecoveryPointSelection Objekt

Status

Der Status der gesetzlichen Sperre.

Typ: Zeichenfolge

Zulässige Werte: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Der Titel der gesetzlichen Sperre.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateLogicallyAirGappedBackupVault

Service: AWS Backup

Erzeugt einen logischen Container, in den Backups kopiert werden können.

Diese Anforderung umfasst einen Namen, die Region, die maximale Anzahl von Aufbewahrungstagen und die Mindestanzahl von Aufbewahrungstagen. Sie kann optional Tags und eine Anforderungs-ID des Erstellers enthalten.

> **Note**
>
> Fügen Sie keine sensiblen Daten wie Passnummern in den Namen eines Backup-Tresors ein.

Anforderungssyntax

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Logische Air-Gapped Backup-Vaults werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupVaultTags

Die Tags, die dem Tresor zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

CreatorRequestId

Die ID der Erstellungsanforderung.

Dieser Parameter ist optional. Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

MaxRetentionDays

Der maximale Aufbewahrungszeitraum, für den der Tresor seine Wiederherstellungspunkte beibehält. Wenn dieser Parameter nicht angegeben wird, erzwingt AWS Backup keine maximale Aufbewahrungsdauer für die Wiederherstellungspunkte im Tresor (und erlaubt somit eine unbegrenzte Speicherung).

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der maximalen Aufbewahrungsdauer entspricht oder kürzer ist. Wenn die Aufbewahrungsdauer des Auftrags länger als die maximale Aufbewahrungsdauer ist, schlägt der Tresor den Backup- oder Kopierauftrag fehl, und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden.

Type: Long

Erforderlich: Ja

MinRetentionDays

Diese Einstellung gibt den Mindestaufbewahrungszeitraum an, in dem der Tresor seine Wiederherstellungspunkte beibehält. Wenn dieser Parameter nicht angegeben wird, wird keine Mindestaufbewahrungsdauer erzwungen.

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der minimalen Aufbewahrungsdauer entspricht oder länger ist. Wenn die Aufbewahrungsfrist des Auftrags länger als die maximale Aufbewahrungsdauer ist, kann der Tresor den Backup- oder Kopierauftrag nicht ausführen und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden.

Type: Long

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Der ARN (Amazon Resource Name) des Tresors.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Logische Air-Gapped Backup-Vaults werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Das Datum und die Uhrzeit, zu der der Tresor erstellt wurde.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

VaultState

Der aktuelle Status des Tresors.

Typ: Zeichenfolge

Zulässige Werte: `CREATING | AVAILABLE | FAILED`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python

- AWS SDK for Ruby V3

CreateReportPlan

Service: AWS Backup

Erstellt einen Berichtsplan. Ein Berichtsplan ist ein Dokument, das Informationen über den Inhalt des Berichts und darüber, wo er geliefert AWS Backup wird, enthält.

Wenn Sie `CreateReportPlan` mit einem Plan aufrufen, der bereits existiert, erhalten Sie ein `AlreadyExistsException`-Beispiel.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `CreateReportPlanInput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

ReportDeliveryChannel

Eine Struktur, die Informationen darüber enthält, wo und wie Sie Ihre Berichte liefern, insbesondere Ihren Amazon-S3-Bucket-Namen, das S3-Schlüsselpräfix und die Formate Ihrer Berichte.

Typ: ReportDeliveryChannel Objekt

Erforderlich: Ja

ReportPlanDescription

Eine optionale Beschreibung des Berichtsplans mit maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

ReportPlanName

Der eindeutige Name des Berichtsplans. Der Name muss eine Länge von maximal 256 Zeichen haben, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

ReportPlanTags

Die Tags, die dem Berichtsplan zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ReportSetting

Identifiziert die Berichtsvorlage für den Bericht. Berichte werden mithilfe einer Berichtsvorlage erstellt. Die Berichtsvorlagen sind:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Wenn die Berichtsvorlage `RESOURCE_COMPLIANCE_REPORT` oder ist`CONTROL_COMPLIANCE_REPORT`, beschreibt diese API-Ressource auch den Berichtsbereich von AWS-Regionen und Frameworks.

Typ: ReportSetting Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Backup-Tresors im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

ReportPlanArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

ReportPlanName

Der eindeutige Name des Berichtsplans.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateRestoreTestingPlan

Service: AWS Backup

Erstellt einen Wiederherstellungstestplan.

Der erste von zwei Schritten zur Erstellung eines Wiederherstellungstestplans. Nachdem diese Anfrage erfolgreich war, beenden Sie den Vorgang mit CreateRestoreTestingSelection.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

CreatorRequestId

Dies ist eine eindeutige Zeichenfolge, die die Anforderung angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional. Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

RestoreTestingPlan

Ein Wiederherstellungstestplan muss eine von Ihnen erstellte eindeutige `RestoreTestingPlanName`-Zeichenfolge und einen `ScheduleExpression` Cron enthalten. Sie können optional eine `StartWindowHours`-Ganzzahl und eine `CreatorRequestId`-Zeichenfolge angeben.

Der `RestoreTestingPlanName` ist eine eindeutige Zeichenfolge, die dem Namen des Wiederherstellungstestplans entspricht. Dieser Wert kann nach der Erstellung nicht geändert werden und darf nur aus alphanumerischen Zeichen und Unterstrichen bestehen.

Typ: RestoreTestingPlanForCreate Objekt

Erforderlich: Ja

Tags

Die Tags, die dem Wiederherstellungstestplan zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
```

```
   "RestoreTestingPlanName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Das Datum und die Uhrzeit der Erstellung des Wiederherstellungsplans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

RestoreTestingPlanArn

Ein Amazon-Ressourcenname (ARN), der den Wiederherstellungstestplan eindeutig identifiziert.

Typ: Zeichenfolge

RestoreTestingPlanName

Diese eindeutige Zeichenfolge, ist der Name des Wiederherstellungstestplans.

Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateRestoreTestingSelection

Service: AWS Backup

Diese Anfrage kann gesendet werden, nachdem die CreateRestoreTestingPlan Anfrage erfolgreich zurückgesendet wurde. Dies ist der zweite Teil der Erstellung eines Ressourcentestplans, der sequentiell abgeschlossen werden muss.

Dies besteht aus `RestoreTestingSelectionName`, `ProtectedResourceType` und einem der folgenden Elemente:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Jeder geschützte Ressourcentyp kann einen einzelnen Wert haben.

Eine Auswahl für den Wiederherstellungstest kann einen Platzhalterwert („*“) für `ProtectedResourceArns` zusammen mit `ProtectedResourceConditions` enthalten. Alternativ können Sie bis zu 30 spezifische ARNs für geschützte Ressourcen in `ProtectedResourceArns` hinzufügen.

Es kann nicht nach geschützten Ressourcentypen ALS und nach bestimmten ARNs ausgewählt werden. Die Anforderung schlägt fehl, wenn beide enthalten sind.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Geben Sie den Namen des Wiederherstellungstestplans ein, der von der entsprechenden CreateRestoreTestingPlan Anfrage zurückgegeben wurde.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anforderung angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

RestoreTestingSelection

Dies besteht aus `RestoreTestingSelectionName`, `ProtectedResourceType` und einem der folgenden Elemente:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Jeder geschützte Ressourcentyp kann einen einzelnen Wert haben.

Eine Auswahl für den Wiederherstellungstest kann einen Platzhalterwert („*“) für `ProtectedResourceArns` zusammen mit `ProtectedResourceConditions` enthalten. Alternativ können Sie bis zu 30 spezifische ARNs für geschützte Ressourcen in `ProtectedResourceArns` hinzufügen.

Typ: RestoreTestingSelectionForCreate Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem die Auswahl für den Ressourcentest erstellt wurde.

Typ: Zeitstempel

RestoreTestingPlanArn

Der ARN des Wiederherstellungstestplans, dem die Auswahl für den Wiederherstellungstest zugeordnet ist.

Typ: Zeichenfolge

RestoreTestingPlanName

Der Name des Wiederherstellungstestplans.

Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

Typ: Zeichenfolge

RestoreTestingSelectionName

Der Name der Auswahl für den Wiederherstellungstest für den zugehörigen Wiederherstellungstestplan.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupPlan

Service: AWS Backup

Löscht einen Sicherungsplan Ein Backup-Plan kann erst gelöscht werden, wenn alle zugehörigen Ressourcenauswahlen gelöscht wurden. Durch das Löschen eines Backup-Plans wird die aktuelle Version des Backup-Plans gelöscht. Frühere Versionen, falls vorhanden, bestehen weiterhin.

Anforderungssyntax

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

DeletionDate

Das Datum und die Uhrzeit der Löschung eines Backup-Plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `DeletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Version-IDs können nicht bearbeitet werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupSelection

Service: AWS Backup

Löscht die Ressourcenauswahl, die einem Backup-Plan zugeordnet ist, der durch die `SelectionId` angegeben ist.

Anforderungssyntax

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

selectionId

Identifiziert den Text einer Anforderung zum Zuweisen einer Gruppe von Ressourcen zu einem Backup-Plan eindeutig.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupVault

Service: AWS Backup

Löscht den durch seinen Namen identifizierten Backup-Tresor. Ein Tresor kann nur gelöscht werden, wenn er leer ist.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupVaultAccessPolicy

Service: AWS Backup

Löscht das Richtliniendokument, das die Berechtigungen für einen Backup-Tresor verwaltet.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind. Sie bestehen aus Kleinbuchstaben, Zahlen und Bindestrichen.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupVaultLockConfiguration

Service: AWS Backup

Löscht AWS Backup Vault Lock aus einem Backup-Tresor, der durch einen Backup-Tresornamen angegeben wurde.

Wenn die Konfiguration von Vault Lock unveränderlich ist, können Sie Vault Lock nicht mithilfe von API-Vorgängen löschen. Wenn Sie versuchen, dies zu tun, erhalten Sie eine `InvalidRequestException`. Weitere Informationen finden Sie unter Vault Lock im AWS Backup Entwicklerhandbuch.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name des Backup-Tresors, aus dem AWS Backup Vault Lock gelöscht werden soll.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteBackupVaultNotifications

Service: AWS Backup

Löscht Ereignisbenachrichtigungen für den angegebenen Backup-Tresor.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteFramework

Service: AWS Backup

Löscht das durch einen Framework-Namen angegebene Framework.

Anforderungssyntax

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

frameworkName

Der eindeutige Name eines Frameworks.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteRecoveryPoint

Service: AWS Backup

Löscht den durch eine Wiederherstellungspunkt-ID angegebenen Wiederherstellungspunkt.

Wenn die Wiederherstellungspunkt-ID zu einem kontinuierlichen Backup gehört, wird durch das Aufrufen dieses Endpunkts das bestehende kontinuierliche Backup gelöscht und zukünftige kontinuierliche Backups werden gestoppt.

Wenn die Berechtigungen einer IAM-Rolle nicht ausreichen, um diese API aufzurufen, sendet der Service eine HTTP-200-Antwort mit einem leeren HTTP-Text zurück. Der Wiederherstellungspunkt wird jedoch nicht gelöscht. Stattdessen wechselt er in einen `EXPIRED`-Status.

`EXPIRED`-Wiederherstellungspunkte können mit dieser API gelöscht werden, sobald die IAM-Rolle die `iam:CreateServiceLinkedRole`-Aktion ausgeführt hat. Weitere Informationen zum Hinzufügen dieser Rolle finden Sie unter Fehlerbehebung bei manuellen Löschungen.

Wenn der Benutzer oder die Rolle gelöscht oder die in der Rolle enthaltene Berechtigung entfernt wird, ist das Löschen nicht erfolgreich und es wird in einen neuen `EXPIRED`-Status gewechselt.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

InvalidResourceStateException

AWS Backup führt bereits eine Aktion an diesem Wiederherstellungspunkt durch. Die von Ihnen angeforderte Aktion kann erst ausgeführt werden, wenn die erste Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteReportPlan

Service: AWS Backup

Löscht den durch einen Berichtsplannamen angegebenen Berichtsplan.

Anforderungssyntax

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

reportPlanName

Der eindeutige Name eines Berichtsplans.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteRestoreTestingPlan

Service: AWS Backup

Diese Anforderung löscht den angegebenen Wiederherstellungstestplan.

Das Löschen kann nur erfolgreich durchgeführt werden, wenn zuerst alle zugehörigen Wiederherstellungstest-Auswahlen gelöscht werden.

Anforderungssyntax

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Erforderlicher eindeutiger Name des Wiederherstellungstestplans, den Sie löschen möchten.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 204
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteRestoreTestingSelection

Service: AWS Backup

Geben Sie den Namen des Wiederherstellungstestplans und den Namen der Wiederherstellungstest-Auswahl ein.

Alle Testauswahlen, die mit einem Wiederherstellungstestplan verknüpft sind, müssen gelöscht werden, bevor der Wiederherstellungstestplan gelöscht werden kann.

Anforderungssyntax

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Erforderlicher eindeutiger Name des Wiederherstellungstestplans, der die Wiederherstellungstest-Auswahl enthält, die Sie löschen möchten.

Erforderlich: Ja

RestoreTestingSelectionName

Erforderlicher eindeutiger Name der Wiederherstellungstest-Auswahl, die Sie löschen möchten.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 204
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeBackupJob

Service: AWS Backup

Gibt die Details des Backup-Auftrags für die angegebene `BackupJobId` zurück.

Anforderungssyntax

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupJobId

Identifiziert eindeutig eine Anfrage AWS Backup zur Sicherung einer Ressource.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AccountId

Gibt die Konto-ID zurück, der der Backup-Auftrag angehört.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

BackupJobId

Identifiziert eindeutig eine Anfrage AWS Backup zur Sicherung einer Ressource.

Typ: Zeichenfolge

BackupOptions

Stellt die Optionen dar, die als Teil eines Backup-Plans oder eines On-Demand-Backup-Auftrags angegeben wurden.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wertemuster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

Die Größe eines Backups in Byte

Type: Long

BackupType

Stellt den tatsächlichen Backup-Typ dar, der für einen Backup-Auftrag ausgewählt wurde. Wenn beispielsweise ein erfolgreiches Backup durch den Windows Volume Shadow Copy Service (VSS) durchgeführt wurde, gibt `BackupType` `"WindowsVSS"` zurück. Wenn `BackupType` leer ist, war der Backup-Typ ein reguläres Backup.

Typ: Zeichenfolge

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

Die Größe in Byte, die zum Zeitpunkt der Abfrage des Auftragsstatus an einen Backup-Tresor übertragen wurden.

Type: Long

ChildJobsInState

Dadurch werden die Statistiken der enthaltenen untergeordneten (verschachtelten) Backup-Aufträge zurückgegeben.

Typ: Zeichenfolge auf eine lange Zuordnung

Gültige Schlüssel: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Erstellen eines Backup-Auftrags abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CreatedBy

Enthält identifizierende Informationen über die Erstellung eines Backup-Auftrags, einschließlich `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` und `BackupRuleId` des Backup-Plans, mit dem er erstellt wurde.

Typ: RecoveryPointCreator Objekt

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Auftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

ExpectedCompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Sichern von Ressourcen abgeschlossen werden soll, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `ExpectedCompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

InitiationDate

Das Datum, an dem ein Backup-Job initiiert wurde.

Typ: Zeitstempel

IsParent

Dies gibt den booleschen Wert zurück, dass es sich bei einem Backup-Auftrag um einen übergeordneten (zusammengesetzten) Auftrag handelt.

Typ: Boolesch

MessageCategory

Die Anzahl der Jobs für die angegebene Nachrichtenkategorie.

Beispielzeichenfolgen können `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` oder `INVALIDPARAMETERS` sein. Unter Überwachung finden Sie eine Liste der akzeptierten MessageCategory Zeichenketten.

Typ: Zeichenfolge

NumberOfChildJobs

Dies gibt die Anzahl der untergeordneten (verschachtelten) Backup-Aufträge zurück.

Type: Long

ParentJobId

Dies gibt die ID des übergeordneten (zusammengesetzten) Ressourcen-Backup-Auftrags zurück.

Typ: Zeichenfolge

PercentDone

Enthält einen geschätzten Prozentsatz der Fertigstellung eines Auftrags zum Zeitpunkt der Abfrage des Auftragsstatus.

Typ: Zeichenfolge

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

ResourceArn

Ein ARN bezeichnet eindeutig eine gespeicherte Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

ResourceName

Der nicht eindeutige Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

ResourceType

Der Typ der AWS Ressource, die gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Gibt die Uhrzeit im Unix-Format und in der koordinierten Weltzeit (UTC) an, zu der ein Backup-Auftrag gestartet werden muss, bevor er abgebrochen wird. Der Wert wird berechnet, indem das Startfenster zur geplanten Zeit hinzugefügt wird. Wenn die geplante Zeit also 18:00 Uhr wäre und das Startfenster zwei Stunden beträgt, wäre die `StartBy`-Uhrzeit am angegebenen Datum 20:00 Uhr. Der Wert von `StartBy` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

State

Der aktuelle Status eines Backup-Auftrags.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Eine ausführliche Meldung, in der der Status des Backup-Auftrags für eine Ressource erläutert wird.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

DependencyFailureException

Ein abhängiger AWS Service oder eine abhängige Ressource hat einen Fehler an den AWS Backup Service gemeldet, und die Aktion kann nicht abgeschlossen werden.

HTTP Status Code: 500

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeBackupVault

Service: AWS Backup

Gibt Metadaten zu einem durch seinen Namen angegebenen Backup-Tresor zurück.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

BackupVaultAccountId

Die Konto-ID des angegebenen Backup-Tresors.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Tresors im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional. Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

EncryptionKeyArn

Die serverseitige Verschlüsselung zum Schutz Ihrer Backups, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

LockDate

Datum und Uhrzeit, zu denen die AWS Backup Vault Lock-Konfiguration nicht geändert oder gelöscht werden kann.

Wenn Sie Vault Lock auf Ihren Tresor angewendet haben, ohne ein Sperrdatum anzugeben, können Sie Ihre Vault Lock-Einstellungen jederzeit ändern oder Vault Lock vollständig aus dem Tresor löschen.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Locked

Ein boolescher Wert, der angibt, ob AWS Backup Vault Lock den Backup-Tresor derzeit schützt. `True`bedeutet, dass Vault Lock dazu führt, dass Lösch- oder Aktualisierungsvorgänge an den im Tresor gespeicherten Wiederherstellungspunkten fehlschlagen.

Typ: Boolesch

MaxRetentionDays

Die AWS Backup Vault Lock-Einstellung, die den maximalen Aufbewahrungszeitraum festlegt, für den der Tresor seine Wiederherstellungspunkte aufbewahrt. Wenn dieser Parameter nicht angegeben wird, erzwingt Vault Lock keine maximale Aufbewahrungsdauer für die Wiederherstellungspunkte im Tresor (und erlaubt somit eine unbegrenzte Speicherung).

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der maximalen Aufbewahrungsdauer entspricht oder kürzer ist. Wenn die Aufbewahrungsdauer des Auftrags länger als die maximale Aufbewahrungsdauer ist, schlägt der Tresor den Backup- oder Kopierauftrag fehl, und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen

anderen Tresor verwenden. Wiederherstellungspunkte, die bereits vor der Tresorsperre im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

MinRetentionDays

Die AWS Backup Vault Lock-Einstellung, die den Mindestaufbewahrungszeitraum festlegt, für den der Tresor seine Wiederherstellungspunkte aufbewahrt. Wenn dieser Parameter nicht angegeben wird, erzwingt Vault Lock keine Mindestaufbewahrungsdauer.

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der minimalen Aufbewahrungsdauer entspricht oder länger ist. Wenn die Aufbewahrungsfrist des Auftrags länger als die maximale Aufbewahrungsdauer ist, kann der Tresor den Backup- oder Kopierauftrag nicht ausführen und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden. Wiederherstellungspunkte, die bereits vor der Tresorsperre im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

NumberOfRecoveryPoints

Die Anzahl der Wiederherstellungspunkte, die in einem Backup-Tresor gespeichert sind.

Type: Long

VaultType

Der beschriebene Tresortyp.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeCopyJob

Service: AWS Backup

Gibt Metadaten zurück, die mit der Erstellung einer Kopie einer Ressource verknüpft sind.

Anforderungssyntax

```
GET /copy-jobs/copyJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

copyJobId

Identifiziert einen Kopierauftrag eindeutig.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
    }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CopyJob

Enthält detaillierte Informationen zu einem Kopierauftrag.

Typ: CopyJob Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeFramework

Service: AWS Backup

Gibt Framwork-Details für die angegebene `FrameworkName` zurück.

Anforderungssyntax

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

frameworkName

Der eindeutige Name eines Frameworks.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Das Datum und die Uhrzeit, zu der ein Framework erstellt wurde, in ISO 8601-Darstellung. Der Wert von `CreationTime` ist auf Millisekunden genau. Beispielsweise steht 2020-07-10T 15:00:00.000-08:00 für den 10. Juli 2020 um 15.00 Uhr, UTC minus 8 Stunden.

Typ: Zeitstempel

DeploymentStatus

Der Bereitstellungsstatus eines Frameworks. Die Status sind:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Typ: Zeichenfolge

FrameworkArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

FrameworkControls

Die Kontrollen, aus denen das Framework besteht. Jedes Steuerelement in der Liste hat einen Namen, Eingabeparameter und einen Bereich.

Typ: Array von FrameworkControl-Objekten

FrameworkDescription

Eine optionale Beschreibung des Frameworks.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

FrameworkName

Der eindeutige Name eines Frameworks.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Ein Framework besteht aus einem oder mehreren Steuerelementen. Jede Steuerung regelt eine Ressource, z. B. Backup-Pläne, Backup-Auswahlen, Backup-Tresore oder Wiederherstellungspunkte. Sie können die AWS Config -Aufzeichnung auch für jede Ressource ein- oder ausschalten. Die Status sind:

- `ACTIVE`, wenn die Aufzeichnung für alle Ressourcen, die das Framework regelt, aktiviert ist.
- `PARTIALLY_ACTIVE`, wenn die Aufzeichnung für mindestens eine Ressource, die das Framework regelt, deaktiviert ist.
- `INACTIVE`, wenn die Aufzeichnung für alle Ressourcen, die das Framework regelt, deaktiviert ist.
- `UNAVAILABLE`wenn AWS Backup der Aufnahmestatus derzeit nicht validiert werden kann.

Typ: Zeichenfolge

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `DescribeFrameworkOutput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeGlobalSettings

Service: AWS Backup

Beschreibt, ob das AWS Konto für die kontoübergreifende Sicherung aktiviert ist. Gibt einen Fehler zurück, wenn das Konto kein Mitglied einer Organisation in Organizations ist. Beispiel: `describe-global-settings --region us-west-2`

Anforderungssyntax

```
GET /global-settings HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GlobalSettings

Der Status der Markierung `isCrossAccountBackupEnabled`.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

LastUpdateTime

Datum und Uhrzeit der letzten Aktualisierung der Markierung `isCrossAccountBackupEnabled`. Diese Aktualisierung ist im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastUpdateTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeProtectedResource

Service: AWS Backup

Gibt Informationen über eine gespeicherte Ressource zurück, einschließlich des letzten Backups, ihres Amazon-Ressourcennamens (ARN) und des AWS Servicetyps der gespeicherten Ressource.

Anforderungssyntax

```
GET /resources/resourceArn HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

resourceArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

LastBackupTime

Das Datum und die Uhrzeit des letzten Backups einer Ressource im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `LastBackupTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

LastBackupVaultArn

Der ARN (Amazon Resource Name) des Backup-Tresors, der den neuesten Backup-Wiederherstellungspunkt enthält.

Typ: Zeichenfolge

LastRecoveryPointArn

Der ARN (Amazon Resource Name) des letzten Wiederherstellungspunkts.

Typ: Zeichenfolge

LatestRestoreExecutionTimeMinutes

Die Zeit in Minuten, die für den Abschluss des letzten Wiederherstellungsauftrags benötigt wurde.

Type: Long

LatestRestoreJobCreationDate

Das Erstellungsdatum des letzten Wiederherstellungsauftrags.

Typ: Zeitstempel

LatestRestoreRecoveryPointCreationDate

Das Datum, an dem der letzte Erholungspunkt erstellt wurde.

Typ: Zeitstempel

ResourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

ResourceName

Der Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

ResourceType

Der Typ der AWS Ressource, die als Erholungspunkt gespeichert wurde, z. B. ein Amazon EBS-Volume oder eine Amazon RDS-Datenbank.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeRecoveryPoint

Service: AWS Backup

Gibt Metadaten zurück, die einem Wiederherstellungspunkt zugeordnet sind, einschließlich ID, Status, Verschlüsselung und Lebenszyklus.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

BackupVaultAccountId

Die Konto-ID des angegebenen Backup-Tresors.

Pattern: `^[0-9]{12}$`

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupSizeInBytes

Die Größe eines Backups in Byte

Type: Long

BackupVaultArn

Ein ARN, der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Ein `CalculatedLifecycle`-Objekt, das `DeleteAt`- und `MoveToColdStorageAt`-Zeitstempel enthält.

Typ: CalculatedLifecycle Objekt

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Erstellen eines Wiederherstellungspunkts abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CompositeMemberIdentifier

Die ID einer Ressource innerhalb einer Verbundgruppe, z. B. eines verschachtelten (untergeordneten) Wiederherstellungspunkts, der zu einem zusammengesetzten (übergeordneten) Stack gehört. Die ID wird von der logischen ID innerhalb eines Stacks übertragen.

Typ: Zeichenfolge

CreatedBy

Enthält identifizierende Informationen über die Erstellung eines Wiederherstellungspunkts, einschließlich `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` und `BackupRuleId` des Backup-Plans, mit dem er erstellt wurde.

Typ: RecoveryPointCreator Objekt

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungspunkts im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

EncryptionKeyArn

Die serverseitige Verschlüsselung zum Schutz Ihrer Backups, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

IsEncrypted

Ein boolescher Wert, der als `TRUE` zurückgegeben wird, wenn der angegebene Wiederherstellungspunkt verschlüsselt ist, oder als `FALSE`, wenn der Wiederherstellungspunkt nicht verschlüsselt ist.

Typ: Boolesch

IsParent

Dies gibt den booleschen Wert zurück, dass es sich bei einem Wiederherstellungspunkt um einen übergeordneten (zusammengesetzten) Auftrag handelt.

Typ: Boolesch

LastRestoreTime

Das Datum und die Uhrzeit der letzten Wiederherstellung eines Wiederherstellungspunkts im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `LastRestoreTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Archivspeicher übertragene Sicherungen müssen mindestens 90 Tage lang im Archivspeicher gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Typ: Lifecycle Objekt

ParentRecoveryPointArn

Dies ist ein ARN, der einen übergeordneten (zusammengesetzten) Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

ResourceArn

Ein ARN bezeichnet eindeutig eine gespeicherte Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

ResourceName

Der Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

ResourceType

Der AWS Ressourcentyp, der als Erholungspunkt gespeichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Ein Amazon-Ressourcenname (ARN), der den Quelltresor, in dem die Ressource ursprünglich gesichert wurde, eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Wenn die Wiederherstellung für dasselbe AWS Konto oder dieselbe Region wiederhergestellt wird, gilt dieser Wert. `null`

Typ: Zeichenfolge

Status

Ein Statuscode, der den Status des Wiederherstellungspunkts angibt.

`PARTIAL`Der Status gibt an, dass der Wiederherstellungspunkt nicht erstellt werden AWS Backup konnte, bevor das Backup-Fenster geschlossen wurde. Informationen zur Verlängerung des Zeitfensters für Ihren Backup-Plan mithilfe der API finden Sie unter UpdateBackupPlan. Sie

können das Fenster Ihres Backup-Plans auch mithilfe der Konsole vergrößern, indem Sie Ihren Backup-Plan auswählen und bearbeiten.

`EXPIRED`Der Status gibt an, dass der Wiederherstellungspunkt seine Aufbewahrungsfrist überschritten hat, aber nicht AWS Backup berechtigt ist oder er aus anderen Gründen nicht gelöscht werden kann. Informationen zum manuellen Löschen dieser Wiederherstellungspunkte finden Sie unter Schritt 3: Löschen der Wiederherstellungspunkte im Abschnitt Ressourcen bereinigen unter Erste Schritte.

Der Status `STOPPED` tritt bei einem kontinuierlichen Backup auf, bei dem ein Benutzer durch eine Aktion das kontinuierliche Backup deaktiviert hat. Dies kann durch das Entfernen von Berechtigungen, das Deaktivieren der Versionsverwaltung, das Deaktivieren von Ereignissen, an die gesendet werden EventBridge, oder das Deaktivieren der EventBridge Regeln, die von eingerichtet wurden, verursacht werden. AWS Backup

Um den Status `STOPPED` zu lösen, stellen Sie sicher, dass alle angeforderten Berechtigungen vorhanden sind und dass die Versionierung für den S3-Bucket aktiviert ist. Sobald diese Bedingungen erfüllt sind, führt die nächste Ausführung einer Backup-Regel dazu, dass ein neuer kontinuierlicher Wiederherstellungspunkt erstellt wird. Die Wiederherstellungspunkte mit dem Status „ANGEHALTEN“ müssen nicht gelöscht werden.

Bei SAP HANA auf Amazon tritt der `STOPPED`-EC2-Status aufgrund einer Benutzeraktion, einer Fehlkonfiguration der Anwendung oder eines Backup-Fehlers auf. Um sicherzustellen, dass zukünftige kontinuierliche Backups erfolgreich sind, beziehen Sie sich auf den Status des Wiederherstellungspunkts und überprüfen Sie SAP HANA auf Einzelheiten.

Typ: Zeichenfolge

Zulässige Werte: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Eine Statusmeldung, die den Status des Wiederherstellungspunkts erklärt.

Typ: Zeichenfolge

StorageClass

Gibt die Speicherklasse des Wiederherstellungspunkts zurück. Gültige Werte sind `WARM` oder `COLD`.

Typ: Zeichenfolge

Zulässige Werte: `WARM | COLD | DELETED`

VaultType

Der Typ des Tresors, in dem der beschriebene Recovery Point gespeichert ist.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeRegionSettings

Service: AWS Backup

Gibt die aktuellen Service-Opt-In-Einstellungen für die Region zurück. Wenn das Service-Opt-In für einen Dienst aktiviert ist, AWS Backup versucht, die Ressourcen dieses Dienstes in dieser Region zu schützen, wenn die Ressource in einem On-Demand-Backup oder einem geplanten Backup-Plan enthalten ist. Andernfalls versucht AWS Backup nicht, die Ressourcen dieses Services in dieser Region zu schützen.

Anforderungssyntax

```
GET /account-settings HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ResourceTypeManagementPreference

Gibt zurück, ob die Backups für einen Ressourcentyp AWS Backup vollständig verwaltet werden.

Informationen zu den Vorteilen der vollständigen AWS Backup Verwaltung finden Sie unter Vollständige AWS Backup Verwaltung.

Eine Liste der Ressourcentypen und ob die einzelnen Ressourcentypen die vollständige AWS Backup Verwaltung unterstützen, finden Sie in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen.

Falls`"DynamoDB":false`, können Sie die vollständige AWS Backup Verwaltung für DynamoDB-Backups aktivieren, indem Sie die erweiterten DynamoDB-Backup-Funktionen aktivieren AWS Backup.

Typ: Zeichenfolge zu boolescher Abbildung

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

Die Dienste zusammen mit den Opt-in-Einstellungen in der Region.

Typ: Zeichenfolge zu boolescher Abbildung

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeReportJob

Service: AWS Backup

Gibt die Details zurück, die mit der Erstellung eines Berichts verknüpft sind, wie von seiner `ReportJobId` angegeben.

Anforderungssyntax

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

reportJobId

Der Bezeichner des Berichtsauftrags. Eine eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolge, die maximal 1 024 Byte lang ist. Die Berichtsauftrags-ID kann nicht bearbeitet werden.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
    }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ReportJob

Die Informationen zu einem Berichtsauftrag, einschließlich der Fertigstellungs- und Bearbeitungszeit, des Berichtsziels, der eindeutigen Berichtsauftrags-ID, des Amazon-Ressourcennamens (ARN), der Berichtsvorlage, des Status und der Statusmeldung.

Typ: ReportJob Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeReportPlan

Service: AWS Backup

Gibt eine Liste aller Berichtspläne für ein AWS-Konto und zurück AWS-Region.

Anforderungssyntax

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

reportPlanName

Der eindeutige Name eines Berichtsplans.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
         }
      }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ReportPlan

Gibt Details über den Berichtsplan zurück, der durch seinen Namen angegeben ist. Zu diesen Details gehören der Amazon-Ressourcenname (ARN) des Berichtsplans, die Beschreibung, die Einstellungen, der Übermittlungskanal, der Bereitstellungsstatus, die Erstellungszeit sowie die letzten Versuche und die erfolgreichen Ausführungen.

Typ: ReportPlan Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DescribeRestoreJob

Service: AWS Backup

Gibt Metadaten zurück, die einem Wiederherstellungsauftrag zugeordnet sind, der durch eine Auftrags-ID angegeben ist.

Anforderungssyntax

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

restoreJobId

Identifiziert den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AccountId

Gibt die Konto-ID zurück, der der Wiederherstellungsauftrag angehört.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

BackupSizeInBytes

Die Größe der wiederhergestellten Ressource in Byte.

Type: Long

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Wiederherstellen eines Wiederherstellungspunkts abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CreatedBy

Enthält identifizierende Informationen zur Erstellung eines Wiederherstellungsauftrags.

Typ: RestoreJobCreator Objekt

CreatedResourceArn

Der Amazon-Ressourcenname (ARN) der Ressource, die durch den Wiederherstellungsauftrag erstellt wurde.

Das Format des ARN hängt vom Typ der gesicherten Ressource ab.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungsauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

DeletionStatus

Der Status der durch den Wiederherstellungstest generierten Daten.

Typ: Zeichenfolge

Zulässige Werte: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Dies beschreibt den Löschstatus des Wiederherstellungsauftrags.

Typ: Zeichenfolge

ExpectedCompletionTimeMinutes

Die Zeit in Minuten, die ein Auftrag zur Wiederherstellung eines Wiederherstellungspunkts voraussichtlich in Anspruch nehmen wird.

Type: Long

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

PercentDone

Enthält einen geschätzten Prozentsatz der Fertigstellung eines Auftrags zum Zeitpunkt der Abfrage des Auftragsstatus.

Typ: Zeichenfolge

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

RecoveryPointCreationDate

Das Erstellungsdatum des Wiederherstellungspunkts, der durch den angegebenen Wiederherstellungsauftrag erstellt wurde.

Typ: Zeitstempel

ResourceType

Gibt Metadaten zurück, die einem Wiederherstellungsauftrag zugeordnet sind, sortiert nach Ressourcentyp.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Identifiziert den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig.

Typ: Zeichenfolge

Status

Statuscode, der den Status des Auftrags angibt, der durch AWS Backup die Wiederherstellung eines Wiederherstellungspunkts initiiert wurde.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Eine Meldung, die den Status eines Auftrags zur Wiederherstellung eines Wiederherstellungspunkts anzeigt.

Typ: Zeichenfolge

ValidationStatus

Der Status der Überprüfung, die für den angegebenen Wiederherstellungsauftrag ausgeführt wurde.

Typ: Zeichenfolge

Zulässige Werte: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

Die Statusmeldung.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

DependencyFailureException

Ein abhängiger AWS Dienst oder eine abhängige Ressource hat einen Fehler an den AWS Backup Dienst zurückgegeben, und die Aktion kann nicht abgeschlossen werden.

HTTP Status Code: 500

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DisassociateRecoveryPoint

Service: AWS Backup

Löscht den angegebenen Continuous Backup-Wiederherstellungspunkt vom Quellservice, wie Amazon RDS, AWS Backup und gibt die Kontrolle über dieses kontinuierliche Backup an den Quellservice weiter. Der Quellservice erstellt und speichert weiterhin fortlaufende Backups unter Verwendung des Lebenszyklus, den Sie in Ihrem ursprünglichen Backup-Plan angegeben haben.

Unterstützt keine Wiederherstellungspunkte für Snapshot-Backups.

Anforderungssyntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der eindeutige Name eines AWS Backup Tresors.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen AWS Backup Wiederherstellungspunkt eindeutig identifiziert.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

InvalidResourceStateException

AWS Backup führt bereits eine Aktion an diesem Wiederherstellungspunkt durch. Die von Ihnen angeforderte Aktion kann erst ausgeführt werden, wenn die erste Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DisassociateRecoveryPointFromParent

Service: AWS Backup

Durch diese Aktion für einen bestimmten untergeordneten (verschachtelten) Wiederherstellungspunkt wird die Beziehung zwischen dem angegebenen und seinem übergeordneten (zusammengesetzten) Wiederherstellungspunkt aufgehoben.

Anforderungssyntax

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem der untergeordnete (verschachtelte) Erholungspunkt gespeichert ist. Backup-Tresore werden anhand von Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und für die AWS Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Der Amazon-Ressourcenname (ARN), der den untergeordneten (verschachtelten) Erholungspunkt eindeutig identifiziert; zum Beispiel `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 204
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ExportBackupPlanTemplate

Service: AWS Backup

Gibt den durch die Plan-ID angegebenen Backup-Plan als Backup-Vorlage zurück.

Anforderungssyntax

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanTemplateJson

Der Text einer Backup-Planvorlage im JSON-Format.

> **Note**
>
> Dies ist ein signiertes JSON-Dokument, das vor der Übergabe an `GetBackupPlanFromJSON`. nicht geändert werden kann.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupPlan

Service: AWS Backup

Gibt `BackupPlan`-Details für die angegebene `BackupPlanId` zurück. Bei den Details handelt es sich zusätzlich zu den Plan-Metadaten um den Text eines Backup-Plans im JSON-Format.

Anforderungssyntax

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Version-IDs können nicht bearbeitet werden.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AdvancedBackupSettings

Enthält eine Liste von `BackupOptions` für jeden Ressourcentyp. Die Liste wird nur aufgefüllt, wenn die erweiterte Option für den Backup-Plan festgelegt ist.

Typ: Array von AdvancedBackupSetting-Objekten

BackupPlan

Gibt den Text eines Backup-Plans an. Beinhaltet einen `BackupPlanName` und einen oder mehrere Sätze von `Rules`.

Typ: BackupPlan Objekt

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung der Domainliste im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird.

Typ: Zeichenfolge

DeletionDate

Das Datum und die Uhrzeit der Löschung eines Backup-Plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `DeletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

LastExecutionDate

Das letzte Mal, als dieser Backup-Plan ausgeführt wurde. Datum und Uhrzeit im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastExecutionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Version-IDs können nicht bearbeitet werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupPlanFromJSON

Service: AWS Backup

Gibt ein gültiges JSON-Dokument zurück, das einen Backup-Plan oder einen Fehler angibt.

Anforderungssyntax

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupPlanTemplateJson

Ein vom Kunden bereitgestelltes Dokument mit einem Backup-Plan im JSON-Format.

Typ: Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
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"
         }
      ]
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlan

Gibt den Text eines Backup-Plans an. Beinhaltet einen `BackupPlanName` und einen oder mehrere Sätze von `Rules`.

Typ: BackupPlan Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupPlanFromTemplate

Service: AWS Backup

Gibt die durch seine `templateId` angegebene Vorlage als Backup-Plan zurück.

Anforderungssyntax

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

templateId

Identifiziert eindeutig eine gespeicherte Backup-Planvorlage.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
         }
      ]
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanDocument

Gibt den Text eines Backup-Plans auf der Grundlage der Zielvorlage zurück, einschließlich des Namens, der Regeln und des Backup-Tresors des Plans.

Typ: BackupPlan Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupSelection

Service: AWS Backup

Gibt Auswahlmetadaten und ein Dokument im JSON-Format zurück, das eine Liste von Ressourcen angibt, die einem Backup-Plan zugeordnet sind.

Anforderungssyntax

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

selectionId

Identifiziert den Text einer Anforderung zum Zuweisen einer Gruppe von Ressourcen zu einem Backup-Plan eindeutig.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

BackupSelection

Gibt den Text einer Anforderung zum Zuweisen einer Reihe von Ressourcen zu einem Sicherungsplan an.

Typ: BackupSelection Objekt

CreationDate

Das Datum und die Uhrzeit der Erstellung einer Backup-Auswahl im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird.

Typ: Zeichenfolge

SelectionId

Identifiziert den Text einer Anforderung zum Zuweisen einer Gruppe von Ressourcen zu einem Backup-Plan eindeutig.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupVaultAccessPolicy

Service: AWS Backup

Gibt das Dokument mit der Zugriffsrichtlinie zurück, das dem benannten Backup-Tresor zugeordnet ist.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

Das Dokument mit der Zugriffsrichtlinie für den Backup-Tresor im JSON-Format.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBackupVaultNotifications

Service: AWS Backup

Gibt Ereignisbenachrichtigungen für den angegebenen Backup-Tresor zurück.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

BackupVaultEvents

Ein Array von Ereignissen, die den Status der Aufträge zur Sicherung von Ressourcen im Sicherungstresor angeben.

Typ: Zeichenfolgen-Array

Zulässige Werte: `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

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

Ein ARN zur eindeutigen Identifizierung eines Amazon Simple Notification Service (Amazon SNS)-Themas, z. B. `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

GetLegalHold

Service: AWS Backup

Diese Aktion gibt Details zu einer bestimmten gesetzlichen Sperre zurück. Bei den Details handelt es sich zusätzlich zu den Metadaten um den Hauptteil einer gesetzlichen Aufbewahrungsfrist im JSON-Format.

Anforderungssyntax

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

legalHoldId

Die ID des gesetzlich vorgeschriebenen Speichers.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CancelDescription

Der Grund für die Aufhebung der gesetzlichen Sperre.

Typ: Zeichenfolge

CancellationDate

Der Zeitpunkt, zu dem die gesetzliche Sperre aufgehoben wurde.

Typ: Zeitstempel

CreationDate

Der Zeitpunkt, zu dem die gesetzliche Sperre eingerichtet wurde.

Typ: Zeitstempel

Description

Die Beschreibung der gesetzlichen Sperre.

Typ: Zeichenfolge

LegalHoldArn

Der Framework-ARN für den angegebenen gesetzlichen Aufbewahrungszeitraum. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

LegalHoldId

Die ID der gesetzlichen Aufbewahrungsfrist.

Typ: Zeichenfolge

RecoveryPointSelection

Die Kriterien für die Zuweisung einer Gruppe von Ressourcen, z. B. Ressourcentypen oder Backup-Tresore.

Typ: RecoveryPointSelection Objekt

RetainRecordUntil

Das Datum und die Uhrzeit, bis zu denen der gesetzliche Aufbewahrungsdatensatz aufbewahrt wird.

Typ: Zeitstempel

Status

Der Status der gesetzlichen Sperre.

Typ: Zeichenfolge

Zulässige Werte: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Der Titel der gesetzlichen Aufbewahrung.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetRecoveryPointRestoreMetadata

Service: AWS Backup

Gibt eine Reihe von Metadaten-Schlüssel-Wert-Paaren zurück, die zur Erstellung des Backups verwendet wurden.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

BackupVaultAccountId

Die Konto-ID des angegebenen Backup-Tresors.

Pattern: `^[0-9]{12}$`

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein ARN, der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

ResourceType

Der Ressourcentyp des Wiederherstellungspunkts.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

Der Satz von Schlüssel-Wert-Paaren für Metadaten, die die ursprüngliche Konfiguration der gesicherten Ressource beschreiben. Diese Werte variieren je nach Service, der wiederhergestellt wird.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetRestoreJobMetadata

Service: AWS Backup

Diese Anforderungen gibt die Metadaten für den angegebenen Wiederherstellungsauftrag zurück.

Anforderungssyntax

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

restoreJobId

Dies ist eine eindeutige Kennung eines darin enthaltenen Wiederherstellungsauftrags AWS Backup.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Metadata

Dies enthält die Metadaten des angegebenen Backup-Auftrags.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

RestoreJobId

Dies ist eine eindeutige Kennung eines darin enthaltenen Wiederherstellungsauftrags AWS Backup.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetRestoreTestingInferredMetadata

Service: AWS Backup

Diese Anforderung gibt den minimal erforderlichen Satz von Metadaten zurück, der zum Starten eines Wiederherstellungsauftrags mit sicheren Standardeinstellungen erforderlich ist. `BackupVaultName` und `RecoveryPointArn` sind erforderliche Parameter. `BackupVaultAccountId` ist ein optionaler Parameter.

Anforderungssyntax

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

BackupVaultAccountId

Die Konto-ID des angegebenen Backup-Tresors.

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden anhand von Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und für die AWS Region, in der sie erstellt wurden, eindeutig sind. Sie bestehen aus Kleinbuchstaben, Zahlen und Bindestrichen.

Erforderlich: Ja

RecoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

InferredMetadata

Dies ist eine Übersicht der Zeichenfolgen der Metadaten, die aus der Anfrage abgeleitet wurden.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetRestoreTestingPlan

Service: AWS Backup

Gibt `RestoreTestingPlan`-Details für die angegebene `RestoreTestingPlanName` zurück. Bei den Details handelt es sich zusätzlich zu den Plan-Metadaten um den Text eines Backup-Plans im JSON-Format.

Anforderungssyntax

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Der eindeutige Name des Wiederherstellungstestplans ist erforderlich.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

RestoreTestingPlan

Gibt den Hauptteil eines Wiederherstellungstestplans an. Beinhaltet `RestoreTestingPlanName`.

Typ: RestoreTestingPlanForGet Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetRestoreTestingSelection

Service: AWS Backup

Retouren RestoreTestingSelection, in dem Ressourcen und Elemente des Wiederherstellungstestplans angezeigt werden.

Anforderungssyntax

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Der eindeutige Name des Wiederherstellungstestplans ist erforderlich.

Erforderlich: Ja

RestoreTestingSelectionName

Der eindeutige Name der Wiederherstellungstest-Auswahl ist erforderlich.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

RestoreTestingSelection

Eindeutiger Name der Wiederherstellungstest-Auswahl.

Typ: RestoreTestingSelectionForGet Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetSupportedResourceTypes

Service: AWS Backup

Gibt die AWS Ressourcentypen zurück, die von unterstützt werden AWS Backup.

Anforderungssyntax

```
GET /supported-resource-types HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ResourceTypes

Enthält eine Zeichenfolge mit den unterstützten AWS Ressourcentypen:

- `Aurora` für Amazon Aurora
- `CloudFormation`für AWS CloudFormation
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)
- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store

- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System
- `FSX` für Amazon FSx
- `Neptune` für Amazon Neptune
- `RDS` für Amazon Relational Database Service
- `Redshift` für Amazon Redshift
- `SAP HANA on Amazon EC2`für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- `S3`für Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`für AWS Storage Gateway
- `Timestream` für Amazon Timestream
- `VirtualMachine`für virtuelle VMware-Maschinen

Typ: Zeichenfolgen-Array

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupJobs

Service: AWS Backup

Gibt eine Liste der vorhandenen Backup-Aufträge für ein authentifiziertes Konto für die letzten 30 Tagen zurück. Erwägen Sie, für einen längeren Zeitraum diese Überwachungstools zu verwenden.

Anforderungssyntax

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByAccountId

Die Konto-ID, von der die Aufträge aufgelistet werden sollen. Gibt nur Backup-Aufträge zurück, die der angegebenen Konto-ID zugeordnet sind.

Wenn es von einem AWS Organizations Verwaltungskonto aus verwendet wird, werden beim Übergeben alle Jobs in der gesamten Organisation * zurückgegeben.

Pattern: `^[0-9]{12}$`

ByBackupVaultName

Gibt nur Backup-Aufträge zurück, die im angegebenen Backup-Tresor gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Gibt nur Backup-Aufträge zurück, die nach einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCompleteBefore

Gibt nur Backup-Aufträge zurück, die vor einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCreatedAfter

Gibt nur Backup-Aufträge zurück, die nach dem angegebenen Datum erstellt wurden.

ByCreatedBefore

Gibt nur Backup-Aufträge zurück, die vor dem angegebenen Datum erstellt wurden.

ByMessageCategory

Dies ist ein optionaler Parameter, der verwendet werden kann, um Jobs herauszufiltern MessageCategory , deren Wert dem von Ihnen eingegebenen Wert entspricht.

Beispielzeichenfolgen können `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` oder `InvalidParameters` sein.

Anzeige Überwachung

Der Platzhalter () gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

ByParentJobId

Dies ist ein Filter, um untergeordnete (verschachtelte) Aufträge auf Grundlage der übergeordneten Auftrags-ID aufzulisten.

ByResourceArn

Gibt nur Backup-Aufträge zurück, die mit dem Amazon-Ressourcennamen (ARN) der angegebenen Ressource übereinstimmen.

ByResourceType

Gibt nur Backup-Aufträge für die angegebenen Ressourcen zurück:

- `Aurora` für Amazon Aurora
- `CloudFormation`für AWS CloudFormation
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)
- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store
- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System

- FSx für Amazon FSx
- Neptune für Amazon Neptune
- Redshift für Amazon Redshift
- RDS für Amazon Relational Database Service
- SAP HANA on Amazon EC2 für SAP-HANA-Datenbanken
- Storage Gatewayfür AWS Storage Gateway
- S3 für Amazon S3
- Timestream für Amazon Timestream
- VirtualMachine für virtuelle Maschinen

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

ByState

Gibt nur Backup-Aufträge zurück, die sich im angegebenen Status befinden.

Completed with issues ist ein Status, der nur in der AWS Backup -Konsole zu finden ist. Bei API bezieht sich dieser Status auf Aufträge mit einem Status von COMPLETED und einer MessageCategory mit einem anderen Wert als SUCCESS; das heißt, der Status ist abgeschlossen, hat aber eine Statusmeldung.

Um die Anzahl der Aufträge für Completed with issues zu ermitteln, führen Sie zwei GET-Anfragen aus und subtrahieren Sie die zweite, kleinere Zahl:

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

Zulässige Werte: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der MaxResults Anzahl von Elementen gestellt

wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupJobs

Eine Reihe von Strukturen, die Metadaten zu Ihren Backup-Aufträgen enthalten, die im JSON-Format zurückgegeben wurden.

Typ: Array von BackupJob-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupJobSummaries

Service: AWS Backup

Dies ist eine Anforderung nach einer Zusammenfassung der Backup-Aufträge, die in den letzten 30 Tagen erstellt oder ausgeführt wurden. Sie können die Parameter AccountID, State,, ResourceType, MessageCategory, oder angeben AggregationPeriod MaxResults, um Ergebnisse NextToken zu filtern.

Diese Anfrage gibt eine Zusammenfassung zurück, die Region, Account, State, ResourceType, MessageCategory, StartTime EndTime, und Anzahl der enthaltenen Jobs enthält.

Anforderungssyntax

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

AccountId

Gibt die Anzahl der Aufträge für das angegebene Konto zurück.

Wenn die Anfrage von einem Mitgliedskonto oder einem Konto gesendet wird, das nicht Teil von AWS Organizations ist, werden Jobs innerhalb des Kontos des Anfragenden zurückgegeben.

Root-, Admin- und delegierte Administratorkonten können den Wert ANY verwenden, um die Anzahl der Aufträge von jedem Konto in der Organisation zurückzugeben.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge aller Konten innerhalb der authentifizierten Organisation und gibt dann die Summe zurück.

Pattern: `^[0-9]{12}$`

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- `ONE_DAY`- Die tägliche Anzahl der Jobs der letzten 14 Tage.

- SEVEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 7 Tage.
- FOURTEEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Zulässige Werte: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Der Wert ist eine Ganzzahl. Der Bereich der akzeptierten Werte liegt zwischen 1 und 500.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Zu den akzeptierten Zeichenfolgen gehören beispielsweise AccessDenied, Success und InvalidParameters. Eine Liste der akzeptierten MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der MaxResults Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen NextToken, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

ResourceType

Gibt die Anzahl der Aufträge für den angegebenen Ressourcentyp zurück. Verwenden Sie Anfrage GetSupportedResourceTypes, um Zeichenfolgen für unterstützte Ressourcentypen abzurufen.

Der Wert ANY gibt die Anzahl aller Ressourcentypen zurück.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge für alle Ressourcentypen und gibt die Summe zurück.

Der Typ der AWS Ressource, die gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Dieser Parameter gibt die Anzahl der Aufträge mit dem angegebenen Zustand zurück.

Der Wert ANY gibt die Anzahl aller Zustände zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Zustände und gibt die Summe zurück.

`Completed with issues` ist ein Status, der nur in der AWS Backup -Konsole zu finden ist. Bei API bezieht sich dieser Status auf Aufträge mit einem Status von `COMPLETED` und einer `MessageCategory` mit einem anderen Wert als `SUCCESS`; das heißt, der Status ist abgeschlossen, hat aber eine Statusmeldung. Um die Anzahl der Aufträge für `Completed with issues` zu ermitteln, führen Sie zwei GET-Anfragen aus und subtrahieren Sie die zweite, kleinere Zahl:

/audit/ abrufen? backup-job-summaries AggregationPeriod=Fourteen_days&state=Abgeschlossen

/audit/ abrufen? backup-job-summaries AggregationPeriod=VIERZEHN_TAGE& =SUCCESS&STATE=Abgeschlossen MessageCategory

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- `ONE_DAY`- Die tägliche Anzahl der Jobs der letzten 14 Tage.
- `SEVEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 7 Tage.
- `FOURTEEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Typ: Zeichenfolge

BackupJobSummaries

Die zusammenfassenden Informationen.

Typ: Array von BackupJobSummary-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupPlans

Service: AWS Backup

Listet die aktiven Backup-Pläne für das Konto auf.

Anforderungssyntax

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

IncludeDeleted

Ein boolescher Wert mit dem Standardwert `FALSE`, der gelöschte Backup-Pläne zurückgibt, wenn er auf `TRUE` gesetzt ist.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlansList

Informationen zu den Backup-Plänen.

Typ: Array von BackupPlansListMember-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupPlanTemplates

Service: AWS Backup

Listet die Backup-Planvorlagen auf.

Anforderungssyntax

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Artikel.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
```

```
   "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanTemplatesList

Eine Reihe von Elementen in der Vorlagenliste, die Metadaten zu Ihren gespeicherten Vorlagen enthalten.

Typ: Array von BackupPlanTemplatesListMember-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupPlanVersions

Service: AWS Backup

Gibt Versionsmetadaten Ihrer Backup-Pläne zurück, einschließlich Amazon-Ressourcennamen (ARNs), Backup-Plan-IDs, Erstellungs- und Löschdaten, Plannamen und Versions-IDs.

Anforderungssyntax

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupPlanVersionsList

Eine Reihe von Versionslistenelementen, die Metadaten zu Ihren Backup-Plänen enthalten.

Typ: Array von BackupPlansListMember-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupSelections

Service: AWS Backup

Gibt eine Reihe mit Metadaten der Ressourcen zurück, die dem Ziel-Backup-Plan zugeordnet sind.

Anforderungssyntax

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSelectionsList": [
```

```
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupSelectionsList

Eine Reihe von Elementen in der Backup-Auswahlliste, die Metadaten zu jeder Ressource in der Liste enthalten.

Typ: Array von BackupSelectionsListMember-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListBackupVaults

Service: AWS Backup

Gibt eine Liste von Wiederherstellungspunkt-Speichercontainern zusammen mit Informationen zu ihnen zurück.

Anforderungssyntax

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByShared

Dieser Parameter sortiert die Liste der Tresore nach gemeinsam genutzten Tresoren.

ByVaultType

Dieser Parameter sortiert die Liste der Tresore nach Tresortyp.

Zulässige Werte: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultList

Eine Reihe von Elementen der Backup-Tresor-Liste mit Tresor-Metadaten, darunter Amazon-Ressourcenname (ARN), Anzeigename, Erstellungsdatum, Anzahl der gespeicherten Wiederherstellungspunkte und Verschlüsselungsinformationen, falls die im Backup-Tresor gespeicherten Ressourcen verschlüsselt sind.

Typ: Array von BackupVaultListMember-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt

wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListCopyJobs

Service: AWS Backup

Gibt Metadaten zu Ihren Kopieraufträgen zurück.

Anforderungssyntax

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByAccountId

Die Konto-ID, von der die Aufträge aufgelistet werden sollen. Gibt nur Kopieraufträge zurück, die der angegebenen Konto-ID zugeordnet sind.

Pattern: `^[0-9]{12}$`

ByCompleteAfter

Gibt nur Kopieraufträge zurück, die nach einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCompleteBefore

Gibt nur Kopieraufträge zurück, die vor einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCreatedAfter

Gibt nur Kopieraufträge zurück, die nach dem angegebenen Datum erstellt wurden.

ByCreatedBefore

Gibt nur Kopieraufträge zurück, die vor dem angegebenen Datum erstellt wurden.

ByDestinationVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Quell-Backup-Tresor eindeutig identifiziert, von dem kopiert werden soll, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Dies ist ein optionaler Parameter, mit dem Jobs herausgefiltert werden können MessageCategory , deren Wert dem von Ihnen eingegebenen Wert entspricht.

Beispielzeichenfolgen können `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` oder `INVALIDPARAMETERS` sein.

Unter Überwachung finden Sie eine Liste der akzeptierten Zeichenfolgen.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

ByParentJobId

Dies ist ein Filter, um untergeordnete (verschachtelte) Aufträge auf Grundlage der übergeordneten Auftrags-ID aufzulisten.

ByResourceArn

Gibt nur Kopieraufträge zurück, die mit dem Amazon-Ressourcennamen (ARN) der angegebenen Ressource übereinstimmen.

ByResourceType

Gibt nur Backup-Aufträge für die angegebenen Ressourcen zurück:

- `Aurora` für Amazon Aurora
- `CloudFormation`für AWS CloudFormation
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)
- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store
- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System
- `FSx` für Amazon FSx
- `Neptune` für Amazon Neptune
- `Redshift` für Amazon Redshift
- `RDS` für Amazon Relational Database Service

- `SAP HANA on Amazon EC2` für SAP-HANA-Datenbanken
- `Storage Gateway`für AWS Storage Gateway
- `S3` für Amazon S3
- `Timestream` für Amazon Timestream
- `VirtualMachine` für virtuelle Maschinen

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Gibt nur Kopieraufträge zurück, die sich im angegebenen Status befinden.

Zulässige Werte: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anfrage zur Rückgabe der MaxResults Anzahl von Elementen gestellt wird, NextToken können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend an der Position, auf die das nächste Token zeigt.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CopyJobs

Eine Reihe von Strukturen, die Metadaten zu Ihren Kopieraufträgen enthalten, die im JSON-Format zurückgegeben wurden.

Typ: Array von CopyJob-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anfrage zur Rückgabe der MaxResults Anzahl von Elementen gestellt wird, NextToken können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend an der Position, auf die das nächste Token zeigt.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

ListCopyJobSummaries

Service: AWS Backup

Diese Anforderung ruft eine Liste der Kopieraufträge ab, die in den letzten 30 Tagen erstellt oder ausgeführt wurden. Sie können die Parameter AccountID, State,, ResourceType, MessageCategory, oder AggregationPeriod verwenden MaxResults, um Ergebnisse NextToken zu filtern.

Diese Anfrage gibt eine Zusammenfassung zurück, die Region, Account, State, RestourceType, MessageCategory, StartTime EndTime, und Anzahl der enthaltenen Jobs enthält.

Anforderungssyntax

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

AccountId

Gibt die Anzahl der Aufträge für das angegebene Konto zurück.

Wenn die Anfrage von einem Mitgliedskonto oder einem Konto gesendet wird, das nicht Teil von AWS Organizations ist, werden Jobs innerhalb des Kontos des Anfragenden zurückgegeben.

Root-, Admin- und delegierte Administratorkonten können den Wert ANY verwenden, um die Anzahl der Aufträge von jedem Konto in der Organisation zurückzugeben.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge aller Konten innerhalb der authentifizierten Organisation und gibt dann die Summe zurück.

Pattern: `^[0-9]{12}$`

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- ONE_DAY- Die tägliche Anzahl der Jobs der letzten 14 Tage.
- SEVEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 7 Tage.
- FOURTEEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Zulässige Werte: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Dieser Parameter stellt die maximale Anzahl der zurückzugebenden Elemente ein.

Der Wert ist eine Ganzzahl. Der Bereich der akzeptierten Werte liegt zwischen 1 und 500.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Zu den akzeptierten Zeichenfolgen gehören beispielsweise `AccessDenied`, `Success` und `InvalidParameters`. Eine Liste der akzeptierten MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

ResourceType

Gibt die Anzahl der Aufträge für den angegebenen Ressourcentyp zurück. Verwenden Sie Anfrage `GetSupportedResourceTypes`, um Zeichenfolgen für unterstützte Ressourcentypen abzurufen.

Der Wert ANY gibt die Anzahl aller Ressourcentypen zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Ressourcentypen und gibt die Summe zurück.

Der Typ der AWS Ressource, die gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Dieser Parameter gibt die Anzahl der Aufträge mit dem angegebenen Zustand zurück.

Der Wert ANY gibt die Anzahl aller Zustände zurück.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge für alle Zustände und gibt die Summe zurück.

Zulässige Werte: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- `ONE_DAY`- Die tägliche Anzahl der Jobs der letzten 14 Tage.
- `SEVEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 7 Tage.
- `FOURTEEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Typ: Zeichenfolge

CopyJobSummaries

Diese Rückgabe enthält eine Zusammenfassung, die Region, Konto, Bundesland,, ResourceType, MessageCategory StartTime EndTime, und die Anzahl der enthaltenen Jobs enthält.

Typ: Array von CopyJobSummary-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListFrameworks

Service: AWS Backup

Gibt eine Liste aller Frameworks für ein AWS-Konto und zurück AWS-Region.

Anforderungssyntax

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die Anzahl der gewünschten Ergebnisse liegt zwischen 1 und 1 000. Optional. Falls nicht angegeben, gibt die Abfrage 1 MB an Daten zurück.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
         "FrameworkName": "string",
```

```
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Frameworks

Die Frameworks mit Details für jedes Framework, einschließlich des Framework-Namens, des Amazon-Ressourcennamens (ARN), der Beschreibung, der Anzahl der Kontrollen, der Erstellungszeit und des Bereitstellungsstatus.

Typ: Array von Framework-Objekten

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListLegalHolds

Service: AWS Backup

Diese Aktion gibt Metadaten zu aktiven und früheren gesetzlichen Aufbewahrungsfristen zurück.

Anforderungssyntax

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente der Ressourcenliste.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

LegalHolds

Dabei handelt es sich um eine Reihe zurückgegebener gesetzlicher Aufbewahrungsfristen, sowohl aktive als auch vorherige.

Typ: Array von LegalHold-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListProtectedResources

Service: AWS Backup

Gibt eine Reihe von Ressourcen zurück AWS Backup, von denen erfolgreich gesichert wurde, einschließlich der Zeit, zu der die Ressource gespeichert wurde, eines Amazon-Ressourcennamens (ARN) der Ressource und eines Ressourcentyps.

Anforderungssyntax

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
```

```
            "LastBackupTime": number,
            "LastBackupVaultArn": "string",
            "LastRecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Results

Eine Reihe von Ressourcen, die erfolgreich gesichert wurden, AWS Backup einschließlich des Zeitpunkts, zu dem die Ressource gespeichert wurde, eines Amazon-Ressourcennamens (ARN) der Ressource und eines Ressourcentyps.

Typ: Array von ProtectedResource-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListProtectedResourcesByBackupVault

Service: AWS Backup

Diese Anfrage listet die geschützten Ressourcen auf, die jedem Backup-Tresor entsprechen.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

BackupVaultAccountId

Die Liste der durch Backup-Tresor geschützten Ressourcen innerhalb des/der Tresore (s), die Sie anhand der Konto-ID angeben.

Pattern: `^[0-9]{12}$`

backupVaultName

Die Liste der durch Backup-Tresor geschützten Ressourcen innerhalb des/der Tresore (s), die Sie nach Namen angeben.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Results

Dies sind die Ergebnisse, die für die Anfrage zurückgegeben wurden ListProtectedResourcesByBackupVault.

Typ: Array von ProtectedResource-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRecoveryPointsByBackupVault

Service: AWS Backup

Gibt detaillierte Informationen zu den Wiederherstellungspunkten zurück, die in einem Backup-Tresor gespeichert sind.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

[BackupVaultAccountId]

Dieser Parameter sortiert die Liste der Wiederherstellungspunkte nach Konto-ID.

Pattern: `^[0-9]{12}$`

[backupVaultName]

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

> **Note**
>
> Der Name des Backup-Tresors ist möglicherweise nicht verfügbar, wenn ein unterstützter Service das Backup erstellt.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

[ByBackupPlanId]

Gibt nur Wiederherstellungspunkte zurück, die der angegebenen Backup-Plan-ID entsprechen.

ByCreatedAfter

Gibt nur Wiederherstellungspunkte zurück, die nach dem angegebenen Zeitstempel erstellt wurden.

ByCreatedBefore

Gibt nur Wiederherstellungspunkte zurück, die vor dem angegebenen Zeitstempel erstellt wurden.

ByParentRecoveryPointArn

Dadurch werden nur Wiederherstellungspunkte zurückgegeben, die dem angegebenen übergeordneten (zusammengesetzten) Wiederherstellungspunkt Amazon-Ressourcenname (ARN) entsprechen.

ByResourceArn

Gibt nur Wiederherstellungspunkte zurück, die mit dem Amazon-Ressourcennamen (ARN) der angegebenen Ressource übereinstimmen.

ByResourceType

Gibt nur Wiederherstellungspunkte zurück, die mit dem/den angegebenen Ressourcentyp(en) übereinstimmen:

- `Aurora` für Amazon Aurora
- `CloudFormation`für AWS CloudFormation
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)
- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store
- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System
- `FSx` für Amazon FSx
- `Neptune` für Amazon Neptune
- `Redshift` für Amazon Redshift
- `RDS` für Amazon Relational Database Service
- `SAP HANA on Amazon EC2` für SAP-HANA-Datenbanken
- `Storage Gateway`für AWS Storage Gateway
- `S3` für Amazon S3
- `Timestream` für Amazon Timestream

- `VirtualMachine` für virtuelle Maschinen

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RecoveryPoints

Eine Reihe von Objekten, die detaillierte Informationen zu Wiederherstellungspunkten enthalten, die in einem Backup-Tresor gespeichert sind.

Typ: Array von RecoveryPointByBackupVault-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRecoveryPointsByLegalHold

Service: AWS Backup

Diese Aktion gibt Wiederherstellungspunkt-ARNs (Amazon Resource Name) der angegebenen gesetzlichen Aufbewahrungsfrist zurück.

Anforderungssyntax

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

legalHoldId

Die ID der gesetzlich vorgeschriebenen Sperre.

Erforderlich: Ja

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente der Ressourcenliste.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen.

Typ: Zeichenfolge

RecoveryPoints

Die Wiederherstellungspunkte.

Typ: Array von RecoveryPointMember-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRecoveryPointsByResource

Service: AWS Backup

Die Informationen über die Wiederherstellungspunkte des Typs, der durch den Amazon Resource Name (ARN) einer Ressource angegeben wird.

> **Note**
>
> Für Amazon EFS und Amazon EC2 listet diese Aktion nur Wiederherstellungspunkte auf, die von AWS Backup erstellt wurden.

Anforderungssyntax

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

[ManagedByAWSBackupOnly](#)

Dieses Attribut filtert Wiederherstellungspunkte auf der Grundlage des Besitzes.

Wenn dies auf gesetzt ist`TRUE`, enthält die Antwort Wiederherstellungspunkte, die den ausgewählten Ressourcen zugeordnet sind und von verwaltet werden AWS Backup.

Wenn dieser Wert auf gesetzt ist`FALSE`, enthält die Antwort alle Wiederherstellungspunkte, die der ausgewählten Ressource zugeordnet sind.

Typ: Boolesch

[MaxResults](#)

Die maximale Anzahl der zurückzugebenden Elemente.

> **Note**
>
> Amazon RDS erfordert einen Wert von mindestens 20.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

resourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RecoveryPoints

Eine Reihe von Objekten, die detaillierte Informationen zu Wiederherstellungspunkten des angegebenen Ressourcentyps enthalten.

> **Note**
>
> Nur Amazon EFS- und Amazon EC2 EC2-Wiederherstellungspunkte kehren zurück BackupVaultName.

Typ: Array von RecoveryPointByResource-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListReportJobs

Service: AWS Backup

Gibt Details zu Ihren Berichtsaufträgen zurück.

Anforderungssyntax

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByCreationAfter

Gibt nur Berichtsaufträge zurück, die nach dem Datum und die Uhrzeit erstellt wurden, angegeben im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert 1516925490 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30 Uhr.

ByCreationBefore

Gibt nur Berichtsaufträge zurück, die vor dem Datum und die Uhrzeit erstellt wurden, angegeben im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert 1516925490 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30 Uhr.

ByReportPlanName

Gibt nur Berichtsaufträge mit dem angegebenen Berichtsplannamen zurück.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Gibt nur Berichtsaufträge zurück, die sich im angegebenen Status befinden. Die Status sind:

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

Die Anzahl der gewünschten Ergebnisse liegt zwischen 1 und 1 000. Optional. Falls nicht angegeben, gibt die Abfrage 1 MB an Daten zurück.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Typ: Zeichenfolge

ReportJobs

Details zu Ihren Berichtsjobs im JSON-Format.

Typ: Array von ReportJob-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListReportPlans

Service: AWS Backup

Gibt eine Liste Ihrer Berichtspläne zurück. Ausführliche Informationen zu einem einzelnen Berichtsplan finden Sie unter `DescribeReportPlan`.

Anforderungssyntax

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die Anzahl der gewünschten Ergebnisse liegt zwischen 1 und 1 000. Optional. Falls nicht angegeben, gibt die Abfrage 1 MB an Daten zurück.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
         }
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Ein Bezeichner, der beim vorherigen Aufruf dieses Vorgangs zurückgegeben wurde und mit dem der nächste Satz von Elementen in der Liste zurückgegeben werden kann.

Typ: Zeichenfolge

ReportPlans

Der Bericht enthält Pläne mit detaillierten Informationen für jeden Plan. Diese Informationen umfassen den Amazon-Ressourcennamen (ARN), den Namen des Berichtsplans, die Beschreibung, die Einstellungen, den Übermittlungskanal, den Bereitstellungsstatus, die Erstellungszeit sowie die letzten Male, die versucht wurde, den Berichtsplan auszuführen bzw. bei denen er erfolgreich ausgeführt wurde.

Typ: Array von ReportPlan-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRestoreJobs

Service: AWS Backup

Gibt eine Liste der Jobs zurück, die zur Wiederherstellung einer gespeicherten Ressource AWS Backup initiiert wurden, einschließlich Details zum Wiederherstellungsprozess.

Anforderungssyntax

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByAccountId

Die Konto-ID, von der die Aufträge aufgelistet werden sollen. Gibt nur Wiederherstellungsaufträge zurück, die der angegebenen Konto-ID zugeordnet sind.

Pattern: `^[0-9]{12}$`

ByCompleteAfter

Gibt nur Kopieraufträge zurück, die nach einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCompleteBefore

Gibt nur Kopieraufträge zurück, die vor einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

ByCreatedAfter

Gibt nur Wiederherstellungsaufträge zurück, die nach dem angegebenen Datum erstellt wurden.

ByCreatedBefore

Gibt nur Wiederherstellungsaufträge zurück, die vor dem angegebenen Datum erstellt wurden.

ByResourceType

Fügen Sie diesen Parameter ein, um nur Wiederherstellungsaufträge für die angegebenen Ressourcen zurückzugeben:

- `Aurora` für Amazon Aurora
- `CloudFormation`für AWS CloudFormation
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)
- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store
- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System
- `FSx` für Amazon FSx
- `Neptune` für Amazon Neptune
- `Redshift` für Amazon Redshift
- `RDS` für Amazon Relational Database Service
- `SAP HANA on Amazon EC2` für SAP-HANA-Datenbanken
- `Storage Gateway`für AWS Storage Gateway
- `S3` für Amazon S3
- `Timestream` für Amazon Timestream
- `VirtualMachine` für virtuelle Maschinen

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Gibt nur Wiederherstellungstestaufträge zurück, die mit dem Amazon-Ressourcennamen (ARN) der angegebenen Ressource übereinstimmen.

ByStatus

Gibt nur Wiederherstellungsaufträge zurück, die dem angegebenen Auftragsstatus zugeordnet sind.

Zulässige Werte: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
      }
   ]
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RestoreJobs

Eine Reihe von Objekten, die detaillierte Informationen zu Aufträgen zur Wiederherstellung gespeicherter Ressourcen enthalten.

Typ: Array von RestoreJobsListMember-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRestoreJobsByProtectedResource

Service: AWS Backup

Dadurch werden Wiederherstellungsaufträge zurückgegeben, die die angegebene geschützte Ressource enthalten.

Sie müssen `ResourceArn` einschließen. Sie können optional `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` und `ByRecoveryPointCreationDateBefore` einschließen.

Anforderungssyntax

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ByRecoveryPointCreationDateAfter

Gibt nur Wiederherstellungsaufträge von Wiederherstellungspunkten zurück, die nach dem angegebenen Datum erstellt wurden.

ByRecoveryPointCreationDateBefore

Gibt nur Wiederherstellungsaufträge von Wiederherstellungspunkten zurück, die vor dem angegebenen Datum erstellt wurden.

ByStatus

Gibt nur Wiederherstellungsaufträge zurück, die dem angegebenen Auftragsstatus zugeordnet sind.

Zulässige Werte: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

resourceArn

Gibt nur Wiederherstellungsaufträge zurück, die mit dem Amazon-Ressourcennamen (ARN) der angegebenen Ressource übereinstimmen.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
        }
    ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RestoreJobs

Eine Reihe von Objekten, die detaillierte Informationen zu Aufträgen zur Wiederherstellung gespeicherter Ressourcen enthalten.>

Typ: Array von RestoreJobsListMember-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRestoreJobSummaries

Service: AWS Backup

Diese Anforderung ruft eine Liste der Wiederherstellungsaufträge ab, die in den letzten 30 Tagen erstellt oder ausgeführt wurden. Sie können die Parameter AccountID, State,, ResourceType, oder angeben AggregationPeriod MaxResults, um Ergebnisse NextToken zu filtern.

Diese Anfrage gibt eine Zusammenfassung zurück, die Region, Account, State, RestourceType, MessageCategory, StartTime EndTime, und Anzahl der enthaltenen Jobs enthält.

Anforderungssyntax

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

AccountId

Gibt die Anzahl der Aufträge für das angegebene Konto zurück.

Wenn die Anfrage von einem Mitgliedskonto oder einem Konto gesendet wird, das nicht Teil von AWS Organizations ist, werden Jobs innerhalb des Kontos des Anfragenden zurückgegeben.

Root-, Admin- und delegierte Administratorkonten können den Wert ANY verwenden, um die Anzahl der Aufträge von jedem Konto in der Organisation zurückzugeben.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge aller Konten innerhalb der authentifizierten Organisation und gibt dann die Summe zurück.

Pattern: `^[0-9]{12}$`

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- ONE_DAY- Die tägliche Anzahl der Jobs der letzten 14 Tage.
- SEVEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 7 Tage.

- FOURTEEN_DAYS- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Zulässige Werte: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Dieser Parameter stellt die maximale Anzahl der zurückzugebenden Elemente ein.

Der Wert ist eine Ganzzahl. Der Bereich der akzeptierten Werte liegt zwischen 1 und 500.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der MaxResults Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen NextToken, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

ResourceType

Gibt die Anzahl der Aufträge für den angegebenen Ressourcentyp zurück. Verwenden Sie Anfrage GetSupportedResourceTypes, um Zeichenfolgen für unterstützte Ressourcentypen abzurufen.

Der Wert ANY gibt die Anzahl aller Ressourcentypen zurück.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge für alle Ressourcentypen und gibt die Summe zurück.

Der Typ der AWS Ressource, die gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

State

Dieser Parameter gibt die Anzahl der Aufträge mit dem angegebenen Zustand zurück.

Der Wert ANY gibt die Anzahl aller Zustände zurück.

AGGREGATE_ALL aggregiert die Anzahl der Aufträge für alle Zustände und gibt die Summe zurück.

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- `ONE_DAY`- Die tägliche Anzahl der Jobs der letzten 14 Tage.
- `SEVEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 7 Tage.
- `FOURTEEN_DAYS`- Die aggregierte Anzahl der Jobs der letzten 14 Tage.

Typ: Zeichenfolge

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RestoreJobSummaries

Diese Rückgabe enthält eine Zusammenfassung, die Region, Konto, Bundesland,, ResourceType, MessageCategory StartTime EndTime, und die Anzahl der enthaltenen Jobs enthält.

Typ: Array von RestoreJobSummary-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRestoreTestingPlans

Service: AWS Backup

Gibt eine Liste der Wiederherstellungstestpläne zurück.

Anforderungssyntax

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
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
        }
    ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RestoreTestingPlans

Dies ist eine zurückgegebene Liste von Wiederherstellungstestplänen.

Typ: Array von RestoreTestingPlanForList-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListRestoreTestingSelections

Service: AWS Backup

Gibt eine Liste der Auswahlen für Wiederherstellungstests zurück. Kann nach `MaxResults` und `RestoreTestingPlanName` gefiltert werden.

Anforderungssyntax

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

RestoreTestingPlanName

Gibt die Wiederherstellungstest-Auswahlen nach dem angegebenen Namen des Wiederherstellungstestplans zurück.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

RestoreTestingSelections

Die zurückgegebenen Wiederherstellungstest-Auswahlen, die dem Wiederherstellungstestplan zugeordnet sind.

Typ: Array von RestoreTestingSelectionForList-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListTags

Service: AWS Backup

Gibt die der Ressource zugewiesenen Tags zurück, z. B. einen Zielwiederherstellungspunkt, einen Backup-Plan oder einen Backup-Tresor.

`ListTags` funktioniert nur für Ressourcentypen, die die vollständige AWS Backup -Verwaltung ihrer Backups unterstützen. Diese Ressourcentypen sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt.

Anforderungssyntax

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

resourceArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab. Gültige Ziele für `ListTags` sind Wiederherstellungspunkte, Backup-Pläne und Backup-Tresore.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Elemente. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Elementen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Tags

Informationen zu den Tags.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutBackupVaultAccessPolicy

Service: AWS Backup

Legt eine ressourcenbasierte Richtlinie fest, die zur Verwaltung von Zugriffsberechtigungen für den Ziel-Backup-Tresor verwendet wird. Erfordert einen Namen für den Backup-Tresor und ein Dokument mit einer Zugriffsrichtlinie im JSON-Format.

Anforderungssyntax

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Policy

Das Dokument mit der Zugriffsrichtlinie für den Backup-Tresor im JSON-Format.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutBackupVaultLockConfiguration

Service: AWS Backup

Wendet AWS Backup Vault Lock auf einen Backup-Tresor an und verhindert so Versuche, in einem Backup-Tresor gespeicherte oder in einem Backup-Tresor erstellte Wiederherstellungspunkte zu löschen. Vault Lock verhindert auch Versuche, die Lebenszyklusrichtlinie zu aktualisieren, die die Aufbewahrungsdauer aller derzeit in einem Backup-Tresor gespeicherten Wiederherstellungspunkte steuert. Falls angegeben, erzwingt Vault Lock eine minimale und maximale Aufbewahrungsdauer für zukünftige Sicherungs- und Kopieraufträge, die auf einen Backup-Tresor abzielen.

> **Note**
>
> AWS Backup Vault Lock wurde von Cohasset Associates für den Einsatz in Umgebungen bewertet, die den Bestimmungen von SEC 17a-4, CFTC und FINRA unterliegen. Weitere Informationen darüber, wie AWS Backup Vault Lock mit diesen Vorschriften zusammenhängt, finden Sie in der Compliance-Bewertung von Cohasset Associates.

Weitere Informationen finden Sie unter AWS Backup Vault Lock.

Anforderungssyntax

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Die AWS Backup Vault Lock-Konfiguration, die den Namen des Backup-Tresors angibt, den es schützt.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ChangeableForDays

Die AWS Backup Vault Lock-Konfiguration, die die Anzahl der Tage vor dem Sperrdatum angibt. Zum Beispiel, wenn Sie am 1. Januar 2022 um 20 Uhr UTC `ChangeableForDays` auf 30 stellen, wird das Sperrdatum auf den 31. Januar 2022 um 20 Uhr UTC gesetzt.

AWS Backup erzwingt eine Bedenkzeit von 72 Stunden, bevor Vault Lock wirksam wird und unveränderlich wird. Deshalb müssen Sie `ChangeableForDays` auf 3 oder höher festlegen.

Vor dem Sperrdatum können Sie Vault Lock mithilfe von `DeleteBackupVaultLockConfiguration` löschen, oder Sie ändern die Vault-Lock-Konfiguration mit `PutBackupVaultLockConfiguration`. Am und nach dem Sperrdatum wird die Vault-Sperre unveränderlich und kann weder geändert noch gelöscht werden.

Wenn dieser Parameter nicht angegeben wird, können Sie jederzeit Vault Lock mithilfe von `DeleteBackupVaultLockConfiguration` löschen, oder Sie ändern die Vault-Lock-Konfiguration mit `PutBackupVaultLockConfiguration`.

Type: Long

Erforderlich: Nein

MaxRetentionDays

Die AWS Backup Vault Lock-Konfiguration, die den maximalen Aufbewahrungszeitraum festlegt, für den der Tresor seine Wiederherstellungspunkte beibehält. Diese Einstellung kann beispielsweise nützlich sein, wenn die Richtlinien Ihrer Organisation verlangen, dass Sie bestimmte Daten löschen, nachdem Sie sie vier Jahre (1460 Tage) aufbewahrt haben.

Wenn dieser Parameter nicht enthalten ist, erzwingt Vault Lock keine maximale Aufbewahrungsdauer für die Wiederherstellungspunkte im Tresor. Wenn dieser Parameter ohne Wert enthalten ist, erzwingt Vault Lock keine maximale Aufbewahrungsdauer.

Wenn dieser Parameter angegeben wird, muss jeder Sicherungs- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der maximalen Aufbewahrungsdauer entspricht oder kürzer ist. Wenn die Aufbewahrungsdauer des Auftrags länger als die maximale Aufbewahrungsdauer ist, schlägt der Tresor den Backup- oder Kopierauftrag fehl, und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden. Die längste maximale Aufbewahrungsdauer, die Sie angeben können, beträgt 36 500 Tage (ungefähr 100 Jahre). Wiederherstellungspunkte, die bereits vor Vault Lock im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

Erforderlich: Nein

MinRetentionDays

Die AWS Backup Vault Lock-Konfiguration, die den Mindestaufbewahrungszeitraum festlegt, für den der Tresor seine Wiederherstellungspunkte beibehält. Diese Einstellung kann beispielsweise nützlich sein, wenn die Richtlinien Ihrer Organisation vorschreiben, dass Sie bestimmte Daten mindestens sieben Jahre (2555 Tage) beibehalten müssen.

Dieser Parameter ist erforderlich, wenn eine Tresorsperre erstellt wird. AWS CloudFormation Andernfalls ist dieser Parameter optional. Wenn dieser Parameter nicht angegeben wird, erzwingt Vault Lock keine Mindestaufbewahrungsdauer.

Wenn dieser Parameter angegeben wird, muss jeder Sicherungs- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der minimalen Aufbewahrungsdauer entspricht oder länger ist. Wenn die Aufbewahrungsfrist des Auftrags länger als die maximale Aufbewahrungsdauer ist, schlägt der Tresor den Backup- oder Kopierauftrag fehl, und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden. Die kürzeste Mindestaufbewahrungsdauer, die Sie angeben können, ist 1 Tag. Wiederherstellungspunkte, die bereits vor Vault Lock im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutBackupVaultNotifications

Service: AWS Backup

Aktiviert Benachrichtigungen auf einem Backup-Tresor für das angegebene Thema und die angegebenen Ereignisse.

Anforderungssyntax

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupVaultEvents

Ein Array von Ereignissen, die den Status der Aufträge zur Sicherung von Ressourcen im Sicherungstresor angeben.

Allgemeine Anwendungsfälle und Codebeispiele finden Sie unter AWS Backup Ereignisse mit Amazon SNS verfolgen.

Folgende Ereignisse werden unterstützt:

- `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**
>
> Die folgende Liste enthält sowohl unterstützte Ereignisse als auch veraltete Ereignisse, die nicht mehr verwendet werden (als Referenz). Veraltete Ereignisse geben keine Statusmeldungen oder Benachrichtigungen zurück. Die unterstützten Ereignisse finden Sie in der obigen Liste.

Typ: Zeichenfolgen-Array

Zulässige Werte: `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`

Erforderlich: Ja

SNSTopicArn

Der Amazon-Ressourcenname (ARN), der das Thema für die Ereignisse eines Backup-Tresors angibt, z. B. `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Typ: Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutRestoreValidationResult

Service: AWS Backup

Diese Anforderung ermöglicht Ihnen, Ihre unabhängigen Validierungsergebnisse für den selbst ausgeführten Wiederherstellungstest zu senden. `RestoreJobId` und `ValidationStatus` sind erforderlich. Optional können Sie eine `ValidationStatusMessage` eingeben.

Anforderungssyntax

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

restoreJobId

Dies ist eine eindeutige Kennung eines darin enthaltenen Wiederherstellungsauftrags AWS Backup.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ValidationStatus

Der Status Ihrer Wiederherstellungsvalidierung.

Typ: Zeichenfolge

Zulässige Werte: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Erforderlich: Ja

ValidationStatusMessage

Dies ist eine optionale Nachrichtenzeichenfolge, die Sie eingeben können, um den Validierungsstatus für die Validierung des Wiederherstellungstests zu beschreiben.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 204
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartBackupJob

Service: AWS Backup

Startet einen On-Demand-Backup-Auftrag für die angegebene Ressource

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupOptions

Die Backup-Option für eine ausgewählte Ressource. Diese Option ist nur für Windows-VSS-Backup-Aufträge (Volume Shadow Copy Service) verfügbar.

Gültige Werte: Stellen Sie diese Option auf `"WindowsVSS":"enabled"` ein, um die `WindowsVSS`-Backup-Option zu aktivieren und ein Windows VSS-Backup zu erstellen. Stellen Sie sie auf `"WindowsVSS""disabled"` ein, um ein reguläres Backup zu erstellen. Die Option `WindowsVSS` ist standardmäßig aktiviert.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wertemuster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

CompleteWindowMinutes

Ein Wert in Minuten, in dem ein erfolgreich gestartetes Backup abgeschlossen werden muss, andernfalls bricht AWS Backup den Auftrag ab. Dieser Wert ist optional. Dieser Wert beginnt mit dem Countdown ab dem Zeitpunkt, zu dem das Backup geplant wurde. Es wird keine zusätzliche Zeit für `StartWindowMinutes` hinzugefügt, oder wenn das Backup später als geplant gestartet wurde.

Wie `StartWindowMinutes` hat dieser Parameter hat einen maximalen Wert von 100 Jahren (52.560.000 Minuten).

Type: Long

Erforderlich: Nein

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `StartBackupJob` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch und läuft entsprechend dem von Ihnen definierten Lebenszyklus ab.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Der Höchstwert für diesen Parameter ist 100 Jahre (36.500 Tage).

Typ: Lifecycle Objekt

Erforderlich: Nein

RecoveryPointTags

Die Tags, die den Ressourcen zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ResourceArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Ja

StartWindowMinutes

Ein Wert in Minuten, nachdem ein Backup geplant ist, bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional und der Standardwert beträgt 8 Stunden. Wenn dieser Wert enthalten ist, muss er mindestens 60 Minuten betragen, um Fehler zu vermeiden.

Dieser Parameter hat einen maximalen Wert von 100 Jahren (52.560.000 Minuten).

Während des Startfensters bleibt der Status des Backup-Auftrags so lange im `CREATED`-Status, bis er erfolgreich gestartet wurde oder bis die Startfensterzeit abgelaufen ist. Wenn Time innerhalb des Startfensters einen Fehler AWS Backup erhält, der einen erneuten Versuch ermöglicht, den Job erneut zu starten, AWS Backup wird automatisch mindestens alle 10 Minuten erneut versucht, den Job zu starten, bis die Sicherung erfolgreich gestartet wird (der Jobstatus ändert sich auf`RUNNING`) oder bis sich der Jobstatus auf ändert `EXPIRED` (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Type: Long

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupJobId

Identifiziert eindeutig eine Anforderung AWS Backup zur Sicherung einer Ressource.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Auftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

IsParent

Dies ist ein zurückgegebener boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Backup-Auftrag handelt.

Typ: Boolesch

RecoveryPointArn

Hinweis: Dieses Feld wird nur für Amazon-EFS- und Advanced-DynamoDB-Ressourcen zurückgegeben.

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartCopyJob

Service: AWS Backup

Startet einen Auftrag zum Erstellen einer einmaligen Kopie der angegebenen Ressource.

Unterstützt keine kontinuierlichen Backups.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

DestinationBackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Ziel-Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Ja

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Kopieren des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `StartCopyJob` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Lifecycle

Gibt den Zeitraum in Tagen an, bevor ein Recovery Point in den Cold Storage übergeht oder gelöscht wird.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Aufbewahrungseinstellung auf der Konsole um 90 Tage höher sein als die Einstellung für den Übergang zur Einstellung „Kalt nach Tagen“. Die Einstellung für den Übergang zu „kalt nach Tagen“ kann nicht geändert werden, nachdem ein Backup auf „kalt“ umgestellt wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Um den bestehenden Lebenszyklus und die Aufbewahrungsfristen zu entfernen und Ihre Wiederherstellungspunkte unbegrenzt beizubehalten, geben Sie -1 für `MoveToColdStorageAfterDays` und an. `DeleteAfterDays`

Typ: Lifecycle Objekt

Erforderlich: Nein

RecoveryPointArn

Ein ARN, der einen für den Kopierauftrag zu verwendenden Wiederherstellungspunkt eindeutig identifiziert, z. B. arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Typ: Zeichenfolge

Erforderlich: Ja

SourceBackupVaultName

Der Name eines logischen Quellcontainers, in dem die Backups gespeichert werden. Backup-Tresore werden anhand von Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und für die AWS Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CopyJobId

Identifiziert einen Kopierauftrag eindeutig.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Kopierauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

IsParent

Dies ist ein zurückgegebener boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Kopierauftrag handelt.

Typ: Boolesch

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartReportJob

Service: AWS Backup

Startet einen On-Demand-Berichtsauftrag für den angegebenen Berichtsplan.

Anforderungssyntax

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

reportPlanName

Der eindeutige Name eines Berichtsplans.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `StartReportJobInput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ReportJobId

Der Bezeichner des Berichtsauftrags. Eine eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolge, die maximal 1 024 Byte lang ist. Die Berichtsauftrags-ID kann nicht bearbeitet werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartRestoreJob

Service: AWS Backup

Stellt die gespeicherte Ressource wieder her, die durch einen Amazon-Ressourcennamen (ARN) identifiziert wurde.

Anforderungssyntax

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

CopySourceTagsToRestoredResource

Dieser Parameter ist optional. Entspricht dies `True`, werden die im Backup enthaltenen Tags in die wiederhergestellte Ressource kopiert.

Dies kann nur auf Backups angewendet werden, die durch erstellt wurden AWS Backup.

Typ: Boolesch

Erforderlich: Nein

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, mit der AWS Backup die Zielressource erstellt wird; zum Beispiel:`arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `StartRestoreJob` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Metadata

Eine Satz von Metadaten-Schlüssel-Wert-Paaren.

Sie können Konfigurationsmetadaten zu einer Ressource zum Zeitpunkt des Backups abrufen, indem Sie `GetRecoveryPointRestoreMetadata` aufrufen. Für die Wiederherstellung einer Ressource sind jedoch möglicherweise zusätzlich zu den von `GetRecoveryPointRestoreMetadata` bereitgestellten Werten weitere Werte erforderlich. Sie müssen beispielsweise möglicherweise einen neuen Ressourcennamen angeben, wenn das Original bereits vorhanden ist.

Weitere Informationen zu den Metadaten für jede Ressource finden Sie im Folgenden:

- Metadaten für Amazon Aurora
- Metadaten für Amazon DocumentDB
- Metadaten für AWS CloudFormation
- Metadaten für Amazon DynamoDB
- Metadaten für Amazon EBS
- Metadaten für Amazon EC2
- Metadaten für Amazon EFS
- Metadaten für Amazon FSx

- Metadaten für Amazon Neptune
- Metadaten für Amazon RDS
- Metadaten für Amazon Redshift
- Metadaten für AWS Storage Gateway
- Metadaten für Amazon S3
- Metadaten für Amazon Timestream
- Metadaten für virtuelle Maschinen

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Ja

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Ja

ResourceType

Startet einen Auftrag zur Wiederherstellung eines Wiederherstellungspunkts für eine der folgenden Ressourcen:

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Amazon Elastic Block Store
- `EC2`- Amazon Elastic Compute Cloud
- `EFS`- Amazon Elastic File System
- `FSx`- Amazon FSx
- `Neptune`- Amazon Neptune
- `RDS`- Amazon Relational Database Service
- `Redshift`- Amazon Redshift
- `Storage Gateway` - AWS Storage Gateway

- `S3`- Amazon Simple Storage Service
- `Timestream`- Amazon Timestream
- `VirtualMachine`- Virtuelle Maschinen

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

RestoreJobId

Identifiziert den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StopBackupJob

Service: AWS Backup

Versucht, einen Auftrag abzubrechen, um ein einmaliges Backup einer Ressource zu erstellen.

Diese Aktion wird für die folgenden Dienste nicht unterstützt: Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon FSx für NetApp ONTAP, Amazon FSx für OpenZFS, Amazon DocumentDB (mit MongoDB-Kompatibilität), Amazon RDS, Amazon Aurora und Amazon Neptune.

Anforderungssyntax

```
POST /backup-jobs/backupJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupJobId

Identifiziert eindeutig eine Anfrage zur Sicherung einer Ressource. AWS Backup

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

TagResource

Service: AWS Backup

Weist einem durch einen Amazon-Ressourcennamen (ARN) identifizierten Wiederherstellungspunkt, Backup-Plan oder Backup-Tresor eine Reihe von Schlüssel-Wert-Paaren zu.

Diese API wird für Wiederherstellungspunkte für Ressourcentypen wie Aurora und Amazon DocumentDB unterstützt. Amazon EBS, Amazon FSx, Neptune und Amazon RDS.

Anforderungssyntax

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

resourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format des ARN hängt vom Typ der markierten Ressource ab.

ARNs, die nicht enthalten sind, sind mit Tagging nicht kompatibel`backup`. `TagResource`und `UntagResource` mit ungültigen ARNs führt dies zu einem Fehler. Zulässige ARN-Inhalte können Folgendes beinhalten: `arn:aws:backup:us-east` Ungültiger ARN-Inhalt könnte so aussehen`arn:aws:ec2:us-east`.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Tags

Schlüssel-Wert-Paare, die verwendet werden, um Ihre Ressourcen zu organisieren. Sie können Ihre eigenen Metadaten den Ressourcen zuweisen, die Sie erstellen. Der Übersichtlichkeit halber ist dies die Struktur für die Zuweisung von Tags:`[{"Key":"string","Value":"string"}]`.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UntagResource

Service: AWS Backup

Entfernt eine Reihe von Schlüssel-Wert-Paaren aus einem durch einen Amazon-Ressourcennamen (ARN) identifizierten Wiederherstellungspunkt, Backup-Plan oder Backup-Tresor.

Diese API wird für Wiederherstellungspunkte für Ressourcentypen wie Aurora und Amazon DocumentDB nicht unterstützt. Amazon EBS, Amazon FSx, Neptune und Amazon RDS.

Anforderungssyntax

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

resourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format des ARN hängt vom Typ der markierten Ressource ab.

ARNs, die nicht enthalten sind, sind mit Tagging nicht kompatibel`backup`. `TagResource`und `UntagResource` mit ungültigen ARNs führt dies zu einem Fehler. Zulässige ARN-Inhalte können Folgendes beinhalten: `arn:aws:backup:us-east` Ungültiger ARN-Inhalt könnte so aussehen`arn:aws:ec2:us-east`.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

TagKeyList

Die Schlüssel zur Identifizierung der Schlüssel-Wert-Tags, die aus einer Ressource entfernt werden sollen.

Typ: Zeichenfolgen-Array

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateBackupPlan

Service: AWS Backup

Aktualisiert den angegebenen Backup-Plan. Die neue Version wird anhand ihrer ID eindeutig identifiziert.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Die ID des Backup-Plans.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupPlan

Der Hauptteil eines Backup-Plans. Beinhaltet einen `BackupPlanName` und einen oder mehrere Sätze von `Rules`.

Typ: BackupPlanInput Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
```

```
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "CreationDate": number,
      "VersionId": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AdvancedBackupSettings

Enthält eine Liste von `BackupOptions` für jeden Ressourcentyp.

Typ: Array von AdvancedBackupSetting-Objekten

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Versions-IDs können nicht bearbeitet werden.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateFramework

Service: AWS Backup

Aktualisiert das angegebene Framework.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

frameworkName

Der eindeutige Name eines Frameworks. Dieser Name hat eine Länge von maximal 256 Zeichen, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

FrameworkControls

Die Steuerelemente, aus denen das Framework besteht. Jedes Steuerelement in der Liste hat einen Namen, Eingabeparameter und einen Bereich.

Typ: Array von FrameworkControl-Objekten

Erforderlich: Nein

FrameworkDescription

Eine optionale Beschreibung des Frameworks mit einer Länge von maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `UpdateFrameworkInput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Das Datum und die Uhrzeit, zu der ein Framework erstellt wurde, in ISO 8601-Darstellung. Der Wert von `CreationTime` ist auf Millisekunden genau. Beispielsweise steht 2020-07-10T 15:00:00.000-08:00 für den 10. Juli 2020 um 15.00 Uhr, UTC minus 8 Stunden.

Typ: Zeitstempel

FrameworkArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

FrameworkName

Der eindeutige Name eines Frameworks. Dieser Name hat eine Länge von maximal 256 Zeichen, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AlreadyExistsException

Die erforderliche Ressource ist bereits vorhanden.

HTTP Status Code: 400

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateGlobalSettings

Service: AWS Backup

Aktualisiert, ob das AWS Konto für die kontoübergreifende Sicherung aktiviert ist. Gibt einen Fehler zurück, wenn es sich bei dem Konto nicht um ein Verwaltungskonto für Organizations handelt. Verwenden Sie die `DescribeGlobalSettings`-API, um die aktuellen Einstellungen zu ermitteln.

Anforderungssyntax

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GlobalSettings

Ein Wert für `isCrossAccountBackupEnabled` und eine Region. Beispiel: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateRecoveryPointLifecycle

Service: AWS Backup

Legt den Übergangslebenszyklus eines Wiederherstellungspunkts fest.

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Kühlspeicher überführt wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Dieser Vorgang unterstützt keine kontinuierlichen Backups.

Anforderungssyntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

recoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage überführt wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Typ: Lifecycle Objekt

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BackupVaultArn

Ein ARN, der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

CalculatedLifecycle

Ein `CalculatedLifecycle`-Objekt, das `DeleteAt`- und `MoveToColdStorageAt`-Zeitstempel enthält.

Typ: CalculatedLifecycle Objekt

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die

Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Typ: Lifecycle Objekt

RecoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateRegionSettings

Service: AWS Backup

Aktualisiert die aktuellen Service-Opt-In-Einstellungen für die Region.

Verwenden Sie die `DescribeRegionSettings`-API, um die unterstützten Ressourcentypen zu ermitteln.

Anforderungssyntax

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ResourceTypeManagementPreference

Aktiviert oder deaktiviert die vollständige AWS Backup Verwaltung von Backups für einen Ressourcentyp. Um die vollständige AWS Backup Verwaltung für DynamoDB zusammen mit AWS Backup den erweiterten DynamoDB-Backup-Funktionen zu aktivieren, gehen Sie wie folgt vor, um erweiterte DynamoDB-Backups programmgesteuert zu aktivieren.

Typ: Zeichenfolge zu boolescher Abbildung

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

ResourceTypeOptInPreference

Aktualisiert die Liste der Services zusammen mit den Opt-in-Einstellungen für die Region.

Wenn Ressourcenzuweisungen nur auf Tags basieren, werden die Service-Opt-In-Einstellungen angewendet. Wenn ein Ressourcentyp explizit einem Backup-Plan wie Amazon S3, Amazon EC2 oder Amazon RDS zugewiesen wird, wird er in das Backup aufgenommen, auch wenn die Anmeldung für diesen bestimmten Service nicht aktiviert ist. Wenn in einer Ressourcenzuweisung sowohl ein Ressourcentyp als auch Tags angegeben sind, hat der im Backup-Plan angegebene Ressourcentyp Vorrang vor der Tag-Bedingung. Die Service-Opt-In-Einstellungen werden in diesem Fall nicht berücksichtigt.

Typ: Zeichenfolge zu boolescher Abbildung

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen SDKs finden Sie im Folgenden: AWS

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateReportPlan

Service: AWS Backup

Aktualisiert den angegebenen Berichtsplan.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

reportPlanName

Der eindeutige Name des Berichtsplans. Dieser Name hat eine Länge von maximal 256 Zeichen, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

IdempotencyToken

Eine vom Kunden gewählte Zeichenfolge, mit der Sie zwischen ansonsten identischen Aufrufen an `UpdateReportPlanInput` unterscheiden können. Der erneute Versuch einer erfolgreichen Anforderung mit demselben Idempotenz-Token führt zu einer Erfolgsmeldung, ohne dass Maßnahmen ergriffen werden.

Typ: Zeichenfolge

Erforderlich: Nein

ReportDeliveryChannel

Die Informationen darüber, wohin Ihre Berichte geliefert werden sollen, insbesondere Ihr Amazon S3 S3-Bucket-Name, Ihr S3-Schlüsselpräfix und die Formate Ihrer Berichte.

Typ: ReportDeliveryChannel Objekt

Erforderlich: Nein

ReportPlanDescription

Eine optionale Beschreibung des Berichtsplans mit maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

ReportSetting

Die Berichtsvorlage für den Bericht. Berichte werden mithilfe einer Berichtsvorlage erstellt. Die Berichtsvorlagen sind:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Wenn die Berichtsvorlage `RESOURCE_COMPLIANCE_REPORT` oder ist`CONTROL_COMPLIANCE_REPORT`, beschreibt diese API-Ressource auch den Berichtsbereich von AWS-Regionen und Frameworks.

Typ: ReportSetting Objekt

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Berichtsplans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

ReportPlanArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

ReportPlanName

Der eindeutige Name des Berichtsplans.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateRestoreTestingPlan

Service: AWS Backup

Diese Anforderung sendet Änderungen an Ihren angegebenen Wiederherstellungstestplan. `RestoreTestingPlanName` kann nach der Erstellung nicht aktualisiert werden.

`RecoveryPointSelection` kann enthalten:

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Der Name des Wiederherstellungstestplans.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

RestoreTestingPlan

Gibt den Hauptteil eines Wiederherstellungstestplans an.

Typ: RestoreTestingPlanForUpdate Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem der Ressourcentestplan erstellt wurde.

Typ: Zeitstempel

RestoreTestingPlanArn

Eindeutiger ARN (Amazon-Ressourcenname) des Wiederherstellungstestplans.

Typ: Zeichenfolge

RestoreTestingPlanName

Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

Typ: Zeichenfolge

UpdateTime

Der Zeitpunkt, zu dem das Update für den Wiederherstellungstestplan abgeschlossen wurde.

Typ: Zeitstempel

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateRestoreTestingSelection

Service: AWS Backup

Aktualisiert die angegebene Auswahl für den Wiederherstellungstest.

Die meisten Elemente außer dem `RestoreTestingSelectionName` können mit dieser Anforderung aktualisiert werden.

Sie können entweder ARNs oder Bedingungen für geschützte Ressourcen verwenden, aber nicht beide.

Anforderungssyntax

```
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-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

RestoreTestingPlanName

Der Name des Wiederherstellungstestplans ist erforderlich, um den angegebenen Testplan zu aktualisieren.

Erforderlich: Ja

RestoreTestingSelectionName

Der Name der erforderlichen Restore-Test-Auswahl der Restore-Test-Auswahl, die Sie aktualisieren möchten.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

RestoreTestingSelection

Um Ihre Auswahl für Wiederherstellungstests zu aktualisieren, können Sie entweder ARNs oder Bedingungen für geschützte Ressourcen verwenden, nicht jedoch beides. Das heißt, wenn Ihre Auswahl den Vorgang `ProtectedResourceArns` durchgeführt hat, wird die Anforderung einer Aktualisierung mit dem Parameter `ProtectedResourceConditions` nicht erfolgreich sein.

Typ: RestoreTestingSelectionForUpdate Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
```

```
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem die Auswahl für den Ressourcentest erfolgreich aktualisiert wurde.

Typ: Zeitstempel

RestoreTestingPlanArn

Eine eindeutige Zeichenfolge, die dem Namen des Wiederherstellungstestplans entspricht.

Typ: Zeichenfolge

RestoreTestingPlanName

Der Wiederherstellungstestplan, dem die aktualisierte Auswahl für den Wiederherstellungstest zugeordnet ist.

Typ: Zeichenfolge

RestoreTestingSelectionName

Der zurückgegebene Name der Auswahl für den Wiederherstellungstest.

Typ: Zeichenfolge

UpdateTime

Der Zeitpunkt, zu dem das Update für die Auswahl der Wiederherstellungstests abgeschlossen wurde.

Typ: Zeitstempel

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

AWS Backup kann die von Ihnen angeforderte Aktion erst ausführen, wenn die Ausführung einer vorherigen Aktion abgeschlossen ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

AWS Backup gateway

Folgende Aktionen werden von AWS Backup gateway unterstützt:

- 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

Service: AWS Backup gateway

Ordnet Ihrem Server ein Backup-Gateway zu. Nachdem Sie den Zuordnungsvorgang abgeschlossen haben, können Sie Ihre VMs über das Gateway sichern und wiederherstellen.

Anforderungssyntax

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den `ListGateways` Vorgang, um eine Liste von Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

ServerArn

Der Amazon-Ressourcenname (ARN) des Servers, der Ihre virtuellen Maschinen hostet.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) eines Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

CreateGateway

Service: AWS Backup gateway

Erstellt ein Backup-Gateway. Nach dem Erstellen eines Gateways können Sie es mit dem `AssociateGatewayToServer`-Vorgang mit einem Server verknüpfen.

Anforderungssyntax

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ActivationKey

Der Aktivierungsschlüssel des erstellten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge = 50 Zeichen.

Pattern: `^[0-9a-zA-Z\-]+$`

Erforderlich: Ja

GatewayDisplayName

Der Anzeigename des erstellten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Ja

GatewayType

Der Typ des erstellten Gateways.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VM`

Erforderlich: Ja

Tags

Eine Liste mit bis zu 50 Tags, die dem Gateway zugeordnet werden können. Jeder Tag ist ein Schlüssel/Wert-Paar.

Typ: Array von Tag-Objekten

Erforderlich: Nein

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des von Ihnen erstellten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3

- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteGateway

Service: AWS Backup gateway

Löscht ein Backup-Gateway.

Anforderungssyntax

```
{
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des zu löschenden Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des von Ihnen gelöschten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteHypervisor

Service: AWS Backup gateway

Löscht einen Hypervisor.

Anforderungssyntax

```
{
   "HypervisorArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des zu löschenden Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "HypervisorArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des von Ihnen gelöschten Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang kann nicht fortgesetzt werden, da Sie nur unzureichende Berechtigungen haben.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DisassociateGatewayFromServer

Service: AWS Backup gateway

Hebt die Zuordnung ein Backup-Gateway vom angegebenen Server auf. Nach Abschluss der Aufhebung der Zuordnung kann das Gateway nicht mehr auf die virtuellen Maschinen auf dem Server zugreifen.

Anforderungssyntax

```
{
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways, dessen Zuordnung aufgehoben werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways, dessen Zuordnung Sie aufgehoben haben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetBandwidthRateLimitSchedule

Service: AWS Backup gateway

Ruft den Zeitplan für das Bandbreitenlimit für ein angegebenes Gateway ab. Standardmäßig haben Gateways keine Zeitpläne für das Bandbreitenlimit, was bedeutet, dass keine Bandbreitenratenbegrenzung wirksam ist. Verwenden Sie dies, um den Zeitplan für das Bandbreitenlimit eines Gateways abzurufen.

Anforderungssyntax

```
{
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den `ListGateways`Vorgang, um eine Liste von Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
```

```
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
         }
      ],
      "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

BandwidthRateLimitIntervals

Ein Array, das Zeitplanintervalle für Bandbreitenratenlimits für ein Gateway enthält. Wenn keine Intervalle für das Bandbreitenlimit geplant wurden, ist das Array leer.

Typ: Array von BandwidthRateLimitInterval-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den `ListGateways`Vorgang, um eine Liste der Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetGateway

Service: AWS Backup gateway

Durch Angabe des ARN (Amazon Resource Name) gibt diese API die virtuelle Maschine zurück.

Anforderungssyntax

```
{
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
```

```
            "DayOfWeek": number,
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Gateway

Durch Angabe des ARN (Amazon Resource Name) gibt diese API die virtuelle Maschine zurück.

Typ: GatewayDetails Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetHypervisor

Service: AWS Backup gateway

Diese Aktion fordert Informationen über den angegebenen Hypervisor an, zu dem das Gateway eine Verbindung herstellen wird. Ein Hypervisor ist Hardware, Software oder Firmware, die virtuelle Maschinen erstellt und verwaltet und ihnen Ressourcen zuweist.

Anforderungssyntax

```
{
   "HypervisorArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
```

```
      "LatestMetadataSyncStatus": "string",
      "LatestMetadataSyncStatusMessage": "string",
      "LogGroupArn": "string",
      "Name": "string",
      "State": "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Hypervisor

Details zum angeforderten Hypervisor

Typ: HypervisorDetails Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetHypervisorPropertyMappings

Service: AWS Backup gateway

Diese Aktion ruft die Eigenschaftszuordnungen für den angegebenen Hypervisor ab. Eine Hypervisor-Eigenschaftenzuordnung zeigt das Verhältnis der Entitätseigenschaften, die auf dem Hypervisor verfügbar sind, zu den in verfügbaren Eigenschaften an. AWS

Anforderungssyntax

```
{
   "HypervisorArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
```

```
            "AwsTagValue": "string",
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 20. Maximale Länge beträgt 2048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Dies ist eine Anzeige der Zuordnungen der VMware-Tags zu den AWS -Tags.

Typ: Array von VmwareToAwsTagMapping-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetVirtualMachine

Service: AWS Backup gateway

Durch Angabe des ARN (Amazon Resource Name) gibt diese API die virtuelle Maschine zurück.

Anforderungssyntax

```
{
   "ResourceArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ResourceArn

Der Amazon-Ressourcenname (ARN) der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

VirtualMachine

Dieses Objekt enthält die grundlegenden Attribute von `VirtualMachine`, die in der Ausgabe von `GetVirtualMachine` enthalten sind.

Typ: VirtualMachineDetails Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ImportHypervisorConfiguration

Service: AWS Backup gateway

Stellen Sie eine Verbindung zu einem Hypervisor her, indem Sie dessen Konfiguration importieren.

Anforderungssyntax

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Host

Der Serverhost des Hypervisors. Dies kann entweder eine IP-Adresse oder ein vollständig qualifizierter Domänenname (Fully Qualified Domain Name, FQDN) sein.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 128 Zeichen.

Pattern: `^.+$`

Erforderlich: Ja

KmsKeyArn

Das AWS Key Management Service für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Erforderlich: Nein

Name

Der Name des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Ja

Password

Das Kennwort für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -~]+$`

Erforderlich: Nein

Tags

Die Tags der Hypervisor-Konfiguration, die importiert werden sollen.

Typ: Array von Tag-Objekten

Erforderlich: Nein

Username

Der Benutzername für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Erforderlich: Nein

Antwortsyntax

```
{
   "HypervisorArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors, dessen Zuordnung Sie aufgehoben haben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang kann nicht fortgesetzt werden, da Sie nur unzureichende Berechtigungen haben.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListGateways

Service: AWS Backup gateway

Listet Backup-Gateways auf, die einem AWS-Konto in an AWS-Region gehören. Die zurückgegebene Liste wird nach Amazon-Ressourcenname (ARN) des Gateways sortiert.

Anforderungssyntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

MaxResults

Die maximale Anzahl von Gateways, die aufgelistet werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1.

Erforderlich: Nein

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

Antwortsyntax

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Gateways

Eine Liste Ihrer Gateways.

Typ: Array von Gateway-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `maxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListHypervisors

Service: AWS Backup gateway

Listet Ihre Hypervisoren auf.

Anforderungssyntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

MaxResults

Die maximale Anzahl von Hypervisoren, die aufgelistet werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1.

Erforderlich: Nein

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `maxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

Antwortsyntax

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Hypervisors

Eine Liste Ihrer `Hypervisor`-Objekte, sortiert nach Amazon-Ressourcennamen (ARNs).

Typ: Array von Hypervisor-Objekten

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `maxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListTagsForResource

Service: AWS Backup gateway

Listet die Tags auf, die auf die Ressource angewendet wurden, die durch den Amazon-Ressourcennamen (ARN) gekennzeichnet ist.

Anforderungssyntax

```
{
   "ResourceArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ResourceArn

Der Amazon-Ressourcenname (ARN) der Tags der Ressource, die aufgelistet werden sollen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
```

```
    ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ResourceArn

Der Amazon-Ressourcenname (ARN) der Tags der Ressource, die Sie aufgelistet haben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Eine Liste der Tags einer Ressource.

Typ: Array von Tag-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

ListVirtualMachines

Service: AWS Backup gateway

Listet Ihre virtuellen Maschinen auf.

Anforderungssyntax

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors, der mit Ihrer virtuellen Maschine verbunden ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

MaxResults

Die maximale Anzahl der virtuellen Maschinen, die aufgelistet werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1.

Erforderlich: Nein

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `maxResults` Anzahl von Ressourcen gestellt wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

Antwortsyntax

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Das nächste Element folgt auf eine unvollständige Liste der zurückgegebenen Ressourcen. Wenn beispielsweise eine Anforderung zur Rückgabe der `maxResults` Anzahl von Ressourcen gestellt

wird, ermöglicht Ihnen `NextToken`, mehr Elemente in Ihrer Liste zurückzugeben, beginnend mit der Position, auf die das nächste Token verweist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 1000 Zeichen.

Pattern: `^.+$`

VirtualMachines

Eine Liste Ihrer `VirtualMachine`-Objekte, sortiert nach Amazon-Ressourcennamen (ARNs).

Typ: Array von VirtualMachine-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutBandwidthRateLimitSchedule

Service: AWS Backup gateway

Diese Aktion legt den Zeitplan für das Bandbreitenlimit für ein bestimmtes Gateway fest. Standardmäßig haben Gateways keinen Zeitplan für das Bandbreitenlimit, was bedeutet, dass keine Bandbreitenratenbegrenzung wirksam ist. Verwenden Sie dies, um den Zeitplan für das Bandbreitenlimit eines Gateways zu initiieren.

Anforderungssyntax

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BandwidthRateLimitIntervals

Ein Array, das Zeitplanintervalle für Bandbreitenratenlimits für ein Gateway enthält. Wenn keine Intervalle für das Bandbreitenlimit geplant wurden, ist das Array leer.

Typ: Array von BandwidthRateLimitInterval-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Ja

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den ListGatewaysVorgang, um eine Liste von Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den ListGatewaysVorgang, um eine Liste der Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutHypervisorPropertyMappings

Service: AWS Backup gateway

Diese Aktion legt die Eigenschaftszuordnungen für den angegebenen Hypervisor fest. Eine Hypervisor-Eigenschaftenzuordnung zeigt das Verhältnis der Entitätseigenschaften, die auf dem Hypervisor verfügbar sind, zu den in verfügbaren Eigenschaften an. AWS

Anforderungssyntax

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 20. Maximale Länge beträgt 2048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

Erforderlich: Ja

VmwareToAwsTagMappings

Diese Aktion fordert die Zuordnungen von VMware-Tags zu den AWS -Tags an.

Typ: Array von VmwareToAwsTagMapping-Objekten

Erforderlich: Ja

Antwortsyntax

```
{
   "HypervisorArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang kann nicht fortgesetzt werden, da Sie nur unzureichende Berechtigungen haben.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutMaintenanceStartTime

Service: AWS Backup gateway

Legen Sie die Startzeit der Wartung für ein Gateway fest.

Anforderungssyntax

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

DayOfMonth

Der Tag des Monats, an dem die Wartung eines Gateways gestartet wird.

Der Bereich gültiger Werte lautet `Sunday` bis `Saturday`.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 31.

Erforderlich: Nein

DayOfWeek

Der Tag der Woche, an dem die Wartung eines Gateways gestartet wird.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 6.

Erforderlich: Nein

GatewayArn

Der Amazon-Ressourcenname (ARN) für das Gateway, der zur Angabe der Startzeit der Wartung verwendet wird.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

HourOfDay

Die Stunde des Tages, an dem die Wartung eines Gateways gestartet wird.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert 23.

Erforderlich: Ja

MinuteOfHour

Die Minute der Stunde, an der die Wartung eines Gateways gestartet wird.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 59.

Erforderlich: Ja

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) eines Gateways, für das Sie die Startzeit der Wartung festlegen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartVirtualMachinesMetadataSync

Service: AWS Backup gateway

Diese Aktion sendet eine Anfrage zur Synchronisierung von Metadaten zwischen den angegebenen virtuellen Maschinen.

Anforderungssyntax

```
{
   "HypervisorArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
   "HypervisorArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang kann nicht fortgesetzt werden, da Sie nur unzureichende Berechtigungen haben.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

TagResource

Service: AWS Backup gateway

Versehen Sie die Ressource mit einem Tag.

Anforderungssyntax

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ResourceARN

Der Amazon-Ressourcenname (ARN) der Ressource, die mit einem Tag versehen werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Tags

Eine Liste der Tags, die der Ressource zugewiesen sind.

Typ: Array von Tag-Objekten

Erforderlich: Ja

Antwortsyntax

```
{
   "ResourceARN": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ResourceARN

Der Amazon-Ressourcenname (ARN) der Ressource, die Sie mit einem Tag versehen haben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

TestHypervisorConfiguration

Service: AWS Backup gateway

Testet Ihre Hypervisor-Konfiguration, um zu überprüfen, ob das Backup-Gateway eine Verbindung zum Hypervisor und seinen Ressourcen herstellen kann.

Anforderungssyntax

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways zum zu testenden Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Host

Der Serverhost des Hypervisors. Dies kann entweder eine IP-Adresse oder ein vollständig qualifizierter Domänenname (Fully Qualified Domain Name, FQDN) sein.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 128 Zeichen.

Pattern: `^.+$`

Erforderlich: Ja

Password

Das Kennwort für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -~]+$`

Erforderlich: Nein

Username

Der Benutzername für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UntagResource

Service: AWS Backup gateway

Entfernt Tags aus der Ressource.

Anforderungssyntax

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ResourceARN

Der Amazon-Ressourcenname (ARN) der Ressource, aus der Tags entfernt werden sollen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

TagKeys

Die Liste der Tag-Schlüssel, die angeben, welche Tags entfernt werden sollen.

Typ: Zeichenfolgen-Array

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 128 Zeichen.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Erforderlich: Ja

Antwortsyntax

```
{
   "ResourceARN": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ResourceARN

Der Amazon-Ressourcenname (ARN) der Ressource, aus der Sie Tags entfernt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateGatewayInformation

Service: AWS Backup gateway

Aktualisiert den Namen eines Gateways. Geben Sie mit dem Amazon-Ressourcenname (ARN) des Gateways in Ihrer Anforderung an, welches Gateway aktualisiert werden soll.

Anforderungssyntax

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des zu aktualisierenden Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

GatewayDisplayName

Der aktualisierte Anzeigename des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

Antwortsyntax

```
{
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des von Ihnen aktualisierten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateGatewaySoftwareNow

Service: AWS Backup gateway

Aktualisiert die Software der virtuellen Maschine (VM) des Gateways. Die Anfrage löst die Softwareaktualisierung sofort aus.

> **Note**
>
> Wenn Sie diese Anforderung erfolgreich stellen, erhalten Sie sofort die entsprechende Antwort `200 OK`. Es kann einige Zeit dauern, bis die Aktualisierung abgeschlossen ist.

Anforderungssyntax

```
{
   "GatewayArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

GatewayArn

Der Amazon-Ressourcenname (ARN) des zu aktualisierenden Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

Antwortsyntax

```
{
```

```
   "GatewayArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

GatewayArn

Der Amazon-Ressourcenname (ARN) des von Ihnen aktualisierten Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge von 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

UpdateHypervisor

Service: AWS Backup gateway

Aktualisiert die Hypervisor-Metadaten, einschließlich Host, Benutzernamen und Kennwort. Geben Sie mit dem Amazon-Ressourcenname (ARN) des Hypervisors in Ihrer Anforderung an, welcher Hypervisor aktualisiert werden soll.

Anforderungssyntax

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter Allgemeine Parameter.

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Host

Der aktualisierte Host des Hypervisors. Dies kann entweder eine IP-Adresse oder ein vollständig qualifizierter Domänenname (Fully Qualified Domain Name, FQDN) sein.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 128 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors, der aktualisiert werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Ja

LogGroupArn

Der Amazon-Ressourcenname (ARN) der Gruppe von Gateways im angeforderten Protokoll.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 2048 Zeichen.

Pattern: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Erforderlich: Nein

Name

Der aktualisierte Name für den Hypervisor

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

Password

Das aktualisierte Kennwort für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -~]+$`

Erforderlich: Nein

Username

Der aktualisierte Benutzername für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Erforderlich: Nein

Antwortsyntax

```
{
   "HypervisorArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

HypervisorArn

Der Amazon-Ressourcenname (ARN) des von Ihnen aktualisierten Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang kann nicht fortgesetzt werden, da Sie nur unzureichende Berechtigungen haben.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

HTTP Status Code: 400

InternalServerException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

HTTP Status Code: 400

ValidationException

Der Vorgang war nicht erfolgreich, da ein Überprüfungsfehler aufgetreten ist.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

Datentypen

Die folgenden Datentypen werden von AWS Backup unterstützt:

- 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

Die folgenden Datentypen werden von AWS Backup gateway unterstützt:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

Die folgenden Datentypen werden von AWS Backup unterstützt:

- 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

Service: AWS Backup

Die Backup-Optionen für jeden Ressourcentyp.

Inhalt

BackupOptions

Gibt die Backup-Option für eine ausgewählte Ressource an. Diese Option ist nur für Windows VSS-Backup-Aufträge verfügbar.

Zulässige Werte:

Stellen Sie diese Option auf `"WindowsVSS":"enabled"` ein, um die `WindowsVSS`-Backup-Option zu aktivieren und ein Windows VSS-Backup zu erstellen.

Stellen Sie sie auf `"WindowsVSS":"disabled"` ein, um ein reguläres Backup zu erstellen. Die Option `WindowsVSS` ist standardmäßig aktiviert.

Wenn Sie eine ungültige Option angeben, erhalten Sie eine `InvalidParameterValueException`-Ausnahme.

Weitere Informationen zu Windows-VSS-Backups finden Sie unter Erstellen eines VSS-fähigen Windows-Backups.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wertemuster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

ResourceType

Gibt ein Objekt an, das den Ressourcentyp und die Backup-Optionen enthält. Der einzige unterstützte Ressourcentyp sind Amazon-EC2-Instances mit Windows Volume Shadow Copy Service (VSS). Ein CloudFormation Beispiel finden Sie in der CloudFormation Beispielvorlage zur Aktivierung von Windows VSS im AWS Backup Benutzerhandbuch.

Zulässige Werte: `EC2`.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJob

Service: AWS Backup

Enthält detaillierte Informationen zu einem Backup-Auftrag.

Inhalt

AccountId

Die Konto-ID, der der Backup-Auftrag angehört.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

BackupJobId

Identifiziert eindeutig eine Anfrage AWS Backup zur Sicherung einer Ressource.

Typ: Zeichenfolge

Erforderlich: Nein

BackupOptions

Gibt die Backup-Option für eine ausgewählte Ressource an. Diese Option ist nur für Windows-VSS-Backup-Aufträge (Volume Shadow Copy Service) verfügbar.

Gültige Werte: Stellen Sie diese Option auf `"WindowsVSS":"enabled"` ein, um die `WindowsVSS`-Backup-Option zu aktivieren und ein Windows VSS-Backup zu erstellen. Stellen Sie sie auf `"WindowsVSS":"disabled"` ein, um ein reguläres Backup zu erstellen. Wenn Sie eine ungültige Option angeben, erhalten Sie eine `InvalidParameterValueException`-Ausnahme.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Schlüssel-Muster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wertemuster: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

BackupSizeInBytes

Die Größe eines Backups in Byte

Type: Long

Erforderlich: Nein

BackupType

Stellt den Backup-Typ für einen Backup-Auftrag dar.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Nein

BytesTransferred

Die Größe in Byte, die zum Zeitpunkt der Abfrage des Auftragsstatus an einen Backup-Tresor übertragen wurden.

Type: Long

Erforderlich: Nein

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Erstellen eines Backup-Auftrags abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von

`CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreatedBy

Enthält identifizierende Informationen über die Erstellung eines Backup-Auftrags, einschließlich `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` und `BackupRuleId` des Backup-Plans, mit dem er erstellt wurde.

Typ: RecoveryPointCreator Objekt

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Auftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

ExpectedCompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Sichern von Ressourcen abgeschlossen werden soll, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `ExpectedCompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

IamRoleArn

Gibt den IAM-Rollen-ARN an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wird. Andere IAM-Rollen als die Standardrolle müssen entweder `AWSBackup` oder `AwsBackup` im Rollennamen enthalten. z. B. `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Rollennamen ohne diese Zeichenfolgen sind nicht berechtigt, Backup-Aufträge auszuführen.

Typ: Zeichenfolge

Erforderlich: Nein

InitiationDate

Das Datum, an dem der Backup-Job initiiert wurde.

Typ: Zeitstempel

Erforderlich: Nein

IsParent

Dies ist ein boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Backup-Auftrag handelt.

Typ: Boolesch

Erforderlich: Nein

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Beispielzeichenfolgen können `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` oder `INVALIDPARAMETERS` sein. Eine Liste der MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

Typ: Zeichenfolge

Erforderlich: Nein

ParentJobId

Dadurch wird eine Anforderung an AWS Backup zur Sicherung einer Ressource eindeutig identifiziert. Bei der Rückgabe handelt es sich um die übergeordnete (zusammengesetzte) Auftrags-ID.

Typ: Zeichenfolge

Erforderlich: Nein

PercentDone

Enthält einen geschätzten Prozentsatz der Fertigstellung eines Auftrags zum Zeitpunkt der Abfrage des Auftragsstatus.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceName

Der nicht eindeutige Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der Typ der AWS Ressource, die gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank. Für Windows-VSS-Backups (Volume Shadow Copy Services) ist der einzige unterstützte Ressourcentyp Amazon EC2.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

StartBy

Gibt die Uhrzeit im Unix-Format und in der koordinierten Weltzeit (UTC) an, zu der ein Backup-Auftrag gestartet werden muss, bevor er abgebrochen wird. Der Wert wird berechnet, indem das Startfenster zur geplanten Zeit hinzugefügt wird. Wenn die geplante Zeit also 18:00 Uhr wäre und das Startfenster zwei Stunden beträgt, wäre die `StartBy`-Uhrzeit am angegebenen Datum 20:00 Uhr. Der Wert von `StartBy` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

State

Der aktuelle Status eines Backup-Auftrags.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Erforderlich: Nein

StatusMessage

Eine ausführliche Meldung, in der der Status des Backup-Auftrags für eine Ressource erläutert wird.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJobSummary

Service: AWS Backup

Dies ist eine Zusammenfassung der Aufträge, die in den letzten 30 Tagen erstellt oder ausgeführt wurden.

Die zurückgegebene Zusammenfassung kann Folgendes enthalten: Region, Konto, Bundesland RestourceType, MessageCategory, StartTime, EndTime, und Anzahl der enthaltenen Jobs.

Inhalt

AccountId

Die Konto-ID, die Eigentümer der Aufträge in der Zusammenfassung ist.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

Count

Der Wert als Anzahl der Aufträge in einer Auftragsübersicht.

Typ: Ganzzahl

Erforderlich: Nein

EndTime

Der Zeitwert im Zahlenformat einer Auftragsendzeit.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Zu den Beispielzeichenfolgen gehören `AccessDenied`, `Success` und `InvalidParameters`. Eine Liste der MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

Typ: Zeichenfolge

Erforderlich: Nein

Region

Die AWS Regionen in der Stellenübersicht.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Dieser Wert ist die Anzahl der Aufträge für den angegebenen Ressourcentyp. Die Anforderung `GetSupportedResourceTypes` gibt Zeichenfolgen für unterstützte Ressourcentypen zurück.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

StartTime

Der Zeitwert im Zahlenformat der Startzeit eines Auftrags.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

State

Dieser Wert ist die Anzahl der Aufträge für Aufträge mit dem angegebenen Status.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlan

Service: AWS Backup

Enthält einen optionalen Anzeigenamen für Sicherungsplan und ein Array von `BackupRule`-Objekten, die jeweils eine Sicherungsregel angeben. Jede Regel in einem Backup-Plan ist eine separate geplante Aufgabe und kann eine unterschiedliche Auswahl an AWS -Ressourcen sichern.

Inhalt

BackupPlanName

Der Anzeigename eines Sicherungsplans. Muss zwischen 1 und 50 alphanumerischen Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Ja

Rules

Ein Array von `BackupRule`-Objekten, von denen jedes eine geplante Aufgabe angibt, die verwendet wird, um eine Auswahl von Ressourcen zu sichern.

Typ: Array von BackupRule-Objekten

Erforderlich: Ja

AdvancedBackupSettings

Enthält eine Liste von `BackupOptions` für jeden Ressourcentyp.

Typ: Array von AdvancedBackupSetting-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

BackupPlanInput

Service: AWS Backup

Enthält einen optionalen Anzeigenamen für Sicherungsplan und ein Array von `BackupRule`-Objekten, die jeweils eine Sicherungsregel angeben. Jede Regel in einem Backup-Plan ist eine separate geplante Aufgabe.

Inhalt

BackupPlanName

Der Anzeigename eines Sicherungsplans. Muss zwischen 1 und 50 alphanumerischen Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Ja

Rules

Ein Array von `BackupRule`-Objekten, von denen jedes eine geplante Aufgabe angibt, die verwendet wird, um eine Auswahl von Ressourcen zu sichern.

Typ: Array von BackupRuleInput-Objekten

Erforderlich: Ja

AdvancedBackupSettings

Gibt eine Liste von `BackupOptions` für jeden Ressourcentyp an. Diese Einstellungen sind nur für Windows-VSS-Backup-Aufträge (Volume Shadow Copy Service) verfügbar.

Typ: Array von AdvancedBackupSetting-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

BackupPlansListMember

Service: AWS Backup

Enthält Metadaten zu einem Backup-Plan.

Inhalt

AdvancedBackupSettings

Enthält eine Liste von `BackupOptions` für einen Ressourcentyp.

Typ: Array von AdvancedBackupSetting-Objekten

Erforderlich: Nein

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanName

Der Anzeigename eines gespeicherten Backups-Plans.

Typ: Zeichenfolge

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Ressourcen-Backup-plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

DeletionDate

Das Datum und die Uhrzeit der Löschung eines Backup-Plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `DeletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

LastExecutionDate

Das letzte Mal, als dieser Backup-Plan ausgeführt wurde. Datum und Uhrzeit im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastExecutionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Version-IDs können nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlanTemplatesListMember

Service: AWS Backup

Ein Objekt, das Metadaten angibt, die mit einer Backup-Planvorlage verknüpft sind.

Inhalt

BackupPlanTemplateId

Identifiziert eindeutig eine gespeicherte Backup-Planvorlage.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanTemplateName

Der optionale Anzeigename einer Backup-Planvorlage.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRule

Service: AWS Backup

Gibt eine geplante Aufgabe an, mit der eine Auswahl von Ressourcen gesichert werden.

Inhalt

RuleName

Ein Anzeigename für eine Sicherungsregel. Muss zwischen 1 und 50 alphanumerischen Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Ja

TargetBackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

CompletionWindowMinutes

Ein Wert in Minuten, nachdem ein Backup-Auftrag erfolgreich gestartet wurde, bevor er abgeschlossen werden muss, oder er wird von AWS Backup abgebrochen. Dieser Wert ist optional.

Type: Long

Erforderlich: Nein

CopyActions

Ein Array von `CopyAction`-Objekten, das die Details des Kopiervorgangs enthält.

Typ: Array von CopyAction-Objekten

Erforderlich: Nein

EnableContinuousBackup

Gibt an, ob kontinuierliche Backups AWS Backup erstellt werden. Wahre Gründe für AWS Backup die Erstellung kontinuierlicher Backups, die point-in-time wiederhergestellt werden können (PITR). Falsch (oder nicht angegeben) führt AWS Backup zur Erstellung von Snapshot-Backups.

Typ: Boolesch

Erforderlich: Nein

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Typ: Lifecycle Objekt

Erforderlich: Nein

RecoveryPointTags

Die Tags, die Ressourcen zugewiesen werden, die dieser Regel zugeordnet sind, wenn sie aus dem Backup wiederhergestellt werden.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

RuleId

Identifiziert eindeutig eine Regel, die verwendet wird, um das Backup einer Auswahl von Ressourcen zu planen.

Typ: Zeichenfolge

Erforderlich: Nein

ScheduleExpression

Ein Cron-Ausdruck in UTC, der angibt, wann ein AWS Backup Backup-Job initiiert wird. Weitere Informationen zu AWS Cron-Ausdrücken finden Sie unter Schedule Expressions for Rules im Amazon CloudWatch Events-Benutzerhandbuch. . Zwei Beispiele für AWS Cron-Ausdrücke sind `15 * ? * * *` (jede Stunde 15 Minuten nach der Stunde ein Backup erstellen) und `0 12 * * ? *` (täglich um 12 Uhr UTC ein Backup erstellen). Eine Tabelle mit Beispielen finden Sie, wenn Sie auf den vorherigen Link klicken und auf der Seite nach unten scrollen.

Typ: Zeichenfolge

Erforderlich: Nein

ScheduleExpressionTimezone

Die Zeitzone, in der der Zeitplanausdruck festgelegt ist. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowMinutes

Ein Wert in Minuten, nachdem ein Backup geplant ist, bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, muss er mindestens 60 Minuten betragen, um Fehler zu vermeiden.

Während des Startfensters bleibt der Status des Backup-Auftrags so lange im `CREATED`-Status, bis er erfolgreich gestartet wurde oder bis die Startfensterzeit abgelaufen ist. Wenn Time innerhalb des Startfensters einen Fehler AWS Backup erhält, der einen erneuten Versuch ermöglicht, den Job erneut zu starten, AWS Backup wird automatisch mindestens alle 10 Minuten erneut versucht, den Job zu starten, bis die Sicherung erfolgreich gestartet wird (der Jobstatus ändert sich auf`RUNNING`) oder bis sich der Jobstatus auf ändert `EXPIRED` (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRuleInput

Service: AWS Backup

Gibt eine geplante Aufgabe an, mit der eine Auswahl von Ressourcen gesichert werden.

Inhalt

RuleName

Ein Anzeigename für eine Sicherungsregel. Muss zwischen 1 und 50 alphanumerischen Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Ja

TargetBackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Ja

CompletionWindowMinutes

Ein Wert in Minuten, nachdem ein Backup-Auftrag erfolgreich gestartet wurde, bevor er abgeschlossen werden muss, oder er wird von AWS Backup abgebrochen. Dieser Wert ist optional.

Type: Long

Erforderlich: Nein

CopyActions

Ein Array von `CopyAction`-Objekten, das die Details des Kopiervorgangs enthält.

Typ: Array von CopyAction-Objekten

Erforderlich: Nein

EnableContinuousBackup

Gibt an, ob kontinuierliche Backups AWS Backup erstellt werden. Wahre Gründe für AWS Backup die Erstellung kontinuierlicher Backups, die point-in-time wiederhergestellt werden können (PITR). Falsch (oder nicht angegeben) führt AWS Backup zur Erstellung von Snapshot-Backups.

Typ: Boolesch

Erforderlich: Nein

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch und läuft entsprechend dem von Ihnen definierten Lebenszyklus ab.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Umstellung auf kalt nach Tagen“ kann nicht geändert werden, nachdem ein Backup in einen kalten Speicher umgestellt wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Der Höchstwert für diesen Parameter ist 100 Jahre (36.500 Tage).

Typ: Lifecycle Objekt

Erforderlich: Nein

RecoveryPointTags

Die Tags, die den Ressourcen zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ScheduleExpression

Ein CRON-Ausdruck in UTC, der angibt, wann ein AWS Backup Backup-Job initiiert wird.

Typ: Zeichenfolge

Erforderlich: Nein

ScheduleExpressionTimezone

Die Zeitzone, in der der Zeitplanausdruck festgelegt ist. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowMinutes

Ein Wert in Minuten, nachdem ein Backup geplant ist, bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, muss er mindestens 60 Minuten betragen, um Fehler zu vermeiden.

Dieser Parameter hat einen maximalen Wert von 100 Jahren (52.560.000 Minuten).

Während des Startfensters bleibt der Status des Backup-Auftrags so lange im `CREATED`-Status, bis er erfolgreich gestartet wurde oder bis die Startfensterzeit abgelaufen ist. Wenn Time innerhalb des Startfensters einen Fehler AWS Backup erhält, der einen erneuten Versuch ermöglicht, den Job erneut zu starten, AWS Backup wird automatisch mindestens alle 10 Minuten erneut versucht, den Job zu starten, bis die Sicherung erfolgreich gestartet wird (der Jobstatus ändert sich auf`RUNNING`) oder bis sich der Jobstatus auf ändert `EXPIRED` (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelection

Service: AWS Backup

Gibt eine Gruppe von Ressourcen für einen Backup-Plan an.

Wir empfehlen, dass Sie Bedingungen, Tags oder Ressourcen angeben, die ein- oder ausgeschlossen werden sollen. Andernfalls versucht Backup, alle unterstützten und aktivierten Speicherressourcen auszuwählen, was unbeabsichtigte Auswirkungen auf die Kosten haben könnte.

Weitere Informationen finden Sie unter Programmgesteuertes Zuweisen von Ressourcen.

Inhalt

IamRoleArn

Der ARN der IAM-Rolle, die zur Authentifizierung beim Sichern der Zielressource AWS Backup verwendet wird; zum Beispiel. `arn:aws:iam::123456789012:role/S3Access`

Typ: Zeichenfolge

Erforderlich: Ja

SelectionName

Der Anzeigename eines Dokuments zur Ressourcenauswahl. Muss zwischen 1 und 50 alphanumerischen Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Ja

Conditions

Die Bedingungen, die Sie definieren, um Ihren Backup-Plänen mithilfe von Tags Ressourcen zuzuweisen. z. B. `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`unterstützt `StringEquals``StringLike`,`StringNotEquals`, und`StringNotLike`. Bei Bedingungsoperatoren wird zwischen Groß- und Kleinschreibung unterschieden.

Wenn Sie mehrere Bedingungen angeben, entsprechen die Ressourcen weitgehend allen Bedingungen (UND-Logik).

Typ: Conditions Objekt

Erforderlich: Nein

ListOfTags

Die Bedingungen, die Sie definieren, um Ihren Backup-Plänen mithilfe von Tags Ressourcen zuzuweisen. z. B. `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`unterstützt nur`StringEquals`. Bei Bedingungsoperatoren wird zwischen Groß- und Kleinschreibung unterschieden.

Wenn Sie mehrere Bedingungen angeben, entsprechen die Ressourcen im Großen und Ganzen einer der Bedingungen (OR-Logik).

Typ: Array von Condition-Objekten

Erforderlich: Nein

NotResources

Die Amazon-Ressourcennamen (ARNs) der Ressourcen, die von einem Backup-Plan ausgeschlossen werden sollen. Die maximale Anzahl von ARNs beträgt 500 ohne Platzhaltern, oder 30 ARNs mit Platzhaltern.

Wenn Sie viele Ressourcen aus einem Backup-Plan ausschließen müssen, sollten Sie eine andere Strategie zur Ressourcenauswahl in Betracht ziehen, z. B. nur einen oder wenige Ressourcentypen zuweisen oder Ihre Ressourcenauswahl mithilfe von Tags verfeinern.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Resources

Die Amazon-Ressourcennamen (ARNs) der Ressourcen, die einem Backup-Plan zugewiesen werden sollen. Die maximale Anzahl von ARNs beträgt 500 ohne Platzhaltern, oder 30 ARNs mit Platzhaltern.

Wenn Sie einem Backup-Plan viele Ressourcen zuweisen müssen, sollten Sie eine andere Strategie zur Ressourcenauswahl in Betracht ziehen, z. B. alle Ressourcen eines Ressourcentyps zuweisen oder Ihre Ressourcenauswahl mithilfe von Tags verfeinern.

Wenn Sie mehrere ARNs angeben, stimmen die Ressourcen weitgehend mit einer der ARNs (OR-Logik) überein.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelectionsListMember

Service: AWS Backup

Enthält Metadaten zu einem `BackupSelection`-Objekt.

Inhalt

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Backup-Plans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

IamRoleArn

Gibt den Amazon-Ressourcennamen (ARN) der IAM-Rolle an, um den Zielwiederherstellungspunkt zu erstellen, z. B. `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

SelectionId

Identifiziert eine Anforderung zum Zuweisen einer Gruppe von Ressourcen zu einem Sicherungsplan eindeutig.

Typ: Zeichenfolge

Erforderlich: Nein

SelectionName

Der Anzeigename eines Dokuments zur Ressourcenauswahl.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupVaultListMember

Service: AWS Backup

Enthält Metadaten zu einem Backup-Tresor.

Inhalt

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Ressourcen-Backups im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage angibt und die Wiederholung fehlgeschlagener Anforderungen ermöglicht, ohne dass das Risiko besteht, dass die Operation zweimal ausgeführt wird. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

EncryptionKeyArn

Ein serverseitiger Verschlüsselungsschlüssel, den Sie angeben können, um Ihre Backups von Diensten zu verschlüsseln, die die vollständige AWS Backup Verwaltung unterstützen, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Falls Sie einen Schlüssel angeben, müssen Sie seinen ARN angeben, nicht seinen Alias. Falls Sie keinen Schlüssel angeben, erstellt AWS Backup standardmäßig einen KMS-Schlüssel für Sie.

Informationen darüber, welche AWS Backup Dienste die vollständige AWS Backup Verwaltung unterstützen und wie mit der Verschlüsselung von Backups von Diensten AWS Backup umgegangen wird, die die vollständige Verwaltung noch nicht unterstützen AWS Backup, finden Sie unter Verschlüsselung für Backups in AWS Backup

Typ: Zeichenfolge

Erforderlich: Nein

LockDate

Datum und Uhrzeit, zu der die AWS Backup Vault Lock-Konfiguration unveränderlich wird, d. h. sie kann nicht geändert oder gelöscht werden.

Wenn Sie eine Tresorsperre auf Ihren Tresor angewendet haben, ohne ein Sperrdatum anzugeben, können Sie Ihre Tresorsperren-Einstellungen jederzeit ändern oder die Vault Lock vollständig aus dem Tresor löschen.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

Locked

Ein boolescher Wert, der angibt, ob AWS Backup Vault Lock für den ausgewählten Backup-Tresor gilt. Falls `true`, verhindert Vault Lock Lösch- und Aktualisierungsvorgänge an den Wiederherstellungspunkten im ausgewählten Tresor.

Typ: Boolesch

Erforderlich: Nein

MaxRetentionDays

Die AWS Backup Vault Lock-Einstellung, die den maximalen Aufbewahrungszeitraum angibt, für den der Tresor seine Wiederherstellungspunkte beibehält. Wenn dieser Parameter nicht angegeben wird, erzwingt Vault Lock keine maximale Aufbewahrungsdauer für die Wiederherstellungspunkte im Tresor (und erlaubt somit eine unbegrenzte Speicherung).

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der maximalen Aufbewahrungsdauer entspricht oder kürzer ist. Wenn die Aufbewahrungsdauer des Auftrags länger als die maximale Aufbewahrungsdauer ist, schlägt der Tresor den Backup- oder Kopierauftrag fehl, und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden. Wiederherstellungspunkte, die bereits vor der Tresorsperre im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

Erforderlich: Nein

MinRetentionDays

Die AWS Backup Vault Lock-Einstellung, die den Mindestaufbewahrungszeitraum festlegt, für den der Tresor seine Wiederherstellungspunkte aufbewahrt. Wenn dieser Parameter nicht angegeben wird, erzwingt Vault Lock keine Mindestaufbewahrungsdauer.

Wenn angegeben, muss jeder Backup- oder Kopierauftrag in den Tresor über eine Lebenszyklusrichtlinie mit einer Aufbewahrungsdauer verfügen, die der minimalen Aufbewahrungsdauer entspricht oder länger ist. Wenn die Aufbewahrungsfrist des Auftrags länger als die maximale Aufbewahrungsdauer ist, kann der Tresor den Backup- oder Kopierauftrag nicht ausführen und Sie sollten entweder Ihre Lebenszyklus-Einstellungen ändern oder einen anderen Tresor verwenden. Wiederherstellungspunkte, die bereits vor der Tresorsperre im Tresor gespeichert wurden, sind nicht betroffen.

Type: Long

Erforderlich: Nein

NumberOfRecoveryPoints

Die Anzahl der Wiederherstellungspunkte, die in einem Backup-Tresor gespeichert sind.

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CalculatedLifecycle

Service: AWS Backup

Enthält `DeleteAt`- und `MoveToColdStorageAt`-Zeitstempel, die verwendet werden, um einen Lebenszyklus für einen Wiederherstellungspunkt anzugeben.

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Kühlspeicher überführt wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Inhalt

DeleteAt

Ein Zeitstempel, der angibt, wann ein Wiederherstellungspunkt gelöscht werden soll.

Typ: Zeitstempel

Erforderlich: Nein

MoveToColdStorageAt

Ein Zeitstempel, der angibt, wann ein Wiederherstellungspunkt in den Cold Storage überführt werden soll.

Typ: Zeitstempel

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Condition

Service: AWS Backup

Enthält ein Array von Dreiergruppen, die aus einem Bedingungstyp (z. B. `StringEquals`), einem Schlüssel und einem Wert bestehen. Wird verwendet, um Ressourcen anhand ihrer Tags zu filtern und sie einem Backup-Plan zuzuweisen. Groß-/Kleinschreibung ist zu beachten.

Inhalt

ConditionKey

Der Schlüssel in einem Schlüssel-Wert-Paar. Beispiel: Im Tag `Department: Accounting` ist der Schlüssel `Department`.

Typ: Zeichenfolge

Erforderlich: Ja

ConditionType

Eine Operation, die auf ein Schlüssel-Wert-Paar zum Zuweisen von Ressourcen zu Ihrem Backup-Plan angewendet wird. Die Bedingung unterstützt nur `StringEquals`. Für flexiblere Zuweisungsoptionen, einschließlich `StringLike` und der Möglichkeit, Ressourcen aus Ihrem Backup-Plan auszuschließen, verwenden Sie `Conditions` (mit einem „s“ am Ende) für Ihre `BackupSelection`.

Typ: Zeichenfolge

Zulässige Werte: `STRINGEQUALS`

Erforderlich: Ja

ConditionValue

Der Wert in einem Schlüssel-Wert-Paar. Beispiel: Im Wert `Department: Accounting` ist der Schlüssel `Accounting`.

Typ: Zeichenfolge

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ConditionParameter

Service: AWS Backup

Enthält Informationen zu einem Backup-Plan an, die einem Backup-Plan zugewiesen werden sollen.

Fügen Sie das Präfix `aws:ResourceTag` in Ihre Tags ein. z. B. `"aws:ResourceTag/TagKey1": "Value1"`.

Inhalt

ConditionKey

Der Schlüssel in einem Schlüssel-Wert-Paar. Beispiel: Im Tag `Department: Accounting` ist der Schlüssel `Department`.

Typ: Zeichenfolge

Erforderlich: Nein

ConditionValue

Der Wert in einem Schlüssel-Wert-Paar. Beispiel: Im Wert `Department: Accounting` ist der Schlüssel `Accounting`.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Conditions

Service: AWS Backup

Enthält Informationen darüber, welche Ressourcen anhand ihrer Tags in einen Backup-Plan aufgenommen oder aus diesem ausgeschlossen werden sollen. Bei Bedingungen wird die Groß- und Kleinschreibung beachtet.

Inhalt

StringEquals

Filtert die Werte Ihrer markierten Ressourcen nur nach den Ressourcen, die Sie mit demselben Wert markiert haben. Wird auch als „exaktes Matching“ bezeichnet.

Typ: Array von ConditionParameter-Objekten

Erforderlich: Nein

StringLike

Filtert die Werte Ihrer markierten Ressourcen nach passenden Tag-Werten, indem Sie ein Platzhalterzeichen (*) an einer beliebigen Stelle in der Zeichenfolge verwenden. Beispielsweise entspricht „prod*“ oder „*rod*“ dem Tag-Wert „production“.

Typ: Array von ConditionParameter-Objekten

Erforderlich: Nein

StringNotEquals

Filtert die Werte Ihrer markierten Ressourcen nur nach den Ressourcen, die Sie markiert haben und die nicht denselben Wert haben. Wird auch als „negiertes Matching“ bezeichnet.

Typ: Array von ConditionParameter-Objekten

Erforderlich: Nein

StringNotLike

Filtert die Werte Ihrer markierten Ressourcen nach nicht übereinstimmenden Tag-Werten, indem Sie an einer beliebigen Stelle in der Zeichenfolge ein Platzhalterzeichen (*) verwenden.

Typ: Array von ConditionParameter-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlInputParameter

Service: AWS Backup

Die Parameter für ein Steuerelement. Ein Steuerelement kann null, einen, oder mehrere Parameter haben. Ein Beispiel für eine Steuerung mit zwei Parametern ist: „Die Häufigkeit des Sicherungsplans ist mindestens `daily` und die Aufbewahrungsdauer beträgt mindestens `1 year`“. Der erste Parameter ist `daily`. Der zweite Parameter ist `1 year`.

Inhalt

ParameterName

Der Name eines Parameters, zum Beispiel `BackupPlanFrequency`.

Typ: Zeichenfolge

Erforderlich: Nein

ParameterValue

Der Wert des Parameters, zum Beispiel `hourly`.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlScope

Service: AWS Backup

Ein Framework besteht aus einem oder mehreren Steuerelementen. Jede Steuerung hat ihren eigenen Steuerungsbereich. Der Umfang der Steuerung kann einen oder mehrere Ressourcentypen, eine Kombination aus Tag-Schlüssel- und Wert oder eine Kombination aus einem Ressourcentyp und einer Ressource-ID enthalten. Wenn kein Bereich angegeben ist, werden Auswertungen für die Regel ausgelöst, wenn sich die Konfiguration einer Ressource in Ihrer Aufzeichnungsgruppe ändert.

> **Note**
>
> Um einen Steuerungsbereich festzulegen, der die gesamte Ressource umfasst, lassen Sie das `ControlScope` leer oder geben Sie es beim Aufruf von `CreateFramework` nicht weiter.

Inhalt

ComplianceResourceIds

Die ID der einzigen AWS Ressource, die Ihr Kontrollbereich enthalten soll.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 100 Elemente.

Erforderlich: Nein

ComplianceResourceTypes

Beschreibt, ob der Steuerungsbereich einen oder mehrere Ressourcentypen umfasst, z. B. `EFS` oder `RDS`.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Tags

Das Tag-Schlüssel-Wert-Paar, das auf die AWS Ressourcen angewendet wird, die Sie für eine Regel auswerten möchten. Es kann maximal ein Schlüssel-Wert-Paar angegeben werden. Der

Tag-Wert ist optional, darf jedoch keine leere Zeichenfolge sein, wenn Sie ein Framework von der Konsole aus erstellen oder bearbeiten (obwohl der Wert eine leere Zeichenfolge sein kann, wenn er in einer CloudFormation Vorlage enthalten ist).

Die Struktur für die Zuweisung eines Tags lautet: `[{"Key":"string","Value":"string"}]`.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyAction

Service: AWS Backup

Die Details des Kopiervorgangs.

Inhalt

DestinationBackupVaultArn

Ein Amazon-Ressourcenname (ARN), der den Zielsicherungstresor für die kopierte Sicherung eindeutig identifiziert. Beispiel, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Ja

Lifecycle

Gibt den Zeitraum in Tagen an, bevor ein Recovery Point in den Cold Storage übergeht oder gelöscht wird.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Aufbewahrungseinstellung auf der Konsole um 90 Tage höher sein als die Einstellung für den Übergang zur Einstellung „Kalt nach Tagen“. Die Einstellung „Nach Tagen kalt“ kann nicht geändert werden, nachdem ein Backup auf „kalt“ umgestellt wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Um den bestehenden Lebenszyklus und die Aufbewahrungsfristen zu entfernen und Ihre Wiederherstellungspunkte unbegrenzt beizubehalten, geben Sie -1 für `MoveToColdStorageAfterDays` und an. `DeleteAfterDays`

Typ: Lifecycle Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJob

Service: AWS Backup

Enthält detaillierte Informationen zu einem Kopierauftrag.

Inhalt

AccountId

Die Konto-ID, der der Kopierauftrag angehört.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

BackupSizeInBytes

Die Größe eines Kopierauftrags in Byte.

Type: Long

Erforderlich: Nein

ChildJobsInState

Dadurch werden die Statistiken der enthaltenen untergeordneten (verschachtelten) Kopieraufträge zurückgegeben.

Typ: Zeichenfolge auf eine lange Zuordnung

Gültige Schlüssel: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Erforderlich: Nein

CompletionDate

Das Datum und die Uhrzeit der Fertigstellung eines Kopierauftrags im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CompositeMemberIdentifier

Der Bezeichner einer Ressource innerhalb einer Verbundgruppe, z. B. eines verschachtelten (untergeordneten) Wiederherstellungspunkts, der zu einem zusammengesetzten (übergeordneten) Stack gehört. Die ID wird von der logischen ID innerhalb eines Stacks übertragen.

Typ: Zeichenfolge

Erforderlich: Nein

CopyJobId

Identifiziert einen Kopierauftrag eindeutig.

Typ: Zeichenfolge

Erforderlich: Nein

CreatedBy

Enthält Informationen über den Sicherungsplan und die Regel, die AWS Backup zur Initiierung des Wiederherstellungspunkt-Backups verwendet wurden.

Typ: RecoveryPointCreator Objekt

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Kopierauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

DestinationBackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Ziel-Kopiertresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

DestinationRecoveryPointArn

Ein ARN, der einen Ziel-Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Kopieren des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

IsParent

Dies ist ein boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Kopierauftrag handelt.

Typ: Boolesch

Erforderlich: Nein

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Beispielzeichenfolgen können `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` oder `InvalidParameters` sein. Eine Liste von MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück

Typ: Zeichenfolge

Erforderlich: Nein

NumberOfChildJobs

Die Anzahl der untergeordneten (verschachtelten) Kopieraufträge.

Type: Long

Erforderlich: Nein

ParentJobId

Dadurch wird eine Anforderung an AWS Backup zum Kopieren einer Ressource eindeutig identifiziert. Bei der Rückgabe handelt es sich um die übergeordnete (zusammengesetzte) Auftrags-ID.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceArn

Die zu kopierende AWS Ressource, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceName

Der nicht eindeutige Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der Typ der zu kopierenden AWS Ressource, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

SourceBackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Quell-Kopiertresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

SourceRecoveryPointArn

Ein ARN, der einen Quell-Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

State

Den aktuellen Status eines Kopierauftrags.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Erforderlich: Nein

StatusMessage

Eine ausführliche Meldung, in der der Status des Auftrags zum Kopieren einer Ressource erläutert wird.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJobSummary

Service: AWS Backup

Dies ist eine Zusammenfassung der Kopieraufträge, die in den letzten 30 Tagen erstellt oder ausgeführt wurden.

Die zurückgegebene Zusammenfassung kann Folgendes enthalten: Region, Konto, Bundesland RestourceType, MessageCategory, StartTime, EndTime, und Anzahl der enthaltenen Jobs.

Inhalt

AccountId

Die Konto-ID, die Eigentümer der Aufträge in der Zusammenfassung ist.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

Count

Der Wert als Anzahl der Aufträge in einer Auftragsübersicht.

Typ: Ganzzahl

Erforderlich: Nein

EndTime

Der Zeitwert im Zahlenformat einer Auftragsendzeit.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenkategorie an.

Zu den Beispielzeichenfolgen gehören `AccessDenied`, `Success` und `InvalidParameters`. Eine Liste der MessageCategory Zeichenketten finden Sie unter Überwachung.

Der Wert ANY gibt die Anzahl aller Nachrichtenkategorien zurück.

`AGGREGATE_ALL` aggregiert die Anzahl der Aufträge für alle Nachrichtenkategorien und gibt die Summe zurück.

Typ: Zeichenfolge

Erforderlich: Nein

Region

Die AWS Regionen in der Stellenübersicht.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Dieser Wert ist die Anzahl der Aufträge für den angegebenen Ressourcentyp. Die Anforderung `GetSupportedResourceTypes` gibt Zeichenfolgen für unterstützte Ressourcentypen zurück

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

StartTime

Der Zeitwert im Zahlenformat der Startzeit eines Auftrags.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

State

Dieser Wert ist die Anzahl der Aufträge für Aufträge mit dem angegebenen Status.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DateRange

Service: AWS Backup

Dies ist ein Ressourcenfilter, der FromDate: DateTime und ToDate: enthält DateTime. Beide Werte sind erforderlich. Zukünftige DateTime Werte sind nicht zulässig.

Datum und Uhrzeit sind im Unix-Format und in Coordinated Universal Time (UTC) angegeben und sind auf Millisekunden genau (Millisekunden sind optional). Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Inhalt

FromDate

Dieser Wert entspricht dem Startdatum (einschließlich).

Datum und Uhrzeit sind im Unix-Format und in Coordinated Universal Time (UTC) angegeben und sind auf Millisekunden genau (Millisekunden sind optional).

Typ: Zeitstempel

Erforderlich: Ja

ToDate

Dieser Wert entspricht dem Enddatum (einschließlich).

Datum und Uhrzeit sind im Unix-Format und in Coordinated Universal Time (UTC) angegeben und sind auf Millisekunden genau (Millisekunden sind optional).

Typ: Zeitstempel

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Framework

Service: AWS Backup

Enthält detaillierte Informationen über ein Framework. Frameworks enthalten Kontrollen, die Ihre Backup-Ereignisse und -Ressourcen auswerten und darüber berichten. Frameworks generieren täglich Compliance-Ergebnisse.

Inhalt

CreationTime

Das Datum und die Uhrzeit, zu der ein Framework erstellt wurde, in ISO 8601-Darstellung. Der Wert von `CreationTime` ist auf Millisekunden genau. Beispielsweise steht 2020-07-10T 15:00:00.000-08:00 für den 10. Juli 2020 um 15.00 Uhr, UTC minus 8 Stunden.

Typ: Zeitstempel

Erforderlich: Nein

DeploymentStatus

Der Bereitstellungsstatus eines Frameworks. Die Status sind:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Typ: Zeichenfolge

Erforderlich: Nein

FrameworkArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

FrameworkDescription

Eine optionale Beschreibung des Frameworks mit einer Länge von maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

FrameworkName

Der eindeutige Name eines Frameworks. Dieser Name hat eine Länge von maximal 256 Zeichen, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Nein

NumberOfControls

Die Anzahl der im Framework enthaltenen Kontrollen.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FrameworkControl

Service: AWS Backup

Enthält detaillierte Informationen über alle Steuerelemente eines Frameworks. Jedes Framework muss mindestens ein Steuerelement enthalten.

Inhalt

ControlName

Der Name des Steuerelements. Dieser Name hat zwischen 1 und 256 Zeichen.

Typ: Zeichenfolge

Erforderlich: Ja

ControlInputParameters

Die Name/Wert-Paare.

Typ: Array von ControlInputParameter-Objekten

Erforderlich: Nein

ControlScope

Der Geltungsbereich einer Steuerung. Der Geltungsbereich der Steuerung legt fest, was die Steuerung auswerten soll. Drei Beispiele für Getungsbereichen für Steurerung sind: ein bestimmter Backup-Plan, alle Backup-Pläne mit einem bestimmten Tag oder alle Backup-Pläne.

Weitere Informationen finden Sie unter `ControlScope`.

Typ: ControlScope Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

KeyValue

Service: AWS Backup

Paar zweier verwandter Zeichenfolgen. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 dargestellt werden können, sowie die folgenden Zeichen: `+ - = . _ : /`

Inhalt

Key

Der Tag-Schlüssel (Zeichenfolge). Der Schlüssel darf nicht mit `aws:` beginnen.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 128 Zeichen.

Pattern: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Typ: Zeichenfolge

Erforderlich: Ja

Value

Der Wert des Schlüssels.

Längenbeschränkungen: Maximale Länge beträgt 256 Zeichen.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Typ: Zeichenfolge

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LegalHold

Service: AWS Backup

Eine gesetzliche Aufbewahrungsfrist ist ein administratives Tool, mit dem verhindert werden kann, dass Backups gelöscht werden, während sie sich noch im Sperrmodus befinden. Solange die Sperre aktiv ist, können Backups, die sich in einer Sperre befinden, nicht gelöscht werden, und Lebenszyklusrichtlinien, die den Backup-Status ändern würden (z. B. der Übergang in Cold Storage), werden verzögert, bis die gesetzliche Sperre aufgehoben wird. Ein Backup kann mehrere gesetzliche Aufbewahrungsfristen haben. Gesetzliche Aufbewahrungsfristen werden auf ein oder mehrere Backups (auch als Wiederherstellungspunkte bezeichnet) angewendet. Diese Backups können nach Ressourcentypen und Ressourcen-IDs gefiltert werden.

Inhalt

CancellationDate

Der Zeitpunkt, zu dem die gesetzliche Sperre aufgehoben wurde.

Typ: Zeitstempel

Erforderlich: Nein

CreationDate

Der Zeitpunkt, zu dem die gesetzliche Sperre eingerichtet wurde.

Typ: Zeitstempel

Erforderlich: Nein

Description

Die Beschreibung einer gesetzlichen Sperre.

Typ: Zeichenfolge

Erforderlich: Nein

LegalHoldArn

Der Amazon-Ressourcenname (ARN) des gesetzlichen Aufbewahrungszeitpunkts, z. B.`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

LegalHoldId

Die ID der gesetzlichen Aufbewahrungsfrist.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Der Status der gesetzlichen Sperre.

Typ: Zeichenfolge

Zulässige Werte: `CREATING | ACTIVE | CANCELING | CANCELED`

Erforderlich: Nein

Title

Der Titel einer gesetzlichen Aufbewahrung.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Lifecycle

Service: AWS Backup

Gibt den Zeitraum in Tagen an, bevor ein Recovery Point in den Cold Storage übergeht oder gelöscht wird.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Aufbewahrungseinstellung auf der Konsole um 90 Tage höher sein als die Einstellung für den Übergang zur Einstellung „Kalt nach Tagen“. Die Einstellung für den Übergang zu „kalt nach Tagen“ kann nicht geändert werden, nachdem ein Backup auf „kalt“ umgestellt wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Um den bestehenden Lebenszyklus und die Aufbewahrungsfristen zu entfernen und Ihre Wiederherstellungspunkte unbegrenzt beizubehalten, geben Sie -1 für `MoveToColdStorageAfterDays` und an. `DeleteAfterDays`

Inhalt

DeleteAfterDays

Die Anzahl der Tage nach der Erstellung, an denen ein Wiederherstellungspunkt gelöscht wird. Dieser Wert muss mindestens 90 Tage nach der unter angegebenen Anzahl von Tagen liegen`MoveToColdStorageAfterDays`.

Type: Long

Erforderlich: Nein

MoveToColdStorageAfterDays

Die Anzahl der Tage nach der Erstellung, an denen ein Recovery Point in einen Cold Storage verschoben wird.

Type: Long

Erforderlich: Nein

OptInToArchiveForSupportedResources

Wenn der Wert wahr ist, wechselt Ihr Backup-Plan die unterstützten Ressourcen gemäß Ihren Lebenszykluseinstellungen auf die Archivierungsstufe (Cold Storage).

Typ: Boolesch

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResource

Service: AWS Backup

Eine Struktur, die Informationen über eine gesicherte Ressource enthält.

Inhalt

LastBackupTime

Das Datum und die Uhrzeit des letzten Backups einer Ressource im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `LastBackupTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

LastBackupVaultArn

Der ARN (Amazon Resource Name) des Backup-Tresors, der den neuesten Backup-Wiederherstellungspunkt enthält.

Typ: Zeichenfolge

Erforderlich: Nein

LastRecoveryPointArn

Der ARN (Amazon Resource Name) des letzten Wiederherstellungspunkts.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceName

Der nicht eindeutige Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der AWS Ressourcentyp, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank. Für Windows-VSS-Backups (Volume Shadow Copy Services) ist der einzige unterstützte Ressourcentyp Amazon EC2.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResourceConditions

Service: AWS Backup

Die Bedingungen, die Sie für Ressourcen in Ihrem Wiederherstellungstestplan mithilfe von Tags definieren.

z. B. `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Bei Bedingungsoperatoren wird zwischen Groß- und Kleinschreibung unterschieden.

Inhalt

StringEquals

Filtert die Werte Ihrer markierten Ressourcen nur nach den Ressourcen, die Sie mit demselben Wert markiert haben. Wird auch als „exaktes Matching“ bezeichnet.

Typ: Array von KeyValue-Objekten

Erforderlich: Nein

StringNotEquals

Filtert die Werte Ihrer markierten Ressourcen nur nach den Ressourcen, die Sie markiert haben und die nicht denselben Wert haben. Wird auch als „negiertes Matching“ bezeichnet.

Typ: Array von KeyValue-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByBackupVault

Service: AWS Backup

Enthält detaillierte Informationen zu den Wiederherstellungspunkten, die in einem Backup-Tresor gespeichert sind.

Inhalt

BackupSizeInBytes

Die Größe eines Backups in Byte

Type: Long

Erforderlich: Nein

BackupVaultArn

Ein ARN, der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Nein

CalculatedLifecycle

Ein `CalculatedLifecycle`-Objekt, das `DeleteAt`- und `MoveToColdStorageAt`-Zeitstempel enthält.

Typ: CalculatedLifecycle Objekt

Erforderlich: Nein

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Wiederherstellen eines Wiederherstellungspunkts abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CompositeMemberIdentifier

Der Bezeichner einer Ressource innerhalb einer Verbundgruppe, z. B. eines verschachtelten (untergeordneten) Wiederherstellungspunkts, der zu einem zusammengesetzten (übergeordneten) Stack gehört. Die ID wird von der logischen ID innerhalb eines Stacks übertragen.

Typ: Zeichenfolge

Erforderlich: Nein

CreatedBy

Enthält identifizierende Informationen über die Erstellung eines Wiederherstellungspunkts, einschließlich `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` und `BackupRuleId` des Backup-Plans, mit dem er erstellt wurde.

Typ: RecoveryPointCreator Objekt

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungspunkts im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

EncryptionKeyArn

Die serverseitige Verschlüsselung zum Schutz Ihrer Backups, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

Erforderlich: Nein

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

IsEncrypted

Ein boolescher Wert, der als `TRUE` zurückgegeben wird, wenn der angegebene Wiederherstellungspunkt verschlüsselt ist, oder als `FALSE`, wenn der Wiederherstellungspunkt nicht verschlüsselt ist.

Typ: Boolesch

Erforderlich: Nein

IsParent

Dies ist ein boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Wiederherstellungspunkt handelt.

Typ: Boolesch

Erforderlich: Nein

LastRestoreTime

Das Datum und die Uhrzeit der letzten Wiederherstellung eines Wiederherstellungspunkts im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `LastRestoreTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

Lifecycle

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Cold Storage übertragen wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

In den Cold Storage übertragene Sicherungen müssen mindestens 90 Tage lang im Cold Storage gespeichert werden. Daher muss die Einstellung für „Ablauf nach Tagen“ 90 Tage größer als die Einstellung für „Übertragung in Archivspeicher nach Tagen“ sein. Die Einstellung „Übertragung in Archivspeicher nach Tagen“ kann nicht geändert werden, sobald eine Sicherung in den Archivspeicher übertragen wurde.

Ressourcentypen, die auf Cold Storage umgestellt werden können, sind in der Tabelle Verfügbarkeit von Funktionen nach Ressourcen aufgeführt. AWS Backup ignoriert diesen Ausdruck für andere Ressourcentypen.

Typ: Lifecycle Objekt

Erforderlich: Nein

ParentRecoveryPointArn

Der Amazon-Ressourcenname (ARN) des übergeordneten (zusammengesetzten) Wiederherstellungspunkts.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceArn

Ein ARN bezeichnet eindeutig eine Ressource. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceName

Der nicht eindeutige Name der Ressource, die zu dem angegebenen Backup gehört.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der Typ der AWS Ressource, die als Erholungspunkt gespeichert wurde, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank. Für Windows-VSS-Backups (Volume Shadow Copy Services) ist der einzige unterstützte Ressourcentyp Amazon EC2.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

SourceBackupVaultArn

Der Backup-Tresor, aus dem der Wiederherstellungspunkt ursprünglich kopiert wurde. Wenn der Wiederherstellungspunkt für dasselbe Konto wiederhergestellt wird, ist dieser Wert `null`.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Ein Statuscode, der den Status des Wiederherstellungspunkts angibt.

Typ: Zeichenfolge

Zulässige Werte: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Erforderlich: Nein

StatusMessage

Eine Meldung, die den aktuellen Status des Wiederherstellungspunkts erklärt.

Typ: Zeichenfolge

Erforderlich: Nein

VaultType

Der Typ des Tresors, in dem der beschriebene Erholungspunkt gespeichert ist.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByResource

Service: AWS Backup

Enthält detaillierte Informationen zu einem gespeicherten Wiederherstellungspunkt.

Inhalt

BackupSizeBytes

Die Größe eines Backups in Byte

Type: Long

Erforderlich: Nein

BackupVaultName

Der Name eines logischen Containers, in dem die Sicherungen gespeichert werden. Backup-Tresore werden durch Namen identifiziert, die für das Konto, mit dem sie erstellt wurden, und die AWS -Region, in der sie erstellt wurden, eindeutig sind.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungspunkts im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

EncryptionKeyArn

Die serverseitige Verschlüsselung zum Schutz Ihrer Backups, z. B. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

Erforderlich: Nein

IsParent

Dies ist ein boolescher Wert, der angibt, dass es sich um einen übergeordneten (zusammengesetzten) Wiederherstellungspunkt handelt.

Typ: Boolesch

Erforderlich: Nein

ParentRecoveryPointArn

Der Amazon-Ressourcenname (ARN) des übergeordneten (zusammengesetzten) Wiederherstellungspunkts.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceName

Der nicht eindeutige Name der Ressource, die zum angegebenen Backup gehört.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Ein Statuscode, der den Status des Wiederherstellungspunkts angibt.

Typ: Zeichenfolge

Zulässige Werte: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Erforderlich: Nein

StatusMessage

Eine Meldung, die den aktuellen Status des Wiederherstellungspunkts erklärt.

Typ: Zeichenfolge

Erforderlich: Nein

VaultType

Der Tresortyp, in dem der beschriebene Erholungspunkt gespeichert ist.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointCreator

Service: AWS Backup

Enthält Informationen über den Sicherungsplan und die Regel, die AWS Backup zur Initiierung des Wiederherstellungspunkt-Backups verwendet wurden.

Inhalt

BackupPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Plan eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanId

Identifiziert einen Backup-Plan.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanVersion

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Sie können nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Nein

BackupRuleId

Identifiziert eindeutig eine Regel, die verwendet wird, um das Backup einer Auswahl von Ressourcen zu planen.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointMember

Service: AWS Backup

Dies ist ein Wiederherstellungspunkt, bei dem es sich um einen untergeordneten (verschachtelten) Wiederherstellungspunkt eines übergeordneten (zusammengesetzten) Wiederherstellungspunkt handelt. Diese Wiederherstellungspunkte können von ihrem übergeordneten (zusammengesetzten) Wiederherstellungspunkt getrennt werden. In diesem Fall sind sie kein Mitglied mehr.

Inhalt

BackupVaultName

Der Name des Backup-Tresors (der logische Container, in dem Backups gespeichert werden).

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Erforderlich: Nein

RecoveryPointArn

Der Amazon-Ressourcenname (ARN) des übergeordneten (zusammengesetzten) Wiederherstellungspunkts.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceArn

Der Amazon-Ressourcenname (ARN), der eine gespeicherte Ressource eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der AWS Ressourcentyp, der als Erholungspunkt gespeichert wird.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointSelection

Service: AWS Backup

Dadurch werden Kriterien für die Zuweisung einer Reihe von Ressourcen festgelegt, z. B. Ressourcentypen oder Backup-Tresore.

Inhalt

DateRange

Dies ist ein Ressourcenfilter, der FromDate: DateTime und ToDate: enthält DateTime. Beide Werte sind erforderlich. Zukünftige DateTime Werte sind nicht zulässig.

Datum und Uhrzeit sind im Unix-Format und in Coordinated Universal Time (UTC) angegeben und sind auf Millisekunden genau (Millisekunden sind optional). Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: DateRange Objekt

Erforderlich: Nein

ResourceIdentifiers

Dies sind die Ressourcen, die in der Ressourcenauswahl enthalten sind (einschließlich Ressourcentyp und Tresore).

Typ: Zeichenfolgen-Array

Erforderlich: Nein

VaultNames

Dies sind die Namen der Tresore, in denen die ausgewählten Wiederherstellungspunkte enthalten sind.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportDeliveryChannel

Service: AWS Backup

Enthält Informationen aus Ihrem Berichtsplan darüber, wo Ihre Berichte bereitgestellt werden sollen, insbesondere Ihren Amazon-S3-Bucket-Namen, das S3-Schlüsselpräfix und die Formate Ihrer Berichte.

Inhalt

S3BucketName

Der eindeutige Name des S3-Buckets, der Ihre Berichte empfängt.

Typ: Zeichenfolge

Erforderlich: Ja

Formats

Das Format Ihrer Berichte: `CSV`, `JSON`, oder beides. Wenn nichts angegeben ist, ist das Standardformat `CSV`.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

S3KeyPrefix

Das Präfix dafür, wo AWS Backup Audit Manager Ihre Berichte an Amazon S3 übermittelt. Das Präfix ist dieser Teil des folgenden Pfads: s3://your-bucket-name/`prefix`/backup/US-West-2/year/month/day/Report-Name. Wenn nicht angegeben, gibt es kein Präfix.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen SDKs finden Sie im Folgenden: AWS

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

ReportDestination

Service: AWS Backup

Enthält Informationen aus Ihrem Berichtsauftrag über Ihr Berichtsziel.

Inhalt

S3BucketName

Der eindeutige Name des Amazon-S3-Buckets, der Ihre Berichte empfängt.

Typ: Zeichenfolge

Erforderlich: Nein

S3Keys

Der Objektschlüssel, der Ihre Berichte eindeutig in Ihrem S3-Bucket identifiziert.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportJob

Service: AWS Backup

Enthält detaillierte Informationen zu einem Berichtsauftrag. Ein Berichtsauftrag erstellt einen Bericht auf der Grundlage eines Berichtsplans und veröffentlicht ihn in Amazon S3.

Inhalt

CompletionTime

Das Datum und die Uhrzeit der Fertigstellung eines Berichtsauftrags im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Berichtsauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

ReportDestination

Der S3-Bucket-Name und die S3-Schlüssel für das Ziel, an dem der Berichtsauftrag den Bericht veröffentlicht.

Typ: ReportDestination Objekt

Erforderlich: Nein

ReportJobId

Der Bezeichner für einen Berichtsauftrag. Eine eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolge, die maximal 1 024 Byte lang ist. Die Berichtsauftrags-IDs können nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Nein

ReportPlanArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

ReportTemplate

Identifiziert die Berichtsvorlage für den Bericht. Berichte werden mithilfe einer Berichtsvorlage erstellt. Die Berichtsvorlagen sind:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Typ: Zeichenfolge

Erforderlich: Nein

Status

Der Status des Berichtsauftrags. Die Status sind:

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` bedeutet, dass der Bericht an Ihrem angegebenen Zielort zur Überprüfung zur Verfügung steht. Wenn der Status lautet `FAILED`, finden Sie in der `StatusMessage` den Grund.

Typ: Zeichenfolge

Erforderlich: Nein

StatusMessage

Eine Meldung, in der der Status des Berichtsauftrags erklärt wird.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportPlan

Service: AWS Backup

Enthält detaillierte Informationen zu einem Berichtsplan.

Inhalt

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Berichtsplans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

DeploymentStatus

Gibt den Bereitstellungsstatus eines Berichtsplans zurück. Die Status sind:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

Typ: Zeichenfolge

Erforderlich: Nein

LastAttemptedExecutionTime

Das Datum und die Uhrzeit des letzten Versuchs einer Ausführung eines mit diesem Berichtsplan verknüpften Berichtsauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `LastAttemptedExecutionTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

LastSuccessfulExecutionTime

Das Datum und die Uhrzeit der letzten erfolgreichen Ausführung eines mit diesem Berichtsplan verknüpften Berichtsauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `LastSuccessfulExecutionTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

ReportDeliveryChannel

Enthält Informationen darüber, wo und wie Sie Ihre Berichte liefern, insbesondere Ihren Amazon-S3-Bucket-Namen, das S3-Schlüsselpräfix und die Formate Ihrer Berichte.

Typ: ReportDeliveryChannel Objekt

Erforderlich: Nein

ReportPlanArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

ReportPlanDescription

Eine optionale Beschreibung des Berichtsplans mit maximal 1 024 Zeichen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 1024 Zeichen.

Pattern: `.*\S.*`

Erforderlich: Nein

ReportPlanName

Der eindeutige Name des Berichtsplans. Dieser Name hat zwischen 1 und 256 Zeichen, die mit einem Buchstaben beginnen und aus Buchstaben (a–z, A–Z), Zahlen (0–9) und Unterstriche (_) bestehen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Erforderlich: Nein

ReportSetting

Identifiziert die Berichtsvorlage für den Bericht. Berichte werden mithilfe einer Berichtsvorlage erstellt. Die Berichtsvorlagen sind:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Wenn die Berichtsvorlage `RESOURCE_COMPLIANCE_REPORT` oder ist`CONTROL_COMPLIANCE_REPORT`, beschreibt diese API-Ressource auch die Berichtsabdeckung von AWS-Regionen und Frameworks.

Typ: ReportSetting Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportSetting

Service: AWS Backup

Enthält detaillierte Informationen zu einer Berichtseinstellung.

Inhalt

ReportTemplate

Identifiziert die Berichtsvorlage für den Bericht. Berichte werden mithilfe einer Berichtsvorlage erstellt. Die Berichtsvorlagen sind:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Typ: Zeichenfolge

Erforderlich: Ja

Accounts

Dies sind die Konten, die in den Bericht aufgenommen werden sollen.

Verwenden Sie den Zeichenkettenwert von`ROOT`, um alle Organisationseinheiten einzubeziehen.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

FrameworkArns

Die Amazon-Ressourcennamen (ARNs) der Frameworks, die ein Bericht abdeckt.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

NumberOfFrameworks

Die Anzahl der Frameworks, die ein Bericht abdeckt.

Typ: Ganzzahl

Erforderlich: Nein

OrganizationUnits

Dies sind die Organisationseinheiten, die in den Bericht aufgenommen werden sollen.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Regions

Dies sind die Regionen, die in den Bericht aufgenommen werden sollen.

Verwenden Sie den Platzhalter als Zeichenfolgenwert, um alle Regionen einzubeziehen.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobCreator

Service: AWS Backup

Enthält Informationen über den Wiederherstellungstestplan, mit dem AWS Backup den Wiederherstellungsauftrag initiiert hat.

Inhalt

RestoreTestingPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungstestplan eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobsListMember

Service: AWS Backup

Enthält Metadaten zu einem Wiederherstellungsauftrag.

Inhalt

AccountId

Die Konto-ID, die Eigentümer der Ressource ist.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

BackupSizeInBytes

Die Größe der wiederhergestellten Ressource in Byte.

Type: Long

Erforderlich: Nein

CompletionDate

Das Datum und die Uhrzeit, zu der ein Auftrag zum Wiederherstellen eines Wiederherstellungspunkts abgeschlossen wird, im Unix-Format und in der koordinierten Weltzeit (UTC). Der Wert von `CompletionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

CreatedBy

Enthält identifizierende Informationen zur Erstellung eines Wiederherstellungsauftrags.

Typ: RestoreJobCreator Objekt

Erforderlich: Nein

CreatedResourceArn

Ein Amazon-Ressourcenname (ARN), der eine Ressource eindeutig identifiziert. Das Format eines ARN hängt vom Ressourcentyp ab.

Typ: Zeichenfolge

Erforderlich: Nein

CreationDate

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungsauftrags im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

DeletionStatus

Darin wird der Status der durch den Wiederherstellungstest generierten Daten angegeben. Der Status kann `Deleting`, `Failed` oder `Successful` sein.

Typ: Zeichenfolge

Zulässige Werte: `DELETING | FAILED | SUCCESSFUL`

Erforderlich: Nein

DeletionStatusMessage

Dies beschreibt den Löschstatus des Wiederherstellungsauftrags.

Typ: Zeichenfolge

Erforderlich: Nein

ExpectedCompletionTimeMinutes

Die Zeit in Minuten, die ein Auftrag zur Wiederherstellung eines Wiederherstellungspunkts voraussichtlich in Anspruch nehmen wird.

Type: Long

Erforderlich: Nein

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zum Erstellen des Ziel-Wiederherstellungspunkts verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

PercentDone

Enthält einen geschätzten Prozentsatz der Fertigstellung eines Auftrags zum Zeitpunkt der Abfrage des Auftragsstatus.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointArn

Ein ARN, der einen Wiederherstellungspunkt eindeutig identifiziert, z. B. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointCreationDate

Das Datum, an dem ein Wiederherstellungspunkt erstellt wurde.

Typ: Zeitstempel

Erforderlich: Nein

ResourceType

Der Ressourcentyp der aufgeführten Wiederherstellungsaufträge, z. B. ein Amazon-EBS-Volume (Elastic Block Store) oder eine Amazon-RDS-Datenbank (Relational Database Service). Für Windows-VSS-Backups (Volume Shadow Copy Services) ist der einzige unterstützte Ressourcentyp Amazon EC2.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

RestoreJobId

Identifiziert den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Ein Statuscode, der den Status des Jobs angibt, der von AWS Backup zur Wiederherstellung eines Wiederherstellungspunkts initiiert wurde.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Erforderlich: Nein

StatusMessage

Eine ausführliche Meldung, in der der Status des Wiederherstellungsauftrags für einen Wiederherstellungspunkt erläutert wird.

Typ: Zeichenfolge

Erforderlich: Nein

ValidationStatus

Der Status der Überprüfung, die für den angegebenen Wiederherstellungsauftrag ausgeführt wurde.

Typ: Zeichenfolge

Zulässige Werte: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Erforderlich: Nein

ValidationStatusMessage

Dies beschreibt den Status der Validierung, die für den angegebenen Wiederherstellungsauftrag ausgeführt wurde.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobSummary

Service: AWS Backup

Dies ist eine Zusammenfassung der Wiederherstellungsaufträge, die in den letzten 30 Tagen erstellt oder ausgeführt wurden.

Die zurückgegebene Zusammenfassung kann Folgendes enthalten: Region, Konto, Bundesland ResourceType, MessageCategory, StartTime, EndTime, und Anzahl der enthaltenen Jobs.

Inhalt

AccountId

Die Konto-ID, die Eigentümer der Aufträge in der Zusammenfassung ist.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

Count

Der Wert als Anzahl der Aufträge in einer Auftragsübersicht.

Typ: Ganzzahl

Erforderlich: Nein

EndTime

Der Zeitwert im Zahlenformat einer Auftragsendzeit.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

Region

Die AWS Regionen in der Stellenübersicht.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Dieser Wert ist die Anzahl der Aufträge für den angegebenen Ressourcentyp. Die Anforderung `GetSupportedResourceTypes` gibt Zeichenfolgen für unterstützte Ressourcentypen zurück.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erforderlich: Nein

StartTime

Der Zeitwert im Zahlenformat der Startzeit eines Auftrags.

Dieser Wert ist im Unix-Format in Coordinated Universal Time (UTC) und ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

State

Dieser Wert ist die Anzahl der Aufträge für Aufträge mit dem angegebenen Status.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForCreate

Service: AWS Backup

Dies enthält Metadaten zu einem Wiederherstellungstestplan.

Inhalt

RecoveryPointSelection

`RecoveryPointSelection`hat fünf Parameter (drei erforderlich und zwei optional). Die von Ihnen angegebenen Werte bestimmen, welcher Erholungspunkt im Wiederherstellungstest enthalten ist. Sie müssen angeben, `Algorithm` ob Sie den neuesten `SelectionWindowDays` oder einen zufälligen Wiederherstellungspunkt verwenden möchten, und Sie müssen angeben, `IncludeVaults` aus welchen Tresoren die Wiederherstellungspunkte ausgewählt werden können.

`Algorithm`(erforderlich) Gültige Werte: "`LATEST_WITHIN_WINDOW`" oder "`RANDOM_WITHIN_WINDOW`“.

`Recovery point types`(erforderlich) Gültige Werte: "`SNAPSHOT`" und/oder "`CONTINUOUS`“. Einbeziehen`SNAPSHOT`, um nur Snapshot-Wiederherstellungspunkte wiederherzustellen; einbeziehen`CONTINUOUS`, um kontinuierliche Wiederherstellungspunkte wiederherzustellen (Point-in-Time-Restore/PITR); beide Optionen verwenden, um entweder einen Snapshot oder einen kontinuierlichen Wiederherstellungspunkt wiederherzustellen. Der Erholungspunkt wird durch den Wert für `Algorithm` bestimmt.

`IncludeVaults`(erforderlich). Sie müssen einen oder mehrere Backup-Tresore hinzufügen. Verwenden Sie den Platzhalter ["*"] oder bestimmte ARNs.

`SelectionWindowDays`(optional) Der Wert muss eine Ganzzahl (in Tagen) zwischen 1 und 365 sein. Wenn nicht enthalten, ist der Standardwert. `30`

`ExcludeVaults`(fakultativ). Sie können wählen, ob Sie einen oder mehrere spezifische Backup-Tresor-ARNs eingeben möchten, um den Inhalt dieser Tresore von der Wiederherstellungsberechtigung auszuschließen. Sie können auch eine Liste mit Selektoren hinzufügen. Wenn dieser Parameter und sein Wert nicht enthalten sind, wird standardmäßig eine leere Liste verwendet.

Typ: RestoreTestingRecoveryPointSelection Objekt

Erforderlich: Ja

RestoreTestingPlanName

Das RestoreTestingPlanName ist eine eindeutige Zeichenfolge, die dem Namen des Wiederherstellungstestplans entspricht. Dieser Wert kann nach der Erstellung nicht geändert werden und darf nur aus alphanumerischen Zeichen und Unterstrichen bestehen.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpressionTimezone

Optional. Dies ist die Zeitzone, in der der Planungsausdruck festgelegt wird. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowHours

Die Standardeinstellung ist 24 Stunden.

Ein Wert in Stunden, nachdem ein Backup geplant wurde und bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, hat dieser Parameter einen Maximalwert von 168 Stunden (eine Woche).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForGet

Service: AWS Backup

Dies enthält Metadaten zu einem Wiederherstellungstestplan.

Inhalt

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungsplans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Ja

RecoveryPointSelection

Die angegebenen Kriterien für die Zuweisung einer Reihe von Ressourcen, z. B. Ressourcentypen oder Backup-Tresore.

Typ: RestoreTestingRecoveryPointSelection Objekt

Erforderlich: Ja

RestoreTestingPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungstestplan eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingPlanName

Der Name des Wiederherstellungstestplans.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Ja

CreatorRequestId

Dies identifiziert die Anforderung und ermöglicht die Wiederholung fehlgeschlagener Anforderungen, ohne dass das Risiko besteht, dass der Vorgang zweimal ausgeführt wird. Wenn die Anforderung eine `CreatorRequestId` enthält, der einem vorhandenen Backup-Plan entspricht, wird dieser Plan zurückgegeben. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

LastExecutionTime

Das letzte Mal, dass ein Wiederherstellungstest mit dem angegebenen Wiederherstellungstestplan ausgeführt wurde. Datum und Uhrzeit im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastExecutionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

LastUpdateTime

Datum und Uhrzeit der Aktualisierung des Wiederherstellungstestplans. Diese Aktualisierung ist im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastUpdateTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

ScheduleExpressionTimezone

Optional. Dies ist die Zeitzone, in der der Planungsausdruck festgelegt wird. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowHours

Die Standardeinstellung ist 24 Stunden.

Ein Wert in Stunden, nachdem ein Backup geplant wurde und bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, hat dieser Parameter einen Maximalwert von 168 Stunden (eine Woche).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForList

Service: AWS Backup

Dies enthält Metadaten zu einem Wiederherstellungstestplan.

Inhalt

CreationTime

Das Datum und die Uhrzeit der Erstellung eines Wiederherstellungsplans im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Ja

RestoreTestingPlanArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungstestplan eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingPlanName

Der Name des Wiederherstellungstestplans.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Ja

LastExecutionTime

Das letzte Mal, dass ein Wiederherstellungstest mit dem angegebenen Wiederherstellungstestplan ausgeführt wurde. Datum und Uhrzeit im Unix-Format sowie in UTC

(Universal Coordinated Time). Der Wert von `LastExecutionDate` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

LastUpdateTime

Datum und Uhrzeit der Aktualisierung des Wiederherstellungstestplans. Diese Aktualisierung ist im Unix-Format sowie in UTC (Universal Coordinated Time). Der Wert von `LastUpdateTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30.087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

ScheduleExpressionTimezone

Optional. Dies ist die Zeitzone, in der der Planungsausdruck festgelegt wird. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowHours

Die Standardeinstellung ist 24 Stunden.

Ein Wert in Stunden, nachdem ein Backup geplant wurde und bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, hat dieser Parameter einen Maximalwert von 168 Stunden (eine Woche).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForUpdate

Service: AWS Backup

Dies enthält Metadaten zu einem Wiederherstellungstestplan.

Inhalt

RecoveryPointSelection

Erforderlich: `AlgorithmRecoveryPointTypes`; `IncludeVaults` (einer oder mehrere).

Optional: SelectionWindowDays('30', falls nicht angegeben); `ExcludeVaults` (standardmäßig eine leere Liste, wenn sie nicht aufgeführt ist).

Typ: RestoreTestingRecoveryPointSelection Objekt

Erforderlich: Nein

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Nein

ScheduleExpressionTimezone

Optional. Dies ist die Zeitzone, in der der Planungsausdruck festgelegt wird. Standardmäßig ScheduleExpressions sind sie in UTC. Sie können dies in eine bestimmte Zeitzone ändern.

Typ: Zeichenfolge

Erforderlich: Nein

StartWindowHours

Die Standardeinstellung ist 24 Stunden.

Ein Wert in Stunden, nachdem ein Backup geplant wurde und bevor ein Auftrag storniert wird, wenn er nicht erfolgreich gestartet werden kann. Dieser Wert ist optional. Wenn dieser Wert enthalten ist, hat dieser Parameter einen Maximalwert von 168 Stunden (eine Woche).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingRecoveryPointSelection

Service: AWS Backup

`RecoveryPointSelection`hat fünf Parameter (drei erforderlich und zwei optional). Die von Ihnen angegebenen Werte bestimmen, welcher Erholungspunkt im Wiederherstellungstest enthalten ist. Sie müssen angeben, `Algorithm` ob Sie den neuesten `SelectionWindowDays` oder einen zufälligen Wiederherstellungspunkt verwenden möchten, und Sie müssen angeben, `IncludeVaults` aus welchen Tresoren die Wiederherstellungspunkte ausgewählt werden können.

`Algorithm`(erforderlich) Gültige Werte: "`LATEST_WITHIN_WINDOW`" oder "`RANDOM_WITHIN_WINDOW`“.

`Recovery point types`(erforderlich) Gültige Werte: "`SNAPSHOT`" und/oder "`CONTINUOUS`“. Einbeziehen`SNAPSHOT`, um nur Snapshot-Wiederherstellungspunkte wiederherzustellen; einbeziehen`CONTINUOUS`, um kontinuierliche Wiederherstellungspunkte wiederherzustellen (Point-in-Time-Restore/PITR); beide Optionen verwenden, um entweder einen Snapshot oder einen kontinuierlichen Wiederherstellungspunkt wiederherzustellen. Der Erholungspunkt wird durch den Wert für `Algorithm` bestimmt.

`IncludeVaults`(erforderlich). Sie müssen einen oder mehrere Backup-Tresore hinzufügen. Verwenden Sie den Platzhalter ["*"] oder bestimmte ARNs.

`SelectionWindowDays`(optional) Der Wert muss eine Ganzzahl (in Tagen) zwischen 1 und 365 sein. Wenn nicht enthalten, ist der Standardwert. `30`

`ExcludeVaults`(optional). Sie können wählen, ob Sie einen oder mehrere spezifische Backup-Tresor-ARNs eingeben möchten, um den Inhalt dieser Tresore von der Wiederherstellungsberechtigung auszuschließen. Sie können auch eine Liste mit Selektoren hinzufügen. Wenn dieser Parameter und sein Wert nicht enthalten sind, wird standardmäßig eine leere Liste verwendet.

Inhalt

Algorithm

Zulässige Werte sind u. a. „LATEST_WITHIN_WINDOW“ oder „RANDOM_WITHIN_WINDOW“

Typ: Zeichenfolge

Zulässige Werte: `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

Erforderlich: Nein

ExcludeVaults

Zu den akzeptierten Werten gehören bestimmte ARNs oder eine Liste von Selektoren. Standardmäßig ist die Liste leer, wenn nicht aufgeführt.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

IncludeVaults

Zu den akzeptierten Werten gehören Platzhalter [„*“] oder bestimmte ARNs oder ARN-Platzhalter [„arn:aws:backup:us-west-2:123456789012:backup-vault:asdf“, ...] [„arn:aws:backup: *:*:backup-vault:asdf-*“, ...]

Typ: Zeichenfolgen-Array

Erforderlich: Nein

RecoveryPointTypes

Dies sind die Arten von Wiederherstellungspunkten.

EinbeziehenSNAPSHOT, um nur Snapshot-Wiederherstellungspunkte wiederherzustellen; einbeziehenCONTINUOUS, um kontinuierliche Wiederherstellungspunkte wiederherzustellen (Point-in-Time-Restore/ PITR); beide Optionen verwenden, um entweder einen Snapshot oder einen kontinuierlichen Wiederherstellungspunkt wiederherzustellen. Der Erholungspunkt wird durch den Wert für `Algorithm` bestimmt.

Typ: Zeichenfolgen-Array

Zulässige Werte: `CONTINUOUS | SNAPSHOT`

Erforderlich: Nein

SelectionWindowDays

Zulässige Werte sind Ganzzahlen von 1 bis 365.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForCreate

Service: AWS Backup

Dies enthält Metadaten zu einer Auswahl für Wiederherstellungstests.

ProtectedResourceType ist erforderlich, z. B. Amazon EBS oder Amazon EC2.

Dies besteht aus `RestoreTestingSelectionName`, `ProtectedResourceType` und einem der folgenden Elemente:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Jeder geschützte Ressourcentyp kann einen einzelnen Wert haben.

Eine Auswahl für den Wiederherstellungstest kann einen Platzhalterwert („*“) für `ProtectedResourceArns` zusammen mit `ProtectedResourceConditions` enthalten. Alternativ können Sie bis zu 30 spezifische ARNs für geschützte Ressourcen in `ProtectedResourceArns` hinzufügen.

`ProtectedResourceConditions`-Beispiele sind u. a. `StringEquals` und `StringNotEquals`.

Inhalt

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die AWS Backup verwendet, um die Zielressource zu erstellen; zum Beispiel: `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

ProtectedResourceType

Der AWS Ressourcentyp, der in einer Auswahl für Wiederherstellungstests enthalten ist, z. B. ein Amazon EBS-Volume oder eine Amazon RDS-Datenbank.

Akzeptierte unterstützte Ressourcentypen sind u. a.:

- `Aurora` für Amazon Aurora
- `DocumentDB` für Amazon DocumentDB (mit MongoDB-Kompatibilität)

- `DynamoDB` für Amazon DynamoDB
- `EBS` für Amazon Elastic Block Store
- `EC2` für Amazon Elastic Compute Cloud
- `EFS` für Amazon Elastic File System
- `FSx` für Amazon FSx
- `Neptune` für Amazon Neptune
- `RDS` für Amazon Relational Database Service
- `S3` für Amazon S3

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingSelectionName

Der eindeutige Name der Auswahl für Wiederherstellungstests, die zum entsprechenden Wiederherstellungstestplan gehört.

Typ: Zeichenfolge

Erforderlich: Ja

ProtectedResourceArns

Jede geschützte Ressource kann nach ihren spezifischen ARNs gefiltert werden, z. B. `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` oder nach einem Platzhalter, etwa `ProtectedResourceArns: ["*"]`, nicht jedoch nach beidem.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

ProtectedResourceConditions

Wenn Sie den Platzhalter angegeben haben ProtectedResourceArns, können Sie Ressourcenbedingungen wie z. B. `ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]` angeben.

Typ: ProtectedResourceConditions Objekt

Erforderlich: Nein

RestoreMetadataOverrides

Sie können bestimmte Schlüssel für Wiederherstellungsmetadaten überschreiben, indem Sie den Parameter `RestoreMetadataOverrides` in den Hauptteil von `RestoreTestingSelection` aufnehmen. Tag-Schlüsselwerte unterscheiden nicht zwischen Groß-/Kleinschreibung.

Sehen Sie sich die vollständige Liste der abgeleiteten Metadaten für Wiederherstellungstests an.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ValidationWindowHours

Dies ist die Anzahl der Stunden (1 bis 168), die für die Ausführung eines Überprüfungsskripts für die Daten zur Verfügung stehen. Die Daten werden nach Abschluss des Validierungsskripts oder nach Ablauf des angegebenen Aufbewahrungszeitraums gelöscht, je nachdem, was zuerst eintritt.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForGet

Service: AWS Backup

Dies enthält Metadaten zu einer Auswahl für Wiederherstellungstests.

Inhalt

CreationTime

Das Datum und die Uhrzeit der Erstellung einer Wiederherstellungstest-Auswahl im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

Erforderlich: Ja

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die AWS Backup verwendet, um die Zielressource zu erstellen; zum Beispiel: `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

ProtectedResourceType

Der AWS Ressourcentyp, der in einer Auswahl für Ressourcentests enthalten ist, z. B. ein Amazon EBS-Volume oder eine Amazon RDS-Datenbank.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingPlanName

Das RestoreTestingPlanName ist eine eindeutige Zeichenfolge, die dem Namen des Wiederherstellungstestplans entspricht.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingSelectionName

Der eindeutige Name der Wiederherstellungstestauswahl, die zum zugehörigen Wiederherstellungstestplan gehört.

Typ: Zeichenfolge

Erforderlich: Ja

CreatorRequestId

Dies identifiziert die Anforderung und ermöglicht die Wiederholung fehlgeschlagener Anforderungen, ohne dass das Risiko besteht, dass der Vorgang zweimal ausgeführt wird. Wenn die Anforderung eine `CreatorRequestId` enthält, der einem vorhandenen Backup-Plan entspricht, wird dieser Plan zurückgegeben. Dieser Parameter ist optional.

Wenn dieser Parameter verwendet wird, muss er 1 bis 50 alphanumerische Zeichen oder „-_“ enthalten. Zeichen.

Typ: Zeichenfolge

Erforderlich: Nein

ProtectedResourceArns

Sie können bestimmte ARNs, z. B. `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, oder einen Platzhalter, etwa `ProtectedResourceArns: ["*"]`, angeben, nicht jedoch beides.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

ProtectedResourceConditions

In einer Auswahl für Ressourcentests filtert dieser Parameter nach bestimmten Bedingungen wie `StringEquals` oder `StringNotEquals`.

Typ: ProtectedResourceConditions Objekt

Erforderlich: Nein

RestoreMetadataOverrides

Sie können bestimmte Schlüssel für Wiederherstellungsmetadaten überschreiben, indem Sie den Parameter `RestoreMetadataOverrides` in den Hauptteil von `RestoreTestingSelection` aufnehmen. Tag-Schlüsselwerte unterscheiden nicht zwischen Groß-/Kleinschreibung.

Sehen Sie sich die vollständige Liste der abgeleiteten Metadaten für Wiederherstellungstests an.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ValidationWindowHours

Dies ist die Anzahl der Stunden (1 bis 168), die für die Ausführung eines Überprüfungsskripts für die Daten zur Verfügung stehen. Die Daten werden nach Abschluss des Validierungsskripts oder nach Ablauf des angegebenen Aufbewahrungszeitraums gelöscht, je nachdem, was zuerst eintritt.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForList

Service: AWS Backup

Dies enthält Metadaten zu einer Auswahl für Wiederherstellungstests.

Inhalt

CreationTime

Das Datum und die Uhrzeit der Erstellung einer Wiederherstellungstest-Auswahl im Unix-Zeitformat und in der koordinierten Weltzeit (UTC). Der Wert von `CreationTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

Erforderlich: Ja

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die AWS Backup verwendet, um die Zielressource zu erstellen; zum Beispiel: `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

ProtectedResourceType

Der AWS Ressourcentyp, der in einer Auswahl für Wiederherstellungstests enthalten ist, z. B. ein Amazon EBS-Volume oder eine Amazon RDS-Datenbank.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingPlanName

Eine eindeutige Zeichenfolge, die dem Namen des Wiederherstellungstestplans entspricht.

Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name darf nur alphanumerische Zeichen und Unterstriche enthalten. Die maximale Länge beträgt 50.

Typ: Zeichenfolge

Erforderlich: Ja

RestoreTestingSelectionName

Eindeutiger Name einer Auswahl für Wiederherstellungstests.

Typ: Zeichenfolge

Erforderlich: Ja

ValidationWindowHours

Dieser Wert gibt die Zeit in Stunden an, für die Daten nach einem Wiederherstellungstest aufbewahrt werden, so dass die optionale Validierung abgeschlossen werden kann.

Der akzeptierte Wert ist eine Ganzzahl zwischen 0 und 168 (das Stundenäquivalent von sieben Tagen).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForUpdate

Service: AWS Backup

Dies enthält Metadaten zu einer Auswahl für Wiederherstellungstests.

Inhalt

IamRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die AWS Backup verwendet, um die Zielressource zu erstellen; zum Beispiel: `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Nein

ProtectedResourceArns

Sie können eine Liste bestimmter ARNs, z. B. `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, oder einen Platzhalter, etwa `ProtectedResourceArns: ["*"]`, angeben, nicht jedoch beides.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

ProtectedResourceConditions

Die Bedingungen, die Sie für Ressourcen in Ihrem Wiederherstellungstestplan mithilfe von Tags definieren.

z. B. `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Bei Bedingungsoperatoren wird zwischen Groß- und Kleinschreibung unterschieden.

Typ: ProtectedResourceConditions Objekt

Erforderlich: Nein

RestoreMetadataOverrides

Sie können bestimmte Schlüssel für Wiederherstellungsmetadaten überschreiben, indem Sie den Parameter `RestoreMetadataOverrides` in den Hauptteil von `RestoreTestingSelection` aufnehmen. Tag-Schlüsselwerte unterscheiden nicht zwischen Groß-/Kleinschreibung.

Sehen Sie sich die vollständige Liste der abgeleiteten Metadaten für Wiederherstellungstests an.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

ValidationWindowHours

Dieser Wert gibt die Zeit in Stunden an, für die Daten nach einem Wiederherstellungstest aufbewahrt werden, so dass die optionale Validierung abgeschlossen werden kann.

Der akzeptierte Wert ist eine Ganzzahl zwischen 0 und 168 (das Stundenäquivalent von sieben Tagen).

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AWS Backup gateway

Die folgenden Datentypen werden von AWS Backup gateway unterstützt:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag

- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Service: AWS Backup gateway

Beschreibt ein Intervall für die Bandbreitenratenbegrenzung für ein Gateway. Ein Zeitplan für die Bandbreitenratenbegrenzung besteht aus einem oder mehreren Intervallen für die Bandbreitenratenbegrenzung. Ein Intervall für die Bandbreitenbegrenzung definiert einen Zeitraum an einem oder mehreren Wochentagen, in dem Bandbreitenbegrenzungen für Uploads, Downloads oder beides festgelegt wurden.

Inhalt

DaysOfWeek

Die Wochentagskomponente des Intervalls für die Bandbreitenbegrenzung, dargestellt als Ordnungszahlen von 0 bis 6, wobei 0 für Sonntag und 6 für Samstag steht.

Typ: Array von ganzen Zahlen

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 7 Elemente.

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 6.

Erforderlich: Ja

EndHourOfDay

Die Stunde des Tages, an dem das Intervall für die Bandbreitenbegrenzung beendet werden soll.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert 23.

Erforderlich: Ja

EndMinuteOfHour

Die Minute der Stunde, in der das Intervall für die Bandbreitenbegrenzung beendet werden soll.

> **Important**
>
> Das Intervall zur Bandbreitenbegrenzung endet, sobald die Minute vorüber ist. Um ein Intervall am Ende einer Stunde zu beenden, verwenden Sie den Wert 59.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 59.

Erforderlich: Ja

StartHourOfDay

Die Stunde des Tages, an dem das Intervall für die Bandbreitenratenbegrenzung gestartet werden soll.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert 23.

Erforderlich: Ja

StartMinuteOfHour

Die Minute der Stunde, in der das Intervall für die Bandbreitenbegrenzung gestartet werden soll. Das Intervall beginnt am Anfang dieser Minute. Um ein Intervall genau am Anfang der Stunde zu beginnen, verwenden Sie den Wert `0`.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 59.

Erforderlich: Ja

AverageUploadRateLimitInBitsPerSec

Die durchschnittliche Upload-Ratenbegrenzungskomponente des Bandbreitenbegrenzungsintervalls in Bits pro Sekunde. Dieses Feld erscheint nicht in der Antwort, wenn die Upload-Ratenbegrenzung nicht festgelegt ist.

Type: Long

Gültiger Bereich: Mindestwert 51 200. Maximaler Wert von 8000000000000.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Gateway

Service: AWS Backup gateway

Ein Gateway ist eine AWS Backup Gateway-Appliance, die im Netzwerk des Kunden läuft, um eine nahtlose Konnektivität zum Backup-Speicher in der AWS Cloud zu gewährleisten.

Inhalt

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den `ListGateways` Vorgang, um eine Liste von Gateways für Ihr Konto und AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

GatewayDisplayName

Der Anzeigename des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

GatewayType

Der Typ des Gateways.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VM`

Erforderlich: Nein

HypervisorId

Die Hypervisor-ID des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Erforderlich: Nein

LastSeenTime

Der Zeitpunkt, zu dem das AWS Backup Gateway das letzte Mal mit dem Gateway kommuniziert hat, im Unix-Format und UTC-Zeit.

Typ: Zeitstempel

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GatewayDetails

Service: AWS Backup gateway

Die Details des Gateways.

Inhalt

GatewayArn

Der Amazon-Ressourcenname (ARN) des Gateways. Verwenden Sie den `ListGateways`-Vorgang, um eine Liste von Gateways für Ihr Konto und die AWS-Region zurückzugeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Die maximale Länge beträgt 180.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

GatewayDisplayName

Der Anzeigename des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

GatewayType

Der Typ des Gateways.

Typ: Zeichenfolge

Zulässige Werte: `BACKUP_VM`

Erforderlich: Nein

HypervisorId

Die Hypervisor-ID des Gateways.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Erforderlich: Nein

LastSeenTime

Details, die zeigen, wann das AWS Backup Gateway das letzte Mal mit der Cloud kommuniziert hat, im Unix-Format und UTC-Zeit.

Typ: Zeitstempel

Erforderlich: Nein

MaintenanceStartTime

Gibt die Startzeit der wöchentlichen Wartung Ihres Gateways einschließlich dem Wochentag und der Uhrzeit zurück. Beachten Sie, dass sich die Werte auf die Zeitzone des Gateways beziehen. Kann wöchentlich oder monatlich sein.

Typ: MaintenanceStartTime Objekt

Erforderlich: Nein

NextUpdateAvailabilityTime

Details zur Verfügbarkeitszeit des nächsten Updates für das Gateway.

Typ: Zeitstempel

Erforderlich: Nein

VpcEndpoint

Der DNS-Name für den Virtual Private Cloud (VPC)-Endpunkt, den das Gateway für die Verbindung mit der Cloud für das Backup-Gateway herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Hypervisor

Service: AWS Backup gateway

Stellt die Berechtigungen des Hypervisors dar, mit denen das Gateway eine Verbindung herstellen wird.

Ein Hypervisor ist Hardware, Software oder Firmware, die virtuelle Maschinen erstellt und verwaltet und ihnen Ressourcen zuweist.

Inhalt

Host

Der Serverhost des Hypervisors. Dies kann entweder eine IP-Adresse oder ein vollständig qualifizierter Domänenname (Fully Qualified Domain Name, FQDN) sein.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 128 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

KmsKeyArn

Der Amazon-Ressourcenname (ARN) des AWS Key Management Service zur Verschlüsselung des Hypervisors verwendeten.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Erforderlich: Nein

Name

Der Name des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

State

Der Status des Hypervisors.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | ONLINE | OFFLINE | ERROR`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

HypervisorDetails

Service: AWS Backup gateway

Dies sind die Details des angegebenen Hypervisors. Ein Hypervisor ist Hardware, Software oder Firmware, die virtuelle Maschinen erstellt und verwaltet und ihnen Ressourcen zuweist.

Inhalt

Host

Der Serverhost des Hypervisors. Dies kann entweder eine IP-Adresse oder ein vollständig qualifizierter Domänenname (Fully Qualified Domain Name, FQDN) sein.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 128 Zeichen.

Pattern: `^.+$`

Erforderlich: Nein

HypervisorArn

Der Amazon-Ressourcenname (ARN) des Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

KmsKeyArn

Der Amazon-Ressourcenname (ARN) des AWS KMS , der zum Verschlüsseln des Hypervisors verwendet wird.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Erforderlich: Nein

LastSuccessfulMetadataSyncTime

Dies ist der Zeitpunkt, an dem die letzte erfolgreiche Synchronisierung von Metadaten stattgefunden hat.

Typ: Zeitstempel

Erforderlich: Nein

LatestMetadataSyncStatus

Dies ist der letzte Status für die angegebene Metadatensynchronisierung.

Typ: Zeichenfolge

Zulässige Werte: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Erforderlich: Nein

LatestMetadataSyncStatusMessage

Dies ist der letzte Status für die angegebene Metadatensynchronisierung.

Typ: Zeichenfolge

Erforderlich: Nein

LogGroupArn

Der Amazon-Ressourcenname (ARN) der Gruppe von Gateways im angeforderten Protokoll.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 2048 Zeichen.

Pattern: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Erforderlich: Nein

Name

Dies ist der Name des angegebenen Hypervisors.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

State

Dies ist der aktuelle Status des angegebenen Hypervisors.

Die möglichen Zustände sind`PENDING`, `ONLINEOFFLINE`, oder`ERROR`.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | ONLINE | OFFLINE | ERROR`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MaintenanceStartTime

Service: AWS Backup gateway

Gibt die Startzeit der wöchentlichen Wartung Ihres Gateways einschließlich dem Wochentag und der Uhrzeit zurück. Beachten Sie, dass sich die Werte auf die Zeitzone des Gateways beziehen. Kann wöchentlich oder monatlich sein.

Inhalt

HourOfDay

Die Stundenkomponente der Wartungsstartzeit, dargestellt als hh, wobei hh die Stunde (0 bis 23) ist. Die Stunde des Tages liegt in der Zeitzone des Gateways.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert 23.

Erforderlich: Ja

MinuteOfHour

Die Minutenkomponente der Startzeit der Wartung, dargestellt als mm, wobei mm die Minute (0 bis 59) ist. Die Minute der Stunde liegt in der Zeitzone des Gateways.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 59.

Erforderlich: Ja

DayOfMonth

Der Tag des Monats der Wartungsstartzeit wird als Ordnungszahl zwischen 1 und 28 dargestellt, wobei 1 den ersten Tag des Monats und 28 den letzten Tag des Monats repräsentiert.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 31.

Erforderlich: Nein

DayOfWeek

Eine Ordinalzahl zwischen 0 und 6, die den Wochentag darstellt, wobei 0 für Sonntag und 6 für Samstag steht. Der Wochentag liegt in der Zeitzone des Gateways.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximaler Wert von 6.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

Service: AWS Backup gateway

Ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen verwalten, filtern und suchen können. Erlaubte Zeichen sind: UTF-8-Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: + - = . _ : /.

Inhalt

Key

Der Schlüssel-Teil des Schlüssel-Wert-Paars eines Tags. Der Schlüssel darf nicht mit `aws:` beginnen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 128 Zeichen.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Erforderlich: Ja

Value

Der Wert-Teil des Schlüssel-Wert-Paares eines Tags.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[^\x00]*$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

VirtualMachine

Service: AWS Backup gateway

Eine virtuelle Maschine, die sich auf einem Hypervisor befindet.

Inhalt

HostName

Der Hostname der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

HypervisorId

Die ID des Hypervisors der virtuellen Maschine.

Typ: Zeichenfolge

Erforderlich: Nein

LastBackupDate

Das letzte Datum, an dem eine virtuelle Maschine gesichert wurde, im Unix-Format und UTC-Zeit.

Typ: Zeitstempel

Erforderlich: Nein

Name

Der Name der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

Path

Der Pfad der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 4096 Zeichen.

Pattern: `^[^\x00]+$`

Erforderlich: Nein

ResourceArn

Der Amazon-Ressourcenname (ARN) der virtuellen Maschine. Beispiel, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VirtualMachineDetails

Service: AWS Backup gateway

Ihre `VirtualMachine`-Objekte, sortiert nach Amazon-Ressourcennamen (ARNs).

Inhalt

HostName

Der Hostname der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

HypervisorId

Die ID des Hypervisors der virtuellen Maschine.

Typ: Zeichenfolge

Erforderlich: Nein

LastBackupDate

Das letzte Datum, an dem eine virtuelle Maschine gesichert wurde, im Unix-Format und UTC-Zeit.

Typ: Zeitstempel

Erforderlich: Nein

Name

Der Name der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `^[a-zA-Z0-9-]*$`

Erforderlich: Nein

Path

Der Pfad der virtuellen Maschine.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 4096 Zeichen.

Pattern: `^[^\x00]+$`

Erforderlich: Nein

ResourceArn

Der Amazon-Ressourcenname (ARN) der virtuellen Maschine. Beispiel, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 50. Maximale Länge beträgt 500 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erforderlich: Nein

VmwareTags

Dies sind die Details der VMware-Tags, die der angegebenen virtuellen Maschine zugeordnet sind.

Typ: Array von VmwareTag-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

VmwareTag

Service: AWS Backup gateway

Ein VMware-Tag ist ein einer bestimmten virtuellen Maschine zugeordneter Tag. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen verwalten, filtern und suchen können.

Der Inhalt von VMware-Tags kann AWS Tags zugeordnet werden.

Inhalt

VmwareCategory

Das ist die Kategorie von VMware.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 80 Zeichen.

Erforderlich: Nein

VmwareTagDescription

Dies ist eine benutzerdefinierte Beschreibung eines VMware-Tags.

Typ: Zeichenfolge

Erforderlich: Nein

VmwareTagName

Dies ist der benutzerdefinierte Name eines VMware-Tags

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 80 Zeichen.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

VmwareToAwsTagMapping

Service: AWS Backup gateway

Dadurch wird die Zuordnung der VMware-Tags zu den entsprechenden AWS Tags angezeigt.

Inhalt

AwsTagKey

Der Schlüsselteil des Schlüssel-Wert-Paares des AWS Tags.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 128 Zeichen.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Erforderlich: Ja

AwsTagValue

Der Wertteil des AWS Schlüssel-Wert-Paares des Tags.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[^\x00]*$`

Erforderlich: Ja

VmwareCategory

Das ist die Kategorie von VMware.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 80 Zeichen.

Erforderlich: Ja

VmwareTagName

Dies ist der benutzerdefinierte Name eines VMware-Tags

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 80 Zeichen.

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Geläufige Parameter

Die folgende Liste enthält die Parameter, die alle Aktionen zum Signieren von Signature-Version-4-Anforderungen mit einer Abfragezeichenfolge verwenden. Alle aktionsspezifischen Parameter werden im Thema für diese Aktion aufgelistet. Weitere Informationen zur Verwendung von Signature Version 4 finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Action

Die auszuführende Aktion.

Typ: Zeichenfolge

Erforderlich: Ja

Version

Die API-Version, für die die Anforderung geschrieben wurde, ausgedrückt im Format JJJJ-MM-TT.

Typ: Zeichenfolge

Erforderlich: Ja

X-Amz-Algorithm

Der Hashalgorithmus, den Sie zum Erstellen der Anforderungssignatur verwendet haben.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Zulässige Werte: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

Der Wert des Anmeldeinformationsumfangs. Dabei handelt es sich um eine Zeichenfolge, die Ihren Zugriffsschlüssel, das Datum, die gewünschte Region und eine Zeichenfolge zur Beendigung („aws4_request“) beinhaltet. Der Wert wird im folgenden Format ausgedrückt: Zugriffsschlüssel/JJJJMMTT/Region/Service/aws4_request.

Weitere Informationen finden Sie unter Erstellen einer signierten AWS-API-Anfrage im IAM-Benutzerhandbuch.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Date

Das Datum, das zum Erstellen der Signatur verwendet wird. Das Format muss das ISO 8601-Basisformat (JJJJMMTT'T'SSMMSS'Z') sein. Die folgende Datumszeit ist beispielsweise ein gültiger X-Amz-Date-Wert: `20120325T120000Z`.

Bedingung: X-Amz-Date ist bei allen Anforderungen optional. Damit kann das Datum überschrieben werden, das zum Signieren von Anforderungen verwendet wird. Wenn der Date-Header im ISO 8601-Basisformat angegeben ist, ist X-Amz-Date nicht erforderlich. Wenn X-Amz-Date verwendet wird, überschreibt es immer den Wert des Date-Headers. Weitere Informationen finden Sie unter Elemente einer AWS-API-Anfragesignatur im IAM-Benutzerhandbuch.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Security-Token

Das temporäre Sicherheitstoken, das durch einen Anruf von AWS Security Token Service (AWS STS) abgerufen wurde. Eine Liste der Services, die temporäre Sicherheits-Anmeldeinformationen

von AWS STS unterstützen, finden Sie im IAM-Benutzerhandbuch unter AWS-Services, die mit IAM funktionieren.

Bedingung: Wenn Sie temporäre Sicherheits-Anmeldeinformationen von AWS STS nutzen, müssen Sie das Sicherheitstoken einschließen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Signature

Gibt die hex-codierte Signatur an, die aus der zu signierenden Zeichenfolge und dem abgeleiteten Signaturschlüssel berechnet wurde.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-SignedHeaders

Gibt alle HTTP-Header an, die als Teil der kanonischen Anforderung enthalten waren. Weitere Informationen zur Angabe signierter Header finden Sie unter Erstellen einer signierten AWS-API-Anfrage im IAM-Benutzerhandbuch.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

Häufige Fehler

In diesem Abschnitt sind Fehler aufgeführt, die häufig bei den API-Aktionen aller AWS-Services auftreten. Informationen zu Fehlern, die spezifisch für eine API-Aktion für diesen Service sind, finden Sie unter dem Thema für diese API-Aktion.

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

HTTP Status Code: 400

IncompleteSignature

Die Anforderungssignatur entspricht nicht den AWS-Standards.

HTTP Status Code: 400

InternalFailure

Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.

HTTP Status Code: 500

InvalidAction

Die angeforderte Aktion oder Operation ist ungültig. Überprüfen Sie, ob die Aktion ordnungsgemäß eingegeben wurde.

HTTP Status Code: 400

InvalidClientTokenId

Das angegebene X.509-Zertifikat oder die AWS-Zugriffsschlüssel-ID ist nicht in unseren Datensätzen vorhanden.

HTTP Status Code: 403

NotAuthorized

Sie haben keine Berechtigung zum Ausführen dieser Aktion.

HTTP Status Code: 400

OptInRequired

Die AWS-Zugriffsschlüssel-ID benötigt ein Abonnement für den Service.

HTTP Status Code: 403

RequestExpired

Die Anforderung hat den Service mehr als 15 Minuten nach dem Datumsstempel oder mehr als 15 Minuten nach dem Ablaufdatum der Anforderung erreicht (z. B. für vorsignierte URLs) oder der Datumsstempel auf der Anforderung liegt mehr als 15 Minuten in der Zukunft.

HTTP Status Code: 400

ServiceUnavailable

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 503

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

HTTP Status Code: 400

ValidationError

Die Eingabe erfüllt nicht die von einem AWS-Service definierten Einschränkungen.

HTTP Status Code: 400

Dokumenthistorie für AWS Backup

- API-Version: 6. Dezember 2023
- Letzte Aktualisierung der Dokumentation: 3. Juni 2024

In der folgenden Tabelle sind alle AWS Backup Starts seit dem Start des Dienstes im Januar 2019 bis heute aufgeführt. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed oben abonnieren.

Änderung	Beschreibung	Datum
AWS Backup Merkmal Regionale Expansion	AWS Backup Die Unterstützung der Amazon EBS-Snapshot-Archivierungsstufe ist jetzt in den folgenden Regionen verfügbar: • China (Peking) • China (Ningxia) • AWS GovCloud (USA, Westen) • AWS GovCloud (US-Ost)	3. Juni 2024
Aktualisierte von AWS verwaltete Richtlinien	AWS Backup den folgenden verwalteten Richtlinien wurden Berechtigungen `backup:TagResource` hinzugefügt: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	17. Mai 2024

Änderung	Beschreibung	Datum
	Weitere Informationen finden Sie unter Richtlinienaktualisierungen.	
AWS Backup jetzt in der Region Kanada West (Calgary) erhältlich	Backup und Wiederherstellung für viele Ressourcentypen sind jetzt in AWS-Region Canada West (Calgary) verfügbar. Informationen zu kompatiblen Backup-Funktionen finden Sie unter Verfügbarkeit von Funktionen von AWS-Region. Informationen zu unterstützten Ressourcentypen finden Sie unter Unterstützte Dienste von AWS-Region.	14. März 2024
Der verwalteten Richtlinie wurden Berechtigungen hinzugefügt	AWS Backup Die Richtlinie wurde aktualisiert, AWSServiceRolePolicyForBackupRestoreTestingindem Berechtigungen zur Unterstützung zusätzlicher Ressourcentypen innerhalb der Funktion zum Testen der Wiederherstellung hinzugefügt wurden. Weitere Informationen zu den hinzugefügten spezifischen Berechtigungen finden Sie unter Richtlinienaktualisierungen.	14. Februar 2024

Änderung	Beschreibung	Datum
Backup- und Wiederherstellungsunterstützung für FSx for FlexGroup ONTAP-Volumes	AWS Backup unterstützt jetzt die Sicherung und Wiederherstellung von FSx for FlexGroup ONTAP-Volumes in den meisten. AWS-Regionen Weitere Informationen finden Sie unter Wiederherstellen eines Amazon-FSx-Dateisystems. .	10. Januar 2024
Unterstützung für SAP-HANA-HA-Backup und -Wiederherstellung	AWS Backup bietet jetzt Unterstützung für SAP HANA-Hochverfügbarkeitsdatenbanken auf Amazon EC2 EC2-Backup und -Wiederherstellung. Weitere Informationen finden Sie unter Backups für SAP HANA auf Amazon EC2 und Wiederherstellen eines SAP-HANA-Hochverfügbarkeitssystems	21. Dezember 2023

Änderung	Beschreibung	Datum
AWS Backup Audit Manager Manager-Steuerung für Wiederherstellungstests	AWS Backup Audit Manager bietet jetzt die Steuerung Wiederherstellungszeit für Ressourcen, die das Ziel erreichen, um die Überwachung der Wiederherstellungszeiten zu unterstützen. Dieses Steuerelement prüft, ob die Wiederherstellungszeit einer Ressource der Zieldauer entspricht. Weitere Informationen finden Sie unter Steuerelemente und Abhilfemaßnahmen und Prüfung eines Wiederherstellungstests.	18. Dezember 2023
Unterstützung für Amazon EBS Cold Storage	AWS Backup unterstützt jetzt den Übergang von EBS-Backups vom Warm- zum Kaltspeicher. Weitere Informationen finden Sie unter • Amazon EBS Archive Tier für Cold Storage • Lebenszyklus und Speicherstufen • Erstellen eines Backup-Plans	8. November 2023

Änderung	Beschreibung	Datum
Einführung zu Wiederher stellungstests	AWS Backup führt Wiederher stellungstests ein, die eine automatische und regelmäßige Bewertung der Durchführbarkeit von Wiederherstellungen sowie die Möglichkeit bieten, die Dauer von Wiederherstellungs aufträgen zu überwachen. Weitere Informationen finden Sie unter Wiederherstellungs tests.	8. November 2023

Änderung	Beschreibung	Datum
Aktualisierte von AWS verwaltete Richtlinien	AWS Backup hat die Berechtigungen `ec2:DescribeSnapshotTierStatus` und `ec2:ModifySnapshotTier` zu den verwalteten Richtlinien hinzugefügt `AWSBackupServiceRolePolicyForBackups` und`AWSBackupServiceLinkedRolePolicyForBackup` . AWS Backup hat auch die Berechtigungen `ec2:DescribeSnapshotTierStatus` und `ec2:RestoreSnapshotTier` die verwaltete Richtlinie hinzugefügt `AWSBackupServiceRolePolicyForRestores` . Diese Berechtigungen sind erforderlich, damit Benutzer die Möglichkeit haben, mit gespeicherten Amazon EBS-Ressourcen AWS Backup auf Archivspeicher umzustellen und Ressourcen aus der Archivspeicherebene wiederherzustellen. Weitere Informationen finden Sie unter Richtlinien-Updates.	8. November 2023

Änderung	Beschreibung	Datum
Es wurde eine Weitergabe-Rollenberechtigung hinzugefügt, um Wiederherstellungstests zu unterstützen.	AWS Backup `restore-testing.backup.amazonaws.com` zu `IamPassRolePermissions` und `IamCreateServiceLinkedRolePermissions` hinzugefügt. Dieser Zusatz ist erforderlich AWS Backup , um Wiederherstellungstests im Auftrag von Kunden durchzuführen.	8. November 2023

Änderung	Beschreibung	Datum
Es wurde eine neue serviceverknüpfte Rolle hinzugefügt	AWS Backup hat die neue dienstbezogene Rolle mit dem Namen hinzugefügt `AWSServiceRoleForBackupRestoreTesting`, die Backup-Berechtigungen für die Durchführung von Wiederherstellungstests bereitstellt. Diese neue dienstbezogene Rolle bietet AWS Backup die für die Durchführung von Wiederherstellungstests erforderlichen Berechtigungen. Die Berechtigungen umfassen die Aktionen `list, read, and write` für die folgenden Services, die in Wiederherstellungstests aufgenommen werden sollen: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx für ONTAP, FSx für OpenZFS, Amazon Neptune, Amazon RDS und Amazon S3.	8. November 2023

Änderung	Beschreibung	Datum
Neues Job-Metrik-Dashboard in der AWS Backup Konsole	In der AWS Backup Konsole wird jetzt ein Job-Dashboard angezeigt, das die Überwachung des Backup-Zustands in großem Maßstab vereinfacht. Es verfügt über eine neue visuelle Benutzeroberfläche und aggregierte Backup-, Kopier- und Wiederherstellungsmetriken für Dienste, die von unterstützt werden. AWS Backup Das Job-Dashboard ist in allen Regionen verfügbar, in denen AWS Backup Audit Manager verfügbar ist. Regionen, die nicht aufgeführt sind, können weiterhin auf das CloudWatch Dashboard zugreifen. Weitere Informationen finden Sie unter AWS Backup -Konsolen-Dashboards.	15. November 2023

Änderung	Beschreibung	Datum
Support für verschachtelte Stack-Backups	AWS Backup hat seine Unterstützung für Backups von AWS CloudFormation Ressourcen erweitert. Ihre CloudFormation Anwendungsstapel, die verschachtelte Stacks enthalten, können in Ihre Backups aufgenommen werden. Weitere Informationen finden Sie unter CloudFormation - Stack-Backups.	8. November 2023
Unterstützung für Amazon S3 in China (Peking) und China (Ningxia)	AWS Backup Unterstützung für Amazon S3 ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	26. Oktober 2023
Support für kontinuierliche Amazon Aurora Aurora-Backups und oint-in-time P-Wiederherstellung	AWS Backup unterstützt jetzt kontinuierliche point-in-time Backups und Wiederherstellungen (PITR) für Aurora-Ressourcen. Weitere Informationen finden Sie unter Kontinuierliche Backups und oint-in-time P-Wiederherstellung.	07. September 2023

Änderung	Beschreibung	Datum
AWS CloudFormation Stacks unterstützen den Ausschluss von Ressourcen	AWS Backup unterstützt jetzt die Option, ausgewählte Ressourcen von Ihrem AWS CloudFormation Stack auszuschließen. Weitere Informationen finden Sie unter AWS CloudFormation -Stack-Backups.	6. September 2023
Regeln für Backup-Pläne sorgen für Flexibilität in der Zeitzone	AWS Backup Planregeln können jetzt eine bestimmte Zeitzone für Backup-Fenster haben. Weitere Informationen finden Sie unter Verwalten von Backup-Plänen.	28. August 2023
AWS Backup jetzt in der Region Israel (Tel Aviv) verfügbar	Viele AWS Backup Funktionen sind jetzt in der neuen Region Israel (Tel Aviv) verfügbar. Besuchen Sie Verfügbarkeit von Features nach AWS-Region, um herauszufinden, welche Ressourcen unterstützt werden.	22. August 2023

Änderung	Beschreibung	Datum
AWS Backup Audit Manager unterstützt jetzt delegierte Administratorkonten	AWS Backup Auf die Generierung von Audit Manager Manager-Berichten können jetzt delegierte Administratorkonten zugreifen . Weitere Informationen finden Sie unter • Prüfen Sie Backups und erstellen Sie Berichte mit AWS Backup Audit Manager • Arbeiten mit Auditberichten • Delegierter Administrator	16. August 2023
Vorschau des logischen Air-Gapped-Backup-Tresors	AWS Backup bietet jetzt eine Vorschau auf eine neue Art von Backup-Tresor als Ergänzung zu Datenschu tzmaßnahmen. Weitere Informationen finden Sie unter Logische Air-Gapped-Tresore (Vorschau).	08. August 2023
AWS Backup verbessert Amazon S3 S3-Backups	AWS Backup hat die Leistungs-, Größen- und Geschwindigkeitsfunktionen für S3-Bucket-Backups verbessert. Weitere Informationen finden Sie unter Amazon-S3-Backups.	1. August 2023

Änderung	Beschreibung	Datum
Markierung des Wiederherstellungs-Feature jetzt in Regionen in China verfügbar	Tags, die Teil eines Backups sind, können jetzt kopiert werden, wenn Sie einen Wiederherstellungsauftrag in den Regionen China (Peking) oder China (Ningxia) erstellen. Weitere Informationen finden Sie unter Tags bei Wiederherstellungsaufträgen kopieren.	17. Juli 2023
AWS Backup unterstützt jetzt Amazon S3 in weiteren Regionen	AWS Backup Support für Amazon S3 ist jetzt in den Regionen Europa (Spanien), Europa (Zürich), Asien-Pazifik (Hyderabad) und Asien-Pazifik (Melbourne) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	6. Juli 2023

Änderung	Beschreibung	Datum
Kontoübergreifendes Kopieren auf weitere Regionen erweitert	AWS Backup unterstützt jetzt kontenübergreifende Backup-Kopien der meisten Ressourcen in den folgenden Regionen: Asien-Pazifik (Jakarta), Naher Osten (Bahrain), Asien-Pazifik (Hongkong), Afrika (Kapstadt), Europa (Mailand), Asien-Pazifik (Osaka), Naher Osten (VAE), Europa (Spanien), Europa (Zürich), Asien-Pazifik (Hyderabad) und Asien-Pazifik (Melbourne). Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	5. Juli 2023
Backup Audit Manager in GovCloud Regionen verfügbar	AWS Backup hat AWS Backup Audit Manager auf AWS GovCloud (US-Ost) und AWS GovCloud (US-West) ausgeweitet. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	29. Juni 2023

Änderung	Beschreibung	Datum
Kontoübergreifende Verwaltung jetzt in Regionen verfügbar GovCloud	AWS Backup unterstützt jetzt die kontenübergreifende Verwaltung von Ressourcen in AWS GovCloud (USA-Ost) und AWS GovCloud (US-West). Weitere Informationen finden Sie unter Verwalten von AWS Backup -Ressourcen über mehrere AWS -Konten hinweg.	29. Juni 2023
Unterstützung für regionsübergreifendes Kopieren von Amazon Aurora in weiteren Regionen	AWS Backup unterstützt jetzt regionsübergreifende Backup-Kopien für Aurora-Cluster in und aus den folgenden Regionen: Asien-Pazifik (Jakarta), Naher Osten (Bahrain), Asien-Pazifik (Hongkong), Afrika (Kapstadt), Europa (Mailand), Naher Osten (VAE), Europa (Spanien), Europa (Zürich), Asien-Pazifik (Hyderabad) und Asien-Pazifik (Melbourne).	5. Juni 2023

Änderung	Beschreibung	Datum
Kopieren von Tags bei der Wiederherstellung	Tags, die Teil eines Backups sind, können jetzt kopiert werden, wenn Sie einen Wiederherstellungsauftrag erstellen. Weitere Informationen finden Sie unter Tags bei Wiederherstellungsaufträgen kopieren.	22. Mai 2023
AWS Backup lässt sich in Benutzerbenachrichtigungen integrieren AWS	Sie können jetzt festlegen, ob Sie Benachrichtigungen zu Backup-, Kopier- und Wiederherstellungsereignissen über die AWS -Benutzerbenachrichtigungskonsole erhalten möchten. Weitere Informationen finden Sie unter Erste Schritte mit AWS Benutzerbenachrichtigungen.	10. Mai 2023
Regionsübergreifende Backups in vier neuen Regionen verfügbar	AWS Backup unterstützt jetzt regionsübergreifendes Backup in den Regionen Naher Osten (VAE), Europa (Spanien), Europa (Zürich) und Asien-Pazifik (Hyderabad).	28. April 2023

Änderung	Beschreibung	Datum
Erweiterte Unterstützung für regionsübergreifendes Kopieren AWS Backup	Regionsübergreifende Backups von Amazon-EFS-, VMware- und DynamoDB-Ressourcen können jetzt in den folgenden Regionen durchgeführt werden: Asien-Pazifik (Jakarta), Asien-Pazifik (Hongkong), Afrika (Kapstadt), Europa (Mailand) und Naher Osten (Bahrain).	28. April 2023
Amazon-S3-Backup und -Wiederherstellung in der Region Südamerika (São Paulo)	AWS Backup Unterstützung für Amazon S3 (Amazon Simple Storage Service) ist jetzt in der Region Südamerika (São Paulo) verfügbar. Weitere Informationen finden Sie unter Amazon-S3-Backups.	20. April 2023
AWS Backup expandiert in die Region Asien-Pazifik (Melbourne)	AWS Backup ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach AWS Regionen.	20. April 2023

Änderung	Beschreibung	Datum
Erweiterte regionale Unterstützung für Amazon S3	AWS Backup Unterstützung für Amazon S3 (Amazon Simple Storage Service) ist jetzt in den Regionen AWS GovCloud (USA Ost) und AWS GovCloud (USA West) verfügbar Weitere Informationen finden Sie unter Amazon-S3-Backups.	19. April 2023
Backup und Wiederherstellung von SAP HANA-Datenbanken auf Amazon-EC2-Instances	AWS Backup bietet jetzt in den meisten Regionen die Möglichkeit, SAP HANA-Datenbanken, die auf Amazon EC2 EC2-Instances laufen, zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Backup von SAP HANA-Datenbanken auf Amazon-EC2-Instances.	17. April 2023

Änderung	Beschreibung	Datum
AWS Backup jetzt in den Regionen Europa (Spanien) , Europa (Zürich) und Asien-Pazifik (Hyderabad) verfügbar	AWS Backup Der Support wurde auf neue Regionen ausgeweitet, darunter Europa (Spanien), Europa (Zürich) und Asien-Pazifik (Hyderaba d). Unterstützte Ressourcen können in diesen Regionen gesichert und wiederher gestellt werden. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach AWS Regionen.	13. April 2023
Die AWS verwaltete Richtlinie wurde aktualisiert `AWSBackup AuditAccess`	Die AWS verwaltete Richtlinie wurde aktualisiert AWSBackup AuditAccess. AWS Backup hat die Ressourcenauswahl innerhalb der API `config:De scribeComplianceBy ConfigRule` durch eine Wildcard-Ressource ersetzt. Weitere Informationen finden Sie unter Richtlinien-Updates für AWS Backup.	11. April 2023

Änderung	Beschreibung	Datum
Hypervisoren mit Amazon Logs CloudWatch	AWS Backup Gateway-Benutzer können jetzt Hypervisoren in Logs integrieren, um CloudWatch Protokolle zu verwalten. Weitere Informationen finden Sie unter Hypervisor-Konfiguration bearbeiten und Protokolle. CloudWatch	29. März 2023
Erweiterte regionale Unterstützung für Amazon S3	AWS Backup Support für Amazon S3 ist jetzt in den Regionen Asien-Pazifik (Jakarta) und Naher Osten (VAE) verfügbar.	22. März 2023
Verbesserung des inkrementellen Backups virtueller Maschinen	VMware-VM-Backups (virtuelle Maschinen), bei denen CBT-Datenprobleme (Changed Block Tracking) auftreten, enthalten jetzt zusätzliche Informationen zur Behebung und Fehlerbehebung. Weitere Informationen finden Sie unter Inkrementelle VM-Backups und Fehlerbehebung für Ihre virtuellen Maschinen.	15. März 2023

Änderung	Beschreibung	Datum
AWS Backup Unterstützung für mehrere Netzwerkadapter	AWS Backup Gateway unterstützt jetzt die Konfiguration mehrerer Netzwerkadapter Weitere Informationen zur Konfiguration Ihrer Netzwerkadapter finden Sie unter Konfigurieren des Gateway für mehrere NICs in VMware im -Entwicklerhandbuch.	08. März 2023
AWS Backup Unterstützung für vSphere 8	AWS Backup unterstützt jetzt die Sicherung und Wiederherstellung von virtuellen Maschinen, die auf VMware vSphere 8 ausgeführt werden. Weitere Informationen zu den unterstützten VMware-Optionen finden Sie unter Unterstützte VMs im AWS Backup -Entwicklerhandbuch.	08. März 2023
AWS Backup Audit Manager unterstützt Amazon RDS Multi-AZ-Backups	Backup Audit Manager bietet jetzt Unterstützung für Multi-AZ-Backups mit Amazon Relational Database Service. Weitere Informationen finden Sie unter So überprüfen Sie Backups und erstellen Berichte mit AWS Backup Audit Manager.	1. Februar 2023

Änderung	Beschreibung	Datum
AWS Backup bietet inkrementelles Backup für Amazon Timestream Timestream-Tabellen	AWS Backup bietet jetzt erweiterte Backup-Funktionen für Timestream-Backups . Backup-Pläne können jetzt inkrementelle Backups vorsehen, um den Zeitaufwand für das Backup von Timestream-Ressourcen zu verringern und die Speicherkosten zu senken. Weitere Informationen finden Sie unter Amazon-Timestream-Backups.	23. Januar 2023
AWS Backup jetzt in Dubai erhältlich	AWS Backup hat sich auf die Region Naher Osten (VAE) ausgeweitet. Unterstützte Ressourcen können in dieser Region gesichert und wiederhergestellt werden.	17. Januar 2023
Regionsübergreifendes Kopieren in weiteren Regionen verfügbar	AWS Backup bietet jetzt für die meisten Ressourcen regionsübergreifende Backups in den Regionen Asien-Pazifik (Jakarta), Naher Osten (Bahrain), Asien-Pazifik (Hongkong), Afrika (Kapstadt) und Europa (Mailand) an. Weitere Informationen finden Sie unter Erstellen von Backup-Kopien über AWS-Regionen hinweg.	21. Dezember 2022

Änderung	Beschreibung	Datum
Bandbreitenlimits und -drosselung des Backup-Gateways	AWS Backup Gateway ermöglicht nun Beschränkungen des Upload-Durchsatzes von Gateways, AWS Backup um die Menge der vom Gateway verwendeten Netzwerkbandbreite zu kontrollieren. Zur Unterstützung dieser Funktion AWS Backup wurden verwaltete Richtlinien erstellt und aktualisiert, darunter `AWSBackupFullAccess` und`AWSBackupOperatorAccess` . Weitere Informationen finden Sie unter Bandbreitendrosselung des Backup-Gateways.	15. Dezember 2022

Änderung	Beschreibung	Datum
Unterstützung für VMware-Tags für Backup-Gateway	AWS Backup Gateway unterstützt jetzt VMware-Tags. Benutzer haben die zusätzliche Flexibilität, AWS Tags zu erstellen, die den für virtuelle Maschinen verwendeten Tags entsprechen. Um diese Funktion zu unterstützen, AWS Backup hat das Unternehmen verwaltete Richtlinien erstellt und aktualisiert`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` , darunter`AWSBackupFullAccess` , und`AWSBackupOperatorAccess` . Weitere Informationen finden Sie unter VMware-Tags.	15. Dezember 2022
AWS Backup Unterstützung für Amazon Timestream	AWS Backup unterstützt jetzt das Sichern und Wiederherstellen von Amazon Timestream Timestream-Tabellen. Weitere Informationen finden Sie unter Amazon-Timestream-Backup.	13. Dezember 2022

Änderung	Beschreibung	Datum
AWS Backup bietet Legal Hold	AWS Backup führt ein neues Tool ein, das beim Schutz von Wiederherstellungspunkten durch eine gesetzliche Sperre hilft. Weitere Informationen finden Sie unter Gesetzliche Aufbewahrungsfrist.	27. November 2022
AWS Backup Audit Manager Regions- und kontenübergreifendes Reporting	AWS Backup Audit Manager bietet zusätzliche Funktionen für Compliance- und Jobberichte. Benutzer können Berichte erstellen, die mehrere Regionen und mehrere Konten umfassen. Weitere Informationen finden Sie unter Arbeiten mit Auditberichten.	27. November 2022
AWS Backup unterstützt Amazon Redshift	AWS Backup bietet jetzt Unterstützung für die Sicherung von Amazon Redshift Redshift-Clustern und die Wiederherstellung von Amazon Redshift Redshift-Clustern und -Tabellen. Weitere Informationen finden Sie unter Amazon-Redshift-Sicherungen.	27. November 2022

Änderung	Beschreibung	Datum
AWS Backup bietet Unterstützung für Backup-Anwendungsstapel AWS CloudFormation	AWS Backup bietet die Möglichkeit, Anwendungen mit mehreren Ressourcen zu sichern CloudFormation und wiederherzustellen, indem ein Stack gesichert und die darin enthaltenen Ressourcen wiederhergestellt werden. Weitere Informationen finden Sie unter Anwendungs-Stack-Backups.	27. November 2022
AWS Backup bietet delegierte Administratorkonten und Delegierung von Backup-Richtlinien	AWS Backup registrierte Konten AWS Organizations können Mitgliedskonten als delegierte Administratorkonten kennzeichnen. Weitere Informationen finden Sie unter Verwaltung mehrerer Konten mit. AWS Organizations	27. November 2022

Änderung	Beschreibung	Datum
Öffentliche Vorschau von Backup und Wiederherstellung von SAP HANA auf Amazon-EC2-Instances	AWS Backup und AWS Backint bieten eine integrierte öffentliche Vorschau der Funktionen zur Sicherung und Wiederherstellung von SAP HANA-Datenbanken auf EC2-Instances. Weitere Informationen finden Sie in unserer Öffentlichen Vorschau von SAP HANA auf Amazon-EC2-Instances. Um diese Vorversion zu unterstützen, AWS Backup hat das Unternehmen Richtlinienaktualisierungen und neue AWS verwaltete Richtlinien für diese Funktionen bereitgestellt.	20. November 2022

Änderung	Beschreibung	Datum
VMware auf Amazon-EC2-Instances wiederherstellen	AWS Backup bietet jetzt die Möglichkeit, virtuelle Maschinen auf Amazon EC2 EC2-Instances wiederher zustellen, zusätzlich zur Möglichkeit, Maschinen auf EBS, VMware, VMware Cloud on AWS und VMware Cloud on wiederherzustellen. AWS Outposts Weitere Informationen finden Sie in der Dokumentation zur Verwendung der AWS Backup Konsole zur Wiederher stellung von Wiederher stellungspunkten für virtuelle Maschinen.	9. November 2022
Erweiterte AWS Backup Vault Lock-Funktionalität	AWS Backup Vault Lock kann jetzt im Governance-Modus für zusätzlichen IAM-Schutz oder im Compliance-Modus erstellt werden, um Unverände rlichkeit zu gewährleisten. Erfahren Sie mehr unter AWS Backup Vault Lock.	4. Oktober 2022

Änderung	Beschreibung	Datum
AWS Backup Audit Manager ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar	AWS Backup Audit Manager expandierte in die Regionen Afrika (Kapstadt) und Europa (Mailand). Weitere Informationen zu Backup Audit Manager finden Sie unter Backups prüfen und Berichte mit AWS Backup Audit Manager erstellen.	14. September 2022
AWS Backup bringt CloudWatch Amazon-Metriken in das Dashboard der Backup-Konsole	AWS Backup erweitert das Dashboard der Backup-Konsole um die Anzeige integrierter CloudWatch Amazon-Metriken für Sicherungs- und Wiederherstellungsaufträge und bietet so zusätzliche Überwachungsmöglichkeiten und Flexibilität.	8. September 2022
Unterstützung für zusätzliche Flexibilität bei der Amazon-EBS-Verschlüsselung während der Wiederherstellung	AWS Backup bietet jetzt zusätzliche Verschlüsselungsoptionen bei der Wiederherstellung von Amazon EBS-Snapshots.	01. September 2022
AWS Backup unterstützt konto- und regionsübergreifendes Kopieren von Amazon S3-Backups	AWS Backup bietet jetzt regionsübergreifendes und kontoübergreifendes Kopieren von Backups für Amazon S3 S3-Backups. Weitere Informationen finden Sie unter Amazon-S3-Backups.	28. Juli 2022

Änderung	Beschreibung	Datum
AWS Backup Audit Manager bietet zusätzliche Kontrollu nterstützung für FSx for ONTAP	AWS Backup Audit Manager bietet jetzt zusätzliche Steuerelemente zur Unterstüt zung der Überwachung und Prüfung von FSx for ONTAP-Volumes, einschlie ßlich Backup-Ressourcen werden durch einen Backup-Plan geschützt und der letzte wiederherstellende Punkt erstellt. Weitere Informationen finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe.	22. Juli 2022
AWS Backup fügt Unterstüt zung für die Sicherung und Wiederherstellung von Amazon RDS Multi-AZ-Clustern für PostgreSQL- und MySQL-Cluster hinzu	AWS Backup hat eine Option zur Sicherung und Wiederher stellung von Clustern in einer Multi-Availability Zone mit einer primären und zwei lesbaren Standby-Datenbank-Instances hinzugefügt. Weitere Informationen finden Sie unter Amazon-RDS-Multi-AZ-Backups.	20. Juli 2022

Änderung	Beschreibung	Datum
AWS Backup Audit Manager fügt eine neue Steuerung für die Erstellung von Wiederherstellungspunkten hinzu	AWS Backup Audit Manager bietet eine neue Auditkontrolle zur besseren Unterstützung bei der Einhaltung von Vorschriften. `Last recovery point created` ist eine optionale zusätzliche Steuerung, die sicherstellt, dass Wiederherstellungspunkte innerhalb bestimmter Zeitrahmen erstellt werden. Weitere Informationen finden Sie unter Steuerung letzter erstellter Wiederherstellungspunkt.	29. Juni 2022
Beispiel für einen AWS Backup Gateway-Endpunkt hinzugefügt	AWS Backup Gateway hat einen Beispielendpunkt bereitgestellt, um Benutzern beim Herstellen einer Verbindung zu VPNs (Virtual Private Networks) zu helfen. Weitere Informationen finden Sie unter AWS Backup VPC-Endpoint erstellen.	14. Juni 2022

Änderung	Beschreibung	Datum
AWS Backup bietet jetzt Amazon VPC-Endpunkte für VMware	AWS Backup unterstützt jetzt Amazon VPC-Endpunkte für VMware, sodass Sie ein virtuelles privates Netzwerk zwischen Ihren VMware-Umgebungen verwenden und AWS verwenden können. AWS PrivateLink Weitere Informationen finden Sie unter Erstellen eines Gateways und AWS Backup und AWS PrivateLink.	1. Juni 2022
AWS Backup Audit Manager bietet zusätzliche Kontrollunterstützung für Amazon S3	Backup Audit Manager bietet jetzt Unterstützung für die Compliance-Kontrolle Durch Backup-Pläne geschützte Backup-Ressourcen für S3-Ressourcentypen. Weitere Informationen finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe.	25. Mai 2022

Änderung	Beschreibung	Datum
AWS Backup Audit Manager bietet zusätzliche Kontrollu nterstützung für Storage Gateway	Backup Audit Manager bietet jetzt Unterstützung für die Compliance-Kontrolle Durch Backup-Pläne geschützt e Backup-Ressourcen für Storage-Gateway-Re ssourcentypen. Weitere Informationen finden Sie unter AWS Backup Au dit Manager – Kontrollen und Abhilfe.	25. Mai 2022
Unterstützung für Amazon FSx für OpenZFS	AWS Backup bietet jetzt zusätzliche Datenschu tzverwaltung für Backups und Wiederherstellung auf FSX für OpenZFS-Dateisysteme.	18. Mai 2022
AWS Backup Audit Manager Manager-Unterstützung für VMware	AWS Backup bietet jetzt Unterstützung für virtuelle Maschinen in den Steuerung s- und Wartungsfunktionen von Backup Audit Manager. Weitere Informationen finden Sie unter AWS Backup Au dit Manager – Kontrollen und Abhilfe.	11. Mai 2022

Änderung	Beschreibung	Datum
Amazon FSx wird jetzt in der Region Asien-Pazifik (Osaka) unterstützt	AWS Backup bietet jetzt Backups von Amazon FSx in der Region Asien-Pazifik (Osaka) sowie regionsüb ergreifende Kopien in und aus der Region Asien-Pazifik (Osaka) an.	26. April 2022
Unterstützung für Amazon FSx für Lustre Persistent_2	AWS Backup bietet jetzt allgemein verfügbare Unterstüt zung für Amazon FSx for Lustre, das im Vergleich zu Persistent_1-Dateisystemen einen höheren Durchsatz pro Speichereinheit unterstützt.	5. April 2022
VMware-Verbesserungen	AWS Backup bietet jetzt Wiederherstellung auf Amazon EBS Volume, Wiederher stellung auf Festplattenebene und Unterstützung für VMware on AWS Outposts. Weitere Informationen finden Sie unter Wiederherstellen einer virtuellen Maschine.	31. März 2022
AWS Backup Verfügbarkeit für Asien-Pazifik (Jakarta)	AWS Backup ist jetzt für Kunden in der Region Asien-Pazifik (Jakarta) verfügbar.	17. März 2022

Änderung	Beschreibung	Datum
Neue Kontrollen für AWS Backup Audit Manager	AWS Backup Audit Manager führt drei neue Überwachungskontrollen ein: Regionsübergreifende Kopie, kontoübergreifende Kopie und Backup Vault Lock. Weitere Informationen finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe.	17. März 2022
Support für AWS PrivateLink	Mit AWS PrivateLink for AWS Backup können Sie eine direkte Verbindung zu AWS Backup einem Schnittstellenendpunkt in Ihrer VPC herstellen, anstatt eine Verbindung über das öffentliche Internet herzustellen. Auf Schnittstellen-Endpunkte kann direkt von Anwendungen aus zugegriffen werden, die sich vor Ort oder in einer anderen AWS Region befinden. Weitere Informationen finden Sie unter AWS Backup und AWS PrivateLink.	28. Februar 2022

Änderung	Beschreibung	Datum
Unterstützung für Amazon Simple Storage Service (Amazon S3)	Die allgemeine Verfügbar keit von AWS Backup für Amazon S3 AWS-Regionen ist in allen Regionen verfügbar, mit Ausnahme der Regionen China (Peking), China (Ningxia), AWS GovCloud (USA West) und AWS GovCloud (USA Ost). Weitere Informationen finden Sie unter Arbeiten mit Amazon-S3-Daten.	14. Februar 2022
Support für erweitertes DynamoDB-Backup in chinesischen Regionen AWS	Erweitertes DynamoDB-Backup ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar . Weitere Informationen finden Sie unter Erweiterte DynamoDB-Backups.	18. Januar 2022
Öffentliche Vorschau der Unterstützung für Amazon S3	AWS Backup bietet eine öffentliche Vorschau von Amazon S3 S3-Backups. Weitere Informationen finden Sie unter Arbeiten mit Daten in Amazon S3.	30. November 2021
Unterstützung für virtuelle VMware-Maschinen (VMs)	Sie können es jetzt verwenden AWS Backup , um VMware-VMs automatisch zu sichern. Weitere Informationen finden Sie unter Backups virtueller Maschinen.	30. November 2021

Änderung	Beschreibung	Datum
Unterstützung für erweitertes DynamoDB-Backup	Sie können jetzt die folgenden Funktionen für alle neuen DynamoDB-Tabellens icherungen verwenden AWS Backup , die Sie erstellen: Cold Storage Tiering, Cost Allocation Tagging, regionsüb ergreifendes Kopieren, kontoübergreifendes Kopieren, unabhängige Verschlüs selung und Kopieren von Tags aus DynamoDB-Quelltabe llen. Weitere Informati onen finden Sie Erweitert es DynamoDB-Backup im Amazon DynamoDB Developer Guide und unter Using AWS Backup with DynamoDB.	23. November 2021
Support bei der Verbesserung der AWS Backup Ressource nzuweisung in AWS chinesisc hen Regionen	AWS Backup Die Verbesser ung der Ressourcenzuweisun g ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan.	16. November 2021

Änderung	Beschreibung	Datum
Einführung der Verbesserung der AWS Backup Ressource nzuweisung	Die Verbesserung der Zuweisung von Backup-Re ssourcen bietet Ihnen zusätzlic he, detaillierte Kontrollen und neue optimierte Prozesse für die Bereitstellung von Backup-Plänen, die Hunderttausende von Ressourcen schützen. AWS Verwenden Sie dieses Feature, um Ihre Geschwind igkeit, Flexibilität und Präzision beim Schutz Ihrer Daten mit AWS Backup zu erhöhen. Weitere Informationen finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan.	10. November 2021
Unterstützung für Amazon Neptune	Sie können es jetzt verwenden AWS Backup , um Amazon Neptune Neptune-Cluster zu sichern. Weitere Informationen finden Sie unter Was ist AWS Backup?	5. November 2021
Unterstützung für Amazon DocumentDB	Sie können es jetzt verwenden AWS Backup , um Amazon DocumentDB-Cluster zu sichern. Weitere Informationen finden Sie unter Was ist AWS Backup?	5. November 2021

Änderung	Beschreibung	Datum
Support für AWS Backup Vault Lock in AWS chinesischen Regionen	AWS Backup Vault Lock ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter AWS Backup Vault Lock.	3. November 2021
Markteinführung von AWS Backup Vault Lock	Mit AWS Backup Vault Lock können Sie das Löschen von in einem AWS Backup Backup-Tresor gespeicherten Backups verhindern. Weitere Informationen finden Sie unter AWS Backup Vault Lock.	7. Oktober 2021
Veröffentlichung der Compliance-Berichte von AWS Backup Audit Manager	Mithilfe von Compliance-Berichten können Sie täglich Berichte darüber erstellen, wie Ihre Backup-Aktivitäten und Ressourcen den Kontrollen entsprechen, die Sie in Ihren AWS Backup Audit Manager Manager-Frameworks definiert haben. Weitere Informationen finden Sie unter Vorlagen für Compliance-Berichte.	5. Oktober 2021

Änderung	Beschreibung	Datum
AWS CloudFormation Unterstützung für AWS Backup Audit Manager	Mit AWS CloudFormation können Sie jetzt AWS Backup Audit Manager Manager-Frameworks, Kontrollen und Berichtspläne auf sichere, wiederholbare Weise und in großem Umfang einsetzen. Weitere Informationen finden Sie unter Backup-Audit und Berichte mit AWS Backup Audit Manager.	4. Oktober 2021
Start von AWS Backup Audit Manager	Mit AWS Backup Audit Manager können Sie jetzt Kontrollen für Ihre Backup-Aktivitäten und -Ressourcen definieren und die Aktivitäten und Ressourcen identifizieren, die Ihren Kontrollen nicht entsprechen. Sie können AWS Backup Audit Manager auch verwenden, um Tages- und On-Demand-Berichte zu erstellen, die als Nachweis dafür dienen, dass Ihre definierten Kontrollen im Laufe der Zeit eingehalten wurden. Weitere Informationen finden Sie unter Backup-Audit und Berichte mit AWS Backup Audit Manager.	24. August 2021

Änderung	Beschreibung	Datum
Unterstützung für neue asynchrone Wiederherstellungspunktvorgänge	AWS Backup nimmt jetzt eine dienstbezogene Rolle an, um Ihre Backup-Lebenszyklusregeln für den Fall zu verwalten, dass Sie Ihre ursprüngliche IAM-Rolle geändert oder gelöscht haben. Weitere Informationen finden Sie unter Löschen von Backups.	23. August 2021
Unterstützung für absturzkonsistentes Amazon-EBS-Multi-Volume-Backup	Wenn Sie AWS Backup jetzt Ihre Amazon EC2 EC2-Instances schützen, erstellt standardmäßig mehrvolumige, AWS Backup absturzsichere Backups aller Amazon EBS-Volumes, die an jede Amazon EC2 EC2-Instance angehängt sind. Weitere Informationen finden Sie unter Erstellen eines absturzkonsistenten Amazon-EBS-Multi-Volume-Backup.	14. Juni 2021

Änderung	Beschreibung	Datum
Zusätzliche Support für Amazon FSx AWS-Regionen	Sie können es jetzt AWS Backup zum Schutz Ihrer Amazon FSx-Dateisysteme in den folgenden Regionen verwenden: AWS GovCloud (US), Region Europa (Mailand), Region Afrika (Kapstadt) und Region Naher Osten (Bahrain). Weitere Informationen finden Sie unter AWS Backup -Endpunkte und -Kontingente in der Allgemein en AWS -Referenz.	15. April 2021
Unterstützung für regions- und kontoübergreifende Amazon-FSx-Backups	Sie können es jetzt verwenden AWS Backup , um Amazon FSx-Backups zwischen Konten AWS-Regionen zu kopieren. Weitere Informati onen finden Sie unter Erstellen einer Backup-Kopie. Wenn Sie vom Kunden verwaltete Richtlinien verwenden, sollten Sie die neue Berechtigung `fsx:CopyBackup` hinzufüge n, um zu verhindern, dass bestehende Backup-Aufträge fehlschlagen. Informationen zu dieser Genehmigung finden Sie in der letzten Erklärung in der Amazon-FSx-Backup-Richtlinie in den Vom Kunden verwalteten Richtlinien.	12. April 2021

Änderung	Beschreibung	Datum
Unterstützung für Kostenzuordnung-Tags für Amazon-EFS-Backups	Sie können jetzt Kostenzuweisungs-Tags verwenden, um die Kosten für Ihre Amazon EFS-Backups detailliert zu verfolgen und diese Tags mithilfe von Tags anzuzeigen und zu filtern AWS Cost Explorer. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags.	7. April 2021
FedRAMP-High-Autorisierung	AWS Backup ist jetzt autorisiert, FedRAMP High-Workloads zu unterstützen. Weitere Informationen finden Sie unterAWS -Services im Rahmen des Compliance-Programms.	25. März 2021
Neu AWS-Region	AWS Backup ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar. In dieser Region unterstützt AWS Backup Storage Gateway, Amazon FSx und kontenübergreifendes Backup in dieser Region derzeit nicht. Weitere Informationen finden Sie unter AWS Backup -Endpunkte und -Kontingente in der Allgemeinen AWS -Referenz.	25. März 2021

Änderung	Beschreibung	Datum
Unterstützung für Batch-Operationen an Wiederherstellungspunkten	Sie können jetzt die AWS Backup Konsole verwenden, um Batch-Operationen zur Bereinigung von Wiederherstellungspunkten in Ihren Backup-Tresoren zu automatisieren. Weitere Informationen finden Sie unter Löschen von Backups.	23. März 2021
Unterstützung für Wiederherstellungen in der Amazon-EFS-One-Zone-Speicherklasse	Sie können Ihre Amazon-EFS-Backups jetzt in der Amazon-EFS-One-Zone-Speicherklasse wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Amazon-EFS-Dateisystems.	12. März 2021
Support für point-in-time Wiederherstellung und kontinuierliche Sicherung durch Amazon Relational Database Service	Sie können es jetzt verwenden AWS Backup , um kontinuierliche Amazon RDS-Backups zu automatisieren und point-in-time Wiederherstellungen (PITR) durchzuführen, zusätzlich zur Orchestrierung Ihrer Snapshot-Backups. Weitere Informationen finden Sie unter Wiederherstellung auf einen bestimmten Zeitpunkt mithilfe point-in-time der Wiederherstellung.	10. März 2021

Änderung	Beschreibung	Datum
Support für Amazon CloudWatch	Sie können es jetzt CloudWatch zur Überwachung von AWS Backup Metriken verwenden. Weitere Informationen finden Sie unter Überwachen von Ereignissen und Metriken mit Amazon CloudWatch und Amazon EventBridge.	3. Februar 2021
Support für Amazon EventBridge	Sie können es jetzt EventBridge zur Überwachung von AWS Backup Ereignissen verwenden. Weitere Informationen finden Sie unter Überwachen von Ereignissen und Metriken mit Amazon CloudWatch und Amazon EventBridge.	3. Februar 2021
Unterstützung des kontoüber greifenden Kopierens	Sie können es jetzt verwenden AWS Backup , um Ihre Ressourcen auf mehreren zu sichern AWS-Konten. Weitere Informationen finden Sie unter Erstellen von Sicherungskopien für mehrere AWS Konten.	18. November 2020
Unterstützung für das Backup und die Wiederherstellung von Amazon-FSx-Dateisystemen	Sie können es jetzt verwenden AWS Backup , um Amazon FSx-Dateisysteme zu sichern. Weitere Informationen finden Sie unter Arbeiten mit Amazon-FSx-Dateisystemen.	9. November 2020

Änderung	Beschreibung	Datum
Neu AWS-Regionen	AWS Backup ist jetzt in Afrika (Kapstadt) und Europa (Mailand) erhältlich AWS-Regionen. Weitere Informationen finden Sie unter AWS Backup -Endpunkte und -Kontingente in der Allgemeinen AWS -Referenz.	21. Oktober 2020
Unterstützung für VSS-fähige Windows-Backups	Sie können jetzt VSS-fähige Windows-Anwendungen (Volume Shadow Copy Service), die auf Amazon-EC2-Instances ausgeführt werden, sichern und wiederherstellen. Weitere Informationen finden Sie unter Erstellen eines VSS-fähigen Windows-Backups.	22. September 2020
Unterstützung für automatische Amazon-EFS-Backups	Sie können es jetzt verwenden AWS Backup , um Amazon EFS-Dateisysteme automatisch zu sichern. Weitere Informationen finden Sie unter Erste Schritte 4: Automatische Amazon-EFS-Backups erstellen.	16. Juli 2020

Änderung	Beschreibung	Datum
Neu AWS-Region	AWS Backup ist jetzt verfügbar in der AWS GovCloud (US) Region. Weitere Informationen finden Sie unter AWS Backup - Endpunkte und -Kontingente in der Allgemeinen AWS - Referenz.	24. Juni 2020
Support für die Verwaltung von Backups über mehrere AWS-Konten	Sie können jetzt Backups für mehrere verwalten, AWS-Konten indem Sie AWS Organizations Weitere Informationen finden Sie unter Funktionsweise der kontenübergreifenden Verwaltung.	24. Juni 2020
Support für Amazon Aurora hinzugefügt AWS Backup	Sie können jetzt konfigurieren AWS Backup , dass Ressourcen für Amazon Aurora gesichert werden. Weitere Informationen finden Sie unter Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters im Amazon-Aurora-Benutzerhandbuch.	10. Juni 2020

Änderung	Beschreibung	Datum
Support für die Konfiguration von Diensten, mit denen gearbeitet werden kann AWS Backup	Sie können jetzt so konfigurieren AWS Backup , dass Ressourcen für bestimmte AWS Dienste gesichert werden. Weitere Informationen finden Sie unter Melden Sie sich für die Verwaltung von Diensten mit an AWS Backup.	20. Mai 2020
Unterstützung für das Sichern von Amazon-EC2-Instances und fügt auch Unterstützung für regionsübergreifendes Backup hinzu	Sie können nun ganze Amazon-EC2-Instances sichern und Ressourcen auch in AWS-Regionen kopieren. Weitere Informationen finden Sie unter Erstellen von Backup-Kopien über AWS-Regionen hinweg.	13. Januar 2020
Neues Handbuch	AWS Produkteinführungen AWS Backup und das AWS Backup Entwicklerhandbuch.	15. Januar 2019

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.