



Entwicklerhandbuch

AWS Backup



AWS Backup: Entwicklerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Backup?	1
Überblick über die Features	1
Zentralisierte Sicherungsverwaltung	1
Richtlinienbasiertes Backup	1
Auf Tags basierende Backup-Richtlinien	2
Richtlinien für das Lebenszyklus-Management	2
Regionsübergreifende Backups	2
Kontoübergreifende Verwaltung und kontoübergreifende Backups	3
Prüfung und Berichterstattung mit AWS Backup Audit Manager	3
Inkrementelle Sicherungen	4
Vollständige Verwaltung AWS Backup	4
Überwachung von Backup-Aktivitäten	5
Schützen Ihrer Daten in Backup-Tresoren	5
Erste Schritte	6
Unterstützte AWS Ressourcen und Anwendungen	6
Preisgestaltung	8
AWS Backup Verfügbarkeit von Funktionen	8
Features, die für alle unterstützten Ressourcen verfügbar sind	8
Feature-Verfügbarkeit nach Ressource	8
Verfügbarkeit der Funktionen von AWS-Region	14
Unterstützte Dienste von AWS-Region	22
Funktionsweise	28
Arbeiten mit unterstützten AWS Diensten	28
Arbeiten mit Daten in Amazon S3	29
Arbeiten mit VMware virtuellen Maschinen	30
Arbeiten mit Amazon DynamoDB	30
Arbeiten mit FSx Amazon-Dateisystemen	31
Mit Amazon arbeiten EC2	32
Arbeiten mit Amazon EFS	33
Arbeiten mit Amazon EBS	34
Arbeiten mit Amazon RDS und Aurora	34
Arbeiten mit Aurora DSQL	35
Arbeiten mit AWS BackInt	36
Arbeiten mit AWS Storage Gateway	36

Arbeiten mit Amazon DocumentDB	36
Arbeiten mit Amazon Neptune	36
Arbeiten mit Amazon Redshift und Amazon Redshift Serverless	37
Arbeiten mit Amazon Timestream	37
Arbeiten mit AWS Organizations	37
Arbeiten mit CloudFormation	37
Arbeiten mit AWS BackInt, AWS Systems Manager für SAP und SAP HANA	37
Arbeiten mit Amazon EKS	38
Mit Amazon arbeiten GuardDuty	38
Wie AWS Dienste ihre eigenen Ressourcen sichern	39
Messung, Kosten und Abrechnung	39
AWS Backup Preisgestaltung	8
AWS Backup Abrechnung	40
Kostenzuordnungs-Tags	40
AWS Backup Preisgestaltung für Audit Manager	41
Amazon Aurora – Preise	41
Blogs, Videos, Tutorials und andere Ressourcen	41
Erste Schritte	45
Voraussetzungen	45
Opt-In für den Service	46
Backup-Pläne	48
Erstellen Sie einen Backup-Plan	48
Erstellen Sie Backup-Pläne mithilfe der AWS Backup Konsole	49
Erstellen Sie Backup-Pläne mit dem AWS CLI	51
Backup-Plan-Optionen und -Konfiguration	52
CloudFormation Vorlagen für Backup-Pläne	62
Löschen Sie einen Backup-Plan	65
Aktualisieren Sie einen Backup-Plan	66
Die Zusammenfassung des Backup-Plans verstehen	67
Zusammenfassung der Komponenten	67
Geplante Backups werden als Vorschau ausgeführt	67
Überprüfung der Funktionskompatibilität	68
Zugreifen auf Zusammenfassungen von Backup-Plänen	69
Melden Sie sich an und weisen Sie Ressourcen zu	70
Melden Sie sich für Dienste an und weisen Sie dann Ressourcen zu	70
Serviceanmeldung	70

Ressourcenzuweisung	71
Weisen Sie Ressourcen über die Konsole zu	72
Ressourcen zuweisen mit AWS CLI	74
Ressourcen zuweisen mit CloudFormation	82
Kontingente für Ressourcenzuweisungen	85
Sicherungstresore	86
Erstellung und Löschung von Backup-Tresoren	86
Erforderliche Berechtigungen	86
Erstellen eines Backup-Tresors (Konsole)	88
Erstellen eines Backup-Tresors (programmgesteuert)	89
Name des Backup-Tresors	89
AWS KMS Verschlüsselungsschlüssel	89
Backup-Tresor-Tags	90
Löschen eines Tresors	90
Logischer Air-Gapped Vault	91
Überblick über Tresore mit logischem Air-Gap	91
Anwendungsfall für Tresore mit logischem Air-Gap	92
Vergleich und Gegenüberstellung mit einem Standard-Backup-Tresor	93
Erstellen Sie einen Tresor mit logischem Air-Gap	96
Details zum Tresor mit logischem Air-Gap anzeigen	99
Erstellen von Backups in einem Tresor mit logischem Air-Gap	100
Teilen Sie einen Tresor mit logischem Air-Gap	103
Stellen Sie ein Backup aus einem Tresor mit logischem Air-Gap wieder her	106
Löschen Sie einen Tresor mit logischem Air-Gap	107
Zusätzliche programmatische Optionen für Tresore mit logischem Air-Gap	107
Grundlegendes zu Verschlüsselungsschlüsseltypen für Tresore mit logischem Air-Gap	108
Beheben Sie ein Problem mit einem Tresor mit logischem Air-Gap	115
Primäre Backups zu logischen Air-Gapped Vaults	117
Genehmigung durch mehrere Parteien für Tresore mit logischem Air-Gap	135
Richtlinien für den Tresorzugriff	153
Verweigern des Zugriffs auf einen Ressourcentyp in einem Backup-Tresor	154
Verweigern des Zugriffs auf einen Backup-Tresor	154
Verweigern des Zugriffs zum Löschen von Wiederherstellungspunkten in einem Backup-Tresor	154
Vault Lock	156
Modi der Tresorsperre	157

Vorteile der Tresorsperre	157
Sperren eines Backup-Tresors über die Konsole	157
Programmgesteuertes Sperren eines Backup-Tresors	159
Überprüfen Sie einen Backup-Tresor auf seine AWS Backup Vault Lock-Konfiguration	161
Aufheben der Tresorsperre während der Kulanzzzeit (Compliance-Modus)	162
AWS-Konto Schließung mit einem verschlossenen Tresor	163
Zusätzliche Sicherheitsüberlegungen	163
Erstellung, Wartung und Wiederherstellung von Backup	165
On-Demand-Sicherungen	166
Kontinuierliche Backups und PITR	168
Überlegungen zu kontinuierlichem Backup und PITR	169
Unterstützte Services	171
Finden eines kontinuierlichen Backups	175
Wiederherstellen eines kontinuierlichen Backups	175
Anhalten oder Löschen kontinuierlicher Backups	176
Kopieren kontinuierlicher Backups	177
Ändern Ihrer Aufbewahrungsfrist	177
Entfernen der einzigen Regel für kontinuierliche Backups aus einem Backup-Plan	178
Backup-Erstellung nach Ressourcentyp	178
Erstellen automatischer Backups	178
Erstellen eines On-Demand-Backups	179
Status von Backup-Aufträgen	179
Inkrementelle Sicherungen	179
Zugriff auf Quellressourcen	180
CloudFormation Backups stapeln	181
Amazon Aurora DSQL-Backups	188
Erweitertes DynamoDB-Backup	189
Amazon-EBS-Backups	195
Amazon RDS-Backups	196
Amazon-Redshift-Backups	199
Serverlose Amazon Redshift Redshift-Backups	201
Amazon EKS	205
SAP HANA-Backup auf Amazon EC2	213
Amazon-S3-Backups	224
Amazon-Timestream-Backups	237
Backups virtueller Maschinen	240

Erstellen Sie Windows VSS-Backups	284
Kopie sichern und markieren	287
Kopierauftrag erneut versuchen	288
Regionsübergreifende Backups	288
Kontenübergreifende Backups	292
Tags auf Backups kopieren	305
Löschen von Backup	306
Manuelles Löschen von Backups	307
Fehlerbehebung bei manuellen Löschungen	308
Änderungen Backup und taggen	309
Backup-Suche	310
Übersicht	310
Anwendungsfälle für Backup-Indizes und Suchvorgänge	311
Zugriff	311
Ablauf des Prozesses	312
Backup-Indizes	312
Suchvorgänge	316
Suchergebnisse	319
Exportieren Sie Suchergebnisse in einen S3-Bucket	320
Kostenüberlegungen und bewährte Verfahren	321
Aus der Suche wiederherstellen	322
Backup-Tiering	322
Übersicht	322
Tiering-Konfigurationen	323
Erstellung von Tiering-Konfigurationen	324
Verwaltung von Tiering-Konfigurationen	326
Wie werden S3-Backup-Tiering-Konfigurationen angewendet	328
Kostenstruktur und Überwachung	328
Beispiele für Konfigurationen	329
Unterstützte Funktionen und Einschränkungen	331
Fehlerbehebung	332
Wiederherstellung nach Ressourcentyp	333
So führen Sie eine Wiederherstellung aus:	333
Zerstörungsfreie Wiederherstellungen	333
Wiederherstellungstests	333
Kopieren von Tags während einer Wiederherstellung	334

Wiederherstellen von Auftragsstatus	338
Aurora wiederherstellen	339
Aurora DSQL-Wiederherstellung	343
CloudFormation wiederherstellen	350
DocumentDB wiederherstellen	352
DynamoDB-Wiederherstellung	355
EBS-Wiederherstellung	358
EC2 wiederherstellen	364
EFS-Wiederherstellung	369
EKS-Wiederherstellung	375
FSx wiederherstellen	384
Neptune wiederherstellen	394
RDS-Wiederherstellung	396
Redshift-Wiederherstellung	397
Serverlose Redshift-Wiederherstellung	402
SAP HANA-Wiederherstellung	406
S3-Wiederherstellung	416
Storage Gateway Gateway-Wiederherstellung	424
Timestream-Wiederherstellung	426
VM-Wiederherstellung	429
Testen wiederherstellen	435
Übersicht	436
Vergleich mit Wiederherstellungen	437
Planverwaltung	438
Erstellen eines Testplans	439
Aktualisieren eines Testplans	445
Anzeigen von Testplänen	446
Anzeigen von Testaufträgen	447
Löschen eines Plans	448
Prüfung von Tests	449
Kontingente und Parameter	450
Fehlerbehebung	450
Abgeleitete Metadaten	452
Die Testvalidierung wiederherstellen	461
Beenden Sie einen Backup-Job	464
Bestehende Backups anzeigen	464

Auflisten von Backups nach geschützter Ressource in der Konsole	464
Auflisten von Backups nach Backup-Tresor in der Konsole	465
Programmgesteuertes Auflisten von Backups	465
AWS Backup Audit Manager	466
Arbeiten mit Audit-Frameworks	467
Auswählen Ihrer Kontrollen	468
Aktivieren der Ressourcennachverfolgung	472
Frameworks mithilfe der AWS Backup Konsole erstellen	478
Frameworks mithilfe der AWS Backup API erstellen	479
Anzeigen des Framework-Compliance-Status	494
Suchen nicht konformer Ressourcen	496
Aktualisieren von Audit-Frameworks	496
Löschen von Audit-Frameworks	496
Arbeiten mit Auditberichten	497
Verbesserter Kontext für Jobberichte	498
Auswählen Ihrer Berichtsvorlage	499
Berichtspläne erstellen	510
Berichtspläne mithilfe der AWS Backup API erstellen	514
Erstellen von On-Demand-Berichten	517
Anzeigen von Auditberichten	517
Aktualisieren von Berichtsplänen	518
Löschen von Berichtsplänen	518
Verwendung CloudFormation zur Bereitstellung von AWS Backup Audit Manager Manager- Ressourcen	519
Aktivieren der Ressourcennachverfolgung	478
Bereitstellen von Standardkontrollen	525
Ausschließen von IAM-Rollen aus der Kontrollauswertung	526
Erstellen eines Berichtsplans	526
Verwenden von AWS Backup Audit Manager mit AWS Audit Manager	527
Steuerelemente und Abhilfemaßnahmen	528
Backup-Ressourcen sind in mindestens einem Backup-Plan enthalten	529
Mindesthäufigkeit und Mindestspeicherung des Backup-Plans	529
Tresore verhindern das manuelle Löschen von Wiederherstellungspunkten.	530
Wiederherstellungspunkte sind verschlüsselt.	531
Mindestaufbewahrungszeitraum ist für den Wiederherstellungspunkt festgelegt.	531
Regionsübergreifende Backup-Kopie ist geplant.	532

Kontenübergreifende Backup-Kopie ist geplant.	532
Ressourcen befinden sich in einem Backup-Plan mit AWS Backup Vault Lock	533
Letzter Wiederherstellungspunkt wurde erstellt.	534
Wiederherstellungszeit für Ressourcen entspricht dem Ziel	535
Ressourcen in einem Tresor mit logischem Air-Gap	535
Verwalte mehrere Konten mit AWS Organizations	537
Überblick über die kontenübergreifende Verwaltung	537
Erstellen eines Verwaltungskontos in Organizations	539
Aktivieren der kontenübergreifenden Verwaltung	539
Sicherungsrichtlinien	540
Delegierter Administrator	540
Voraussetzungen	542
Registrieren eines Mitgliedskontos als delegiertes Administratorkonto	543
Aufheben der Registrierung eines Mitgliedskontos	544
Delegieren Sie AWS Backup Richtlinien über AWS Organizations	545
Überwachen von Aktivitäten in mehreren AWS-Konten	545
Opt-In-Regeln für Ressourcen	546
Definieren von Richtlinien, Richtliniensyntax und Richtlinienvererbung	546
AWS Backup und CloudFormation	547
Allgemeines	547
Bereitstellen eines Backup-Tresors, eines Backup-Plans und einer Ressourcenzuweisung mit CloudFormation	547
Bereitstellen von Backup-Plänen mit CloudFormation	547
Bereitstellung von AWS Backup Audit Manager Manager-Frameworks und Berichtsplänen mit CloudFormation	548
Verwenden CloudFormation mit AWS Organizations	548
Mehr lernen	548
Netzwerk	549
Endpunkte	549
AWS PrivateLink	549
Überlegungen zu Amazon VPC-Endpunkten	550
Erstellen Sie einen AWS Backup VPC-Endpunkt	550
Verwenden Sie einen VPC-Endpunkt	551
Erstellen einer VPC-Endpunktrichtlinie	551
Sicherheit	554
Compliance-Validierung	555

Datenschutz	555
Verschlüsselung für Backups in AWS Backup	556
Verschlüsselung der Hypervisor-Anmeldeinformationen für virtuelle Maschinen	568
Identity and Access Management	570
Authentifizierung	571
Zugriffskontrolle	573
IAM-Servicerollen	582
Verwaltete Richtlinien	586
Verwenden von servicegebundenen Rollen	675
Serviceübergreifende Confused-Deputy-Prävention	684
Sicherheit der Infrastruktur	685
Integrität	686
AWS Backup Ziel der Datenintegrität	686
AWS Backup Implementierung der Datenintegrität	686
Objektive Bestätigung und Prüfung der AWS Backup -Datenintegrität	687
Rechtliche Aufbewahrungsfristen	687
Überblick über gesetzliche Aufbewahrungsfristen	687
Mehrere gesetzliche Sperren	688
Erstellen einer gesetzlichen Aufbewahrungsfrist	688
Sehen von rechtlichen Aufbewahrungsfristen	690
Erstellen einer gesetzlichen Aufbewahrungsfrist	692
Schutz vor Schadsoftware	694
Integration mit Amazon GuardDuty	695
Sofortiger Zugriff	695
Wie verwendet man das Scannen nach Schadsoftware	695
Zugriff	696
Inkrementelle oder vollständige Scans	697
Überwachung Ihrer Malware-Scans	698
Die Scanergebnisse verstehen	699
Behebung von Scanfehlern	700
Metering (Messung)	701
Kontingente	701
Schritte zur Verwendung von Konsole und CLI für Malware-Scantypen	701
Ausfallsicherheit	706
Kontingente	707
Backup	707

Backup-Index und Suchkontingente	709
Richtlinienkontingente	710
Kontingente für Malware-Scans	711
Amazon Timestream Timestream-Ressourcenkontingente	712
AWS Backup Quoten für Audit Manager	712
Kontingente des Testplans wiederherstellen	713
AWS Backup gateway Kontingente	715
Amazon EKS-Kontingente	715
Logisch zugeordnete Tresorkontingente	716
Verwandte Quotas	716
Überwachung AWS Backup	718
Konsolen-Dashboards	718
Übersicht	719
Job-Dashboard	719
Gründe für Probleme	721
Dashboard-Daten mit AWS CLI	725
Überwachung von Ereignissen mit EventBridge	727
Backup-Job-Ereignisse	728
Ereignisse im Backup-Plan	733
Backup Vault-Ereignisse	735
Job-Ereignisse kopieren	737
Recovery Point-Ereignisse	740
Ereignisse in den Regionseinstellungen	741
Job-Ereignisse wiederherstellen	742
Ereignisse bei der Indexierung von Wiederherstellungspunkten	745
Auftragseignisse für Malware-Scans	748
AWS Backup Metriken mit Amazon CloudWatch	755
CloudWatch Armaturenbrett	755
Metriken mit CloudWatch	757
AWS Backup API-Aufrufe protokollieren mit CloudTrail	761
AWS Backup Ereignisse in CloudTrail	763
Grundlegendes zu AWS Backup Einträgen in Protokolldateien	764
Protokollieren von Ereignissen der kontenübergreifenden Verwaltung	768
Benachrichtigungsoptionen mit AWS Backup	772
Benutzerbenachrichtigungen und AWS Backup	772
Amazon SNS und Ereignisse AWS Backup	773

Problembehebung AWS Backup	780
Fehlerbehebung bei allgemeinen Problemen	780
Fehlerbehebung beim Erstellen von Ressourcen	781
Fehlerbehebung beim Löschen von Ressourcen	782
Fehlerbehebung beim Wiederherstellen von Ressourcen	782
Behebung von Formatierungsfehlern	783
AWS Backup API	784
Aktionen	784
AWS Backup	789
AWS Backup gateway	1281
AWS Backup	1377
Datentypen	1439
AWS Backup	1442
AWS Backup gateway	1624
AWS Backup	1650
Geläufige Parameter	1684
Häufige Fehler	1686
Dokumentverlauf	1689
.....	mdcclxii

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 APIs Backups 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 Sicherheitsstrategie für Ihre gesamte Organisation und für alle Ihre Anwendungen in skalierbarer Weise.

Alle Konfigurationsoptionen für Backup-Pläne finden Sie unter [Backup-Plan-Optionen und -Konfiguration](#).

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 [Wählen Sie die zu AWS sichernden Dienste aus](#).

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 Kühltaspeicherebene 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 [Feature-Verfügbarkeit 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 Organizations](#) Struktur zu verwalten. Mit der kontoübergreifenden 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 kontoübergreifende 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 [Feature-Verfügbarkeit nach Ressource](#).

Weitere Informationen zum Verhalten in Tresoren finden Sie unter [Inkrementelle Sicherungen](#)

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). Das Backup ARNs beginnt mit `arn:aws:backup` statt mit `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 [Erfassung, Kosten und Abrechnung für AWS Backup](#).

Informationen darüber, welche Ressourcentypen für die vollständige AWS Backup Verwaltung in Frage kommen, finden Sie unter [Feature-Verfügbarkeit 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](#) [Amazon SNS und AWS Backup Ereignissen](#).

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 EC2 Amazon-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](#).

Erste Schritte

Um mehr darüber zu erfahren AWS Backup, empfehlen wir Ihnen, mit zu beginnen [Erste 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 “AWS Backup Verfügbarkeit von Funktionen”](#).

Service	Unterstützte Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	EC2 Amazon-Instances, die von Amazon EBS-Volumes unterstützt werden
Amazon Simple Storage Service (Amazon-S3)	Amazon-S3-Daten
Amazon Elastic Block Store (Amazon EBS)	Amazon-EBS-Volumes
Amazon-DynamoDB	Amazon-DynamoDB-Tabellen
Amazon Relational Database Service (Amazon RDS)	Amazon-RDS-Datenbank-Instances (einschließlich aller Datenbank-Engines); Cluster mit mehreren Availability Zones
Amazon Aurora DSQL	Cluster mit einer Region und Cluster mit mehreren Regionen
Amazon Aurora	Aurora-Cluster
Amazon Elastic File System (Amazon EFS)	Amazon-EFS-Dateisysteme

Service	Unterstützte Ressourcentypen
FSx für Lustre	FSx für Lustre-Dateisysteme
FSx für Windows-Dateiserver	FSx für Windows-Dateiserver-Dateisysteme
Amazon FSx für NetApp ONTAP	FSx für ONTAP-Dateisysteme
Amazon FSx für OpenZFS	FSx für OpenZFS-Dateisysteme
AWS Storage Gateway (Volume Gateway)	AWS Storage Gateway Bänder
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	VMware Cloud™ virtuelle Maschinen an AWS
VMware Cloud™ aktiviert AWS Outposts	VMware Cloud™ virtuelle Maschinen an AWS Outposts
CloudFormation	CloudFormation stapelt
SAP-HANA-Datenbanken	SAP HANA-Datenbanken auf EC2 Amazon-Instances
Amazon Elastic Kubernetes Service (Amazon EKS)	Amazon EKS-Cluster und persistente Speicher-Backups

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 – Preise](#).

AWS Backup Verfügbarkeit von Funktionen

AWS Backup Funktionen werden je nach Ressource und angebotenen 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](#)
- [Feature-Verfügbarkeit nach Ressource](#)
- [Verfügbarkeit der Funktionen von AWS-Region](#)
- [Unterstützte Dienste von AWS-Region](#)

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](#)

Feature-Verfügbarkeit 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.

Informationen zu Regionen, in denen Sie sich anmelden können und welche Ressourcen und Funktionen in diesen Regionen unterstützt werden, finden Sie unter. [Verfügbarkeit der Funktionen von AWS-Region](#)

AWS Backup unterstützt	Regionen	Kontingenz	AWS Backup Audit Manager	Inkrementelle Backup	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Leber bis zur Kühlung	Wiederherstellung auf Objektebene 1	Testen	Logische Air-Gapped Vault	Backup-Suche	Backup-Tiering	Malware Protection
Amazon EC2	✓	✓	✓	✓					✓	✓			✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Amazon EBS	✓	✓	✓	✓			✓	✓	✓	✓	✓		✓
Amazon RDS-Instanz	✓ ³	✓ ³	✓ ⁴	✓	✓				✓				
Amazon RDS-Cluster	✓ ³	✓ ³	✓ ⁴	✓					✓				
Amazon Aurora	✓ ³	✓ ³	✓	✓ ⁶	✓				✓	✓			

AWS Backup unterstützt	Regionale Backup	Kontingente Backup	AWS Backup Audit Manager	Inkrementelle Backup	Kontingente Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Leber bis zur Kühlung	Wiederherstellung auf Objektebene 1	Testwiederherstellung	Logische Air-Gapped Vault	Backup-Suche	Backup-Timing	Malware Protection
Amazon Aurora DSQL	✓	✓				✓	✓			✓			
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓	✓			
FSx für Lustre	✓	✓	✓	✓					✓	✓			
FSx für Windows Dateispeicher	✓	✓	✓	✓					✓ ⁸	✓			
FSx für ONTAP			✓ ²	✓					✓				
FSx für Open	✓	✓					✓	✓					

AWS Backup unterstützt	Regionale Backups	Kontingente Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontingente Sicherungen und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Leber bis zur Kühlung	Wiederherstellung auf Objektebene 1	Testwiederherstellung	Logische Air-Gapped Vault	Backup-Suche	Backup-Timing	Malware Protection
AWS Storage Gateway	✓	✓	✓	✓						✓			
Amazon DocumentDB	✓ ³	✓ ³							✓	✓			
Amazon Neptune	✓ ³	✓ ³							✓	✓ ⁹			
Amazon Redshift Serverless								✓					
Amazon TimeStream	✓	✓		✓		✓	✓			✓			
Windows VSS	✓	✓	✓	✓						✓			
Virtual Machine Snapshots	✓	✓	✓	✓		✓	✓	✓		✓			

AWS Backup unterstützt	Regionale Backups	Kontingente Backups	AWS Backup Audit Manager	Inkrementelle Backups	Kontingente Sicherungen und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Leber bis zur Kühlung	Wiederherstellung auf Objektebene 1	Testwiederherstellung	Logische Appare und Vault	Backup-Suche	Backup-Timing	Malware Protection
AWS CloudFormation	✓ ⁵		✓	✓ ⁵			✓						
Amazon DynamoDB			✓						✓				
DynamoDB mit erweiterten AWS Backup-Funktionen	✓	✓	✓			✓	✓		✓	✓			
SAP HANA Database auf EC2 Amazon Instance	✓	✓		✓ ⁶	✓	✓	✓						

AWS Backup unterstützt	Regionsübergreifendes Kopieren	Kontoübergreifendes Kopieren	AWS Backup Audit Manager	Inkrementelles Kopieren	Kontinuierliche Sicherung und point-in-time Wiederherstellung	Vollständige Verwaltung	Vom Leber bis zur Kühlung	Wiederherstellung auf Objektebene ¹	Testen und Validieren	Logische Suche	Backup-Timing	Malware Protection
Amazon EKS ¹⁰	✓	✓				✓		✓				

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). PITR (Point-in-Time Restore) ist für diese Kopien nicht verfügbar.

- Amazon RDS und Amazon S3 unterstützen konto- und regionsübergreifendes Kopieren von inkrementellen Backups. Amazon RDS unterstützt auch das gleichzeitige regionsübergreifende und kontoübergreifende Kopieren von Snapshots in einer einzigen Aktion.
- Amazon Aurora und SAP HANA auf EC2 Amazon-Instances unterstützen konto- und regionsübergreifendes Kopieren von vollständigen Backups. Amazon Aurora unterstützt auch das gleichzeitige regionsübergreifende und kontoübergreifende Kopieren von Snapshots in einer einzigen Aktion.

¹ Das „Objekt“ bei einer Wiederherstellung auf Artelebene 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 [Stellen Sie ein Backup nach Ressourcentyp wieder her](#) für die unterstützte Ressource.

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

³ Amazon RDS, Aurora, DocumentDB und Neptune unterstützen jetzt regionsübergreifendes und kontoübergreifendes Kopieren von Snapshots in einer einzigen Aktion. RDS-Multi-AZ-Datenbank-Instances (Multi Availability Zone) können kopiert werden, aber Multi-AZ-Cluster unterstützen derzeit kein regionsübergreifendes oder kontoübergreifendes Kopieren. Weitere Informationen finden Sie unter [Überlegungen zum regionsübergreifenden Kopieren mit bestimmten Ressourcen](#)

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 ihre Quellressourcenfunktionen bei. Ressourcen innerhalb des Stacks behalten jedoch keine Point-in-Time Restore-Funktionalität (PITR) bei (wie Amazon S3 und Amazon RDS).

⁶ Snapshots sind vollständig und inkrementelle Backups werden über PITR angeboten.

⁷ Amazon FSx for OpenZFS Multi-AZ-Dateisysteme (Multi-Availability Zone) können nur über die FSx Amazon-Konsole oder die API-Anfrage wiederhergestellt werden. [createFileSystemFromBackup](#)

⁸ Wird in einem Wiederherstellungstest unterstützt, wenn FSx für Windows File Server verwaltetes Active Directory verwendet AWS

⁹ ist derzeit in der Region Asien-Pazifik (Jakarta) nicht verfügbar

¹⁰ Funktionen für persistente Speicher-Backups (z. B. Amazon EBS), die Teil von Amazon EKS Backups sind, geben die Funktionsunterstützung für die jeweiligen Ressourcentypen in dieser Tabelle wieder.

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.

In einigen Regionen ist eine Kontoanmeldung erforderlich, wie in der folgenden Tabelle angegeben. Die Verfügbarkeit einiger Funktionen hängt davon ab, ob eine Anmeldung erforderlich ist oder nicht. Weitere Informationen finden Sie im AWS -Kontenverwaltung Referenzhandbuch unter [AWS-Regionen Ihr Konto kann verwendet](#) werden.

Überlegungen zu Opt-in-Regionen:

- Kontoübergreifendes Kopieren wird für Amazon DocumentDB in Regionen, in denen eine Anmeldung erforderlich ist, nicht unterstützt.

- Regionsübergreifendes Kopieren wird für Amazon DocumentDB in Regionen, in denen eine Anmeldung erforderlich ist, nicht unterstützt.
- Das regionsübergreifende Kopieren von Neptune-Backups wird derzeit in den Regionen Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Jakarta), Israel (Tel Aviv), Naher Osten (Bahrain) und Naher Osten (VAE) unterstützt.

Das regionsübergreifende Kopieren von FSx für Lustre, für Windows File Server, FSx für ONTAP und FSx für OpenZFS wird in Regionen, in denen eine Anmeldung erforderlich ist, nicht unterstützt.

- Kontoübergreifendes Kopieren wird für CloudFormation Neptune und Timestream in Regionen, in denen eine Anmeldung erforderlich ist, nicht unterstützt.

Überlegungen und Einschränkungen bei der kontoübergreifenden Verwaltung in Opt-in-Regionen:

- Die kontoübergreifende Verwaltung AWS-Regionen, bei der eine Anmeldung erforderlich ist, umfasst die kontoübergreifende Überwachung und den Zugriff auf Backup-Richtlinien. Delegierte Administratorkonten können Richtlinien einrichten, haben aber keinen Zugriff auf die Überwachungsfunktionen.
- Es können sowohl Verwaltungskonten als auch deren Kinderkonten aktiviert werden. AWS Organizations Wenn für ein Kinderkonto die kontoübergreifende Verwaltung aktiviert wurde, bevor das zugehörige Verwaltungskonto für die kontoübergreifende Verwaltung aktiviert wurde, dauert es eine Verzögerung (bis zu 24 Stunden), bis die kontoübergreifende Überwachung den Stellenstatus im gesamten Unternehmen anzeigt.

AWS Backup unterstützt	Melden Sie sich an	Regionsübergreifende Sicherung	Kontoübergreifende Verwaltung	Kontoübergreifende Sicherungskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
US East (N.	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionen ergreifen	Kontenübergreifend	Kontoübergreifende Sicherungskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
Virginia)									
USA Ost (Ohio)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
US West (N. California)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
US West (Oregon)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Africa (Cape Town)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Hong Kong)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Hyderabad)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionale Sicherungsskopia	Kontenübergreifende Verwaltung	Kontoübergreifende Sicherungsskopia	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
Asien-Pazifik (Jakarta)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Malaysia)	Erforderlich	✓	✓	✓			✓	✓	✓
Asien-Pazifik (Melbourne)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Mumbai)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Neuseeland)	Erforderlich	✓		✓				✓	
Asien-Pazifik (Osaka)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionale Sicherungskopie	Kontenübergreifende Verwaltung	Kontoübergreifende Sicherungskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
Asia Pacific (Seoul)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Singapur)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Sydney)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Taipeh)	Erforderlich	✓		✓				✓	✓
Asien-Pazifik (Thailand)	Erforderlich	✓		✓			✓	✓	✓
Asien-Pazifik (Tokio)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Canada (Central)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionen ergreifen	Kontenübergreifend	Kontoübergreifende Sicherungskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
Kanada West (Calgary)	Erforderlich	✓	✓	✓			✓	✓	✓
China (Peking)	AWS in China	✓ ²						✓	
China (Ningxia)	AWS in China	✓ ²						✓	
Europa (Frankfurt)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Irland)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europe (London)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Milan)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionale Sicherungskopie	Kontenübergreifende Verwaltung	Kontoübergreifende Sicherungskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
Europe (Paris)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Spain)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Stockholm)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Zürich)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Israel (Tel Aviv)	Erforderlich	✓	✓	✓			✓	✓	✓
Mexiko (Zentral)	Erforderlich	✓		✓			✓	✓	✓
Middle East (Bahrain)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
Naher Osten (VAE)	Erforderlich	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup unterstützt	Melden Sie sich an	Regionsübergreifende Sicherungsskopie	Kontenübergreifende Verwaltung	Kontoübergreifende Sicherungsskopie	AWS Backup Audit Manager und Job-Dashboard	Testen Sie erneut	Backup-Suche	Backup-Tiering	Malware Protection
South America (São Paulo)	Nicht erforderlich	✓	✓	✓	✓	✓	✓	✓	✓
AWS GovCloud (US-Ost)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓
AWS GovCloud (US-West)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓

¹ Regions- und kontoübergreifende Kopie in einen Tresor mit logischem Air-Gap ist derzeit in den Regionen Kanada West (Calgary), China (Peking), China (Ningxia), (USA Ost) oder AWS GovCloud (USA West) nicht verfügbar. AWS GovCloud

² China (Peking) und China (Ningxia) unterstützen regionsübergreifendes 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.

³ Das Job-Dashboard und die Organisationsberichterstattung von AWS Backup Audit Manager sind in AWS GovCloud (USA-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.

⁴ AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützen regionsübergreifendes Kopieren von einer dieser beiden Regionen in die andere. Regionsübergreifendes Kopieren von diesen Regionen in andere Regionen oder von anderen Regionen in diese Regionen wird nicht unterstützt.

Unterstützte Dienste von AWS-Region

AWS Backup ist für diese Ressourcentypen in allen Regionen verfügbar, in denen die AWS Backup aufgelistete Ressource aktiv ist:

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

AWS Backup Die Unterstützung von Amazon Neptune ist in den meisten kommerziellen Regionen verfügbar, in denen Neptune unterstützt wird. Backup und Wiederherstellung sind derzeit in der Region Europa (Spanien) nicht verfügbar.

AWS Backup Die Unterstützung von Amazon DocumentDB ist in Afrika (Kapstadt), Asien-Pazifik (Hongkong), Israel (Tel Aviv) oder AWS GovCloud (USA Ost) nicht verfügbar.

In der folgenden Tabelle ist die AWS Backup Unterstützung für andere AWS Dienste nach Regionen aufgeführt:

Region und Service	Aurora SQL	Amazon FSx	SAP HANA auf Instanzen EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup-Gateway	Amazon EKS
USA Ost (Nord-Virginia)	✓	✓	✓	✓	✓	✓	✓	✓
USA Ost (Ohio)	✓	✓	✓	✓	✓	✓	✓	✓
USA West (Nordkalifornien)		✓	✓	✓	✓		✓	✓
USA West (Oregon)	✓	✓	✓	✓	✓	✓	✓	✓
Africa (Cape Town)		✓	✓	✓	✓		✓	✓
Asien-Pazifik (Hongkong)		✓	✓	✓	✓		✓	✓
Asien-Pazifik (Hyderabad)		✓		✓	✓			✓

Region und Service	Aurora SQL	Amazon FSx	SAP HANA auf Instanzen EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Asien-Pazifik (Jakarta)		✓		✓	✓			✓
Asien-Pazifik (Malaysia)				✓				✓
Asien-Pazifik (Melbourne)		Windows; Lustre; ONTAP		✓	✓			✓
Asien-Pazifik (Mumbai)		✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Neuseeland)				✓				✓
Asien-Pazifik (Osaka)	✓	✓	✓	✓	✓		✓	✓
Asien-Pazifik (Seoul)	✓	✓	✓	✓	✓		✓	✓

Region und Service	Aurora SQL	Amazon FSx	SAP HANA auf Instanzen EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Asien-Pazifik (Singapur)		✓	✓	✓	✓		✓	✓
Asien-Pazifik (Sydney)		✓	✓	✓	✓	✓	✓	✓
Asien-Pazifik (Taipeh)				✓				✓
Asien-Pazifik (Thailand)				✓				✓
Asien-Pazifik (Tokio)	✓	✓	✓	✓	✓	✓	✓	✓
Canada (Central)		✓	✓	✓	✓		✓	✓
Kanada West (Calgary)				✓				✓
China (Peking)		Windows; Lustre		✓ ¹	✓			

Region und Service	Aurora SQL	Amazon FSx	SAP HANA auf Instanzen EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
China (Ningxia)		Windows; Lustre		✓ ¹	✓			
Europe (Frankfurt)	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Irland)	✓	✓	✓	✓	✓	✓	✓	✓
Europa (London)	✓	✓	✓	✓	✓		✓	✓
Europa (Milan)		✓	✓	✓	✓		✓	✓
Europa (Paris)	✓	✓	✓	✓	✓		✓	✓
Europa (Spain)		✓		✓	✓			✓
Europa (Stockholm)		✓	✓	✓	✓		✓	✓
Europa (Zürich)		✓		✓	✓			✓
Israel (Tel Aviv)		✓		✓	✓			✓

Region und Service	Aurora SQL	Amazon FSx	SAP HANA auf Instanzen EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Mexiko (Zentral)				✓				✓
Middle East (Bahrain)		✓	✓	✓	✓		✓	✓
Naher Osten (VAE)		✓		✓	✓			✓
Südamerika (São Paulo)		✓	✓	✓	✓		✓	✓
AWS GovCloud (US-West)		Windows; Lustre; ONTAP		✓	✓	✓	✓	✓
AWS GovCloud (US-Ost)		Windows; Lustre; ONTAP		✓	✓		✓	✓

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

¹ 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](#)
- [Erfassung, Kosten und Abrechnung für AWS Backup](#)
- [AWS Backup Blogs, Videos, Tutorials und andere Ressourcen](#)

Wie AWS Backup funktioniert mit unterstützten AWS Diensten

Einige von ihnen 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.

Informationen zur Auswahl der Dienste (Ressourcentypen), die Sie sichern möchten, finden Sie unter Ressourcen [zuweisen](#).

Themen

- [Arbeiten mit Daten in Amazon S3](#)
- [Arbeiten mit VMware virtuellen Maschinen](#)
- [Arbeiten mit Amazon DynamoDB](#)
- [Arbeiten mit FSx Amazon-Dateisystemen](#)
- [Mit Amazon arbeiten EC2](#)
- [Arbeiten mit Amazon EFS](#)
- [Arbeiten mit Amazon EBS](#)
- [Arbeiten mit Amazon RDS und Aurora](#)
- [Arbeiten mit Aurora DSQL](#)
- [Arbeiten mit AWS BackInt](#)
- [Arbeiten mit AWS Storage Gateway](#)
- [Arbeiten mit Amazon DocumentDB](#)
- [Arbeiten mit Amazon Neptune](#)
- [Arbeiten mit Amazon Redshift und Amazon Redshift Serverless](#)
- [Arbeiten mit Amazon Timestream](#)
- [Arbeitet mit AWS Organizations](#)
- [Arbeitet mit CloudFormation](#)
- [Arbeiten mit AWS BackInt, AWS Systems Manager für SAP und SAP HANA](#)
- [Arbeiten mit Amazon EKS](#)
- [Mit Amazon arbeiten GuardDuty](#)
- [Wie AWS Dienste ihre eigenen Ressourcen sichern](#)

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](#).

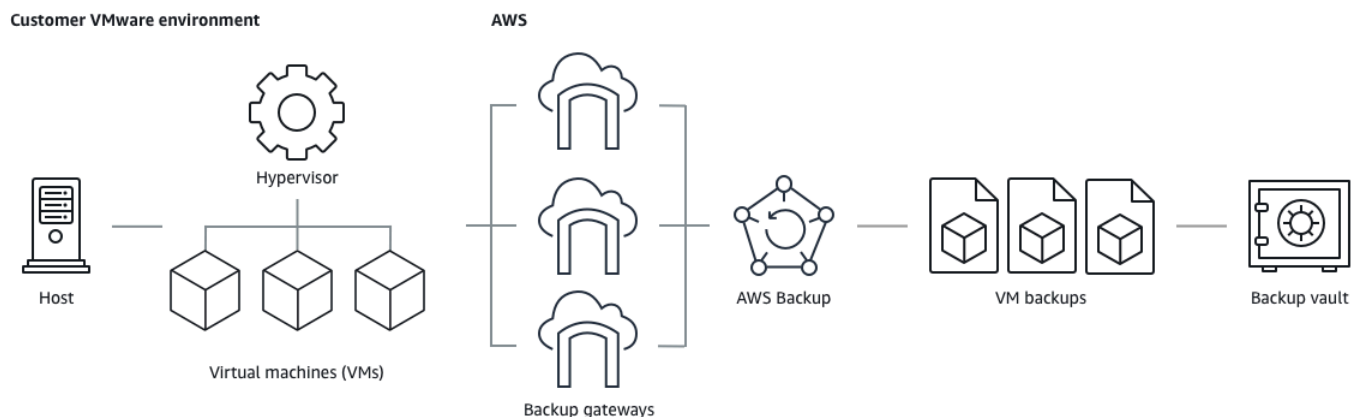
- So sichern Sie Ressourcen: [Erste Schritte mit AWS Backup](#)
- So stellen Sie Amazon S3 S3-Daten wieder her mit AWS Backup: [Stellen Sie S3-Daten wieder her mit AWS Backup](#)

Detaillierte Informationen über S3-Daten finden Sie in der [Amazon-S3-Dokumentation](#).

Arbeiten mit VMware virtuellen Maschinen

AWS Backup unterstützt zentralisierten und automatisierten Datenschutz für lokale VMware virtuelle Maschinen (VMs) zusammen mit VMs In the 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 in Ihrer VMware Infrastruktur bereitstellen, um eine Verbindung herzustellen AWS Backup. VMware VMs Das Gateway stellt eine Verbindung zu Ihrem VM-Managementserver her, um Ihre Daten zu erkennen VMs, zu verschlüsseln und Daten effizient zu AWS Backupübertragen. Das folgende Diagramm zeigt, wie das Backup-Gateway eine Verbindung zu Ihrem herstellt VMs:



- So sichern Sie Ressourcen: [Backups virtueller Maschinen](#)
- So stellen Sie VM-Ressourcen wieder her: [Stellen Sie eine virtuelle Maschine wieder her 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 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: [Eine Amazon DynamoDB-Tabelle wiederherstellen](#)

Detaillierte Informationen über DynamoDB finden Sie unter [Was ist Amazon DynamoDB?](#) im Amazon-DynamoDB-Entwicklerhandbuch.

Arbeiten mit FSx Amazon-Dateisystemen

AWS Backup unterstützt das Sichern und Wiederherstellen von FSx Amazon-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 die gleiche Konsistenz und Leistung des Dateisystems und dieselben Wiederherstellungsoptionen wie Backups, die über die FSx Amazon-Konsole erstellt werden.

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 FSx Amazon-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 Dienste erweitert.

- So sichern Sie Ressourcen: [Erste Schritte mit AWS Backup](#)
- So stellen Sie FSx Amazon-Ressourcen wieder her: [Stellen Sie ein FSx Dateisystem wieder her](#)

Ausführliche Informationen zu FSx Amazon-Dateisystemen finden Sie in der [FSx Amazon-Dokumentation](#).

Mit Amazon arbeiten EC2

AWS Backup unterstützt EC2 Amazon-Instances.

- So sichern Sie Ressourcen: [Erste Schritte mit AWS Backup](#)
- So stellen Sie EC2 Amazon-Ressourcen wieder her: [Eine EC2 Amazon-Instance wiederherstellen](#)

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 EC2 Amazon-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 Sie Windows VSS-Backups](#).

AWS Backup startet Ihre EC2 Instances zu keinem Zeitpunkt neu.

Bilder und Schnappschüsse

Erstellt beim Sichern einer EC2 Amazon-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 die Instance von einem AMI aus gestartet wurde AWS Marketplace, hat die Instance einen Produktcode. Ein aus der Instance erstelltes AMI hat auch einen Produktcode. Bei Amazon EC2 können Sie ein AMI mit einem Produktcode nicht auf ein anderes Konto kopieren. Daher gilt AWS Backup auch diese Einschränkung.

Wenn Sie einen Amazon Machine Image (AMI) - oder Amazon EBS-Snapshot löschen, der AWS Backup mithilfe von verwendet wird, AWS Backup und Sie den EC2 Amazon-Papierkorb konfiguriert haben, können für das Image oder den Snapshot Gebühren gemäß der EC2 Amazon-Papierkorb-Richtlinie anfallen. Snapshots und Bilder im EC2 Amazon-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 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-Backup verknüpft sind. EC2 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 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 [EC2 Amazon-Instances](#) im EC2 Amazon-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: [Stellen Sie ein Amazon EFS-Dateisystem wieder her](#)

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 mit anderen nicht automatisierten Backup-Plänen erstellt wurden. Wenn Sie ihn als Ziel für andere Backup-Pläne verwenden, erhalten Sie die Fehlermeldung „unzureichende Berechtigungen“.

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 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: [Ein Amazon EBS-Volume wiederherstellen](#)

Weitere Informationen finden Sie auch im folgenden Tutorial: [Amazon EBS Backup and Restore Using AWS Backup](#)

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](#)
- [Backups von Amazon Relational Database Service](#)
- So stellen Sie Amazon-RDS-Ressourcen wieder her: [Stellen Sie eine RDS-Datenbank wieder her](#)
- So stellen Sie Aurora-Cluster wieder her: [Wiederherstellung eines Amazon-Aurora-Clusters](#)

Sie können dies auch anhand der folgenden Anleitung lernen: [Amazon RDS Backup and Restore Using AWS Backup](#)

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.

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.

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 Bereitstellung erfolgen). blue/green

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.

Arbeiten mit Aurora DSQL

AWS Backup unterstützt Aurora DSQL-Cluster für zentralisierte Sicherungs- und Wiederherstellungsvorgänge. Aurora DSQL ist eine serverlose, verteilte SQL-Datenbank, die ACID-Transaktionen mit starker Konsistenz und Snapshot-Isolation über mehrere hinweg bietet. AWS-Regionen

Aurora DSQL unterstützt sowohl Cluster-Konfigurationen mit einer Region als auch mit mehreren Regionen. Zu Clustern mit mehreren Regionen gehören verknüpfte Cluster-Regionen, die Lese- und Schreibvorgänge abwickeln, sowie Regionen, die am Konsens teilnehmen, ohne den Client-Verkehr zu bedienen.

- So sichern Sie Ressourcen: [Erste Schritte mit AWS Backup](#)
- So stellen Sie Aurora DSQL-Cluster wieder her: [Amazon Aurora DSQL Wiederherstellung](#)

Ausführliche Informationen zu Aurora DSQL finden Sie unter [Was ist Aurora DSQL?](#) im Aurora DSQL-Benutzerhandbuch.

Bei der Sicherung von Aurora DSQL-Clustern mit mehreren Regionen AWS Backup koordiniert es die Backup-Operationen in allen verknüpften Cluster-Regionen und nutzt gleichzeitig Zeugenregionen für die Transaktionskonsistenz. Dadurch wird sichergestellt, dass Ihr Backup einen konsistenten Status im gesamten verteilten Datenbanksystem erfasst.

Arbeiten mit AWS BackInt

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

- Anweisungen zum Sichern und Wiederherstellen von SAP HANA-Ressourcen: [Sicherung und Wiederherstellung von SAP HANA Amazon 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: [Ein Storage Gateway Gateway-Volume wiederherstellen](#).

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: [Einen Neptun-Cluster wiederherstellen](#).

Arbeiten mit Amazon Redshift und Amazon Redshift Serverless

AWS Backup unterstützt von Amazon Redshift bereitgestellte Cluster und Redshift Serverless-Namespaces.

- So [sichern Sie von Amazon Redshift](#) bereitgestellte Cluster.
- So [sichern Sie Redshift Serverless](#) Data Warehouses.
- So [stellen Sie Amazon Redshift wieder her](#).
- So [stellen Sie Redshift Serverless wieder her](#).

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 CloudFormation

AWS Backup unterstützt CloudFormation Vorlagen und Anwendungsstapel

- [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.

- [Sicherung von SAP HANA-Datenbanken auf EC2 Amazon-Instances](#)
- [Beginnen Sie mit AWS Systems Manager für SAP](#)
- [AWS Backint Agent für SAP HANA](#)

Arbeiten mit Amazon EKS

AWS Backup unterstützt Backups von Amazon EKS-Clustern, einschließlich Kubernetes-Clusterstatus und persistentem Speicher, der über einen persistenten Volume-Claim an den EKS-Cluster angehängt ist (EBS-Volumes, EFS-Dateisysteme und S3-Buckets).

Ein Amazon EKS-Backup erstellt einen zusammengesetzten Wiederherstellungspunkt, an dem für jede gesicherte Ressource ein untergeordneter Wiederherstellungspunkt eingerichtet wird.

- So sichern Sie Ressourcen: [Erste Schritte mit AWS Backup](#)
- So sichern Sie Amazon EKS-Cluster: [Amazon-EKS-Backups](#)
- So stellen Sie Amazon EKS-Cluster wieder her: [Einen Amazon EKS-Cluster wiederherstellen](#)

Ausführliche Informationen zu Amazon EKS finden Sie unter [Was ist Amazon EKS?](#) im Amazon EKS-Benutzerhandbuch.

Mit Amazon arbeiten GuardDuty

AWS Backup lässt sich in Amazon integrieren GuardDuty , um automatisierte Malware-Scans Ihrer Wiederherstellungspunkte zu ermöglichen. Diese Integration hilft Ihnen dabei, potenzielle Malware in Ihren EC2, EBS- und S3-Backups zu erkennen.

- Automatisiertes Scannen — Konfigurieren Sie Backup-Pläne so, dass Wiederherstellungspunkte automatisch gescannt werden, sobald sie erstellt werden
- Scannen auf Anforderung — Initiieren Sie mithilfe der StartScanJob API manuell Scans bestimmter Wiederherstellungspunkte
- Inkrementelles Scannen — Es werden nur Daten gescannt, die seit dem letzten Scan geändert wurden, um die Kosten zu senken
- Scanergebnisse — Zeigen Sie den Scanstatus und die Ergebnisse in der AWS Backup Konsole an und APIs

Um den Malware-Scan zu aktivieren, müssen Sie IAM-Rollen konfigurieren, mit denen GuardDuty Sie Ihre Wiederherstellungspunkte lesen und Scans AWS Backup initiieren können. Weitere Informationen finden Sie unter [the section called “Verwaltete Richtlinien”](#).

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. Im Folgenden finden Sie eine Liste der Dokumentation:

- [Services EC2 im Zusammenhang mit Amazon](#)
- [Verwendung AWS Backup mit Amazon EFS](#)
- [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](#)
- [Verwenden von AWS Backup mit FSx für Windows File Server](#)
- [Verwendung von AWS Backup with FSx for Lustre](#)
- [Ihre Volumes sichern](#)
- [Sichern und Wiederherstellen in Amazon DocumentDB](#)
- [Sichern und Wiederherstellen eines Amazon-Neptune-Clusters](#)

Erfassung, Kosten und Abrechnung für AWS Backup

AWS Backup Preisgestaltung

Aktuelle AWS Backup Preise finden Sie unter [AWS Backup Preisangaben](#).

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 [Feature-Verfügbarkeit 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 im Folgenden:

- [AWS Backup fügt eine neue Mehrparteien-Zulassung für Tresore mit logischem Luftspalt von Veliswa Boya](#) hinzu (Juni 2025)
- [Optimieren Sie die Suche und die Wiederherstellung auf Artekelebene mit AWS Backup](#) Mit Bismar Sethi (Dezember 2024).
- [Aufbau von Cyber-Resilienz mit AWS Backup logischem Air-Gap-Tresor](#). Mit Sushmitha Srinivasa Murthy und Sabith Venkitachalopathy (August 2024).
- [Hängen Sie ein EC2 Amazon-Schlüsselpaar an eine AWS Backup Wiederherstellung einer VMware virtuellen Maschine](#) an. Mit Olumuyiwa Koya und Kenie Ogunsemowo (August 2024).
- [Optimieren und automatisieren Sie die Compliance-Überwachung und -Berichterstattung mit AWS Backup Audit Manager](#). Mit Sabith Venkitachalopathy, Glenn Chia und Mark Rowland (Juni 2024).
- [Anwendungskonsistentes Backup für Windows-Anwendungen auf Amazon EC2 mit AWS Backup](#) Mit Bhaskar Mazumdar und Karthikeyan KM (Mai 2024).
- [AWS Backup Optimierung der Kosten](#). Mit Kenneth Hui (April 2024).

- [Entwicklung einer belastbaren und kostengünstigen Backup-Strategie für Amazon S3](#). Mit Mojgan Toth und Harish Mandhadi (März 2024).
- [Automatisieren Sie die Zustellung von AWS Backup Audit Manager Manager-Berichten per E-Mail](#). Mit Ezekiel Oyerinde, Charles Meruwoma und Sri Gudavalli. (Januar 2024)
- [Streamlining Point-in-Time Recovery \(PITR\) für Aurora](#) mit. AWS Backup Mit Enrique Ramirez (Januar 2024)
- [Backup und Wiederherstellen von VMware virtuellen 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 CSPM 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 \(und Optimierung der Disaster Recovery mithilfe von AWS Backup\)](#). 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, Ameer 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).
- [Point-in-time 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.

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 Management-Konsole im anderen Fenster folgen.

Voraussetzungen

Beginnen Sie erst, wenn Folgendes vorliegt:

- Ein AWS-Konto. Weitere Informationen finden Sie unter [AWS Konto erstellen](#).
- Mindestens eine Ressource, die von unterstützt wird AWS Backup. 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.

- Wenn Sie beabsichtigen, mehrere Ressourcentypen, wie Amazon EBS-Volumes und Amazon S3 S3-Buckets, in denselben Backup-Plan aufzunehmen, stellen Sie sicher, dass sich diese Ressourcen im selben Plan befinden. AWS-Region

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

1. Melden Sie sich AWS-Managementkonsole bei <https://console.aws.amazon.com/backup> an und öffnen Sie die AWS Backup Konsole.
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 verwendet werden. AWS Backup 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 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.

Um dieses Tutorial abzuschließen, können Sie sich mit Ihrem AWS-Konto Root-Benutzer bei der AWS-Managementkonsole 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.

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.

Opt-In für den Service

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 für NetApp ONTAP, wenn Sie die tagbasierte Ressourcenauswahl verwenden, Tags auf einzelne Volumes statt auf das gesamte Dateisystem an.

Die Opt-in-Optionen gelten für das jeweilige Konto und die AWS-Region. Wenn ein Konto in einer Region verwendet wird, um 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-Managementkonsole 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. Wählen Sie Bestätigen aus.

Backup-Pläne

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 Backup-Pläne erstellen, wenn es Workloads mit unterschiedlichen Backup-Anforderungen gibt. 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 Sie einen Backup-Plan](#)
- [Die Zusammenfassung des Backup-Plans verstehen](#)
- [Wählen Sie die zu AWS sichernden Dienste aus](#)

Erstellen Sie einen Backup-Plan

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

Themen

- [Erstellen Sie Backup-Pläne mithilfe der AWS Backup Konsole](#)
- [Erstellen Sie Backup-Pläne mit dem AWS CLI](#)

- [Backup-Plan-Optionen und -Konfiguration](#)
- [CloudFormation Vorlagen für Backup-Pläne](#)
- [Löschen Sie einen Backup-Plan](#)
- [Aktualisieren Sie einen Backup-Plan](#)

Erstellen Sie Backup-Pläne 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:

- Erstellen Sie einen Backup-Plan auf der Grundlage eines vorhandenen Plans
- Erstellen eines neuen Plans
- [Erstellen Sie einen Backup-Plan mit dem AWS CLI](#)

In diesem Verfahren erstellen wir einen neuen Plan. 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-Menü Standard oder wählen Sie Neuen Backup-Tresor erstellen, um einen Tresor zu erstellen.

- c. Wählen Sie im Menü für die Häufigkeit der Backups aus, wie oft dieser Plan ein Backup erstellen soll.
5. Backup-Zeitfenster:
 - a. Die Startzeit ist standardmäßig auf 12:30 Uhr (00:30 Uhr innerhalb von 24 Stunden) in der lokalen Zeitzone Ihres Systems voreingestellt.
 - 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. Stellen Sie sicher, dass genügend Zeit für den Abschluss des Backups zur Verfügung steht, auch wenn der Job am Ende des Startfensters gestartet wird.
6. [Kontinuierliche Backups und point-in-time Wiederherstellung \(PITR\)](#): Sie können „Kontinuierliche Backups für die point-in-time Wiederherstellung aktivieren“ (PITR) auswählen. Informationen dazu, welche Ressourcen für diese Art von Backup unterstützt werden, finden Sie in der [Feature-Verfügbarkeit 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) Sie können festlegen, dass mit jeder regelmäßigen Sicherung eines unterstützten Ressourcentyps ein Backup-Index erstellt wird (bei kontinuierlichen Backups werden tägliche Indizes erstellt). Nur Wiederherstellungspunkte (Backups), denen ein Index zugeordnet ist, können in eine [Backup-Suche](#) einbezogen werden.

Beispielsweise können Sie jedes Mal, wenn Ihr Backup-Plan ein S3-Backup erstellt, auch einen Backup-Index für dieses Backup erstellen lassen. Dadurch kann dieses spezielle Backup in eine future Suche aufgenommen werden.

Setzen Sie ein Häkchen neben den Ressourcentypen, für die Sie Indizes erstellen möchten.

9. (Optional) Aktivieren Sie den Malware-Scan, damit Backups nach ihrer Erstellung automatisch gescannt werden. Geben Sie bei der Konfiguration des Malware-Schutzes an, welche Ressourcentypen gescannt werden sollen (Amazon EC2, Amazon EBS, Amazon S3 oder alle unterstützten Ressourcen) und welche Scantypen (vollständig oder inkrementell) gescannt werden sollen. Der Malware-Scan gilt nur für die von Ihnen ausgewählten Ressourcentypen. Wenn Ihr Backup-Plan beispielsweise sowohl Amazon S3- als auch EC2 Amazon-Ressourcen umfasst, Sie den Malware-Scan jedoch nur für Amazon aktivieren EC2, scannt der Service nur Ihre EC2 Backups. Für jede Backup-Regel können Sie konfigurieren, welcher Scan-Typ verwendet werden soll. Der Zeitplan der Backup-Regel bestimmt, wie oft der Scan-Typ durchgeführt wird.

 Important

Bevor Sie den Malware-Schutz aktivieren, stellen Sie sicher, dass Ihre Backup-Rolle und Ihre Scanner-Rolle über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie in [der Dokumentation zu den Berechtigungen](#).

10. (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.
11. (Optional) Zu Wiederherstellungspunkten hinzugefügte Tags.
12. Wenn alle Abschnitte Ihren Spezifikationen entsprechen, wählen Sie Backup-Regel speichern.

Erstellen Sie Backup-Pläne 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
  "IndexActions": [
    {
      "ResourceTypes": [ "string" ]
    }
  ],
  "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- und Rate-Ausdrücke](#). Weitere Informationen zu Zeitzonen finden Sie [TimeZone](#) in der Amazon Location Service API-Referenz.

Backup-Plan-Optionen und -Konfiguration

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

Name des Backup-Plans

Sie müssen einen Namen für Ihren Backup-Plan angeben. Namen sind auf 50 Zeichen begrenzt, einschließlich alphanumerischer Zeichen, Bindestriche, Unterstriche und Punkte.

Backup-Regeln

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-Häufigkeit

Die Häufigkeit der Backups 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 kontinuierlichen Backups finden Sie unter [Point-in-Time Wiederherstellung](#).

Backup window

Backup-Fenster bestehen aus dem Zeitpunkt, an dem das Backup-Fenster beginnt, und der Dauer des Fensters in Stunden. Backup-Aufträge 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
- Abschluss innerhalb von 7 Tagen

(Der Parameter vollständig innerhalb des Parameters gilt nicht für FSx Amazon-Ressourcen)

Sie können die Backup-Häufigkeit und die Anfangszeit des Backup-Fensters mithilfe eines Cron-Ausdrucks anpassen. Die sechs Felder mit AWS Cron-Ausdrücken finden Sie unter [Cron und Rate-Ausdrücke](#) im EventBridge Amazon-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.

Backup-Pläne in einer Zeitzone, in der die Sommerzeit eingehalten wird, könnten durch die Zeitverschiebung beeinträchtigt werden. Sie können zu UTC wechseln oder an dem Tag, an dem sich die Zeit verschiebt, ein manuelles Backup erstellen. Weitere Informationen finden Sie unter [Sommerzeit im EventBridge Scheduler](#).

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.

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

Während dieses Startfensters	erstellt diese Regel 1 Backup
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. [Feature-Verfügbarkeit 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 warmen Speicher 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

Ressourcentyp	Inkrementelles oder vollständiges Backup im Cold Storage
Amazon EBS (mit EBS Snapshot Archive)	Vollständig; inkrementelle Backups werden nach der Umstellung vollständig.
Amazon EFS	Inkrementell
SAP HANA-Datenbanken, die auf EC2 Amazon-Instances laufen	Inkrementell
Amazon Timestream	Inkrementell
VMware virtuelle 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-stepAnweisungen zum Erstellen eines Backup-Tresors finden Sie unter. Erstellung und Löschung von Backup-Tresoren](#)

In Regionen kopieren

Im Rahmen Ihres Backup-Plans können Sie optional eine Sicherungskopie in demselben oder einem anderen Ordner erstellen AWS-Region. Diese Kopien können entweder in demselben Konto oder in einem anderen Konto erstellt werden. 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 übernehmen 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 Archivspeicher übertragene Backups müssen mindestens

90 Tage lang im Archivspeicher 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.

Wenn der Wert für [Lifecycle:DeleteAfterDays](#) (in der Konsole als Ablaufen angezeigt) nicht in den Kopiereinstellungen angegeben ist, entspricht die Kopie den Lebenszykluseinstellungen des Backups, aus dem sie kopiert wurde.

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

Mit den erweiterten Backup-Einstellungen können Sie ressourcenspezifische Backup-Optionen für verschiedene AWS Dienste konfigurieren.

EC2 Erweiterte Backup-Einstellungen von Amazon

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

Erweiterte Backup-Einstellungen von Amazon S3

AWS Backup bietet erweiterte Einstellungen, mit denen Sie steuern können, welche Metadaten in Ihren Amazon S3 S3-Backups enthalten sind. Sie können optional Zugriffskontrolllisten (ACLs) und Objekt-Tags aus Ihren Backups ausschließen. Dies entspricht den Best Practices von Amazon S3, bei denen Berechtigungen auf Bucket-Ebene statt auf Objektebene verwendet werden. ACLs

Ausführliche Informationen zur Konfiguration von Amazon S3 S3-Backup-Optionen ACLs und Objekt-Tags finden Sie unter [Erweiterte Amazon S3 S3-Backup-Einstellungen](#).

 Important

Wenn Sie die ACLs von Backups ausschließen, verwenden Objekte, die ohne ACLs diese Daten wiederhergestellt wurden, die standardmäßigen Besitzeinstellungen des Ziel-Buckets. Der Ziel-Bucket muss über eine entsprechende Objektbesitzkonfiguration verfügen.

 Note

Wenn ein kontinuierlicher Backup-Job für einen Amazon S3 S3-Bucket ausgeführt wird und Sie einen Snapshot-Backup-Job initiieren, verwendet der Snapshot dieselben ACL- und Objekt-Tag-Einstellungen wie das kontinuierliche Backup, unabhängig von den Einstellungen, die für den Snapshot-Job angegeben wurden.

Scannen nach Schadsoftware

AWS Backup lässt sich in Amazon integrieren GuardDuty , um automatisierte Malware-Scans Ihrer Wiederherstellungspunkte zu ermöglichen. Wenn Sie den Malware-Scan in Ihrem Backup-Plan aktivieren, scannt es Ihre Backups AWS Backup automatisch auf Malware und liefert Scanergebnisse, damit Sie fundierte Entscheidungen über die Wiederherstellung Ihrer Daten treffen können.

So konfigurieren Sie den Malware-Scan für Ihren Backup-Plan:

1. Erstellen Sie eine IAM-Rolle, die der AWS verwalteten Richtlinie vertraut, `malware-protection.guardduty.amazonaws.com` und fügen Sie sie hinzu. `AWSBackupGuardDutyRolePolicyForScans`
2. Ordnen Sie die AWS verwaltete Richtlinie der IAM-Rolle Ihrer Backup-Auswahl `AWSBackupServiceRolePolicyForScans` zu.
3. Fügen Sie in der Konfiguration Ihres Backup-Plans Scaneinstellungen hinzu, die Folgendes angeben:
 - Der Scandienst (GuardDuty)
 - Die zu scannenden Ressourcentypen (Amazon EC2, Amazon EBS, Amazon S3)
 - Die IAM-Rolle, die ARN übernehmen GuardDuty soll
4. Konfigurieren Sie die Scanaktionen in Ihren Backup-Regeln, um Folgendes anzugeben:

- Der Scandienst (GuardDuty)
- Der Scan-Typ (inkrementeller oder vollständiger Scan)

Weitere Informationen zu den verwalteten Richtlinien finden Sie unter [the section called “AWSBackupGuardDutyRolePolicyForScans”](#) und [the section called “AWSBackupServiceRolePolicyForScans”](#).

CloudFormation Vorlagen für Backup-Pläne

Wir stellen Ihnen zwei 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, *service-role* ersetzen Sie sie 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
```

Löschen Sie einen Backup-Plan

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-Managementkonsole 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 Sie einen Backup-Plan

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 Backup-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.

Die Zusammenfassung des Backup-Plans verstehen

Die Funktion zur Zusammenfassung des Backup-Plans bietet einen umfassenden Überblick über die Konfiguration Ihres Backup-Plans, sodass Sie überprüfen können, ob Ihre Backup-Strategie Ihren Anforderungen entspricht. Die Zusammenfassung umfasst drei Hauptkomponenten, mit denen Kunden häufig konfrontiert werden, wenn sie komplexe Backup-Konfigurationen für mehrere AWS Services verwalten.

Zusammenfassung der Komponenten

Jede Zusammenfassung des Sicherungsplans enthält die folgenden Informationen:

- Die nächsten 10 geplanten Backup-Läufe: Zeigt an, wann Ihre Backup-Regeln ausgeführt werden, einschließlich zusammengeführter Regeln und der korrekten Handhabung von Zeitzonen
- Hinweise zur Funktionskompatibilität: Informationen darüber, welche Dienste point-in-time Recovery (PITR) und Cold-Tier-Storage unterstützen, sofern diese Teil Ihrer Backup-Plan-Regel sind.

Geplante Backups werden als Vorschau ausgeführt

In der Vorschau für geplante Läufe werden bis zu 10 future Backup-Ausführungen basierend auf den Regeln Ihres Backupplans angezeigt. Diese Vorschau hilft Ihnen zu verstehen, wann Backups durchgeführt werden und wie mehrere Regeln miteinander interagieren.

Wie mehrere Regeln zusammengeführt werden

Wenn Sie mehrere Backup-Regeln in einem Plan haben, AWS Backup wendet die Zusammenführungslogik an, um das endgültige Backup-Verhalten zu bestimmen:

- Überlappende Backup-Fenster: Es hat sich bewährt, zwei Regeln mit widersprüchlichen Regeln nicht zu verwenden. Wenn zwei Regeln gleichzeitig ausgeführt werden würden, wird eine AWS Backup ausgewählt.
- Kombinationen aus PITR und Snapshot: PITR gilt für unterstützte Ressourcen, während Snapshots für alle Ressourcen in der Auswahl gelten
- Mehrere Zeitzonen: Jede Regel berücksichtigt ihre konfigurierte Zeitzone für die Ausführungsplanung

- **Regionsübergreifende Kopieraktionen:** Kopieraktionen werden beibehalten und mit ihren Zielinformationen angezeigt. Beachten Sie, dass, wenn eine Kopierregel an eine widersprüchliche Zeitplanregel angehängt ist, die Kopierregel nur ausgeführt wird, wenn die Zeitplanregel ausgeführt wurde.

Example Beispiel für das Zusammenführen von Regeln

Stellen Sie sich einen Backup-Plan mit zwei Regeln vor:

- Regel 1: Täglicher Snapshot um 8 Uhr PDT, Aufbewahrung 35 Tage
- Regel 2: Wöchentlicher Snapshot um 8 Uhr PDT, Aufbewahrung 90 Tage

Wenn beide Regeln am selben Tag (z. B. Sonntag) ausgeführt würden, wird in der Vorschau Regel 2 angezeigt, da sie länger aufbewahrt wird (90 Tage gegenüber 35 Tagen).

Arten der Ausführung

In der Vorschau für geplante Läufe werden je nach Ihrer Regelkonfiguration verschiedene Ausführungstypen angezeigt:

- **CONTINUOUS:** Kontinuierliche Backups für unterstützte Dienste
- **SNAPSHOTS:** Snapshot-Backups (periodische Backups) für alle Ressourcen in der Auswahl
- **CONTINUOUS_AND_SNAPSHOTS:** Point-in-time-restore (PITR) für Ressourcentypen, die dies unterstützen; Snapshot (periodisch) für alle anderen Ressourcentypen.

Überprüfung der Funktionskompatibilität

Die Zusammenfassung enthält Hinweise zur Kompatibilität, damit Sie besser verstehen, welche AWS Dienste erweiterte Backup-Funktionen unterstützen. Dadurch werden Konfigurationsfehler und unerwartete Kosten vermieden.

Point-in-time Unterstützung bei der Wiederherstellung

Wenn Sie kontinuierliche Backups in einer Regel aktivieren, werden Sie in der Zusammenfassung daran erinnert, dass PITR nur für folgende Zwecke unterstützt wird:

- Aurora-Datenbanken

- Amazon-RDS-Datenbanken
- SAP HANA-Datenbanken
- Amazon-S3-Buckets

Unterstützung für Cold-Tier-Speicher

Wenn Sie Cold-Tier-Übergänge konfigurieren, zeigt die Zusammenfassung, welche Dienste diese Funktion unterstützen:

- Amazon-DynamoDB-Tabellen
- Dateisysteme des Amazon Elastic File System
- SAP HANA-Datenbanken
- Amazon Timestream Timestream-Datenbanken
- VMware virtuelle Maschinen

Zugreifen auf Zusammenfassungen von Backup-Plänen

Nachdem Sie einen Backup-Plan erstellt oder aktualisiert haben, können Sie sich die Zusammenfassungen der Backup-Pläne in der AWS Backup Konsole ansehen. Die Zusammenfassung wird auf der Seite mit den Plandetails angezeigt und bietet sofortiges Feedback zu Ihrer Konfiguration.

Um eine Zusammenfassung des Backup-Plans einzusehen

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 den Backup-Plan aus, den Sie überprüfen möchten.
4. Die Zusammenfassung des Backup-Plans wird auf der Seite mit den Plandetails angezeigt. Erweitern Sie die Zusammenfassung, um geplante Läufe und Kompatibilitätshinweise einzusehen.

Sie können Informationen zum Backup-Plan auch mit den folgenden Methoden abrufen AWS CLI:

```
aws backup get-backup-plan --backup-plan-id 012345678
```

Wählen Sie die zu AWS sichernden Dienste aus

Melden Sie sich für Dienste an und weisen Sie dann Ressourcen zu

AWS Backup funktioniert mit vielen [verschiedenen AWS Diensten](#). Bevor Sie entscheiden, welche Dienste in den Backup-Plan aufgenommen werden [AWS CLI](#)sollen, verwenden Sie die [AWS Backup Konsole](#) oder entscheiden Sie sich für die Verwendung AWS Backup mit diesen Diensten.

Geben Sie dann in jedem Backup-Plan in der [Konsole](#) oder über die [CLI](#) an, welche Ressourcentypen in diesen Plan aufgenommen werden sollen.

Sie können sich beispielsweise für alle Services entscheiden, die dies AWS Backup unterstützen, und dann nur Amazon S3 S3-Buckets und Aurora-Cluster in einen Backup-Plan aufnehmen.

Themen

- [AWS Backup Service-Opt-In](#)
- [Ressourcenzuweisung für den Backup-Plan](#)
- [Weisen Sie Ressourcen mithilfe der AWS Backup Konsole zu](#)
- [Weisen Sie Ressourcen zu mit AWS CLI](#)
- [Weisen Sie AWS Backup Ressourcen zu über CloudFormation](#)
- [Kontingente für Ressourcenzuweisungen im Backupplan](#)

AWS Backup Service-Opt-In

Service-Opt-In über die Konsole AWS Backup

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

1. Melden Sie sich AWS-Managementkonsole bei <https://console.aws.amazon.com/backup> an und öffnen Sie die AWS Backup Konsole.
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 verwendet werden. AWS Backup 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

Service-Opt-In über AWS CLI

Verwenden Sie den [aws backup update-region-settings](#) Befehl, um die Dienste (Ressourcentypen) zu ändern, die Ihr Konto oder Ihre Organisation AWS Backup zur Orchestrierung der Backup-Erstellung verwenden wird. Verwenden Sie den [aws backup describe-region-settings](#) Befehl, um zu ermitteln, für welche Dienste Sie sich in einer bestimmten Region entschieden haben.

Ressourcenzuweisung für den Backup-Plan

Über die [AWS Backup Konsole](#) oder über [AWS CLI](#) die Konsole gibt die Ressourcenzuweisung in Ihrem Backup-Plan an, welche Ressourcen enthalten AWS Backup sein sollen. AWS Backup bietet sowohl einfache Standardeinstellungen als auch detaillierte Steuerelemente für die Zuweisung von Ressourcen.

Sie können Ressourcen auf folgende Weise zuweisen:

- Weisen Sie dem Backup-Plan explizit Ressourcentypen zu
- Schließt alle Ressourcen ein (scannt AWS Backup dann nach allen unterstützten Ressourcentypen)
- Verwenden Sie Tags, um Ressourcen ein- oder auszuschließen

Wenn Sie Tags nur für die Ressourcenzuweisung verwenden, gelten die Opt-In-Einstellungen für den Service trotzdem.

Sie können die Ressourcenzuweisung mithilfe von Bedingungen und Tags weiter verfeinern. Es gibt einige Beschränkungen in Bezug auf die Anzahl der ARNs Bedingungen und Tags, die in einer einzelnen Ressourcenzuweisung verwendet werden können.

Die Ressourcenauswahl über CLI basiert auf Dienstnamen und Ressourcentypen. Überlegungen [Weisen Sie Ressourcen zu mit AWS CLI](#) zur Ressourcenauswahl finden Sie unter.

Weisen Sie Ressourcen mithilfe der AWS Backup Konsole zu

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.

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 bestimmte Ressourcen IDs aus den ausgewählten Ressourcentypen ausschließen. 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 mit 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 zu Stichwörtern finden Sie unter [AWS Ressourcen taggen](#).

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 einen Schlüssel aus der Liste aus.
2. Wählen Sie eine Bedingung für den Wert aus der Liste 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 einen Wert aus der Liste aus.
4. Wählen Sie Tag hinzufügen aus, um mithilfe eines anderen Tags die Auswahl weiter zu verfeinern.

Weisen Sie Ressourcen zu mit AWS CLI

Filtern Sie nach Diensten oder Ressourcentypen

Die Ressourcenauswahl basiert auf Dienstnamen und Ressourcentypen. Die Methode der Ressourcenauswahl bestimmt, ob eine Ressource in der Sicherung enthalten ist. Diese Aufnahme hängt von den Namen der Dienste, den Ressourcentypen und den Opt-in-Einstellungen ab.

Auswahl nach Dienstnamen

Wenn Sie in der Ressourcenauswahl nur einen Dienstnamen angeben, hängt die Einbeziehung des Backups von der Opt-in-Einstellung für die zugrunde liegenden Ressourcentypen ab. Beispielsweise werden EC2 Instanzen mit nur dann in das Backup aufgenommen `arn:aws:ec2:*`, wenn die Opt-In-Einstellung für den EC2 Ressourcentyp aktiviert ist.

Auswahl nach Ressourcentyp

Wenn Sie die Ressourcenauswahl direkt mit dem Ressourcentyp angeben, wird sie unabhängig von der Opt-In-Einstellung für den jeweiligen Dienst in das Backup aufgenommen. Bei `arn:aws:ec2:::instance/*` beispielsweise werden EC2 Instanzen unabhängig von der Opt-In-Einstellung gesichert.

Typen gemeinsam genutzter Ressourcen

Wenn sich mehrere Ressourcen denselben Ressourcentyp teilen, müssen Sie die Opt-in-Einstellungen für bestimmte Ressourcentypen aktivieren, um Backups zu initiieren.

Example

Aurora- und RDS-Cluster teilen sich das ARN-Format: `arn:aws:rds:::cluster:*`. Um Aurora-Datenbanken zu sichern, müssen Sie die Opt-In-Einstellung für Aurora aktivieren.

FSx und FSx für OpenZFS das ARN-Format teilen. `arn:aws:fsx:::file-system/*` Aktivieren Sie die entsprechenden Opt-In-Einstellungen, um diese Dateisysteme zu sichern.

Verwenden Sie eine JSON-Datei, um die Ressourcenzuweisung für den Sicherungsplan zu definieren

Sie können eine Ressourcenzuweisung in einem JSON-Dokument definieren.

Sie können Bedingungen, Tags oder Ressourcen angeben, um zu definieren, was in Ihrem Backup-Plan enthalten sein soll. Weitere Informationen zur Bestimmung der einzubeziehenden Parameter finden Sie unter [BackupSelection](#).

Mit dieser Beispielressourcenzuweisung werden alle EC2 Amazon-Instances dem Backup-Plan ***BACKUP-PLAN-ID*** zugewiesen:

```
{
  "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 zusammen mit dem entsprechenden 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 `"backup": "true"` markiert sind, aber schließen Sie EBS-Volumes aus

```
{
```

```

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

```

Important

RDS, Aurora, Neptune und DocumentDB beginnen ARNs mit. `arn:aws:rds:` Verfeinern Sie Ihre Auswahl mit Tags und Bedingungsoperatoren, wenn Sie nicht beabsichtigen, all diese Typen einzubeziehen.

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

```

Weisen Sie AWS Backup Ressourcen zu über CloudFormation

Diese end-to-end 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 Ressourcenzuweisungen im Backupplan

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)

Sicherungstresore

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](#).

Die folgenden Abschnitte bieten einen Überblick darüber, wie Sie Ihre Backup-Tresore in AWS Backup verwalten können.

Themen

- [Erstellung und Löschung von Backup-Tresoren](#)
- [Logischer Air-Gapped Vault](#)
- [Richtlinien für den Tresorzugriff](#)
- [AWS Backup Vault Lock](#)

Erstellung und Löschung von Backup-Tresoren

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

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

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

Erforderliche Berechtigungen

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Sid": "AllowCreateBackupVault",
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:us-east-1:444455556666:backup-vault:*"
    },
    {
      "Sid": "AllowMountCapsule",
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```


Erstellen eines Backup-Tresors (Konsole)

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.

So erstellen Sie einen Backup-Tresor

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 [Feature-Verfügbarkeit 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.

- 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.

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.

Löschen eines 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.

Sie können den Standard-Backup-Tresor oder den automatischen Amazon EFS-Backup-Tresor nicht mit dem löschen AWS-Managementkonsole. Sie können einen Standard-Backup-Tresor mit dem löschen AWS CLI , falls dieser leer ist. Wenn Sie jedoch die AWS Backup Konsole öffnen und diese Region auswählen, erstellt die Konsole den Standard-Backup-Tresor neu. Sie können unbenutzte Snapshots im automatischen Backup-Tresor von Amazon EFS löschen.

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

1. Melden Sie sich bei der AWS-Managementkonsole 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 Tresors ein und wählen Sie dann Backup-Tresor löschen.

Logischer Air-Gapped Vault

Überblick über Tresore mit logischem Air-Gap

AWS Backup bietet einen sekundären Tresortyp, in dem Backups in einem Container mit zusätzlichen Sicherheitsfunktionen gespeichert werden können. Ein Tresor mit logischem Air-Gapped ist ein spezialisierter Tresor, der mehr Sicherheit bietet als ein herkömmlicher Backup-Tresor und die Möglichkeit bietet, den Zugriff auf den Tresor gemeinsam mit anderen Konten zu nutzen, sodass Recovery Time Objectives (RTOs) im Falle eines Vorfalls, der eine schnelle Wiederherstellung von Ressourcen erfordert, schneller und flexibler gestaltet werden können.

Logical Air-Gapped Tresore sind mit zusätzlichen Schutzfunktionen ausgestattet. Jeder Tresor ist entweder mit einem [AWS eigenen Schlüssel](#) (Standard) oder optional mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt, und jeder Tresor ist mit dem Compliance-Modus von [AWS Backup Vault Lock](#) ausgestattet. Die Informationen zum Typ des Verschlüsselungsschlüssels sind in der Konsole sichtbar und sorgen so für AWS Backup APIs Transparenz und Konformitätsberichte.

Sie können Ihre Tresore mit logischem Air-Gap mit [Multi-Party Approval](#) (MPA) integrieren, um die Wiederherstellung von Backups in den Tresoren auch dann zu ermöglichen, wenn auf das Konto, das den Tresor besitzt, nicht zugegriffen werden kann. Dies trägt zur Aufrechterhaltung der Geschäftskontinuität bei. Darüber hinaus können Sie sich für die Integration mit [AWS Resource Access Manager](#) (RAM) entscheiden, um einen Tresor mit logischem Air-Gap gemeinsam mit anderen AWS Konten (einschließlich Konten in anderen Organisationen) zu nutzen, sodass die im Tresor gespeicherten Backups von einem Konto wiederhergestellt werden können, mit dem der Tresor gemeinsam genutzt wird, falls dies für die Wiederherstellung nach Datenverlust oder für [Wiederherstellungstests](#) erforderlich ist. Als Teil dieser zusätzlichen Sicherheit speichert ein Tresor mit logischem Air-Gap seine Backups in einem AWS Backup diensteigenen Konto (was dazu führt, dass Backups in AWS CloudTrail Protokollen als außerhalb Ihrer Organisation gemeinsam genutzt angezeigt werden).

Um die Ausfallsicherheit zu erhöhen, empfehlen wir, regionsübergreifende Kopien in Tresoren mit logischem Air-Gap in denselben oder separaten Konten zu erstellen. Wenn Sie jedoch die Speicherkosten senken möchten, indem Sie nur eine einzige Kopie verwalten, können Sie nach der Einführung in MPA [primäre Backups für Tresore mit logischem Air-Gap](#) verwenden. AWS

[Sie können die Speicherpreise für Backups der unterstützten Services in einem Tresor mit logischem Air-Gap auf der Preisseite einsehen.](#)[AWS Backup](#)

Informationen zu [Feature-Verfügbarkeit nach Ressource](#) den Ressourcentypen, die Sie in einen Tresor mit logischem Air-Gap kopieren können, finden Sie unter.

Themen

- [Anwendungsfall für Tresore mit logischem Air-Gap](#)
- [Vergleich und Gegenüberstellung mit einem Standard-Backup-Tresor](#)
- [Erstellen Sie einen Tresor mit logischem Air-Gap](#)
- [Details zum Tresor mit logischem Air-Gap anzeigen](#)
- [Erstellen von Backups in einem Tresor mit logischem Air-Gap](#)
- [Teilen Sie einen Tresor mit logischem Air-Gap](#)
- [Stellen Sie ein Backup aus einem Tresor mit logischem Air-Gap wieder her](#)
- [Löschen Sie einen Tresor mit logischem Air-Gap](#)
- [Zusätzliche programmatische Optionen für Tresore mit logischem Air-Gap](#)
- [Grundlegendes zu Verschlüsselungsschlüsseltypen für Tresore mit logischem Air-Gap](#)
- [Beheben Sie ein Problem mit einem Tresor mit logischem Air-Gap](#)
- [Primäre Backups zu logischen Air-Gapped Vaults](#)
- [Genehmigung durch mehrere Parteien für Tresore mit logischem Air-Gap](#)

Anwendungsfall für Tresore mit logischem Air-Gap

Ein logischer Air-Gapped Vault ist ein sekundärer Tresor, der als Teil einer Datenschutzstrategie dient. Dieser Tresor kann dazu beitragen, die Aufbewahrungsstrategie und die Wiederherstellung Ihres Unternehmens zu verbessern, wenn Sie einen Tresor für Ihre Backups benötigen

- Wird automatisch mit einer Tresorsperre im [Compliance-Modus](#) eingerichtet
- Bietet standardmäßig Verschlüsselung mit einem AWS eigenen Schlüssel. Optional können Sie einen vom Kunden verwalteten Schlüssel bereitstellen
- Enthält Backups, die über AWS RAM oder MPA mit einem anderen Konto als dem Konto, das die Sicherung erstellt hat, geteilt und von dort wiederhergestellt werden können

Überlegungen und Einschränkungen

- Regionsübergreifendes Kopieren in oder aus einem Tresor mit logischem Air-Gap ist derzeit nicht für Backups verfügbar, die Amazon Aurora, Amazon DocumentDB und Amazon Neptune enthalten.

- Ein Backup, das ein oder mehrere Amazon EBS-Volumes enthält und in einen Tresor mit logischem Air-Gap kopiert wird, muss kleiner als 16 TB sein. Größere Backups für diesen Ressourcentyp werden nicht unterstützt.
- EC2 Amazon-Angebote [EC2 sind zulässig AMIs](#). Wenn diese Einstellung in Ihrem Konto aktiviert ist, fügen Sie den Alias `aws-backup-vault` zu Ihrer Zulassungsliste hinzu.

Wenn dieser Alias nicht enthalten ist, schlagen Kopiervorgänge von einem Tresor mit logischem Air-Gap in einen Backup-Tresor und Wiederherstellungsvorgänge von EC2 Instances aus einem Tresor mit logischem Air-Gap fehl und es wird eine Fehlermeldung wie „Source AMI ami-xxxxxx not found in Region“ angezeigt.

- Der ARN (Amazon Resource Name) eines Wiederherstellungspunkts, der in einem Tresor mit logischem Air-Gap gespeichert ist, wird anstelle des zugrunde liegenden Ressourcentyps verwendet. backup Wenn der ursprüngliche ARN beispielsweise mit `beginntarn:aws:ec2:region::image/ami-*`, dann ist dies der ARN des Wiederherstellungspunkts im Tresor mit logischem Air-Gapped. `arn:aws:backup:region:account-id:recovery-point:*`

Sie können den CLI-Befehl verwenden [list-recovery-points-by-backup-vault](#), um den ARN zu ermitteln.

Vergleich und Gegenüberstellung mit einem Standard-Backup-Tresor

Ein Backup-Tresor ist der primäre und standardmäßige Tresortyp, der in AWS Backup verwendet wird. 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 primäre Backups oder Kopien von Backups gespeichert, die ursprünglich in einem Standard-Backup-Tresor erstellt und gespeichert wurden.

Backup-Tresore werden mit einem Schlüssel verschlüsselt, einem Sicherheitsmechanismus, der den Zugriff auf die vorgesehenen Benutzer beschränkt. Diese Schlüssel können vom Kunden verwaltet oder AWS verwaltet werden. Informationen zum [Verschlüsselungsverhalten bei Kopieraufträgen](#), einschließlich des Kopierens in einen Tresor mit logischem Air-Gap, finden Sie unter [Kopierverschlüsselung](#).

Darüber hinaus kann ein Backup-Tresor durch eine Tresorsperre zusätzliche Sicherheit bieten. Logischerweise sind Tresore mit Air-Gaps im Compliance-Modus mit einem Tresorschloss ausgestattet.

Ähnlich wie Backup-Tresore unterstützen auch Tresore mit logischem Air-Gap [eingeschränkte](#) Tags für Amazon-Backups. EC2

Feature	Sicherungstresor	Logischer Air-Gapped Vault
AWS Backup Audit Manager	Sie können AWS Backup Audit Manager verwenden Steuerelemente und Abhilfemaßnahmen , um Ihre Backup-Tresore zu überwachen.	Stellen Sie sicher, dass ein Backup einer bestimmten Ressource in mindestens einem Tresor mit logischem Air-Gap nach einem von Ihnen festgelegten Zeitplan gespeichert wird, zusätzlich zu den für Standardtresore verfügbaren Kontrollen.
Fakturierung	Speicher- und Datenübertragungsgebühren für Ressourcen, die vollständig von "verwaltet werden, AWS Backup fallen unter"" an.AWS Backup Speicher- und Datenübertragungsgebühren für andere Arten von Ressourcen fallen im Rahmen der jeweiligen Dienste an. Beispielsweise werden Amazon EBS-Backups unter „Amazon EBS“ angezeigt ; Amazon S3 S3-Backups werden unter "AWS Backup“ angezeigt.	Alle Abrechnungsgebühren für diese Tresore (Speicherung oder Datenübertragung) werden unter "" ausgewiesen.AWS Backup

Feature	Sicherungstresor	Logischer Air-Gapped Vault
Regionen	Verfügbar in allen Regionen, in denen tätig ist AWS Backup	Verfügbar in den meisten Regionen, die von unterstützt werden AWS Backup. Derzeit nicht verfügbar in Asien-Pazifik (Malaysia), Kanada West (Calgary), Mexiko (Zentral), Asien-Pazifik (Thailand), Asien-Pazifik (Taipeh), Asien-Pazifik (Neuseeland), China (Peking), China (Ningxia), AWS GovCloud (USA-Ost) oder AWS GovCloud (US-West).
Ressourcen	Kann Kopien von Backups für die meisten Ressourcentypen speichern, die kontoübergreifendes Kopieren unterstützen.	Ressourcen, die in diesen Tresor kopiert werden können, finden Sie in der Feature-Verfügbarkeit nach Ressource Spalte Tresor mit logischem Air-Gapped unter.
Wiederherstellen	Backups können mit demselben Konto wiederhergestellt werden, zu dem der Tresor gehört.	Backups können mit einem anderen Konto als dem, zu dem der Tresor gehört, wiederhergestellt werden, wenn der Tresor mit diesem separaten Konto geteilt wird.

Feature	Sicherungstresor	Logischer Air-Gapped Vault
Sicherheit	Kann optional mit einem Schlüssel verschlüsselt werden (kundenseitig verwaltet oder von AWS verwaltet) Wahlweise kann eine Tresorsperre im Compliance- oder Governance-Modus verwendet werden	Kann mit einem AWS eigenen Schlüssel oder einem vom Kunden verwalteten Schlüssel verschlüsselt werden Ist immer mit einer Tresorsperre im Compliance-Modus gesperrt Informationen zum Typ des Verschlüsselungsschlüssels bleiben erhalten und sind sichtbar, wenn Tresore über AWS RAM MPA gemeinsam genutzt werden
Teilen	Zugriff kann über Richtlinien und AWS Organizations verwaltet werden. Nicht kompatibel mit AWS RAM	Kann optional mit AWS RAM über mehrere Konten hinweg gemeinsam genutzt werden

Erstellen Sie einen Tresor mit logischem Air-Gap

Sie können einen Tresor mit logischem Air-Gap entweder über die AWS Backup Konsole oder über eine Kombination aus AWS Backup und AWS RAM CLI-Befehlen erstellen.

Jeder Logic Air-Gapped ist im Compliance-Modus mit einer Tresorsperre ausgestattet. Weitere Informationen finden Sie unter [AWS Backup Vault Lock](#), um die für Ihren Betrieb am besten geeigneten Werte für die Aufbewahrungsdauer zu ermitteln

Console

Erstellen eines logischen Air-Gapped Vault von der Konsole aus

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. Wählen Sie das Optionsfeld für Logically Air-Gapped Vault aus.
6. (Optional) Wählen Sie einen Verschlüsselungsschlüssel. Sie können einen vom Kunden verwalteten KMS-Schlüssel für zusätzliche Kontrolle über die Verschlüsselung auswählen oder den standardmäßigen AWS eigenen Schlüssel verwenden (empfohlen).
7. 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.

Der zulässige Mindestwert ist 7 Tage. Werte für Monate und Jahre entsprechen diesem Mindestwert.

8. 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.

9. (Optional) Legen Sie den Verschlüsselungsschlüssel fest.

Geben Sie den Schlüssel an, der mit Ihrem Tresor verwendet werden soll. Sie können einen AWS eigenen Schlüssel (verwaltet von AWS Backup) wählen oder den ARN für einen vom Kunden verwalteten Schlüssel eingeben, der vorzugsweise zu einem anderen Konto gehört, auf das Sie Zugriff haben. AWS Backup empfiehlt die Verwendung eines AWS eigenen Schlüssels.

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

13. Die Konsole leitet Sie zur Detailseite Ihres neuen Tresors weiter. Vergewissern Sie sich, dass die Tresordetails wie gewünscht festgelegt sind.
14. Wählen Sie Tresore aus, um die Tresore in Ihrem Konto anzuzeigen. Ihr Tresor mit logischem Air-Gap wird angezeigt. Der KMS-Schlüssel ist etwa 1 bis 3 Minuten nach der Erstellung des Tresors verfügbar. Aktualisieren Sie die Seite, um den zugehörigen Schlüssel zu sehen. Sobald der Schlüssel sichtbar ist, ist der Tresor verfügbar und kann verwendet werden.

AWS CLI

Erstellen Sie über die CLI einen Tresor mit logischem Air-Gapped

Sie können es verwenden AWS CLI , 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.

Verwenden Sie den CLI-Befehl [create-logically-air-gapped-backup-vault](#), der mit den folgenden Parametern geändert wurde:

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1 // optional
--backup-vault-name sampleName // required
--min-retention-days 7 // required Value must be an integer 7 or greater
--max-retention-days 35 // required
--encryption-key-arn arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012 // optional
--creator-request-id 123456789012-34567-8901 // optional
```

Mit dem optionalen `--encryption-key-arn` Parameter können Sie einen vom Kunden verwalteten KMS-Schlüssel für die Tresorverschlüsselung angeben. Falls nicht angegeben, verwendet der Tresor einen AWS eigenen Schlüssel.

Beispiel für einen CLI-Befehl zum Erstellen eines Tresors mit logischem Air-Gapped:

```
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
```

Beispiel für einen CLI-Befehl zum Erstellen eines Tresors mit logischem Air-Gapped und kundenverwalteter Verschlüsselung:

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1
--backup-vault-name sampleName
--min-retention-days 7
--max-retention-days 35
--encryption-key-arn arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012
--creator-request-id 123456789012-34567-8901 // optional
```

Informationen nach dem Erstellungsvorgang finden Sie unter [CreateLogicallyAirGappedBackupVault API-Antwortelemente](#). Wenn der Vorgang erfolgreich war, wird im neuen Tresor mit logischem Air-Gap der Wert „Aus“ angezeigt. VaultState CREATING

Sobald die Erstellung abgeschlossen ist und der KMS-verschlüsselte Schlüssel zugewiesen wurde, VaultState erfolgt der Übergang zu. AVAILABLE Sobald der Tresor verfügbar ist, kann er verwendet werden. VaultState kann telefonisch [DescribeBackupVault](#) oder abgerufen werden [ListBackupVaults](#).

Details zum Tresor mit logischem Air-Gap anzeigen

Sie können die Tresordetails wie Zusammenfassung, Wiederherstellungspunkte, geschützte Ressourcen, Kontofreigabe, Zugriffsrichtlinien und Tags über die AWS Backup Konsole oder die AWS Backup CLI einsehen.

Console

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 drei Listen: Tresore, die mit diesem Konto erstellt wurden, Tresore, die über RAM gemeinsam genutzt werden, und Tresore, auf die durch eine Genehmigung durch mehrere Parteien zugegriffen werden kann. 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.

Die Details werden je nach Kontotyp angezeigt: Konten, die einen Tresor besitzen, können die gemeinsame Nutzung von Konten einsehen; Konten, die keinen Tresor besitzen, können die gemeinsame Nutzung von Konten nicht einsehen. Bei gemeinsam genutzten Tresoren wird der Typ des Verschlüsselungsschlüssels (AWS eigener oder vom Kunden verwalteter KMS-Schlüssel) in der Tresorübersicht angezeigt.

AWS CLI

Details eines Tresors mit logischem Air-Gap über CLI anzeigen

Der CLI-Befehl [describe-backup-vault](#) kann verwendet werden, um Details zu einem Tresor abzurufen. Der Parameter `backup-vault-name` ist erforderlich; `region` ist optional.

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

Beispiel für eine Antwort:

```
{
  "BackupVaultName": "LOG-AIR-GAP-VAULT-TEST",
  "BackupVaultArn": "arn:aws:backup:us-east-1:234567890123:backup-vault:IAD-LAGV-01",
  "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
  "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
  "CreationDate": "2024-07-25T16:05:23.554000-07:00",
  "NumberOfRecoveryPoints": 0,
  "Locked": true,
  "MinRetentionDays": 8,
  "MaxRetentionDays": 30,
  "LockDate": "2024-07-25T16:05:23.554000-07:00"
}
```

Erstellen von Backups in einem Tresor mit logischem Air-Gap

Tresore mit logischem Air-Gap können ein Ziel für Kopieraufträge in einem Backup-Plan oder ein Ziel für einen On-Demand-Kopierauftrag sein. Es kann auch als primäres Backup-Ziel verwendet werden. Siehe [Primäre Backups in Tresoren mit logischem Air-Gap](#).

Kompatible Verschlüsselung

Für einen erfolgreichen Kopiervorgang von einem Backup-Tresor in einen Tresor mit logischem Air-Gap ist ein Verschlüsselungsschlüssel erforderlich, der durch den zu kopierenden Ressourcentyp bestimmt wird.

Wenn Sie ein Backup eines [vollständig verwalteten Ressourcentyps](#) erstellen oder kopieren, kann die Quellressource mit einem vom Kunden verwalteten Schlüssel oder mit einem verwalteten Schlüssel verschlüsselt werden. AWS

Wenn Sie ein Backup anderer Ressourcentypen (solche, die [nicht vollständig verwaltet](#) werden) erstellen oder kopieren, muss die Quelle mit einem vom Kunden verwalteten Schlüssel verschlüsselt werden. AWS verwaltete Schlüssel für nicht vollständig verwaltete Ressourcen werden nicht unterstützt.

Erstellen oder kopieren Sie Backups mithilfe eines Backup-Plans in einen Tresor mit logischem Air-Gap

Sie können ein Backup (Recovery Point) von einem Standard-Backup-Tresor in einen Tresor mit logischem Air-Gap kopieren, indem Sie in der AWS Backup Konsole oder mithilfe der Befehle und [einen neuen Backup-Plan erstellen](#) oder [einen vorhandenen aktualisieren](#). AWS CLI [create-backup-planupdate-backup-plan](#) Sie können Backups auch direkt in einem Tresor mit logischem Air-Gap erstellen, indem Sie ihn als primäres Ziel verwenden. Weitere Informationen finden Sie unter [Primäre Backups in Tresoren mit logischem Air-Gap](#).

Sie können bei Bedarf ein Backup von einem Tresor mit logischem Air-Gap in einen anderen Tresor mit logischem Air-Gap kopieren (diese Art von Backup kann nicht in einem Backup-Plan geplant werden). Sie können ein Backup von einem Tresor mit logischem Air-Gap in einen Standard-Backup-Tresor kopieren, sofern die Kopie mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist.

On-Demand-Backup-Kopie in einen Tresor mit logischem Air-Gap

Um eine einmalige [On-Demand-Kopie](#) eines Backups in einen Tresor mit logischem Air-Gap zu erstellen, können Sie aus einem Standard-Backup-Tresor kopieren. Regions- oder kontoübergreifende Kopien sind verfügbar, wenn der Ressourcentyp den Kopiertyp unterstützt.

Verfügbarkeit kopieren

Eine Kopie eines Backups kann von dem Konto aus erstellt werden, zu dem der Tresor gehört. Konten, mit denen der Tresor gemeinsam genutzt wurde, haben die Möglichkeit, ein Backup anzusehen oder wiederherzustellen, aber keine Kopie zu erstellen.

Es können nur [Ressourcentypen berücksichtigt werden, die regionsübergreifendes oder kontoübergreifendes Kopieren unterstützen](#).

Console

1. [Öffnen Sie die AWS Backup Konsole unter /backup. `https://console.aws.amazon.com`](#)
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. Geben Sie die Zielregion an.
 - 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.

AWS CLI

Verwenden Sie [start-copy-job](#), um ein vorhandenes Backup in einem Backup-Tresor in einen logischen Air-Gapped Vault zu kopieren.

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
```

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](#).

Teilen Sie einen Tresor mit logischem Air-Gap

Sie können AWS Resource Access Manager (RAM) verwenden, um einen Tresor mit logischem Air-Gap gemeinsam mit anderen von Ihnen angegebenen Konten zu nutzen. Bei der gemeinsamen Nutzung von Tresoren bleiben die Informationen zum Typ des Verschlüsselungsschlüssels (AWS eigener oder vom Kunden verwalteter KMS-Schlüssel) erhalten und sind für Konten sichtbar, mit denen der Tresor gemeinsam genutzt wird.

Ein Tresor kann mit einem Konto in seiner Organisation oder mit einem Konto in einer anderen Organisation geteilt werden. Der Tresor kann nicht mit einer gesamten Organisation geteilt werden, sondern nur mit Konten innerhalb der Organisation.

Nur Konten mit bestimmten IAM-Rechten können Tresore gemeinsam nutzen und verwalten.

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, das einen Tresor besitzt und das teilen möchte, verfügt über die erforderlichen RAM-Berechtigungen. Die Berechtigung `ram:CreateResourceShare` ist für dieses Verfahren erforderlich. Die Richtlinie `AWSResourceAccessManagerFullAccess` enthält alle erforderlichen RAM-bezogenen Berechtigungen:
 - `backup:DescribeBackupVault`
 - `backup:DescribeRecoveryPoint`
 - `backup:GetRecoveryPointRestoreMetadata`
 - `backup:ListProtectedResourcesByBackupVault`
 - `backup:ListRecoveryPointsByBackupVault`
 - `backup:ListTags`
 - `backup:StartRestoreJob`
- Mindestens einen logischen Air-Gapped Vault

Console

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. Tresore, die dem Konto gehören, können gemeinsam genutzt werden.
4. Wählen Sie unter Tresorname den Namen des logischen Air-Gapped Vault aus, um die Detailseite zu öffnen.
5. Im Bereich Kontofreigabe wird angezeigt, mit welchen Konten der Tresor geteilt 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.
7. Die AWS RAM 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](#) im RAM-Benutzerhandbuch.
8. 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.
9. 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.

AWS CLI

AWS RAM verwendet den CLI-Befehl `create-resource-share`. Der Zugriff auf diesen Befehl ist nur für Konten mit ausreichenden Berechtigungen verfügbar. 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 [AWSResourceAccessManagerFullAccess](#) enthält alle RAM-bezogenen Berechtigungen.
3. Verwenden Sie [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
```

- c. 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).

Sie können AWS RAM CLI-Befehle verwenden, um gemeinsam genutzte Elemente anzuzeigen:

- Ressourcen, die Sie geteilt haben:

```
aws ram list-resources --resource-owner SELF --resource-type
backup:backup-vault --region us-east-1
```

- Zeigen Sie dem Schulleiter:

```
aws ram get-resource-share-associations --association-type PRINCIPAL
--region us-east-1
```

- Ressourcen, die von anderen Konten gemeinsam genutzt werden:

```
aws ram list-resources --resource-owner OTHER-ACCOUNTS --resource-type
backup:backup-vault --region us-east-1
```

Stellen Sie ein Backup aus einem Tresor mit logischem Air-Gap wieder her

Sie können ein in einem Tresor mit logischem Air-Gap gespeichertes Backup entweder von dem Konto aus wiederherstellen, dem der Tresor gehört, oder von einem beliebigen Konto, mit dem der Tresor gemeinsam genutzt wird.

Informationen zum [Wiederherstellen eines Wiederherstellungspunkts](#) über die Konsole finden Sie unter [Wiederherstellung eines Backups](#). AWS Backup

Sobald ein Backup aus einem Tresor mit logischem Air-Gap für Ihr Konto freigegeben wurde, können Sie es [start-restore-job](#) zur Wiederherstellung verwenden.

Eine CLI-Beispieleingabe kann den folgenden Befehl und die folgenden Parameter enthalten:

```
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 Sie einen Tresor mit logischem Air-Gap

Siehe [Löschen](#) eines 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.

Beim Löschen eines Tresors wird auch der dem Tresor zugeordnete Schlüssel sieben Tage nach dem Löschen des Tresors gemäß der Richtlinie zum Löschen von Schlüsseln gelöscht.

Der folgende CLI-Beispielbefehl [delete-backup-vault](#) kann verwendet werden, um einen Tresor zu löschen.

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

Zusätzliche programmatische Optionen für Tresore mit logischem Air-Gap

Der CLI-Befehl [list-backup-vaults](#) 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
```

Fügen Sie den Parameter `by-shared` hinzu, um die zurückgegebene Tresorliste so zu filtern, dass nur gemeinsam genutzte Tresore mit logischem Air-Gap angezeigt werden. Die Antwort enthält Informationen zum Typ des Verschlüsselungsschlüssels für jeden gemeinsam genutzten Tresor.

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

Beispielantwort mit Informationen zum Typ des Verschlüsselungsschlüssels:

```
{
  "BackupVaultList": [
    {
      "BackupVaultName": "shared-logically air-gapped-vault",
      "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:shared-logically air-gapped-vault",
      "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
      "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
      "CreationDate": "2024-07-25T16:05:23.554000-07:00",
      "Locked": true,
      "MinRetentionDays": 7,
      "MaxRetentionDays": 30
    }
  ]
}
```

Grundlegendes zu Verschlüsselungsschlüsseltypen für Tresore mit logischem Air-Gap

Tresore mit logischem Air-Gap unterstützen verschiedene Verschlüsselungsschlüsseltypen, und diese Informationen sind sowohl über die Konsole als auch über die Konsole sichtbar. AWS Backup APIs Wenn Tresore über MPA gemeinsam genutzt werden, bleiben die Informationen zum Typ des Verschlüsselungsschlüssels erhalten und sind für Konten sichtbar, mit denen der AWS RAM Tresor gemeinsam genutzt wird. Diese Transparenz hilft Ihnen, die Verschlüsselungskonfiguration von Tresoren zu verstehen und fundierte Entscheidungen über Sicherungs- und Wiederherstellungsvorgänge zu treffen.

Werte des Typs des Verschlüsselungsschlüssels

Das `EncryptionKeyType` Feld kann die folgenden Werte haben:

- **AWS_OWNED_KMS_KEY**- Der Tresor ist mit einem AWS eigenen Schlüssel verschlüsselt. Dies ist die Standardverschlüsselungsmethode für Tresore mit logischem Air-Gap, wenn kein vom Kunden verwalteter Schlüssel angegeben ist.
- **CUSTOMER_MANAGED_KMS_KEY**- Der Tresor ist mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt, den Sie kontrollieren. Diese Option bietet zusätzliche Kontrolle über Verschlüsselungsschlüssel und Zugriffsrichtlinien.

Note

- AWS Backup empfiehlt die Verwendung von AWS eigenen Schlüsseln mit Tresoren mit logischem Air-Gap. Wenn Ihre Unternehmensrichtlinie jedoch die Verwendung eines vom Kunden verwalteten Schlüssels vorschreibt, sollten Sie als bewährte Methode Schlüssel von einem anderen Konto in einer sekundären Organisation verwenden, die für die Wiederherstellung vorgesehen ist. Im Blog [Encrypt AWS Backup Logically Air-Gapped Vaults with Customer-managed Keys](#) finden Sie weitere Informationen zur Einrichtung von CMK-basierten Logic Air-Gapped Tresoren.
- Sie können bei der Tresorerstellung nur einen KMS-Verschlüsselungsschlüssel auswählen. AWS Nach der Erstellung werden alle im Tresor enthaltenen Backups mit diesem Schlüssel verschlüsselt. Sie können Ihre Tresore nicht ändern oder migrieren, sodass sie einen anderen Verschlüsselungsschlüssel verwenden.

Wichtige Richtlinie für die Erstellung von mit CMK verschlüsselten Tresoren mit logischem Air-Gap

Wenn Sie einen Tresor mit logischem Air-Gapped mit einem vom AWS Kunden verwalteten Schlüssel erstellen, müssen Sie die Richtlinie „-managed“ auf Ihre Kontorolle anwenden. `AWSBackupFullAccess` Diese Richtlinie umfasst `Allow` Aktionen, die es ermöglichen AWS Backup , bei Sicherungs-, Kopier AWS KMS - und Speichervorgängen auf KMS-Schlüsseln zu interagieren oder Zuweisungen zu erstellen. Darüber hinaus müssen Sie sicherstellen, dass Ihre Richtlinie für vom Kunden verwaltete Schlüssel (falls verwendet) bestimmte erforderliche Berechtigungen enthält.

- Das CMK muss mit dem Konto geteilt werden, auf dem sich der Tresor mit logischem Air-Gap befindet

```
{
  "Sid": "Allow use of the key to create a logically air-gapped vault",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[account-id]:role/TheRoleToAccessAccount"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "backup.*.amazonaws.com"
    }
  }
}
```

Wichtige Richtlinie für das Kopieren/Wiederherstellen

Um Auftragsausfälle zu vermeiden, überprüfen Sie Ihre AWS KMS wichtigsten Richtlinien, um sicherzustellen, dass sie alle erforderlichen Berechtigungen enthält und keine Ablehnungsaussagen enthält, die Vorgänge blockieren könnten. Es gelten die folgenden Bedingungen:

- Für alle Kopierszenarien CMKs muss die Rolle mit der Quellkopierrolle gemeinsam genutzt werden

```
{
  "Sid": "Allow use of the key for copy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[source-account-id]:role/service-role/AWSBackupDefaultServiceRole" // [Source copy role]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
```

```

        "StringLike": {
            "kms:ViaService": "backup.*.amazonaws.com"
        }
    },
    {
        "Sid": "Allow AWS Backup to create grant on the key for copy",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::[source-account-id]:role/service-role/AWSBackupDefaultServiceRole" //[Source copy role]
        },
        "Action": [
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            },
            "StringLike": {
                "kms:ViaService": "backup.*.amazonaws.com"
            }
        }
    }
}

```

- Beim Kopieren von einem CMK-verschlüsselten Tresor mit logischem Air-Gap in einen Backup-Tresor muss der CMK auch für das Zielkonto SLR freigegeben werden

```

{
    "Sid": "Allow use of the key for copy from a CMK encrypted logically air-gapped vault to normal backup vault",
    "Effect": "Allow",
    "Principal": {
        "AWS": ["arn:aws:iam::[source-account-id]:role/service-role/AWSBackupDefaultServiceRole",
                "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup"], //[Destination SLR]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",

```



```

        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
        "AWS": ["arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole", // [Source copy role]
                "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"], // [Destination SLR]
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
}
}

```

- Beim Kopieren oder Wiederherstellen von einem Wiederherstellungskonto mithilfe eines gemeinsam genutzten Tresors mit logischem Air-Gap RAM/MPA

```

{
    "Sid": "Allow use of the key for copy/restore from a recovery account",
    "Effect": "Allow",
    "Principal": {
        "AWS": ["arn:aws:iam::[recovery-account-id]:role/service-role/
AWSBackupDefaultServiceRole", // [Recovery account copy/restore role]
                "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"] // [Destination SLR]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
    ]
}

```

```

        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::[recovery-account-id]:role/service-role/AWSBackupDefaultServiceRole" // [Recovery account copy/restore role]
            "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup", // [Destination SLR]
        ]
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
}
}

```

IAM Role (IAM-Rolle)

Bei Kopiervorgängen im Tresor mit logischem Air-Gapped können Kunden die Richtlinie verwenden, die auch die `AWSBackupDefaultServiceRole` verwaltete Richtlinie beinhaltet. `AWSAWSBackupServiceRolePolicyForBackup` Wenn Kunden es jedoch vorziehen, einen Richtlinienansatz mit den geringsten Rechten zu implementieren, muss ihre IAM-Richtlinie eine bestimmte Anforderung beinhalten:

- Die Kopierrolle des Quellkontos muss über Zugriffsberechtigungen sowohl für die Quelle als auch für das Ziel verfügen. CMKs

```

{
    "Version": "2012-10-17"
    ,
    "Statement": [
        {

```

```

        "Sid": "KMSPermissions",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": [
            "arn:aws:kms:*:source-account-id:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*:destination-account-id:key/*". - Destination
logically air-gapped vault CMK -
        ]
    },
    {
        "Sid": "KMSCreateGrantPermissions",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": [
            "arn:aws:kms:*:source-account-id:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*:destination-account-id:key/*". - Destination
logically air-gapped vault CMK -
        ]
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
]
}

```

Folglich tritt einer der häufigsten Kundenfehler beim Kopieren auf, wenn Kunden nicht genügend Berechtigungen für ihre Rollen CMKs und die Kopierrolle bereitstellen.

Verschlüsselungsschlüsseltypen anzeigen

Sie können Informationen zum Typ des Verschlüsselungsschlüssels sowohl über die AWS Backup Konsole als auch programmgesteuert mithilfe von oder anzeigen. AWS CLI SDKs

Konsole: Bei der Anzeige von Tresoren mit logischem Air-Gap in der AWS Backup Konsole wird der Typ des Verschlüsselungsschlüssels auf der Seite mit den Tresordetails im Bereich Sicherheitsinformationen angezeigt.

AWS CLI/API: Der Typ des Verschlüsselungsschlüssels wird als Antwort auf die folgenden Operationen zurückgegeben, wenn Tresore mit logischem Air-Gap abgefragt werden:

- `list-backup-vaults`(auch für gemeinsam genutzte Tresore) `--by-shared`
- `describe-backup-vault`
- `describe-recovery-point`
- `list-recovery-points-by-backup-vault`
- `list-recovery-points-by-resource`

Überlegungen zur Tresorverschlüsselung

Beachten Sie bei der Arbeit mit Tresoren und Verschlüsselungsschlüsseltypen mit logischem Air-Gap Folgendes:

- Schlüsselauswahl bei der Erstellung: Sie können optional einen vom Kunden verwalteten KMS-Schlüssel angeben, wenn Sie einen Tresor mit logischem Air-Gapped erstellen. Falls nicht angegeben, wird ein AWS eigener Schlüssel verwendet.
- Sichtbarkeit gemeinsam genutzter Tresore: Konten, mit denen ein Tresor gemeinsam genutzt wird, können den Typ des Verschlüsselungsschlüssels sehen, die Verschlüsselungskonfiguration jedoch nicht ändern.
- Informationen zum Wiederherstellungspunkt: Der Typ des Verschlüsselungsschlüssels ist auch verfügbar, wenn Sie Wiederherstellungspunkte in Tresoren mit logischem Air-Gap anzeigen.
- Wiederherstellungsvorgänge: Wenn Sie den Typ des Verschlüsselungsschlüssels kennen, können Sie Wiederherstellungsvorgänge besser planen und mögliche Zugriffsanforderungen besser verstehen.
- Konformität: Die Informationen zum Typ des Verschlüsselungsschlüssels unterstützen die Anforderungen an Compliance-Berichte und Audits, indem sie Transparenz über die für Backup-Daten verwendeten Verschlüsselungsmethoden bieten.

Beheben Sie ein Problem mit einem Tresor mit logischem Air-Gap

Wenn Sie während Ihres Workflows auf Fehler stoßen, sehen Sie sich die folgenden Beispielfehler und Lösungsvorschläge an:

AccessDeniedException

Fehler: An error occured (AccessDeniedException) when calling the `[command]` operation: Insufficient privileges to perform this action."

Mögliche Ursache: Der Parameter `--backup-vault-account-id` war nicht enthalten, als eine der folgenden Anforderungen in einem vom RAM gemeinsam genutzten Tresor ausgeführt wurde:

- `describe-backup-vault`
- `describe-recovery-point`
- `get-recovery-point-restore-metadata`
- `list-protected-resources-by-backup-vault`
- `list-recovery-points-by-backup-vault`

Lösung: Wiederholen Sie den Befehl, der den Fehler zurückgegeben hat, geben Sie jedoch den Parameter an, der `--backup-vault-account-id` das Konto angibt, dem der Tresor gehört.

OperationNotPermittedException

Fehler: `OperationNotPermittedException` wird nach einem `CreateResourceShare` Aufruf zurückgegeben.

Mögliche Ursache: Wenn Sie versuchen, eine Ressource, z. B. einen Tresor mit logischem Air-Gap, mit einer anderen Organisation gemeinsam zu nutzen, tritt möglicherweise diese Ausnahme auf. Ein Tresor kann mit einem Konto in einer anderen Organisation geteilt werden, aber er kann nicht mit der anderen Organisation selbst geteilt werden.

Lösung: Versuchen Sie den Vorgang erneut, geben Sie jedoch ein Konto als Wert für `principals` anstelle einer Organisation oder Organisationseinheit an.

Der Typ des Verschlüsselungsschlüssels wird nicht angezeigt

Problem: Der Typ des Verschlüsselungsschlüssels ist nicht sichtbar, wenn ein Tresor mit logischem Air-Gap oder dessen Wiederherstellungspunkten angezeigt wird.

Mögliche Ursachen:

- Sie sehen einen älteren Tresor, der erstellt wurde, bevor die Unterstützung für Verschlüsselungsschlüsseltypen hinzugefügt wurde
- Sie verwenden eine ältere Version des AWS CLI oder SDK
- Die API-Antwort enthält nicht das Feld für den Typ des Verschlüsselungsschlüssels

Auflösung

- Aktualisieren Sie Ihre AWS CLI auf die neueste Version
- Bei älteren Tresoren wird der Typ des Verschlüsselungsschlüssels automatisch ausgefüllt und sollte in nachfolgenden API-Aufrufen erscheinen
- Stellen Sie sicher, dass Sie die richtigen API-Operationen verwenden, die Informationen zum Typ des Verschlüsselungsschlüssels zurückgeben
- Stellen Sie bei gemeinsam genutzten Tresoren sicher, dass der Tresor ordnungsgemäß gemeinsam genutzt wird über AWS Resource Access Manager

AccessDeniedException In CloudTrail den Protokollen steht „FEHLGESCHLAGEN“ VaultState

Fehler in CloudTrail: "User: <assumed role> is not authorized to perform: kms:CreateGrant on this resource because the resource does not exist in this Region, no resource-based policies allow access, or a resource-based policy explicitly denies access"

Mögliche Ursachen:

- Der Tresor wurde mit einem vom Kunden verwalteten Schlüssel erstellt, aber die übernommene Rolle verfügt nicht über die erforderlichen CreateGrant Berechtigungen für die Schlüsselrichtlinie, um den Schlüssel für die Tresorerstellung zu verwenden

Auflösung

- Erteilen Sie die im [the section called “Wichtige Richtlinie für die Erstellung von mit CMK verschlüsselten Tresoren mit logischem Air-Gap”](#) Abschnitt angegebenen Berechtigungen und versuchen Sie dann erneut, den Workflow zur Tresorerstellung auszuführen.

Primäre Backups zu logischen Air-Gapped Vaults

Übersicht

Die primäre Backup-Funktion mit logischem Air-Gapped bietet Ihnen die Möglichkeit, einen Tresor mit logischem Air-Gapped als primäres Backup-Ziel innerhalb desselben Kontos anzugeben, und zwar sowohl für geplante als auch für On-Demand-Backup-Jobs. Dadurch entfällt die Notwendigkeit, separate Kopien sowohl in einem Standard-Backup-Tresor als auch in einem Tresor mit logischem

Air-Gap zu verwalten, was die Kosten senkt und Arbeitsabläufe vereinfacht, während gleichzeitig die Sicherheitsvorteile des logischen Air-Gappings erhalten bleiben.

In Backup-Plänen, unternehmensweiten Richtlinien oder On-Demand-Backups können Sie einen Tresor mit logischem Air-Gapped als primäres Ziel festlegen. Bisher mussten Sie zur Sicherung in einem Tresor mit logischem Air-Gap zunächst ein Backup in einem Backup-Tresor erstellen und es dann in einen Tresor mit logischem Air-Gap kopieren. Mit dieser Funktion AWS Backup können Sie je nach Ressourcentyp Backups direkt in Ihrem Tresor mit logischem Air-Gap erstellen oder temporäre Backups automatisch verwalten, die in Ihren Tresor mit logischem Air-Gapped kopiert und dann gelöscht werden.

Das Verhalten hängt von zwei Faktoren ab:

- Ob der Ressourcentyp von einem Tresor mit logischem Air-Gap unterstützt wird.
- [Ob der Ressourcentyp die vollständige Verwaltung unterstützt. AWS Backup](#)

 Warning

Wenn Sie diese Funktion nutzen, empfehlen wir Ihnen, Ihre Tresore mit logischem Air-Gapped mit [Multi-Party Approval](#) (MPA) zu integrieren. Dadurch können Backups im Tresor auch dann wiederhergestellt werden, wenn auf das Konto, dem der Tresor gehört, nicht zugegriffen werden kann.

Für diese Funktion gibt es keine neuen Preise. Ihnen werden nur Backups in Tresoren mit logischem Air-Gap und temporäre Snapshots (während der Aufbewahrungszeit im System) für entsprechende Ressourcen zu den jeweils geltenden Tarifen in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS Backup Preise](#).

Themen

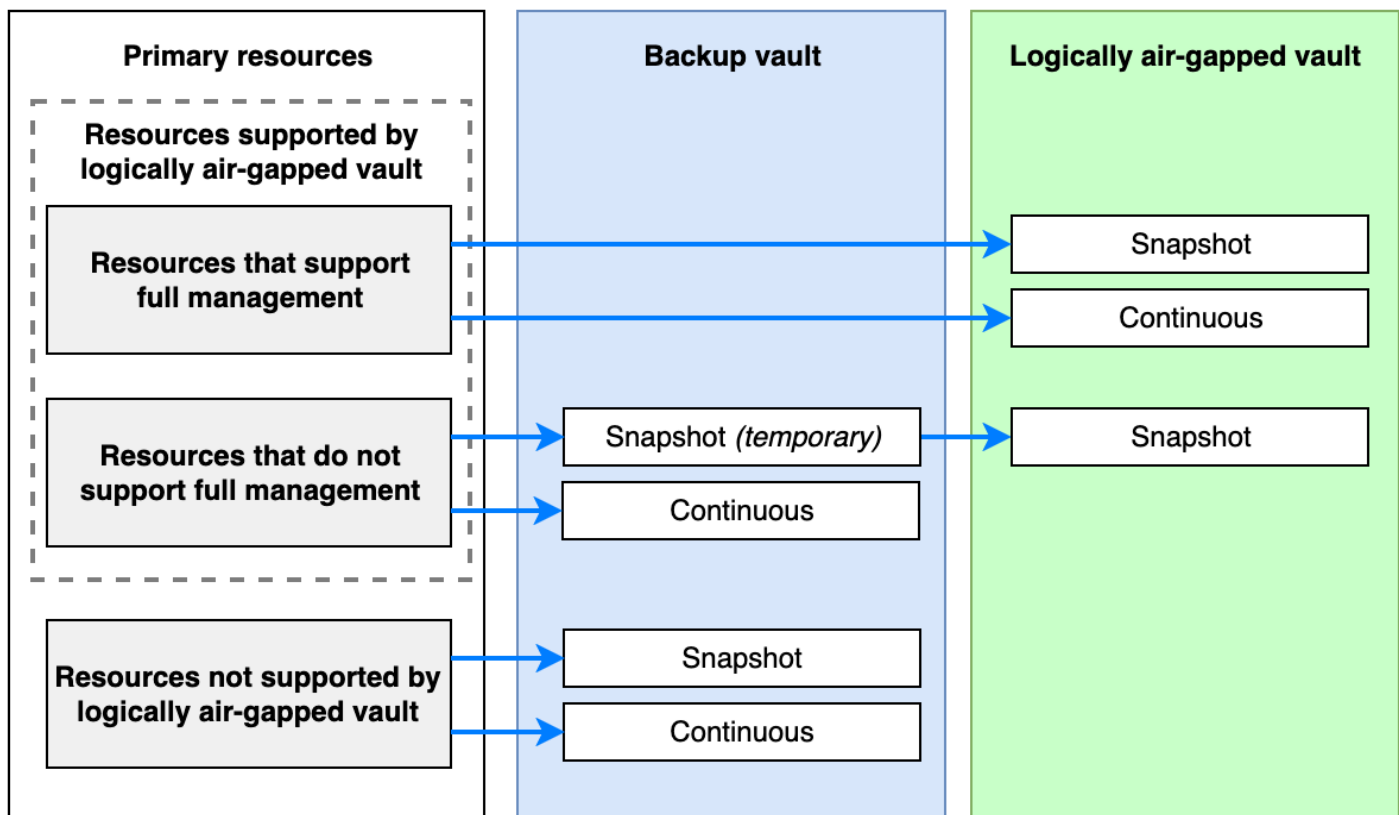
- [Funktionsweise](#)
- [Kostenüberlegungen](#)
- [Konfigurieren Sie das primäre Vault-Backup mit logischem Air-Gapped](#)
- [Überwachen Sie das primäre Vault-Backup mit logischem Air-Gap](#)
- [Onboarding und Migration](#)
- [Fehlerbehebung](#)

Funktionsweise

Sie können diese Funktion nutzen, indem Sie Ihren bestehenden Backup-Plan aktualisieren oder einen neuen erstellen und einen Vault-ARN (Feldname: `TargetLogicallyAirGappedBackupVaultArn`) mit logischem Air-Gapped als primäres Backup-Ziel hinzufügen. Sie können diesen Vorgang entweder über die AWS Backup Konsole oder über AWS Backup CLI-Befehle ausführen.

```
"TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:AirGappedVault",
```

Wenn Sie sowohl einen Backup-Tresor als auch einen Tresor mit logischem Air-Gap als Ziele für Ihre Backup-Jobs angeben, AWS Backup bestimmt der entsprechende Workflow auf der Grundlage des Ressourcentyps und der Verschlüsselungskonfiguration.



Unterstützte Ressourcen für primäres Backup in Tresoren mit logischem Air-Gap

[Die vollständige Liste der unterstützten Ressourcen für Tresore mit logischem Air-Gap finden Sie unter Verfügbarkeit der Funktionen.](#) **AWS Backup** Alle Ressourcen, die Tresore mit logischem Air-

Gap unterstützen, folgen dem Prinzip, dass bei Verwendung dieser Funktion nur eine Kopie Ihres Backups gespeichert wird, anstatt zwei separate Kopien zu speichern.

 Warning

Für Ressourcen, die derzeit nicht für diese Funktion unterstützt werden, wird ihre Unterstützung möglicherweise in future aktiviert. In diesem Fall beginnt Ihre neu unterstützte Ressource automatisch mit der Sicherung im Tresor mit logischem Air-Gap. Dabei wird der oben dargestellte Arbeitsablauf verwendet.

Überlegungen und Einschränkungen:

- Nur dasselbe Konto und dieselbe Region — Ihr logischer Air-Gap-Tresor muss sich in demselben AWS Konto und derselben Region wie Ihre Ressourcen befinden, um diese Funktion nutzen zu können. Sie können Backups nicht direkt konto- oder regionsübergreifend erstellen. Wir empfehlen, Backups in einem Tresor mit logischem Air-Gap in derselben Region zu speichern, um eine schnellere Wiederherstellung zu ermöglichen, ohne dass eine Kopie erforderlich ist. Wenn Sie eine Kopie Ihrer Daten in einer zweiten Region für Disaster Recovery (DR) benötigen, empfehlen wir entweder eine regionsübergreifende Replikation Ihrer primären Ressourcen für ein schnelles Failover oder regionsübergreifende Wiederherstellungspunktkopien in einen gesperrten Backup-Tresor.
- Einschränkungen bei der Verwendung AWS verwalteter Schlüssel — Ressourcen, die keine vollständige AWS Backup Verwaltung unterstützen und mit AWS verwalteten Schlüsseln verschlüsselt sind (z. B. `aws/rds`), `aws/ebs`, können nicht in Tresore mit logischem Air-Gap kopiert werden. Diese Ressourcen müssen mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt oder unverschlüsselt sein. Für Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, gilt diese Einschränkung nicht.
- Sicherungshäufigkeit und gleichzeitige Kopien — Stellen Sie bei Ressourcen, die keine vollständige AWS Backup Verwaltung unterstützen, sicher, dass Ihre Sicherungshäufigkeit ausreichend Zeit für die Fertigstellung der Kopien bietet. Wenn Backups häufiger geplant werden, als Kopien abgeschlossen werden können, werden Kopieraufträge in eine Warteschlange gestellt und können irgendwann fehlschlagen. Hinweise zu den Beschränkungen für gleichzeitige Kopien finden Sie [unter Kontingente](#).

- **Lebenszykluskompatibilität** — Der in Ihrem Backup-Plan angegebene Aufbewahrungszeitraum muss mit den Mindest- und Höchstaufbewahrungszeiträumen kompatibel sein, die für Ihren Logic Air-Gapped Vault konfiguriert sind.
- **Gesperrte Backup-Tresore** — Wenn in Ihrem Ziel-Backup-Tresor eine Tresorsperre aktiviert ist, können temporäre Wiederherstellungspunkte nicht manuell gelöscht werden. Sie werden aufbewahrt, bis entweder der Kopiervorgang abgeschlossen ist oder die Aufbewahrungsfrist abgelaufen ist.
- **Testen, Indizieren und Scannen wiederherstellen** — Bei Wiederherstellungstests, bei der Indizierung von Wiederherstellungspunkten und beim Scannen auf Schadsoftware werden temporäre Wiederherstellungspunkte mit einem Lebenszyklus ignoriert. `DELETE_AFTER_COPY` Die Indizierung von Wiederherstellungspunkten unterstützt keine Wiederherstellungspunkte in einem Tresor mit logischem Air-Gap. Das Scannen auf Schadsoftware unterstützt keine geplanten Scans kopierter Wiederherstellungspunkte. Dazu gehören automatische Kopien, die als Teil primärer Backups in den Tresor mit logischem Air-Gap erstellt wurden.

Ressourcen zur Unterstützung der vollständigen Verwaltung AWS Backup

Einige Ressourcentypen, wie Amazon EFS, Amazon S3, Amazon DynamoDB mit [AWS Backup erweiterten Funktionen](#) usw., die die vollständige AWS Backup Verwaltung unterstützen, können direkt in Ihrem Logical Air-Gapped Vault gesichert werden. In Ihrem Backup-Tresor wird kein Wiederherstellungspunkt erstellt, und es ist kein Kopiervorgang erforderlich. Für alle geplanten Kopieraktionen in Ihrem Backup-Plan wird der Recovery Point in Ihrem Tresor mit logischem Air-Gap als Quelle verwendet.

Ressourcen, die kontinuierliche Backups unterstützen, wie Amazon S3, können auch kontinuierliche Backups direkt in einem Tresor mit logischem Air-Gap durchführen.

Eine Liste der Ressourcentypen, die vollständige AWS Backup Verwaltung und Tresore mit logischem Air-Gap unterstützen, finden Sie unter [Verfügbarkeit von Funktionen nach Ressourcen](#) in den Spalten „Vollständige Verwaltung“ und „Tresore mit logischem Air-Gap“.

AWS Backup Ressource unterstützt keine vollständige Verwaltung

Ressourcen wie Amazon EBS/EC2, Amazon Aurora und Amazon FSx können keine direkten Backups in Tresoren mit logischem Air-Gap erstellen. AWS Backup Erstellt für diese Ressourcentypen einen temporären Wiederherstellungspunkt in Ihrem Backup-Tresor und kopiert ihn dann automatisch in Ihren Tresor mit logischem Air-Gap.

Für den temporären Erholungspunkt gibt es eine spezielle Lebenszykluseinstellung namens `DELETE_AFTER_COPY`. Sobald der Kopiervorgang in Ihren Tresor mit logischem Air-Gap erfolgreich abgeschlossen wurde, AWS Backup wird der temporäre Erholungspunkt automatisch gelöscht. Alle anderen geplanten Kopieraktionen in Ihrem Backup-Plan beginnen parallel mit der Kopie in Ihren Tresor mit logischem Air-Gap und wirken sich nicht auf Ihr derzeitiges Kopiererlebnis aus.

Wenn die Kopie in Ihren Tresor mit logischem Air-Gap fehlschlägt, wird der temporäre Wiederherstellungspunkt gemäß dem von Ihnen angegebenen Aufbewahrungszeitraum in Ihrem Backup-Tresor aufbewahrt. Auf diese Weise wird sichergestellt, dass Sie nach Abschluss eines Backup-Jobs immer über einen verwendbaren Erholungspunkt verfügen. Wenn der Wiederherstellungspunkt später manuell in den Tresor mit logischem Air-Gap kopiert wird, wird er gemäß der Regel automatisch bereinigt. `DELETE_AFTER_COPY`

 Warning

Ressourcen, die mit AWS verwalteten Schlüsseln verschlüsselt wurden (z. B. `aws/ebs`), werden für das Kopieren in Tresore mit logischem Air-Gap nicht unterstützt. Diese Ressourcen müssen mit einem vom AWS Key Management Service Kunden verwalteten Schlüssel verschlüsselt oder unverschlüsselt sein. Für Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, gilt diese Einschränkung nicht.

Nach dem Kopierzyklus löschen

Temporäre Wiederherstellungspunkte verfügen über ein neues Lebenszyklusattribut `DeleteAfterEvent` mit dem Wert `DELETE_AFTER_COPY`. Dieses Attribut gibt an, dass der Recovery Point automatisch gelöscht wird, wenn alle Kopieraufträge abgeschlossen sind oder nach Ablauf der von Ihnen angegebenen Aufbewahrungszeit, je nachdem, was zuerst eintritt.

Ein temporärer Erholungspunkt wird gelöscht, wenn alle der folgenden Bedingungen erfüllt sind:

- Alle automatischen und geplanten Kopieraufträge wurden abgeschlossen.
- Es wurde ein Kopierauftrag für Ihren Ziel-Tresor mit logischem Air-Gap abgeschlossen, dessen Aufbewahrungsdauer mindestens so lang ist wie der des Quell-Wiederherstellungspunkts.

Wenn Sie das manuelle Löschen des temporären Wiederherstellungspunkts während laufender Kopien verhindern möchten, sollten Sie einen gesperrten Backup-Tresor als Ziel-Backup-Tresor verwenden.

Kontinuierliches Backup für Resource unterstützt keine vollständige AWS Backup Verwaltung

Wenn Sie für Ressourcen wie Amazon Aurora Continuous Backup aktivieren, AWS Backup wird ein kontinuierlicher Wiederherstellungspunkt in Ihrem Backup-Tresor erstellt und ein temporärer Snapshot erstellt, der in Ihren Tresor mit logischem Air-Gap kopiert wird. Der temporäre Snapshot wird immer gelöscht, nachdem der Kopiervorgang abgeschlossen ist, unabhängig davon, ob der Kopiervorgang erfolgreich ist oder nicht, da Sie in Ihrem Backup-Tresor einen kontinuierlichen Wiederherstellungspunkt beibehalten.

Wenn Sie in Ihrem Backup-Tresor keinen Continuous Recovery Point für Amazon Aurora erstellen möchten, sondern einen Continuous Recovery Point für Amazon S3 in Ihrem Tresor mit logischem Air-Gap wünschen, können Sie die Einstellung Continuous Backup (EnableContinuousBackup) im aktuellen Plan deaktivieren und S3 Continuous von einem anderen Plan aus aktivieren.

Weitere Informationen zum Aurora-Backup-Speicher finden Sie unter [Grundlegendes zur Nutzung des Amazon Aurora Aurora-Backup-Speichers](#).

Nicht unterstützte Ressourcen

Wenn ein Ressourcentyp von Tresoren mit logischem Air-Gap nicht unterstützt wird oder wenn eine nicht vollständig verwaltete Ressource mit einem AWS verwalteten Schlüssel verschlüsselt ist, wird das Backup nur in Ihrem Backup-Tresor AWS Backup erstellt. Es wird nicht versucht, eine Kopie in Ihren Tresor mit logischem Air-Gap zu kopieren. Der Backup-Job wurde erfolgreich abgeschlossen und es wird eine Meldung angezeigt, die angibt, warum das Backup nicht in Ihren Tresor mit logischem Air-Gap verschoben wurde.

Kostenüberlegungen

- Für diese Funktion fallen keine neuen Gebühren an. Sie zahlen nur für den Speicher in Ihren Tresoren.
- Bei Ressourcen, die eine vollständige AWS Backup Verwaltung unterstützen, kann die ausschließliche Aufbewahrung von Backups in Ihrem Tresor mit logischem Air-Gap zu erheblichen Kosteneinsparungen im Vergleich zur Aufbewahrung von zwei Sicherungskopien sowohl in einem Backup-Tresor als auch in einem Tresor mit logischem Air-Gapped führen.
- Bei Ressourcen, die keine vollständige AWS Backup Verwaltung unterstützen, werden Ihnen sowohl der temporäre Wiederherstellungspunkt in Ihrem Backup-Tresor als auch die Wiederherstellungspunkte in Ihrem Tresor mit logischem Air-Gap in Rechnung gestellt.

- Sie können immer noch erhebliche Kosteneinsparungen erzielen, wenn Sie nur eine einzige Sicherungskopie aufbewahren. Diese Einsparungen können jedoch je nach Backup-Häufigkeit und Änderungsrate variieren.
- Niedrigere Backup-Frequenzen führen in der Regel zu größeren Einsparungen, da temporäre Wiederherstellungspunkte Speicherplatz für einen kürzeren Prozentsatz Ihres Abrechnungszeitraums belegen.
- Einige Ressourcen haben eine Mindestabrechnungsdauer, wodurch die Kosten für temporäre Wiederherstellungspunkte steigen.
- Deaktivieren Sie das Abrufen von Tags oder ACLs Metadaten in Ihrer Backup-Konfiguration, wenn Sie diese S3-Funktionen nicht verwenden. Dadurch werden API-Aufrufe und die damit verbundenen Gebühren für Metadatenprüfungen bei Kopiervorgängen reduziert.

Konfigurieren Sie das primäre Vault-Backup mit logischem Air-Gapped

Sie können das primäre Vault-Backup mit logischem Air-Gapped über die AWS Backup Konsole, die, oder die Backup-Richtlinien konfigurieren. AWS CLI AWS CloudFormation AWS Organizations

Einen Backup-Plan konfigurieren

Console

So konfigurieren Sie das primäre Vault-Backup mit logischem Air-Gapped für einen Backup-Plan

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich Backup-Pläne und dann Backup-Plan erstellen aus oder wählen Sie einen vorhandenen Backup-Plan zur Bearbeitung aus.
3. Geben Sie im Abschnitt Konfiguration der Backup-Regel Ihre Backup-Regeleinstellungen an.
4. Wählen Sie für Backup-Tresor den Backup-Tresor aus, in dem temporäre Wiederherstellungspunkte gespeichert werden (für nicht vollständig verwaltete Ressourcen) oder in dem Backups gespeichert werden, wenn sie nicht in Ihrem Tresor mit logischem Air-Gap platziert werden können.
5. Wählen Sie für Tresor mit logischem Air-Gap (optional) den Tresor mit logischem Air-Gap aus, in dem Ihre Backups gespeichert werden sollen.

Note

Der Tresor mit logischem Air-Gap muss sich in demselben Konto und derselben Region wie Ihr Backup-Tresor befinden.

6. Konfigurieren Sie die übrigen Einstellungen für die Backup-Regel, einschließlich Lebenszyklus- und Kopieroptionen.
7. Wählen Sie Plan erstellen oder Änderungen speichern.

AWS CLI

Verwenden Sie den CLI-Befehl, [create-backup-plan](#) um einen neuen Plan [update-backup-plan](#) zu erstellen oder einen vorhandenen Plan zu aktualisieren und den `TargetLogicallyAirGappedBackupVaultArn` Parameter in Ihre Backup-Regel aufzunehmen.

Beispiel für einen CLI-Befehl zum Erstellen eines Backup-Plans mithilfe eines JSON-Dokuments:

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

Beispiel für einen CLI-Befehl zum Erstellen eines Backup-Plans direkt in CLI:

```
aws backup create-backup-plan --backup-plan '{
  "BackupPlanName": "MyPlan",
  "Rules": [
    {
      "RuleName": "MyRule",
      "TargetBackupVaultName": "MyBackupVault",
      "TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:MyLagVault",
      "ScheduleExpression": "cron(0 1 ? * * *)",
      "ScheduleExpressionTimezone": "America/Los_Angeles",
      "StartWindowMinutes": 60,
      "CompletionWindowMinutes": 120,
      "Lifecycle": {
        "DeleteAfterDays": 35
      }
    }
  ]
}
```

```
}'
```

Konfigurieren Sie das Backup auf Abruf

Console

So konfigurieren Sie das primäre Vault-Backup mit logischem Air-Gapped für ein On-Demand-Backup

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Wählen Sie auf der Seite Geschützte Ressourcen die Option On-Demand-Backup erstellen aus.
4. Wählen Sie den Ressourcentyp und den Ressourcen-ARN aus, die Sie sichern möchten.
5. Wählen Sie für Backup-Tresor den Backup-Tresor aus.
6. Wählen Sie für Logically Air-Gapped Tresor (optional) den Tresor mit logischem Air-Gapped aus, in dem das Backup gespeichert werden soll.
7. Konfigurieren Sie die übrigen Einstellungen und wählen Sie Backup auf Abruf erstellen.

AWS CLI

Verwenden Sie den `start-backup-job` Befehl mit dem neuen `--logically-air-gapped-backup-vault-arn` Parameter:

```
aws backup start-backup-job \
  --backup-vault-name MyBackupVault \
  --logically-air-gapped-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-vault:MyLagVault \
  --resource-arn arn:aws:ec2:us-east-1:123456789012:volume/vol-abcd1234 \
  --iam-role-arn arn:aws:iam::123456789012:role/service-role/AWSBackupDefaultServiceRole \
  --lifecycle DeleteAfterDays=35
```

Überwachen Sie das primäre Vault-Backup mit logischem Air-Gap

Sie können den Status Ihrer Backups und Kopieraufträge über die AWS Backup Konsole oder über Amazon EventBridge Events überwachen. AWS CLI

Auf Backup-Jobs achten

Überwachen Sie den Status der Backup-Jobs ([DescribeBackupJob](#)), um sicherzustellen, dass Ihre Ressourcen geschützt bleiben. Ein fehlgeschlagener Backup-Job weist darauf hin, dass kein Erholungspunkt erstellt wurde.

- Überprüfen Sie den Speicherort für die Erstellung des Wiederherstellungspunkts — Wenn ein Backup-Job erfolgreich abgeschlossen wurde, haben Sie entweder in Ihrem Ziel-Backup-Tresor oder in Ihrem Ziel-Tresor mit logischem Air-Gap einen Wiederherstellungspunkt. Überprüfen Sie das `BackupVaultArn` Feld, um festzustellen, wo der Recovery Point erstellt wurde.
- Auftragsstatus überprüfen — Wenn eine Ressource nicht von Tresoren mit logischem Air-Gap unterstützt wird, wird der Backup-Job mit der Meldung „Von“ `LOGICALLY_AIR_GAPPED_BACKUP_VAULT_NOT_SUPPORTED` und einer Statusmeldung abgeschlossen, in `MessageCategory` der erklärt wird, warum das Backup stattdessen in Ihrem Backup-Tresor erstellt wurde.
- Überprüfen Sie den Typ des temporären Wiederherstellungspunkts — Suchen Sie nach dem `RecoveryPointLifecycle.DeleteAfterEvent` Feld mit dem Wert von, um zu überprüfen, ob es sich um einen temporären Wiederherstellungspunkt handelt. `DELETE_AFTER_COPY`

Überwachen Sie die Anzahl der Kopieraufträge

Überwachen Sie Kopieraufträge ([ListCopyJobs](#)) in Ihren Tresor mit logischem Air-Gap auf Fehler. Ein fehlgeschlagener Kopierauftrag bedeutet, dass Ihr Recovery Point in Ihrem Standard-Backup-Tresor verbleibt, ohne dass ein logischer Air-Gap-Schutz erforderlich ist.

- Status des Kopierauftrags überprüfen — Sie können den Status des Kopierauftrags anhand des vorhandenen Ereignisses überwachen. `Copy Job State Change EventBridge` Filtern Sie optional nach dem Zieldepot (`destinationBackupVaultArn`), um den Fokus auf Tresorkopien mit logischem Air-Gap zu legen.
- Kopien für einen Quellwiederherstellungspunkt verifizieren — Verwenden Sie die [ListCopyJobs](#) API mit dem neuen `BySourceRecoveryPointArn` Filter, um alle Kopieraufträge zu finden, die mit einem bestimmten Wiederherstellungspunkt verknüpft sind, einschließlich automatischer Kopien in Ihren Tresor mit logischem Air-Gap und geplanten Kopien an andere Ziele.
- Überprüfen Sie das Löschen des temporären Wiederherstellungspunkts — Verfolgen Sie den Abschluss des Löschvorgangs des temporären Wiederherstellungspunkts. Wenn der Status des `RUNNING` Kopierauftrags lautet, wurde der Wiederherstellungspunkt noch nicht gelöscht. Wenn die

Kopie in Ihrem Tresor mit logischem Air-Gap gespeichert wurde `FAILED`, wird der Recovery Point für den von Ihnen angegebenen Aufbewahrungszeitraum aufbewahrt.

Note

Die Aufzeichnungen von Kopieraufträgen laufen ab und werden 30 Tage nach Abschluss gelöscht. Nach Ablauf dieses Zeitraums können Sie `ListCopyJobs` den Status historischer Kopien nicht mehr ermitteln.

Überwachen Sie den Erholungspunkt

Suchen Sie nach `EXPIRED` Wiederherstellungspunkten ([ListRecoveryPointsByBackupVault](#)), was darauf hindeutet, dass sie nicht gelöscht werden AWS Backup konnten (möglicherweise aufgrund fehlender Berechtigungen). `EXPIRED` Wiederherstellungspunkte können sich auf Kosten auswirken.

- Überprüfen Sie den Status des Wiederherstellungspunkts — Verwenden Sie das bestehende `EventBridge` Ereignis zur Änderung des Wiederherstellungspunkts, um die Ablaufzeiten zu überwachen.
- Überprüfen Sie das Löschen des temporären Wiederherstellungspunkts — Falls ein Recovery Point, der noch nicht gelöscht wurde, ermitteln Sie mithilfe der `ListCopyJobs` API den Grund, wie oben beschrieben. `DeleteAfterEvent`: `DELETE_AFTER_COPY`

Onboarding und Migration

Wenn Sie derzeit Kopieraktionen verwenden, um Backups in einen Tresor mit logischem Air-Gap zu kopieren, können Sie zur Kostensenkung auf ein primäres Backup mit logischem Air-Gapped Tresor migrieren. Sie können auch Ihre bestehenden kontinuierlichen Amazon S3 S3-Backups von einem Backup-Tresor in einen Tresor mit logischem Air-Gap migrieren. In diesem Handbuch werden die Voraussetzungen und Schritte erläutert, die für die Migration zur primären Backup-Funktion des Tresors mit logischem Air-Gapped erforderlich sind.

Voraussetzungen und bewährte Methoden

Bevor Sie die primäre Backup-Funktion von Vault mit logischem Air-Gap effektiv nutzen können, müssen einige Voraussetzungen und empfohlene bewährte Methoden erfüllt sein.

Voraussetzungen

Derzeit unterstützt ein Tresor mit logischem Air-Gapped als primäres Backup-Ziel nur Backups innerhalb desselben AWS Kontos und AWS derselben Region wie Ihre Backup-Ressourcen. Tresor-Backups mit logischem Air-Gap werden grundsätzlich in separaten Dienstkonten gespeichert, wodurch eine kontoübergreifende und organisationsübergreifende Isolierung gewährleistet wird, ohne dass Kopien auf separate Konten erforderlich sind. Wenn Sie regionsübergreifende Backups benötigen, verwenden Sie weiterhin den Tresor mit logischem Air-Gapped als Kopierziel. Stellen Sie vor der Migration zu dieser Funktion sicher, dass Sie die folgenden Anforderungen erfüllen:

- Regions- und Kontoanforderungen
 - Ihr Tresor mit logischem Air-Gap muss sich in demselben AWS Konto und derselben Region befinden wie Ihre Ressourcen
- Kompatibilität mit Ressourcen
 - Vergewissern Sie sich unter Verfügbarkeit von [Funktionen](#) nach Ressourcen, dass Ihre Ressourcen durch Tresore mit logischem Air-Gap unterstützt werden.
 - Prüfen Sie, ob Ihre Ressourcen die [vollständige AWS Backup](#) Verwaltung unterstützen oder nicht. Die Erfahrung mit der Erstellung von Air-Gap-Backups unterscheidet sich zwischen diesen beiden Ressourcentypen, auch wenn das Ergebnis für beide ähnlich ist.
- Anforderungen an die Verschlüsselung
 - Ressourcen, die keine vollständige AWS Backup Verwaltung unterstützen, müssen entweder unverschlüsselt oder mit vom Kunden verwalteten Schlüsseln (CMKs) verschlüsselt werden. AWS Mit Managed Key (AMK) verschlüsselte Ressourcen werden von einem Tresor mit logischem Air-Gap nicht unterstützt.

Bewährte Methoden

- Beginnen Sie mit einer Pilotmigration unkritischer Ressourcen.
- Überprüfen und passen Sie die Häufigkeit der Backups auf der Grundlage der Leistung von Kopieraufträgen an.
- Implementieren Sie vor der vollständigen Migration eine umfassende Überwachung.
- Überprüfen Sie regelmäßig, ob die Wiederherstellungspunkte in den dafür vorgesehenen Tresoren erstellt wurden.

Planen Sie Ihre Migration

- Überprüfen Sie die bestehenden Backup-Pläne und -Richtlinien.
- Identifizieren Sie, welche Ressourcen die vollständige AWS Backup Verwaltung unterstützen und welche nicht.
 - Ressourcen, die das vollständige AWS Backup Management unterstützen (z. B. EFS, S3) — können direkt in einen Tresor mit logischem Air-Gap gesichert werden
 - Ressourcen, die kein vollständiges AWS Backup Management unterstützen (z. B. EBS EC2, FSx) — erfordern eine temporäre Sicherung im Backup-Tresor, bevor sie in den Logical-Air-Gapped-Tresor kopiert werden
- Überprüfen Sie Ihr aktuelles Backup-Volumen und die Häufigkeit Ihrer Backups und stellen Sie sicher, dass Ihre Konfiguration den Limits für gleichzeitige Kopien für alle Ressourcen entspricht, die kein vollständiges Management unterstützen. AWS Backup
 - Überspringen Sie diesen Schritt, wenn Sie bereits mit derselben Häufigkeit wie Ihre Standard-Tresor-Backups in einen Tresor mit logischem Air-Gap kopieren.
 - Erwägen Sie, die Häufigkeit der Backups bei Bedarf anzupassen, um zu verhindern, dass Kopieraufträge in die Warteschlange gestellt werden.
 - Wenn es zu einer Warteschlange für Kopieraufträge kommt, haben Sie in Ihrem Standard-Backup-Tresor immer noch einen verwendbaren Wiederherstellungspunkt, bis der Kopiervorgang in Ihren Tresor mit logischem Air-Gap abgeschlossen ist. Dieser Recovery Point bietet jedoch nicht das Schutzniveau, das Logically Air-Gapped Tresor bietet.

Ressourcen, die den Migrationspfad zur vollständigen Verwaltung AWS Backup unterstützen

Bei vollständig verwalteten Ressourcen können Sie Daten direkt in Ihrem Tresor mit logischem Air-Gap sichern, ohne dass Kopiervorgänge erforderlich sind.

Für Backups, die auf Snapshots basieren

Dieser Prozess gilt für alle Snapshot-Szenarien, unabhängig davon, ob Ihr Backup-Tresor gesperrt ist. Wenn Sie einen vorhandenen Backup-Plan migrieren oder einen vorhandenen Backup-Tresor (primär) und einen Logic-Air-Gap-Tresor (Kopie) in einem neuen Backup-Plan verwenden:

1. Behalten Sie Ihren vorhandenen Backup-Tresor bei oder fügen Sie ihn als Backup-Ziel hinzu ().
TargetBackupVaultName Dieser Tresor speichert keine Backups, muss aber aus Gründen der Abwärtskompatibilität bereitgestellt werden.

2. Aktualisieren Sie Ihren Backup-Plan so, dass er den Tresor mit logischem Air-Gap (`TargetLogicallyAirGappedBackupVaultArn`), der sich in demselben Konto befindet, als primäres Ziel enthält.
3. Prüfen Sie alle bestehenden Kopieraktionen in einen anderen Tresor mit logischem Air-Gap, um festzustellen, ob sie noch benötigt werden. Sie können diesen Tresor in Schritt 2 auch als primäres Ziel verschieben, wenn er sich in demselben Konto befindet.

Für kontinuierliche Amazon S3 S3-Backups

Logischerweise unterstützt Air-Gapped Vault als primäres Backup-Ziel kontinuierliche Backups für Amazon S3. Sie können jedoch nur einen aktiven kontinuierlichen Wiederherstellungspunkt pro Ressource in einem einzigen Tresor verwalten. Wenn Sie bereits über einen aktiven Amazon S3 Continuous Recovery Point verfügen, müssen Sie ihn trennen oder löschen, bevor Sie einen neuen in einem anderen Tresor erstellen können. Wenn Sie Ihrem Backup-Plan ein Vault-Ziel mit logischem Air-Gap (von demselben Konto) hinzufügen, das über einen aktiven kontinuierlichen Amazon S3 S3-Wiederherstellungspunkt verfügt, schlägt der kontinuierliche Backup-Job fehl.

So migrieren Sie Ihren Amazon S3 S3-Continuous-Recovery-Point von einem entsperrten Backup-Tresor zu Ihrem Logic Air-Gap-Speicher:

1. Aktualisieren Sie Ihren Backup-Plan, um Ihrem Tresor mit logischem Air-Gap eine Kopieraktion hinzuzufügen. Dadurch sinken Ihre Kosten für die Erstellung des ersten Backups in Ihrem Tresor mit logischem Air-Gap. Überspringen Sie diesen Schritt, wenn Sie bereits Daten in Ihren lokalen Tresor mit logischem Air-Gap kopieren.
2. Stellen Sie sicher, dass mindestens eine Snapshot-Kopie in Ihrem Tresor mit logischem Air-Gap erfolgreich abgeschlossen wurde, bevor Sie fortfahren.
3. Trennen Sie den bestehenden Amazon S3 Continuous Recovery Point. Rufen Sie die [DisassociateRecoveryPoint](#) API auf, um den Status des Wiederherstellungspunkts von VERFÜGBAR auf GESTOPPT zu ändern. Durch diese Aktion werden Ihre vorhandenen Backup-Daten beibehalten und gleichzeitig verhindert, dass neue Daten hinzugefügt werden.
4. Aktualisieren Sie den Backup-Plan, um den Tresor (`TargetLogicallyAirGappedBackupVaultArn`) mit logischem Air-Gapped als Backup-Ziel hinzuzufügen.
5. Entfernen Sie alle vorherigen Kopieraktionen aus dem Plan.

6. Bei der nächsten Ausführung des Backup-Plans wird ein neuer kontinuierlicher Wiederherstellungspunkt in Ihrem Tresor mit logischem Air-Gap erstellt. Dieser Wiederherstellungspunkt wird inkrementell und basiert auf dem kopierten Snapshot aus Schritt 1.

So migrieren Sie Ihren Amazon S3 S3-Continuous-Recovery-Point von einem gesperrten Backup-Tresor zu Ihrem Logic Air-Gap-Speicher:

1. Aktualisieren Sie Ihren Backup-Plan, um Ihrem Tresor mit logischem Air-Gap eine Kopieraktion hinzuzufügen. Dadurch sinken Ihre Kosten für die Erstellung des ersten Backups in Ihrem Tresor mit logischem Air-Gap. Überspringen Sie diesen Schritt, wenn Sie bereits Daten in Ihren lokalen Tresor mit logischem Air-Gap kopieren.
2. Stellen Sie sicher, dass mindestens eine Snapshot-Kopie in Ihrem Tresor mit logischem Air-Gap erfolgreich abgeschlossen wurde, bevor Sie fortfahren. Stellen Sie sicher, dass der kopierte Snapshot über einen ausreichend langen Aufbewahrungszeitraum verfügt, um verfügbar zu bleiben, bis Sie alle Schritte abgeschlossen haben.
3. Fügen Sie den Tresor mit logischem Air-Gap als primäres Ziel hinzu und entfernen Sie alle Kopieraktionen.
 - a. Dieser Schritt ist erforderlich, da gesperrte Tresore die Trennung von kontinuierlichen Wiederherstellungspunkten nicht unterstützen.
 - b. Ihr vorhandener Continuous Recovery Point im gesperrten Backup-Tresor sammelt weiterhin Daten an, bis er entsprechend seinem Lebenszyklus abläuft.
 - c. Neue kontinuierliche Backup-Jobs schlagen fehl, da pro Ressource nur ein aktiver kontinuierlicher Wiederherstellungspunkt existieren kann. Da diese Jobs fehlschlagen, werden keine Kopieraktionen ausgeführt.
4. Warten Sie, bis der bestehende Continuous Recovery Point abläuft. Nach Ablauf wird im Tresor mit logischem Air-Gap ein neuer Continuous Recovery Point erstellt. Dieser Wiederherstellungspunkt wird auf der Grundlage des kopierten Snapshots aus Schritt 1 inkrementell berechnet, sofern der Snapshot noch in Ihrem Tresor mit logischem Air-Gap vorhanden ist.
5. Alle in Ihrem Standardspeicher gesammelten Daten gehen nach Ablauf verloren. Nur Daten, die nach der Erstellung des neuen Wiederherstellungspunkts im Tresor mit Logical-Air-Gaps gesichert wurden, werden beibehalten.

Ressourcen, die den Migrationspfad für die vollständige AWS Backup Verwaltung nicht unterstützen

Nicht vollständig verwaltete Ressourcen erfordern einen Kopiervorgang in den Tresor mit logischem Air-Gap. Bei diesem Vorgang wird in Ihrem Standard-Backup-Tresor ein temporärer (kostenpflichtiger) Recovery Point erstellt, der automatisch in Ihren Tresor mit logischem Air-Gap kopiert und nach Abschluss des Kopiervorgangs gelöscht wird. Wenn Sie Ihren Backup-Plan so aktualisieren, dass er ein Tresor-Ziel mit logischem Air-Gap enthält, gehen Sie wie folgt vor:

- Backup-Jobs erstellen einen Wiederherstellungspunkt in Ihrem Backup-Tresor. Dieser Lebenszyklus ist vom DELETE_AFTER_COPY Ereignis abhängig.
- Ein Kopierauftrag leitet automatisch die Übertragung des Wiederherstellungspunkts in Ihren Tresor mit logischem Air-Gap ein.
- Nachdem der Kopiervorgang erfolgreich abgeschlossen wurde, wird der temporäre Erholungspunkt in Ihrem Tresor gelöscht.
- Wenn der Kopiervorgang fehlschlägt, wird der temporäre Recovery Point für eine maximale Dauer gemäß dem von Ihnen angegebenen Aufbewahrungszeitraum aufbewahrt, sodass sichergestellt ist, dass Sie über einen verwendbaren Recovery Point verfügen.

Fehlerbehebung

Der Backup- oder Kopierauftrag schlägt mit einem Lebenszyklus-Inkompatibilitätsfehler fehl

Fehler bei Backup-Jobs: Backup job failed because the lifecycle is outside the valid range for backup vault.

Fehler bei Kopierjobs: Copy job failed. The retention specified in the job is not within the range specified for the target Backup Vault.

Mögliche Ursache: Backup- oder Kopieraufträge schlagen fehl, weil der Aufbewahrungszeitraum nicht mit den Mindest- oder Höchstaufbewahrungseinstellungen des Logic Air-Gapped Tresors vereinbar ist.

Lösung: Aktualisieren Sie Ihren Backup-Plan und geben Sie einen Aufbewahrungszeitraum an, der innerhalb der für Ihren Logic Air-Gap-Speicher konfigurierten Mindest- und Höchstaufbewahrungszeiträume liegt.

Kontinuierliche Backup-Jobs schlagen mit der Meldung „Kontinuierliches Backup ist bereits aktiviert“ fehl

Fehler: Bucket {bucket_name} already has continuous backup enabled for another vault Backup job failed.

Mögliche Ursache: Kontinuierliche Backup-Jobs schlagen fehl, weil es in einem anderen Tresor bereits einen kontinuierlichen Wiederherstellungspunkt für die Ressource gibt.

Lösung: Jede Ressource kann nur über einen kontinuierlichen Wiederherstellungspunkt verfügen. Wenn Ihr Backup-Tresor entsperrt ist, trennen Sie den vorhandenen Continuous Recovery Point mit dem [disassociate-recovery-point](#) folgenden Befehl. Wenn Ihr Backup-Tresor gesperrt ist, warten Sie, bis der bestehende Continuous Recovery Point entsprechend seinem Lebenszyklus abläuft.

Der Backup-Job wird mit „Mit Problemen abgeschlossen“ abgeschlossen — Ressourcentyp wird nicht unterstützt

Meldung: Backup job completed successfully to the target backup vault. This resource type is not supported by logically air-gapped backup vault.

Mögliche Ursache: Bei Sicherungsaufträgen für nicht unterstützte, nicht vollständig verwaltete Ressourcen wird die Meldung „Mit Problemen abgeschlossen“ angezeigt. Die Meldung weist darauf hin, dass die Ressource nicht unterstützt wird.

Lösung: Ressourcentypen, die nicht unterstützt werden, werden nur im Backup-Tresor gesichert. Wenn Sie diese Backups in Ihrem Backup-Tresor behalten möchten, sind keine Maßnahmen erforderlich. Wenn Sie es vorziehen, nicht unterstützte Ressourcen mit Ihrem Logic-Air-Gap-Tresor zu kombinieren, haben Sie folgende Möglichkeiten:

- Entfernen Sie die Ressource oder das Ziel des Tresors mit logischem Air-Gap aus Ihrem Backup-Plan für diese Ressourcen und setzen Sie die Sicherung ausschließlich in Ihrem Backup-Tresor fort. Sie können die Ressource anschließend als Teil eines anderen Plans hinzufügen.

Der Backup-Job wird mit „Mit Problemen abgeschlossen“ abgeschlossen — Verschlüsselungsschlüssel wird nicht unterstützt

Meldung: Backup job completed successfully to the target backup vault. This resource is encrypted with an AWS managed key and cannot be copied to a logically air-gapped backup vault.

Mögliche Ursache: Bei Sicherungsaufträgen für nicht unterstützte, nicht vollständig verwaltete Ressourcen wird die Meldung „Mit Problemen abgeschlossen“ angezeigt. Außerdem wird eine Meldung angezeigt, dass die Ressource mit einem AWS verwalteten Schlüssel verschlüsselt ist.

Lösung: Nicht vollständig verwaltete Ressourcen, die mit verwalteten Schlüsseln verschlüsselt wurden, können nicht in Tresore mit AWS logischem Air-Gap kopiert werden. Wenn Sie diese Backups in Ihrem Backup-Tresor behalten möchten, sind keine Maßnahmen erforderlich. Wenn Sie es vorziehen, nicht unterstützte Ressourcen mit Ihrem Logic-Air-Gap-Tresor zu kombinieren, haben Sie folgende Möglichkeiten:

- Verschlüsseln Sie Ihre Ressourcen erneut mit einem vom Kunden verwalteten KMS-Schlüssel, oder
- Entfernen Sie die Ressource oder das Vault-Ziel mit logischem Air-Gap aus Ihrem Backup-Plan für diese Ressourcen und setzen Sie die Sicherung ausschließlich in Ihrem Backup-Tresor fort. Sie können die Ressource anschließend als Teil eines anderen Plans hinzufügen.

Die Wiederherstellungspunkte bleiben im **EXPIRED** Status

Mögliche Ursache: Temporäre Wiederherstellungspunkte wechseln in den EXPIRED Status, werden aber nicht gelöscht.

Lösung: AWS Backup Möglicherweise fehlen die Berechtigungen zum Löschen der Wiederherstellungspunkte. Stellen Sie sicher, dass Ihre Backup-Rolle über die erforderlichen IAM-Berechtigungen verfügt. Möglicherweise müssen Sie `expired` Wiederherstellungspunkte manuell löschen.

Kopieraufträge befinden sich in der Warteschlange oder schlagen aufgrund der hohen Sicherungshäufigkeit fehl

Mögliche Ursache: Kopieraufträge in Tresore mit logischem Air-Gap befinden sich in Warteschlangen oder schlagen fehl, weil Backups häufiger geplant werden, als Kopien abgeschlossen werden können.

Lösung: Reduzieren Sie die Häufigkeit Ihrer Backups oder passen Sie Ihren Backup-Zeitplan an, um mehr Zeit zwischen den Backups zu haben. Informationen zu den Beschränkungen für gleichzeitige Kopien finden Sie in der [Dokumentation zu den AWS Backup Kontingenten](#).

Genehmigung durch mehrere Parteien für Tresore mit logischem Air-Gap

Überblick über die Genehmigung durch mehrere Parteien in einem Tresor mit logischen Lücken

AWS Backup bietet Ihnen die Möglichkeit, Ihren Tresoren mit logischem [Air-Gap eine Genehmigung durch mehrere Parteien](#) hinzuzufügen AWS Organizations, eine Funktion von. Die Genehmigung durch mehrere Parteien bietet eine zusätzliche Option, mit der kritische Abläufe durch einen verteilten Genehmigungsprozess geschützt werden können.

Die Genehmigung durch mehrere Parteien dient dem Schutz kritischer Ressourcen und der Minimierung der Zeit bis zur Wiederherstellung des vollen Betriebs, z. B. bei Störungen durch böswillige Akteure oder Malware-Ereignisse. Diese Konfiguration kann Ihnen helfen, den Inhalt eines Tresors mit logischem Air-Gap wiederherzustellen, der möglicherweise kompromittiert wurde.

[Es fallen keine zusätzlichen Kosten für die Integration und den Einsatz von Genehmigungsteams mit mehreren Parteien und AWS Backup Logic-Air-Gap-Tresoren an \(es fallen Gebühren für Speicher und regionsübergreifende Übertragungen an, wie auf der Preisseite angegeben\).](#)

Als AWS Backup Kunde können Sie die Mehrparteigenehmigung verwenden, um einer Gruppe vertrauenswürdiger Personen Genehmigungsfunktionen für einige Operationen zu gewähren, die gemeinsam den Zugriff auf einen Tresor mit logischem Air-Gap von einem separat erstellten Wiederherstellungskonto aus genehmigen können, falls der Verdacht auf böswillige Aktivitäten besteht, die die Nutzung des Hauptkontos gefährden könnten.

In den folgenden Schritten wird der empfohlene Ablauf für die Einrichtung einer AWS Wiederherstellungsorganisation, die Einrichtung der Mehrparteigenehmigung und die anschließende Verwendung der Mehrparteigenehmigung mit Ihren Tresoren mit logischen Air-Gaps beschrieben:

1. Ein Administrator [erstellt über Organizations eine neue Organisation](#), die für Wiederherstellungsvorgänge verwendet wird.
2. Im Verwaltungskonto dieser neuen Organisation erstellt und konfiguriert der Administrator eine IAM Identity Center (IDC) -Instanz (Informationen zur Aktivierung einer Organisationsinstanz finden Sie unter [Aktivieren von IAM Identity Center im IAM Identity Center-Benutzerhandbuch](#)). Weitere Informationen finden Sie im Benutzerhandbuch für die Genehmigung [mehrerer Parteien in der Reihenfolge „Identitätsquelle für die Genehmigung durch mehrere Parteien erstellen“](#).
3. Der Administrator stellt dann [ein Genehmigungsteam zusammen. Dabei handelt es sich um](#) die Kerngruppe vertrauenswürdiger Personen, die die Hauptnutzer von Multi-Party Approval sein werden.

4. Der Administrator [teilt AWS RAM sich ein Genehmigungsteam](#) für jedes Konto, das mindestens einen Tresor mit logischem Air-Gap besitzt (wahrscheinlich Ihr primäres Konto). Sowohl für das Konto, dem der Tresor gehört, als auch für das sekundäre Unternehmen muss RAM eingerichtet sein.
5. Ein Administrator dieser Konten [ordnet einen Tresor mit logischem Air-Gap einem Genehmigungsteam](#) zu.
6. Ein Wiederherstellungskonto [fordert Zugriff auf](#) ein Konto an, das über einen Tresor mit logischem Air-Gap verfügt, dem ein Genehmigungsteam („Team“) mit mehreren Parteien zugeordnet ist. Das dem Konto zugeordnete Team [genehmigt](#) die Anfrage oder lehnt sie ab.
7. Der Administrator des Accounts, dem der Tresor mit logischem Air-Gap gehört, kann beantragen, dass das [Genehmigungsteam vom Tresor getrennt wird](#). Für die Anfrage ist eine aktuelle Genehmigung durch das Team erforderlich.
8. Ein Administrator kann die [Mitglieder des Genehmigungsteams bei Bedarf entsprechend seinen Sicherheitspraktiken aktualisieren](#) oder wenn Personen Ihrer Organisation beitreten oder sie verlassen.

Voraussetzungen und bewährte Methoden für die Verwendung der Genehmigung durch mehrere Parteien bei einem Tresor mit logischem Air-Gap

Bevor Sie die Genehmigung durch mehrere Parteien effektiv und sicher für Ihre Datenspeicher mit logischen Air-Gaps nutzen können, müssen zunächst einige Voraussetzungen und empfohlene bewährte Verfahren erfüllt sein.

Bewährte Verfahren:

- Zwei (oder mehr) AWS Organizations über Organisationen. Eines sollte Ihre primäre Organisation sein, in der Sie über ein oder mehrere Konten verfügen, die über mindestens einen Tresor mit logischem Air-Gap verfügen. Bei der sekundären Organisation sollte es sich um Ihre Wiederherstellungsorganisation handeln. In dieser Organisation wird Ihr Genehmigungsteam für mehrere Parteien verwaltet.

Voraussetzungen

1. Sie haben die [Genehmigung durch mehrere Parteien eingerichtet](#) und verfügen über mindestens ein Genehmigungsteam.

2. Mindestens ein Konto in Ihrer primären Organisation muss über einen Tresor mit logischem Air-Gap (und den ursprünglichen Backup-Tresor) verfügen.
3. Für das Verwaltungskonto in der primären Organisation wurde die Genehmigung durch mehrere Parteien aktiviert.

 Tip

AWS Backup empfiehlt, eine Service Control Policy (SCP) auf Ihre primäre Organisation anzuwenden und diese mit den entsprechenden Berechtigungen für die Organisation und jedes Genehmigungsteam zu konfigurieren. Ein Beispiel für eine Richtlinie finden Sie im Abschnitt [Bedingungen für die Genehmigung durch mehrere Parteien](#).

4. Ihr Mehrparteien-Genehmigungsteam aus der sekundären Organisation (Wiederherstellung) wird sowohl AWS RAM mit Ihren [Konten geteilt](#), denen die Logic Air-Gapped Tresore gehören, als auch mit Ihren Wiederherstellungskonten.

Regionalübergreifende Überlegungen und Abhängigkeiten bei der Verwendung der Genehmigung durch mehrere Parteien

Wenn Sie die Genehmigung durch mehrere Parteien aktivieren und Ihre IAM Identity Center-Instanz in verschiedenen Regionen aktiviert haben, werden bei der Genehmigung durch mehrere Parteien regionsübergreifend Anrufe an IAM Identity Center weitergeleitet. Das bedeutet, dass Benutzer- und Gruppeninformationen zwischen den Regionen übertragen werden. Ressourcen des Genehmigungsteams mit mehreren Parteien können nur in AWS-Region USA Ost (Nord-Virginia) erstellt und gespeichert werden.

Andere AWS-Regionen, die sich auf Ressourcen des Genehmigungsteams mehrerer Parteien beziehen, hängen von AWS-Region US East (Nord-Virginia) ab. Dementsprechend werden bei der Genehmigung durch mehrere Parteien regionsübergreifende Anrufe getätigt, wenn sich Ihr Identity Center-Instance and/or logischerweise Air-Gap-Tresor nicht in USA Ost (Nord-Virginia) befindet.

Bedingungen, Konzepte und Benutzerpersönlichkeiten für die Genehmigung durch mehrere Parteien

Die Genehmigung durch mehrere Parteien in Ihrem Tresor mit logischem Air-Gap ist eine Integration von AWS Organizations, und AWS -Kontenverwaltung AWS Backup, zusammen mit AWS Identity and Access Management (IAM) - und (RAM) -Funktionen. AWS RAM Über die CLI können Sie mit

jedem Dienst interagieren, um die entsprechenden Befehle zu senden. Sie können auch die Konsole verwenden, müssen jedoch zur Konsole des entsprechenden Dienstes navigieren, um bestimmte Aufgaben auszuführen.

Wie Sie mit der Genehmigung durch mehrere Parteien umgehen, hängt von Ihren Rollen und Verantwortlichkeiten in Ihren Organisationen sowie von den Berechtigungen ab, die Sie in Ihren AWS Backup Konten haben.

Wie im [Benutzerhandbuch für Mehrparteigenehmigungen beschrieben, handelt](#) es sich bei Mitgliedern Ihrer Organisation, die die Mehrparteigenehmigung verwenden, entweder um Antragsteller, Administrator oder Genehmiger. [Für jede Stellenfunktion gelten spezifische Berechtigungen.](#) Gemäß den bewährten Sicherheitsmethoden sollte ein Benutzer nur eine Jobfunktion erfüllen.

Konsolen, Portale und Sitzungen

AWS Backup Für Konten mit einem oder mehreren Tresoren mit logischem Air-Gap kann eine Genehmigung durch mehrere Parteien erforderlich sein.

Vor dem Genehmigungsprozess durch mehrere Parteien erstellt ein Administrator für Wiederherstellungszwecke eine sekundäre Organisation (eine Wiederherstellungsorganisation), sofern noch keine solche eingerichtet wurde. AWS Organizations

Anschließend verwendet der Administrator AWS Resource Access Manager (RAM), um die organisationsübergreifende gemeinsame Nutzung zwischen der primären Organisation und der Wiederherstellungsorganisation einzurichten.

In der primären Organisation befinden sich Konten, die über einen Tresor mit logischem Air-Gap verfügen und diesen nutzen, in dem die geschützten Daten gespeichert werden.

In der Wiederherstellungsorganisation gibt es mindestens ein Wiederherstellungskonto. Dieses Konto beherbergt einen Zugriffspunkt, der als wichtige „Hintertür“ zum gemeinsam genutzten Tresor mit logischem Air-Gap dienen kann. Dieser Zugriffspunkt wird als Backup-Tresor mit Wiederherstellungszugriff bezeichnet. Dieser Access Vault speichert keine Daten, sondern dient als Zugriffs- oder Bereitstellungspunkt, der den Inhalt des Quell-Tresors mit logischem Air-Gap wiedergibt, aber keine Daten enthält, die geändert oder gelöscht werden können. Wenn ein Kunde beispielsweise den Wiederherstellungsprozess für einen Recovery Point in einem Backup-Tresor mit Wiederherstellungszugriff durchläuft, ist es der Recovery Point im Tresor mit logischem Air-Gap, der durch eine kontenübergreifende Wiederherstellung über das Wiederherstellungskonto wiederhergestellt wird.

Um zusätzliche Sicherheit zu gewährleisten, verwenden Kunden dieses Wiederherstellungskonto, um geschützte Vorgänge im Hauptkonto durchzuführen, jedoch erst, nachdem diese Vorgänge vom zugehörigen [Genehmigungsteam in einer Genehmigungssitzung genehmigt](#) wurden. Eine Sitzung wird erstellt, AWS sobald eine Genehmigungsanfrage gesendet wurde. Diese Sitzung endet, wenn eine bestimmte Anzahl von Mitgliedern des Genehmigungsteams die Anfrage genehmigt oder ablehnt oder wenn die zulässige Sitzungszeit abgelaufen ist.

Ein Team besteht aus Genehmigungsberechtigten (also die Parteien sind Teil der Genehmigung durch mehrere Parteien), die E-Mail-Benachrichtigungen über geschützte Operationsanfragen erhalten. Diese E-Mails bestätigen, dass eine Genehmigungssitzung für die Anfrage begonnen hat. Die Genehmigung wird erteilt, sobald die erforderliche Mindestgenehmigungsschwelle erreicht ist. Dieser Schwellenwert kann bei der Erstellung des Genehmigungsteams mit mehreren Parteien („Team“) festgelegt werden.

Genehmigungsteams mit mehreren Parteien werden über das Mehrparteien-Genehmigungsportal („Portal“) von Organizations verwaltet, eine AWS verwaltete Anwendung, die Identitäten einen zentralen Ort bietet, an dem Mitglieder des Genehmigungsteams Einladungen und Vorgangsanfragen des Genehmigungsteams empfangen und darauf antworten können.

Aufgaben des Administrators

Für mehrere Aufgaben, die AWS Backup einen Überblick über mehrere Parteien erforderten, war ein Benutzer mit Administratorberechtigungen und Zugriff auf das Verwaltungskonto erforderlich.

Stellen Sie ein Genehmigungsteam zusammen

Ein Benutzer in Ihrer Organisation mit Administratorberechtigungen für ein AWS Konto muss die [Genehmigung durch mehrere Parteien einrichten](#) (Schritt 3 in der [Übersicht](#)).

Bevor Sie diesen Schritt ausführen, empfiehlt es sich als bewährte Methode, sowohl eine primäre Organisation als auch eine sekundäre Organisation (für Wiederherstellungszwecke) einzurichten AWS Organizations (Schritt 1 in der [Übersicht](#)).

Informationen zur [Erstellung Ihres Teams finden Sie unter Erstellen eines Genehmigungsteams](#) im Benutzerhandbuch zur Genehmigung mehrerer Parteien.

Während der [aws mpa create-approval-team](#) Operation ist `policies` einer der Parameter. Dies ist eine Liste von Ressourcenrichtlinien ARNs (Amazon Resource Names) für die Genehmigung durch mehrere Parteien, die Berechtigungen zum Schutz des Teams definieren.

Die Richtlinie, die im Beispiel im Benutzerhandbuch für die Genehmigung mehrerer Parteien im Verfahren [Ein Genehmigungsteam erstellen](#) dargestellt ist, enthält die Richtlinie `["arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault"]` mit mehreren erforderlichen Berechtigungen.

Gehen Sie wie folgt vor, um eine Liste der verfügbaren Richtlinien zurückzugeben, indem Sie Folgendes verwenden `mpa list-policies`:

1. Richtlinien auflisten:

```
aws mpa list-policies --region us-east-1
```

2. Alle Richtlinienversionen auflisten:

```
aws mpa list-policy-versions --policy-arn arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault --region us-east-1
```

3. Einzelheiten zu einer Richtlinie abrufen:

```
aws mpa get-policy-version --policy-version-arn arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault/1 --region us-east-1
```

Weiter unten finden Sie die Richtlinie, die im Rahmen dieses Vorgangs erstellt und dann Ihrem Genehmigungsteam zugewiesen wird:

Access Vault-Richtlinie wiederherstellen

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VaultOwnerPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*",
      "Action": [
```

```

        "mpa:StartSession",
        "mpa:CancelSession"
    ],
    "Condition": {
        "StringEquals": {
            "mpa:RequestedOperation": "backup:RevokeRestoreAccessBackupVault",
            "mpa:ProtectedResourceAccount": "${aws:PrincipalAccount}"
        },
        "Bool": {
            "aws:ViaAWSService": "true"
        }
    }
}
]
}

```

Teilen Sie sich ein Genehmigungsteam mit mehreren Parteien unter AWS RAM

[Mithilfe von AWS Resource Access Manager \(RAM\), Schritt 4 in der Übersicht, können Sie ein Mehrparteien-Genehmigungsteam mit anderen AWS Accounts teilen.](#)

Console

Teilen Sie sich ein Mehrparteien-Genehmigungsteam mit AWS RAM

1. Melden Sie sich bei der [AWS RAM -Konsole](#) an.
2. Wählen Sie im Navigationsbereich Resource Shares aus.
3. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.
4. Geben Sie im Feld Name einen aussagekräftigen Namen für Ihre Ressourcenfreigabe ein.
5. Wählen Sie im Dropdownmenü unter Ressourcentyp die Option Genehmigungsteam für mehrere Parteien aus.
6. Wählen Sie unter Ressourcen das Genehmigungsteam aus, das Sie gemeinsam nutzen möchten.
7. Geben Sie unter Principals die AWS Accounts an, mit denen Sie das Genehmigungsteam teilen möchten.
8. Um die Daten für bestimmte AWS Konten freizugeben, wählen Sie AWS Konten aus und geben Sie das 12-stellige Konto ein. IDs

9. Um Inhalte mit einer Organisation oder Organisationseinheit zu teilen, wählen Sie Organisation oder Organisationseinheit aus und geben Sie die entsprechende ID ein.
10. (Optional) Fügen Sie unter Tags alle Tags hinzu, die Sie dieser gemeinsamen Ressource zuordnen möchten.
11. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

Der Status der Ressourcenfreigabe wird zunächst als angezeigt `PENDING`. Sobald die Empfängerkonten die Einladung annehmen, ändert sich der Status auf `ACTIVE`.

CLI

Verwenden Sie die folgenden Befehle, um ein Genehmigungsteam mit mehreren Parteien gemeinsam AWS RAM über die CLI zu verwenden:

Identifizieren Sie zunächst den ARN des Genehmigungsteams, das Sie teilen möchten:

```
aws mpa list-approval-teams --region us-east-1
```

Erstellen Sie eine Ressourcenfreigabe mit dem `create-resource-share` folgenden Befehl:

```
aws ram create-resource-share \  
--name "MPA-Team-Share" \  
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \  
--principals "ACCOUNT_ID_TO_SHARE_WITH" \  
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \  
--region us-east-1
```

Um sie mit einer Organisation statt mit bestimmten Konten zu teilen:

```
aws ram create-resource-share \  
--name "MPA-Team-Share" \  
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \  
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \  
--allow-external-principals \  
--region us-east-1
```

Prüfen Sie den Status Ihrer gemeinsam genutzten Ressource:

```
aws ram get-resource-shares \  
--resource-owner SELF \  

```



```
--region us-east-1
```

Die Empfängerkonten müssen die Einladung zur gemeinsamen Nutzung von Ressourcen annehmen:

```
aws ram get-resource-share-invitations --region us-east-1
```

Führen Sie das Empfängerkonto aus, um eine Einladung anzunehmen:

```
aws ram accept-resource-share-invitation \  
--resource-share-invitation-arn "arn:aws:ram:REGION:ACCOUNT_ID:resource-share-  
invitation/INVITATION_ID" \  
--region us-east-1
```

Sobald die Einladung angenommen wurde, steht das Team für die Genehmigung mehrerer Parteien im Empfängerkonto zur Verfügung.

AWS bietet Tools für den gemeinsamen Kontozugriff, einschließlich Durchgangs [AWS Resource Access Manager](#)- und [Mehrparteienzugriff](#). Wenn Sie sich dafür entscheiden, einen Tresor mit logischem Air-Gap gemeinsam mit einem anderen Konto zu nutzen, sollten Sie die folgenden Details berücksichtigen:

Feature	AWS RAM basiertes Teilen	Auf Genehmigung durch mehrere Parteien basierender Zugriff
Zugriff auf Tresore mit logischem Air-Gap	Sobald die gemeinsame Nutzung des RAM abgeschlossen ist, kann auf die Tresore zugegriffen werden.	Jeder Versuch mit einem anderen Konto muss von einer bestimmten Anzahl von Mitgliedern des Genehmigungsteams für mehrere Parteien genehmigt werden. Die Genehmigungssitzung läuft automatisch 24 Stunden nach der Initiierung der Anfrage ab.

Feature	AWS RAM basiertes Teilen	Auf Genehmigung durch mehrere Parteien basierender Zugriff
Entfernung des Zugriffs	Das Konto, dem der Tresor mit logischem Air-Gap gehört, kann die RAM-basierte gemeinsame Nutzung jederzeit beenden.	Der Zugriff auf einen Tresor kann nur durch eine Anfrage an das Genehmigungsteam für mehrere Parteien entzogen werden.
Zwischen Konten and/or und Regionen kopieren	Wird derzeit nicht unterstützt.	Backups können innerhalb desselben Kontos oder mit anderen Konten in derselben Organisation wie das Wiederherstellungskonto kopiert werden.
Abrechnung bei regionsübergreifender Überweisung		Regionsübergreifende Übertragungen werden demselben Konto in Rechnung gestellt, dem der Backup-Tresor mit Wiederherstellungszugriff gehört.
Empfohlene Verwendung	Es wird hauptsächlich für die Wiederherstellung nach Datenverlust und für Wiederherstellungstests verwendet.	Hauptsächlich wird es in Situationen verwendet, in denen der Verdacht besteht, dass der Kontozugriff oder die Sicherheit gefährdet sind.
Regionen	Verfügbar in allen Bereichen, in AWS-Regionen denen Tresore mit logischem Air-Gap unterstützt werden.	Verfügbar in allen Bereichen, in AWS-Regionen denen Tresore mit logischem Air-Gap unterstützt werden.

Feature	AWS RAM basiertes Teilen	Auf Genehmigung durch mehrere Parteien basierender Zugriff
Wiederherstellungen	Alle unterstützten Ressourcentypen können von einem gemeinsamen Konto aus wiederhergestellt werden.	Alle unterstützten Ressourcentypen können von einem gemeinsamen Konto aus wiederhergestellt werden.
Einrichtung	Die gemeinsame Nutzung kann erfolgen, sobald das AWS Backup Konto die RAM-Sharing eingerichtet hat und das Empfängerkonto die gemeinsame Nutzung akzeptiert.	Für die gemeinsame Nutzung muss das Verwaltungskonto zuerst ein Team erstellen und dann die RAM-Sharing einrichten. Anschließend entscheidet sich das Verwaltungskonto für die Genehmigung durch mehrere Parteien und weist das Team einem Tresor mit logischem Air-Gap zu.
Teilen	Die gemeinsame Nutzung erfolgt über RAM innerhalb derselben AWS Organisation oder zwischen AWS Organisationen. Der Zugriff wird nach dem „Push“-Modell gewährt, bei dem das Konto, dem der Tresor mit logischem Air-Gap gehört, zuerst Zugriff gewährt. Dann akzeptiert das andere Konto den Zugriff.	Der Zugriff auf einen Tresor mit logischem Air-Gap erfolgt über von Organisationen unterstützte Genehmigungsteams innerhalb derselben AWS Organisation oder organisationsübergreifend. Der Zugriff wird nach dem „Pull“-Modell gewährt, bei dem das empfangende Konto zuerst Zugriff anfordert und dann das Genehmigungsteam die Anfrage gewährt oder ablehnt.

Aufgaben des Anfragenden

Ordnen Sie einem Tresor mit logischem Air-Gap ein Genehmigungsteam mit mehreren Parteien zu

Anforderer: Benutzer mit Zugriff auf das Konto, dem der Tresor mit logischem Air-Gap gehört.

[Sie können einem Tresor mit logischem Air-Gap ein Genehmigungsteam mit mehreren Parteien zuordnen, um gemeinsam den Zugriff auf den Tresor genehmigen zu können \(Schritt 5 in der Übersicht\).](#)

Console

Ordnen Sie einem Tresor mit logischen Lücken ein Genehmigungsteam mit mehreren Parteien zu

1. [Öffnen Sie die Konsole unter AWS Backup /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Navigieren Sie im linken Navigationsbereich zum Abschnitt Backup-Tresore.
3. Wählen Sie den Backup-Tresor mit logischem Air-Gap aus, den Sie einem MPA-Team zuordnen möchten.
4. Wählen Sie auf der Seite mit den Tresordetails die Option Genehmigungsteam zuweisen aus.
5. Wählen Sie im Dropdownmenü das Genehmigungsteam aus, das Sie dem Tresor zuordnen möchten
6. Optional Geben Sie einen Kommentar ein, in dem der Grund für die Zuordnung erläutert wird.
7. Wählen Sie Anfrage senden aus, um die Zuordnungsanfrage einzureichen.

Wenn dies das erste Genehmigungsteam ist, das dem Tresor zugeordnet wird, wird das Team dem Tresor zugeordnet. Falls dem Tresor bereits ein Team zugeordnet ist, finden Sie die entsprechenden Schritte unter [Genehmigungsteam für mehrere Parteien aktualisieren](#).

CLI

Verwenden Sie den CLI-Befehl `associate-backup-vault-mpa-approval-team`, der mit den folgenden Parametern geändert wurde:

```
aws backup associate-backup-vault-mpa-approval-team \
--backup-vault-name VAULT_NAME \
--mpa-approval-team-arn MPA_TEAM_ARN \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Wenn dies das erste Genehmigungsteam ist, das dem Tresor zugeordnet wird, wird das Team dem Tresor zugeordnet. Falls dem Tresor bereits ein Team zugeordnet ist, finden Sie die entsprechenden Schritte unter [Genehmigungsteam für mehrere Parteien aktualisieren](#).

Beantragen Sie Zugriff auf einen Tresor mit logischem Air-Gap

Anforderer: Benutzer mit Zugriff auf das Wiederherstellungskonto.

[Sie können den Zugriff auf einen Tresor mit logischem Air-Gap in einem anderen Konto beantragen \(Schritt 6 in der Übersicht\).](#)

Nachdem ein Genehmigungsteam der Anfrage stattgegeben hat, AWS Backup erstellt es in Ihrem angegebenen Wiederherstellungskonto einen Backup-Tresor mit Wiederherstellungszugriff, sodass dieses Konto Zugriff auf Wiederherstellungspunkte im verbundenen Tresor mit logischem Air-Gap hat.

Console

Beantragen Sie Zugriff auf einen Tresor mit logischem Air-Gap

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](#)
2. Navigieren Sie im linken Navigationsbereich zum Abschnitt Backup-Tresore.
3. Wählen Sie die Tresore, auf die Sie über die Registerkarte MPA zugreifen können
4. Wählen Sie Tresorzugriff anfordern aus.
5. Geben Sie den ARN des Quell-Backup-Tresors des Tresors mit logischem Air-Gap ein, auf den Sie zugreifen möchten.
6. Geben Sie einen optionalen Namen für den Backup-Tresor mit Wiederherstellungszugriff ein. Wenn Sie keinen Namen eingeben, AWS Backup wird ein Name zugewiesen, der auf dem Namen des Tresors mit logischem Air-Gap basiert.
7. Geben Sie optional einen Kommentar des Anforderers ein, in dem der Grund für die Zugriffsanfrage erläutert wird.
8. Wählen Sie Anfrage senden aus, um die Zugriffsanfrage einzureichen.

Die Mitglieder des Genehmigungsteams, die dem Quelltresor zugeordnet sind, erhalten eine E-Mail-Benachrichtigung zur Genehmigung der Anfrage.

Sobald die Anfrage von der erforderlichen Anzahl („Schwellenwert“) von Teammitgliedern genehmigt wurde, wird der Backup-Tresor für den Wiederherstellungszugriff im Wiederherstellungskonto erstellt.

CLI

Verwendung des `create-restore-access-backup-vault`-CLI-Befehls:

```
aws backup create-restore-access-backup-vault \
--source-backup-vault-arn SOURCE_VAULT_ARN \
--backup-vault-name OPTIONAL_VAULT_NAME \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Die Mitglieder des MPA-Genehmigungsteams, die dem Quell-Tresor zugeordnet sind, erhalten eine Benachrichtigung zur Genehmigung der Anfrage. Sobald die Anfrage von der erforderlichen Anzahl („Schwellenwert“) von Teammitgliedern genehmigt wurde, wird der Backup-Tresor für den Wiederherstellungszugriff im Wiederherstellungskonto erstellt.

Sie können den Status des Tresors wie folgt überprüfen:

```
aws backup describe-backup-vault \
--backup-vault-name VAULT_NAME \
--region REGION
```

Trennen Sie das aus mehreren Parteien bestehende Genehmigungsteam vom Tresor mit logischem Air-Gapped

Anforderer: Administrator des Kontos, dem der Tresor mit logischem Air-Gap gehört.

[Sie können die Zuordnung eines Genehmigungsteams mit mehreren Parteien zu einem Tresor mit logischem Air-Gap trennen \(Schritt 7 in der Übersicht\).](#)

Console

Trennen Sie die Zuordnung des Genehmigungsteams zu einem Tresor mit logischem Air-Gap

1. [Öffnen Sie die Konsole unter /backup AWS Backup . https://console.aws.amazon.com](https://console.aws.amazon.com)
2. Navigieren Sie im linken Navigationsbereich zum Abschnitt Backup-Tresore.

3. Wählen Sie den Backup-Tresor mit logischem Air-Gap aus, von dem Sie die Verbindung zum Genehmigungsteam trennen möchten.
4. Wählen Sie auf der Seite mit den Tresordetails die Option Genehmigungsteam trennen aus.
5. Geben Sie optional einen Kommentar des Anforderers ein, in dem der Grund für die Trennung erläutert wird.
6. Wählen Sie Anfrage senden aus, um die Anfrage zur Trennung einzureichen.

Die aktuellen Mitglieder des Genehmigungsteams erhalten eine Benachrichtigung zur Genehmigung der Anfrage.

Nach der Genehmigung durch die erforderliche Anzahl von Teammitgliedern wird das Team vom Tresor getrennt.

CLI

Verwendung des `disassociate-backup-vault-mpa-approval-team`-CLI-Befehls:

```
aws backup disassociate-backup-vault-mpa-approval-team \
--backup-vault-name VAULT_NAME \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Die aktuellen Mitglieder des MPA-Genehmigungsteams erhalten eine Benachrichtigung zur Genehmigung des Antrags. Nach der Genehmigung durch die erforderliche Anzahl von Teammitgliedern wird das Team vom Tresor getrennt.

Widerrufen und Zugriff auf Backup-Tresor wiederherstellen

Anforderer: Administrator des Kontos, dem der Tresor mit logischem Air-Gap gehört.

Sie können den Zugriff auf einen Backup-Tresor mit Wiederherstellungszugriff vom Quelltresorkonto aus widerrufen.

Console

Den Zugriff auf den Backup-Tresor mit Wiederherstellung

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Navigieren Sie im linken Navigationsbereich zum Abschnitt Backup-Tresore.

3. Wählen Sie den Backup-Tresor mit logischem Air-Gap aus, für den Sie den Zugriff widerrufen möchten.
4. Scrollen Sie auf der Seite mit den Tresordetails nach unten zum Abschnitt Zugriff durch Genehmigung durch mehrere Parteien.
5. Suchen Sie den Backup-Tresor mit Wiederherstellungszugriff, den Sie widerrufen möchten, und wählen Sie dann Anfrage, um den Tresorzugriff zu entfernen.
6. Geben Sie optional einen Kommentar des Anforderers ein, in dem der Grund für den Widerruf erläutert wird.
7. Wählen Sie Anfrage senden aus, um die Widerrufs-anfrage einzureichen.

Die Mitglieder des Genehmigungsteams erhalten eine Benachrichtigung zur Genehmigung der Anfrage.

Nach der Genehmigung durch die erforderliche Anzahl von Teammitgliedern wird der Backup-Tresor mit Wiederherstellungszugriff aus dem Wiederherstellungskonto gelöscht

CLI

Führen Sie zunächst die Backup-Tresore mit Wiederherstellungszugriff auf, die Ihrem Quell-Tresor zugeordnet sind:

```
aws backup list-restore-access-backup-vaults \
--backup-vault-name SOURCE_VAULT_NAME \
--region REGION
```

Verwenden Sie dann den CLI-Befehl `revoke-restore-access-backup-vault`:

```
aws backup revoke-restore-access-backup-vault \
--backup-vault-name SOURCE_VAULT_NAME \
--restore-access-backup-vault-arn RESTORE_ACCESS_VAULT_ARN \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Die Mitglieder des Genehmigungsteams erhalten eine Benachrichtigung zur Genehmigung der Anfrage. Nach der Genehmigung durch die erforderliche Anzahl von Teammitgliedern wird der Backup-Tresor mit Wiederherstellungszugriff aus dem Wiederherstellungskonto gelöscht.

Aktualisieren Sie das Genehmigungsteam für mehrere Parteien, das einem Tresor mit logischem Air-Gap zugeordnet ist

Anforderer: Administrator des Kontos, dem der Tresor mit logischem Air-Gap gehört.

[Sie können das Genehmigungsteam für mehrere Parteien, das einem Tresor mit logischem Air-Gap zugeordnet ist, auf den neuesten Stand bringen \(Schritt 8 in der Übersicht\).](#)

Console

Aktualisieren Sie das Genehmigungsteam, das einem Tresor mit logischen Air-Gaps zugeordnet ist

1. [Öffnen Sie die AWS Backup Konsole unter /backup. <https://console.aws.amazon.com>](https://console.aws.amazon.com/backup)
2. Navigieren Sie im linken Navigationsbereich zum Abschnitt Backup-Tresore.
3. Wählen Sie den Backup-Tresor mit logischem Air-Gap aus, für den Sie das Genehmigungsteam aktualisieren möchten.
4. Wählen Sie auf der Seite mit den Tresordetails die Option Änderung des Genehmigungsteams beantragen aus.
5. Wählen Sie im Dropdownmenü das neue Genehmigungsteam aus, das Sie dem Tresor zuordnen möchten.
6. Geben Sie optional einen Kommentar des Anforderers ein, in dem der Grund für die Änderung erläutert wird.
7. Wählen Sie Anfrage senden aus, um die Änderungsanfrage einzureichen.

Die aktuellen Mitglieder des Genehmigungsteams erhalten eine E-Mail-Benachrichtigung zur Genehmigung der Anfrage.

Nach der Genehmigung durch die erforderliche Anzahl von Teammitgliedern (Schwellenwert) aus dem aktuellen MPA-Team wird das neue Team dem Tresor zugeordnet.

CLI

Verwenden Sie den CLI-Befehl `associate-backup-vault-mpa-approval-team` mit dem neuen Team-ARN:

```
aws backup associate-backup-vault-mpa-approval-team \  
--backup-vault-name VAULT_NAME \  
--team-arn TEAM_ARN
```

```
--mpa-approval-team-arn NEW_MPA_TEAM_ARN \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Die aktuellen Mitglieder des Genehmigungsteams erhalten eine Benachrichtigung zur Genehmigung der Anfrage. Sobald die erforderliche Anzahl von Teammitgliedern (Schwellenwert) aus dem aktuellen Team die Genehmigung erteilt hat, wird das neue MPA-Team dem Tresor zugeordnet.

Aufgaben des Genehmigers

Ein Benutzer, der Mitglied eines Genehmigungsteams mit mehreren Parteien ist, kann [Anfragen, die Teil einer Sitzung sind, genehmigen oder ablehnen](#). Zu den weiteren Aufgaben gehören:

- [Reagieren Sie auf angeforderte Operationen](#)
- [Sehen Sie sich ein Genehmigungsteam an](#)
- [Vorgangsverlauf anzeigen](#)

Richtlinien für den Tresorzugriff

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 Ressource ARNs](#) Ressourcenspezifische Wiederherstellungspunkte. ARNs

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

Unabhängig von der Zugriffsrichtlinie für den AWS Backup Tresor `backup:CopyIntoBackupVault` wird der kontoübergreifende Zugriff für alle Aktionen abgelehnt, AWS Backup d. h. alle anderen Anfragen von einem Konto, das sich von dem Konto der Ressource unterscheidet, auf die verwiesen wird, abgelehnt.

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.

Verweigern des Zugriffs auf einen Backup-Tresor

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

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 AWS-Managementkonsole <https://console.aws.amazon.com/backup> an und öffnen Sie die AWS Backup Konsole.
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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "backup:DeleteRecoveryPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:userId": [
            "AIDA1234567890EXAMPLE",
            "ARO1234567890EXAMPLE:my-role-session",
            "ARO1234567890EXAMPLE:*",
            "112233445566"
          ]
        }
      }
    }
  ]
}
```

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

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 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.](#)

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 ist und die Übergangszeit abgelaufen ist, kann die Tresorkonfiguration nicht von einem Kunden oder account/data Eigentümer geändert oder gelöscht werden, AWS solange sie Wiederherstellungspunkte enthält. 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 nach Ablauf der Bedenkzeit (" Grace Time „) nicht gelöscht werden, sofern sich irgendwelche Wiederherstellungspunkte im Tresor befinden. 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, was bedeutet, dass die Sperre nicht aufgehoben werden kann (der Tresor selbst kann gelöscht werden, wenn er leer ist und keine Wiederherstellungspunkte enthält).

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. Für eine Tresorsperre im Compliance-Modus gilt eine von Ihnen festgelegte Übergangszeit, bis sie gesperrt wird und der Inhalt und die Tresorsperre unveränderlich werden.

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-Managementkonsole 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 Sicherungs- und Kopieraufträge, die im Tresor erstellt werden, schlagen fehl, wenn sie nicht den von Ihnen festgelegten Aufbewahrungsfristen 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 Kulanzzzeit), sie muss jedoch mindestens 3 Tage (72 Stunden) betragen.

 Important

Sobald die Kulanzzzeit 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 [PutBackupVaultLockConfiguration](#), um AWS Backup Vault Lock zu konfigurieren. 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 an AWS Backup, dass die Tresorsperre im Compliance-Modus erstellt werden soll. 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 unter [DescribeBackupVault](#) oder überprüfen [ListBackupVaults](#) APIs.

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 Löscher 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 (der Zeit nach dem Sperren des Tresors, aber vor IhremLockDate) mithilfe der AWS Backup Konsole zu löschen,

1. Melden Sie sich bei der AWS-Managementkonsole 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 ein AWS-Konto schließen, das 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 [Ressourcen befinden sich in einem Backup-Plan mit AWS Backup Vault Lock](#) 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 Glacier Vault Lock](#), das nur mit Amazon Glacier kompatibel ist.

Erstellung, Wartung und Wiederherstellung von Backup

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 Recovery Point ARNs und Unique IDs finden Sie in der Tabelle unter [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 [Erfassung, Kosten und Abrechnung für AWS Backup](#).

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

Themen

- [Erstellen eines On-Demand-Backups mit AWS Backup](#)
- [Kontinuierliche Backups und point-in-time Wiederherstellung \(PITR\)](#)
- [Backup-Erstellung nach Ressourcentyp](#)
- [Kopie sichern und markieren](#)
- [Löschen von Backup](#)

- [Änderungen Backup und taggen](#)
- [Backup-Suche](#)
- [Backup-Tiering](#)
- [Stellen Sie ein Backup nach Ressourcentyp wieder her](#)
- [Testen wiederherstellen](#)
- [Beenden Sie einen Backup-Job](#)
- [Bestehende Backups anzeigen](#)

Erstellen eines On-Demand-Backups mit AWS Backup

Auf 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 Recovery (PITR) verwendet werden, da bei einem On-Demand-Backup die Ressourcen in dem Zustand erhalten bleiben, in dem sie sich zum Zeitpunkt der Sicherung befinden. PITR verwendet jedoch [kontinuierliche Backups](#), 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 EC2 Amazon-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 ausgeführt werden EC2, und bestimmte Instance-Typen werden nicht unterstützt. Weitere Informationen finden Sie unter [Erstellen Sie 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. Die Optionen für erweiterte Backup-Einstellungen variieren je nach Ressourcentyp:

- **EC2Ressourcen:** Um mithilfe des Windows Volume Shadow Copy Service (VSS) anwendungskonsistente Snapshots zu erstellen, wählen Sie Windows VSS.
 - **Für Amazon S3 S3-Ressourcen:** Sie können sich dafür entscheiden, Access Control Lists (ACLs) aus Ihrem Backup auszuschließen, indem Sie Backup-Zugriffskontrolllisten (ACLs) nicht ausgewählt lassen.
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)

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. PITR greift auf Ihr vollständiges Backup zu und spielt das Transaktionsprotokoll bis zu dem Zeitpunkt ab, zu dem Sie es wiederherstellen möchten. 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.

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.

Sie können [On-Demand-Backups](#) nicht mit PITR verwenden, da bei einem On-Demand-Backup die Ressourcen in dem Zustand erhalten bleiben, in dem sie sich zum Zeitpunkt der Sicherung befinden, während 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. Der Plan für kontinuierliches Backup erstellt einen kontinuierlichen Wiederherstellungspunkt und aktualisiert diesen bei jeder Ausführung des Jobs.

Inhalt

- [Point-in-time Überlegungen zur Wiederherstellung](#)
- [Unterstützte Dienste für kontinuierliches Backup und PITR](#)
- [Finden eines kontinuierlichen Backups](#)
- [Wiederherstellen eines kontinuierlichen Backups](#)
- [Anhalten oder Löschen kontinuierlicher Backups](#)
- [Kopieren kontinuierlicher Backups](#)
- [Ändern Ihrer Aufbewahrungsfrist](#)
- [Entfernen der einzigen Regel für kontinuierliche Backups aus einem Backup-Plan](#)

Point-in-time Überlegungen zur Wiederherstellung

Beachten Sie die folgenden Überlegungen zur point-in-time Wiederherstellung:

- 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.

 Important

Eine einzelne Ressource kann nur ein kontinuierliches Backup haben. Im Folgenden finden Sie weitere Informationen und bewährte Methoden.

Überlappende kontinuierliche Backups auf derselben Ressource

Jede Ressource (z. B. ein Amazon S3 S3-Bucket oder eine Amazon RDS-Datenbank) kann nur über ein kontinuierliches Backup (Wiederherstellungspunkt) verfügen. Zusätzliche kontinuierliche Backups sind überflüssig. Wenn mehrere Backup-Richtlinien, -Pläne oder Regeln die Erstellung AWS Backup mehrerer kontinuierlicher Backups für dieselbe Ressource vorschreiben, gilt der folgende Prozess:

- Wenn mehrere Regeln angeben, dass sich mehr als ein kontinuierliches Backup in einem einzigen Tresor befinden sollte, AWS Backup folgt die Regel mit der längsten Aufbewahrungsdauer (Lebenszyklus) und ignoriert zusätzliche Regeln.
- Wenn mehrere Regeln angeben, dass sich mehr als ein kontinuierliches Backup in mehr als einem Tresor befinden sollte, AWS Backup wird ein kontinuierliches Backup gemäß der zuerst verarbeiteten Regel erstellt. Jede nachfolgende Regel, die ein kontinuierliches Backup für eine Ressource spezifiziert, für die bereits ein kontinuierliches Backup vorhanden ist, führt stattdessen zu einem (periodischen) Snapshot-Backup.

Wenn doppelte kontinuierliche Backup-Pläne vorhanden sind, können die nach dem Continuous Recovery Point erstellten Snapshot-Backups den Status von `Completed with issues`. In den detaillierten Informationen zu diesem Wiederherstellungspunkt wird ein Fehler angezeigt, der dem ähnelt `Enabling continuous backup failed, because of the following error: PITR already configured in backup plan: [ARN]`. Dieser Fehler weist darauf hin, dass bereits mindestens ein kontinuierliches Backup konfiguriert ist (für einen anderen als den, auf dem der Fehler aufgetreten ist). Dieses erste kontinuierliche Backup (Recovery Point) kann für die Point-in-Time-Wiederherstellung (PITR) verwendet werden, sofern es den Status hat. `COMPLETED`

Um zu verhindern, dass unbeabsichtigte Snapshots mit Problemen (und Fehlermeldungen) erstellt werden, sollten Sie die Backup-Strategie Ihres Unternehmens überprüfen. Passen Sie bei Bedarf die Backup-Pläne und -Richtlinien an, sodass mehrere kontinuierliche Backups derselben Ressource erstellt werden.

Nachdem Sie Anpassungen vorgenommen haben, die zu nur einem kontinuierlichen Backup für eine Ressource führen, werden die Snapshot-Backups gemäß dem angegebenen Lebenszyklus

des Plans aufbewahrt, mit dem sie erstellt wurden. Anschließend werden sie in den Speicher übertragen EXPIRED und gelöscht. Das kontinuierliche Backup und seine point-in-time Wiederherstellungsfähigkeit werden gemäß der Regel beibehalten, mit der es erstellt wurde.

Unterstützte Dienste für kontinuierliches Backup und 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.

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](#).

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 einmal täglich Snapshots, auch wenn 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 der AWS Backup 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:DescribeDBInstanceAutomatedBackups` Sie auf, um den Zeitraum zu beschreiben, der für die point-in-time Wiederherstellung zur Verfügung steht. In der AWS Backup Konsole müssen Sie über die `rds:DescribeDBInstanceAutomatedBackups` API-Berechtigung verfügen, die in Ihrer AWS Identity and Access Management (IAM) verwalteten Richtlinie enthalten ist. 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, AWS Backup ruft [diese Änderung auf ModifyDBInstance und wendet](#) sie an, beginnend mit dem nächsten Backup, das gemäß der im Backup-Plan festgelegten Häufigkeitsregel durchgeführt wird.

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 EC2 Amazon-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, 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 Instanz wiederherstellen, indem Sie sie innerhalb von 1 Sekunde genau auf einen bestimmten Zeitpunkt zurückspulen (maximal 35 Tage). Bei kontinuierlichen Backups wird zunächst ein vollständiges Backup Ihrer Ressource erstellt und anschließend die Transaktionsprotokolle Ihrer Ressource kontinuierlich gesichert. Die PITR-Wiederherstellung funktioniert, indem Sie auf Ihr vollständiges Backup zugreifen und das Transaktionsprotokoll bis zu dem Zeitpunkt wiedergeben, zu dem Sie die Wiederherstellung angeben 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-Managementkonsole 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 entspricht. EXPIRED) 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 mithilfe 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 Sie können 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 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 `Always On` eingestellt ist, 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 eine Regel für kontinuierliches Backup auch eine konto- oder regionsübergreifende Kopie festlegt und den Vorgang für den Ressourcentyp AWS Backup unterstützt, AWS Backup wird ein Snapshot der Ressource erstellt und der Snapshot in den Zieltresor 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 Sicherungsplanregel für die Region des Zielkontos and/or 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. Die Änderung der Aufbewahrungsfrist wird wirksam, wenn das nächste Backup nach dieser Änderung abgeschlossen ist.

Aufbewahrungszeitraum nach Service

Das Aufbewahrungsverhalten kann für den Ressourcentyp spezifisch sein, der am Wiederherstellungspunkt gesichert wird.

Amazon S3

Wenn sich die Aufbewahrungsdauer eines kontinuierlichen Amazon S3 S3-Wiederherstellungspunkts geändert (verlängert oder verringert) hat, wird dieser Wiederherstellungspunktstatus geändert STOPPED. Ein neuer kontinuierlicher Wiederherstellungspunkt mit den geänderten Aufbewahrungseinstellungen wird erstellt.

Amazon Aurora und Amazon RDS

Für Wiederherstellungspunkte von Aurora- und Amazon RDS-Ressourcen ist jeweils nur ein Wiederherstellungspunkt möglich. Wenn ein Aufbewahrungszeitraum geändert wird, werden keine

neuen Wiederherstellungspunkte erstellt. Stattdessen wird der bestehende Wiederherstellungspunkt mit den Aufbewahrungsspezifikationen im Backup-Plan AWS Backup aktualisiert.

Stellen Sie sicher, dass Sie den Aufbewahrungszeitraum für diese Backups so einstellen, dass er höher als die Sicherungshäufigkeit ist, um ein Szenario zu vermeiden, in dem der Wiederherstellungspunkt in den EXPIRED Status übergeht.

Tip

Eine Regel zur Sicherungshäufigkeit für ein kontinuierliches Backup ist nicht dasselbe wie ein periodischer Backup-Snapshot. Jeder Backup-Plan, auch wenn er keinen Snapshot erstellt, hat eine Frequenz, die Sie für Wartungs- und Synchronisierungszwecke festlegen (z. B. stündlich, täglich, wöchentlich oder monatlich).

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.

Backup-Erstellung nach Ressourcentyp

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 [Backup-Pläne](#).

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-timeRestore \(PITR\)](#) 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. 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, PENDING, RUNNING, ABORTING, ABORTED, COMPLETED, FAILED, EXPIRED, und PARTIAL.

Inkrementelle Sicherungen

Viele Ressourcen unterstützen inkrementelle Backups mit AWS Backup. Eine vollständige Liste ist im Abschnitt inkrementelle Backups der [Feature-Verfügbarkeit nach Ressource](#) Tabelle verfügbar.

Obwohl jedes Backup nach dem ersten (vollständigen) Backup 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.

Inkrementelle Backups und Regionen

Backups von Ressourcen, die vollständig verwaltet werden, AWS Backup können nur inkrementell sein, wenn der Tresor, in dem das Backup erstellt wird, auch ein früheres Backup (inkrementell oder vollständig) enthält. Andere Ressourcentypen (nicht vollständig verwaltet von AWS Backup) können inkrementelle Backups haben, sofern ein Tresor in derselben Region über ein früheres Backup verfügt.

Zugriff auf Quellressourcen

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

- Um eine EC2 Amazon-Instance zu sichern, kann sich die Instance im `stopped` Status `running` oder, aber nicht im `terminated` Status befinden. Das liegt daran, dass eine `running` `stopped` Oder-Instance mit kommunizieren kann AWS Backup, eine `terminated` Instance 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 FSx Amazon-Dateisystem zu sichern, muss es den Status `AVAILABLE` haben. Wenn der Status `UPDATING` lautet, wird die Backup-Anfrage in die Warteschlange gestellt, bis das Dateisystem `AVAILABLE` anzeigt.

FSx denn ONTAP unterstützt nicht die Sicherung bestimmter Volumetypen, einschließlich DP-Volumes (Datenschutz), LS-Volumes (Load-Sharing), ganzer Volumes oder Volumes auf Dateisystemen, die voll sind. Weitere Informationen finden Sie unter [FSx ONTAP](#): Arbeiten mit Backups.

AWS Backup bewahrt zuvor erstellte Backups gemäß Ihrer Lebenszyklusrichtlinie auf, unabhängig vom Zustand Ihrer Quellressource.

Themen

- [CloudFormation Backups stapeln](#)

- [Amazon Aurora DSQL-Backups](#)
- [Erweitertes DynamoDB-Backup](#)
- [Amazon EBS und AWS Backup](#)
- [Backups von Amazon Relational Database Service](#)
- [Amazon-Redshift-Backups](#)
- [Serverlose Amazon Redshift Redshift-Backups](#)
- [Amazon-EKS-Backups](#)
- [SAP HANA-Backup auf Amazon EC2](#)
- [Amazon-S3-Backups](#)
- [Amazon-Timestream-Backups](#)
- [Backups virtueller Maschinen](#)
- [Erstellen Sie Windows VSS-Backups](#)

CloudFormation Backups stapeln

Ein CloudFormation Stack besteht aus mehreren zustandsbehafteten 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 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 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 [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).

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 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 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.

Amazon Aurora DSQL-Backups

Sie können AWS Backup verwenden, um Backups Ihrer Amazon Aurora DSQL-Cluster mit einer oder mehreren Regionen zu erstellen. Amazon Aurora DSQL-Cluster-Backups sind immer vollständige Backups.

Bei der Erstellung von Backup für Amazon Aurora DSQL-Cluster wird der standardmäßige Backup-Prozess verwendet. Weitere Informationen finden Sie hier:

- [Erstellen eines On-Demand-Backups mit AWS Backup](#)
- [Erstellen Sie einen Backup-Plan](#)

Um Backups Ihrer Amazon Aurora DSQL-Cluster AWS Backup zu erstellen, müssen Sie den Schutz für Aurora DSQL aktivieren. Weitere Informationen finden Sie unter [Opt-In für den Service](#).

Beachten Sie bei der Sicherung eines Clusters mit mehreren Regionen die folgenden Punkte:

- Für ein Cluster-Backup mit mehreren Regionen ist ein separates Backup für jede Region innerhalb des Clusters erforderlich. Ein Backup in einer Region erstellt keinen Wiederherstellungspunkt für alle Regionen in einem Cluster mit mehreren Regionen.
- Als bewährte Methode AWS Backup empfiehlt es sich, einen Erholungspunkt in einer Region zu erstellen und ihn in eine andere verwandte Region zu kopieren. Für die [Wiederherstellung mehrerer Regionen](#) benötigen Sie einen Erholungspunkt in einer unterstützten Region und eine

Kopie dieses Wiederherstellungspunkts in einer anderen Region innerhalb derselben regionalen Triplette.

Die folgenden unterstützten Triplets sind verfügbar. Wenn es mehr als Regionen gibt, wählen Sie drei in derselben Gruppierung aus.

- USA Ost (Nord-Virginia); USA Ost (Ohio); USA West (Nordkalifornien)
- Europa (Irland); Europa (London); Europa (Paris); Europa (Frankfurt)
- Asien-Pazifik (Tokio); Asien-Pazifik (Seoul); Asien-Pazifik (Osaka)

AWS Backup empfiehlt, dass Sie die Regel für Sicherungskopien zum Backup-Plan hinzufügen. Wenn Sie die Kopierregel nicht zum Backup-Plan hinzufügen, müssen Sie das Backup manuell in die Region kopieren, in der die Wiederherstellung durchgeführt werden soll. Dadurch verlängern sich Ihre RTO-Zeiten (Recovery Time Objective).

Hinweise zur Wiederherstellung eines Aurora DSQL-Wiederherstellungspunkts (Backup) finden Sie unter [Amazon Aurora DSQL Wiederherstellung](#).

Erweitertes DynamoDB-Backup

AWS Backup unterstützt zusätzliche, erweiterte Funktionen für Ihre Amazon DynamoDB DynamoDB-Datenschutzanforderungen.

Bei Kunden, die AWS Backup nach November 2021 mit der Nutzung begonnen haben, 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.

Für AWS Backup Bestandskunden ist es eine bewährte Methode, 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 potenziell Geld sparen, indem Sie Backups in einen Cold Storage verschieben und Ihre Kosten mithilfe von Tags zur Kostenzuweisung optimieren. Sie können auch damit beginnen, die Vorteile der AWS Backup regionsübergreifenden und kontoübergreifenden Kopier- und Sicherheitsfunktionen zu nutzen.

Themen

- [Vorteile von erweitertem DDB-Backup](#)
- [Überlegungen zum Advanced DynamoDB-Backup](#)
- [Aktivieren erweiterter DynamoDB-Backups über die Konsole](#)

- [Programmgesteuertes Aktivieren erweiterter DynamoDB-Backups](#)
- [Bearbeiten eines erweiterten DynamoDB-Backups](#)
- [Bearbeiten eines erweiterten DynamoDB-Backups](#)
- [Löschen eines erweiterten DynamoDB-Backups](#)
- [Weitere Vorteile der vollständigen AWS Backup -Verwaltung, wenn Sie das erweiterte DynamoDB-Backup aktivieren](#)

Vorteile von erweitertem DDB-Backup

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](#)
- Zusätzliche Kopieroptionen:
 - [Regionsübergreifende Kopie](#)
 - [Regionsübergreifende Kopie](#)
- Sicherheit:
 - Backups erben Tags aus ihren DynamoDB-Quellentabellen, sodass Sie diese Tags verwenden können, um Berechtigungen und [Dienststeuerungsrichtlinien](#) festzulegen (). SCPs

Überlegungen zum Advanced DynamoDB-Backup

Sie melden sich an

Backups, einschließlich solcher von Advanced DDB-Ressourcen, können im Rahmen eines Backup-Plans, eines On-Demand-Backups oder mithilfe einer Backup-Richtlinie erstellt werden. Bei Backups, die im Rahmen eines Plans oder auf Abruf erstellt wurden, wird Ihr Konto automatisch so konfiguriert, dass Backups von Advanced DDB-Ressourcen möglich sind.

[Wenn Ihr Backup-Job durch eine Backup-Richtlinie erstellt wird, müssen Sie sich manuell für Advanced DynamoDB-Backups anmelden, entweder über die Backup-Konsole oder über die CLI.](#)

Benutzerdefinierte Richtlinien und Rollen

Wenn Sie anstelle der AWS Backup Standarddienstrolle 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](#)

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.

So aktivieren Sie erweiterte DynamoDB-Backup-Funktionen von der AWS Backup Konsole aus:

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](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 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 unter [Eine Amazon DynamoDB-Tabelle wiederherstellen](#).

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 von Backup](#).

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`. [ARNs Weitere](#) Informationen finden Sie AWS Backup in der Service Authorization Reference.

Mit dieser Änderung können Sie oder Ihr Backup-Administrator mithilfe von `awsbackup`-Dienst-Namespaces Zugriffsrichtlinien für Backups erstellen, die jetzt für DynamoDB-Backups gelten, die nach der Aktivierung erweiterter Features erstellt wurden. Mithilfe des `awsbackup`-Dienst-

Namespaces 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 [Erfassung, Kosten und Abrechnung für AWS Backup](#).

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](#).

Absturzkonsistente Amazon-EBS-Backups mit Multi-Volume

AWS Backup Erstellt standardmäßig absturzsichere Backups von Amazon EBS-Volumes, die an eine Amazon-Instance angehängt sind. EC2 Absturzkonsistenz bedeutet, dass die Snapshots für jedes Amazon EBS-Volume, das an dieselbe EC2 Amazon-Instance angehängt ist, genau zum selben Zeitpunkt aufgenommen werden. Sie müssen Ihre Instances nicht mehr anhalten oder mehrere Amazon-EBS-Volumes koordinieren, um die Absturzkonsistenz Ihres Anwendungsstatus sicherzustellen.

Da es sich bei Snapshots mit mehreren Volumes um absturzsichere Snapshots handelt, müssen Sie nichts anderes tun, um diese AWS Backup Funktion zu verwenden.

Die Rolle, die zum Erstellen eines EBS-Snapshot-Wiederherstellungspunkts verwendet wird, ist 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 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](#).

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 und manuelle Backups zu erstellen](#). In der Amazon RDS-Terminologie werden alle Wiederherstellungspunkte, die von erstellt wurden AWS Backup, einschließlich der in einem Backup-Plan enthaltenen, als manuelle Backups betrachtet.

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 wird eine inkrementelle Snapshot-Kopie erstellt (copy-db-snapshotVorgang). Wenn kein Backup vorhanden ist, AWS Backup wird anstelle einer Kopie ein Snapshot der von Ihnen angegebenen Instanz erstellt (create-db-snapshotVorgang).

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.

Überlegungen

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

AWS Backup unterstützt keine Sicherung und Wiederherstellung von RDS auf Outposts.

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 erstellt 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.

Backup-Verhalten bei Instanzen und Clustern

- [Point-in-TimeRecovery](#) (PITR) kann Instanzen unterstützen, aber keine Cluster.
- Das Kopieren eines Multi-AZ-DB-Cluster-Snapshots wird nicht unterstützt.
- Der Amazon-Ressourcenname (ARN) für einen RDS-Wiederherstellungspunkt hängt davon ab, 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.

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 entscheiden Sie sich für den Schutz von Amazon Redshift Redshift-Clustern:

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 Redshift-Cluster hinzufügen möchten, oder die Kästchen neben den Clustern aktivieren, die Sie in Ihren Backup-Plan aufnehmen möchten.

programmgesteuert sichern.

Sie können Ihren Backup-Plan auch in einem JSON-Dokument definieren und ihn mithilfe der AWS Backup -Konsole oder der AWS CLI bereitstellen. 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

 Note

BackupSizeInBytesMetadaten werden für die folgenden Ressourcentypen unterstützt: Amazon EBS-Volumes, Amazon EFS-Dateisysteme, Amazon RDS-Datenbanken, DynamoDB-Tabellen, EC2 Amazon-Instances, FSx Amazon-Dateisysteme und Amazon S3-Buckets. Dieses Feld gibt die Größe des Backups in Byte an und ist über die API und die DescribeRecoveryPoint Konsole verfügbar. AWS Backup Bei nicht unterstützten Ressourcentypen wird dieses Feld nicht gefüllt.

- 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](#).

Serverlose Amazon Redshift Redshift-Backups

Übersicht

AWS Backup bietet eine vollständige Backupverwaltung Ihrer Amazon Redshift Serverless-Namespaces. Über AWS Backup können Sie manuelle Redshift Serverless-Snapshots über die Konsole oder über die CLI planen und wiederherstellen.

Redshift Serverless Data Protection AWS Backup bietet mehrere Optionen für die Sicherung und Wiederherstellung Ihrer Data Warehouses. Sie können einen geplanten Snapshot oder einen On-Demand-Snapshot Ihres Namespace erstellen. Anschließend können Sie wählen, ob Sie alle Datenbanken in diesem Snapshot in einem von Amazon Redshift bereitgestellten Cluster oder einem Serverless-Namespace wiederherstellen möchten. Alternativ können Sie eine einzelne Tabelle wiederherstellen.

Redshift Serverless bietet sowohl automatisierte als auch manuelle Snapshots. AWS Backup Kann derzeit für die Verwaltung manueller Snapshots verwendet werden, jedoch nicht für automatisierte.

Backup-Optionen für Redshift Serverless

Sie können die AWS Backup Konsole oder CLI verwenden, um Backups bei Bedarf oder als Teil eines Backup-Plans zu erstellen.

Erstellen Sie ein Backup auf Abruf

Mithilfe der folgenden Schritte können Sie On-Demand-Backups von Redshift Serverless-Namespace erstellen:

Console

1. Öffnen Sie die [AWS Backup -Konsole](#).
2. Wählen Sie im Dashboard die Option On-Demand-Backup erstellen aus.
3. Wählen Sie im Drop-down-Menü für den Ressourcentyp die Option Redshift Serverless aus.
4. Wählen Sie den Namespace aus, den Sie sichern möchten.
5. Stellen Sie sicher, dass die Option Backup jetzt erstellen ausgewählt ist.
6. Geben Sie den Aufbewahrungszeitraum für das Backup an.
7. Wählen Sie einen vorhandenen Sicherungstresor aus oder erzeugen Sie einen neuen.
8. Wählen Sie die IAM-Rolle aus, die für das Backup verwendet werden soll.
9. Fügen Sie dem Backup optional Tags hinzu. 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 Tag-Schlüssel und einen Tag-Wert ein.
10. Wählen Sie On-Demand-Backup erstellen aus, um den Backup-Job zu starten.
11. Sobald der Job initiiert wurde, zeigt die Konsole den Jobs-Bildschirm an, auf dem Sie eine Liste Ihrer Backup-Jobs und deren Status sehen können.

AWS CLI

Verwenden Sie den Befehl `start-backup-job`.

Erforderliche Parameter

- `BackupVaultName`
- `IamRoleArn`
- `ResourceArn`

Optionale Parameter

- `CompleteWindowMinutes`
- `IdempotencyToken`
- `Lifecycle`
- `StartWindowMinutes`

Example Beispiel

Das folgende Beispiel erstellt ein On-Demand-Backup eines Redshift Serverless-Namespace.

```
aws backup start-backup-job \  
  --backup-vault-name sample-vault \  
  --iam-role-arn arn:aws:iam::account:role/service-role/  
AWSBackupDefaultServiceRole \  
  --resource-arn arn:aws:redshift-serverless:region:account:namespace/namespace-  
name-UUID
```

Erstellen Sie geplante Redshift Serverless-Backups in einem Backup-Plan

Sie können einen neuen Backup-Plan für ihre Redshift Serverless-Namespace über die AWS Backup Konsole oder über die CLI erstellen, oder Sie können Redshift Serverless zu einem vorhandenen Backup-Plan hinzufügen.

Ihre geplanten Backups können Redshift Serverless-Namespace enthalten, wenn es sich um eine geschützte Ressource handelt. Gehen Sie wie folgt vor, um Redshift Serverless in der AWS Backup Konsole zu schützen:

Console

Gehen Sie wie folgt vor, um Redshift Serverless in der AWS Backup Konsole zu schützen:

1. Öffnen Sie die [AWS Backup -Konsole](#).
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Schalten Sie Amazon Redshift Serverless auf Ein.
4. Weitere Informationen finden [Wählen Sie die zu AWS sichernden Dienste aus](#) Sie unter Hinzufügen von Redshift Serverless Namespaces in einen bestehenden oder neuen Plan. Wenn Sie den Ressourcentyp Redshift Serverless hinzufügen, können Sie wählen, ob Sie Alle Amazon Redshift Redshift-Namespaces hinzufügen möchten, oder Sie können die Kästchen neben den Namespaces aktivieren, die Sie sichern möchten.

Unter Backup-Pläne verwalten können Sie:

- [Erstellen Sie einen Backup-Plan](#) und schließen Sie Redshift Serverless ein;
- [Aktualisieren Sie](#) einen bestehenden Backup-Plan mit Redshift Serverless.

AWS CLI

Hinweise [Erstellen Sie Backup-Pläne mit dem AWS CLI](#) zur Verwendung finden Sie unter. create-backup-plan

Wenn Sie einen bestehenden Plan so ändern möchten, dass er Ihre serverlosen Ressourcen einbezieht, verwenden Sie den Befehlupdate-backup-plan.

Der ARN (Amazon Resource Name) für serverlose Ressourcen, der in "BackupSelection,,: {„Resources“ aufgenommen werden soll, hat das folgende Format:

```
arn:aws:redshift-serverless:Region:account:snapshot/a12bc34d-567e-890f-123g-h4ijk56l78m9
```

Informationen [Serverlose Wiederherstellung mit Amazon Redshift](#) zum Wiederherstellen von Daten aus einem Snapshot in einem serverlosen Namespace finden Sie unter.

Amazon-EKS-Backups

Ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster besteht aus mehreren Ressourcen, die Sie als eine Einheit sichern können. Wenn Sie einen Amazon EKS-Cluster sichern, AWS Backup wird ein zusammengesetzter Wiederherstellungspunkt erstellt, der sowohl den EKS-Cluster-Status als auch persistente Volume-Backups umfasst.

Wenn ein Amazon EKS-Cluster gesichert wird, werden Wiederherstellungspunkte für den Amazon EKS-Clusterstatus und die persistenten Volumes erstellt, die von unterstützt werden AWS Backup. Diese Wiederherstellungspunkte sind innerhalb eines übergreifenden Wiederherstellungspunkts zusammengefasst, der als Verbundpunkt bezeichnet wird.

Ein Amazon EKS-Backup besteht aus zwei unterschiedlichen Komponenten:

- Amazon EKS-Clusterstatus: Dies ist eine Sicherungskopie des Amazon EKS-Clusterstatus. Was enthalten ist, finden Sie weiter unten in der Amazon EKS-Backup-Terminologie.
- Persistenter Speicher: Dies ist eine Sicherung des persistenten Speichers (Amazon EBS, Amazon S3, Amazon Elastic File System), der über Persistent Volume Claims an den Amazon EKS-Cluster angehängt und [vom EKS Add Ons CSI-Treiber unterstützt wird](#).

Amazon EKS-Backup-Terminologie

Die folgenden Begriffe werden in der gesamten Amazon EKS-Backup-Dokumentation verwendet. Die Amazon EKS-spezifische Terminologie finden Sie in der [Amazon EKS-Dokumentation](#).

EKS Backup-Terminologie

- Verbundwiederherstellungspunkt — Ein Wiederherstellungspunkt, der verwendet wird, um verschachtelte Wiederherstellungspunkte für ein Amazon EKS-Cluster-Backup zu gruppieren.
- Verschachtelter Erholungspunkt — Ein Erholungspunkt einer Ressource, die Teil eines Amazon EKS-Clusters ist und als Teil des zusammengesetzten Wiederherstellungspunkts gesichert wird.
- EKS-Clusterstatus — Die Kubernetes-Manifeste (YAML- oder JSON-Dateien), die den gewünschten Status der Kubernetes-Ressourcen in Ihrem Cluster definieren. Dazu gehören Kubernetes-Ressourcen und -Bereitstellungen wie: Secrets, Config-Maps, Stateful-Sets, Speicherklassen, Speicherzuordnungen DaemonSets, Replikatsätze, persistente Volume-Ansprüche, benutzerdefinierte Ressourcendefinitionen, Rollen und Rollenbindungen.
- Amazon EKS-Cluster-Konfiguration — Untergeordneter Wiederherstellungspunkt — Enthält den Amazon EKS-Clusterstatus.

- Persistent Volume Child Recovery Points — Enthält persistente Volume-Backups für unterstützte Speichertypen (EBS, S3, EFS), die [vom EKS Add Ons CSI-Treiber unterstützt werden](#).

Amazon EKS-Backup-Struktur

Amazon EKS-Backups umfassen die folgenden Komponenten:

- Status des Amazon EKS-Clusters
- Persistenter Speicher: Backups unterstützter Speichertypen wie Amazon EBS, Amazon EFS und Amazon S3

Amazon EKS Backups werden die folgenden Komponenten nicht enthalten:

- Container-Images aus externen Repositorys (ECR, Docker)
- EKS-Cluster-Infrastrukturkomponenten (z. B. VPCs Subnetze)
- Automatisch generierte EKS-Ressourcen wie Knoten, automatisch generierte Pods, Ereignisse, Leases und Jobs.

Einrichtung und Voraussetzungen für das EKS-Backup („Vor dem Backup“)

- EKS-Cluster-Einstellungen:
 - Der [EKS-Cluster-Autorisierungsmodus](#) ist auf API oder API_AND _CONFIG_MAP eingestellt, AWS Backup um [Zugriffseinträge für den Zugriff auf](#) den EKS-Cluster zu erstellen.
- Berechtigungen:
 - AWS Backup Die verwaltete Richtlinie [AWSBackupServiceRolePolicyForBackup](#) enthält die erforderlichen Berechtigungen zum Sichern Ihres Amazon EKS-Clusters und des persistenten EBS- und EFS-Speichers
 - Wenn Ihr EKS-Cluster einen S3-Bucket enthält, müssen Sie sicherstellen, dass die folgenden Richtlinien und Voraussetzungen für Ihren S3-Bucket wie dokumentiert hinzugefügt und aktiviert werden:
 - [AWSBackupServiceRolePolicyForS3 Backup](#)
 - [Voraussetzungen für S3-Backups](#)
- Verschlüsselung:
 - Untergeordnete Amazon EKS-Wiederherstellungspunkte werden mit dem Amazon KMS-Schlüsselsatz des Ziel-Backup-Tresors verschlüsselt

- Wiederherstellungspunkte für persistenten Speicher werden gemäß der aktuellen Unterstützung für jede Speicherklasse verschlüsselt: EBS-Snapshots, S3-Backups, EFS-Backups. [Weitere Informationen finden Sie unter Verschlüsselung für Backups AWS Backup](#)

Erstellen Sie ein Amazon EKS-Backup

Der Vorgang der Backup-Erstellung wird als Backup-Auftrag bezeichnet. Ein Amazon EKS-Cluster-Backup-Job hat einen Status. Wenn ein Backup-Job abgeschlossen ist, hat er den Status Abgeschlossen. Dies bedeutet, dass ein Wiederherstellungspunkt (ein Backup) erstellt wurde.

Erstellen eines Amazon EKS-Backups auf Abruf

Console

So erstellen Sie ein On-Demand-Backup Ihres Amazon EKS-Clusters:

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen aus.
3. Wählen Sie unter Ressourcentyp Amazon EKS aus.
4. Aktivieren Sie das Kontrollkästchen neben dem Amazon EKS-Cluster, den Sie sichern möchten.
5. Wählen Sie On-Demand-Backup erstellen.
6. Konfigurieren Sie Ihre Backup-Einstellungen, einschließlich Backup-Fenster, Umstellung auf Cold Storage und Aufbewahrungszeitraum.
7. Wählen Sie On-Demand-Backup erstellen.

AWS CLI

Um ein On-Demand-Backup Ihres Amazon EKS-Clusters zu erstellen, verwenden Sie AWS CLI:

Verwenden Sie den `start-backup-job`-Befehl:

```
aws backup start-backup-job \
                                --backup-vault-name my-backup-vault \
                                --resource-arn arn:aws:eks:us-
west-2:123456789012:cluster/my-cluster \
                                --iam-role-arn arn:aws:iam::123456789012:role/
service-role \
```



```
--region us-west-2
```

Geben Sie optional zusätzliche Parameter wie Lebenszykluseinstellungen an:

```
aws backup start-backup-job \  
                                --backup-vault-name my-backup-vault \  
                                --resource-arn arn:aws:eks:us-  
west-2:123456789012:cluster/my-cluster \  
                                --iam-role-arn arn:aws:iam::123456789012:role/  
service-role \  
                                --lifecycle  
MoveToColdStorageAfterDays=30,DeleteAfterDays=365 \  
                                --region us-west-2
```

Überwachen Sie den Status des Backup-Jobs:

```
aws backup describe-backup-job \  
                                --backup-job-id backup-job-id \  
                                --region us-west-2
```

ARN-Backup-Format von Amazon EKS

Composite-Wiederherstellungspunkt `arn ::backup: partition ::recovery-point:composite:eks/ - region accountId cluster-name timestamp`

Wiederherstellungspunkt für Kinder `arn ::backuppartition: ::recovery-point:eks/ - region accountId cluster-name timestamp`

Amazon EKS-Wiederherstellungspunkte

Status des Wiederherstellungspunkts

Wenn der Backup-Job eines Amazon EKS-Clusters abgeschlossen ist (der Job-Status lautet `Completed`), wurde ein Backup des Clusters erstellt. Dieses Backup wird auch als zusammengesetzter Wiederherstellungspunkt bezeichnet. Ein zusammengesetzter Wiederherstellungspunkt kann einen der folgenden Status haben: `Completed`, `Failed` oder `Partial`.

Jedes Amazon EKS-Backup erstellt einen übergeordneten Backup-Job für den Composite Recovery Point und untergeordnete Backup-Jobs für jeden untergeordneten Recovery Point (Cluster-Konfiguration und persistente Volumes).

- Ein abgeschlossener Backup-Job bedeutet, dass Ihr gesamter Amazon EKS-Cluster 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 Cluster gesichert wurden. Dies kann passieren, wenn einer oder mehrere der Backup-Jobs, die zu Ressourcen innerhalb des Clusters gehören (verschachtelte Ressourcen), einen anderen Status als `Completed` haben. Sie können manuell ein On-Demand-Backup erstellen, um alle Ressourcen erneut auszuführen, die zu einem anderen Status als `Completed` geführt haben.

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.

AWS Backup unterstützt Lebenszyklusübergänge zu Cold Storage für persistente Volume-Wiederherstellungspunkte. Sie können Benachrichtigungen abonnieren, um Benachrichtigungen zum Status von Backup-Jobs zu erhalten.

Verwalten von Wiederherstellungspunkten

Zusammengesetzte Wiederherstellungspunkte (Backups) können kopiert werden; untergeordnete Wiederherstellungspunkte für persistente Volumes können kopiert, gelöscht, getrennt oder wiederhergestellt werden. Der untergeordnete Amazon EKS-Cluster-Statuswiederherstellungspunkt kann nicht kopiert, gelöscht oder getrennt werden, da er eine 1:1-Beziehung zu seinem übergeordneten Verbundwiederherstellungspunkt unterhält.

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 Konsole oder mit dem AWS CLI löschen.

Gehen Sie wie folgt vor, um Wiederherstellungspunkte mit der Konsole zu löschen:

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

1. Klicken Sie in der linken Navigation auf Geschützte Ressourcen. Geben Sie in das Textfeld EKS ein, um nur Ihre Amazon EKS-Cluster anzuzeigen.
2. 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.
3. 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 mithilfe der API zu löschen.

Wenn Sie API mit dem verwenden, müssen AWS Command Line Interface Sie alle verschachtelten Wiederherstellungspunkte löschen, bevor Sie einen zusammengesetzten Punkt löschen.

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. Der untergeordnete Wiederherstellungspunkt des Amazon EKS-Cluster-Status kann nicht getrennt werden, da er eine 1:1-Beziehung zu seinem übergeordneten Verbundwiederherstellungspunkt unterhält.

Sie können die Zuordnung des Wiederherstellungspunkts mithilfe der Konsole aufheben oder die API aufrufen. `DisassociateRecoveryPointFromParent`

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, EKS um nur Ihre Amazon EKS-Cluster 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.

Amazon EKS-Backups unterstützen alle Kopiertypen:

- Gleiche Region/dasselbe Konto
- Kontoübergreifend
- Regionsübergreifend
- Opt-in-Regionen

Einschränkungen

- Persistente Volumes, die einen CSI-Treiber über die CSI-Migration, In-Tree-Storage-Plug-ins oder ACK-Controller verwenden, werden nicht unterstützt.
- Amazon S3 S3-Buckets mit bestimmten Präfixen, die an den CSI-Treiber angehängt sind, MountPoints können nicht gesichert werden. Es werden nur Amazon S3 S3-Buckets als Ziele unterstützt, keine spezifischen Präfixe

- Amazon S3 S3-Bucket-Backups als Teil eines EKS-Cluster-Backups unterstützen nur Snapshot-Backups.
- Amazon FSx via CSI-Treiber wird nicht über EKS Backups unterstützt
- Vorbehaltlich der [Sicherungs- und Wiederherstellungskontingente](#)

Häufig gestellte Fragen

1. „Was ist im Amazon EKS-Backup enthalten?“

Im Rahmen jeder Sicherung eines Amazon EKS-Clusters werden der Status des Amazon EKS-Clusters und die von AWS Backup unterstützten persistenten Volumes gesichert. Der Amazon EKS-Clusterstatus umfasst Details wie Clustername, IAM-Rolle, Amazon VPC-Konfiguration, Netzwerkeinstellungen, Protokollierung, Verschlüsselung, Add-Ons, Zugriffseinträge, verwaltete Knotengruppen, Fargate-Profilen, Pod-Identitätszuordnungen und Kubernetes-Manifestdateien.

2. „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 zwei Bedingungen, um zu überprüfen, ob Sie ein Backup-Ergebnis erwartet haben: *Completed*

- a. Einer oder mehrere der Backup-Jobs, die zu Ressourcen innerhalb des Clusters gehören, waren nicht erfolgreich und der Job muss erneut ausgeführt werden.
- b. Ein verschachtelter Wiederherstellungspunkt wurde gelöscht oder vom zusammengesetzten Wiederherstellungspunkt getrennt.

3. „Muss ich vor dem Backup einen Agenten oder ein Amazon EKS-Add-on auf meinem Amazon EKS-Cluster installiert haben?“

Nein. AWS Backup erfordert keine Installation von Agenten oder Add-Ons auf Ihrem Amazon EKS-Cluster. Die einzige Voraussetzung ist, dass der [Autorisierungsmodus](#) Ihres EKS-Clusters auf `API` oder `API_AND_CONFIG_MAP` gesetzt ist, um [Zugriffseinträge für den Zugriff auf](#) den EKS-Cluster AWS Backup zu erstellen.

4. „Umfasst Amazon EKS Backups Amazon EKS-Infrastrukturkomponenten oder Amazon ECR-Images?“

Nein. Amazon EKS-Backups konzentrieren sich auf den EKS-Cluster-Status und die Anwendungs-Workloads, nicht auf die zugrunde liegenden Infrastrukturkomponenten oder Container-Images.

5. „Kann ich meinen EKS Composite Recovery Point in einen Kühltpeicher umwandeln?“

Sie können für zugrunde liegende untergeordnete Wiederherstellungspunkte, die Cold Storage-Stufen unterstützen, auf Cold Storage umsteigen. Eine vollständige Liste der unterstützten [AWS Backup Funktionen finden Sie in der Matrix zur Verfügbarkeit](#) von Funktionen.

6. „Sind meine EKS-Backups inkrementell?“

AWS Backup erstellt inkrementelle Backups jedes untergeordneten Wiederherstellungspunkts, sofern dies derzeit unterstützt wird. Dazu gehören EBS-Volumes, EFS-Dateisysteme und S3-Buckets. Der untergeordnete Wiederherstellungspunkt für den EKS-Clusterstatus wird ein vollständiges Backup sein. Sehen Sie sich die [Matrix zur Verfügbarkeit von AWS Backup Funktionen](#) an.

7. „Kann ich einen Index erstellen und meine EKS-Backups durchsuchen?“

Nein. Sie können jedoch On-Demand-Indizes erstellen und persistente Volumes durchsuchen, sofern der zugrunde liegende Speichertyp diese Funktion unterstützt. AWS Backup Weitere Informationen finden Sie in der [Matrix zur Verfügbarkeit von AWS Backup Funktionen](#).

SAP HANA-Backup auf Amazon EC2

Note

[Unterstützte Dienste von AWS-Region](#) enthält die derzeit unterstützten Regionen, in denen SAP HANA-Datenbanksicherungen auf EC2 Amazon-Instances verfügbar sind.

AWS Backup unterstützt Backups und Wiederherstellungen von SAP HANA-Datenbanken auf EC2 Amazon-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](#)
- [Problembehandlung 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 Instanzen](#)

Überblick über SAP HANA-Datenbanken mit AWS Backup

Neben der Möglichkeit, Backups zu erstellen und Datenbanken wiederherzustellen, ermöglicht die AWS Backup Integration mit Amazon EC2 Systems Manager for SAP 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 EC2 Amazon-Instance ein, auf der die SAP HANA-Datenbank ausgeführt wird](#)
2. [Registrieren Sie Ihre Anmeldeinformationen 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 und die SSM-Einstellungen für SAP erfüllt 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 bei Amazon an EC2. .
5. Klicken Sie auf Bestätigen.

Das Service-Opt-In 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 auszuschließen IDs.

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 EC2 Amazon-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 [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 abgerufen wurden; PITR hingegen verwendet kontinuierliche Backups, bei denen Änderungen über einen bestimmten Zeitraum aufgezeichnet werden).

Mit kontinuierlichen Backups können Sie Ihre SAP HANA-Datenbank auf einer EC2 Instanz wiederherstellen, indem Sie sie innerhalb von 1 Sekunde genau auf einen bestimmten Zeitpunkt zurückspulen (maximal 35 Tage). Bei kontinuierlichen Backups wird zunächst ein vollständiges Backup Ihrer Ressource erstellt und anschließend die Transaktionsprotokolle Ihrer Ressource kontinuierlich gesichert. Die PITR-Wiederherstellung funktioniert, indem Sie auf Ihr vollständiges Backup zugreifen und das Transaktionsprotokoll bis zu dem Zeitpunkt wiedergeben, zu dem Sie die Wiederherstellung angeben 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-Managementkonsole 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 entspricht. EXPIRED) 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.

Um die zugehörigen Ressourcen programmgesteuert zu konfigurieren und zu verwalten AWS Backup , verwenden Sie den API-Aufruf, [StartBackupJob](#)um eine SAP HANA-Datenbank auf einer EC2 Instanz zu sichern.

Verwenden Sie `start-backup-job` als CLI-Befehl.

Problembehandlung 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 unterstützt SP5 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 `'/ 3'` zu erstellen. `usr/local/bin/` instead of directly using `'usr/bin/python` Dieser Befehl legt Python 3.4 als Standardversion fest. 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.

Erkennung und Registrierung von Amazon EC2 Systems Manager für SAP

- Fehler: SSM für SAP konnte die Arbeitslast aufgrund eines blockierten Zugriffs auf den öffentlichen Endpunkt 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 EC2 Amazon-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: 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.

- Fehler: Die SSM-Registrierung für SAP schlägt fehl, da das HANA-Passwort Sonderzeichen enthält. Zu den Fehlern können beispielsweise `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 mit `hdbsql` einer EC2 Amazon-Instance der HANA-Datenbank gehören `systemdb` und `tenantdb` 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 anzeigen `Miscellaneous: b'* 10: authentication failed SQLSTATE: 28000\n'`.

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, aufgrund des Kennworts mit Sonderzeichen fehlschlug. 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 von `AWS Systems Manager SAP-Discovery`.
5. Führen Sie im AWS CLI den Befehl aus `aws ssm-sap register-application status`. 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 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-Zugang zum öffentlichen Endpunkt.

- Fehler: `Database cannot be backed up while it is stopped`.

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.

AWS Backup Versionshinweise zur Unterstützung von SAP HANA-Datenbanken auf EC2 Instanzen

Bestimmte Features werden derzeit nicht unterstützt:

- Kontinuierliche Backups (die Transaktionsprotokolle verwenden) können nicht in andere Regionen oder Konten kopiert werden. Snapshot-Backups können aus vollständigen Backups in unterstützte Regionen und Konten kopiert werden.
- Backup Audit Manager und Reporting werden derzeit nicht unterstützt.
- [Unterstützte Dienste von AWS-Region](#) enthält die derzeit unterstützten Regionen für SAP HANA-Datenbank-Backups auf EC2 Amazon-Instances.

Amazon-S3-Backups

Übersicht

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.

Backup-Tiering

Amazon S3 ist die einzige Ressource, die Backup-Tiering auf eine kostengünstigere Warm-Storage-Stufe unterstützt. Weitere Informationen finden Sie unter [Backup-Tiering](#).

Voraussetzungen für S3-Backups

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 [AWSBackupServiceRolePolicyForS3Backup](#) und [AWSBackupServiceRolePolicyForS3Restore](#) zu den Rollen hinzu, die Sie zum Sichern und Wiederherstellen von S3-Buckets verwenden möchten.

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.

Backups und Versionierung

Sie müssen die [S3-Versionierung in Ihrem S3-Bucket aktivieren](#), um sie AWS Backup für Amazon S3 verwenden zu können.

Wir empfehlen Ihnen, [einen Ablaufzeitraum für den Lebenszyklus Ihrer S3-Versionen festzulegen](#).

Alle Objekte (einschließlich aller Versionen), die sich zu Beginn der Sicherung im Bucket befinden, werden am Wiederherstellungspunkt gespeichert (abgeschlossenes Backup). Dazu können die aktuelle Version jedes Objekts, ältere Versionen, Löschmarkierungen und Objekte gehören, für die Lebenszyklusaktionen noch ausstehen.

Die Speicherkosten werden für alle Objekte im Backup berechnet, einschließlich der Objekte, deren Löschung geplant ist (Objekte, die ablaufen). Sie können CLI oder Skripts verwenden, um die Aufnahme von Objekten zu entfernen, deren Ablauf geplant ist.

Um mehr über die Einrichtung von S3-Lebenszyklusrichtlinien zu erfahren, folgen Sie den Anweisungen [auf dieser Seite](#).

Überlegungen zu Amazon S3 S3-Backups

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.
- AWS Backup Wendet beim Wiederherstellen eines S3-Objekts einen Prüfsummenwert an, auch wenn das ursprüngliche Objekt die Prüfsummenfunktion nicht verwendet hat.

- 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.

- Umstellung auf Cold Storage — Verwenden Sie die AWS Backup Lifecycle-Management-Richtlinie, um den Zeitplan für den Ablauf von Backups festzulegen. Die Umstellung von S3-Backups auf kalte Speichersysteme wird 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 keine Unterstützung für Backups von [SSE-C-encrypted](#) Objekten. AWS Backup unterstützt auch keine Backups von Bucket-Konfigurationen, einschließlich Bucket-Richtlinien, Einstellungen, Namen oder Zugriffspunkten.
- AWS Backup unterstützt keine Backups von S3 on AWS Outposts.
- CloudTrail Protokollierung — Wenn Sie Ereignisse beim Lesen von Daten protokollieren, müssen die CloudTrail Protokolle an einen anderen Ziel-Bucket gesendet werden. Wenn Sie CloudTrail Logs in dem Bucket speichern, den sie protokollieren, entsteht eine Endlosschleife, die zu unerwarteten Gebühren führen kann.

Weitere Informationen finden Sie unter [Datenereignisse](#) im Benutzerhandbuch für CloudTrail .

- Serverzugriffsprotokollierung — Wenn Sie die Serverzugriffsprotokollierung aktivieren, müssen Sie dafür sorgen, dass die Protokolle an einen anderen Ziel-Bucket gesendet werden. Wenn Sie diese Protokolle in dem Bucket speichern, den sie protokollieren, entsteht eine Endlosschleife. Weitere Informationen finden Sie unter [Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung](#).

Unterstützte Bucket-Typen und -Mengen

AWS Backup unterstützt die Sicherung und Wiederherstellung von S3-Buckets für allgemeine Zwecke. Verzeichnis-Buckets werden derzeit nicht unterstützt.

Die Obergrenze der in einem AWS Konto zulässigen Ressourcenmenge (ein sogenanntes Kontingent), z. B. ein Bucket, hängt vom Dienst ab. [Amazon S3 S3-Kontingente](#) unterscheiden sich von [AWS Backup Kontingenten](#).

In jedem AWS Konto können Sie standardmäßig Backups für bis zu 100 Buckets erstellen. Sie können eine Erhöhung des Kontingents auf bis zu 1.000 Buckets beantragen.

Für Konten mit mehr als 1.000 Buckets gelten Kontingentbeschränkungen. Wenn Anfragen das Kontingent überschreiten, kann dies zu fehlgeschlagenen Aufträgen führen. Es hat sich bewährt, ein Konto auf 1.000 Buckets zu beschränken.

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 — Infrequent Access (IA) und S3 One Zone-IA, fallen unter die S3-Speichergebühr „Häufiger Zugriff“ (gilt für die Tarife „Infrequent Access“ oder „Archive Instant Access“).

Die archivierten Speicherklassen S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive werden nicht unterstützt.

Weitere Informationen zu den Speicherpreisen für Amazon S3 finden Sie unter [Amazon S3 S3-Preise](#).

S3-Backup-Typen

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.

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](#).

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

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 den Aufbewahrungszeitraum 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.
- Für Sicherungspläne, die Sie über CLI erstellen, sind die erweiterten Backup-Einstellungen für Amazon S3 (einschließlich der Option, Tags und ACLs in das Backup aufzunehmen) standardmäßig aktiviert. Sie können diese in den Backup-Optionen ausschließen. Ein Beispiel [Erweiterte Amazon S3 S3-Backup-Einstellungen](#) für die Syntax finden Sie unter.

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

- AWS Backup scannt den gesamten S3-Bucket, ruft die ACL und die 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 periodic/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 Erholungspunkt 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.
- Wenn erweiterte Amazon S3 S3-Backup-Einstellungen, wie z. B. das Einbeziehen von Tags und ACLs in einem Backup, für einen continuous Recovery Point geändert werden, AWS Backup stoppt dieser Recovery Point und erstellt einen neuen mit den aktualisierten Einstellungen.

Wenn ein kontinuierlicher Backup-Job für einen S3-Bucket ausgeführt wird, können Sie dennoch regelmäßige (Snapshot-) Backup-Jobs initiieren. Es gilt jedoch das folgende Verhalten:

- Snapshot-Backup-Jobs verwenden dieselben Backup-Optionen (ACLs und Objekt-Tag-Einstellungen) wie die bestehende kontinuierliche Sicherung.
- Wenn Sie für einen Snapshot-Job andere Backup-Optionen als für das kontinuierliche Backup angeben, verwendet der Snapshot-Job trotzdem die Einstellungen des kontinuierlichen Backups und wird mit dem Status „Mit Problemen abgeschlossen“ abgeschlossen abgeschlossen.

In diesem Fall wird Ihnen die folgende Statusmeldung angezeigt: "Periodic/snapshot backup for bucket <bucket name> has different backup options than the continuous backup. When using continuous backups along with snapshot backups for the same bucket, the snapshot will use the same settings for backing up ACLs and Object tags as the continuous backup."

Die folgende Tabelle zeigt, wann ein vollständiger Scan erforderlich ist, wenn ein Wechsel BackupOptions zu bestehenden kontinuierlichen Wiederherstellungspunkten erforderlich ist:

Verhalten bei vollständigem Scan, BackupOptions wenn geändert

Bisherige BackupOptions	Neu BackupOptions	Vollständiger Scan
gesichert ACLs und backupObjectTags aktiviert	gesichert ACLs und backupObjectTags deaktiviert	Nein
gesichert ACLs und backupObjectTags aktiviert	Backup ACLs aktiviert; backupObjectTags deaktiviert	Nein

Bisherige BackupOptions	Neu BackupOptions	Vollständiger Scan
gesichert ACLs und backupObjectTags aktiviert	Backup ACLs deaktiviert; backupObjectTags aktiviert	Nein
gesichert ACLs und backupObjectTags deaktiviert	gesichert ACLs und backupObjectTags aktiviert	Ja
Backup ACLs aktiviert; backupObjectTags deaktiviert	gesichert ACLs und backupObjectTags aktiviert	Ja
Backup ACLs deaktiviert; backupObjectTags aktiviert	gesichert ACLs und backupObjectTags aktiviert	Ja

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

Bewährte Methoden und Kostenüberlegungen für S3-Backups

Bewährte Methoden für große Buckets

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.

Optimierung der Backup-Strategie

- 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 Löschrage 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.

Objekt-Lebenszyklus und Markierungen zum Löschen

- 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.

Überlegungen zu den Kosten der Speicherklasse

- 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 Optimierung der Servicekosten

- Die Nutzung der Funktionen von AWS KMS, CloudTrail CloudWatch, Amazon und Amazon GuardDuty als Teil Ihrer Backup-Strategie kann 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 the Console \(einfache Event-Selektoren\)](#) 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.
- [Schätzung der GuardDuty Nutzungskosten](#) im GuardDuty Amazon-Benutzerhandbuch.

S3-Backup-Nachrichten

Wenn ein Backup-Job abgeschlossen ist oder fehlschlägt, wird möglicherweise die folgende Meldung angezeigt. Anhand der folgenden Tabelle können Sie die mögliche Ursache für die Statusmeldung ermitteln.

Szenario	Aufgabenstatus	Fehlermeldung	Beispiel
Alle Objekte konnten nicht für einen Snapshot oder ein erstes kontinuierliches Backup gesichert werden	FAILED	„Es wurden keine Objekte aus dem Quell-Bucket gesichert <i>BucketName</i> . Um über diese Fehler informiert zu werden, aktivieren Sie SNS-Ereignisbenachrichtigungen.“	Die Backup-Rolle hat nicht die Berechtigung, die ACL für die Objektversion abzurufen. Folglich wird keines der Objekte gesichert.

Szenario	Aufgabenstatus	Fehlermeldung	Beispiel
Alle Objekte konnten nicht für eine nachfolgende kontinuierliche Sicherung gesichert werden.	COMPLETED	„Es wurden keine Objekte aus dem Quell-Bucket gesichert <i>BucketName</i> . Um über diese Fehler informiert zu werden, aktivieren Sie SNS-Ereignisbenachrichtigungen.“	

Erweiterte Amazon S3 S3-Backup-Einstellungen

AWS Backup bietet erweiterte Einstellungen, mit denen Sie steuern können, welche Metadaten in Ihren Amazon S3 S3-Backups enthalten sind. Sie können optional Zugriffskontrolllisten (ACLs) und Objekt-Tags ausschließen. Dies kann hilfreich sein, wenn Ihre Objekte ohne ACLs Objekt-Tags eingerichtet sind. Mit anderen Worten, wenn Sie keine Objekt-Tags für Ihre S3-Ressourcen verwenden ACLs , kann es für Sie von Vorteil sein, sie aus Ihren Backups auszuschließen.

Konfiguration von Backups ACLs und Objekt-Tags

Sie können die Backup-Optionen für ACL und Objekt-Tags entweder über die AWS Backup Konsole oder über die konfigurieren AWS CLI.

Console

Konfigurieren Sie die ACL- und Tag-Optionen mithilfe der Konsole

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup/>.
2. Wählen Sie im Navigationsbereich Backup-Pläne und anschließend Backup-Plan erstellen aus.
3. Erweitern Sie in den Einstellungen Ihres Backupplans die Option Erweiterte Backup-Einstellungen.
4. Konfigurieren Sie für Amazon S3 S3-Ressourcen die folgenden Optionen:
 - Sichern ACLs: Aktivieren Sie das Kontrollkästchen, um sie einzubeziehen, ACLs oder lassen Sie es deaktiviert, um sie auszuschließen.

Objekt-Tags sichern: Aktivieren Sie das Kontrollkästchen, um Objekt-Tags in Ihr Backup aufzunehmen.

5. Vervollständigen Sie die Konfiguration des Backup-Plans und wählen Sie Plan erstellen.

AWS CLI

Mit den folgenden Backup-Optionen können Sie wahlweise Zugriffskontrolllisten (ACLs) und Objekt-Tags in Ihre Amazon S3 S3-Backups aufnehmen oder ausschließen:

Backup ACLs

Steuert, ob Objekte in der Sicherung enthalten ACLs sind. Auf „disabledAusschließen“ setzen ACLs. Standard: enabled

BackupObjectTags

Steuert, ob Objekt-Tags in der Sicherung enthalten sind. Auf einstellendisabled, um Tags auszuschließen. Standard: enabled

Konfigurieren Sie ACL- und Tag-Optionen mit dem AWS CLI

Verwenden Sie den `update-backup-plan` Befehl mit erweiterten Backup-Einstellungen AWS CLI, um die ACL- und Objekt-Tag-Backup-Optionen mit dem zu konfigurieren:

```
aws backup update-backup-plan \
  --backup-plan-id "your-backup-plan-id" \
  --backup-plan '{
    "BackupPlanName": "MyS3BackupPlan",
    "Rules": [{
      "RuleName": "MyS3BackupRule",
      "TargetBackupVaultName": "MyBackupVault",
      "ScheduleExpression": "cron(0 2 ? * * *)",
      "Lifecycle": {
        "DeleteAfterDays": 30
      },
      "RecoveryPointTags": {},
      "CopyActions": [],
      "EnableContinuousBackup": false
    }],
    "AdvancedBackupSettings": [{
```

```
    "ResourceType": "S3",
    "BackupOptions": {
        "BackupACLs": "disabled",
        "BackupObjectTags": "disabled"
    }
  }
}
```

Die BackupOptions Parameter steuern die Aufnahme von Metadaten:

- "BackupACLs": "disabled"- Aus Backups ACLs ausgeschlossen
- "BackupObjectTags": "disabled"- Schließt Objekt-Tags aus Backups aus
- "BackupACLs": "enabled"- ACLs In Backups enthalten (Standard)
- "BackupObjectTags": "enabled"- Schließt Objekt-Tags in Backups ein (Standard)

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 EC2 Amazon-Instance oder ein Temperaturmesswert. AWS Backup kann Timestream-Tabellen zentral sichern und wiederherstellen. Sie können diese Tabellen-Backups 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 Kühltagerung 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.

Nachdem 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](#)

Backups virtueller Maschinen

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

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 [Feature-Verfügbarkeit nach Ressource](#)-Tabelle.

[Sie können es verwenden AWS Backup , um Ihre virtuellen Maschinen auf Cloud™ on VMware zu schützen. AWS Outposts](#) AWS Backup speichert Ihre VM-Backups in AWS-Region dem Ordner, mit dem Ihre VMware Cloud™ on verbunden AWS Outposts ist. Sie können AWS Backup es verwenden, um Ihre VMware Cloud™ on zu schützen, AWS Backup VMs wenn Sie VMware Cloud™ on 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 AWS Outposts verbunden sind.

Unterstützt 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 der Quelle zur lokalen Umgebung VMs AWS VMware
- Hot-Add-Modus zum Schutz in der Cloud on VMs VMware AWS

Derzeit nicht unterstützt:

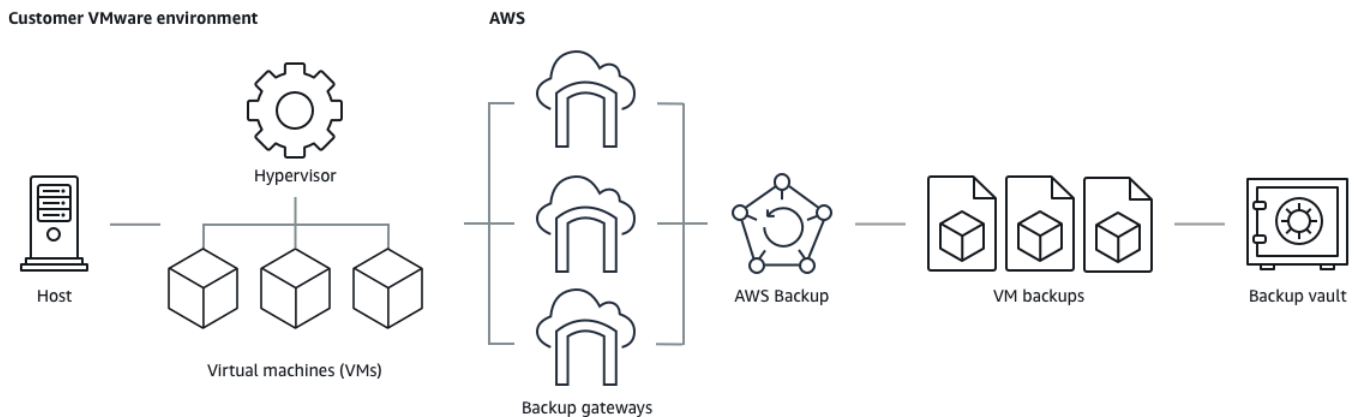
- RDM-Laufwerke oder NVMe Controller (Raw Disk Mapping) und ihre Festplatten
- Modi für unabhängige persistente und unabhängige, nicht persistente Festplatten

Backup-Konsistenz

AWS Backup, erfasst standardmäßig anwendungskonsistente Backups, wenn die Ruhezustandseinstellung der Tools auf der VM VMs verwendet wird. VMware Ihre Backups sind anwendungskonsistent, wenn Ihre Anwendungen mit Tools kompatibel sind. VMware Wenn die Ruhefunktion nicht verfügbar ist, werden absturzsichere AWS Backup Backups erfasst. 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 eine Verbindung herzustellen AWS Backup. VMware VMs Das Gateway stellt eine Verbindung zu Ihrem VM-Managementserver her VMs, um Ihre Daten zu ermitteln VMs, zu erkennen, zu verschlüsseln und effizient zu übertragen. AWS Backup Das folgende Diagramm zeigt, wie das Backup-Gateway eine Verbindung zu Ihrem herstellt VMs:



Folgen Sie dem Verfahren für [Arbeiten mit Gateways](#), um die Backup-Gateway-Software herunterzuladen.

Laden Sie die VM-Software herunter

Das Backup-Gateway wird als OVF-Vorlage (Open Virtualization Format) verteilt, die Sie in Ihrer VMware Infrastruktur bereitstellen. Die Gateway-Software stellt eine Verbindung her VMs, AWS Backup indem sie Daten erkennt, verschlüsselt und effizient überträgt. VMware VMs AWS Backup

Verwenden Sie die AWS Backup Konsole, um die OVF-Vorlage abzurufen:

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 unter Externe Ressourcen die Option Gateways aus.
3. Wählen Sie Create gateway (Gateway erstellen).
4. Laden Sie im Abschnitt Gateway einrichten die OVF-Vorlage herunter und stellen Sie sie in Ihrer VMware Umgebung bereit.

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.

Netzwerkconfiguration

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: Ermöglicht die Kommunikation des Backup-Gateways mit AWS.

2. TCP 80 Inbound

- Quelle: Der Host, mit dem Sie eine Verbindung herstellen AWS-Managementkonsole
- 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-Managementkonsole, 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: Support
- Verwendung: Ermöglicht 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: Ermöglicht dem Backup-Gateway die Kommunikation mit VMware vCenter.

7. TCP 443 Outbound

- Quelle: Backup-Gateway
- Ziel: Hosts ESXi
- Verwendung: Ermöglicht 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 zur Konfiguration von Amazon [VPC-Endpunkten für finden Sie unter VPC-Endpoint erstellen](#). 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.

Endpunkttypen

Standardendpunkte: Support Sie den IPv4 Verkehr zwischen Ihrer Gateway-Appliance und AWS.

Die folgenden Dienstendpunkte werden von allen Gateways für Steuerpfad- (anon-cpclient-cp,proxy-app) und Datenpfadoperationen (dp-1) benötigt.

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

Dual-Stack-Endpunkte: Support IPv4 sowohl den IPv6 Datenverkehr zwischen Ihrer Gateway-Appliance als auch. AWS

Die folgenden Dual-Stack-Dienstendpunkte werden von allen Gateways für den Betrieb von Steuerpfaden (Aktivierung, Steuerungsebene, Proxy) und Datenpfad (Datenebene) benötigt.

```
activation-backup-gateway.region.api.aws:443  
controlplane-backup-gateway.region.api.aws:443  
proxy-backup-gateway.region.api.aws:443  
dataplane-backup-gateway.region.api.aws:443
```

Konfigurieren Sie Ihr Gateway für mehrere Eingänge NICs VMware

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

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 das Kontextmenü (mit einem Rechtsklick) für Ihre virtuelle Gateway-Maschine und wählen Sie Einstellungen bearbeiten aus.
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 der 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 Verwaltungskonsole, 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

- Konfigurieren Sie statisch IPs für jede neue Netzwerkkarte
- 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 unter [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.

VMware Berechtigungen

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

Um das Backup-Gateway mit VMware eingeschalteter VMware Cloud™ AWS oder 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 VMware lokalen virtuellen 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

Netzwerk

- Zuweisen eines Netzwerks

dvPort-Gruppe

- Create
- Delete

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

- 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

Sie können ein Backup-Gateway auf zwei Arten erstellen:

- Konsolenmethode (Standard): Erstellt IPv4 ausschließlich Gateways über die AWS Backup Konsole mit automatischer Aktivierung
- Manuelle Methode: Unterstützt IPv4 sowohl das Abrufen IPv6 von Aktivierungsschlüsseln als auch das Verwenden von Befehlen AWS CLI

Bei beiden Methoden muss zuerst die OVF-Vorlage heruntergeladen und bereitgestellt werden (siehe [Laden Sie die VM-Software herunter](#)).

Konsolenmethode (IPv4 nur)

Verwenden Sie diese Methode für die Erstellung eines IPv4 Standard-Gateways über die AWS Backup Konsole mit automatischer Aktivierung.

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.

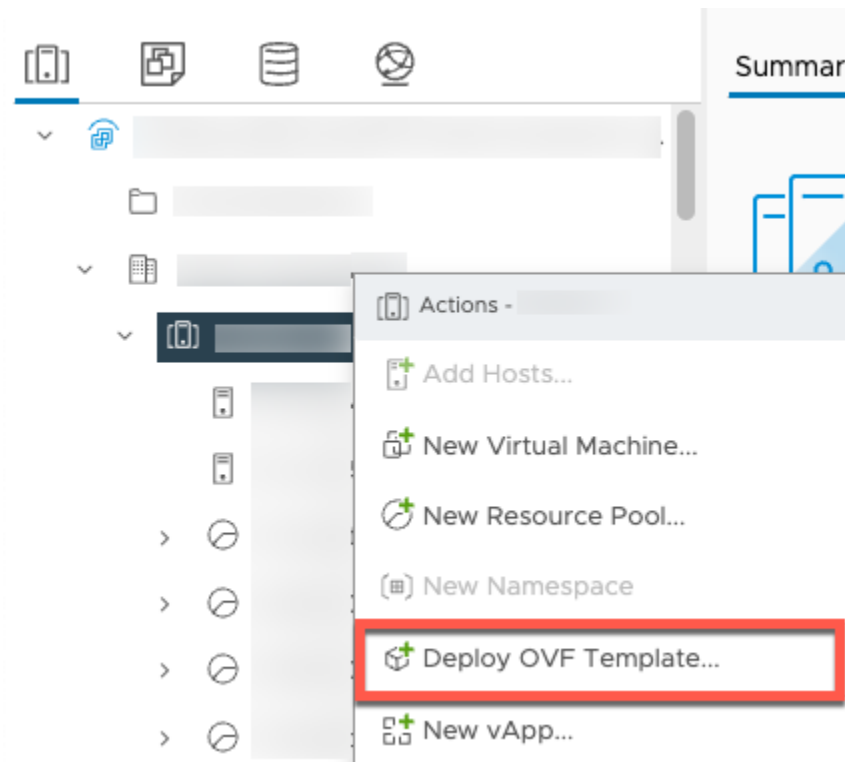
Software wird heruntergeladen VMware

Verbinden des Hypervisors

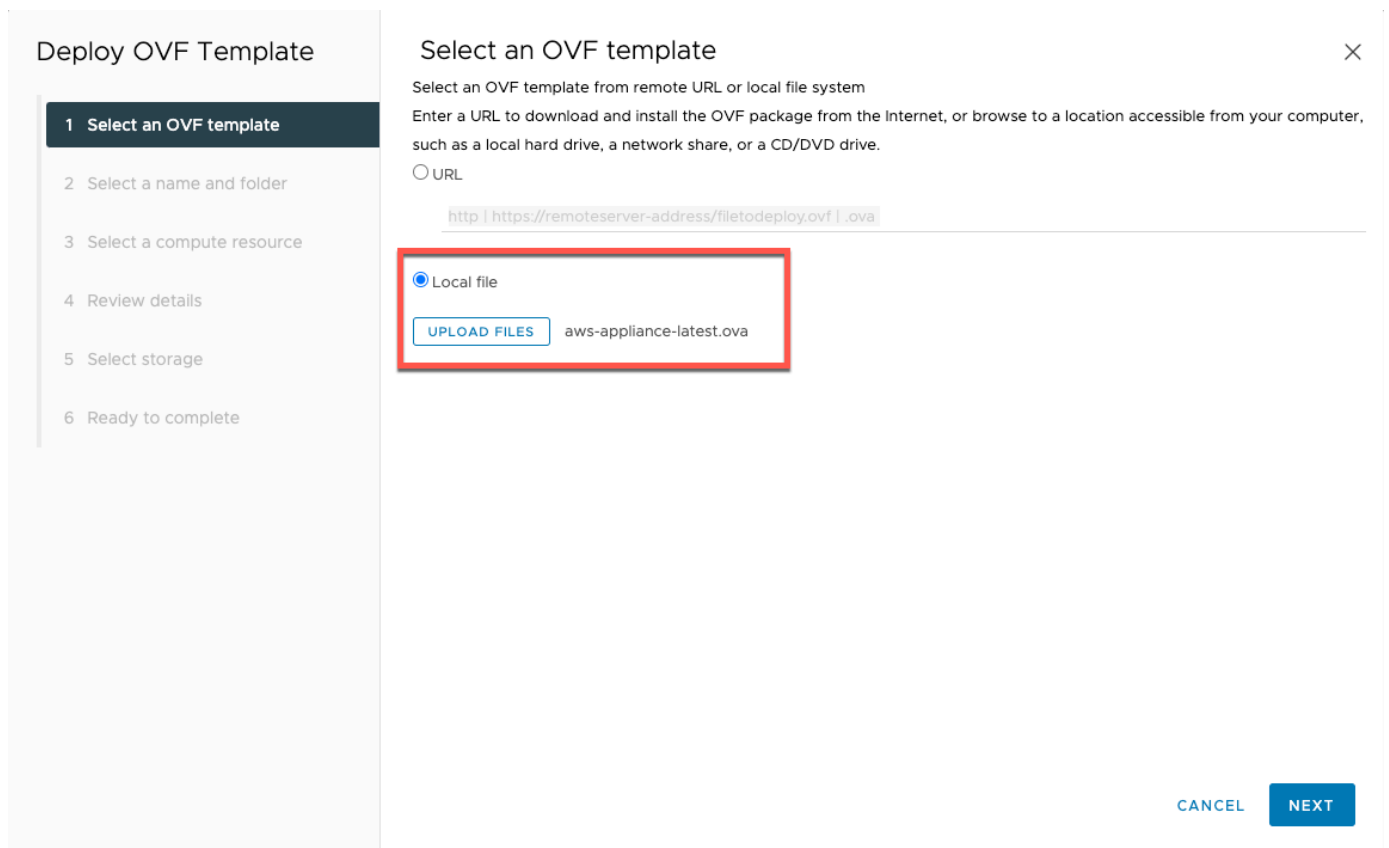
Gateways stellen eine Verbindung AWS Backup zu Ihrem Hypervisor her, sodass Sie Backups Ihrer virtuellen Maschinen erstellen und speichern können. Laden Sie die [OVF-Vorlage](#) herunter VMware ESXi, um Ihr Gateway einzurichten. Der Download kann ca. 10 Minuten dauern.

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

1. Stellen Sie mithilfe von VMware vSphere eine Connect zu Ihrem virtuellen Maschinen-Hypervisor 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.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage

Select the storage for the configuration and disk files

Select virtual disk format

✓ Thick Provision Lazy Zeroed

Thin Provision

Thick Provision Eager Zeroed

VM Storage Policy

☐ Disable Storage DRS for this storage

Default

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Placement
☐	vsanDatastore	--	20.74 TB	8.72 TB	13.37 TB	vSAN	Local
☐	WorkloadDatasto...	--	20.74 TB	67.44 TB	13.37 TB	vSAN	Local

2 Items

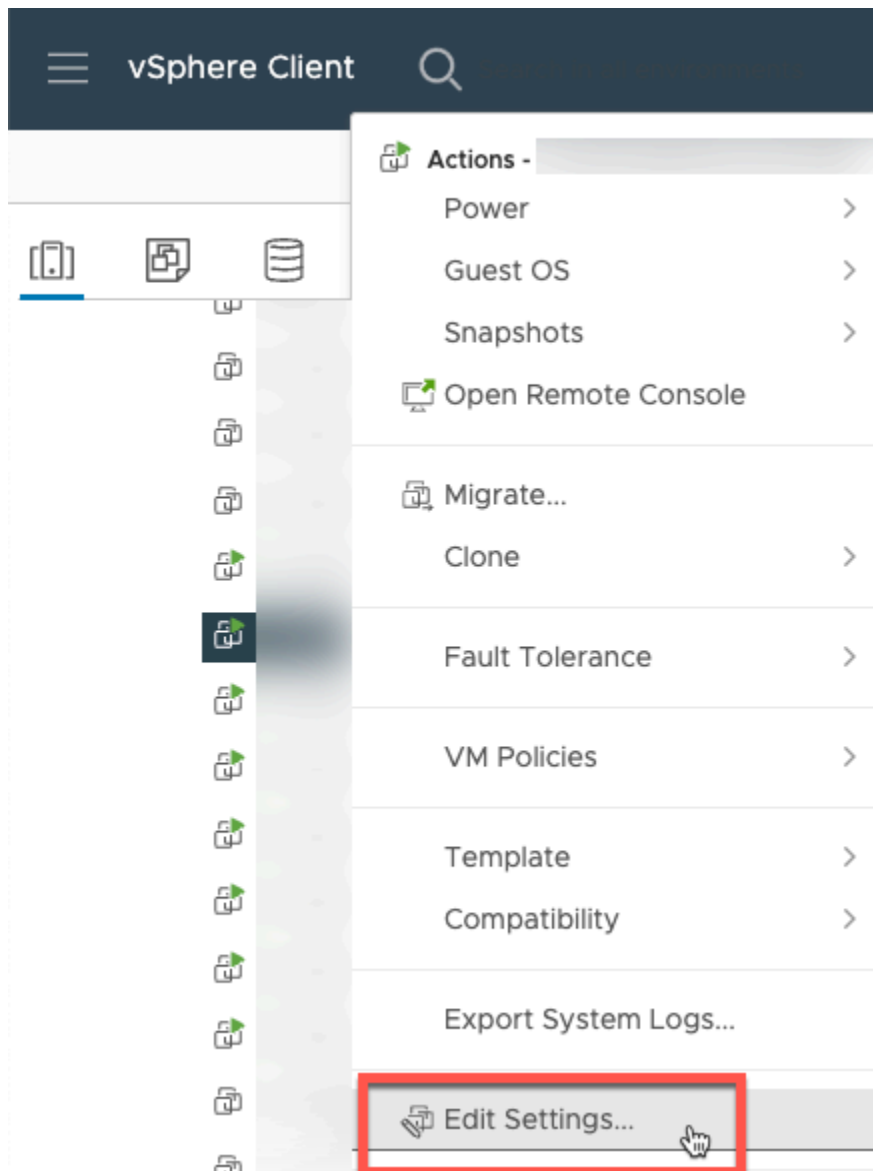
Compatibility

CANCEL

BACK

NEXT

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.

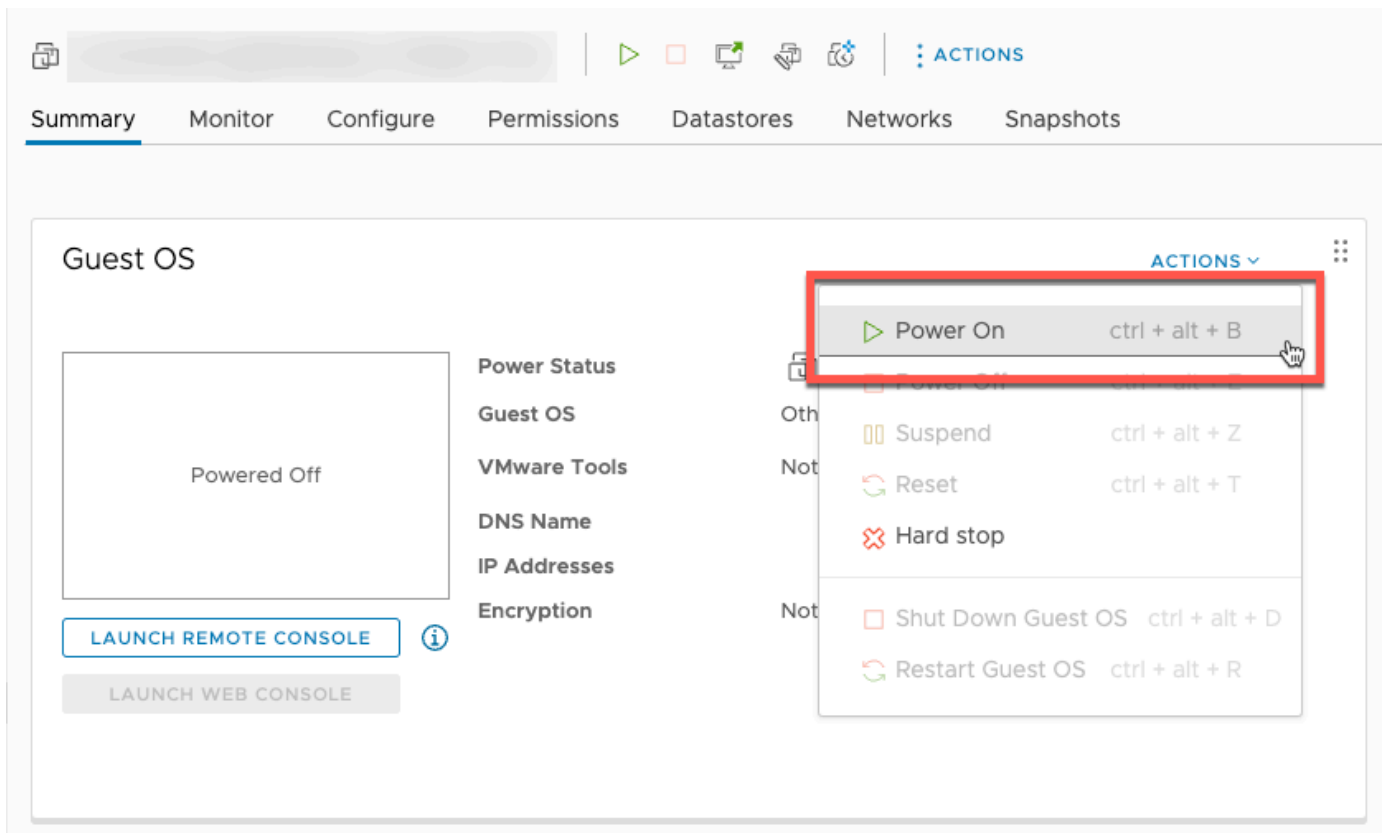
Edit Settings ✕

Virtual Hardware VM Options

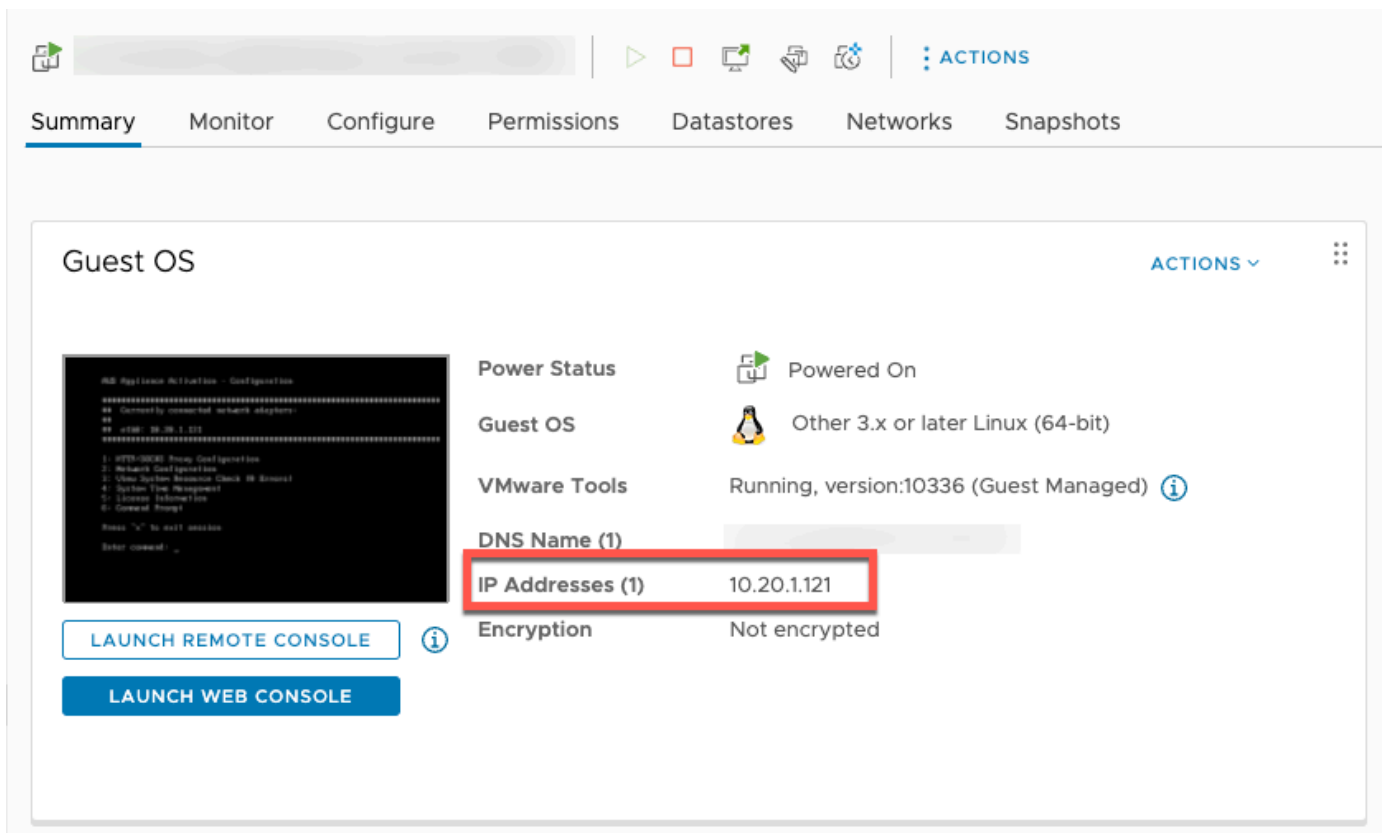
> General Options	VM Name:
VMware Remote Console Options	☐
>	Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
▼ VMware Tools	
Power Operations	▶ Power On / Resume VM ◻ Shut Down Guest (Default) ▼ ⏸ Suspend (Default) ▼ ↺ Restart Guest (Default) ▼
Tools Upgrades	☐ Check and upgrade VMware Tools before each power on
Synchronize Time with Host ⓘ	☒ Synchronize at startup and resume (recommended) ☐ Synchronize time periodically
Run VMware Tools Scripts	☒ After powering on ☒ After resuming ☒ Before suspending ☒ Before shutting down guest

CANCEL OK

- 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 [VPC-Endpunkt erstellen](#).
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.

Manuelle Gateway-Erstellung (IPv4 und IPv6)

Um IPv6 Unterstützung zu erhalten, erstellen Sie Gateways manuell mithilfe von Aktivierungsschlüsseln. IPv6 [Für die Unterstützung sind die Gateway-Appliance-Version 2.x+ und eine zusätzliche Firewallkonfiguration auf Dual-Stack-Endpunkten erforderlich.](#)

Important

IPv6 Hypervisor-Anforderung: Wenn Ihr Gateway über aktiviert ist IPv6, müssen Sie einen Hypervisor mit einer Adresse erstellen. IPv6 Verwenden Sie z. B. 2607:fda8:1001:210::252 statt 10.0.0.252. Wenn Sie ein IPv6 Gateway einem IPv4 Hypervisor zuordnen, schlagen Sicherungs- und Wiederherstellungsaufträge wahrscheinlich fehl.

Einen Aktivierungsschlüssel erhalten

Um einen Aktivierungsschlüssel für Ihr Gateway zu erhalten, stellen Sie eine Webanfrage an die virtuelle Gateway-Maschine (VM) oder verwenden Sie die lokale Gateway-Konsole. Die Gateway-VM gibt eine Antwort zurück, die den Aktivierungsschlüssel enthält, der dann als einer der Parameter für die CreateGateway API übergeben wird, um die Konfiguration Ihres Gateways zu spezifizieren.

Tip

Gateway-Aktivierungsschlüssel laufen nach 30 Minuten ab, wenn sie nicht verwendet werden.

Abrufen eines Aktivierungsschlüssels mithilfe einer Webanfrage

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe einer HTTP-Anfrage einen Aktivierungsschlüssel erhalten. Sie können entweder einen Webbrowser oder den Linux-Befehl curl oder einen gleichwertigen Befehl wie folgt URLs verwenden.

Note

Ersetzen Sie die hervorgehobenen Variablen durch tatsächliche Werte für Ihr Gateway. Zulässige Werte sind:

- **gateway_ip_address**- Die IPv4 Adresse Ihres Gateways, zum Beispiel 172.31.29.201
- **region_code**- Die Region, in der Sie Ihr Gateway aktivieren möchten. Weitere Informationen finden Sie unter [Regionale Endpunkte](#) im Allgemeinen Referenzhandbuch zu AWS . Wenn dieser Parameter nicht angegeben ist oder wenn der angegebene Wert falsch geschrieben ist oder nicht mit einer gültigen Region übereinstimmt, verwendet der Befehl standardmäßig die us-east-1 Region.

Dual-Stack-Endpunkte (Unterstützung) IPv6

IPv4:

```
curl "http://gateway_ip_address/?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv4&no_red
```

IPv6:

```
curl "http://gateway_ip_address/?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv6&no_red
```

Einen Aktivierungsschlüssel über die lokale Konsole abrufen

Die folgenden Beispiele zeigen Ihnen, wie Sie über die lokale Konsole des Gateway-Hosts einen Aktivierungsschlüssel erhalten

1. Melden Sie sich bei der Konsole Ihrer virtuellen Maschine an.
2. Wählen Sie im Hauptmenü AWS Appliance-Aktivierung — Konfiguration 0 die Option Aktivierungsschlüssel abrufen
3. Wählen Sie die Option 2 Backup Gateway für die Gateway-Familie
4. Geben Sie die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten
5. Geben Sie als Netzwerktyp 1 für Öffentlich oder 2 für VPC-Endpunkt ein
6. Geben Sie als Endpunkttyp den Wert 1 für Standard-Endpunkt oder 2 für Dual-Stack-Endpunkt ein
 - Wählen Sie für einen Dual-Stack-Endpunkt 1 für oder für IPv4 2 IPv6
7. Der Aktivierungsschlüssel wird automatisch ausgefüllt

Das Gateway wird erstellt

Verwenden Sie den AWS CLI , um das Gateway zu erstellen, nachdem Sie einen Aktivierungsschlüssel erhalten haben:

1. Besorgen Sie sich den Aktivierungsschlüssel mithilfe von Curl-Befehlen oder der lokalen Konsolenmethode
2. Gateway erstellen mit AWS CLI, weitere Informationen finden Sie [CreateGateway](#) in der Backup-Gateway-API-Referenz.

```
aws backup-gateway create-gateway \  
    --region region_code \  
    --activation-key activation_key \  
    --gateway-display-name gateway_name \  
    --gateway-type BACKUP_VM
```

3. Stellen Sie sicher, dass das Gateway in der AWS Backup Konsole unter Externe Ressourcen → Gateways angezeigt wird

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 gelöscht 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 Uploadrate beträgt 8.000.000 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 /backup. https://console.aws.amazon.com](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 sind [Erstellen 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 Domännennamen (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 Hypervisoren 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 die Sicherung und Wiederherstellung von Daten verwendet wird, die vom Hypervisor verwaltet werden. VMs

Hypervisor-Status

Status	Bedeutung und Behebung
ONLINE	Sie haben einen Hypervisor hinzugefügt AWS Backup und diesem 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 durchzuführen.

Status	Bedeutung und Behebung
	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 • 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 zugeordnet, 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 Netzwerkconfiguration. Wenn das Problem weiterhin besteht, überprüfen Sie, ob die IP-Adresse oder der FQDN 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.

Status	Bedeutung und Behebung
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 eine Funktion namens [Changed Block Tracking](#), mit der die Speicherblöcke virtueller Maschinen verfolgt werden, während sie sich im Laufe der Zeit ändern. Wenn Sie eine virtuelle Maschine sichern, AWS Backup versucht es, die CBT-Daten zu verwenden, sofern sie verfügbar sind. 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 ein eigener Mechanismus zur Erkennung von VMware Änderungen AWS Backup verwendet wurde, um die Sicherung 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 Problembehandlung weitere 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 Schlagworte

[Tags](#) sind Schlüssel-Wert-Paare, mit denen Sie Ihre Ressourcen verwalten, filtern und suchen können.

Ein VMware Tag besteht aus einer Kategorie und einem Tagnamen. 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 Externe Ressourcen > Virtuelle Maschinen > AWS Tags oder VMware Tags.

VMware Tag-Zuordnung

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 VMware Tag-Informationen in die entsprechenden AWS Tags eingeben können. Die vier Felder sind VMware-Tag-Kategorie, VMware Tag-Name, AWS Tag-Schlüssel und AWS Tag-Wert (Beispiel: Kategorie = OS; Tag-Name = Windows; AWS Tag-Schlüssel = OS-Windows und AWS Tag-Wert = Windows).
4. Nachdem Sie Ihre bevorzugten Werte eingegeben haben, klicken Sie auf Zuordnung 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 VMware virtuellen 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.amazonaws.com` und `backup-gateway.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:

JSON

```
{
  "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-Zuordnungen 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-Zuordnungen ist. Falls Sie noch keine Zuordnungen haben, beachten Sie die Option „Keine VMware Tag-Zuordnungen“. angezeigt.

Von hier aus können Sie die Metadaten der vom Hypervisor erkannten virtuellen Maschinen synchronisieren, Sie können Zuordnungen auf Ihre (n) Hypervisor (en) kopieren, Sie können der Backup-Auswahl eines Backup-Plans zugeordnete AWS VMware Tags 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 Tags oder Tags.AWS VMware Sie können die mit dieser virtuellen Maschine verbundenen Tags anzeigen und diese Tags verwalten.

Weisen Sie mithilfe von VMware Tag-Zuordnungen virtuelle Maschinen dem Plan zu

So können Sie virtuelle Maschinen mithilfe zugeordneter Tags einem Backup-Plan zuweisen:

1. [Öffnen Sie die AWS Backup Konsole unter /backup. <https://console.aws.amazon.com>](#)
2. Gehen Sie in der Konsole auf der Hypervisor-Detailseite zu VMware Tag-Zuordnungen (klicken Sie auf Externe Ressourcen, dann auf Hypervisoren und 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, die AWS CLI

AWS Backup verwendet den API-Aufruf [PutHypervisorPropertyMappings](#), um Hypervisor-Entitätseigenschaften 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 Zuordnungen sind, synchronisiert. Außerdem werden AWS Tags, die den auf der virtuellen Maschine vorhandenen VMware Tags zugeordnet sind, auf die Ressource der AWS virtuellen 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 [VmwareTag](#) und [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 [Stellen Sie eine virtuelle Maschine wieder her 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:

- Für Gateways, die auf bereitgestellt werden VMware ESXi, laden Sie [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 von 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 AWS Appliance-Software enthalten sind:

- [Laden Sie für Gateways, die auf bereitgestellt werden VMware ESXi, 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

Fehlermeldung: "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](#) gemäß den Anweisungen von VMware zurück.

In der Nachricht 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 Funktionen verwenden. up-to-date VMware 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.

VMware Backup-Fehler

Wenn ein VMware Backup fehlschlägt, kann dies auf eine der folgenden Ursachen zurückzuführen sein:

Fehlermeldung: "Failed to process backup data. Aborted backup job." oder "Error opening disk on the virtual machine".

Mögliche Ursachen: Dieser Fehler kann aufgrund eines Konfigurationsproblems auftreten, oder die VMware Version oder Festplatte wird nicht unterstützt.

Abhilfe 1: Stellen Sie sicher, dass Ihre Infrastruktur für die Verwendung eines Gateways konfiguriert ist, und stellen Sie sicher, dass alle erforderlichen Ports geöffnet sind.

1. Greifen Sie auf die [Backup-Gateway-Konsole](#) zu. Beachten Sie, dass sich dies von der AWS Backup Konsole unterscheidet.
2. Geben Sie auf der Konfigurationsseite des Backup-Gateways Option 3 ein, um die Netzwerkkonnektivität zu testen.
3. Wenn der Netzwerktest erfolgreich ist, geben Sie X ein.
4. Kehren Sie zur Konfigurationsseite des Backup-Gateways zurück.
5. Geben Sie 7 ein, um auf die Befehlszeile zuzugreifen.
6. Führen Sie die folgenden Befehle aus, um die Netzwerkkonnektivität zu überprüfen:

```
ncport -d ESXi Host -p 902
```

```
ncport -d ESXi Host -p 443
```

Abhilfe 2: Verwenden Sie [Unterstützt VMs](#) Versionen.

Abhilfe 3: Wenn eine Gateway-Appliance mit falschen DNS-Servern konfiguriert ist, schlägt das Backup fehl. Gehen Sie wie folgt vor, um die DNS-Konfiguration zu überprüfen:

1. Rufen Sie die [Backup-Gateway-Konsole](#) auf.
2. Geben Sie auf der Konfigurationsseite des Backup-Gateways Option 2 ein, um zur Netzwerkkonfiguration zu navigieren.
3. Geben Sie im Feld Netzwerkkonfiguration den Wert 7 ein, um die DNS-Konfiguration anzuzeigen.
4. Überprüfen Sie die IP-Adressen der DNS-Server. Wenn die IP-Adresse des DNS-Servers falsch ist, erscheint die Aufforderung, zur Netzwerkkonfiguration zurückzukehren.
5. Geben Sie unter Netzwerkkonfiguration den Wert 6 ein, um die DNS-Konfiguration zu bearbeiten.
6. Geben Sie die richtigen IP-Adressen des DNS-Servers ein. Geben Sie dann X ein, um Ihre Netzwerkkonfiguration abzuschließen.

Weitere Informationen zu Ihrem Hypervisor, z. B. zu Fehlern, Netzwerkkonfiguration und Verbindung, finden Sie unter [Bearbeiten einer Hypervisor-Konfiguration](#). So konfigurieren Sie den Hypervisor für die Integration mit Amazon CloudWatch Logs.

Backup-Fehler aufgrund von Netzwerkverbindungsproblemen

Fehlermeldung: "Failed to upload backup during data ingestion. Aborted backup job." oder "Cloud network request timed out during data ingestion".

Mögliche Ursachen: Dieser Fehler kann auftreten, wenn die Netzwerkverbindung nicht ausreicht, um Datenuploads zu verarbeiten. Wenn die Netzwerkbandbreite niedrig ist, AWS Backup kann die Verbindung zwischen der VM und der VM überlastet werden und dazu führen, dass Backups fehlschlagen.

Die erforderliche Netzwerkbandbreite hängt von mehreren Faktoren ab, darunter der Größe der VM, den inkrementellen Daten, die für jedes VM-Backup generiert werden, dem Backup-Fenster und den Wiederherstellungsanforderungen.

Abhilfe: Zu den bewährten Methoden und Empfehlungen gehört eine Mindestbandbreite von 1000 Mbit/s Upload-Bandbreite für lokale Verbindungen VMs . AWS Backup Sobald die Bandbreite bestätigt wurde, wiederholen Sie den Backup-Job.

Abgebrochener Backup-Job

Fehlermeldung: `"Failed to create backup during snapshot creation. Aborted backup job."`

Mögliche Ursache: Auf dem VMware Host, auf dem sich die Gateway-Appliance befindet, liegt möglicherweise ein Problem vor.

Abhilfe: Überprüfen Sie die Konfiguration Ihres VMware Hosts und überprüfen Sie ihn auf Probleme. Weitere Informationen finden Sie unter [Bearbeiten einer Hypervisor-Konfiguration](#).

Keine verfügbaren Gateways

Fehlermeldung: `"No gateways available to work on job."`

Mögliche Ursache: Alle verbundenen Gateways sind mit anderen Jobs beschäftigt. Jedes Gateway hat ein Limit von vier gleichzeitigen Jobs (Backup oder Restore).

Abhilfemaßnahmen finden Sie im nächsten Abschnitt mit Schritten zur Erhöhung der Anzahl von Gateways und zur Verlängerung des Zeitfensters für den Backup-Plan.

VMware Fehler beim Backup-Job

Fehlernachricht: `"Abort signal detected"`

Mögliche Ursachen:

- **Niedrige Netzwerkbandbreite:** Eine unzureichende Netzwerkbandbreite kann den Abschluss von Backups innerhalb des Abschlussfensters behindern. Wenn der Backup-Job mehr Bandbreite benötigt als verfügbar, kann dies zu einem Fehler führen und den Fehler „Abort-Signal erkannt“ auslösen.
- **Unzureichende Anzahl von Backup-Gateways:** Wenn die Anzahl der Backup-Gateways nicht ausreicht, um die Backup-Rotation für alle konfigurierten zu bewältigen VMs, schlägt der Backup-Job möglicherweise fehl. Dies kann der Fall sein, wenn das Zeitfenster des Backup-Plans für den Abschluss von Backups zu kurz ist oder die Anzahl der Backup-Gateways nicht ausreicht.
- **Das Abschlussfenster für den Backup-Plan ist zu klein.**

Abhilfe:

Bandbreite erhöhen: Erwägen Sie, die Netzwerkkapazität zwischen AWS und der lokalen Umgebung zu erhöhen. Durch diesen Schritt wird mehr Bandbreite für den Backup-Prozess bereitgestellt, sodass Daten problemlos übertragen werden können, ohne dass der Fehler ausgelöst wird. Es wird empfohlen, dass Sie über eine Bandbreite von mindestens 100 Mbit/s für AWS die lokale VMware VMs Sicherung verfügen. AWS Backup

Wenn für das Backup-Gateway eine Bandbreitenbegrenzung konfiguriert ist, kann dies den Datenfluss einschränken und zu Backup-Fehlern führen. Eine Erhöhung der Bandbreitenratenbegrenzung, um eine ausreichende Datenübertragungskapazität sicherzustellen, kann dazu beitragen, Ausfälle zu reduzieren. Durch diese Anpassung kann das Auftreten des Fehlers „Abort Signal Detected“ verringert werden. Weitere Informationen finden Sie unter [Bandbreitendrosselung des Backup-Gateways](#).

Erhöhen Sie die Anzahl der Backup-Gateways: Ein einzelnes Backup-Gateway kann bis zu 4 Sicherungs- und Wiederherstellungsaufträge gleichzeitig verarbeiten. Zusätzliche Jobs werden in die Warteschlange gestellt und warten, bis das Gateway wieder freigegeben wird, bis das Backup-Startfenster abgelaufen ist. Wenn das Backup-Fenster abgelaufen ist und die Jobs in der Warteschlange noch nicht gestartet wurden, schlagen diese Backup-Jobs mit der Meldung „Abbruchsignal erkannt“ fehl. Sie können die Anzahl der Backup-Gateways erhöhen, um die Anzahl fehlgeschlagener Jobs zu verringern. Weitere Details finden Sie unter [Arbeiten mit Gateways](#).

Erhöhen Sie das Zeitfenster für den Backup-Plan: In Ihrem Backup-Plan können Sie das gesamte Zeitfenster innerhalb des Backup-Plans verlängern. Weitere Details finden Sie unter [Backup-Plan-Optionen und -Konfiguration](#).

Hilfe zur Lösung dieser Probleme finden Sie im [AWS Knowledge Center](#).

Erstellen Sie Windows VSS-Backups

Mit AWS Backup können Sie VSS-fähige Windows-Anwendungen (Volume Shadow Copy Service) sichern und wiederherstellen, die auf EC2 Amazon-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. Wenn anwendungskonsistente Windows-Backups aktiviert sind EC2, erhalten Sie dieselben

Konsistenzeneinstellungen und dieselbe Anwendungsorientierung wie bei herkömmlichen Backup-Tools.

 Note

AWS Backup unterstützt nur anwendungskonsistente Backups von Ressourcen, die auf Amazon laufen EC2, 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 [Erstellen von VSS-basierten Snapshots](#) im EC2 Amazon-Benutzerhandbuch.

Gehen Sie wie folgt vor, um VSS-fähige Windows-Ressourcen zu sichern und wiederherzustellen EC2, auf denen Amazon ausgeführt wird, um die erforderlichen Voraussetzungen zu erfüllen. Anweisungen finden Sie unter [Voraussetzungen für die Erstellung von Windows VSS-basierten EBS-Snapshots](#) im EC2 Amazon-Benutzerhandbuch.

1. Laden Sie den SSM-Agenten herunter, installieren Sie ihn und konfigurieren Sie ihn. AWS Systems Manager Dieser Schritt ist erforderlich. Anweisungen finden Sie im AWS Systems Manager Benutzerhandbuch unter [Arbeiten mit dem SSM-Agenten auf EC2 Instanzen für Windows Server](#).
2. Fügen Sie der IAM-Rolle eine IAM-Richtlinie hinzu und fügen Sie die Rolle der EC2 Amazon-Instance hinzu, bevor Sie das Windows VSS-Backup (Volume Shadow Copy Service) durchführen. Anweisungen finden Sie im EC2 Amazon-Benutzerhandbuch unter [Verwenden einer IAM-verwalteten Richtlinie, um Berechtigungen für VSS-basierte Snapshots zu gewähren](#). Die IAM-Beispielrichtlinie finden Sie unter [Verwaltete Richtlinien für AWS Backup](#).
3. [Laden Sie VSS-Komponenten herunter und installieren Sie](#) sie auf der EC2 Windows-on-Amazon-Instance
4. Aktivieren Sie VSS in: AWS Backup
 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 Instanzen 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-Instances EC2

Die folgenden EC2 Amazon-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

Kopie sichern und markieren

Für die meisten Ressourcentypen können Sie Backups AWS-Regionen auf mehrere AWS-Konten , bei Bedarf oder automatisch als Teil eines geplanten Backup-Plans kopieren. Backups in Cold Storage- oder Archivierungsebenen können jedoch nicht kopiert werden. Weitere Informationen finden Sie unter [the section called “Feature-Verfügbarkeit nach Ressource”](#) [Verschlüsselung für eine Sicherungskopie auf ein anderes Konto](#). AWS-Region

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 der kopierte Recovery Point (Backup) zu einem (periodischen) Snapshot-Backup (nicht für alle Ressourcentypen verfügbar, die beide Backup-Typen unterstützen). Je nach [Ressourcentyp](#) kann es sich bei den Snapshots um eine inkrementelle Kopie oder um eine vollständige Kopie handeln. PITR (Point-in-Time Restore) ist für diese Kopien nicht verfügbar.

Important

Kopien behalten ihre Quellkonfiguration, einschließlich Erstellungsdatum und Aufbewahrungsfrist. Das Erstellungsdatum bezieht sich auf den Zeitpunkt, an dem die Quelle erstellt wurde, nicht auf den Zeitpunkt, an dem die Kopie erstellt wurde. Sie können die Aufbewahrungsfrist überschreiben.

Die Konfiguration des kopierten Quell-Backups überschreibt die Ablaufeinstellung der Kopie, wenn der Aufbewahrungszeitraum für Kopien in der AWS Backup Konsole auf Immer gesetzt

ist (oder der [DeleteAfterDays](#)Wert -1 in der API-Anfrage auf eingestellt ist). Das heißt, eine Kopie, deren Aufbewahrungseinstellung niemals abläuft, behält das Ablaufdatum des Quell-Wiederherstellungspunkts bei.

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.

Kopierauftrag erneut versuchen

AWS Backup implementiert die folgende Wiederholungsstrategie für Kopieraufträge: Wenn AWS Backup Systemfehler auftreten, geht der Kopierauftrag in eine Wiederholungsphase über, die 2 Stunden dauert. Während dieser Zeit bleibt der Status des Kopierauftrags unverändert, während das CREATED System in regelmäßigen Abständen versucht, den Auftrag zu initiieren. Wenn der Job in diesem Fenster erfolgreich gestartet wird, wechselt er in den RUNNING Status.

Wenn die Probleme nach Ablauf der zweistündigen Wiederholungszeit weiterhin bestehen, wird das AWS Backup Serviceteam automatisch benachrichtigt. Das Team untersucht dann alle zugrunde liegenden Probleme und behebt sie. Sobald das Problem behoben ist, wiederholen sie die Kopieranforderung manuell und stellen so sicher, dass die Kopieraufträge wie gewünscht abgeschlossen werden.

Der Vorgang zum erneuten Versuch eines Kopierauftrags unterscheidet sich vom Vorgang zur Wiederholung von Backup-Jobs, bei dem ein definiertes Startfenster mit regelmäßigen Wiederholungsversuchen verwendet wird, bis der Vorgang erfolgreich ist oder abläuft. Der Kopierauftragsmechanismus bietet eine zusätzliche Zuverlässigkeitsebene, indem er direkte Eingriffe des Serviceteams bei hartnäckigen Problemen vorsieht.

Inhalt

- [Erstellen von Sicherungskopien von AWS-Regionen](#)
- [Erstellen von Backup-Kopien über mehrere AWS-Konten hinweg.](#)
- [Tags auf Backups kopieren](#)

Erstellen von Sicherungskopien von AWS-Regionen

Mit AWS Backup dieser Option können Sie Backups bei Bedarf oder automatisch im Rahmen eines geplanten Sicherungsplans AWS-Regionen 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, wo 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 [Feature-Verfügbarkeit 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.

Regionsübergreifende Kopierverschlüsselung

Weitere Informationen [zur Funktionsweise der Verschlüsselung bei Kopieraufträgen finden Sie unter Verschlüsselung AWS-Region für eine Sicherungskopie auf ein anderes Konto](#).

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 Zioptionsgruppe 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. 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 [Feature-Verfügbarkeit 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.

IAM role (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 [Feature-Verfügbarkeit 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 Backup-Kopien über mehrere AWS-Konten hinweg.

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 [Feature-Verfügbarkeit 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 `seinsAWSBackupFullAccess`, 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 kontoübergreifende Backups in Ihrem AWS-Konto 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“.

EC2 Amazon-Angebote [EC2 sind zulässig AMIs](#). Wenn diese Einstellung in Ihrem Konto aktiviert ist, fügen Sie Ihre Quellkonto-ID zu Ihrer Zulassungsliste hinzu. Andernfalls schlägt der Kopiervorgang mit einer Fehlermeldung fehl, z. B. „Das Quell-AMI wurde in der Region nicht gefunden“.

Kontoübergreifendes Backup aktivieren

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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012: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 Archivspeicher übertragene Backups

müssen mindestens 90 Tage lang im Archivspeicher 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 [Feature-Verfügbarkeit 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, um anwendungsspezifische Snapshots für die ausgewählte Drittanbietersoftware zu aktivieren, auf der ausgeführt wird. EC2
12. Wählen Sie Plan erstellen aus.

Durchführen eines kontoübergreifenden On-Demand-Backups

Sie können ein Backup bei Bedarf auf ein anderes kopieren. AWS-Konto

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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012: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 Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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 [Feature-Verfügbarkeit 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

Weitere Informationen [zur Funktionsweise der Verschlüsselung für Kopieraufträge finden Sie unter Verschlüsselung AWS-Region für eine Sicherungskopie auf ein anderes Konto](#).

Weitere Hilfe zur Behebung von Fehlern bei kontoübergreifenden Kopierfehlern finden Sie im [AWS Knowledge Center](#).

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.

JSON

```
{
  "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, eine Organisationseinheit, in AWS Organizations

Die folgende Richtlinie gibt einen Backup-Tresor für Organisationseinheiten, die ihre `PrincipalOrgPaths` verwenden, frei.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
          ]
        }
      }
    }
  ]
}

```

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“.

JSON

```
{
  "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 Dienststeuerungsrichtlinien (SCPs) einzurichten AWS Organizations , 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.

JSON

```
{
  "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.

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 Konten OUs.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyFromBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLike": {
          "backup:CopyTargetOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
          ]
        }
      }
    }
  ]
}
```

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 dazu SCPs finden Sie unter [Entfernen eines Mitgliedskontos aus Ihrer Organisation](#) im Benutzerhandbuch für Organizations.

- 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 Kopiervorgang abgeschlossen ist. In diesem Fall wird der Backup-Auftrag abgeschlossen, der Status des Kopierauftrags wird jedoch als Snapshot konnte nicht rückgängig gemacht werden angezeigt.

Tags auf Backups kopieren

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 EC2 Amazon-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 EC2 Amazon-Instances angehängt sind, sind verschachtelte Ressourcen. Tags auf den Amazon EBS-Volumes, die an EC2 Amazon-Instances angehängt sind, sind verschachtelte Tags. Wenn verschachtelte Tags nicht kopiert werden AWS Backup können, schlägt der Backup-Job fehl.
- Wenn ein EC2 Amazon-Backup einen Image-Wiederherstellungspunkt und eine Reihe von Snapshots erstellt, werden Tags in das resultierende AMI AWS Backup kopiert. Wenn AWS Backup die Tags von den Volumes, die der EC2 Amazon-Instance zugeordnet sind, nicht in die resultierenden Snapshots kopiert werden können, schlägt der Backup-Job fehl.

Wenn Sie Ihr Backup auf ein anderes kopieren AWS-Region, werden alle Tags des ursprünglichen Backups an das Ziel AWS Backup AWS-Region kopiert.

Löschen von Backup

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. Beispiel:

- 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 EC2 Amazon-Wiederherstellungspunkt eine Amazon EBS-Snapshot-Sperre angewendet wurde und AWS Backup der Lebenszyklusprozess, der normalerweise zum Löschen des Wiederherstellungspunkts führen würde, nicht abgeschlossen werden kann. Beachten Sie, dass diese abgelaufenen Wiederherstellungspunkte über die EC2 Amazon-Konsole und [-API](#) oder die Amazon EBS-Konsole und [-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 Backup-Tresore aus.
2. Wählen Sie auf der Seite Backup vaults (Sicherungstresore) den Sicherungstresor, in dem Sie die Sicherungen gespeichert haben.
3. Wählen Sie Wiederherstellungspunkte und anschließend Aktionen, Löschen aus.
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 ausgewählten Wiederherstellungspunkte zu löschen, geben Sie Löschen ein und wählen Sie dann Wiederherstellungspunkte löschen.

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](#).

Änderungen Backup und taggen

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 [Feature-Verfügbarkeit 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 mehr geändert werden, nachdem ein Backup 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-Managementkonsole an und öffnen Sie die AWS Backup Konsole unter `https://console.aws.amazon.com /backup`.](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).

Backup-Suche

Übersicht

Mit AWS Backup können Sie Backups, auch Wiederherstellungspunkte genannt, von AWS Ressourcen erstellen. Sie können mit der AWS Backup Konsole oder der Befehlszeile nach Backups bestimmter Ressourcentypen wie Amazon S3 und Amazon EBS sowie nach Elementen und Dateien in diesen Backups suchen.

AWS Backup bietet Ihnen die Möglichkeit, die Metadaten Ihrer Backups unterstützter Ressourcentypen auf detaillierter Ebene nach Dateien oder Objekten zu durchsuchen, die den Eigenschaften entsprechen, die Sie bei Ihrer Suche definiert haben, wie Größe, Erstellungsdatum und Ressourcentyp. Sie können noch tiefer eintauchen, indem Sie die Eigenschaften der Elemente definieren, nach denen Sie suchen möchten.

Erstellen Sie zunächst einen Backup-Index, den Sie in eine future Suche einbeziehen möchten. Die Erstellung eines Backup-Indexes kann durch einen Backup-Plan automatisiert werden oder Sie können manuell einen für jeden vorhandenen Wiederherstellungspunkt erstellen. Wenn Sie bereit für die Suche sind, legen Sie die Sicherungs- und Elementeeigenschaften fest, die in den Suchergebnissen angezeigt werden sollen. Optional können Sie das Backup oder das Element wiederherstellen, nach dem Sie bei der Suche gesucht haben.

In diesem Dokument werden die Schritte zum Erstellen eines Backup-Index, zum Durchsuchen indizierter Backups, zum Wiederherstellen anhand Ihrer Suchergebnisse und zur Behebung von Problemen mit den Index- und Suchfunktionen in AWS Backup beschrieben.

Anwendungsfälle für Backup-Indizes und Suchvorgänge

Möglicherweise sind Sie ein Administrator, der eine bestimmte Datei oder ein bestimmtes Objekt wiederherstellen möchte. Anstatt manuell zu ermitteln oder zu erraten, welche Backups die Daten enthalten, können Sie die Metadaten Ihrer Wiederherstellungspunkte durchsuchen und genau die Backups, Dateien oder Objekte wiederherstellen, die Sie benötigen.

Das Wiederherstellen eines vollständigen Backups, nur um das spezifische Element zu finden, das sich möglicherweise darin befindet, kann Stunden oder Tage dauern. Stattdessen können Sie mit einer Backup-Suche genau die Datei oder das Objekt finden und wiederherstellen, die Sie benötigen.

Backup-Suchen sind nützlich für Backup-Administratoren, Backup-Betreiber, Datenbesitzer und andere IT-Experten, die mit Datensicherung, Wiederherstellung und Compliance zu tun haben.

Zugriff

Bevor Sie einen Index und eine Suche erstellen können, muss Ihr Konto über die erforderlichen Berechtigungen für die Vorgänge verfügen.

Indexberechtigungen

Bei Indexvorgängen basiert die AWS Backup Authentifizierung auf der IAM-Rolle, nicht auf Benutzeranmeldedaten (Informationen zu IAM-Benutzern und IAM-Rollen finden Sie unter).

[Authentifizierung](#)

Die folgenden Berechtigungen sind erforderlich, um einen Index einer EBS-Backup zu erstellen. Diese Berechtigungen sind in der verwalteten Richtlinie [AWSBackupServiceRolePolicyForIndexing](#) enthalten:

- `ec2:DescribeSnapshots`
- `ebs:ListSnapshotBlocks`
- `ebs:GetSnapshotBlock`
- `kms:Decrypt`

Für die Erstellung eines S3-Indexes sind keine Indexberechtigungen erforderlich.

Suchberechtigungen

Die folgenden Berechtigungen sind erforderlich, um eine Suche zu erstellen. Diese Berechtigungen sind in der verwalteten Richtlinie [AWSBackupSearchOperatorAccess](#):

- `backup:ListIndexedRecoveryPointsForSearch`
- `backup:SearchRecoveryPoint`

Wenn Sie sich dafür entscheiden, die Suchergebnisse mit einem vom Kunden verwalteten AWS KMS Schlüssel zu verschlüsseln, stellen Sie sicher, dass der Schlüssel die folgenden Berechtigungen enthält:

- `kms:GenerateDataKey`
- `kms:Decrypt`

Ablauf des Prozesses

Eine Backup-Suche umfasst drei Schritte sowie einen optionalen vierten Wiederherstellungsschritt, wenn Sie die bei Ihrer Suche zurückgegebenen Elemente wiederherstellen möchten.

Indizieren Sie Ihre Backups: Aktivieren Sie die Indizierung in Ihren Backup-Plänen oder erstellen Sie manuell über die Konsole oder CLI einen Backup-Index für jedes bestehende Backup (Recovery Point), das für Suchen in Frage kommen soll.

Backup-Metadaten nach einem Wiederherstellungspunkt, einer Datei oder einem Objekt durchsuchen: Geben Sie die Eigenschaften der Backups und Elemente an, die Sie bei Ihrer Suche finden möchten, z. B. beim Durchsuchen Ihrer zwischen dem 2. und 6. April erstellten S3-Buckets mit Tags von `Administration` und für Objekte, die größer als 100 MB sind, wobei der Schlüsselname `enthältAdmin`.

Suchergebnisse überprüfen: Wenn Sie den gewünschten Wiederherstellungspunkt oder das Element finden, haben Sie die Möglichkeit, es wiederherzustellen. Wenn Sie den Wiederherstellungspunkt oder das Element nicht gefunden haben, können Sie die Backup-Eigenschaften und Elementeeigenschaften verfeinern und dann eine neue Suche starten.

Bestimmte Elemente wiederherstellen (optional): Geben Sie Dateipfade oder wiederherzustellende Elemente sowie die Wiederherstellungsbedingungen an.

Backup-Indizes

Um durchsuchbar zu sein, muss ein Backup (Erholungspunkt) zunächst über einen entsprechenden Index verfügen.

Die Erstellung eines Backup-Indexes kann in einem Backup-Plan aktiviert werden, sodass jedem future Backup auch ein Backup-Index zugeordnet ist. Sie können auch einen Index erstellen, während Sie ein On-Demand-Backup erstellen.

Alternativ können Sie rückwirkend einen Index für einen vorhandenen Recovery Point erstellen, entweder über den Detailbildschirm des Vault-Wiederherstellungspunkts in der AWS Backup Konsole oder über AWS CLI.

Wiederherstellungspunkte unterstützter Ressourcentypen können über einen Backup-Index verfügen, wenn sie in einem Standard-Backup-Tresor gespeichert sind (Wiederherstellungspunkte in einem logischen Air-Gap-Depot unterstützen derzeit keine Backup-Indizes).

S3-Backup-Indizes

Ein S3-Backup kann in regelmäßigen Abständen erfolgen, wobei es in einem festen Intervall gemäß Ihrem Backup-Plan geplant wird. Jedes Mal, wenn ein regelmäßiges Backup erstellt wird, wird dafür ein Backup-Index erstellt. Ein S3-Backup kann auch kontinuierlich sein, wobei jede Änderung im Backup protokolliert wird. Da es täglich zahlreiche Änderungen geben kann, wird für ein kontinuierliches Backup täglich nur ein Backup-Index erstellt.

Der erste Backup-Index, der für einen kontinuierlichen S3-Recovery Point erstellt wird, ist voll; nachfolgende Indizes für denselben Recovery Point können inkrementell sein.

EBS-Backup-Indizes

Jeder für einen EBS-Wiederherstellungspunkt erstellte Backup-Index ist voll (nicht inkrementell).

AWS Backup versucht, Snapshot-Probleme bei der Erstellung eines Backup-Index automatisch zu reparieren. Wenn sich ein Dateisystem bei der Erstellung des Wiederherstellungspunkts in einem fehlerhaften Zustand befand, AWS Backup wird automatisch versucht, das Dateisystem wiederherzustellen. Wenn diese Wiederherstellung fehlschlägt, schlägt auch der Job zur Indexerstellung fehl.

Die Art des Snapshots bestimmt, ob er indexiert werden kann:

Kann indexiert werden:

- Dateisysteme: ext2, ext3, ext4, vfat, xfs und ntfs

Kann nicht indexiert werden:

- Schnappschüsse in der Archivschicht (Cold Storage)
- RAID und andere Speicheroptionen für mehrere Festplatten
- Symbolische Verknüpfungen
- Hard-Links

Schritte zur Erstellung eines Backup-Indexes

Console

Fügen Sie Ihrem Backup-Plan die Erstellung eines Backup-Indexes hinzu.

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie in der linken Navigationsleiste unter Mein Konto die Option Backup-Pläne aus.
3. Wählen Sie im Bereich Backup-Pläne den Link mit dem Namen des Plans aus, für den Sie die Indexerstellung hinzufügen möchten.
4. Wählen Sie im zweiten Bereich Backup-Regeln die Option Backup-Regel hinzufügen aus.
5. Scrollen Sie nach unten zum Bereich Backup-Indizes. Markieren Sie das Kästchen neben den Ressourcentypen, für die Sie einen Index erstellen möchten.

Bei jeder neuen Sicherung, die dieser Plan erstellt, wird gleichzeitig auch ein entsprechender Index für diesen Wiederherstellungspunkt erstellt.

Erstellen Sie einen Index für einen vorhandenen Erholungspunkt

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie in der linken Navigationsleiste Tresor aus.
3. Wählen Sie in der Spalte mit dem Tresornamen den Link aus, in dem das Backup gespeichert ist, für das Sie einen Backup-Index erstellen möchten.
4. Setzen Sie ein Häkchen neben den Wiederherstellungspunkt, für den Sie einen Backup-Index erstellen möchten.
5. Wählen Sie die Aktionsschaltfläche und dann Index erstellen aus.

Während der Erstellung hat der Index den Indexstatus `In progress`. Sobald der Status auf `geändert wurdeAvailable`, kann der Recovery Point in eine Suche einbezogen werden.

Erstellen Sie einen Index, während Sie ein On-Demand-Backup erstellen.

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Weitere Informationen finden Sie in den Schritten zum [Erstellen eines On-Demand-Backups mit AWS Backup](#) Erstellen eines On-Demand-Backups mit AWS Backup.
3. Wenn Sie in den Einstellungen einen Ressourcentyp ausgewählt haben, der Index und Suche unterstützt, wird der Zeilenpunkt Backup-Suchindex angezeigt. Aktivieren Sie die Option Backup-Suchindex erstellen, damit gleichzeitig mit diesem On-Demand-Backup ein Index erstellt wird.

AWS CLI

Erstellen Sie einen Backup-Index über CLI

Verwenden Sie den AWS CLI Befehl [create-backup-plan](#), um einen neuen Backup-Plan zu erstellen. Oder verwenden Sie ihn, [update-backup-plan](#) um einen vorhandenen Plan zu ändern.

Fügen Sie für beide Operationen innerhalb des Parameters `--backup-plan -rules` Folgendes ein `IndexActions`.

Weitere Informationen finden Sie [IndexActionsBackupRuleInput](#) im AWS Backup API-Referenzhandbuch.

Sobald ein Recovery Point über einen Index verfügt, können Sie seine Einstellungen aktualisieren.

Beispiel:

```
aws backup update-recovery-point-index-settings
--recovery-point-arn arn:aws:ec2:us-west-2::snapshot/snap-012345678901234567

--backup-vault-name [vaultname] //
--index ENABLED
--endpoint-url [URL]
--iam-role-arn arn:aws:iam::012345678901:role/Admin
```

Suchvorgänge

Sobald Sie über ein oder mehrere Backups mit einem Index verfügen, können Sie diese indizierten Backups über die AWS Backup Konsole oder über AWS CLI durchsuchen.

Wenn Sie eine Suche erstellen, wählen Sie einen Ressourcentyp aus. Die Ergebnisse geben nur Wiederherstellungspunkte zurück, die diesen Typ enthalten, z. B. S3-Buckets oder EBS-Snapshots.

Anschließend geben Sie die Eigenschaften der Backups (Wiederherstellungspunkte) an, die Sie in die Suche einbeziehen möchten. Sie können bis zu 9 Eigenschaften angeben. Eigenschaftstypen, die mehrmals enthalten sind, geben Ergebnisse zurück, die allen eingeschlossenen Werten entsprechen.

Geben Sie die Eigenschaften der Elemente an, die Sie in den zurückgegebenen Wiederherstellungspunkten suchen möchten, z. B. den Bucket-Namen oder die Dateigröße. Grenzen Sie Ihre Ergebnisse ein, indem Sie mehrere Eigenschaften einbeziehen.

Wenn Sie bei der Erstellung einer Suche über die AWS Backup Konsole einen Wert für eine Elementeigenschaft angeben, werden in den Ergebnissen nur Elemente zurückgegeben, die dieser Elementeigenschaft (UND-Logik) entsprechen. Wenn Sie dieselbe Elementeigenschaft wiederholen, jedoch mit unterschiedlichen Werten, werden in den Ergebnissen alle Elemente zurückgegeben, die einem der enthaltenen Werte entsprechen (ODER-Logik). Wenn Sie beispielsweise zwei EBS-Dateipfade angeben, werden alle Elemente von Wiederherstellungspunkten, die in der Suche enthalten sind und mit einem der beiden Dateipfade übereinstimmen, in den Suchergebnissen angezeigt.

- Zu den Eigenschaften von S3-Elementen gehören Erstellungszeit, ETags, Objektschlüssel, Objektgröße und Versions-ID.
- Zu den Eigenschaften von EBS-Elementen, mit denen Sie Ihre Suche filtern können, gehören Erstellungszeit, Dateipfad, Zeitpunkt der letzten Änderung und Größe.

Optional können Sie eine AWS KMS Schlüssel-ID angeben, um Ihre Ergebnisse zu verschlüsseln. Wenn kein Schlüssel enthalten ist, AWS Backup wird ein Schlüssel verwendet, der dem Dienst gehört, um die Ergebnisse zu verschlüsseln.

Console

Suchen Sie nach Elementen in Ihren Backups

Es gibt mehrere Pfade, um eine Suche nach indizierten Backups zu erstellen:

Sie können Ihren bevorzugten Wiederherstellungspunkt finden, indem Sie zu Backup-Tresoren navigieren und den spezifischen Wiederherstellungspunkt auswählen, den Sie suchen möchten. Wählen Sie dann Suchen aus. Sie können eine Suche auch von der Detailseite des Wiederherstellungspunkts aus starten.

Während einer Wiederherstellung, bei der Sie bestimmte Elemente haben, die Sie hinzufügen möchten, können Sie Ihre Backups durchsuchen, um die URL (s) oder Dateipfade zu finden, die die Elemente enthalten.

Gehen Sie wie folgt vor, um mehr als ein Backup zu durchsuchen:

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Navigieren Sie im linken Navigationsmenü zu Suchen.
3. Wählen Sie im Abschnitt Suchverlauf die Option Suche erstellen aus.
4. Wählen Sie einen Ressourcentyp aus. Sie müssen für jede Suche einen Ressourcentyp auswählen. Wenn Sie den Ressourcentyp ändern, nachdem zusätzliche Felder eingegeben wurden, gehen Ihre Eingaben verloren und Sie müssen sie erneut eingeben.
5. Wählen Sie 1 bis 9 Backup-Eigenschaften, um die Wiederherstellungspunkte einzugrenzen, die bei Ihrer Suche zurückgegeben werden.

AWS Backup scannt alle Ihre Backups, die einen Index haben. Es werden nur Wiederherstellungspunkte zurückgegeben, die allen unterschiedlichen Backup-Eigenschaften entsprechen. Zum Beispiel `backup tag = "savings"` und `backup creation date = May 20, 2019 through May 23, 2019` einschließlich.

Sie können mehrere Werte derselben Eigenschaft angeben, z. B. drei verschiedene Tags. Wenn die Eigenschaft mit unterschiedlichen Werten wiederholt wird, gibt die Suche alle Elemente zurück, die einem der angegebenen Werte entsprechen (bekannt als „ODER“-Logik). Zum Beispiel `backup tag = "savings"; backup tag = "checking"; backup creation date = May 20, 2019 through May 23, 2019, inklusive; und backup creation date = May 20, 2020 through May 23, 2020, inklusive`.

Ein Datumsbereich für die Erstellung eines Backups zählt als eine Backup-Eigenschaft. Nur ein Datumsbereich für die Erstellung eines Backups kann als Backup-Eigenschaft angegeben werden.

6. Wählen Sie 1 bis 9 Arteikeleigenschaften aus, um die Ergebnisse bei Ihrer Suche weiter einzugrenzen.

Sie können mehrere Werte derselben Eigenschaft angeben. Wenn die Eigenschaft mit unterschiedlichen Werten wiederholt wird, gibt die Suche alle Elemente zurück, die einem der angegebenen Werte entsprechen.

7. Optional: Um Ihre Suchergebnisse zu verschlüsseln, können Sie einen vorhandenen AWS KMS Schlüssel im Dropdownmenü oder ARN angeben oder einen neuen KMS-Schlüssel erstellen.
8. AWS Backup empfiehlt, einen eindeutigen Namen für den Suchauftrag zu erstellen.
9. Wählen Sie Suche starten aus.

Möglicherweise wird eine Warnung angezeigt, die besagt, dass Ihre Suche möglicherweise eine große Anzahl von Wiederherstellungspunkten umfasst. Es empfiehlt sich, zu den Backup-Eigenschaften zurückzukehren und zusätzliche Kriterien auszuwählen, um die Suche einzugrenzen. Weniger Backups bei einer Suche können zu niedrigeren Kosten führen.

AWS CLI

Verwenden Sie den AWS CLI Befehl [start-search-job](#).

Erforderliche Parameter

```
--search-scope // defines the backup properties you wish to include in the search
```

Optionale Parameter

```
--client-token // string
--encryption-key-arn // if not included, AWS Backup uses service-owned key to
  encrypt results
--item-filters // accepted keys and values depend on which resource type is included
  in the search
--name // If not included, AWS Backup auto-assigns a name
```

Zu den akzeptierten S3-Artikelfiltern gehören:

```
--object-keys // string
--sizes // long condition
--creation-times // time condition
--version-ids // string
--etags // string
```

Zu den akzeptierten EBS-Artikelfiltern gehören:

```
--file-paths //  
--sizes //  
--creation-times //  
--last-modification-time //
```

Beenden Sie eine Suche

Sie können einen Suchauftrag beenden, wenn er sich im Status befindet `RUNNING`.

Ein Suchauftrag wird fortgesetzt, bis er `COMPLETED` den Status erreicht hat (oder `FAILED` den Status, falls ein Fehler vorliegt). Sie können einen `RUNNING` Suchauftrag unterbrechen, wenn Sie einen laufenden Suchauftrag beenden möchten. Dies kann sinnvoll sein, wenn Sie das Backup oder das Objekt, nach dem Sie gesucht haben, gefunden haben, bevor der Auftrag abgeschlossen wurde.

- Klicken Sie in der AWS Backup Konsole auf die Schaltfläche Suchauftrag beenden.
- Senden Sie in der CLI den Vorgang `stop-search-job` mit der Suchauftrags-ID, die Sie beenden möchten.

Suchergebnisse

Sobald ein Suchauftrag gestartet wurde, beginnt er, Ergebnisse zu aggregieren, auch wenn er noch einen `Running` Status hat. Solange ein Suchauftrag ausgeführt wird und bis er abgeschlossen ist, sind Teilergebnisse verfügbar:

- In der Konsole werden die Ergebnisse so angezeigt, wie sie während der Suche abgerufen wurden. Die Ergebnisse werden nicht automatisch aktualisiert, aber Sie können die neuesten Ergebnisse anzeigen, indem Sie auf die Schaltfläche „Aktualisieren“ klicken. Um Ergebnisse anzuzeigen, die über die ersten 1.000 Elemente hinausgehen, wählen Sie Ergebnisse exportieren aus.
- Die CLI-Operationen [get-search-job](#) und der Status der [list-search-jobs](#) zurückgegebenen Suchaufträge. Wenn der Auftragsstatus lautet `RUNNING`, gibt der Vorgang eine unvollständige Liste zurück.

Die Ergebnisse eines Suchauftrags sind in der Konsole und über die CLI 7 Tage lang verfügbar, sobald eine Suche gestoppt oder abgeschlossen wurde. Während dieser Zeit können Sie die

Ergebnisse in Ihren bevorzugten Amazon S3 S3-Bucket exportieren, sodass Sie auch nach Ablauf dieses Zeitraums auf die Ergebnisse zugreifen können.

Jeder Suchauftrag enthält detaillierte Informationen, die in der Konsole oder über die CLI verfügbar sind, darunter, welche Wiederherstellungspunkte durchsucht wurden, den Namen und Status der Suche, ihre Beschreibung, Datum und Uhrzeit der Erstellung und Fertigstellung sowie Informationen über die zurückgegebenen Objekte oder Elemente sowie die Anzahl der gescannten Elemente und Wiederherstellungspunkte.

Wenn die Ergebnisse den gesuchten Wiederherstellungspunkt, das Element oder das Objekt nicht enthalten, können Sie eine neue Suche mit unterschiedlichen Sicherungs- und Elementeigenschaften erstellen. Jede Suche wird einzeln berechnet.

Für jeden Ressourcentyp gelten eigene Überlegungen zu den Ergebnissen, die die Suche liefert:

- Bei einer Suche nach S3-Wiederherstellungspunkten werden keine Löschmarkierungen als Teil des Suchergebnisses zurückgegeben, auch wenn diese Objekte den angegebenen Elementeigenschaften der Suche entsprechen.
- Die Ergebnisse einer EBS-Suche können einen Nullwert für die Erstellungszeit von Dateisystemen enthalten, in denen dieses Feld nicht unterstützt wird. Zu diesen Dateisystemen können unter anderem vfat, ext2/3 und XFS-Versionen vor Version 5 gehören.

Exportieren Sie Suchergebnisse in einen S3-Bucket

AWS Backup speichert die Suchergebnisse für 7 Tage, beginnend mit der Uhrzeit und dem Datum der Fertigstellung. Diese Ergebnisse können in der AWS Backup Konsole angezeigt oder über die CLI-Operation abgerufen werden. `list-search-job-results`

Es hat sich bewährt, Ihre Suchergebnisse in einen S3-Bucket zu exportieren, um die Ergebnisse auch nach Ablauf der 7-tägigen Aufbewahrungsfrist aufzubewahren. Der Exportjob erstellt einen Ordner mit dem Namen `Export Job ID` in Ihrem angegebenen Bucket und exportiert dann die Ergebnisse in diesen Ordner. Sobald die Ergebnisse dorthin exportiert wurden, sind sie verfügbar, solange Sie den Bucket behalten.

Sie können die Suchergebnisse aller unterstützten Ressourcentypen exportieren, nicht nur einer S3-Suche.

Console

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Navigieren Sie zu Jobs > Jobs suchen.
3. Wählen Sie Ergebnisse für Suchaufträge aus.
4. Setzen Sie ein Häkchen neben den Ergebnissen, die Sie exportieren möchten.
5. Wählen Sie Nach S3 exportieren aus.
6. Wählen Sie den Ziel-S3-Bucket für den Exportjob aus.
7. Nachdem Sie alle Felder konfiguriert haben, wählen Sie Exportieren aus.

Die Exportaktion erstellt einen Exportauftrag. Diese können unter Jobs > Jobs exportieren angezeigt werden. Sobald ein Exportauftrag COMPLETED den Status erreicht hat, stehen die Suchergebnisinformationen im S3-Bucket zum Abrufen oder Herunterladen als eine oder mehrere CSV-Dateien zur Verfügung.

AWS CLI

Verwenden Sie den AWS CLI Befehl [start-search-result-export-job](#).

Erforderliche Parameter

```
--search-job-identifizier  
--export-specification
```

Optionale Parameter

```
--client-token  
--role-arn  
--tags
```

Die Operation wird zurückkehren `ExportJobArn` und `ExportJobIdentifier`.

Verwenden Sie [list-search-result-export-jobs](#), um den Status von Exportaufträgen abzurufen.

Kostenüberlegungen und bewährte Verfahren

Für jede Erstellung eines Backup-Indexes und für jeden Suchauftrag fallen Gebühren an. Für jeden Backup-Index fallen Speichergebühren an. Jede Wiederherstellung anhand von Suchergebnissen

(wie bei allen anderen All-Restore-Aufträgen) wird in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS Backup Preise](#).

Sie können die möglichen Ergebnisse eines Suchauftrags einschränken, indem Sie mehrere Sicherungs- und Artefakteigenschaften angeben. Dies kann zu geringeren Kosten führen als eine Suche, die alle möglichen Wiederherstellungspunkte umfasst.

Aus der Suche wiederherstellen

Viele Kunden entscheiden sich dafür, ihre Backups — und die darin enthaltenen Objekte oder Dateien — nach einem oder mehreren wiederherzustellenden Objekten zu durchsuchen. Allgemeine Informationen [Stellen Sie ein Backup nach Ressourcentyp wieder her](#) zu Wiederherstellungen finden Sie unter.

Sie können Daten aus Ihren Suchergebnissen in der AWS Backup Konsole wiederherstellen, indem Sie zu Jobs > Suchauftragsergebnisse > Wiederherstellen navigieren. Verwenden Sie [start-restore-job](#) für die Wiederherstellung Metadaten AWS CLI, die für den Ressourcentyp, den Erholungspunkt und die an der Wiederherstellung beteiligten Elemente spezifisch sind.

Informationen [Stellen Sie S3-Daten wieder her mit AWS Backup](#) zum Wiederherstellen eines Wiederherstellungspunkts mit S3-Daten, zum Wiederherstellen eines S3-Buckets oder zum Wiederherstellen von bis zu fünf Objekten oder Ordnern mit einem S3-Bucket finden Sie unter.

Informationen [Ein Amazon EBS-Volume wiederherstellen](#) zum Wiederherstellen eines EBS-Snapshots auf einem neuen Volume, das an eine Instance angehängt ist, finden Sie unter. EC2

Backup-Tiering

Übersicht

AWS Backup bietet eine kostengünstigere Warm-Storage-Stufe für Amazon S3 S3-Backups, die die langfristigen Speicherkosten um bis zu 30% senkt und gleichzeitig Schutz- und Wiederherstellungsfunktionen auf Unternehmensniveau bietet. Die kostengünstigste Stufe bietet dieselbe Leistung und dieselben Funktionen wie die Warm-Speicherstufe. Sie können Tiering so konfigurieren, dass S3-Backup-Daten je nach Alter der Objekte in Ihren Backup-Tresoren in kostenoptimierten Speicher verschoben werden.

AWS Backup Tiering bietet die Möglichkeit, die Speicherkosten für S3-Backup-Daten zu optimieren, die aufgrund der Einhaltung gesetzlicher Vorschriften, der Notfallvorsorge und der Strategien zum

Schutz vor Ransomware über längere Zeiträume aufbewahrt werden. Sie können Tiering für alle S3-Backups für alle Tresore in einem Konto konfigurieren oder gezielte Konfigurationen für bestimmte Tresore und geschützte Ressourcen erstellen.

Erstellen Sie zunächst eine Tiering-Konfiguration, die festlegt, welche S3-Ressourcen nach wie vielen Tagen (mindestens 60 Tage) abgestuft werden sollen. Tiering-Konfigurationen können automatisiert werden, sodass sie auf alle Backups oder auf bestimmte Ressourcen angewendet werden. Wenn Backup-Daten den angegebenen Altersschwellenwert erreichen, werden sie auf die kostengünstigere Speicherstufe umgestellt, wobei die identischen Wiederherstellungsfunktionen beibehalten werden.

In diesem Dokument werden die Schritte zur Erstellung von Tiering-Konfigurationen, zur Verwaltung von mehrstufigen Backup-Daten, zur Überwachung von Kosteneinsparungen und zur Behebung von Problemen mit der Tiering-Funktion unter beschrieben. AWS Backup

Important

Überlegungen zu den Kosten beim Backup-Tiering:

- Das Backup-Tiering besteht aus drei Kostenkomponenten: Warmes Speicher-Tier, kostengünstiges Warm-Storage-Tier und Übergangskosten. Wenn Backup-Daten auf die kostengünstigere Stufe umgestellt werden, fällt eine einmalige Übergangsgebühr pro Objekt an, die auf der Anzahl der Objekte basiert, die für das Tiering in Frage kommen.
- Bei großen Datensätzen mit vielen Objekten können die Übergangskosten anfangs erheblich sein, werden aber in der Regel durch kontinuierliche Speichereinsparungen für Daten ausgeglichen, die über den Mindestschwellenwert von 60 Tagen hinaus aufbewahrt werden.

Tiering-Konfigurationen

Beim S3-Backup-Tiering wird eine Tiering-Konfiguration erstellt, die festlegt, welche Ressourcen gestaffelt werden sollen und wie viele Tage vor dem Übergang (mindestens 60 Tage) zur kostengünstigeren Stufe vergehen. Um eine Kostenoptimierung zu ermöglichen, müssen die Backup-Daten durch eine Tiering-Konfiguration abgedeckt werden.

Die Erstellung einer Tiering-Konfiguration kann so eingerichtet werden, dass sie für alle Backups aller S3-Ressourcen in Ihrem Konto gilt oder gezielt auf bestimmte Tresore und Ressourcen ausgerichtet ist. Sie können mehrere Konfigurationen erstellen, um unterschiedlichen Anforderungen an Datenaufbewahrung und Kostenoptimierung gerecht zu werden.

Tiering-Konfigurationen gelten sowohl für vorhandene Backup-Daten in Tresoren als auch für neue Backups, die nach der Einrichtung der Konfiguration erstellt wurden.

S3-Backup-Tiering-Konfigurationen spezifizieren:

- **Ressourcenumfang:** Alle Ressourcen in allen Tresoren, alle Ressourcen in einem bestimmten Tresor oder ausgewählte einzelne Ressourcen. Eine Tiering-Konfiguration, die für alle Tresore und alle Ressourcen gilt, wird als Standardkonfiguration betrachtet.
- **Übergangszeit:** Mindestens 60 Tage, bevor die Daten in die kostengünstigere Stufe verschoben werden
- **Tresorzuweisung:** Für welche Backup-Tresore gilt die Konfiguration (für alle Tresore oder für einen bestimmten Tresornamen)
- **Ressourcenauswahl:** Bis zu 5 verschiedene Regeln für die Ressourcenauswahl pro Konfiguration

Einschränkungen bei der Konfiguration:

- **Eine Konfiguration pro Tresor:** Jeder Tresor kann außer der Standardkonfiguration nur eine Tiering-Konfiguration haben
- **Maximal 5 Ressourcenauswahlen:** Die vault-spezifische Konfiguration unterstützt bis zu 5 verschiedene Ressourcengruppen und entsprechende Tiering-Einstellungen
- **Maximal 100 Ressourcen:** Pro Konfiguration können bis zu 100 spezifische Ressourcen für alle Ressourcengruppen ausgewählt werden
- **Tresorpriorität:** Wenn sowohl „alle Tresore“ als auch bestimmte Tresorkonfigurationen vorhanden sind, hat die spezifische Tresorkonfiguration Vorrang

Erstellung von Tiering-Konfigurationen

Tiering-Konfigurationen erstellen

Console

Um eine Tiering-Konfiguration für alle Tresore zu erstellen (Standard)

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich S3 Backup Tiering.
3. Wählen Sie Create configuration (Konfiguration erstellen).

4. Geben Sie als Konfigurationsnamen einen eindeutigen beschreibenden Namen ein.
5. Wählen Sie Alle S3-Ressourcen in allen Tresoren aus.
6. Wenn Sie die Einstellungen in Tagen reduzieren möchten, geben Sie die Anzahl der Tage (mindestens 60) ein, bis die Daten auf die kostengünstigere Stufe umgestellt werden.
7. (Optional) Fügen Sie Tags hinzu.
8. Wählen Sie Create configuration (Konfiguration erstellen).

Um eine bestimmte Vault-Tiering-Konfiguration zu erstellen

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich S3 Backup Tiering.
3. Wählen Sie Create configuration (Konfiguration erstellen).
4. Geben Sie als Konfigurationsnamen einen eindeutigen beschreibenden Namen ein.
5. Wählen Sie S3-Ressourcen in einem bestimmten Tresor aus.
6. Wählen Sie für die Tresorauswahl einen bestimmten Backup-Tresor aus der Drop-down-Liste aus.
7. Wählen Sie für die Ressourcenauswahl eine der folgenden Optionen:
 - a. Alle S3-Ressourcen in diesem Tresor, die auf alle S3-Ressourcen im Tresor angewendet werden sollen
 - b. Spezifische S3-Ressourcen in diesem Tresor zur Auswahl einzelner S3-Buckets
8. Wenn Sie bestimmte Ressourcen auswählen:
 - a. Wählen Sie einzelne S3-Ressourcen aus (insgesamt bis zu 100 Ressourcen für alle Ressourcengruppen in einer Konfiguration)
 - b. Lege für jede Ressourcengruppe die Einstellungen für die Abstufung innerhalb von Tagen fest
 - c. Wählen Sie Tiering-Einstellung hinzufügen, um zusätzliche Regeln zu erstellen (bis zu 5 insgesamt)
9. (Optional) Fügen Sie Tags hinzu.
10. Wählen Sie Create configuration (Konfiguration erstellen).

AWS CLI

Um eine Tiering-Konfiguration für alle Tresore (Standard) zu erstellen, verwenden Sie AWS CLI

```
aws backup create-tiering-configuration \  
--tiering-configuration '{  
  "TieringConfigurationName": "MyTieringConfig",  
  "BackupVaultName": "*",  
  "ResourceSelection": [{  
    "Resources": ["*"],  
    "TieringDownSettingsInDays": 60,  
    "ResourceType": "S3"  
  }]  
'
```

Verwaltung von Tiering-Konfigurationen

Tiering-Konfigurationen anzeigen

Sie können vorhandene Tiering-Konfigurationen über die AWS Backup Konsole oder die AWS CLI REST-API anzeigen.

Console

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich S3 Backup Tiering.
3. Sehen Sie sich die Liste der Konfigurationen mit Umfang, Übergangseinstellungen und Status an.

AWS CLI

Um alle Tiering-Konfigurationen aufzulisten, verwenden Sie den AWS CLI

```
aws backup list-tiering-configurations --max-results 50
```

Um spezifische Informationen zur Tiering-Konfiguration abzurufen

```
aws backup get-tiering-configuration --tiering-configuration-name "MyTieringConfig"
```

Ändern von Tiering-Konfigurationen

Sie können bestehende Tiering-Konfigurationen aktualisieren, um den Übergangszeitpunkt, die Ressourcenauswahl oder die Tresorzuweisungen zu ändern.

Console

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich S3 Backup Tiering.
3. Wählen Sie die zu ändernde Konfiguration aus.
4. Wählen Sie Bearbeiten aus.
5. Aktualisieren Sie die gewünschten Einstellungen.
6. Geben Sie für die Einstellung der Einstellungen in Tagen die Anzahl der Tage (mindestens 60) ein, bevor Daten auf die kostengünstigere Stufe umgestellt werden.
7. Wählen Sie Änderungen speichern aus.

AWS CLI

Um eine Tiering-Konfiguration mit dem zu aktualisieren AWS CLI

```
aws backup update-tiering-configuration \
--tiering-configuration-name "MyTieringConfig" \
--tiering-configuration '{
  "BackupVaultName": "*",
  "ResourceSelection": [{
    "Resources": ["*"],
    "TieringDownSettingsInDays": 60,
    "ResourceType": "S3"
  }]
}'
```

Löschen von Tiering-Konfigurationen

Sie können Tiering-Konfigurationen löschen, wenn sie nicht mehr benötigt werden.

Console

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

2. Wählen Sie im Navigationsbereich S3 Backup Tiering.
3. Wählen Sie die zu löschende Konfiguration aus.
4. Wählen Sie Löschen aus.
5. Geben Sie den Namen der Tiering-Konfiguration ein, um das Löschen zu bestätigen.
6. Wählen Sie Tiering-Konfiguration löschen aus.

AWS CLI

Um eine Tiering-Konfiguration mit dem zu löschen AWS CLI

```
aws backup delete-tiering-configuration \  
--tiering-configuration-name "MyTieringConfig"
```

Hinweis: Beim Löschen einer Tiering-Konfiguration bleiben die vorhandenen Daten in der kostengünstigeren Stufe erhalten, es wird jedoch verhindert, dass neue Daten heruntergestuft werden.

Wie werden S3-Backup-Tiering-Konfigurationen angewendet

AWS Backup bewertet Objekte in Backups auf Grundlage ihres Alters auf ihre Eignung für die Tiererteilung. Der Service überprüft täglich das Alter der Objekte und leitet die geeigneten Objekte entsprechend Ihren Konfigurationseinstellungen in die kostengünstigere Stufe um. Die Tiering-Bewertung erfolgt automatisch im Hintergrund. Wenn Objekte innerhalb eines Backups den angegebenen Altersschwellenwert (mindestens 60 Tage) erreichen, kommen sie für eine Umstellung während des nächsten Evaluierungszyklus in Frage.

Sowohl Objekte in vorhandenen Backups als auch neu erstellte Backup-Objekte unterliegen Tiering-Konfigurationen. Wenn Sie mehrere Konfigurationen haben, die für dieselben Backup-Objekte gelten könnten, haben tresorspezifische Einstellungen Vorrang vor den Konfigurationen, die für alle Tresore gelten. Der Tiering-Prozess ist irreversibel. Sobald Objekte in die kostengünstigere Stufe verschoben wurden, verbleiben sie dort, bis das Backup gemäß Ihren Aufbewahrungsrichtlinien gelöscht wird.

Kostenstruktur und Überwachung

Preismodell

Das S3-Backup-Tiering verwendet eine kostenoptimierte Preisstruktur:

- **Speicherkosten:** Niedrigere Kosten pro GB pro Monat im Vergleich zu herkömmlichen Warme-Tarifen
- **Übergangsgebühr:** Einmalige Gebühr pro Objekt bei Umstellung auf eine kostengünstigere Stufe
- **Wiederherstellungskosten:** Gebühr pro GB, wenn Daten genauso wiederhergestellt werden wie bei der Warm-Tier-Wiederherstellung
- **Keine Abrufgebühren:** Es fallen keine zusätzlichen Abrufgebühren an

Kostenüberwachung

Überwachen Sie Ihre Einsparungen bei der Staffelung der Kosten durch:

- **AWS Cost Explorer:** Separate Nutzungstypen für jede Speicherebene
- **AWS Kosten- und Nutzungsberichte:** Detaillierte Aufschlüsselung mit Tags zur Kostenzuweisung
- **AWS Backup-Konsole:** Informationen zur Konfiguration

Beispiel für Kosteneinsparungen

Für einen 500-TB-S3-Bucket mit 1 Milliarde Objekten, bei dem 60% für ein Tiering in Frage kommen:

- Vor dem Tiering: 25.600 USD/Monat
- Nach dem Tiering: 21.000 USD/Monat
- Monatliche Ersparnis: 4.600 USD/Monat (Ermäßigung um 18%)
- Einmalige Übergangsgebühr: 6.000 USD

Beispiele für Konfigurationen

Beispiel 1: Kontoweites Tiering

Wenden Sie Tiering auf alle S3-Ressourcen in allen Backup-Tresoren an:

```
{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [
    {
      "Resources": ["*"],
      "TieringDownSettingsInDays": 60,

```

```

    "ResourceType": "S3"
  }
]
}
```

Beispiel 2:

Ordnen Sie alle Ressourcen in einem Tresor mit MyBackupVault 4 Ebenen zu:

```

{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "MyBackupVault4",
  "ResourceSelection": [
    {
      "Resources": ["*"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    }
  ]
}
```

Beispiel 3:

Stufenspezifische Bereiche mit unterschiedlichen Regeln:

```

{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "MyBackupVault",
  "ResourceSelection": [
    {
      "Resources": ["arn:aws:s3:::mybucket1", "arn:aws:s3:::mybucket2"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    },
    {
      "Resources": ["arn:aws:s3:::mybucket3"],
      "TieringDownSettingsInDays": 120,
      "ResourceType": "S3"
    }
  ]
}
```

Beispiel 4:

Stellen Sie die Regel so ein, dass ein Bucket nicht eingestuft wird (setzen Sie das Tiering auf 36500):

```
{
  "TieringConfigurationName":"MyTieringConfig",
  "BackupVaultName":"*",
  "ResourceSelection":[
    {
      "Resources":["arn:aws:s3:::mybucket7", "arn:aws:s3:::mybucket8"],
      "TieringDownSettingsInDays":36500,
      "ResourceType":"S3"
    }
  ]
}
```

Unterstützte Funktionen und Einschränkungen

Unterstützte Funktionen

- Backup-Typen: Sowohl kontinuierliche als auch regelmäßige Backups
- Tresortypen: Standard-Backup-Tresore und Tresore mit logischem Air-Gap
- Tresorsperre: Vollständige Kompatibilität mit gesperrten Backup-Tresoren
- Regional- und kontoübergreifend: Mehrstufige Daten werden kopiert (Kopien landen am Zielort in der Standardstufe)
- Wiederherstellungsfunktionen: Point-in-time Wiederherstellung und Wiederherstellungen auf Objektebene
- Suche und Indizierung: Vollständige Kompatibilität mit der Backup-Suchfunktion
- Konformität: Behält alle Compliance- und Auditfunktionen bei

Einschränkungen

- Minimale Übergangszeit: 60 Tage, bevor Daten auf eine kostengünstigere Stufe verschoben werden können
- Ressourcenlimit: Bis zu 100 spezifische Ressourcen pro Konfiguration
- Konfigurationslimit: Bis zu 5 verschiedene Regeln für die Ressourcenauswahl pro Konfiguration
- Eine Konfiguration pro Tresor: Jeder Tresor kann außer der Standardkonfiguration nur eine tresorspezifische Tiering-Konfiguration haben

- Einseitiger Übergang: Daten, die auf eine kostengünstigere Stufe verschoben wurden, bleiben dort, bis sie gelöscht werden

Fehlerbehebung

Häufig auftretende Probleme

Die Konfiguration gilt nicht für bestehende Backups

- Stellen Sie sicher, dass die Konfiguration ordnungsgemäß den richtigen Tresoren zugewiesen ist
- Vergewissern Sie sich, dass die Ressourcen in den Zielkonfigurationen richtig ausgewählt sind
- Stellen Sie sicher, dass die Backup-Daten das Mindestalter (60 Tage) erfüllen

`AlreadyExistsException` bei der Erstellung der Konfiguration

- Stellen Sie sicher, dass der Name der Tiering-Konfiguration in Ihrem Konto eindeutig ist
- Prüfen Sie, ob der Zieltresor bereits über eine aktive Tiering-Konfiguration verfügt

`LimitExceededException`-Fehler

- Stellen Sie sicher, dass Sie das Maximum von 5 Ressourcenauswahlgruppen pro Konfiguration nicht überschritten haben
- Vergewissern Sie sich, dass Sie nicht mehr als 100 spezifische Ressourcen ausgewählt haben

Höhere Umstellungskosten als erwartet

- Überprüfen Sie die Anzahl der Objekte, die umgestellt werden
- Bedenken Sie die Auswirkungen der Übergangsgebühr bei häufig wechselnden Daten
- Prüfen Sie, ob die Einstellungen für den Mindestschwellenwert für Ihren Anwendungsfall geeignet sind

Stellen Sie ein Backup nach Ressourcentyp wieder her

So führen Sie eine Wiederherstellung aus:

Anweisungen zur Wiederherstellung auf der Konsole 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 EC2 Amazon-Instances, virtuellen Maschinen und Amazon Timestream-Ressourcen ist diese Funktion 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 über das Tag-Beschränkungen finden Sie unter [Markieren von AWS - Ressourcen](#).

- 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 AWS Outposts, lokale Systeme, SAP HANA auf EC2 Amazon-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 EC2Amazon-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, [AWSBackupServiceRolePolicyForRestores](#), enthält die erforderlichen Berechtigungen für diese Aufgabe.

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

- [Wiederherstellung eines Amazon-Aurora-Clusters](#)
- [Amazon Aurora DSQL Wiederherstellung](#)
- [Stacks wiederherstellen CloudFormation](#)
- [Wiederherstellen eines DocumentDB-Clusters](#)
- [Eine Amazon DynamoDB-Tabelle wiederherstellen](#)
- [Ein Amazon EBS-Volume wiederherstellen](#)
- [Eine EC2 Amazon-Instance wiederherstellen](#)
- [Stellen Sie ein Amazon EFS-Dateisystem wieder her](#)
- [Einen Amazon EKS-Cluster wiederherstellen](#)
- [Stellen Sie ein FSx Dateisystem wieder her](#)
- [Einen Neptun-Cluster wiederherstellen](#)
- [Stellen Sie eine RDS-Datenbank wieder her](#)
- [Wiederherstellen eines Amazon-Redshift-Clusters](#)
- [Serverlose Wiederherstellung mit Amazon Redshift](#)
- [Stellen Sie eine SAP HANA-Datenbank auf einer EC2 Amazon-Instance wieder her](#)

- [Stellen Sie S3-Daten wieder her mit AWS Backup](#)
- [Ein Storage Gateway Gateway-Volume wiederherstellen](#)
- [Wiederherstellen einer Amazon-Timestream-Tabelle](#)
- [Stellen Sie eine virtuelle Maschine wieder her mit AWS Backup](#)

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 Amazon Aurora Aurora-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie [StartRestoreJob](#). Die Metadaten, die Sie für einen Wiederherstellungsauftrag angeben können, hängen davon ab, ob Sie ein kontinuierliches Backup bis zu einem bestimmten Zeitpunkt (PITR) oder einen Snapshot wiederherstellen.

Stellen Sie einen Cluster aus einem Snapshot wieder her

Sie können die folgenden Metadaten für einen Aurora-Snapshot-Wiederherstellungsauftrag angeben. Weitere Informationen und akzeptierte Werte finden Sie [RestoreDBClusterFromSnapshot](#) in der Amazon Relational Database Service API-Referenz.

```
// Required metadata:  
dbClusterIdentifier // string  
engine // string  
  
// Optional metadata:  
availabilityZones // array of strings  
backtrackWindow // long  
copyTagsToSnapshot // Boolean  
databaseName // string  
dbClusterParameterGroupName // string  
dbSubnetGroupName // string  
enableCloudwatchLogsExports // array of strings  
enableIAMDatabaseAuthentication // Boolean  
engineMode // string  
engineVersion // string  
kmsKeyId // string
```

```
optionGroupName // string
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings
```

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":[]}}}
```

Stellen Sie einen Cluster auf einen bestimmten Zeitpunkt (PITR) wieder her

Sie können die folgenden Metadaten angeben, wenn Sie ein kontinuierliches Aurora-Backup (Recovery Point) zu einem bestimmten Zeitpunkt (PITR) wiederherstellen möchten. Weitere Informationen und akzeptierte Werte finden Sie [RestoreDBClusterToPointInTime](#) in der Amazon Relational Database Service API-Referenz.

```
// Required metadata:
dbClusterIdentifier // string
engine // string
restoreToTime // timestamp; must be specified if UseLatestRestorableTime parameter isn't provided

// Optional metadata:
backtrackWindow // long
copyTagsToSnapshot // Boolean
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // array of strings
enableIAMDatabaseAuthentication // Boolean
engineMode // string
engineVersion // string
kmsKeyId // string
optionGroupName // string
```

```
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings
```

Amazon Aurora DSQL Wiederherstellung

Themen

- [Übersicht](#)
- [Aurora DSQL-Cluster mit einer einzelnen Region wiederherstellen](#)
- [Einen Aurora DSQL-Cluster mit mehreren Regionen wiederherstellen](#)
- [Beheben Sie Probleme mit der Aurora DSQL-Wiederherstellung](#)
- [Häufig gestellte Fragen zur Aurora DSQL-Wiederherstellung](#)

Übersicht

Um einen Amazon Aurora DSQL Single-Region-Cluster wiederherzustellen, verwenden Sie die AWS Backup Konsole oder CLI, um den Wiederherstellungspunkt (Backup) auszuwählen, den Sie wiederherstellen möchten. Um einen Aurora DSQL-Cluster mit mehreren Regionen wiederherzustellen, können Sie jetzt entweder die AWS Backup Konsole oder die CLI verwenden.

Geben Sie bei der Wiederherstellung einer einzelnen Region den Namen, die Clusterverschlüsselung und den Löschschutz an und initiieren Sie dann die Wiederherstellung auf einem neu erstellten Cluster.

Für die Wiederherstellung in mehreren Regionen müssen Sie zusätzliche Parameter angeben, darunter eine Zeugenregion, Peer-Region (en) und regionale Konfigurationseinstellungen.

Bei der Wiederherstellung in mehreren Regionen wird ein Cluster erstellt, der sich über mehrere AWS-Regionen erstreckt und so eine verbesserte Verfügbarkeit und Notfallwiederherstellungsfunktionen bietet.

Aurora DSQL-Cluster mit einer einzelnen Region wiederherstellen

Sie können einen Aurora DSQL-Cluster in einer einzelnen Region wiederherstellen, indem Sie die AWS Backup Konsole oder AWS CLI verwenden.

Console

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

2. Wählen Sie die Schaltfläche „Wiederherstellen“ neben dem Wiederherstellungspunkt, den Sie wiederherstellen möchten.
3. Konfigurieren Sie die Einstellungen für den neuen Cluster, auf dem Ihr Recovery Point wiederhergestellt werden soll.
 - a. Standardmäßig wird der AMK (AWS Managed Key) zur Verschlüsselung der wiederhergestellten Daten verwendet. Sie können alternativ einen anderen Schlüssel angeben.
 - b. [Der Löschschutz](#) für Ihre Aurora-Cluster ist standardmäßig aktiviert, aber deaktivieren Sie das Kästchen, um die Option auszuschalten.
4. Überprüfen Sie die Einstellungen. Wenn sie zufriedenstellend sind, klicken Sie auf die Schaltfläche Backup wiederherstellen.

AWS Backup wird einen neuen Aurora DSQL-Cluster erstellen.

AWS CLI

Wiederherstellung einer einzelnen Region

1. Verwenden Sie den CLI-Befehls `backup start-restore-job`, um einen Aurora-Cluster vom angegebenen Wiederherstellungspunkt wiederherzustellen.
2. Fügen Sie die erforderlichen Metadaten für den Wiederherstellungsjob hinzu. Beispiel:

Example

```
aws backup start-restore-job \
  --recovery-point-arn "arn:aws:dsql:us-east-1:123456789012:cluster/example-
cluster/backup/example-backup" \
  --iam-role-arn "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole" \
  --metadata '{"regionalConfig":[{"region\":"us-east-1",
\isDeletionProtectionEnabled\:true,\kmsKeyId\:"my_key"}]}' \
  --copy-source-tags-to-restored-resource
```

Einen Aurora DSQL-Cluster mit mehreren Regionen wiederherstellen

Die Aurora DSQL Multiregion Cluster-Wiederherstellung erfolgt innerhalb eines geschlossenen Region-Triplets, das aus einer Gruppe von drei Peers besteht. AWS-Regionen Für die

Wiederherstellung mehrerer Regionen müssen die Regionen, die Sie im Vorgang angeben, in einem Tripletts enthalten sein. [Weitere Informationen zu Clustern mit mehreren Regionen finden Sie unter Konfiguration von Clustern mit mehreren Regionen.](#)

Tripletts aus den folgenden Gruppen werden unterstützt. Wenn es mehr als Regionen gibt, wählen Sie drei in derselben Gruppe aus.

- USA Ost (Nord-Virginia); USA Ost (Ohio); USA West (Nordkalifornien)
- Europa (Irland); Europa (London); Europa (Paris); Europa (Frankfurt)
- Asien-Pazifik (Tokio); Asien-Pazifik (Seoul); Asien-Pazifik (Osaka)

Um die Wiederherstellung in mehreren Regionen abzuschließen, stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

- `backup:StartRestoreJob`
- `dsq1:UpdateCluster`
- `dsq1:AddPeerCluster`
- `dsq1:RemovePeerCluster`

Sie können ein Backup eines Aurora DSQL-Clusters in mehreren Regionen wiederherstellen, indem Sie entweder die AWS Backup Konsole oder die CLI-Befehle verwenden.

 Tip

Wenn Sie über einen Backup-Plan mit einer Regel verfügen, die automatisch eine regionsübergreifende Kopie in eine der angegebenen Regionen erstellt, kann die erstellte Kopie für diese Wiederherstellung in mehreren Regionen verwendet werden.

Die Wiederherstellung mehrerer Regionen beginnt mit Ihrer aktuellen Region. Sie benötigen außerdem:

- Peer-Region mit einer identischen regionsübergreifenden Kopie des Wiederherstellungspunkts in Ihrer aktuellen Region
- Zeugenregion, eine Region, AWS-Region die an Clusterkonfigurationen mit mehreren Regionen teilnimmt, indem sie Schreibvorgänge nur im Transaktionsprotokoll unterstützt, ohne Speicherplatz

für die eigentlichen Daten zu beanspruchen. Weitere Informationen zu Zeugenregionen finden Sie unter [Erstellen eines](#) Clusters mit mehreren Regionen.

Die einzelnen Schritte sind unten dargestellt:

Console

Die AWS Backup Konsole unterstützt jetzt die Wiederherstellung mehrerer Regionen für Aurora DSQL-Cluster und bietet so einen optimierten Prozess für die Erstellung von Clustern, die sich über mehrere Regionen erstrecken. [Weitere Informationen zu Clustern mit mehreren Regionen finden Sie unter Konfiguration von Clustern mit mehreren Regionen.](#)

1. [Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com /backup.](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie den Backup-Tresor aus, der den Aurora DSQL-Wiederherstellungspunkt enthält, den Sie wiederherstellen möchten.
4. Wählen Sie den Wiederherstellungspunkt aus, den Sie wiederherstellen möchten, und wählen Sie dann Wiederherstellen.
5. Wählen Sie auf der Wiederherstellungsseite unter Wiederherstellungsoptionen die Option Peer-Regionen hinzufügen aus, um die Wiederherstellung in mehreren Regionen zu aktivieren.
6. Wählen Sie im Dropdownmenü eine Peer-Cluster-Region aus. Diese Region muss sich innerhalb desselben Triplets wie Ihre aktuelle Region befinden und muss außerdem eine regionsübergreifende Kopie des Wiederherstellungspunkts in der aktuellen (ersten) Region enthalten.
7. Wählen Sie im Dropdownmenü eine Zeugenregion aus. Diese Region muss ebenfalls innerhalb desselben Triplets liegen.
8. Konfigurieren Sie die Clustereinstellungen sowohl für die Cluster der primären Region als auch für die Peer-Region:
 - a. Konfigurieren Sie für den primären Cluster:
 - Clusterverschlüsselung (optional): Wählen Sie einen KMS-Schlüssel für die Verschlüsselung aus.
 - Löschschutz: Aktiviert oder deaktiviert den Löschschutz.

- b. Konfigurieren Sie für den Peer-Region-Cluster:
 - Clusterverschlüsselung in der Peer-Region (optional): Wählen Sie einen KMS-Schlüssel für die Verschlüsselung aus.
 - Löschschutz für Peer-Region-Cluster: Aktivieren oder deaktivieren Sie den Löschschutz.
9. Überprüfen Sie Ihre Einstellungen und wählen Sie Backup wiederherstellen.
10. Die Konsole leitet den Wiederherstellungsprozess für mehrere Regionen ein, bei dem Cluster in beiden Regionen erstellt und diese automatisch miteinander verknüpft werden.

AWS CLI

Die Wiederherstellung mehrerer Regionen kann jetzt mithilfe der neuen orchestrierten Wiederherstellungsmetadaten mit AWS Backup CLI-Befehlen durchgeführt werden. Dieser Ansatz vereinfacht den Prozess, indem er die Cluster-Verknüpfung automatisch abwickelt. Weitere Informationen zur programmgesteuerten Erstellung von Clustern mit mehreren Regionen finden Sie unter [Konfiguration von Clustern mit mehreren Regionen](#) im Aurora DSQL-Benutzerhandbuch.

Important

Sowohl der primäre Cluster als auch der Peer-Cluster müssen sich in Regionen innerhalb derselben Gruppe befinden. Der Vorgang schlägt fehl, wenn sich die Cluster in Regionen außerhalb der Gruppe befinden. Zu den unterstützten Gruppen gehören:

- USA Ost (Nord-Virginia); USA Ost (Ohio); USA West (Nordkalifornien)
- Europa (Irland); Europa (London); Europa (Paris); Europa (Frankfurt)
- Asien-Pazifik (Tokio); Asien-Pazifik (Seoul); Asien-Pazifik (Osaka)

Wiederherstellung in mehreren Regionen AWS CLI mithilfe von orchestrierten Wiederherstellungsmetadaten

1. Erstellen Sie mit dem CLI-Befehl einen Wiederherstellungsauftrag `aws backup start-restore-job` mit den neuen Metadaten für die Orchestrierung mehrerer Regionen:

Example

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-
point:abcd1234" \
--iam-role-arn "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole" \
--metadata '{
    "witnessRegion":"us-west-1",
    "useMultiRegionOrchestration":"true",
    "peerRegion":["us-east-2"],
    "regionalConfig":[{"region":"us-east-1","isDeletionProtectionEnabled
":true,"kmsKeyId":"arn:aws:kms:us-east-1:123456789012:key/
ba4b3773-4bb8-4a7a-994c-46ede70202f5"}, {"region":"us-west-2",
"isDeletionProtectionEnabled":true,"kmsKeyId":"arn:aws:kms:us-
west-2:123456789012:key/ba4b3773-4bb8-4a7a-994c-46ede70202f5"}]
}' \
--copy-source-tags-to-restored-resource
```

Die Metadatenstruktur umfasst:

- **witnessRegion:** Die Region, die als Zeuge für den multiregionalen Cluster dienen wird. Weitere Informationen finden Sie unter [Resilience in Amazon Aurora DSQL](#).
- **useMultiRegionOrchestration:** Auf einstellen, true um die Orchestrierung mehrerer Regionen zu aktivieren.
- **peerRegion:** Ein Array, das die Region (en) mit Peer-Clustern im Multiregions-Cluster enthält. Weitere Informationen finden Sie [MultiRegionProperties](#) in der Aurora DSQL API-Referenz.
- **regionalConfig:** Ein Array, das die Konfiguration für jede Region enthält:
 - **region:** Der AWS-Region Bezeichner.
 - **isDeletionProtectionEnabled:** Boolesches Kennzeichen für den enable/disable Löschschutz. Weitere Informationen finden Sie [CreateCluster](#) in der Aurora DSQL API-Referenz.
 - **kmsKeyId:** Der KMS-Schlüssel-ARN für die Verschlüsselung (optional).

Wenn keine **regionalConfig** Eigenschaften angegeben werden, werden Standardwerte angewendet: Standardverschlüsselung und **isDeletionProtectionEnabled** =TRUE.

2. Überwachen Sie den Status des Wiederherstellungsauftrags mit dem `aws backup describe-restore-job` folgenden Befehl:

```
aws backup describe-restore-job --restore-job-id job-12345678
```

3. Sobald der Wiederherstellungsauftrag abgeschlossen ist, können Sie die Cluster-Konfiguration mit mehreren Regionen mithilfe der Aurora DSQL-CLI überprüfen:

```
aws dsql describe-cluster --cluster-identifier your-cluster-id
```

Weitere Informationen zu Clusteroperationen mit mehreren Regionen finden Sie [UpdateCluster](#) in der Aurora DSQL API-Referenz.

Beheben Sie Probleme mit der Aurora DSQL-Wiederherstellung

Fehler: Unzureichende Berechtigungen

Mögliche Ursache: Wenn Sie versuchen, einen Aurora DSQL-Wiederherstellungspunkt in ein Konto zu kopieren (kontoübergreifende Kopie), das noch nie mit der DSQL-API interagiert hat, wird möglicherweise ein Berechtigungsfehler angezeigt, da die mit dem DSQL-Dienst verknüpfte Rolle nicht im Zielkonto eingerichtet ist.

Abhilfe: Hängen Sie die [verwaltete DSQL-Richtlinie](#), die die mit dem DSQL-Dienst verknüpfte Rolle enthält, [AuroraDsqlServiceLinkedRolePolicy](#) an eine Rolle im Zielkonto an.

Wenn beim Sicherungs- oder Wiederherstellungsvorgang weitere Probleme auftreten, können Sie den Status Ihrer Sicherungs- und Wiederherstellungsaufträge in der AWS Backup Konsole oder mit dem überprüfen. AWS CLI Darüber hinaus können Sie die AWS CloudTrail Protokolle auf relevante Fehlermeldungen oder Ereignisse im Zusammenhang mit Ihren AWS Backup Vorgängen überprüfen.

Häufig gestellte Fragen zur Aurora DSQL-Wiederherstellung

1. „Kann ich AWS Backup für Aurora DSQL von der Aurora DSQL-Konsole aus verwenden?“

Nein, Sie können Backups und Wiederherstellungen sowie die Verwaltung von Backups nur über die AWS Backup Konsole, das SDK oder die CLI durchführen.

2. „Welche Backup-Granularität ist für Aurora DSQL verfügbar? Kann ich bestimmte Tabellen oder Datenbanken in meinem Cluster sichern?“

Sie können nur einen ganzen Aurora DSQL-Cluster sichern und wiederherstellen.

3. „Sind Backups von Aurora DSQL vollständige Backups oder inkrementelle Backups?“

Wiederherstellungspunkte von Aurora DSQL-Clustern (Backups) sind vollständige Backups Ihrer Cluster.

4. „Kann ich Backups für meine Aurora DSQL-Cluster mit mehreren Regionen erstellen?“

Ja, Sie können Backups für jeden Cluster in Clustern mit mehreren Regionen erstellen, indem Sie dieselben Schritte verwenden, wie wenn Sie ein Backup eines einzelnen Clusters in einer einzelnen Region erstellen.

AWS Backup empfiehlt als bewährte Methode, eine regionsübergreifende Kopie Ihres Backups in der anderen Region zu erstellen, aus der Sie den Multiregions-Cluster wiederherstellen möchten, da für die Wiederherstellung mehrerer Regionen eine identische Kopie desselben Wiederherstellungspunkts erforderlich ist [identisch bei diesem Vorgang bedeutet, dass die Wiederherstellungspunkte denselben Ressourcennamen und dieselbe Erstellungszeit haben].

5. „Wird mein wiederhergestellter Cluster meinen vorhandenen Cluster überschreiben?“

Nein. Wenn Sie Ihre Aurora DSQL-Daten wiederherstellen, AWS Backup erstellt aus Ihren Snapshots einen neuen Cluster. Der wiederhergestellte Cluster überschreibt den Quell-Cluster nicht.

Stacks 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.

CloudFormation Mit der AWS Backup Konsole wiederherstellen

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 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 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 CloudFormation Wiederherstellungspunkt und dann auf Wiederherstellen. Stellen Sie sicher, dass für den Wiederherstellungspunkt mit Ressourcentyp: CloudFormation und Backup-Typ: Backup festgelegt ist.
4. Sobald der Wiederherstellungsauftrag für die CloudFormation Vorlage abgeschlossen ist, wird Ihre wiederhergestellte CloudFormation Vorlage in der [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
```

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. Stellen Sie sicher, dass Sie sich auf der Konsoleseite Amazon DocumentDB-Cluster-Snapshots wiederherstellen befinden.
5. Wählen Sie im Bereich Instance-Spezifikationen eine DB-Engine für die Instance aus.
6. Geben Sie im Bereich Einstellungen einen eindeutigen Namen für Ihre DB-Cluster-ID ein.

Sie können Buchstaben, Zahlen und Bindestriche verwenden, allerdings dürfen Sie nicht zwei aufeinanderfolgende Bindestriche verwenden oder den Namen nicht mit einem Bindestrich beenden. Der endgültige Name wird ausschließlich in Kleinbuchstaben geschrieben sein.

7. Wählen Sie im Bereich Netzwerk und Sicherheit eine Availability Zone aus, oder lassen Sie uns eine für Sie auswählen.
8. Wählen Sie im Bereich Datenbankoptionen den Datenbankport aus.

Dies ist der TCP/IP Port, den die DB-Instance oder der Cluster für Anwendungsverbindungen verwenden wird. Die Verbindungszeichenfolge jeder Anwendung, die eine Verbindung mit der DB-Instance oder dem Cluster herstellt, muss ihre Portnummer angeben. Sowohl die auf die DB-Instance oder den Cluster angewendete Sicherheitsgruppe als auch die Firewalls Ihrer Organisation müssen Verbindungen zum Port zulassen. Alle DB-Instances in einem DB-Cluster verwenden denselben Port.

9. Wählen Sie ebenfalls im Bereich Datenbankoptionen die DB-Cluster-Parametergruppe aus.

Dies ist die Parametergruppe, die dem DB-Cluster dieser Instance zugeordnet ist. Die DB-Cluster-Parametergruppe dient als Container für Engine-Konfigurationswerte, die auf jede DB-Instance in dem Cluster angewendet werden.

10. Wählen Sie im Bereich Verschlüsselung den Schlüssel aus, der zur Verschlüsselung dieses Datenbank-Volumes verwendet werden soll. Der Standardwert ist `aws/rds`. Sie können alternativ einen vom Kunden verwalteten Schlüssel (CMK) verwenden.
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“ entweder die Standard-IAM-Rolle für den Wiederherstellungsauftrag oder eine andere IAM-Rolle aus.
13. Im Bereich Geschützte Ressourcen-Tags können Sie optional wählen, ob Sie Tags aus der Sicherung in den wiederhergestellten Datenbank-Cluster kopieren möchten.
14. 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.

15. 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
vpcSecurityGroupIds // string
```

Fügen Sie dann Ihren wiederhergestellten Amazon DocumentDB-Cluster mit `create-db-instance` einer Amazon RDS-Instance hinzu.

- 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
```

Eine Amazon DynamoDB-Tabelle wiederherstellen

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 /backup. https://console.aws.amazon.com](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 Tabellename) 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 unter [Erweitertes 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,kmsMasterKeyArn=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://endpointurl.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\n","kmsMasterKeyArn\":"Not Applicable"`

Um Ihre wiederhergestellte Tabelle mit einem AWS verwalteten Schlüssel zu verschlüsseln, geben Sie die folgenden Wiederherstellungsmetadaten an: `"encryptionType\":"KMS\n","kmsMasterKeyArn\":"Not Applicable"`

Um Ihre wiederhergestellte Tabelle mit einem vom Kunden verwalteten Schlüssel zu verschlüsseln, geben Sie die folgenden Wiederherstellungsmetadaten an:

`"encryptionType\":"KMS\n","kmsMasterKeyArn\":"arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"`.

Ein Amazon EBS-Volume wiederherstellen

Wenn Sie einen Amazon Elastic Block Store (EBS) -Snapshot wiederherstellen, können Sie wählen, ob Sie ihn als EBS-Volume, auf einem AWS Storage Gateway Volume oder ausgewählte Elemente daraus in einem Amazon S3 S3-Bucket wiederherstellen möchten.

Auf einem EBS-Volume wiederherstellen

Wenn Sie einen Snapshot (regelmäßige Sicherung von EBS-Daten) auf einem neuen Volume wiederherstellen, geben Sie den Volume-Typ, die Größe in GiB und eine Availability Zone an. Sie können optional wählen, ob Sie das neue Volume mit einem vorhandenen oder einem neuen Schlüssel verschlüsseln möchten. AWS KMS

Auf einem Gateway-Volume wiederherstellen

Wenn Sie auf einem Gateway-Volume wiederherstellen, müssen Sie ein Gateway mit erreichbarbarem Status angeben, Ihren iSCSI-Zielnamen und eine Festplatten-ID wählen, wenn Ihr Gateway auf einem Volume gespeichert ist, oder eine Kapazität, die Ihrem Snapshot entspricht oder größer ist, wenn Ihr Gateway zwischengespeichert ist.

Wiederherstellung auf Dateiebene in einem Amazon S3 S3-Bucket

Bevor Sie mit der Wiederherstellung von EBS-Ressourcen in einem Amazon S3 S3-Bucket beginnen, sollten Sie die [EBS-Berechtigungen](#) und die [Amazon S3 S3-Wiederherstellungsberechtigungen](#) Zugriffsanforderungen überprüfen. Die erforderlichen Berechtigungen sind in der verwalteten Richtlinie enthalten [AWSBackupServiceRolePolicyForItemRestores](#) und sollten in der [IAM-Rolle enthalten sein, die für den Wiederherstellungsvorgang](#) verwendet wird.

Alle Uploads neuer Objekte, einschließlich wiederhergestellter Daten, in einen S3-Bucket werden automatisch verschlüsselt. Wenn Sie diesen Wiederherstellungstyp wählen, geben Sie SSE-S3 (serverseitiger Amazon S3 S3-verwalteter Schlüssel) oder SSE-KMS (serverseitiger verwalteter Schlüssel) an. AWS KMS SSE-S3 ist die Standardeinstellung.

Sie können bei der Wiederherstellung über die AWS Backup Konsole bis zu fünf Pfade eingeben. Sie können mehrere Pfade über die Befehlszeile angeben. Ein Pfad muss eine Länge von weniger als 1024 Byte in UTF-8-kodierten Zeichenketten haben, einschließlich der benutzerdefinierten und -designierten Präfixe AWS Backup

Wenn Ihr Snapshot mehrere Partitionen enthält, geben Sie die Dateisystem-ID der Partition an, die die Daten enthält, die Sie wiederherstellen möchten. Diese Kennung kann anhand der UUID oder der Festplatten-ID des Dateisystems ermittelt werden [Backup-Suche](#) und ist mit dieser identisch.

	Auf ein neues EBS-Volume	Zum Gateway	Wiederherstellung auf Dateiebene im S3-Bucket
Verschlüsselung	Optional. Sie können einen vorhandenen AWS KMS Schlüssel auswählen oder einen neuen KMS-Schlüssel erstellen.		Erforderlich Wählen Sie zwischen SSE-S3, SSE-KMS oder der Standard-Ziel-Bucket-Verschlüsselung 1.
Berechtigungen und Rollen	Wählen Sie eine vorhandene Rolle aus. Wenn keine vorhanden ist, wird eine Standardrolle mit den richtigen Berechtigungen erstellt.	Wählen Sie eine bestehende Rolle aus. Wenn keine vorhanden ist, wird die Standardrolle mit den richtigen Berechtigungen erstellt	Für die Rollenauswahl müssen ausreichend EBS und Amazon S3 S3-Wiederherstellungsberechtigungen vorhanden sein.
Wiederherstellung aus dem Cold Storage (EBS Archive Tier)	Available (Verfügbar)	Nicht verfügbar	Nicht verfügbar
Zu spezifizierende Einstellungen	Datenträgertyp; Größe (GiB); Verfügbarkeitszone; Durchsatz	Gateway (in erreichbarem Zustand); iSCSI-Zielname; Festplatten-ID (für Volume Stored Gateways); Kapazität (für Volume Cache-Gateways)	Wiederherstellungstyp, einschließlich: Name des Ziel-Buckets; Pfad (e) für die Wiederherstellung; Verschlüsselungstyp; KMS-Schlüssel-ID für die Wiederherstellung auf Dateiebene, wenn SSE-KMS als

	Auf ein neues EBS-Volume	Zum Gateway	Wiederherstellung auf Dateiebene im S3-Bucket
			Verschlüsselungstyp festgelegt ist

¹ In der AWS Backup Konsole wählen Sie eine der drei Verschlüsselungsoptionen aus. Wenn Sie CLI für die Wiederherstellung verwenden, lassen Sie die Wiederherstellung `encryptionType` auf die standardmäßige Ziel-Bucket-Verschlüsselung aus.

Stellen Sie einen EBS-Snapshot mit der Konsole wieder her 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 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.

Wenn Sie die Wiederherstellung auf Dateiebene wählen, können Sie bis zu 5 Objekte oder Ordner aus dem Snapshot einbeziehen. Sie können [Ihre indizierten Backups nach dem Dateinamen oder Pfad durchsuchen](#).

- Geben Sie die Dateipfade ein.
 - Wählen Sie, ob Sie einen vorhandenen Amazon S3 S3-Bucket verwenden oder einen neuen Bucket für das Ziel erstellen möchten, an dem die Objekte oder Ordner wiederhergestellt werden sollen.
 - Stellen Sie die Verschlüsselung der wiederhergestellten Objekte ein. Sie können die Standard-Ziel-Bucket-Verschlüsselung, SSE-S3 oder SSE-KMS, wählen. Weitere Informationen finden Sie unter [Stellen Sie S3-Daten wieder her mit AWS Backup](#)
6. Wählen Sie unter Wiederherstellungsrolle die IAM-Rolle aus, die für diese Wiederherstellung übernommen AWS Backup werden soll. 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 „Backup wiederherstellen“ (bei der Wiederherstellung auf Dateiebene wird „Elemente wiederherstellen“ angezeigt).

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

Aus archivierten EBS-Snapshots wiederherstellen

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.

Tip

EBS-Volumes im Cold Storage können nicht auf einem Gateway-Volume oder auf Dateiebene 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 [Amazon-EBS-Snapshots archivieren](#) 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 > **Vault** > Archivierten EBS-Snapshot wiederherstellen.
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. Geben Sie die erforderlichen Parameter für die Wiederherstellung archivierter EBS-Snapshots an:

```
--recovery-point-arn arn:aws:backup:region:account-id:recovery-point:recovery-point-id
--metadata
  '{"temporaryRestoreDays":"value","volumeType":"value","volumeSize":"value","availabilityZone":"value"}'
--iam-role-arn arn:aws:iam::account-id:role/service-role/AWSBackupDefaultServiceRole
--resource-type EBS
```

3. Geben Sie die Dauer der temporären Wiederherstellung (0-180 Tage) im temporaryRestoreDays Parameter an. Dies bestimmt, wie lange der archivierte Snapshot im Warmspeicher verfügbar sein wird.
4. Konfigurieren Sie die neuen EBS-Volume-Einstellungen, einschließlich volumeType (gp2, gp3, io1, io2, st1, sc1), in GiB und Ziel. volumeSize availabilityZone

- Überwachen Sie den Status des Wiederherstellungsauftrags anhand [describe-restore-job](#) der zurückgegebenen Wiederherstellungsauftrags-ID. Archivwiederherstellungen können bis zu 72 Stunden dauern.

Stellen Sie einen EBS-Snapshot wieder her, indem Sie AWS CLI

Um Amazon EBS mithilfe der API oder CLI wiederherzustellen, verwenden Sie [StartRestoreJob](#). Sie können während einer Amazon EBS-Wiederherstellung die folgenden Metadaten angeben:

```
aws:backup:request-id
availabilityZone
encrypted // if set to true, encryption will be enabled as volume is restored
iops
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
  of default KMS Key Id
restoreType // include for file level restore - see details below
throughput
temporaryRestoreDays
volumeType
volumeSize
```

Beispiel:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
  \"availabilityZone\":null}"
```

Spezifikationen für die Wiederherstellung auf Dateiebene

`restoreType` ist für die Wiederherstellung auf Dateiebene erforderlich. Für diese Art der Wiederherstellung sind die folgenden eindeutigen Metadaten erforderlich:

```
destinationBucketName //
pathsToRestore //
encryptionType // You can specify SSE-S3 or SSE-KMS; do not include if you want to
  restore to default encryption
kmsKeyId //
```

Die Dateisystem-ID ist für Snapshots einzelner Partitionen optional. Wenn diese Information nicht übergeben wird, wird nur der absolute Pfad ohne das Trennzeichen „:“ (z. B. {"/data/process/abc.txt", "/data/departement/xyz.txt"}) akzeptiert.

Eine EC2 Amazon-Instance wiederherstellen

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 mithilfe der AWS Backup Konsole oder eine größere Anzahl von Einstellungen mithilfe des AWS CLI oder eines SDK anpassen. AWS

Die folgenden Überlegungen gelten für die Wiederherstellung von EC2 Instanzen:

- 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 EC2 Amazon-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 EC2 Amazon-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"
},
```

role-name Ersetzen Sie es durch den Namen der EC2 Instanzprofilrolle, die der wiederhergestellten EC2 Instanz zugewiesen wird. Dies ist nicht die AWS Backup Serviceroles, sondern die IAM-Rolle, die Berechtigungen für Anwendungen bereitstellt, die auf der EC2 Instanz ausgeführt werden.

- Während einer Wiederherstellung gelten alle EC2 Amazon-Kontingente und Konfigurationsbeschränkungen.

- Falls der Tresor mit Ihren EC2 Amazon-Wiederherstellungspunkten über eine Tresorsperre verfügt, finden Sie [Zusätzliche Sicherheitsüberlegungen](#) weitere Informationen unter.

Verwenden Sie die AWS Backup Konsole, um EC2 Amazon-Wiederherstellungspunkte wiederherzustellen

Sie können eine gesamte EC2 Amazon-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 EC2 Amazon-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 EC2 Amazon-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 wieder her EC2 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 enthält die akzeptierten Metadaten, die Sie zur Wiederherstellung eines EC2 Amazon-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
BlockDeviceMappings
aws:backup:request-id
```

AWS Backup akzeptiert die folgenden reinen Informationsattribute. Ihre Aufnahme wirkt sich jedoch nicht auf die Wiederherstellung aus:

vpcId

[BlockDeviceMappings](#) ist ein optionaler Parameter, den Sie einbeziehen können. AWS Backup unterstützt die folgenden BlockDeviceMappings Attribute.

 Note

SnapshotId und OutpostArn werden nicht unterstützt.

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName" : string,
      "NoDevice" : string,
      "VirtualName" : string,
      "Ebs": {
        "DeleteOnTermination": boolean,
        "Iops": number,
        "VolumeSize": number,
        "VolumeType": string,
        "Throughput": number,
        "Encrypted": boolean,
        "KmsKeyId": string
      }
    }
  ]
}
```

Beispiel:

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName": "/def/tuvw",
      "Ebs": {
        "DeleteOnTermination": true,
        "Iops": 3000,
        "VolumeSize": 16,
        "VolumeType": "gp3",
        "Throughput": 125,
        "Encrypted": true,

```



```
    "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/ab3cde45-67f8-9g01-  
hi2j-3456klmno7p8"  
  },  
  {  
    "DeviceName": "/abc/xyz",  
    "Ebs": {  
      "DeleteOnTermination": false,  
      "Iops": 3000,  
      "VolumeSize": 16,  
      "VolumeType": "gp3",  
      "Throughput": 125,  
      "Encrypted": false  
    }  
  }  
]  
}
```

Sie können eine EC2 Amazon-Instance auch ohne Angabe von gespeicherten Parametern wiederherstellen. Diese Option ist auf der Registerkarte Geschützte Ressource in der AWS Backup Konsole verfügbar.

Important

Wenn Sie den AWS KMS Schlüssel in der BlockDeviceMappings bei der Wiederherstellung aus konto- oder regionsübergreifenden Backups nicht überschreiben, schlägt Ihre Wiederherstellung möglicherweise fehl. Weitere Informationen finden Sie unter [Probleme mit der Wiederherstellung von EC2 Amazon-Instances beheben](#).

Probleme mit der Wiederherstellung von EC2 Amazon-Instances beheben

Beheben von -Problemen

- [Fehler bei der kontoübergreifenden Wiederherstellung](#)
- [Fehler bei der regionsübergreifenden Wiederherstellung](#)

Fehler bei der kontoübergreifenden Wiederherstellung

Beschreibung: Die Wiederherstellung der EC2 Amazon-Instanz schlägt fehl, wenn versucht wird, eine Wiederherstellung aus einem Backup durchzuführen, das mit Ihrem Konto geteilt wurde.

Mögliche Probleme: Ihr Konto hat möglicherweise keinen Zugriff auf die AWS KMS Schlüssel, die zur Verschlüsselung der Quellvolumes im Sharing-Konto verwendet wurden. Die KMS-Schlüssel werden möglicherweise nicht mit Ihrem Konto geteilt.

Oder die an die Quellinstanz angehängten Volumes sind unverschlüsselt.

Lösung: Um dieses Problem zu beheben, setzen Sie das `encrypted` Attribut auf `true` und führen Sie einen der folgenden Schritte aus:

- Überschreiben Sie die KMS-Schlüssel in `BlockDeviceMappings` und geben Sie einen KMS-Schlüssel an, den Sie in Ihrem Konto besitzen.
- Bitten Sie das Eigentümerkonto, Ihnen Zugriff auf die KMS-Schlüssel zu gewähren, die zur Verschlüsselung der Volumes verwendet werden, indem Sie die KMS-Schlüsselrichtlinie aktualisieren. Weitere Informationen finden Sie unter [Erlauben Sie Benutzern mit anderen Konten, einen KMS-Schlüssel zu verwenden](#).

Fehler bei der regionsübergreifenden Wiederherstellung

Beschreibung: Die Wiederherstellung der EC2 Amazon-Instance schlägt fehl, wenn versucht wird, die Wiederherstellung aus einem regionsübergreifenden Backup durchzuführen.

Problem: Die Volumes im Backup sind möglicherweise mit AWS KMS Schlüsseln für einzelne Regionen verschlüsselt, die in der Zielregion nicht verfügbar sind. Oder die an die Quell-Instance angehängten Volumes sind unverschlüsselt.

Lösung: Um dieses Problem zu beheben, setzen Sie das `encrypted` Attribut auf `true` und überschreiben Sie den KMS-Schlüssel in der `BlockDeviceMappings` mit einem KMS-Schlüssel in der Zielregion.

Stellen Sie ein Amazon EFS-Dateisystem wieder her

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.

Wenn Sie eine bestimmte Datei oder ein bestimmtes Verzeichnis wiederherstellen möchten, 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 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.

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 `hatTrue`).

- **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. Gültige Werte sind `generalPurpose` (Standard) und `maxIO`. Dieser `generalPurpose` Modus bietet die niedrigste Latenz pro Vorgang und kann bis zu 7.000 Dateioperationen pro Sekunde erreichen. Der `maxIO` Modus kann auf einen höheren Gesamtdurchsatz und höhere Operationen pro Sekunde mit einer etwas höheren Latenz für Dateioperationen skaliert werden.
- **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.

Wiederherstellungen in einer Zone können 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.

Einen Amazon EKS-Cluster wiederherstellen

Sie können EKS-Cluster-Backups über die AWS Backup Konsole oder CLI wiederherstellen. EKS-Backups sind zusammengesetzte Wiederherstellungspunkte, die sowohl den EKS-Clusterstatus als auch persistente Volume-Backups enthalten.

AWS Backup unterstützt mehrere Wiederherstellungen, einschließlich granularer Wiederherstellungen auf Namespace-Ebene. Wiederherstellungen sind zerstörungsfrei und überschreiben keine vorhandenen Kubernetes-Objekte in Ihrem EKS-Zielcluster. Bei Wiederherstellungen werden auch die Kubernetes-Versionen des EKS-Zielclusters nicht überschrieben.

EKS-Backups müssen auf einem EKS-Ziel-Cluster wiederhergestellt werden, d. h. auf einem Amazon EKS-Cluster, der vorab bereitgestellt wurde. Als Teil des Wiederherstellungs-Workflows können Sie sich dafür entscheiden, einen neuen EKS-Cluster zu erstellen, der in Ihrem Namen erstellt AWS Backup wird.

Note

AWS Backup bietet eine begrenzte Anzahl von Optionen für die Erstellung eines neuen EKS-Clusters als Teil einer Wiederherstellung. Für alle Funktionen zur Erstellung von EKS-Clustern können Kunden mithilfe der [EKS-Konsole einen neuen EKS-Cluster](#) erstellen oder APIs diesen als Wiederherstellungsziel auswählen.

Wiederherstellungsfunktionen für Amazon EKS

Art der Wiederherstellung	Ziel wiederherstellen	Verhalten wiederherstellen
Wiederherstellung vorhandener Cluster	Stellen Sie die Wiederherstellung auf dem Quell-EKS-Cluster oder dem vorhandenen EKS-Cluster her	Stellt alle Kubernetes-Ressourcen und persistenten Volumes in vorhandenen EKS-Clustern wieder her. Alle Wiederherstellungen sind zerstörungs

Art der Wiederherstellung	Ziel wiederherstellen	Verhalten wiederherstellen
		gsfrei und bestehende Objekte werden nicht überschrieben. Für Objekte, die übersprungen werden, können Sie SNS-Benachrichtigungen abonnieren
Neue Cluster-Wiederherstellung	Erstellt einen neuen Amazon EKS-Cluster als Teil Ihrer EKS-Wiederherstellung	Restore erstellt einen neuen EKS-Cluster und stellt alle Kubernetes-Ressourcen und persistenten Volumes auf dem neu erstellten Cluster wieder her
Namespace-Wiederherstellung	Bestehender Amazon EKS-Cluster	Stellt nur bestimmte Namespaces wieder her, deren Kubernetes-Ressourcen und entsprechende persistente Speicherwiederherstellungen sind zerstörungsfrei und bestehende Objekte werden nicht überschrieben. Für Objekte, die übersprungen werden, können Sie SNS-Benachrichtigungen abonnieren
Persistenter Speicher wiederherstellen	Abhängig von persistentem Speicher	Stellen Sie einzelne persistente Speicher als eigenständige Wiederherstellungen wieder her. Siehe Wiederherstellungsverhalten von Amazon EBS, Amazon S3, Amazon EFS.

Berechtigungen

Die erforderlichen Berechtigungen hängen vom Wiederherstellungstyp und vom Zielziel ab.

- AWS Backup Die verwaltete Richtlinie [AWSBackupServiceRolePolicyForRestores](#) enthält die erforderlichen Berechtigungen zur Wiederherstellung Ihres Amazon EKS-Clusters und des persistenten EBS- und EFS-Speichers.
- Wenn Ihr EKS-Cluster einen S3-Bucket enthält oder Sie nur den untergeordneten S3-Wiederherstellungspunkt wiederherstellen, müssen Sie sicherstellen, dass die folgenden darin enthaltenen Richtlinien oder Berechtigungen Ihrer Rolle [AWSBackupServiceRolePolicyForS3Restore](#) zugewiesen sind.

Überlegungen vor der Wiederherstellung

Bevor Sie mit einem EKS-Wiederherstellungsauftrag beginnen, sollten Sie Folgendes überprüfen. Wenn Sie ein EKS-Backup wiederherstellen, das konto- oder regionsübergreifend kopiert wurde, stellen Sie sicher, dass Sie diese Überlegungen vor der Wiederherstellung überprüfen, um Wiederherstellungsfehler zu vermeiden.

1. IAM-Rollen: Bei der Wiederherstellung auf einem anderen Cluster die im Quellcluster verwendeten IAM-Rollen (z. B. Pod-Identität, IRSA). OIDC-Anbieterkonfigurationen usw. müssen im Konto/in der Region als Zielcluster vorhanden sein.
2. Stellen Sie die EKS-Version und -Kompatibilität sicher: Die API-Versionen der Objekte, die Sie wiederherstellen möchten, sollten dieselbe Version (oder so nah wie möglich) haben und im neuen Cluster unterstützt werden. AWS Backup führt nach besten Kräften eine Wiederherstellung zwischen EKS-Versionen durch, obwohl Kompatibilitätsprobleme auftreten können, wenn zwischen stark unterschiedlichen Versionen wiederhergestellt wird.
3. Passende Speicherklassen: Stellen Sie bei Wiederherstellungen auf einem vorhandenen EKS-Cluster sicher, dass vor der Wiederherstellung die entsprechenden CSI-Speichertreiber-Add-Ons installiert sind
4. S3-Buckets: Stellen Sie bei der Wiederherstellung eines EKS-Clusters mit S3-Buckets sicher, dass Ihr S3-Bucket versioniert ist und im Zielkonto oder in der Zielregion darauf zugegriffen werden kann.
5. Image-Repository: Stellen Sie beim Wiederherstellen eines EKS-Clusters sicher, dass das Konto oder die Region des EKS-Ziel-Clusters Zugriff auf die Images hat, auf die im Rahmen der Wiederherstellung verwiesen wird. Vergewissern Sie sich, dass Ihre Registrierung über ausreichende regionsübergreifende /kontoübergreifende Richtlinienberechtigungen verfügt.

6. Sicherheitsgruppen: Sicherheitsgruppen sollten für ALB, Pod Identities, EKS Node Groups usw. im Zielkonto und in der Region vorab erstellt werden, wenn Sie im Rahmen Ihrer Wiederherstellung einen neuen EKS-Cluster erstellen
7. EBS-Verfügbarkeitszonen und -Knoten: Die Availability Zones, in denen Sie Ihre EBS-Volumes wiederherstellen, sollten der Availability Zone eines vorhandenen EKS-Knotens zugeordnet werden
8. Zerstörungsfreie Wiederherstellungen: Alle EKS-Wiederherstellungen sind zerstörungsfrei und überschreiben keine Kubernetes-Objekte der Zielwiederherstellung.
9. EKS-Audit-Logs aktivieren: Aktivieren Sie EKS-Audit-Logs für zusätzliche Protokollierung und Fehlerbehebung vor der Wiederherstellung. Sie können auch [SNS-Benachrichtigungen](#) abonnieren, um Sie über übersprungene oder fehlgeschlagene Objekte bei der Wiederherstellung zu informieren.

EKS-Konfigurationen

Wenn Sie das zusammengesetzte Amazon wiederherstellen AWS Backup, wählen Sie den Wiederherstellungstyp und das Zielziel aus. Sie können wählen, ob Sie auf dem Quell-EKS-Cluster, einem vorhandenen EKS-Cluster oder einem neuen EKS-Cluster als Wiederherstellungsziel wiederherstellen möchten. Für neue EKS-Cluster können Sie wählen, ob Sie dieselben vorhandenen Infrastruktureinstellungen (z. B. VPC, Subnetze) wie der gesicherte Cluster verwenden oder neue konfigurieren möchten. AWS Backup führt immer eine zerstörungsfreie Wiederherstellung durch, bei der keine vorhandenen Ressourcen überschrieben werden.

Für Namespace-Wiederherstellungen können Sie bis zu 5 Namespaces angeben, die selektiv wiederhergestellt werden sollen. Nur Ressourcen im Namespace-Bereich werden wiederhergestellt, während Ressourcen im Clusterbereich mit Ausnahme verwandter persistenter Volumes ausgeschlossen sind.

Als erweiterte Einstellung können Sie die Wiederherstellungsreihenfolge der Kubernetes-Objekte ändern. Standardmäßig AWS Backup werden alle Kubernetes-Objekte in der folgenden Reihenfolge wiederhergestellt:

Kubernetes-Ressourcen mit Clusterbereich

1. Benutzerdefinierte Ressourcendefinitionen
2. Namespaces (der Namespace selbst, nicht die Ressourcen in diesem Namespace)
3. StorageClasses

4. PersistentVolumes

Kubernetes-Ressourcen mit Namespace-Gültigkeitsbereich

1. PersistentVolumeClaims
2. Secrets
3. ConfigMaps
4. ServiceAccounts
5. LimitRanges
6. Pods
7. ReplicaSets

Persistente Speicherkonfigurationen

Im Rahmen der zusammengesetzten Amazon EKS-Backup-Wiederherstellung besteht der zweite Schritt darin, Ihre Persistent Storage-Konfigurationen zu konfigurieren. Dies hängt vom persistenten Speicher ab, der als Teil Ihres EKS-Clusters gesichert wurde.

Für Amazon EBS-Snapshots müssen Sie eine Availability Zone angeben, in der das Amazon EBS-Volume wiederhergestellt und erstellt wird. AWS Backup versucht dann, den EKS-Pod in derselben Availability Zone wie ausgewählt zu erstellen, sodass Ihr Volume im Rahmen der Wiederherstellung wieder in Ihren EKS-Cluster eingebunden werden kann.

Im Rahmen der Wiederherstellung AWS Backup werden Ihre Amazon EBS-Volumes und Amazon S3 S3-Buckets erneut in Ihren wiederhergestellten EKS-Cluster eingebunden. Amazon EFS-Dateisysteme stellen auf zufällige Präfixe wieder her und erfordern nach der Wiederherstellung die manuelle Erstellung eines Access Points, um sie erneut in Ihren EKS-Cluster einzubinden. AWS Backup [erstellt keine Access Points oder Mount-Ziele in Ihrem Namen. Informationen zu Zugriffspunkten und Mount-Zielen finden Sie hier.](#)

Amazon EKS-Wiederherstellungsverfahren

Gehen Sie wie folgt vor, um Amazon EKS-Backups mithilfe der AWS Backup Konsole wiederherzustellen, oder AWS CLI:

Console

So stellen Sie Ihren Amazon EKS-Cluster wieder her

1. 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 Backup-Tresor, der Ihr Amazon EKS-Backup enthält, und wählen Sie dann den Wiederherstellungspunkt für Ihr Amazon EKS-Backup aus.
4. Wählen Sie Restore (Wiederherstellen) aus.
5. Wählen Sie im Bereich Wiederherstellungsoptionen Ihren Wiederherstellungstyp aus:
 - Vollständigen EKS-Cluster wiederherstellen — Stellt den gesamten Amazon EKS-Verbundwiederherstellungspunkt wieder her
 - Wählen Sie die wiederherzustellenden Namespaces aus — Stellt bis zu fünf spezifische Namespaces wieder her
6. Konfigurieren Sie das Zielziel:
 - Wählen Sie für die Cluster-Wiederherstellung, ob Sie einen neuen Cluster erstellen oder einen vorhandenen Cluster verwenden möchten
 - Geben Sie für neue Cluster den Clusternamen, die Kubernetes-Version, die VPC-Konfiguration, IAM-Rollen, Subnetze, zusätzliche Sicherheitsgruppen, Knotengruppeneinstellungen, Fargate-Profil und Pod-Identity-IAM-Rollen an
 - Wählen Sie für bestehende Cluster den Zielcluster aus der Dropdownliste aus
 - Geben Sie für die Namespace-Wiederherstellung den Zielcluster und die Namespace-Namen an
7. Konfigurieren Sie optional erweiterte Einstellungen für die benutzerdefinierte Wiederherstellungsreihenfolge für Kubernetes-Ressourcen.
8. Wählen Sie die IAM-Wiederherstellungsrolle für den Job aus. Wenn Sie nicht die Standardrolle verwenden, stellen Sie sicher, dass die ausgewählte Rolle die iam: PassRole - Berechtigung enthält.
9. Wählen Sie Restore backup aus.

AWS CLI

Verwenden Sie den `aws backup start-restore-job` Befehl mit Amazon EKS-spezifischen Metadaten.

Die erforderlichen Metadaten hängen von Ihrem Wiederherstellungstyp ab. Für alle Wiederherstellungsvorgänge ist der `clusterName` Parameter erforderlich.

Stellen Sie Amazon EKS-Wiederherstellungspunkte wieder her über AWS CLI

Verwenden `StartRestoreJob`. Sie können bei Amazon EKS-Wiederherstellungen die folgenden Metadaten angeben:

Obligatorische Metadaten:

- `clusterName`- Name des Clusters, auf dem wiederhergestellt werden soll

Optionale Metadaten:

- `newCluster`- (wahr/falsch) Wenn wir während der Wiederherstellung einen neuen EKS-Cluster erstellen sollen
 - Wenn `newCluster` „true“ ist, gelten die folgenden Metadatenfelder:
 - `eksClusterVersion`- Gewünschte K8s-Version des Clusters, wenn die Clusterversion während der Wiederherstellung erhöht werden soll
 - `clusterRole`— Der IAM-Rollen-ARN, der an den erstellten EKS-Cluster angehängt werden soll
 - `clusterVpcConfig`- VPC/Networking Konfiguration für den erstellten EKS-Cluster. Dieses Feld hat die folgenden verschachtelten Felder:
 - `vpcId`- Die mit Ihrem Cluster verknüpfte VPC
 - `subnetIds`- Die mit Ihrem Cluster verknüpften Subnetze
 - `securityGroupIds`- Die zusätzlichen Sicherheitsgruppen, die Ihrem Cluster zugeordnet sind
 - `nodeGroups`— Die verwalteten Knotengruppen, die auf dem EKS-Cluster erstellt werden sollen. `NodeGroups` Für die Wiederherstellung müssen alle Knotengruppen aus dem Zeitpunkt des Backups dieselben und übereinstimmenden Knotengruppen enthalten `nodeGroupId`.
 - `nodeGroupId`- Die ID der Knotengruppe
 - `subnetIds`- Die Subnetze, die für die Auto Scaling Scaling-Gruppe angegeben wurden, die Ihrer Knotengruppe zugeordnet ist
 - `instanceTypes`— Wenn die Knotengruppe nicht mit einer Startvorlage bereitgestellt wurde, ist dies der Instanztyp, der der Knotengruppe zugeordnet ist

- `nodeRole`— Die Ihrer Knotengruppe zugeordnete IAM-Rolle
- `securityGroupIds`— Die Sicherheitsgruppe IDs , der SSH-Zugriff auf die Knoten gewährt wird
- `remoteAccessEc2SshKey`— Der Amazon EC2 SSH-Schlüsselname, der Zugriff auf die SSH-Kommunikation mit den Knoten in der verwalteten Knotengruppe ermöglicht
- `fargateProfiles`- Die Fargate-Profil, die auf dem EKS-Cluster erstellt werden sollen. Die Fargate-Profil für die Wiederherstellung müssen dieselben Fargate-Profil aus der Backup-Zeit haben und einen passenden Namen haben.
 - `name`- Der Name des Fargate-Profil
 - `subnetIds`- Die IDs Subnetze, in denen ein Pod gestartet werden soll
 - `podExecutionRoleArn`— Der IAM-Rollen-ARN der Pod-Ausführungsrolle, der für einen Pod verwendet werden soll, der den Selektoren im Fargate-Profil entspricht
- `podIdentityAssociations`— Die Pod-Identitätszuordnungen, die auf dem EKS-Cluster erstellt werden sollen
 - `associationId`- Die ID der Pod Identity Association
 - `roleArn`- Die IAM-Rolle ARN für die Pod Identity Association
- `kubernetesRestoreOrder`— Überschreibt die Reihenfolge, in der die Kubernetes-Manifeste wiederhergestellt werden. Diese Reihenfolge hat Vorrang vor der Standardreihenfolge für die Servicewiederherstellung. Dies folgt dem Format: `group/version/kind` or `version/kind`

[`"v1/persistentvolumes"`, `"v1/pods"`, `"`] `customresource/v2/custom`

- `namespaceLevelRestore`- (`true/false`) Wenn Sie eine Wiederherstellung auf Namespace-Ebene durchführen möchten
- `namespaces`- Eine Liste von Namespaces, die wiederhergestellt werden sollen, falls der Wert „wahr“ ist. `namespaceLevelRestore` Kann bis zu 5 Namespaces für die Wiederherstellung bereitstellen
- `restoreKubernetesManifestsOnly`- (`wahr/falsch`) Wenn Sie nur die Kubernetes-Manifestdateien und keine persistenten Speichersysteme (EBS, S3, EFS usw.) wiederherstellen möchten
- `nestedRestoreJobs`- Stellt die Metadatenkonfiguration aller verschachtelten Wiederherstellungspunkte für die PersistentVolume Speichersysteme im zusammengesetzten Wiederherstellungspunkt wieder her. Dies ist eine Abbildung von `RecoveryPointArn`: dieses `RestoreMetadata` Wiederherstellungspunkts

Auf vorhandenem Cluster wiederherstellen

```
aws backup start-restore-job \
    --recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
    --iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
    --metadata '{"clusterName":"existing-
cluster","newCluster":false}' \
    --resource-type "EKS"
```

Auf einem neuen Cluster wiederherstellen

```
aws backup start-restore-job \
    --recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
    --iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
    --metadata '{"clusterName":"new-
cluster","newCluster":true,"clusterRole":"arn:aws:iam::123456789012:role/
EKSClusterRole","eksClusterVersion":"1.33","clusterVpcConfig":{"vpcId
":"vpc-1234","subnetIds":["subnet-1","subnet-2","subnet-3"],
"securityGroupIds":["sg-123"]},"nodeGroups":[{"nodeGroupId":
"nodegroup-1","subnetIds":["subnet-1","subnet-2","subnet-3"],
"nodeRole":"arn:aws:iam::123456789012:role/EKSNodeGroupRole","instanceTypes
":["t3.small"]},"fargateProfiles":[{"name":"fargate-profile-1",
"subnetIds":["subnet-1","subnet-2","subnet-3"],"podExecutionRoleArn":
"arn:aws:iam::123456789012:role/EKSFargateProfileRole"}]}' \
    --resource-type "EKS"
```

Verwenden Sie nach dem Start des Wiederherstellungsauftrags Folgendes, `describe-restore-job` um den Fortschritt zu überwachen:

```
aws backup describe-restore-job --restore-job-id restore-job-id
```

Sie können Benachrichtigungsereignisse für fehlgeschlagene und übersprungene Objekte zur Wiederherstellung abonnieren. Weitere Informationen finden Sie unter [Benachrichtigungsoptionen mit AWS Backup](#).

Stellen Sie ein FSx Dateisystem wieder her

Die Wiederherstellungsoptionen, die bei der Wiederherstellung von FSx Amazon-Dateisystemen verfügbar sind, sind dieselben wie bei der Verwendung des nativen FSx Amazon-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 unterstützt die Wiederherstellung von Dateisystemen, die Intelligent Tiering-Speicher sowohl für Lustre- als auch FSx FSx für OpenZFS-Dateisysteme verwenden. Intelligent Tiering-Dateisysteme haben bei Wiederherstellungsvorgängen spezifische Konfigurationsanforderungen.

AWS Backup Erstellt bei der Wiederherstellung von FSx Amazon-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 Dateisysteme FSx 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 kein vorhandenes FSx Amazon-Dateisystem wiederherstellen, und Sie können keine einzelnen Dateien oder Ordner wiederherstellen.

FSx denn ONTAP unterstützt nicht die Sicherung bestimmter Volumetypen, einschließlich DP-Volumes (Datenschutz), LS-Volumes (Load-Sharing), ganzer Volumes oder Volumes auf vollen Dateisystemen. Weitere Informationen finden Sie unter [FSx ONTAP: Arbeiten mit Backups](#).

AWS Backup Tresore, die Wiederherstellungspunkte von FSx Amazon-Dateisystemen enthalten, sind außerhalb von AWS Backup sichtbar. Sie können die Wiederherstellungspunkte mit Amazon wiederherstellen FSx , aber Sie können sie nicht löschen.

In der AWS Backup Konsole können Sie Backups sehen, die mit der integrierten FSx automatischen Backup-Funktion von Amazon erstellt wurden. Sie können diese Backups auch mithilfe von wiederherstellen AWS Backup. Sie können diese Backups jedoch nicht löschen oder die automatischen Backup-Zeitpläne Ihrer FSx Amazon-Dateisysteme mithilfe von ändern AWS Backup.

Verwenden Sie die AWS Backup Konsole, um FSx Amazon-Wiederherstellungspunkte wiederherzustellen

Sie können die meisten FSx Amazon-Backups wiederherstellen, die AWS Backup mit der AWS Backup Konsole, der API oder erstellt wurden AWS CLI.

In diesem Abschnitt erfahren Sie, wie Sie die AWS Backup Konsole zum Wiederherstellen von FSx Amazon-Dateisystemen verwenden.

Wiederherstellen eines Dateisystems FSx für Windows File Server

So stellen Sie ein Dateisystem FSx für Windows File Server 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 FSx Amazon-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 Backup unter Backup-ID und der Dateisystemtyp unter Dateisystemtyp angezeigt. Sie können sowohl FSx für Windows File Server- als auch 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 aus, 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 Dateisystem FSx für Windows File Server wiederherstellen, geben Sie die Windows-Authentifizierungsinformationen an, die für den Zugriff auf das Dateisystem verwendet wurden, oder Sie können ein neues erstellen.

 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 for Windows File Server](#) im Amazon FSx for Windows File Server-Benutzerhandbuch.

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 FSx for Lustre-Dateisystems

AWS Backup unterstützt Amazon FSx for Lustre-Dateisysteme mit persistentem Speicherbereitstellungstyp, die nicht mit einem Daten-Repository wie Amazon S3 verknüpft sind.

 Note

Sie können Ihr Backup nur in einem Dateisystem wiederherstellen, das denselben Bereitstellungstyp, dieselbe Speicherkategorie, dieselbe Durchsatzkapazität, dieselbe Speicherkapazität, denselben Datenkomprimierungstyp und dieselbe AWS Region aufweist wie das Original. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, sobald es verfügbar ist.

So stellen Sie ein Amazon FSx for 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 FSx Amazon-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. Wählen Sie einen Bereitstellungstyp. 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 For Lustre finden Sie [unter Verwenden verfügbarer Bereitstellungsoptionen für Amazon FSx for Lustre-Dateisysteme](#) im Amazon FSx for Lustre-Benutzerhandbuch.

7. Wählen Sie den Durchsatz pro Speichereinheit, den Sie verwenden möchten.

 Note

Der Durchsatz pro Speichereinheit kann für Dateisysteme, die die Intelligent-Tiering-Speicherkategorie verwenden, nicht konfiguriert werden.

8. (Optional) Wählen Sie für Dateisysteme, die die Intelligent-Tiering-Speicherkategorie verwenden, den Modus und die Kapazität des SSD-Lesecaches. Weitere Informationen finden Sie in der FSx Dokumentation zur [Verwaltung des bereitgestellten](#) SSD-Lesecache.
9. (Optional) For file systems using Intelligent-Tiering storage class, choose whether to enable EFA (Elastic Fabric Adapter). To enable EFA, make sure that your security group allows all inbound and outbound traffic within the security group.
10. Geben Sie die zu verwendende Speicherkapazität an. Geben Sie eine Kapazität zwischen 32 GiB und 64.436 GiB ein.

 Note

Bei Intelligent Tiering-Dateisystemen ist die Speicherkapazität elastisch und kann bei der Wiederherstellung nicht angegeben werden. Die Kapazität wird automatisch auf der Grundlage Ihrer Datennutzung skaliert.

11. Geben Sie im Abschnitt Netzwerk und Sicherheit die erforderlichen Informationen ein.
12. (Optional) Geben Sie im Abschnitt Backup und Wartung die Informationen an, mit denen Sie Ihre Backup-Einstellungen festlegen können.
13. 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.
14. 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 FSx Amazon-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 von AWS Backup für die Wiederherstellung von Backups verwendet werden soll.
13. Überprüfen Sie alle Ihre Eingaben und wählen Sie Backup wiederherstellen.

Wiederherstellen eines Amazon FSx for OpenZFS-Dateisystems

Note

Die Wiederherstellung von einem Backup mit einer bestimmten Speicherklasse auf ein Dateisystem mit einer anderen Speicherklasse wird nicht unterstützt.

Um ein Dateisystem FSx für OpenZFS wiederherzustellen

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich Geschützte Ressourcen und dann die FSx Amazon-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 vorgesehen 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.

 Note

SSD-IOPS können nicht für Dateisysteme festgelegt werden, die die Inteling-Tiering-Speicherklasse verwenden

- b. Durchsatzkapazität: Sie können die empfohlene Durchsatzkapazität von 64 MB/sec (für die SSD-Speicherklasse) und 160 MB/sec (für die Intelligent-Tiering-Speicherklasse) wählen oder die Durchsatzkapazität angeben.
 - 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. Die SSD-Speicherkapazität zeigt die Speicherkapazität des Dateisystems an.

 Note

Bei Intelligent Tiering-Dateisystemen ist die Speicherkapazität elastisch und kann bei der Wiederherstellung nicht angegeben werden. Die Kapazität wird automatisch auf der Grundlage Ihrer Datennutzung skaliert.

7. (Optional) Wählen Sie für Dateisysteme, die die Intelligent-Tiering-Speicherklasse verwenden, den Modus und die Kapazität des SSD-Lesecaches. Weitere Informationen finden Sie in der FSx Dokumentation zur [Verwaltung des bereitgestellten](#) SSD-Lesecache.

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 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 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 FSx Amazon-Wiederherstellungspunkte wiederherzustellen

Um Amazon FSx mithilfe der API oder CLI wiederherzustellen, verwenden Sie [StartRestoreJob](#). Sie können während einer FSx Amazon-Wiederherstellung die folgenden Metadaten angeben:

```
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

 Note

Die Speicherkapazität kann für Intelligent Tiering-Dateisysteme nicht angegeben werden, da sie elastischen Speicher verwenden, der je nach Datennutzung automatisch skaliert wird.

FSx für Windows File Server Metadaten wiederherstellen

Sie können bei einer Wiederherstellung FSx für Windows-Dateiserver die folgenden Metadaten angeben:

- `ThroughputCapacity`
- `PreferredSubnetId`
- `ActiveDirectoryId`

FSx für Lustre Metadaten wiederherstellen

Sie können während einer Wiederherstellung FSx für Lustre die folgenden Unterfelder `LustreConfiguration` in den Metadaten angeben:

- `PerUnitStorageThroughput`- Gibt die Durchsatzkapazität pro bereitgestellter Speichereinheit an, gemessen in MB/s pro TiB Speicher.
- `DriveCacheType`- Der Typ des Laufwerkscaches, der von `PERSISTENT_1` Dateisystemen verwendet wird, die mit HDD-Speichergeräten ausgestattet sind. Dieser Parameter ist erforderlich, wenn `StorageType` auf „Festplatte“ eingestellt ist.
- `DataReadCacheConfiguration`- Gibt den bereitgestellten SSD-Lesecache für Intelligent Tiering-Dateisysteme an. Erforderlich, wenn `StorageType` auf `INTELLIGENT_TIERING` eingestellt ist. Weitere Informationen finden [LustreReadCacheConfiguration](#) Sie unter.
- `EfaEnabled`— Gibt an, ob die Unterstützung von Elastic Fabric Adapter (EFA) und GPUDirect Storage (GDS) für das FSx for Lustre-Dateisystem aktiviert ist.

Vollständige Informationen zu allen verfügbaren Parametern finden Sie [CreateFileSystemLustreConfiguration](#) in der Amazon FSx API-Referenz. `LustreConfiguration`

FSx für ONTAP: Metadaten wiederherstellen

Sie können während einer Wiederherstellung FSx für ONTAP die folgenden Metadaten angeben:

- Name des zu erstellenden Volumes: `#name`
- `OntapConfiguration`: `# ontap-Konfiguration`
- `junctionPath`
- `sizeInMegabytes`

- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx für OpenZFS Metadaten wiederherstellen

Sie können bei einer Wiederherstellung FSx für OpenZFS die folgenden Unterfelder `OpenZFSConfiguration` in den Metadaten angeben:

- `ThroughputCapacity`- Gibt die Durchsatzkapazität des wiederhergestellten Dateisystems an, gemessen in MB/s.
- `DiskIopsConfiguration`- Verwenden Sie bei der Angabe von IOPS für die SSD-Speicherkategorie einen Wert zwischen 0 und 160.000. Schließen Sie den Modus nicht ein, wenn IOPS angegeben ist.
- `ReadCacheConfiguration`- Gibt den bereitgestellten SSD-Lese-Cache für Intelligent Tiering-Dateisysteme an. Erforderlich, wenn `StorageType` auf `INTELLIGENT_TIERING` eingestellt ist. Weitere Informationen finden Sie [ZFSRead CacheConfiguration unter Öffnen](#).

Vollständige Informationen zu allen verfügbaren Parametern finden Sie [CreateFileSystemOpenZFSConfiguration](#) in der Amazon FSx API-Referenz.

OpenZFSConfiguration

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\\\\"}\\"]\\"}
```

Einen Neptun-Cluster wiederherstellen

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 /backup. https://console.aws.amazon.com](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
vpcSecurityGroupIds // string
```

Fügen Sie dann Ihren wiederhergestellten Neptune-Cluster mit einer Amazon RDS-Instance an.
`create-db-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.

Stellen Sie eine RDS-Datenbank wieder her

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. Akzeptieren Sie im Bereich Instanzspezifikationen die Standardeinstellungen, oder geben Sie die gewünschten Optionen 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 gewünschten Optionen an.
7. Akzeptieren Sie im Bereich Datenbankoptionen die Standardeinstellungen, oder geben Sie die Optionen an, die Sie benötigen.

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. 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 RDS-Wiederherstellungspunkte wiederherzustellen

Verwenden Sie [StartRestoreJob](#). Informationen zu akzeptierten Metadaten und Werten finden Sie unter [RestoreDBInstanceFromDBSnapshot](#) und [RestoreDBInstanceToPointInTime](#) 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
```

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 Quelltable sowie der Zielcluster, das Schema und der neue Tabellename 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 Quelltable 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 or NAMESPACE_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 \
```

Serverlose Wiederherstellung mit Amazon Redshift

Sie können manuelle Snapshots von Datenbanken oder Tabellen mithilfe der Konsole oder wiederherstellen. AWS Backup AWS CLI

Redshift Serverless und AWS Backup unterstützt austauschbare Wiederherstellung für Data Warehouse-Snapshots. Das bedeutet, dass Sie Redshift Serverless-Backups auf von [Amazon Redshift bereitgestellten Clustern oder bereitgestellte Backups in Redshift](#) Serverless-Namespaces wiederherstellen können. Dies gilt nur für die vollständige Datenbankwiederherstellung, nicht für die Wiederherstellung einzelner Tabellen.

Wiederherstellungsfunktionen für Redshift Serverless

Funktionen wiederherstellen	Namespace	Eine einzige Tabelle
Art des Snapshots	Manuell	Manuell
Benötigte Informationen	• Quell-Snapshot • Ziel-Namespace • Arbeitsgruppe	• Quell-Snapshot • Quelldatenbank • Name der Quelltabelle • Zieldatenbank • Neuer Tabellenname
Zieleffekt wiederherstellen	Stellt mithilfe einer destruktiven Wiederherstellung, bei der vorhandene Daten überschrieben werden, einen vorhandenen Namespace wieder her	Stellt eine neue Tabelle wieder her

Funktionen wiederherstellen	Namespace	Eine einzige Tabelle
Austauschbare Wiederherstellung?	Ja. • Serverlose Redshift-Backups können auf von Amazon Redshift bereitgestellten Clustern wiederhergestellt werden. • Von Amazon Redshift bereitgestellte Backups können auf Redshift Serverless-Clustern wiederhergestellt werden.	Nicht unterstützt

Weitere Informationen zu Konfigurationen finden Sie unter [Snapshots und Wiederherstellungspunkte](#) im Amazon Redshift Management Guide.

Überlegungen vor der Wiederherstellung

Bevor Sie mit einem Wiederherstellungsauftrag beginnen, sollten Sie Folgendes überprüfen:

Konfigurationen

Wenn Sie einen Redshift Serverless-Snapshot wiederherstellen, wählen Sie den Ziel-Namespace aus, in dem Sie alle Datenbanken oder eine einzelne Tabelle wiederherstellen möchten.

Wenn Sie die Datenbanken in einem Snapshot in einem Serverless-Namespace wiederherstellen, handelt es sich um eine destruktive Wiederherstellung. Das bedeutet, dass alle zuvor vorhandenen Daten im Ziel-Wiederherstellungs-Namespace überschrieben werden, wenn Sie in diesem Namespace wiederherstellen.

Wenn Sie eine einzelne Tabelle wiederherstellen, handelt es sich nicht um eine destruktive Wiederherstellung. Um eine Tabelle wiederherzustellen, geben Sie die Arbeitsgruppe, den Snapshot, die Quelldatenbank, die Quelltabelle, den Zielsicherungs-Namespace und den neuen Tabellennamen an.

Berechtigungen

Die erforderlichen Berechtigungen werden vom Ziel-Data Warehouse bestimmt (d. h. vom Namespace oder dem bereitgestellten Cluster, in dem Sie die Datenbanken oder die Tabelle wiederherstellen werden). Die folgende Tabelle kann Ihnen helfen, die zu verwendenden Berechtigungen, Rollen und Richtlinien zu bestimmen. Weitere Informationen zur Verwaltung von IAM-Richtlinien finden Sie unter [Identitäts- und Zugriffsmanagement in Amazon Redshift](#).

Erforderliche Berechtigungen und Rollen für Wiederherstellungsvorgänge

Ziel wiederherstellen	Erforderliche Genehmigung (en)	Rolle und Richtlinie von IAM
Von Amazon Redshift bereitgestellter Cluster	<code>redshift:RestoreFromSnapshot</code>	<code>AWSBackupServiceRolePolicyF</code> <code>orRestores</code> enthält diese Berechtigung; sie kann für verwendet werden. <code>aws backup start-restore-job</code>
Serverloser Redshift-Namespace	<code>redshift-serverless:RestoreFromSnapshot</code>	Sie müssen diese Berechtigung zu der Rolle und Richtlinie hinzufügen, die Sie für den Anruf verwenden möchten. <code>aws backup start-restore-job</code> Da es sich um einen destruktiven Wiederherstellungsauftrag handelt, kann die <code>Servicerollenrichtlinie</code> für Wiederherstellungen nicht verwendet werden.

Redshift Serverloses Wiederherstellungsverfahren

Gehen Sie wie folgt vor, um Redshift Serverless-Backups mithilfe der AWS Backup Konsole wiederherzustellen, oder: AWS CLI

Console

1. [Öffnen Sie die AWS Backup Konsole unter /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Wählen Sie im Navigationsbereich Einstellungen und wählen Sie die wiederherzustellende Redshift Serverless Resource ID aus.
3. Wählen Sie auf der Seite mit den Ressourcendetails die Wiederherstellungspunkt-ID im Bereich Wiederherstellungspunkte aus und wählen Sie dann Wiederherstellen aus.

4. Wählen Sie im Bereich Wiederherstellungsoptionen aus, ob Sie das gesamte Data Warehouse oder eine einzelne Tabelle wiederherstellen möchten.
5. Wählen Sie das Zielziel im Bereich Ziel-Data Warehouse-Konfiguration aus.
 - Für eine vollständige Data Warehouse-Wiederherstellung wählen Sie zwischen einem von Amazon Redshift bereitgestellten Cluster oder dem Redshift Serverless Namespace.
 - Geben Sie für die Wiederherstellung einer einzelnen Tabelle den Quell-Snapshot, die Datenbank, das Schema, den Tabellennamen und die Zieldetails an.
6. Wählen Sie die IAM-Wiederherstellungsrolle für den Job aus. Wenn Sie die Standardrolle nicht verwenden, stellen Sie sicher, dass die ausgewählte Rolle die `iam:PassRole` entsprechende Berechtigung enthält.

AWS CLI

Verwenden Sie den Befehl `aws backup start-restore-job`.

AWS Backup arbeitet mit Redshift Serverless zusammen, um den Wiederherstellungsjob zu orchestrieren. Dem CLI-Befehl wird vorangestellt, er enthält `aws backup` aber auch Metadaten, die für Redshift Serverless oder Amazon Redshift relevant sind.

Die erforderlichen und optionalen Metadaten hängen davon ab, ob Sie ein ganzes Data Warehouse oder eine einzelne Tabelle wiederherstellen.

- Informationen zur Wiederherstellung einzelner Tabellen finden Sie [restore-table-from-snapshot](#) in der AWS CLI Befehlsreferenz.
- Informationen zur Namespace-Wiederherstellung finden Sie [restore-from-snapshot](#) in der AWS CLI Befehlsreferenz.
- Informationen zur Wiederherstellung auf einem von Amazon Redshift bereitgestellten Cluster finden Sie [restore-from-cluster-snapshot](#) in der AWS CLI Befehlsreferenz.

Example Vorlage für die Wiederherstellung **start-restore-job** in einem serverlosen Namespace:

```
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 Serverless \
```

```
--region Region \  
--endpoint-url URL
```

Example Beispiel für die Wiederherstellung **start-restore-job** in einem serverlosen Namespace:

```
aws backup start-restore-job \  
--recovery-point-arn "arn:aws:redshift-serverless:us-east-1:123456789012:snapshot/  
a12bc34d-567e-890f-123g-h4ijk56l78m9" \  
--iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \  
--metadata 'RestoreType=NAMESPACE_RESTORE,NamespaceIdentifier=redshift-namespace-1-  
restore' \  
--resource-type "RedshiftServerless" \  
--region us-west-2
```

Verwenden Sie nach dem Start des Wiederherstellungsauftrags, `describe-restore-job` um den Fortschritt zu überwachen.

Stellen Sie eine SAP HANA-Datenbank auf einer EC2 Amazon-Instance wieder her

SAP HANA-Datenbanken auf EC2 Instances können mithilfe der AWS Backup Konsole, mithilfe der API oder mithilfe von wiederhergestellt werden AWS CLI.

Themen

- [Stellen Sie eine SAP HANA-Datenbank mit der AWS Backup Konsole wieder her](#)
- [StartRestoreJob API für SAP HANA auf EC2](#)
- [CLI für SAP HANA auf EC2](#)
- [Wiederherstellung mit hoher Verfügbarkeit \(HA\) von SAP HANA](#)
- [Fehlerbehebung](#)

Stellen Sie eine SAP HANA-Datenbank mit der AWS Backup Konsole wieder her

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 EC2Instanz der Zieldatenbank sehen.
5. Optional können Sie Erweiterte Wiederherstellungseinstellungen erweitern, um Ihre Option für die Katalogwiederherstellung zu ändern. Die verfügbaren Optionen variieren je nach den ausgewählten Wiederherstellungseinstellungen.

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.

IdempotencyToken Eine 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 on EC2 Amazon-Instance wiederherzustellen. Informationen zu SAP HANA-spezifischen Elementen finden Sie unter [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 Ressourcenamen, 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 bestimmte Metadaten angeben, um eine SAP HANA on EC2 Amazon-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 der EC2 SAP-HANA-on-Amazon-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 Instanz 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 Job 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.

Wiederherstellung mit hoher Verfügbarkeit (HA) von SAP HANA

Bei der Wiederherstellung eines Hochverfügbarkeitssystems (HA) von SAP HANA sind wichtige Überlegungen und zusätzliche Schritte zu berücksichtigen. Erweitern Sie den Abschnitt unten, der Ihrem Anwendungsfall am besten entspricht.

Szenario wiederherstellen:

Systemdatenbank zu einem SAP HANA HA-Ziel

Bevor Sie die Wiederherstellung auf das SAP HANA HA-Zielsystem (Ziel) durchführen,

1. Wenn ein Cluster installiert ist, versetzen Sie alle Clusternotizen in den Wartungsmodus.
2. Stoppen Sie die SAP HANA-Datenbank auf allen Knoten, einschließlich primärer und sekundärer Knoten.
3. (Empfohlen) Deaktivieren Sie alle Sicherungspläne, um sicherzustellen, dass sie den Wiederherstellungsvorgang nicht beeinträchtigen.

Gehen Sie nach Abschluss des Wiederherstellungsauftrags zum wiederhergestellten SAP HANA HA-System und gehen Sie dann wie folgt vor:

1. Starten Sie die SAP HANA-Datenbank im Primärmodus.
2. Starten Sie manuell jede Tenant-Datenbank, in der die Systemdatenbank wiederhergestellt wurde, ihre Mandanten jedoch nicht wiederhergestellt wurden.
3. Stellen Sie die SAP HANA-Systemreplikation (HSR) zwischen dem primären und dem sekundären Knoten wieder her.
4. Starten Sie die SAP HANA-Datenbank auf dem sekundären Knoten.
5. Wenn ein Cluster installiert ist, stellen Sie sicher, dass alle Clusterknoten online sind.
6. Aktivieren Sie alle Sicherungspläne, die Sie vor dem Wiederherstellungsvorgang deaktiviert haben.

(Optional) Sie können die Anwendung auf [AWS Systems Manager for SAP](#) synchronisieren, indem Sie sie aufrufen [StartApplicationRefresh](#), oder Sie können auf die geplante Anwendungsaktualisierung warten, die die neuesten SAP-Metadaten bereitstellt.

Systemdatenbank zu einem SAP HANA-Einzelknoten-Ziel

Bevor Sie mit der Wiederherstellung beginnen, wechseln Sie zum Zielsystem SAP HANA mit einem Knoten und gehen dann wie folgt vor:

1. Stoppen Sie die SAP HANA-Datenbank auf dem SAP HANA-Zielsystem.
2. (Empfohlen) Deaktivieren Sie alle Sicherungspläne, um sicherzustellen, dass sie den Wiederherstellungsvorgang nicht beeinträchtigen.

Gehen Sie nach Abschluss des Wiederherstellungsauftrags zum SAP HANA-Zielsystem mit einem Knoten und gehen Sie dann wie folgt vor:

1. Starten Sie SAP HANA auf dem SAP HANA-Zielsystem.

2. Starten Sie jede Tenant-Datenbank manuell auf dem Zielknoten.
3. Aktivieren Sie alle Backup-Pläne, die Sie vor dem Wiederherstellungsvorgang deaktiviert haben.

(Optional) Sie können die Anwendung auf [AWS Systems Manager for SAP](#) synchronisieren, indem Sie sie aufrufen [StartApplicationRefresh](#), oder Sie können auf die geplante Anwendungsaktualisierung warten, die die neuesten SAP-Metadaten bereitstellt.

Mandantendatenbank (direkt oder Systemkopie)

Bevor Sie einen Wiederherstellungsauftrag starten, gehen Sie zum SAP HANA-Zielsystem und gehen Sie dann wie folgt vor:

1. (Optional, aber empfohlen) Versetzen Sie alle installierten Cluster in den Wartungsmodus, um eine unerwartete Übernahme während des Wiederherstellungsvorgangs zu vermeiden.
2. Stellen Sie sicher, dass die Systemdatenbank auf dem SAP HANA-Zielsystem läuft.
3. (Empfohlen) Deaktivieren Sie alle Sicherungspläne, um sicherzustellen, dass sie den Wiederherstellungsvorgang nicht beeinträchtigen.

Nach Abschluss des Wiederherstellungsauftrags:

- Aktivieren Sie alle Sicherungspläne, die Sie vor dem Wiederherstellungsvorgang deaktiviert haben.

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, die Sicherung durchzuführen, 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 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: Bei der Wiederherstellung einer Tenant-Datenbank auf einem SAP HANA-Hochverfügbarkeitssystem ist ein Problem aufgetreten: `b* -10709: Connection failed (RTE:[89006] System call 'connect' failed, rc=111:Connection refused (:::1]:40404 # localhost:30013))\n`

Lösung: Überprüfen Sie SAP HANA, um sicherzustellen, dass die SYSTEMDB betriebsbereit ist.

- Fehler: `b'* 448: recovery could not be completed: [301102] exception 301153: Sending root key to secondary failed: connection refused. This may be caused by a stopped system replication secondary. Please keep the secondary online to receive the restored root key. Alternatively you could unregister the secondary site in case of an urgent recovery.\n SQLSTATE: HY000\n'`

Lösung: Auf einem SAP HANA-Hochverfügbarkeitssystem wird SAP HANA möglicherweise nicht auf dem sekundären Knoten ausgeführt, während ein aktiver Wiederherstellungsvorgang ausgeführt wird. Starten Sie SAP HANA auf dem sekundären Knoten und wiederholen Sie dann den Wiederherstellungsauftrag erneut.

- 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](#).

Stellen Sie S3-Daten wieder her mit AWS Backup

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

- Wenn wir während des Backups aktiviert ACLs wurden, muss der Ziel-Bucket für die Wiederherstellung ACLs aktiviert worden sein. Andernfalls schlägt der Wiederherstellungsauftrag fehl.
- Wenn Block Public Access im Ziel-Bucket aktiviert ist, wird der Wiederherstellungsauftrag erfolgreich abgeschlossen, Objekte mit dem Status public ACLs werden jedoch nicht wiederhergestellt.
- Wiederherstellungen von Objekten werden übersprungen, wenn der Ziel-Bucket ein Objekt mit demselben Namen oder derselben Versions-ID enthält.
- 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.

Wiederherstellung ACLs und Objekt-Tags

Bei der Wiederherstellung von Amazon S3 S3-Daten wählen Sie aus, ob ACLs sie Teil der Wiederherstellung sind.

Wenn sie im Wiederherstellungspunkt verfügbar ACLs sind, wählen Sie ACLs mit der ACLs Einstellung Wiederherstellen aus, ob sie wiederhergestellt oder ausgeschlossen werden sollen. Wenn ACLs sie nicht im Backup enthalten sind, können sie unabhängig von der Einstellung nicht wiederhergestellt werden. Wenn Sie versuchen, einen Wiederherstellungsauftrag mit ACLs aktivierter Option zu erstellen, diese aber nicht Teil des Backups waren, wird möglicherweise ein Fehler angezeigt, wie `Unable to restore Access Control Lists (ACLs) for bucket because backup was created with the 'BackupACLs' option disabled. Please proceed with restoring without ACLs`.

Objekt-Tags werden automatisch wiederhergestellt, wenn sie in der ursprünglichen Sicherung enthalten waren

Note

Wiederherstellungspunkte wiederherstellen ohne ACLs

Wenn AWS CLI Sie versuchen, ACLs aus einer Sicherung wiederherzustellen, die ausgeschlossen wurde ACLs, schlägt der Wiederherstellungsvorgang fehl und es wird eine Fehlermeldung angezeigt, die auf ungültige Wiederherstellungsparameter hinweist.

Stellen Sie mehrere Versionen wieder her

AWS Backup Stellt standardmäßig nur die neueste Version Ihrer Objekte wieder her. Sie haben die Wahl, ob Sie weitere oder alle Versionen der Objekte wiederherstellen möchten.

In Schritt 6 des folgenden Abschnitts erfahren Sie, wie Sie die 10 neuesten Versionen oder alle Versionen mithilfe der AWS Backup Konsole wiederherstellen können.

Weitere Informationen [???](#) zu Metadaten, die bei der programmgesteuerten Wiederherstellung berücksichtigt werden müssen, finden Sie weiter unten auf dieser Seite.

Wiederherstellung über die Konsole AWS Backup

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 „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 zum S3-Bucket URIs finden Sie unter [Methoden für den Zugriff auf einen Bucket](#) im Amazon Simple Storage Service-Benutzerhandbuch.)

- b. Wählen Sie Objekt hinzufügen, um ein anderes Element für die Wiederherstellung anzugeben.
6. Standardmäßig wird nur die neueste Version eines Objekts wiederhergestellt. Sie können bis zu den letzten 10 Versionen oder alle Versionen der Objekte wiederherstellen. Wählen Sie Ihre Präferenz aus dem Drop-down-Menü aus.
7. 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 Menü aus, das alle vorhandenen Buckets in Ihrer aktuellen AWS Region anzeigt.
- b. Wenn Sie Neuen Bucket erstellen wählen, geben Sie den neuen Bucket-Namen ein. Nachdem der Bucket erstellt wurde, können Sie die Standardeinstellungen für BPA (Block Public Access) und S3-Versionierung ändern.
8. Für die Verschlüsselung von Objekten in Ihrem S3-Bucket können Sie Ihre Verschlüsselung für wiederhergestellte Objekte wählen. 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.
9. Wählen Sie im Bereich Rolle wiederherstellen die IAM-Rolle aus, die AWS Backup für diese Wiederherstellung annimmt.
10. Wählen Sie Restore backup aus. Der Bereich Aufträge wiederherstellen wird angezeigt. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsauftrag.

Stellen Sie Amazon S3 S3-Wiederherstellungspunkte wieder her über AWS CLI

Verwenden Sie [StartRestoreJob](#). Sie können bei Amazon-S3-Wiederherstellungen die folgenden Metadaten angeben:

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.

// Optional metadata:
RestoreACLs // Boolean. If ACLs were part of the backup, include and set to TRUE. If
the backup
does not include ACLs and this parameter is included, set to FALSE.
EncryptionType // The type of encryption to encrypt your restored objects. Options
are original (same encryption as the original object), SSE-S3, or SSE-KMS).
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
required for item-level restore.
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
```

```
RestoreLatestVersionsUpTo // Include this optional parameter to multiple versions.  
RestoreTime // The restore time (only valid for continuous recovery points where it is  
required, in format 2021-11-27T03:30:27Z).
```

`RestoreLatestVersionsUpTo` ist ein optionales Schlüssel-Wert-Paar für Metadaten. Standardmäßig oder wenn dies weggelassen wird, wird die neueste Version wiederhergestellt. Fügen Sie diese Metadaten hinzu, um zusätzliche Versionen Ihrer Objekte wiederherzustellen. Zulässige Werte sind:

- `1` (um die neueste Version wiederherzustellen)
- `n`, wobei `n` eine beliebige positive Ganzzahl größer als 1 ist. Die neuesten `n` Versionen Ihrer Objekte werden wiederhergestellt. Wenn die tatsächliche Versionsanzahl eines Objekts weniger als `n` beträgt, wird diese Anzahl von Versionen für dieses Objekt wiederhergestellt.
- `all` (um alle Versionen wiederherzustellen)

Status des Wiederherstellungspunkts

Bei den Wiederherstellungspunkten wird der jeweilige Status angezeigt.

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.

S3-Wiederherstellungsnachrichten

Wenn ein Wiederherstellungsauftrag abgeschlossen ist oder fehlschlägt, wird möglicherweise die folgende Meldung angezeigt. Anhand der folgenden Tabelle können Sie die mögliche Ursache für die Statusmeldung ermitteln.

Szenario	Aufgabenstatus	Fehlermeldung	Beispiel
Alle Objekte konnten nicht wiederhergestellt werden.	FAILED	„Es wurden keine Objekte von <i>RecoveryPoint</i> bis wiederhergestellt <i>bucket</i> . Um über diese Fehler informiert zu werden, aktivieren Sie SNS-Ereignisbenachrichtigungen.“	Die Rolle, die zum Starten des Wiederherstellungsauftrags verwendet wurde, ist nicht berechtigt, Objekte in den Ziel-Bucket zu legen. Die Wiederherstellungsrolle ist nicht berechtigt, zu überprüfen, ob die Objektversion im Ziel-Bucket vorhanden ist.
Ein oder mehrere (aber nicht alle) Objekte konnten nicht wiederhergestellt werden.	COMPLETED	„Ein oder mehrere Objekte konnten von <i>RecoveryPoint</i> bis nicht wiederhergestellt werden <i>bucket</i> . Um über diese Fehler informiert zu werden, aktivieren Sie SNS-Ereignisbenachrichtigungen.“	Die Rolle, die zum Starten des Wiederherstellungsauftrags verwendet wurde, hat keinen Zugriff auf den KMS-Schlüssel, der von einem oder mehreren der ursprünglichen Objekte verwendet wurde.
Es sind keine wiederherzustellen	COMPLETED	„Es gibt keine Objekte, die	Der Wiederherstellungspunkt

Szenario	Aufgabenstatus	Fehlermeldung	Beispiel
den Objekte vorhanden.		der Wiederherstellungsanforderung entsprechen <i>RecoveryPointNotARN</i> .“	(Backup) des wiederherzustellen den Quell-Buckets enthält keine Objekte. Das für den Wiederherstellungsauftrag verwendet e Präfix entspricht keinem Objekt.

Ein Storage Gateway Gateway-Volume wiederherstellen

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-Tabelle mithilfe der AWS Backup -Konsole wieder her

Sie können Timestream-Tabellen in der AWS Backup Konsole wiederherstellen, die von AWS Backup erstellt wurden.

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,MemoryStoreWrites=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
```

Stellen Sie eine virtuelle Maschine wieder her 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 EC2 Amazon-Instance](#) wiederherstellen. Für das Wiederherstellen (oder Migrieren) einer virtuellen Maschine EC2 ist eine Lizenz erforderlich. Standardmäßig ist eine Lizenz enthalten (es fallen Gebühren an). AWS Weitere Informationen finden Sie unter [Lizenzoptionen](#) im Import/Export VM-Benutzerhandbuch.

Sie können eine VMware virtuelle 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 bei der Wiederherstellung einer VM auf einer EC2 Amazon-Instance](#)

- [Verwenden Sie die AWS Backup Konsole, um die Wiederherstellungspunkte virtueller Maschinen wiederherzustellen](#)
- [Wird AWS CLI zum Wiederherstellen von Wiederherstellungspunkten für virtuelle Maschinen verwendet](#)

Überlegungen bei der Wiederherstellung einer VM auf einer EC2 Amazon-Instance

- Für das Wiederherstellen (oder Migrieren) einer virtuellen Maschine EC2 ist eine Lizenz erforderlich. Standardmäßig beinhaltet eine AWS Lizenz (es fallen Gebühren an). Weitere Informationen finden Sie unter [Lizenzoptionen](#) im Import/Export VM-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 EC2 Amazon-Benutzerhandbuch beschrieben) ein key pair hinzufügen.
- Vergewissern Sie [sich EC2 im Import/Export VM-Benutzerhandbuch, dass Ihr Betriebssystem für den Import zu und Export von Amazon unterstützt](#) wird.
- Lesen Sie die Einschränkungen im [Zusammenhang mit dem Import VMs zu Amazon EC2](#) im Import/Export VM-Benutzerhandbuch.
- Wenn Sie mithilfe von einer EC2 Amazon-Instance wiederherstellen AWS CLI, müssen Sie Folgendes angeben `"RestoreTo": "EC2Instance"`. Alle anderen Attribute haben Standardwerte.
- EC2 Amazon-Angebote [EC2 erlaubt AMIs](#). Wenn diese Einstellung in Ihrem Konto aktiviert ist, fügen Sie den Alias `aws-backup-vault` zu Ihrer Zulassungsliste hinzu. Andernfalls schlagen Wiederherstellungsvorgänge von VM-Wiederherstellungspunkten auf EC2 Instanzen fehl und es wird eine Fehlermeldung wie „Source AMI not found in Region“ angezeigt.

Verwenden Sie die AWS Backup Konsole, um die Wiederherstellungspunkte virtueller Maschinen 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

- [Wiederherstellen auf VMware](#)
- [Auf einem Amazon EBS-Volume wiederherstellen](#)
- [Auf einer EC2 Amazon-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 VMware lauten 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 finden Sie unter [Wie verwende ich LVM, um ein logisches Volume auf der Partition eines Amazon EBS-Volumes zu erstellen?](#) um mehr darüber zu erfahren, wie Sie verwaltete Volumes bereitstellen und auf Daten auf dem wiederhergestellten Amazon EBS-Volume zugreifen können.

So stellen Sie eine virtuelle Maschine auf einer EC2 Amazon-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 als Speicherort für die Wiederherstellung aus EC2.
6. Wählen Sie als Instance-Typ 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 auf 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
NetworkInterfaces

```

Sie können die folgenden Metadaten für die Wiederherstellung einer virtuellen Maschine in VMware, VMware Cloud on AWS und VMware Cloud on AWS Outpost angeben:

```

RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore

```

Dieses Beispiel zeigt, wie eine vollständige Wiederherstellung durchgeführt wird auf VMware:

```

'{"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"}'

```

Testen wiederherstellen

Wiederherstellungstests, eine von angebotene Funktion AWS Backup, ermöglichen eine automatische und regelmäßige Bewertung der Durchführbarkeit von Wiederherstellungen sowie die Überwachung der Dauer von Wiederherstellungsaufträgen.

Inhalt

- [Übersicht](#)
- [Wiederherstellungstests im Vergleich zum Wiederherstellungsprozess](#)
- [Verwaltung von Wiederherstellungstests](#)
- [Erstellen eines Wiederherstellungstestplans](#)
- [Aktualisieren eines Wiederherstellungstestplans](#)
- [Anzeigen bestehender Wiederherstellungstestpläne](#)
- [Anzeigen von Wiederherstellungstestaufträgen](#)
- [Löschen eines Wiederherstellungstestplans](#)
- [Prüfung eines Wiederherstellungstests](#)
- [Kontingente und Parameter für Wiederherstellungstests](#)
- [Fehler beim Wiederherstellen, Testen und Beheben von Fehlern](#)
- [Abgeleitete Metadaten bei Wiederherstellungstests](#)
- [Die Testvalidierung wiederherstellen](#)

Übersicht

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, [Die Testvalidierung wiederherstellen](#) um die Ergebnisse des Wiederherstellungstests zu bestätigen.

Sobald die optionale Überprüfung abgeschlossen ist oder das Validierungsfenster geschlossen wird, werden die am Wiederherstellungstest beteiligten Ressourcen AWS Backup gelöscht, und die Ressourcen werden entsprechend dem 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	Wiederherstellen
Account	Es wird empfohlen, ein Konto festzulegen, das für Wiederherstellungstests verwendet werden soll	Sie können Ressourcen von einem Konto aus wiederherstellen
AWS Backup Audit Manager	Kann ein Steuerelement aktivieren, um zu bestätigen, ob ein Wiederherstellungstest die angegebenen Wiederherstellungsziele erfüllt	
Kadenz	Regelmäßig als Teil eines geplanten Plans.	On-Demand
Ressourcen	Zu den Ressourcentypen, die Sie Ihrem Testplan zuweisen können, gehören: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon, Amazon EC2, Amazon FSx (Lustre, ONTAP,	Alle Ressourcen können wiederhergestellt werden.

	Wiederherstellungstests	Wiederherstellen
	OpenZFS, Windows), Amazon Neptune, Amazon RDS und Amazon S3.	
Ergebnisse	Nach Abschluss des Wiederherstellungstests wird die wiederhergestellte Ressource gelöscht, sobald das Fenster geschlossen ist. Die Testvalidierung wiederherstellen	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 Wiederherstellungstestplan 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 `beginntawsbackup-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-plansie](#) zuerst. Nachdem Sie eine erfolgreiche Antwort erhalten haben und der Plan erstellt wurde,

verwenden Sie für jeden Ressourcentyp [create-restore-testing-selection](#), den Sie in Ihren Plan aufnehmen möchten.

Wenn Sie einen Testplan für die Wiederherstellung erstellen, erstellen wir für Sie eine Rolle, die mit dem Service verknüpft ist. Weitere Informationen finden Sie unter [Rollen für Wiederherstellungstests verwenden](#).

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. General
 - 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) gibt den Zeitraum an, 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 Wiederherstellungsbereich 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. **Point-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. General

- 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 [AWSBackupServiceRolePolicyForRestores](#) 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, FSx Amazon-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 über eine oder mehrere geschützte Ressourcen ARNs oder über eine oder mehrere Bedingungen verfügen, aber sie kann nicht beides 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:

 Note

`RestoreTestingSelectionName` Anforderungen an die Benennung:

- Muss zwischen 1 und 256 Zeichen lang sein
- Kann Buchstaben (a-z, A-Z), Zahlen (0-9), Bindestriche (-) und Unterstriche (_) enthalten
- Muss mit einem Buchstaben oder einer Zahl beginnen
- Kann nicht mit einem Bindestrich oder Unterstrich enden
- Muss innerhalb des Wiederherstellungstestplans eindeutig sein

- `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 geschützte Ressourcen ARNs einbeziehen `ProtectedResourceArns`.

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). Um das zu tun,

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 [UpdateRestoreTestingPlan](#) und [UpdateRestoreTestingSelection](#) kann 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.

Bevor Sie eine Aktualisierungsanfrage senden, verwenden Sie [GetRestoreTestingPlan](#) und [GetRestoreTestingSelection](#) um festzustellen, ob Ihre Anfrage bestimmte RestoreTestingSelection enthält ARNs oder ob sie den Platzhalter und die Bedingungen verwendet.

Wenn in Ihrer Auswahl für den Wiederherstellungstest ein Platzhalter ARNs (anstelle eines Platzhalters) angegeben wurde und Sie ihn in einen Platzhalter mit Bedingungen ändern möchten, muss die Aktualisierungsanforderung sowohl den ARN-Platzhalter als auch die Bedingungen enthalten. Eine Auswahl kann entweder eine geschützte Ressource enthalten ARNs 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 [Die Testvalidierung wiederherstellen](#) 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 [DeleteRestoreTestingSelection](#) kann 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, [DeleteRestoreTestingPlan](#) um 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 geschützte Ressourcen ARNs 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](#).

Fehler beim Wiederherstellen, Testen und Beheben von Fehlern

Wenn Sie über Wiederherstellungstestaufträge mit dem Wiederherstellungsstatus von `verfügenFailed`, 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](#) SubnetId Sie den 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](#) DBSubnetGroupName Sie den 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 der Wiederherstellungsrolle den Zugriff darauf.

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) kein vollständiger Satz von Metadaten abgeleitet werden kann. AWS Backup

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 AWS Backup Konsole nicht verfügbar.

Jede unterstützte Ressource verfügt sowohl über abgeleitete Schlüssel und Werte für Wiederherstellungsmetadaten als auch über überschreibbare Schlüssel für Wiederherstellungsmetadaten. Nur `RestoreMetadataOverrides` Schlüssel-Wert-Paare oder verschachtelte Schlüssel-Wert-Paare, die mit gekennzeichnet *required for successful restore* sind, müssen eingeschlossen werden; 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 EC2 Amazon-Instance oder ein Amazon RDS-Cluster, die auf der Standard-VPC wiederhergestellt wurden. 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	encryptionType kmsMasterKeyArn

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
	awsbackup-restore-test- beginnt	
Amazon EBS	availabilityZone , dessen Wert auf eine zufällige Availability Zone gesetzt ist encrypted , dessen Wert auf true gesetzt ist	availabilityZone iops kmsKeyId throughput volumesize volumetype
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 (null oder) UseBackedUpValue instanceType requireImdsV2 securityGroupIds subnetId

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon EFS	Der <code>encrypted</code> -Wert ist auf <code>true</code> gesetzt Der <code>file-system-id</code> -Wert ist auf die Dateisystem-ID des wiederherzustellenden Wiederherstellungspunkts gesetzt <code>kmsKeyId</code> value wird auf <code>alias/aws/elasticfilesystem</code> gesetzt Der <code>newFileSystem</code> -Wert ist auf <code>true</code> gesetzt Der <code>performanceMode</code> -Wert ist auf <code>generalPurpose</code> gesetzt	<code>kmsKeyId</code> <code>performanceMode</code>
Amazon FSx für Lustre	<code>lustreConfiguration</code> hat verschachtelte Schlüssel. Ein verschachtelter Schlüssel ist <code>automaticBackupRetentionDays</code> , dessen Wert auf <code>0</code> gesetzt ist	<code>kmsKeyId</code> <code>lustreConfiguration</code> hat den verschachtelten Schlüssel <code>logConfiguration</code> <code>securityGroupIds</code> <code>subnetIds</code> , <i>required for successful restore</i>

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon FSx für NetApp ONTAP	name ist auf einen zufälligen Wert gesetzt, der mit <code>awsbackup_restore_test_</code> beginnt ontapConfiguration hat verschachtelte Schlüssel, darunter: • <code>junctionPath</code> , wobei <code>/name</code> der Name des wiederherzustellenden Volumes ist • <code>sizeInMegabytes</code> , dessen Wert auf die Größe des wiederherzustellenden Wiederherstellungspunkts in Megabyte festgelegt ist • <code>snapshotPolicy</code> , wobei der Wert auf <code>none</code> gesetzt ist	ontapConfiguration hat bestimmte verschachtelte Schlüssel, die überschrieben werden können, darunter: • <code>junctionPath</code> • <code>ontapVolumeType</code> • <code>securityStyle</code> • <code>sizeInMegabytes</code> • <code>storageEfficiencyEnabled</code> • <code>storageVirtualMachineId</code> , <i>required for successful restore</i> • <code>tieringPolicy</code>

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon FSx für OpenZFS	<code>openZfsConfiguration</code> , das über verschachtelte Schlüssel verfügt, darunter: • <code>automaticBackupRetentionDays</code> mit dem Wert auf 0 • <code>deploymentType</code> , wobei der Wert auf den Bereitstellungstyp des wiederherzustellenden Wiederherstellungspunkts gesetzt ist • <code>throughputCapacity</code> , dessen Wert auf dem <code>deploymentType</code> basiert. Wenn <code>deploymentType</code> <code>SINGLE_AZ_1</code> ist, wird der Wert auf 64 gesetzt; wenn <code>deploymentType</code> <code>SINGLE_AZ_2</code> or <code>MULTI_AZ_1</code> ist, wird der Wert auf 160 gesetzt	<code>kmsKeyId</code> <code>openZfsConfiguration</code> hat bestimmte verschachtelte Schlüssel, die überschrieben werden können, darunter: • <code>deploymentType</code> • <code>throughputCapacity</code> • <code>diskiopsConfiguration</code> <code>securityGroupIds</code> <code>subnetIds</code>

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon FSx für Windows-Dateiserver	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 <i>required for successful restore</i> windowsConfiguration , mit bestimmten verschachtelten Schlüsseln, die überschreibbar sind • throughputCapacity • activeDirectoryId <i>required for successful restore</i> • preferredSubnetId

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon-RDS-, Aurora-, Amazon-DocumentDB- und Amazon-Neptune-Cluster	<code>availabilityZones</code> , wobei der Wert auf eine Liste von bis zu drei zufälligen Availability Zones gesetzt ist <code>dbClusterIdentifier</code> mit einem zufälligen Wert, der mit <code>awsbackup-restore-test</code> beginnt <code>engine</code>, wobei der Wert auf die Engine des wiederherzustellenden Wiederherstellungspunkts gesetzt ist	<code>availabilityZones</code> <code>databaseName</code> <code>dbClusterParameterGroupName</code> <code>dbSubnetGroupName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>engine</code> <code>engineMode</code> <code>engineVersion</code> <code>kmskeyId</code> <code>port</code> <code>optionGroupName</code> <code>scalingConfiguration</code> <code>vpcSecurityGroupIds</code>

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon-RDS-Instances	<code>dbInstanceIdentifier</code> mit einem zufälligen Wert, der mit <code>awsbackup-restore-test-</code> beginnt <code>deletionProtection</code> mit dem Wert auf <code>false</code> <code>multiAz</code> mit dem Wert auf <code>false</code> <code>publiclyAccessible</code> , wobei der Wert auf „false“ gesetzt ist	<code>allocatedStorage</code> <code>availabilityZones</code> <code>dbInstanceClass</code> <code>dbName</code> <code>dbParameterGroupName</code> <code>dbSubnetGroupName</code> <code>domain</code> <code>domainIamRoleName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>iops</code> <code>licensemodel</code> <code>multiAz</code> <code>optionGroupName</code> <code>port</code> <code>processorFeatures</code> <code>publiclyAccessible</code> <code>storageType</code>

Ressourcentyp	Schlüssel und Werte für abgeleitete Wiederherstellungsmetadaten	Überschreibbare Metadaten
Amazon Simple Storage Service (Amazon-S3)	<code>destinationBucketName</code> mit einem zufälligen Wert, der mit <code>awsbackup-restore-test-</code> beginnt <code>encrypted</code> mit dem Wert auf <code>true</code> <code>encryptionType</code> mit dem Wert auf <code>SSE-S3</code> <code>newBucket</code> mit dem Wert auf <code>true</code>	<code>vpcSecurityGroupIds</code> <code>encryptionType</code> <code>kmsKey</code>

Die Testvalidierung wiederherstellen

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 in der [AWS Backup Konsole](#) ein Validierungsstatus 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 EC2 Amazon-Instance enthält, können Sie Code hinzufügen, der einen Healthcheck-Endpoint anpingt.

Sie können anhand der Details des Ereignisses bestimmen, welche Ressource (n) validiert werden sollen.

Sie können [Lambda-Ebenen](#) verwenden, um das neueste SDK zu verwenden (da `PutRestoreValidationResult` es 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.

Beenden Sie einen Backup-Job

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-Managementkonsole 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).

Bestehende Backups anzeigen

Sie können eine Liste Ihrer Backups über die [AWS Backup Konsole](#) oder programmgesteuert anzeigen.

Themen

- [Auflisten von Backups nach geschützter Ressource in der Konsole](#)
- [Auflisten von Backups nach Backup-Tresor in der Konsole](#)
- [Programmgesteuertes Auflisten von Backups](#)

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 AWS-Managementkonsole/backup an https://console.aws.amazon.com und öffnen Sie die AWS Backup Konsole.](#)
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 EC2 Amazon-Instance in einem laufenden Zustand ausgewertet. Eine EC2 Instance, die sich im Status „Gestoppt“ befindet, wird nicht in die Compliance-Bewertung 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](#)
- [Arbeiten mit Auditberichten](#)
- [Verwenden von AWS Backup Audit Manager mit CloudFormation](#)
- [Verwenden von AWS Backup Audit Manager mit AWS Audit Manager](#)
- [Steuerelemente und Abhilfemaßnahmen](#)

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](#)
- [Aktivieren der Ressourcennachverfolgung](#)
- [Erstellen von Frameworks mithilfe der AWS Backup -Konsole](#)
- [Frameworks mithilfe der AWS Backup API erstellen](#)
- [Anzeigen des Framework-Compliance-Status](#)
- [Suchen nicht konformer Ressourcen](#)
- [Aktualisieren von Audit-Frameworks](#)
- [Löschen von Audit-Frameworks](#)

Auswählen Ihrer Kontrollen

In der folgenden Tabelle sind die AWS Backup Audit Manager Manager-Steuerelemente, ihre anpassbaren Parameter und ihre AWS Config Aufzeichnungsressourcentypen aufgeführt.

Verfügbare Kontrollen

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
Backup-Ressourcen sind in mindestens einem Backup-Plan enthalten	Prüft, ob Ressourcen in mindestens einem Backup-Plan enthalten sind.	Keine	AWS Backup: backup selection
Backup-Plan hat eine Mindestfrequenz	Prüft, ob die Backup-Frequenz mindestens [1 Tag] und der	Backup-Frequenz; Aufbewahrungszeitraum	AWS Backup: backup plans

Name der Kontrolle	Beschreibung der Kontrolle	Anpassbare Parameter	AWS Config Art der Aufzeichnungsressource
und einen Mindestaufbewahrungszeitraum.	Aufbewahrungszeitraum mindestens [35 Tage] beträgt.		
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.	Keine	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
Ressourcen befinden sich in einem Backup-Plan mit AWS Backup Vault Lock	Prüft, ob für eine Ressource ein Backup-Plan 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 Wiederherstellungsauftrag innerhalb der Zielwiederherstellungszeit abgeschlossen wurde	Wert in Minuten	Keine
Ressourcen befinden sich in einem Tresor mit logischem Air-Gap	Prüft, ob für Ressourcen innerhalb des angegebenen Werts und Zeitrahmens mindestens ein Wiederherstellungspunkt in einen Tresor mit logischem Air-Gap kopiert wurde.	Wert in Minuten, Stunden oder Tagen	AWS Backup: recovery points

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 [Feature-Verfügbarkeit 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 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

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 Ressourcenverfolgung bereits aktiviert. Sie müssen den Rest dieses Verfahrens nicht abschließen, um AWS Backup Audit Manager zu verwenden.

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']"
```

3. Beschreiben Sie Ihren AWS Config Rekorder.

```
$ aws configservice describe-configuration-records
```

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"
        ]
      }
    }
  ]
}
```

4. Erstellen Sie einen Amazon S3 S3-Bucket als Ziel zum Speichern der AWS Config Konfigurationsdateien.

```
$ aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

5. Verwenden Sie diese *policy.json* Option, um die AWS Config Erlaubnis für den Zugriff auf Ihren Bucket zu erteilen. Sehen Sie sich das folgende Beispiel an *policy.json*.

```
$ aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json
```

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      }
    }
  ]
}
```

```

    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  },
  {
    "Sid": "AWSConfigBucketExistenceCheck",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  },
  {
    "Sid": "AWSConfigBucketDelivery",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  }
]
}

```

6. Konfigurieren Sie Ihren Bucket als AWS Config Lieferkanal

```

$ aws configservice put-delivery-channel --delivery-channel
name=default,s3BucketName=amzn-s3-demo-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 CloudFormation -Vorlage

Eine CloudFormation Vorlage, die die Ressourcenverfolgung aktiviert, finden Sie unter [AWS Backup Audit Manager verwenden mit 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.

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Backup resources are included in at least one backup plan	<pre>{ "FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": { "key1": "foo" } }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Backup plan minimum frequency and minimum retention	<pre> {"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_F REQUENCY_AND_MIN_R ETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "required RetentionDays", "ParameterValue": "35"}, {"ParameterName": "required FrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "required FrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }]], </pre>	<pre> {"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us -east-1:1234567890 12:framework/Contr ol2-de7655ae-1e31- 45cb-96a0-4f43d8c1 969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_F REQUENCY_AND_MIN_R ETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "required RetentionDays", "ParameterValue": "35"}, {"ParameterName": "required FrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "required FrequencyValue", "ParameterValue": "24"}], "ControlScope": { </pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework - Antwort
	<pre>"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>	<pre> "Tags": {"key1": "prod"} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Vaults prevent manual deletion of recovery points	<pre>{ "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/RDAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:role/service-role/QuickSightAction" }], "ControlScope": { "ComplianceResourceIds": ["default"], </pre>	<pre>{ "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/RDAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:r</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
	<pre>"ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"], "ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework - Antwort
Minimum retention established for recovery point	<pre>{ "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" } }</pre>	<pre>{ "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": {} }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework - Antwort
		<pre>{ "key1": "foo" } }</pre>

Backup recovery points are encrypted

```
{ "FrameworkName":
  "Control5",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls":
    [
      { "ControlName":
        "BACKUP_RECOVERY_POINT_ENCRYPTED",
        "ControlInputParameters":
          [],
        "ControlScope":
          {} // Default scope (no scope input) is all recovery points
        }
    ],
  "IdempotencyToken":
    "Control5",
  "FrameworkTags":
    { "key1": "foo" }
}
```

```
{ "FrameworkName":
  "Control5",
  "FrameworkArn":
    "arn:aws:backup:us-east-1:123456789012:framework/Control7-7e7655ae-1e31-45cb-96a0-4f43d8c19642",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls":
    [
      { "ControlName":
        "BACKUP_RECOVERY_POINT_ENCRYPTED",
        "ControlInputParameters":
          [],
        "ControlScope": {}
      }
    ],
  "CreationTime":
    1516925490,
  "DeploymentStatus":
    "Active",
  "FrameworkStatus":
    "Completed",
  "IdempotencyToken":
    "Control5",
  "FrameworkTags":
    { "key1": "foo" }
}
```

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Cross-Region backup copy is scheduled	<pre> {"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"} } </pre>	<pre> {"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"} } </pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Cross-account backup copy is scheduled	<pre>{ "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" } }</pre>	<pre>{ "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" } }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Resources are in a backup plan with an AWS Backup Vault Lock	<pre> {"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_ PROTECTED_BY_BACKU P_VAULT_LOCK", "ControlInputParam eters":[], "ControlScope": {"Complia nceResourceTypes": ["EC2"] // Evaluate only EC2 instances } },], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} } </pre>	<pre> {"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us -east-1:1234567890 12:framework/Contr ol8-ce7655ae-1e31- 45cb-96a0-4f43d8c1 9642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_ PROTECTED_BY_BACKU P_VAULT_LOCK", "ControlInputParam eters":[], "ControlScope": {"Complia nceResourceTypes": ["EC2"] } },], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} } </pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Last recovery point was created	<pre>{ "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" } }] }</pre>	<pre>{ "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" } }] }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
Restore time for resources meet target	<pre> {"FrameworkName": "Control10", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters": [{ "ParameterName": "maxRestoreTime", "ParameterValue": "720" }], "ControlScope": { "ComplianceResourceIds": ["DynamoDB"], "ComplianceResourceTypes": ["DynamoDB"], " // Evaluates only DynamoDB databases } }], "IdempotencyToken": "Control10", "FrameworkTags": { "key1": "foo" } </pre>	<pre> {"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control10-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" } </pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework - Antwort
	<pre>}</pre>	

Steuerung	CreateFramework -Anfrage	DescribeFramework -Antwort
RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT	<pre>{ "FrameworkName": "Control11", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT", "ControlInputParameters": [{ "ParameterName": "recoveryPointAgeValue", "ParameterValue": "10" }, { "ParameterName": "recoveryPointAgeUnit", "ParameterValue": "days" }], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "IdempotencyToken": "Control11", "FrameworkTags": {</pre>	<pre>{ "FrameworkName": "Control11", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control11-ab1234cd-5e67-89fg-06a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2", "EBS"] } }], "CreationTime": 1726087776.316, "DeploymentStatus": "COMPLETED", "FrameworkStatus": "ACTIVE", "IdempotencyToken": "Control11", "FrameworkTags": { "key1": "foo" } }</pre>

Steuerung	CreateFramework -Anfrage	DescribeFramework - Antwort
	<pre> "key1": "foo" } } </pre>	

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 zwei Arten 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 Jobs und alle aktiven Jobs mit umfassendem Kontext zu Tresoreigenschaften, Backup-Plankonfigurationen und Lebenszykluseinstellungen angezeigt werden. Auftragsberichte zeigen nicht den Status `completed with issues` an. Um diesen Status zu ermitteln, 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.

Tip

Um sicherzustellen, dass die von delegierten Administratorkonten generierten Berichte alle Mitgliedskontendaten enthalten, [erstellen Sie Frameworks](#) für jedes dieser Mitgliedskonten.

Verbesserter Kontext für Jobberichte

AWS Backup Die Jobberichte von Audit Manager enthalten jetzt einen erweiterten Kontext, damit Kunden Backup-Operationen besser verstehen können, insbesondere für die Überwachung delegierter Administratorkonten in verschiedenen Organisationen.

Die erweiterten Berichte beinhalten jetzt:

- Tresorinformationen: Tresortyp, Sperrstatus und Verschlüsselungsdetails
- Kontext des Backup-Plans: Plannamen, Regelnamen, Zeitpläne und Zeitzonen
- Lebenszykluseinstellungen: Aufbewahrungszeiträume und Einstellungen für die Umstellung auf Cold Storage
- Ressourcendetails: Ressourcennamen und erweiterte Job-Metadaten

Dieser erweiterte Kontext macht zusätzliche API-Aufrufe für `DescribeBackupVault`, `DescribeBackupPlan`, `DescribeRecoveryPoint`, und überflüssig und stellt umfassende Jobinformationen in einem einzigen Bericht bereit.

Note

Der erweiterte Kontext stellt Informationen bereit, für die zuvor separate API-Aufrufe mit zusätzlichen Berechtigungen erforderlich waren. Stellen Sie sicher, dass Benutzer mit Zugriff auf diese Berichte über die entsprechenden Berechtigungen für die bereitgestellten erweiterten Informationen verfügen.

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](#)
- [Erstellen von Berichtsplänen mithilfe der AWS Backup -Konsole](#)
- [Berichtspläne mithilfe der AWS Backup API erstellen](#)
- [Erstellen von On-Demand-Berichten](#)
- [Anzeigen von Auditberichten](#)
- [Aktualisieren von Berichtsplänen](#)
- [Löschen von Berichtsplänen](#)

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 Diese Vorlagen bieten Ihnen tägliche Updates zu Ihren Sicherungs-, Wiederherstellungs- oder Kopieraufträgen mit erweitertem Kontext, einschließlich Tresoreigenschaften, Backup-Plandetails und Lebenszykluseinstellungen. Sie können diese Berichte verwenden, um Ihren Betriebsstatus zu überwachen, Backup-Konfigurationen zu verstehen 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	<pre>{ "reportItems": [{ "reportTimePeriodStart": "2021-07-14T00:00:00Z", "reportTimePeriodEnd": "2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2",</pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
	<pre> "backupJobId": "FCCB040A -9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "MyEC2Ins tance", "backupPlanArn": "arn:aws: backup:us-west-2:1122334455 66:backup-plan:349f2247-b48 9-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8- ff4e-4f1b-92e7-e13d3e65dcfb", "initiationDate": "2021-07- 14T23:53:47.229Z", "backupPlanName": "MyBackup Plan", "backupRuleName": "DailyBac kups", "backupRuleSchedule": "cron(0 5 ? * * *)", "backupRuleTimezone": "UTC", "startWindowEnd": "2021-07- 14T23:53:47.229Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "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", </pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
	<pre data-bbox="850 212 1422 961">{ "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "UNLOCKED", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/12345678-1234-1234-1234 -123456789012", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }</pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
COPY_JOB_REPORT	<pre> { "reportItems": [{ "reportTimePeriodStart": "2021-07-14T15:48:31Z", "reportTimePeriodEnd": "2021-07-15T15:48:31Z", "accountId": "112233445566", "region": "us-west-2", "copyJobId": "E0AD48A9-0560-B66 8-3EF0-941FDC0AD6B1", "jobStatus": "RUNNING", "jobRunTime": "2021-07- 16T00:00:00.010Z", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "string", "initiationDate": "2021-07- 14T15:48:31Z", "backupPlanName": "string", "backupRuleName": "string", "backupRuleSchedule": "string", "backupRuleTimezone": "string", "startWindowEnd": "2021-07- 14T15:48:31Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "creationDate": "2021-07- 15T15:42:04.771Z", "completionDate": "2021-07- 16T00:16:07.282Z", "backupSizeInBytes": 858993459 2, "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ ami-007b3819f25697299", </pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
	<pre data-bbox="847 214 1409 1159">{ "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1 12233445566:backup-vault:Default", "destinationRecoveryPointAr n": "arn:aws:ec2:us-east-2::image/ ami-0eba2199a0bcece3c", "destinationBackupVaultArn" : "arn:aws:backup:us-east-2:1 12233445566:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "string", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/...", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }</pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
RESTORE_JOB_REPORT	<pre>{ "reportItems": [{ "reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z", "accountId": "112233445566", "region": "us-west-2", "restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E", "jobStatus": "RUNNING", "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae", "resourceName": "string", "initiationDate": "2021-07-14T15:53:30Z", "backupPlanName": "string", "backupRuleName": "string", "backupRuleSchedule": "string", "backupRuleTimezone": "string", "startWindowEnd": "2021-07-14T15:53:30Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "vaultType": "BACKUP_VAULT", "vaultLockStatus": "string", "isEncrypted": true, "encryptionKeyArn": "arn:aws:kms:us-west-2:112233445566:key/...", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "sourceResourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75", }] }</pre>

Vorlagen für Backup-Berichte	Beispielbericht im JSON-Format
	<pre> "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "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	<pre>{</pre>

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format
	<pre> "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_Hours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:19.995Z", "numResourcesCompliant": 0, "numResourcesNonCompliant": 25, "controlScope": "{ComplianceResourceTypes: [],}", "controlParameters": "{\n requiredFrequencyValue\n":\n "1\n",\n </pre>

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format
	<pre>"requiredRetentionDays\" : \"35\", \"requiredFrequencyUnit\" : \"hours \"}" }] }</pre>

Vorlage für einen Compliance-Bericht	Beispielbericht im JSON-Format
RESOURCE_COMPLIANCE_REPORT	<pre> { "reportItems": [{ "accountId": "112233445566", "region": "us-west-2", "frameworkName": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "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": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "resourceId": "AWS::EFS ::FileSystem/fs-b3d7c218", "resourceType": "AWS::EFS ::FileSystem", "resourceComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-07- 07T18:55:40.961Z" }] } </pre>

Berichtsvorlagen scannen

Berichtsvorlagen werden gescannt. Mit diesen Vorlagen erhalten Sie tägliche Updates zu Ihren Scanaufträgen mit erweitertem Kontext, einschließlich Tresoreigenschaften und Details zum Sicherungsplan. Sie können diese Berichte verwenden, um den Status und die Berichte Ihrer Scanaufträge zu überwachen und Fehler zu identifizieren, bei denen möglicherweise weitere Maßnahmen erforderlich sind. In der folgenden Tabelle sind der Name einer Vorlage für einen Scanbericht und die zugehörige Beispielausgabe aufgeführt.

Berichtsvorlage für das Scannen	Beispielbericht im JSON-Format
MALWARE_JOB_REPORT	<pre>{ "reportTimePeriodStart": "2025-11-09T00:00:00Z", "reportTimePeriodEnd": "2025-11-10T00:00:00Z", "accountId": "025066259999", "region": "us-east-1", "scanJobId": "489abba3-0a57-4207-93ff-d3947d85a8d3", "scanId": "9ddd3144f68ea3ee6e388c66a0b55467", "malwareScanner": "GUARDDUTY", "jobStatus": "RUNNING", "scanResultStatus": "", "statusMessage": "", "resourceType": "EBS", "resourceArn": "arn:aws:ec2:us-east-1:025066259999:volume/vol-0f1c480a6a9b33cb7", "backupPlanArn": "arn:aws:backup:us-east-1:025066259999:backup-plan:orgs/4232272a-ed54-3a88-b1d0-ace894b6c24c", "creationDate": "2025-10-28T17:30:50.820Z", "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-03fef858bad24c7a6", "backupVaultName": "Default",</pre>

Berichtsvorlage für das Scannen	Beispielbericht im JSON-Format
	<pre>"backupVaultArn": "arn:aws: backup:us-east-1:0250662599 99:backup-vault:Default", "iamRoleArn": "arn:aws:iam::0250 66259999:role/service-role/ AWSBackupDefaultServiceRole", "scannerRoleArn": "arn:aws: iam::025066259999:role/AWSB ackupGuardDutyRolePolicyForScans" }</pre>

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.

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. Sie können keinen Bucket von einem anderen Konto aus verwenden. 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 eine der Berichtsvorlagen aus der Liste 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 Ihre AWS Region.
 2. Wählen Sie ein Framework aus dieser Region.
 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 im JSON-Format exportiert werden.
12. Wählen Sie für den S3-Bucket-Namen einen Bucket aus Ihrem Konto aus.
13. (Optional) Geben Sie ein Bucket-Präfix ein.

AWS Backup übermittelt Ihr Girokonto, aktuelle Region berichtet ans3://*amzn-s3-demo-bucket*/prefix/Backup/*accountID*/*Region*/year/month/day/report-name.

AWS Backup übermittelt Ihre kontenübergreifenden Berichte an `s3://amzn-s3-demo-bucket/prefix/Backup/crossaccount/Region/year/month/day/report-name`

AWS Backup übermittelt Ihre regionsübergreifenden Berichte an `s3://amzn-s3-demo-bucket/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 vom Kunden verwalteten 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 enthalten `kms:GenerateDataKey`:

Die Richtlinie [AWSServiceRolePolicyForBackupReports](#) verfügt 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, was zu dem Fehler „Ungültiger Prinzipal“ führt.

8. Kopieren Sie die Berechtigungen in die Richtlinie.

Bucket-Beispielrichtlinie

JSON

```
{
  "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 Berichtsplán, um die Erstellung Ihrer Berichte zu automatisieren und deren Amazon-S3-Ziel-Bucket zu definieren. Ein Berichtsplán 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 enthalten `kms:GenerateDataKey`:

Die Richtlinie [AWSServiceRolePolicyForBackupReports](#) verfügt 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 CloudFormation

Wir stellen Ihnen die folgenden 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.comAction: s3:GetBucketAcl
Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}"
- Sid: AWSConfigBucketDelivery
Effect: Allow
Principal:
Service:
 - config.amazonaws.comAction: 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 Ihre AWS Backup Audit Manager Manager-Compliance-Ergebnisse 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 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 EC2 Amazon-Instance im laufenden Zustand durch das Steuerelement [Last Recovery Point was created](#) ausgewertet. Eine EC2 Instance, die sich im Status „Gestoppt“ befindet, wird nicht in die Compliance-Bewertung einbezogen.

Backup-Ressourcen sind in mindestens einem Backup-Plan enthalten

Beschreibung: Prüft, ob Ressourcen in mindestens einem Backup-Plan enthalten 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, mit denen Wiederherstellungspunkte manuell gelöscht werden können.

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 Backup-Tresor-Zugriffsrichtlinie 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 [Feature-Verfügbarkeit 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 Sicherungsplan](#), 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.

Ressourcen befinden sich in einem Backup-Plan mit AWS Backup Vault Lock

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.

Ressourcen in einem Tresor mit logischem Air-Gap

Beschreibung: Dieses Steuerelement bewertet, ob für Ressourcen innerhalb des angegebenen Werts und Zeitrahmens mindestens ein Wiederherstellungspunkt in einen Tresor mit logischem Air-Gap kopiert wurde. Dieses Steuerelement ist `NON_COMPLIANT`, wenn innerhalb des für das Steuerelement konfigurierten Zeitraums kein Recovery Point in einen Tresor mit logischem Air-Gap kopiert wurde.

Ressource: AWS Backup: `recovery points`

Parameter:

- `recoveryPointAgeValue`
- `recoveryPointAgeUnit`

Geben Sie den Zeitraum ein. Geben Sie die Einheit in `days` oder `anhours`. Geben Sie einen Wert für diese Einheit an. Stundenwerte können innerhalb 24 bis 2184 einschließlich angegeben werden. Werte für Tage können innerhalb 1 bis 91 einschließlich angegeben werden.

Ein Mindestwert von 7 Tagen oder 168 Stunden wird empfohlen. Der Kontrollwert sollte nicht häufiger sein als die Häufigkeit der Erstellung von Kopien in Ihrem Backup-Plan. Andernfalls wird möglicherweise ein unerwarteter `NON_COMPLIANT` Status angezeigt, bis Ihr nächstes Backup in einen Tresor mit logischem Air-Gap kopiert und diese Steuerung ausgeführt wird.

Tritt auf: Automatisch alle 24 Stunden

Umfang:

- Ressourcen nach Typ
- Einzelne Ressource

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.

Überblick über die kontenübergreifende Verwaltung

Sie können die Funktion zur kontenübergreifenden Verwaltung verwenden, AWS Backup um Ihre Sicherungs-, Wiederherstellungs- und Kopieraufträge, mit AWS-Konten denen Sie die Konfiguration vornehmen, zu verwalten und zu überwachen. AWS Organizations [AWS Organizations](#) ist 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.

Die kontenübergreifende Verwaltung besteht aus kontenübergreifender Überwachung, kontenübergreifenden Backups, Backup-Richtlinien und delegierten Administratorkonten. Nicht alle diese Elemente sind in allen Regionen verfügbar. Informationen darüber, wo kontenübergreifende Verwaltung verfügbar ist, finden Sie unter [Verfügbarkeit von Funktionen nach AWS Regionen](#).

So verwenden Sie die kontenübergreifende Verwaltung

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.

Erstellen eines Verwaltungskontos in Organizations

Zunächst müssen Sie [Ihre Organisation erstellen](#) und sie mit AWS Mitgliedskonten in konfigurieren AWS Organizations. Anweisungen finden Sie unter [Praktische Anleitung: Erstellen und Konfigurieren einer Organisation](#) im AWS Organizations -Benutzerhandbuch.

Wenn Sie Ihrer Organisation Mitgliedskonten hinzufügen, stellen Sie sicher, dass jedes Konto über Folgendes verfügt:

- Mindestens ein Backup-Tresor mit and/or logischem Air-Gap
- Eine IAM-Rolle

Die von Ihnen erstellten Backup-Richtlinien verfügen zwar über einen Backup-Plan AWS-Regionen, identifizieren aber auch die im Backup-Plan verwendeten Tresore, die zu sichernden Ressourcen und die IAM-Rolle, die für die Erstellung des Backups verwendet wird. Backup-Richtlinien, die auf Konten verweisen, denen die erforderlichen Informationen fehlen, funktionieren nicht wie erwartet.

Weitere Informationen finden Sie unter [Syntax für Backup-Richtlinien](#) im AWS Organizations Benutzerhandbuch.

Aktivieren der kontenübergreifenden Verwaltung

Bevor Sie die kontenübergreifende Verwaltung in verwenden können AWS Backup, muss das Verwaltungskonto die Funktion aktivieren (d. h. Sie müssen sich dafür anmelden). Nachdem das Verwaltungskonto die kontenübergreifende Verwaltung aktiviert hat, können Sie Backup-Richtlinien erstellen, mit denen Ressourcen in mehreren Konten verwaltet werden.

So aktivieren Sie die kontenübergreifende Verwaltung

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 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.

Sicherungsrichtlinien

Sie können Backup-Pläne mit der Skalierbarkeit von [Richtlinien](#) kombinieren AWS Organizations, um [Backup-Richtlinien](#) zu erstellen, um die Verwaltung in Ihrem Unternehmen zu vereinfachen.

Im AWS Organizations Benutzerhandbuch finden Sie Informationen darüber, wie Sie Backup-Richtlinien für Ihr Unternehmen aktivieren können, sodass Sie:

- [Erstellen Sie eine Backup-Richtlinie](#)
- [Eine Backup-Richtlinie aktualisieren](#); oder
- [Löschen Sie eine Backup-Richtlinie](#)
- [Syntax und Beispiele für Backup-Richtlinien](#)

AWS Backup Spezifische Kontingente [AWS Backup Kontingente](#) für Elemente, die in einer Richtlinie enthalten sind, finden Sie unter.

Delegierter Administrator

Die delegierte Verwaltung 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
Aktivieren Sie die kontenübergreifende Verwaltung	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.
- Es wird empfohlen, dass für das Organisationsverwaltungskonto die mit dem AWS Backup Backup-Service verknüpfte Rolle (AWS Backup ServiceRoleForBackup) vorhanden ist, um delegierte Administratorrechte automatisch mit Organizations zu synchronisieren. Dadurch wird sichergestellt, dass delegierte Administratoren den richtigen Zugriff haben, wenn Sie Opt-in-Regionen aktivieren oder die Administratorzuweisung ändern. Wenn die mit dem Backup-Service verknüpfte Rolle nicht vorhanden ist oder gelöscht wurde, haben Kunden mehrere Möglichkeiten, sie zu erstellen:
 - Enabling the Delegated Administrator feature.
 - Access the Backup Vaults Console page.
 - Manually create it following the documentation in [Die Standard-Servicerolle erstellen](#).
- Stellen Sie sicher, dass in der AWS Backup Konsole Backup-Richtlinien, kontenübergreifende Überwachung, kontoübergreifende Sicherung und Funktionen für delegierte Administratoren 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).
- Optional: Delegierter Administrator, sodass AWS Backup Backup automatisch die mit dem Backup-Service verknüpfte Rolle erstellen kann, um delegierte Administratorberechtigungen mit Organizations zu synchronisieren.
- 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.

Stellen Sie sicher, dass der delegierte Administrator über die von [the section called “AWSBackupOrganizationAdminAccess”](#) erteilten Berechtigungen verfügt.

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 entziehen, 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. AWS-Backup-Konsole <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 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.

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 CloudFormation

Allgemeines

Mit können Sie Ihre AWS Ressourcen mithilfe von Vorlagen CloudFormation, die Sie erstellen, auf sichere und wiederholbare Weise bereitstellen und verwalten. Sie können CloudFormation Vorlagen verwenden und StackSets Ihre Backup-Pläne, Backup-Ressourcenauswahl und Backup-Tresore verwalten. Weitere Informationen zur Verwendung von CloudFormation finden Sie unter [Wie funktioniert CloudFormation ?](#) im AWS CloudFormation -Benutzerhandbuch .

Bevor Sie Ihre CloudFormation Vorlage oder erstellen StackSet, sollten Sie Folgendes beachten:

- 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](#).

Bereitstellung eines Backup-Tresors, eines Backup-Plans und einer Ressourcenzuweisung mit CloudFormation

Eine CloudFormation Beispielvorlage, die einen Backup-Tresor, Backup-Pläne und Ressourcenzuweisungen bereitstellt, finden Sie unter [Weisen Sie AWS Backup Ressourcen zu über CloudFormation](#).

Bereitstellen von Backup-Plänen mit CloudFormation

CloudFormation Beispielvorlagen für die Bereitstellung von Backup-Plänen finden Sie unter [the section called "CloudFormation Vorlagen für Backup-Pläne"](#).

Bereitstellung von AWS Backup Audit Manager Manager-Frameworks und Berichtsplänen mit CloudFormation

CloudFormation Beispielvorgängen, die AWS Backup Audit Manager Manager-Frameworks und Berichtspläne bereitstellen, finden Sie unter [the section called “Verwendung CloudFormation zur Bereitstellung von AWS Backup Audit Manager Manager-Ressourcen”](#).

Kontenübergreifende Bereitstellung von Backup-Plänen mit CloudFormation

Sie können es [AWS CloudFormation StackSets für mehrere Konten in einer AWS Organisation verwenden](#). Beispielvorgängen stehen im [CloudFormation -Benutzerhandbuch](#) zur Verfügung.

Ein hervorragender Ausgangspunkt und eine Referenz ist die Publikation [Automatisieren zentralisierter Backups im großen Maßstab für alle AWS Dienste mithilfe AWS Backup](#). Mit Ibukun Oyewumi und Sabith Venkitachalapathy (Juli 2021).

Erfahren Sie mehr über CloudFormation

Informationen zur Verwendung von CloudFormation mit AWS Backup finden Sie unter [AWS Backup Resource Type Reference](#) im AWS CloudFormation Benutzerhandbuch.

Informationen zur Steuerung des Zugriffs auf AWS Dienstressourcen bei der Verwendung CloudFormation finden Sie unter [Steuern des Zugriffs mit AWS Identity and Access Management](#) im AWS CloudFormation Benutzerhandbuch.

AWS Backup Netzwerk

AWS Backup Endpunkte

AWS Backup bietet sowohl öffentliche als auch private Endpunkte für Ihre Konnektivitätsanforderungen. AWS Backup unterstützt für diese Endpunkte sowohl Internetprotokolle Version 4 (IPv4) als auch Version 6 (IPv6) für Ressourcentypen, die diese Unterstützung bieten. IPv6

Der neuere öffentliche Endpunkt `backup.[Region].api.aws` verfügt über Dual-Stack-Funktionen und kann einen oder beide IPv4 Endpunkte und Endpunkte auflösen. IPv6 Wenn Sie eine Anfrage an einen AWS Backup Dual-Stack-API-Endpunkt stellen, wird der Endpunkt an die Adresse aufgelöst, die durch die Konfiguration des von Ihrem Netzwerk und Client verwendeten Protokolls bestimmt wird.

Der ältere Endpunkt `backup.[Region].amazonaws.com` kann nur IPv4 für Aufrufe verwendet werden, auf die verwiesen wird.

Sie können die [Endpunkte des öffentlichen Dienstes für AWS Backup](#) in der Allgemeine Amazon Web Services-Referenz einsehen. Sie können die Schritte zum Einrichten von privaten Endpunkten [AWS Backup über VPC](#) einsehen.

AWS Backup über VPC-Endpunkte

Sie können eine private Verbindung zwischen Ihrer Virtual Private Cloud (VPC) herstellen und AWS Backup einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte basieren auf einer Technologie [AWS PrivateLink](#), mit der Sie auf die AWS Backup API zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung verwenden zu müssen. 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.

Weitere Informationen finden Sie unter [Access AWS Services bis AWS PrivateLink](#) im AWS PrivateLink Guide.

Überlegungen zu Amazon VPC-Endpunkten

Alle AWS Backup Operationen, die für die Verwaltung Ihrer Ressourcen relevant sind, 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. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr AWS Backup über den Schnittstellenendpunkt zu steuern.

Sie können IPv4, IPv6, oder Dual Stack wählen, wenn Sie einen Endpunkt erstellen. Sie erhalten dieselben DNS-Namen (die beide IPv4 IPv6 Adressen enthalten, wenn Sie Dual Stack wählen).

AWS Backup für SAP HANA wird nicht unterstützt AWS PrivateLink. SAP HANA-Backups werden durch den aktiviert AWS Backint Agent, der keine VPC-Endpunkte unterstützt; er sendet Backup-Daten an den Speicherendpunkt für. AWS Backup

Erstellen Sie einen AWS Backup VPC-Endpunkt

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 [Erstellen eines Schnittstellenendpunkts](#) im AWS PrivateLink -Leitfaden.

PrivateLink Endpoints verwenden dieselbe Namensstruktur von IPv4, obwohl jeder Endpunkt für IPv4, IPv6 oder Dual-Stack konfiguriert werden kann.

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

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Usage
TCP	443 (HTTPS)	Ausgehend	Backup-Gateway	AWS	Für die Kommunikation vom Backup Gateway zum AWS Service-Endpoint

Verwenden Sie einen VPC-Endpunkt

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.api.aws` 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

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 `fehlgeschlagenRequestLimitExceeded`, möglicherweise nicht bei Amazon AWS CloudTrail oder Amazon protokolliert. CloudWatch

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Services mit Endpunktrichtlinien](#) im AWS PrivateLink -Leitfaden.

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.

JSON

```
{
  "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](#).

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. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Ihnen bei der Überwachung und Sicherung Ihrer AWS Backup Ressourcen helfen.

Topics

- [Überprüfung der Einhaltung von Vorschriften für AWS Backup](#)
- [Datenschutz in AWS Backup](#)
- [Identitäts- und Zugriffsmanagement in AWS Backup](#)
- [Sicherheit der Infrastruktur in AWS Backup](#)
- [Integrität der Daten in AWS Backup](#)
- [Rechtliche Bestimmungen und AWS Backup](#)
- [Malware-Schutz in AWS Backup](#)
- [Belastbarkeit in AWS Backup](#)

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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

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. Dazu gehört auch, wenn Sie mit AWS Backup oder anderen AWS Diensten arbeiten, die die Konsole, die API oder verwenden AWS SDKs. AWS CLI 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

Unabhängige -Verschlüsselung

AWS Backup bietet unabhängige Verschlüsselung für [Ressourcentypen, die eine vollständige AWS Backup Verwaltung unterstützen](#). Unabhängige Verschlüsselung bedeutet, dass für Wiederherstellungspunkte (Backups), die Sie erstellen, eine andere Verschlüsselungsmethode als die, die durch die Verschlüsselung der Quellressource bestimmt wird, verwendet werden AWS Backup kann. Beispielsweise kann Ihr Backup eines Amazon S3 S3-Buckets eine andere Verschlüsselungsmethode haben als das Quell-Bucket, das Sie mit der Amazon S3 S3-Verschlüsselung verschlüsselt haben. Diese Verschlüsselung wird über die AWS KMS Schlüsselkonfiguration im Backup-Tresor gesteuert, in dem Ihr Backup gespeichert ist.

Backups von Ressourcentypen, die nicht vollständig von verwaltet werden, erben AWS Backup in der Regel die Verschlüsselungseinstellungen von ihrer Quellressource. Sie können diese Verschlüsselungseinstellungen gemäß den Anweisungen dieses Dienstes konfigurieren, z. B. die [Amazon EBS-Verschlüsselung](#) im Amazon EBS-Benutzerhandbuch.

Ihre IAM-Rolle muss Zugriff auf den KMS-Schlüssel haben, der zum Sichern und Wiederherstellen des Objekts verwendet wird. Andernfalls ist der Job erfolgreich, aber die Objekte werden nicht gesichert oder wiederhergestellt. Die Berechtigungen in der IAM-Richtlinie und der KMS-Schlüsselrichtlinie müssen konsistent sein. Weitere Informationen finden Sie im [AWS Key Management Service Entwicklerhandbuch unter Angabe von KMS-Schlüsseln in IAM-Richtlinienerklärungen](#).

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. [Weitere Informationen zur Verschlüsselung in AWS Backup finden Sie unter Regions- und kontoübergreifendes Backup](#).

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige Verschlüsselung AWS Backup
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. Der AWS KMS-Schlüssel kann entweder ein vom Kunden verwalteter Schlüssel oder ein AWS verwalteter Schlüssel sein, der AWS Backup dem Service zugeordnet ist. AWS Backup verschlüsselt alle Backups, auch wenn die Amazon S3 S3-Quell-Buckets nicht verschlüsselt sind.	Unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige Verschlüsselung AWS Backup
VMware virtuelle Maschinen	VM-Backups sind immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für Backups virtueller Maschinen wird in dem AWS Backup Tresor konfiguriert, in dem die Backups der virtuellen Maschinen gespeichert sind.	Unterstützt
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 Verschlüsselung AWS Backup
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. Um eine Sicherungskopie einer verschlüsselten DynamoDB-Tabelle AWS Backup zu erstellen, müssen Sie die Berechtigungen <code>kms:Decrypt</code> und <code>kms:GenerateDataKey</code> zur IAM-Rolle hinzufügen, die für die Sicherung verwendet wird. Alternativ können Sie die Standard-Servicerolle verwenden. AWS Backup	Nicht unterstützt
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

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige Verschlüsselung AWS Backup
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
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.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige Verschlüsselung AWS Backup
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
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. 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 Verschlüsselung AWS Backup
Amazon FSx	Die Verschlüsselungsfunktionen für FSx Amazon-Dateisysteme unterscheiden sich je nach dem zugrunde liegenden Dateisystem. Weitere Informationen zu Ihrem speziellen FSx Amazon-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 Verschlüsselung AWS Backup
Amazon Timestream	Sicherungen von Timestream-Tabellen-Snapshots sind immer verschlüsselt. Der AWS KMS Verschlüsselungsschlüssel für Timestream-Backups wird im Backup-Tresor konfiguriert, in dem die Timestream-Backups 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
Amazon Redshift Serverless	Redshift Serverless-Snapshots werden automatisch mit demselben Verschlüsselungsschlüssel verschlüsselt, der zur Verschlüsselung der Quelle verwendet wurde.	Nicht unterstützt

Ressourcentyp	Konfigurieren der Verschlüsselung	Unabhängige Verschlüsselung AWS Backup
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
SAP HANA-Datenbanken auf EC2 Amazon-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



Tip

[AWS Backup Audit Manager](#) hilft Ihnen dabei, unverschlüsselte Backups automatisch zu erkennen.

Verschlüsselung für Kopien eines Backups auf ein anderes Konto oder AWS-Region

Wenn Sie Ihre Backups zwischen Konten oder Regionen kopieren, AWS Backup werden diese Kopien für die meisten Ressourcentypen automatisch verschlüsselt, auch wenn das ursprüngliche Backup unverschlüsselt ist. AWS Backup verschlüsselt die Kopie mithilfe des KMS-Schlüssels des Zieltresors.

Bevor Sie ein Backup von einem Konto auf ein anderes kopieren (kontoübergreifender Kopierauftrag) oder ein Backup von einer Region in eine andere kopieren (regionsübergreifender Kopierauftrag), beachten Sie die folgenden Bedingungen, von denen viele davon abhängen, ob der Ressourcentyp im Backup (Recovery Point) [vollständig verwaltet wird AWS Backup oder nicht](#).

- Eine Kopie eines Backups auf ein anderes AWS-Region wird mit dem Schlüssel des Zieltresors verschlüsselt.
- Für eine Kopie eines Wiederherstellungspunkts (Backup) einer Ressource, die vollständig von verwaltet wird, können Sie wählen AWS Backup, ob Sie sie mit einem vom [Kunden verwalteten Schlüssel \(CMK\) oder einem AWS Backup verwalteten Schlüssel \(aws/backup\)](#) verschlüsseln möchten.

Für eine Kopie des Wiederherstellungspunkts einer Ressource, die nicht vollständig verwaltet wird AWS Backup, muss es sich bei dem dem Zieltresor zugewiesenen Schlüssel um einen CMK oder um den verwalteten Schlüssel des Dienstes handeln, dem die zugrunde liegende Ressource gehört. Wenn Sie beispielsweise eine EC2 Instanz kopieren, kann ein verwalteter Backup-Schlüssel nicht verwendet werden. Stattdessen muss ein CMK- oder Amazon EBS-KMS-Schlüssel (aws/ebs) verwendet werden, um ein Fehlschlagen des Kopierauftrags zu vermeiden.

- Kontoübergreifendes Kopieren mit AWS verwalteten Schlüsseln wird nicht für Ressourcen unterstützt, die nicht vollständig von verwaltet werden. AWS Backup Die [Schlüsselrichtlinie](#) eines AWS verwalteten Schlüssels ist unveränderlich, wodurch verhindert wird, dass der Schlüssel kontenübergreifend kopiert wird. Wenn Ihre Ressourcen mit AWS verwalteten Schlüsseln verschlüsselt sind und Sie eine kontoübergreifende Kopie durchführen möchten, können Sie [die Verschlüsselungsschlüssel in einen vom Kunden verwalteten Schlüssel ändern](#), der für kontoübergreifendes Kopieren verwendet werden kann. Oder folgen Sie den Anweisungen unter [Schützen verschlüsselter Amazon RDS-Instances durch konto- und regionsübergreifende Backups](#), um weiterhin AWS verwaltete Schlüssel zu verwenden.
- Kopien von unverschlüsselten Amazon Aurora-, Amazon DocumentDB- und Amazon Neptune Neptune-Clustern sind ebenfalls unverschlüsselt.

AWS Backup Erklärungen zu Berechtigungen, Bewilligungen und Ablehnungen

Um Fehlschläge bei Aufträgen zu vermeiden, können Sie die AWS KMS Schlüsselrichtlinie überprüfen, um sicherzustellen, dass sie über erforderliche Berechtigungen verfügt und keine Ablehnungsaussagen enthält, die erfolgreiche Operationen verhindern.

Fehlgeschlagene Aufträge können entweder auf eine oder mehrere Deny-Anweisungen zurückzuführen sein, die auf den KMS-Schlüssel angewendet wurden, oder darauf, dass eine [Zuweisung](#) für den Schlüssel aufgehoben wurde.

In einer Richtlinie für AWS verwalteten Zugriff [AWSBackupFullAccess](#), z. B. im Rahmen von Sicherungs-, Kopier- und Speichervorgängen, gibt es „Zulassen“-Aktionen, die es ermöglichen, im Namen eines Kunden eine Genehmigung AWS Backup für einen KMS-Schlüssel zu erstellen. AWS KMS

Für die Schlüsselrichtlinie sind mindestens die folgenden Berechtigungen erforderlich:

- `kms:createGrant`
- `kms:generateDataKey`
- `kms:decrypt`

Wenn Ablehnungsrichtlinien erforderlich sind, müssen Sie die erforderlichen Rollen für Sicherungs- und Wiederherstellungsvorgänge auf eine Zulassungsliste setzen.

Diese Elemente können wie folgt aussehen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "KmsPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
      },
      "Action": [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
```

```

    "Sid": "KmsCreateGrantPermissions",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "kms:EncryptionContextKeys": "aws:backup:backup-vault"
        },
        "Bool": {
            "kms:GrantIsForAWSResource": true
        },
        "StringLike": {
            "kms:ViaService": "backup.*.amazonaws.com"
        }
    }
}
]
}

```

Diese Berechtigungen müssen Teil des Schlüssels sein, unabhängig davon, ob er AWS verwaltet oder vom Kunden verwaltet wird.

1. Stellen Sie sicher, dass die erforderlichen Berechtigungen Teil der KMS-Schlüsselrichtlinie sind
 - a. Führen Sie KMS CLI `get-key-policy` ([kms:GetKeyPolicy](#)) aus, um die Schlüsselrichtlinie anzuzeigen, die dem angegebenen KMS-Schlüssel zugeordnet ist.
 - b. Überprüfen Sie die zurückgegebenen Berechtigungen.
2. Stellen Sie sicher, dass keine Deny-Anweisungen vorhanden sind, die sich auf den Betrieb auswirken
 - a. Führen Sie CLI () aus `get-key-policy` (oder führen Sie es erneut aus [kms:GetKeyPolicy](#)), um die Schlüsselrichtlinie anzuzeigen, die dem angegebenen KMS-Schlüssel zugeordnet ist.
 - b. Überprüfen Sie die Richtlinie.
 - c. Entfernen Sie die entsprechenden Deny-Anweisungen aus der KMS-Schlüsselrichtlinie.

3. Führen Sie bei Bedarf das Programm aus, [kms:put-key-policy](#) um die Schlüsselrichtlinie durch überarbeitete Berechtigungen und entfernte Deny-Anweisungen zu ersetzen oder zu aktualisieren.

Darüber hinaus muss der Schlüssel, der der Rolle zugeordnet ist, die einen regionsübergreifenden Kopierauftrag initiiert, über die `DescribeKey` entsprechende `"kms:ResourcesAliases"`: `"alias/aws/backup"` Berechtigung verfügen.

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 für die Nutzung Ihres vom Kunden verwalteten Schlüssels ist ein [Zuschuss](#) erforderlich. 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](#)
- [Zugriffskontrolle](#)
- [IAM-Servicerollen](#)
- [Verwaltete Richtlinien für AWS Backup](#)
- [Verwenden von serviceverknüpften Rollen für AWS Backup](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)

Authentifizierung

Für den Zugriff AWS Backup auf 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-ManagementkonsoleAWSDiskussionsforen 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 [einen der verschiedenen](#) Schlüssel SDKs oder mithilfe der [AWS Command Line Interface \(AWS CLI\)](#). 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 AWS Dienste und Ressourcen verwendet werden können. IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:
 - Förderierter Benutzerzugriff — Anstatt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Benutzeridentitäten aus 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 EC2 Amazon-Instance ausgeführt werden und AWS API-Anfragen stellen. Das ist empfehlenswerter, 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 im IAM-Benutzerhandbuch [unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden](#).

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.

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](#)
- [Angaben von Bedingungen in einer Richtlinie](#)
- [API-Berechtigungen: Referenztablelle 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 (ARNs) zugeordnet. ARNs AWS Ressourcen eindeutig identifizieren. 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 Ressource ARNs

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Sicherungsplan	arn:aws:b ackup: <i>region</i> : <i>account-id</i> :backup-plan:*	
Sicherungstresor	arn:aws:b ackup: <i>region</i> : <i>account-id</i> :backup-vault:*	
Wiederherstellungspunkt für Amazon EBS	arn:aws:e c2: <i>region</i> ::snapshot/ *	snapshot/snap-05f426fd8kdjb4224
Erholungspunkt für EC2 Amazon-Bilder	arn:aws:e c2: <i>region</i> ::image/a mi-*	image/ami-1a2b3e4f5e6f7g890

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Wiederherstellungspunkt für Amazon RDS	arn:aws:rds: <i>region</i> : <i>account-id</i> :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Wiederherstellungspunkt für Aurora	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Erholungspunkt für Aurora DSQL	arn:aws:partition :backup: <i>region</i> : <i>account-id</i> :recovery-point: <i>recovery-point-id</i>	arn:aws:backup:us-east-1:012345678901:recovery-point:8a92c3f1-b475-4d9e-95e6-7c138f2d4b0a
Wiederherstellungspunkt für Storage Gateway	arn:aws:ec2: <i>region</i> ::snapshot/*	snapshot/snap-0d40e49137e31d9e0
Wiederherstellungspunkt für DynamoDB ohne Erweitertes DynamoDB-Backup	arn:aws:dynamodb: <i>region</i> : <i>account-id</i> :table/*/backup/*	table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3
Wiederherstellungspunkt für DynamoDB mit aktiviertem Erweitertes DynamoDB-Backup	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Wiederherstellungspunkt für Amazon EFS	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e
Erholungspunkt für Amazon FSx	arn:aws:fsx: <i>region</i> : <i>account-id</i> :backup/backup-*	backup/backup-1a20e49137e31d9e0

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Wiederherstellungspunkt für virtuelle Maschinen	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	1801234a-5b6b-7dc8 -8032-836f7ffc623b
Wiederherstellungspunkt für kontinuierliche Amazon S3-Sicherung	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucket</i> -5ec207d0
Wiederherstellungspunkt für regelmäßige S3-Sicherung	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucket</i> -20211231900000-5ec207d0
Erholungspunkt für Amazon DocumentDB	arn:aws:r ds: <i>region:account-id</i> :cluster-snapshot: awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Erholungspunkt für Neptune	arn:aws:r ds: <i>region:account-id</i> :cluster-snapshot: awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Erholungspunkt für Amazon Redshift	arn:aws:r edshift: <i>region:account-id</i> :snapshot : <i>resource</i> /awsbacku p:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Erholungspunkt für Amazon Redshift Serverless	arn:aws:redshift- serverless : <i>region:account-id</i> :snapshot: <i>resource</i> / awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012

Ressourcentyp	ARN-Format	Beispiel für eine eindeutige ID
Erholungspunkt für Amazon Timestream	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012_beta
Erholungspunkt für die Vorlage AWS CloudFormation	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012
Erholungspunkt für die SAP HANA-Datenbank auf einer EC2 Amazon-Instance	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012

Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, haben alle Wiederherstellungspunkte in diesem Format `arn:aws:backup:region:account-id::recovery-point:*`, sodass Sie leichter Berechtigungsrichtlinien anwenden können, um diese Wiederherstellungspunkte zu schützen. Informationen zu den Ressourcen, die die vollständige AWS Backup Verwaltung unterstützen, finden Sie in diesem Abschnitt der [Feature-Verfügbarkeit nach Ressource](#) Tabelle.

AWS Backup bietet eine Reihe von Operationen 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 [Prinzipalidentität](#) (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 unter [API-Berechtigungen: Referenztable 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 zu [AWS Backup Ressource ARNs](#) ressourcenspezifischen Wiederherstellungspunkten finden Sie unter `ARNs`

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.

Weitere Informationen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup](#) in der Service-Autorisierungs-Referenz.

Berechtigungen zum Kopieren von Tags

Bei der AWS Backup Ausführung eines Sicherungs- oder Kopierauftrags wird versucht, die Tags von Ihrer Quellressource (oder vom 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.

- 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.
- 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 Backup-Plan (zu Wiederherstellungspunkten hinzugefügte Tags) 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	<code>elasticfilesystem:DescribeTags</code>

Ressourcentyp	Erforderliche Berechtigung
FSx Amazon-Dateisystem	<code>fsx:ListTagsForResource</code>
Amazon RDS-Datenbank und Amazon Aurora-Cluster	<code>rds:AddTagsToResource</code> <code>rds:ListTagsForResource</code>
Storage Gateway-Volume	<code>storagegateway:ListTagsForResource</code>
EC2 Amazon-Instance und Amazon EBS-Volume	<code>EC2:CreateTags</code> <code>EC2:DescribeTags</code>

DynamoDB unterstützt das Zuweisen von Tags zu Backups nur, wenn Sie zuerst [Erweitertes DynamoDB-Backup](#) aktivieren.

Wenn ein EC2 Amazon-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 EC2 Amazon-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. Richtlinien, die mit einer Ressource verknüpft sind, 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 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 anzusehen 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 es verwenden AWS Backup APIs. Auf einige Backup-Typen, wie Amazon Elastic Block Store (Amazon EBS) und Amazon Relational Database Service (Amazon RDS) -Snapshots, kann auch über diese Dienste zugegriffen werden. APIs Sie können in IAM separate Zugriffsrichtlinien erstellen, die den Zugriff auf diese steuern, um den Zugriff auf APIs Backups vollständig zu kontrollieren.

Informationen zur Erstellung einer Zugriffsrichtlinie für Sicherungstresore finden Sie unter [Richtlinien für den Tresorzugriff](#).

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 Backup übergeben 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 unter [Verwaltete 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-Managementkonsole 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 Backup übergeben. 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 [AWSBackupServiceRolePolicyForBackup](#) und [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 EC2 Amazon-Instance wiederherzustellen, müssen Sie eine neue Instance starten.

Erstellen der Standardservicerolle mithilfe der Konsole

Bestimmte Aktionen, die Sie in der AWS Backup Konsole ausführen, erstellen die AWS Backup Standard-Servicerolle.

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 [Einen Backup-Plan 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-Managementkonsole 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.

JSON

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

Ersetzen Sie für China Regionen *aws* durch *aws-cn*. Ersetzen Sie für AWS GovCloud (US) Regionen *aws* 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 Backup übergeben. 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](#)
- [AWSBackupGuardDutyRolePolicyForScans](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupSearchOperatorAccess](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForItemRestores](#)
- [AWSBackupServiceRolePolicyForIndexing](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3 Backup](#)
- [AWSBackupServiceRolePolicyForS3 Restore](#)
- [AWSBackupServiceRolePolicyForScans](#)
- [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 Audits 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.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupAuditAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupDataTransferAccess

Diese Richtlinie gewährt Berechtigungen für die Datenübertragung auf der AWS Backup Speicherebene APIs, sodass der AWS Backup-Agent die Backup-Datenübertragung mit der AWS Backup Speicherebene abschließen kann. Sie können diese Richtlinie an Rollen anhängen, die von EC2 Amazon-Instances übernommen werden, auf denen SAP HANA mit dem Backup-Agenten ausgeführt wird.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupDataTransferAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupFullAccess

Der Backup-Administrator hat vollen Zugriff auf alle AWS Backup Vorgänge, einschließlich der Erstellung oder Bearbeitung von Backup-Plänen, der Zuweisung von AWS Ressourcen zu Backup-Plänen und der Wiederherstellung von Backups. Sicherheitsadministratoren sind verantwortlich für die Festlegung und Durchsetzung der Sicherheits-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.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupFullAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Diese Richtlinie gewährt dem Backup-Gateway die Berechtigung, die Metadaten virtueller Maschinen in Ihrem Namen zu synchronisieren.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupGuardDutyRolePolicyForScans

Diese Richtlinie muss zu einer neuen Scanrolle hinzugefügt werden, die Amazon die GuardDuty Erlaubnis erteilt, Ihre Backups zu lesen und zu scannen. Sie müssen diese Scan-Rolle in den Malware-Schutz- oder Scan-Einstellungen zu Ihrem Backup-Plan hinzufügen. Wenn AWS Backup einen Scan initiiert, übergibt es diese Scan-Rolle an Amazon GuardDuty.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupGuardDutyRolePolicyForScans](#) in der Referenz zu von 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 unter [AWSBackupOperatorAccess](#) in der Referenz zu von 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.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupOrganizationAdminAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupRestoreAccessForSAPHANA

Diese Richtlinie gewährt die AWS Backup Erlaubnis, ein Backup von SAP HANA auf Amazon wiederherzustellen EC2.

Die Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupRestoreAccessForSAPHANA in der](#) Referenz für AWS verwaltete Richtlinien.

AWSBackupSearchOperatorAccess

Die Suchoperatorrolle hat Zugriff auf die Erstellung von Backup-Indizes und die Erstellung von Suchvorgängen in indizierten Backup-Metadaten.

Diese Richtlinie enthält die erforderlichen Berechtigungen für diese Funktionen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupSearchOperatorAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupServiceLinkedRolePolicyForBackup

Diese Richtlinie ist der dienstbezogenen Rolle zugeordnet, die so benannt ist `AWSServiceRoleForBackup`, dass Sie AWS Dienste AWS Backup in Ihrem Namen aufrufen können, um Ihre Backups zu verwalten. Weitere Informationen finden Sie unter [the section called “Sichern und Kopieren”](#).

Die Berechtigungen für diese Richtlinie finden Sie [AWSBackupServiceLinkedRolePolicyforBackup](#) in der Referenz zu AWS verwalteten Richtlinien.

AWSBackupServiceLinkedRolePolicyForBackupTest

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceLinkedRolePolicyForBackupTest](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupServiceRolePolicyForBackup

Bietet AWS Backup Berechtigungen zum Erstellen von Backups aller unterstützten Ressourcentypen in Ihrem Namen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceRolePolicyForBackup](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSBackupServiceRolePolicyForItemRestores

Beschreibung

Diese Richtlinie gewährt Benutzern die Berechtigung, einzelne Dateien und Elemente in einem Snapshot (periodischer Backup-Wiederherstellungspunkt) auf einem neuen oder vorhandenen Amazon S3 S3-Bucket oder einem neuen Amazon EBS-Volume wiederherzustellen. Zu diesen Berechtigungen gehören: Leseberechtigungen für Amazon EBS für Snapshots, die über AWS Backup Lese-/Schreibberechtigungen für Amazon S3 S3-Buckets verwaltet werden, sowie Berechtigungen zum Generieren und Beschreiben von Schlüsseln. AWS KMS

Verwenden dieser Richtlinie

Sie können `AWSBackupServiceRolePolicyForItemRestores` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. November 2024, 22:45 UTC
- Bearbeitungszeit: Erste Instanz
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Richtlinienversion: v1 (Standard)

Die Version dieser Richtlinie definiert die Berechtigungen für die Richtlinie. Wenn der Benutzer oder die Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist oder nicht.

JSON-Richtliniendokument:

AWSBackupServiceRolePolicyForItemRestores JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
```



```

        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshots"
        ],
        "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
        "Sid": "KMSReadOnlyPermissions",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": "*"
    },
    {
        "Sid": "EBSDirectReadAPIPermissions",
        "Effect": "Allow",
        "Action": [
            "ebs:ListSnapshotBlocks",
            "ebs:GetSnapshotBlock"
        ],
        "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
        "Sid": "S3ReadonlyPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketLocation",
            "s3:ListBucket"
        ],
        "Resource": "arn:aws:s3::*:"
    },
    {
        "Sid": "S3PermissionsForFileLevelRestore",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:AbortMultipartUpload",
            "s3:ListMultipartUploadParts"
        ],
        "Resource": "arn:aws:s3::*:/*"
    },
    {
        "Sid": "KMSTDataKeyForS3AndEC2Permissions",
        "Effect": "Allow",
        "Action": [

```

```

        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "ec2.*.amazonaws.com",
                "s3.*.amazonaws.com"
            ]
        }
    }
}

```

AWSBackupServiceRolePolicyForIndexing

Beschreibung

Diese Richtlinie gewährt Benutzern Berechtigungen zum Indexieren von Snapshots, auch bekannt als periodische Wiederherstellungspunkte. Zu diesen Berechtigungen gehören: Leseberechtigungen für Amazon EBS für Snapshots, die über AWS Backup Lese-/Schreibberechtigungen für Amazon S3 S3-Buckets verwaltet werden, sowie Berechtigungen zum Generieren und Beschreiben von Schlüsseln. AWS KMS

Verwenden dieser Richtlinie

Sie können `AWSBackupServiceRolePolicyForIndexing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Zeitpunkt der Bearbeitung: Erste Instanz
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Richtlinienversion: v1 (Standard)

Die Version dieser Richtlinie definiert die Berechtigungen für die Richtlinie. Wenn der Benutzer oder die Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, wird anhand der Standardversion der Richtlinie AWS geprüft, ob die Anfrage zugelassen werden soll oder nicht.

JSON-Richtliniendokument:

AWSBackupServiceRolePolicyForIndexing JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "EBSDirectReadAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSTDataKeyForEC2Permissions",
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:*::key/*",
      "Condition": {
        "StringLike": {
```

```
    "kms:ViaService": [
      "ec2.*.amazonaws.com"
    ]
  }
}
]
```

AWSBackupServiceRolePolicyForRestores

Bietet AWS Backup Berechtigungen zum Wiederherstellen von Backups aller unterstützten Ressourcentypen in Ihrem Namen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceRolePolicyForRestores](#) in der Referenz zu von AWS verwalteten Richtlinien.

Für EC2 Instanzwiederherstellungen müssen Sie außerdem die folgenden Berechtigungen angeben, um die EC2 Instanz zu starten:

AWSBackupServiceRolePolicyForS3 Backup

Diese Richtlinie enthält die erforderlichen Berechtigungen, AWS Backup um einen beliebigen S3-Bucket zu sichern. Dies beinhaltet den Zugriff auf alle Objekte in einem Bucket und alle zugehörigen AWS KMS Schlüssel.

Die Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceRolePolicyForS3Backup](#) in der Referenz für AWS verwaltete Richtlinien.

AWSBackupServiceRolePolicyForS3 Restore

Diese Richtlinie enthält die erforderlichen Berechtigungen, AWS Backup um ein S3-Backup in einem Bucket wiederherzustellen. Dazu gehören Lese- und Schreibberechtigungen für die Buckets sowie die Verwendung beliebiger AWS KMS Schlüssel im Zusammenhang mit S3-Vorgängen.

Die Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceRolePolicyForS3Restore](#) in der Referenz für AWS verwaltete Richtlinien.

AWSBackupServiceRolePolicyForScans

Die Richtlinie sollte der IAM-Rolle zugeordnet werden, die Sie in der Ressourcenauswahl Ihres Backup-Plans verwenden. Diese Rolle erteilt AWS Backup die Berechtigung, Scans in Amazon zu initiieren GuardDuty.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSBackupServiceRolePolicyForScans](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSServiceRolePolicyForBackupReports

AWS Backup verwendet diese Richtlinie für die [AWSServiceRoleForBackupReports](#) serviceverknüpfte 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.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSServiceRolePolicyForBackupReports](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWSServiceRolePolicyForBackupRestoreTesting

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSServiceRolePolicyForBackupRestoreTesting](#) in der Referenz zu von AWS verwalteten Richtlinien.

Kundenverwaltete Richtlinien

In den folgenden Abschnitten werden die empfohlenen Sicherungs- und Wiederherstellungsberechtigungen für die AWS Dienste und Drittanbieteranwendungen beschrieben, die von AWS Backup unterstützt werden. Sie können die vorhandenen AWS verwalteten Richtlinien als Modell verwenden, wenn Sie Ihre eigenen Richtliniendokumente erstellen, und diese dann anpassen, um den Zugriff auf Ihre AWS Ressourcen weiter einzuschränken.

Important

Wenn Sie benutzerdefinierte IAM-Rollen für verwenden AWS Backup, müssen Sie zusätzlich zu den Berechtigungen auch ressourcenspezifische Berechtigungen angeben. AWS Backup Wenn Sie beispielsweise eine `backup:ListTags` Amazon RDS-Ressource aufrufen, muss Ihre benutzerdefinierte IAM-Rolle auch `rds:ListTagsForResource` Berechtigungen enthalten. Diese Berechtigungen sind zwar in der AWS Backup Standard-Servicerolle

enthalten, müssen aber explizit zu den vom Kunden verwalteten Richtlinien hinzugefügt werden. Die erforderlichen zugrundeliegenden Ressourcenberechtigungen hängen vom jeweiligen AWS Dienst und Vorgang ab.

Amazon Aurora

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Wiederherstellen

Beginnen Sie mit der `RDSPermissions` Aussage von [AWSBackupServiceRolePolicyForRestores](#).

Amazon Aurora DSQL

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- `DSQLBackupPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Wiederherstellen

Beginnen Sie mit der `DSQLRestorePermissions` Aussage von [AWSBackupServiceRolePolicyForRestores](#).

Amazon DynamoDB

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Wiederherstellen

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`

Wiederherstellen

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

Wiederherstellen

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"
},
```

role-name Ersetzen Sie durch den Namen der EC2 Instanzprofilrolle, die der wiederhergestellten EC2 Instanz zugewiesen wird. Dies ist nicht die AWS Backup Servicerolle, sondern die IAM-Rolle, die Berechtigungen für Anwendungen bereitstellt, die auf der EC2 Instanz ausgeführt werden.

Amazon EFS

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- EFSPermissions
- GetResourcesPermissions
- BackupVaultPermissions

Wiederherstellen

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

Wiederherstellen

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForRestores](#):

- FsxPermissions
- FsxTagPermissions
- FsxBackupPermissions
- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon Neptune

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- DynamoDBBackupPermissions
- RDSClusterModifyPermissions
- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

Wiederherstellen

Beginnen Sie mit der RDSPermissions Aussage von [AWSBackupServiceRolePolicyForRestores](#).

Amazon RDS

Backup

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Wiederherstellen

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.

Wiederherstellen

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": "*"
},
```

Wiederherstellen

Beginnen Sie mit den folgenden Aussagen von [AWSBackupServiceRolePolicyForRestores](#):

- StorageGatewayVolumePermissions
- StorageGatewayGatewayPermissions
- StorageGatewayListPermissions

Virtuelle Maschine

Backup

Beginnen Sie mit der BackupGatewayBackupPermissions Aussage von [AWSBackupServiceRolePolicyForBackup](#).

Wiederherstellen

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 [AWSBackupServiceRolePolicyForRestores](#) Wiederherstellungen 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.

Änderungen	Beschreibung	Date
AWSBackupGuardDutyRolePolicyForScans – Neue Richtlinie	AWS Backup hat eine neue AWS verwaltete Richtlinie hinzugefügt, die Amazon die GuardDuty Erlaubnis gibt, Kunden-Backups zu lesen und zu scannen. AWS Backup übergibt GuardDuty bei der Initiierung der Operationen <code>StartMalwareScan</code> eine Rolle mit dieser Richtlinie an. Dies ist erforderlich, um alle erforderlichen Berechtigungen für Malware-Scans auf Wiederherstellungspunkten von Amazon- EC2, Amazon EBS- und Amazon S3 S3-Ressourcen bereitzustellen. Weitere Informationen finden Sie in der verwalteten Richtlinie AWSBackupGuardDutyRolePolicyForScans.	19. November 2025
AWSBackupServiceRolePolicyForScans – Neue Richtlinie	AWS Backup hat eine neue AWS verwaltete Richtlinie hinzugefügt, die AWS Backup berechtigt, Malware-Scans auf Ihren Wiederherstellungspunkten zu initiieren.	19. November 2025

Änderungen	Beschreibung	Date
	Dies ist erforderlich, um alle erforderlichen Berechtigungen für Malware-Scans auf Wiederherstellungspunkten von Amazon- EC2, Amazon EBS- und Amazon S3 S3-Ressourcen bereitzustellen. Weitere Informationen finden Sie in der verwalteten Richtlinie AWSBackupServiceRolePolicyForScans.	
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt <code>malware-protection.guardduty.amazonaws.com</code> zu <code>IamPassRolePermissions</code> , was notwendig ist, um Malware-Scan-Jobs zu initiieren.	19. November 2025
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>malware-protection.guardduty.amazonaws.com</code> auf <code>IamPassRolePermissions</code> • <code>backup:StartScanJob</code> Diese Berechtigungen sind erforderlich, um Malware-Scanaufträge zu initiieren.	19. November 2025

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> Diese Berechtigungen ermöglichen AWS Backup das Sichern und Wiederherstellen von Amazon EKS-Clustern.	10. November 2025
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> Diese Berechtigungen ermöglichen AWS Backup das Sichern und Wiederherstellen von Amazon EKS-Clustern.	10. November 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10. November 2025

Änderungen	Beschreibung	Date
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Diese Berechtigungen ermöglichen AWS Backup die Erstellung von Backups von Amazon EKS-Clustern und den zugehörigen Ressourcen im Auftrag von Kunden.	

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10. November 2025

Änderungen	Beschreibung	Date
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Diese Berechtigungen ermöglichen AWS Backup die Erstellung von Backups von Amazon EKS-Clustern und den zugehörigen Ressourcen im Auftrag von Kunden.	

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>eks:CreateCluster</code> • <code>eks:DescribeCluster</code> • <code>eks:CreateAccessEntry</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:AssociateAccessPolicy</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:CreateAddon</code> • <code>eks:DescribeAddon</code> • <code>eks:CreateNodegroup</code> • <code>eks:DescribeNodegroup</code> • <code>eks:CreateFargateProfile</code> • <code>eks:DescribeFargateProfile</code> • <code>eks:CreatePodIdentityAssociation</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:TagResource</code> • <code>eks:DisassociateAccessPolicy</code> • <code>iam:PassRole</code>	10. November 2025

Änderungen	Beschreibung	Date
	• <code>ec2:DescribeLaunchTemplateVersions</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:RunInstances</code> • <code>ec2:CreateTags</code> • <code>iam:GetRole</code> • <code>iam:ListAttachedRolePolicies</code> • <code>backup:StartRestoreJob</code> • <code>backup:ListRestoreJobs</code> • <code>backup:ListRecoveryPointsByBackupVault</code> • <code>backup:DescribeRestoreJob</code> Diese Berechtigungen ermöglichen AWS Backup die Durchführung von Wiederherstellungsvorgängen für Amazon EKS-Cluster und die zugehörigen Ressourcen im Auftrag von Kunden.	

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgende Berechtigung hinzugefügt: • <code>organizations:ListDelegatedAdministrators</code> Mit dieser Berechtigung können delegierte Administratorinformationen mit Organizations synchronisiert werden, AWS Backup um kontoübergreifende Verwaltungsfunktionen zu nutzen.	9. September 2025

Änderungen	Beschreibung	Date
AWSBackupGuardDutyRolePolicyForScans – Neue Richtlinie	AWS Backup hat eine neue AWS verwaltete Richtlinie hinzugefügt, die Amazon die GuardDuty Erlaubnis gibt, Kunden-Backups zu lesen und zu scannen. AWS Backup übergibt GuardDuty bei der Initiierung der Operationen <code>StartMalwareScan</code> eine Rolle mit dieser Richtlinie an. Dies ist erforderlich, um alle erforderlichen Berechtigungen für Malware-Scans auf Wiederherstellungspunkten von Amazon- EC2, Amazon EBS- und Amazon S3 S3-Ressourcen bereitzustellen. Weitere Informationen finden Sie in der verwalteten Richtlinie AWSBackupGuardDutyRolePolicyForScans.	24. November 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForScans – Neue Richtlinie	AWS Backup hat eine neue AWS verwaltete Richtlinie hinzugefügt, die AWS Backup berechtigt, Malware-Scans auf Ihren Wiederherstellungspunkten zu initiieren. Dies ist erforderlich, um alle erforderlichen Berechtigungen für Malware-Scans auf Wiederherstellungspunkten von Amazon- EC2, Amazon EBS- und Amazon S3 S3-Ressourcen bereitzustellen. Weitere Informationen finden Sie in der verwalteten Richtlinie AWSBackupServiceRolePolicyForScans.	24. November 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>dsql:UpdateCluster</code> • <code>dsql:AddPeerCluster</code> • <code>dsql:RemovePeerCluster</code> • <code>dsql:GetCluster</code> Diese Berechtigungen sind erforderlich AWS Backup , um orchestrierte Wiederherstellungsvorgänge für DSQL-Ressourcen in mehreren Regionen im Namen von Kunden durchzuführen.	17. Juli 2025

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>mpa:GetApprovalTeam</code> • <code>mpa:ListApprovalTeams</code> • <code>mpa:StartSession</code> • <code>mpa:CancelSession</code> • <code>mpa:GetSession</code> • <code>mpa:ListSessions</code> Diese Berechtigungen sind für die AWS Backup Integration mit AWS -Kontenverwaltung erforderlich, AWS Organizations sodass Kunden die Möglichkeit haben, die Genehmigung durch mehrere Parteien (MPA) als Teil ihrer Logical Air-Gapped Tresore zu beantragen.	17. Juni 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores — Aktualisierung einer bestehenden Richtlinie:	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> Diese Berechtigungen sind erforderlich, damit Kunden Amazon FSx for OpenZFS Multi-Availability Zone (Multi-AZ) -Snapshots wiederherstellen können. AWS Backup	27. Mai 2025
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Diese Berechtigungen ermöglichen AWS Backup das Sichern und Wiederherstellen von Amazon Aurora DSQL-Ressourcen.	21. Mai 2025

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Diese Berechtigungen ermöglichen AWS Backup das Sichern und Wiederherstellen von Amazon Aurora DSQL-Ressourcen.	21. Mai 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • kms:Decrypt • kms:ReEncryptTo • kms:ReEncryptFrom • dsql:StartBackupJob • dsql:GetBackupJob • dsql:StopBackupJob • dsql:GetCluster • dsql:ListClusters • dsql:ListTagsForResource Diese Berechtigungen AWS Backup ermöglichen das Erstellen, Löschen, Abrufen und Verwalten von Amazon Aurora DSQL-Snapshots im Namen von Kunden.	21. Mai 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> • <code>dsql:StartRestoreJob</code> • <code>dsql:GetRestoreJob</code> • <code>dsql:StopRestoreJob</code> • <code>dsql:TagResource</code> • <code>dsql>CreateCluster</code> • <code>dsql:PutMultiRegionProperties</code> • <code>dsql:PutWitnessRegion</code> • <code>kms:DescribeKey</code> Diese Berechtigungen AWS Backup ermöglichen das Erstellen, Löschen, Abrufen, Verschlüsseln, Entschlüsseln und Verwalten von Amazon Aurora DSQL-Snapshots im Namen von Kunden.	21. Mai 2025

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Diese Berechtigungen ermöglichen AWS Backup die Verwaltung von Aurora DSQL-Backups in vom Kunden festgelegten Intervallen.	21. Mai 2025

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die folgenden Berechtigungen zu dieser Richtlinie hinzugefügt: • <code>aws:CalledVia</code> • <code>redshift-serverless>DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Diese Berechtigungen sind erforderlich, damit bestimmte Kunden vollen Zugriff auf Amazon Redshift Serverless-Backups haben, einschließlich der erforderlichen Leseberechtigungen sowie der Möglichkeit, Amazon Redshift Serverless-Wiederherstellungspunkte (Snapshot-Backups) zu löschen.	31. März 2025

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Diese Berechtigungen sind erforderlich, damit bestimmte Kunden über alle erforderlichen Backup-Berechtigungen für Amazon Redshift Serverless verfügen, einschließlich der erforderlichen Leseberechtigungen.	31. März 2025

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>redshift-serverless:DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:ListWorkgroups</code> Diese Berechtigungen sind erforderlich, AWS Backup um Amazon Redshift Serverless-Snapshots in vom Kunden festgelegten Intervallen zu verwalten.	31. März 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>redshift-serverless:CreateSnapshot</code> • <code>redshift-serverless>DeleteSnapshot</code> mit der Bedingung, nur das Löschen von Schnappschüssen mit dem <code>"aws:backup:source-resource"</code> Tag zuzulassen • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:TagResource</code> Diese Berechtigungen sind erforderlich, um Amazon Redshift Serverless-Snapshots im Namen von Kunden erstellen, löschen, abrufen	31. März 2025

Änderungen	Beschreibung	Date
	und verwalten zu können AWS Backup .	
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat dieser Richtlinie die folgenden Berechtigungen hinzugefügt: • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetTableRestoreStatus</code> • <code>redshift-serverless:RestoreTableFromSnapshot</code> Diese Berechtigungen sind erforderlich, um Amazon Redshift- und Amazon Redshift Serverless-Snapshots im Namen des Kunden wiederherstellen zu können AWS Backup .	31. März 2025
AWSBackupSearchOperatorAccess — Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die <code>AWSBackupSearchOperatorAccess</code> AWS verwaltete Richtlinie hinzugefügt.	27. Februar 2025

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die Erlaubnis <code>rds:AddTagsToResource</code> , kontoübergreifende Kopien von Backups mit Amazon RDS-Mehrmandanten-Snapshots zu unterstützen. Diese Genehmigung ist erforderlich, um Vorgänge abzuschließen, wenn ein Kunde eine kontoübergreifende Kopie eines mandantenfähigen RDS-Snapshots erstellen möchte.	8. Januar 2025
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat die Berechtigungen <code>rds:CreateTenantDatabase</code> und <code>rds>DeleteTenantDatabase</code> zu dieser Richtlinie hinzugefügt, um den Wiederherstellungsprozess von Amazon RDS-Ressourcen zu unterstützen. Diese Berechtigungen sind erforderlich, um Kundenvorgänge zur Wiederherstellung von Multi-Tenant-Snapshots abzuschließen.	8. Januar 2025

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForItemRestores — Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupServiceRolePolicyForItemRestores AWS verwaltete Richtlinie hinzugefügt.	26. November 2024
AWSBackupServiceRolePolicyForIndexing — Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupServiceRolePolicyForIndexing AWS verwaltete Richtlinie hinzugefügt.	26. November 2024
AWSBackupServiceRolePolicyForBackup – 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
AWSBackupServiceRolePolicyForS3Backup — Aktualisierung einer bestehenden 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

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Dieser Richtlinie wurde <code>backup:TagResource</code> eine Genehmigung hinzugefügt. Die Genehmigung ist erforderlich, um bei der Erstellung eines Wiederherstellungspunkts Tagging-Berechtigungen zu erhalten.	17. Mai 2024
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die Erlaubnis wurde hinzugefügt <code>trds:DeleteDBInstanceAutomatedBackups</code>. 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 <code>storagegateway:ListVolumes</code> von bis aktualisiert <code>arn:aws:storagegateway:*:*:gateway/*</code>, * um einer Änderung des Storage Gateway Gateway-API-Modells Rechnung zu tragen.	1. Mai 2024

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Backup hat den Amazon-Ressourcennamen (ARN) mit Genehmigung <code>storagegateway:ListVolumes</code> von <code>arn:aws:storagegateway:*:*:gateway/*</code> , * um einer Änderung des Storage Gateway Gateway-API-Modells Rechnung zu tragen.	1. Mai 2024

Änderungen	Beschreibung	Date
AWSServiceRolePolicyForBackupRestoreTesting – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen hinzugefügt, um Wiederherstellungspunkte und geschützte Ressourcen zu beschreiben und aufzulisten, um Wiederherstellungstestpläne durchzuführen: <pre>backup:DescribeRecoveryPoint backup:DescribeProtectedResource ,backup:ListProtectedResources ,undbackup:ListRecoveryPointsByResource .</pre> Die Berechtigung <code>ec2:DescribeSnapshotTierStatus</code> zur Unterstützung von Amazon EBS-Archiv-Tier-Speicher wurde hinzugefügt. Die Erlaubnis <code>rds:DescribeDBClusterAutomatedBackups</code> zur Unterstützung kontinuierlicher Amazon Aurora Aurora-Backups wurde hinzugefügt. Die folgenden Berechtigungen wurden hinzugefügt, um Wiederherstellungstests von Amazon Redshift Redshift-Backups zu unterstützen: <pre>redshift:DescribeC</pre>	14. Februar 2024

Änderungen	Beschreibung	Date
	clusters und redshift: DeleteCluster . Es wurde die Erlaubnis timestream:DeleteTable hinzugefügt, Wiederherstellungstests von Amazon Timestream-Backups zu unterstützen.	
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigungen ec2:DescribeSnapshots und ec2:RestoreSnapshot wurden hinzugefügt. Diese Berechtigungen sind erforderlich, damit Benutzer die Möglichkeit haben, Amazon EBS-Ressourcen, die mit gespeichert wurden, AWS Backup aus dem Archivspeicher wiederherzustellen. Für EC2 Instance-Wiederherstellungen müssen Sie auch die in der folgenden Richtlinienerklärung aufgeführten Berechtigungen angeben, um die EC2 Instance zu starten:	8. November 2023

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die Berechtigungen <code>ec2:DescribeSnapshotsTierStatus</code> und <code>ec2:ModifySnapshotTier</code> 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

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die Berechtigungen <code>ec2:DescribeSnapshots</code> und <code>ec2:ModifySnapshotAttribute</code> der <code>Tier</code> 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 <code>rds:DescribeDBClusterSnapshots</code> und wurden hinzugefügt <code>rds:RestoreDBClusterToPointInTime</code> , was für PITR (point-in-time Wiederherstellungen) von Aurora-Clustern erforderlich ist.	

Änderungen	Beschreibung	Date
AWSServiceRolePolicyForBackupRestoreTesting – Neue Richtlinie	Stellt die für die Durchführung von Wiederherstellungstests erforderlichen Berechtigungen bereit. Die Berechtigungen umfassen die Aktionen <code>list</code> , <code>read</code> , and <code>write</code> für die folgenden Dienste, die in Wiederherstellungstests aufgenommen werden sollen: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon, Amazon EFS EC2, FSx für Lustre, für Windows File Server, FSx für ONTAP, FSx FSx für OpenZFS, Amazon Neptune, Amazon RDS und Amazon S3.	8. November 2023
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	<code>restore-testing.backup.amazonaws.com</code> wurde <code>IamPassRolePermissions</code> und <code>IamCreateServiceLinkedRolePermissions</code> hinzugefügt. Dieser Zusatz ist erforderlich, um Wiederherstellungstests im Auftrag von Kunden durchzuführen. AWS Backup	8. November 2023

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die Berechtigungen <code>rds:DescribeDBClusterSnapshots</code> und <code>rds:RestoreDBClusterToPointInTime</code> wurden hinzugefügt, 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 <code>rds:DescribeDBClusterAutomatedBackups</code> , 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 <code>rds:DescribeDBClusterAutomatedBackups</code> , die für die kontinuierliche Sicherung und point-in-time Wiederherstellung von Aurora-Clustern erforderlich ist.	6. September 2023

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die Erlaubnis wurde hinzugefügt <code>trds:DescribeDBClusterAutomatedBackups</code> . Diese Genehmigung ist für die AWS Backup Unterstützung der kontinuierlichen Sicherung und point-in-time Wiederherstellung von Aurora-Clustern erforderlich. Es wurde die Erlaubnis <code>rds>DeleteDBClusterAutomatedBackups</code> 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 EXPIRED-Status zu verhindern. Die Erlaubnis <code>rds:ModifyDBCluster</code> , mit Aurora-Clustern AWS Backup zu interagieren, wurde hinzugefügt. Dieser Zusatz ermöglicht es Benutzern, kontinuierliche Sicherungen auf der Grundlage der gewünschten	6. September 2023

Änderungen	Beschreibung	Date
	Konfigurationen zu aktivieren oder zu deaktivieren.	
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde die Aktion hinzugefügt <code>gtram:GetResourceShareAssociations</code> , um dem Benutzer die Erlaubnis zu erteilen, Ressourcenfreigabezuordnungen für einen neuen Tresortyp abzurufen.	08. August 2023
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde die Aktion hinzugefügt <code>gtram:GetResourceShareAssociations</code> , um dem Benutzer die Erlaubnis zu erteilen, Ressourcenfreigabezuordnungen für einen neuen Tresortyp abzurufen.	08. August 2023
AWSBackupServiceRolePolicyForS3Backup — Aktualisierung auf eine bestehende Richtlinie	Es wurde die Erlaubnis hinzugefügt <code>s3:PutInventoryConfiguration</code> , die Geschwindigkeit der Backup-Leistung mithilfe eines Bucket-Inventars zu erhöhen.	1. August 2023

Änderungen	Beschreibung	Date
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: <code>storagegateway:AddTagsToResource</code> , <code>elasticfilesystem:TagResource</code> , „nur <code>ec2:CreateTags</code> für <code>ec2:CreateAction</code> das, was entweder <code>RunInstances</code> oder <code>CreateVolume</code> , <code>fsx:TagResource</code> , und beinhalte <code>tcloudformation:TagResource</code> .	22. Mai 2023
AWSBackupAuditAccess – Aktualisierung auf eine bestehende Richtlinie	Die Ressourcenauswahl innerhalb der API wurde <code>config:DescribeComplianceByConfigRule</code> durch eine Platzhalterressource ersetzt, um Benutzern die Auswahl von Ressourcen zu erleichtern.	11. April 2023

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Wiederherstellung von Amazon EFS mithilfe eines vom Kunden verwalteten Schlüssels wurde hinzugefügt: <code>kms:GenerateDataKeyWithoutPlaintext</code> . 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 <code>config:DescribeConfigRuleEvaluationStatus</code> Aktionen <code>config:DescribeConfigRules</code> und wurden aktualisiert, sodass AWS Backup Audit Manager auf von AWS Backup Audit Manager verwaltete Regeln zugreifen kann AWS Config .	9. März 2023

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForS3Restore — Aktualisierung auf eine bestehende Richtlinie	Der Richtlinie wurden die folgenden Berechtigungen hinzugefügt: <code>kms:Decrypt</code> , <code>s3:PutBucketOwnershipControls</code> , <code>s3:GetBucketOwnershipControls</code> , und <code>AWSBackupServiceRolePolicyForS3Restore</code> . 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

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen hinzugefügt, um Backups mithilfe von VMware Tags virtuelle r 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

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurden die folgenden Berechtigungen zur Unterstützung von Timestream-Backup-Jobs hinzugefügt: <code>timestream:StartAwsBackupJob</code> <code>timestream:GetAwsBackupStatus</code> <code>timestream:ListTables</code> <code>timestream:ListDatabases</code> <code>timestream:ListTagsForResource</code> , <code>timestream:DescribeTable</code> <code>timestream:DescribeDatabase</code> , und <code>timestream:DescribeEndpoints</code>	13. Dezember 2022

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Wiederherstellungsaufträgen wurden hinzugefügt: <code>timestream:StartAwsRestoreJob</code> , <code>timestream:GetAwsRestoreStatus</code> , <code>timestream:ListTables</code> , <code>timestream:ListTagsForResource</code> , <code>timestream:ListDatabases</code> , <code>timestream:DescribeTable</code> , <code>timestream:DescribeDatabase</code> , <code>s3:GetBucketAcl</code> , und <code>timestream:DescribeEndpoints</code>	13. Dezember 2022
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt: <code>timestream:ListTables</code> , <code>timestream:ListDatabases</code> , <code>s3:ListAllMyBuckets</code> und <code>timestream:DescribeEndpoints</code>	13. Dezember 2022

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt: <code>timestream:ListDatabases</code> , <code>timestream:ListTables</code> <code>s3:ListAllMyBuckets</code> , und. <code>timestream:DescribeEndpoints</code>	13. Dezember 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Timestream-Ressourcen wurden hinzugefügt: <code>timestream:ListDatabases</code> <code>timestream:ListTables</code> , <code>timestream:ListTagsForResource</code> , <code>timestream:DescribeDatabase</code> , <code>timestream:DescribeTable</code> , <code>timestream:GetAwsBackupStatus</code> <code>timestream:GetAwsRestoreStatus</code> , und. <code>timestream:DescribeEndpoints</code>	13. Dezember 2022

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Ressourcen wurden hinzugefügt: <code>redshift:DescribeClusters</code> , <code>redshift:DescribeClusterSubnetGroups</code> , <code>redshift:DescribeNodeConfigurationOptions</code> , <code>redshift:DescribeOrderableClusterOptions</code> , <code>redshift:DescribeClusterParameterGroups</code> , <code>redshift:DescribeClusterTracks</code> , <code>redshift:DescribeSnapshotSchedules</code> , und <code>ec2:DescribeAddresses</code>	27. November 2022

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Wiederherstellungsaufträgen wurden hinzugefügt: <code>redshift:RestoreFromClusterSnapshot</code> , <code>redshift:RestoreTableFromClusterSnapshot</code> , <code>redshift:DescribeClusters</code> , <code>redshift:DescribeTableRestoreStatus</code> .	27. November 2022
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von Amazon Redshift Redshift-Backup-Jobs wurden hinzugefügt: <code>redshift:CreateClusterSnapshot</code> , <code>redshift:DescribeClusterSnapshots</code> , <code>redshift:DescribeTags</code> , <code>redshift>DeleteClusterSnapshot</code> , <code>redshift:DescribeClusters</code> , <code>redshift:CreateTags</code> .	27. November 2022

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von CloudFormation Ressourcen wurde hinzugefügt: <code>cloudformation:ListStacks</code> .	27. November 2022
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von CloudFormation Ressourcen wurde hinzugefügt: <code>cloudformation:ListStacks</code> .	27. November 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von CloudFormation Ressourcen wurden hinzugefügt: <code>redshift:DescribeClusterSnapshots</code> <code>redshift:DescribeTags</code> , <code>redshift>DeleteClusterSnapshot</code> , und <code>redshift:DescribeClusters</code> .	27. November 2022

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um Backup-Jobs für den CloudFormation Anwendungsstapel zu unterstützen: <code>cloudformation:GetTemplate</code> <code>cloudformation:DescribeStacks</code> , und <code>cloudformation:ListStackResources</code> .	16. November 2022
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um Backup-Jobs für den CloudFormation Anwendungsstapel zu unterstützen: <code>cloudformation:CreateChangeSet</code> und <code>cloudformation:DescribeChangeSet</code>	16. November 2022

Änderungen	Beschreibung	Date
AWSBackupOrganizationAdminAccess – Aktualisierung auf eine bestehende Richtlinie	Dieser Richtlinie wurden die folgenden Berechtigungen hinzugefügt, damit Organisationsadministratoren die Funktion „Delegierter Administrator“ verwenden können: <code>organizations:ListDelegatedAdministrator</code> , und <code>organizations:RegisterDelegatedAdministrator</code> <code>organizations:DeregisterDelegatedAdministrator</code>	27. November 2022
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf EC2 Amazon-Instances wurden hinzugefügt: <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> <code>ssm-sap:BackupDatabase</code> , <code>ssm-sap:UpdateHanaBackupSettings</code> , <code>ssm-sap:GetDatabase</code> , und <code>ssm-sap:ListTagsForResource</code> .	20. November 2022

Änderungen	Beschreibung	Date
AWSBackupFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf EC2 Amazon-Instances wurden hinzugefügt: <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> , <code>ssm-sap:GetDatabase</code> , und <code>ssm-sap:ListTagsForResource</code> .	20. November 2022
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen zur Unterstützung von SAP HANA auf EC2 Amazon-Instances wurden hinzugefügt: <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> , <code>ssm-sap:GetDatabase</code> , und <code>ssm-sap:ListTagsForResource</code> .	20. November 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von SAP HANA auf EC2 Amazon-Instances wurde hinzugefügt: <code>ssm-sap:GetOperation</code> .	20. November 2022
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgende Berechtigung zur Unterstützung von Backup-Gateway-Wiederherstellungsaufträgen wurde einer EC2 Instanz hinzugefügt: <code>ec2:CreateTags</code> .	20. November 2022

Änderungen	Beschreibung	Date
AWSBackupDataTransferAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Berechtigungen wurden hinzugefügt, um die sichere Speicherdatenübertragung für EC2 Ressourcen von SAP HANA On Amazon zu unterstützen: backup-storage:StartObject backup-storage:Put Chunk backup-storage:Get Chunk ,backup-storage:Lis tChunks ,backup-storage:Lis tObjects ,backup-storage:GetObjectMetadata ,undbackup-storage:NotifyObject Complete .	20. November 2022

Änderungen	Beschreibung	Date
AWSBackupRestoreAccessForSAPHANA — Aktualisierung einer bestehenden Richtlinie	Es wurden die folgenden Berechtigungen für Ressourcenesitzer hinzugefügt, um die Wiederherstellung von EC2 Ressourcen von SAP HANA On Amazon durchzuführen: <pre> 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“.</pre>	20. November 2022
AWSBackupServiceRolePolicyForS3Backup — Aktualisierung einer bestehenden Richtlinie	Die Erlaubnis <code>s3:GetBucketAcl</code> zur Unterstützung von Backup-Vorgängen von AWS Backup für Amazon S3 wurde hinzugefügt.	24. August 2022

Änderungen	Beschreibung	Date
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: <code>rds:CreateDBInstance</code>	20. Juli 2022
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde die <code>s3:GetBucketTagging</code> 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 Aktionen hinzugefügt <code>fsx:CreateBackup</code> und neue <code>fsx:ListTagsForResource</code> Aktionen <code>fsx:DescribeVolumes</code> FSx zur Unterstützung von ONTAP-Backups auf Volume-Ebene hinzugefügt.	27. April 2022

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um den Benutzern Berechtigungen FSx zur Wiederherstellung von ONTAP-Volumes <code>fsx:DescribeVolumes</code> , <code>fsx:CreateVolumeFromBackup</code> <code>fsx:DeleteVolume</code> , und zu gewähren. <code>fsx:UntagResource</code>	27. April 2022
AWSBackupServiceRolePolicyForS3Backup — Aktualisierung einer bestehenden 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: <code>s3:GetBucketNotification</code> und <code>s3:PutBucketNotification</code> .	25. Februar 2022

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForS3Backup — Neue Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um den 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 , und s3:GetObjectVersion . Die folgenden Aktionen wurden hinzugefügt, um	17. Februar 2022

Änderungen	Beschreibung	Date
	Benutzern Berechtigungen zum Sichern ihrer verschlüsselten Amazon S3 S3-Daten zu gewähren: <code>kms:Decrypt</code> und <code>kms:DescribeKey</code> . 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: <code>events:DescribeRule</code> , <code>events:EnableRule</code> , <code>events:PutRule</code> , <code>events>DeleteRule</code> , <code>events:PutTargets</code> , <code>events:RemoveTargets</code> , <code>events:ListTargetsByRule</code> , <code>events:DisableRule</code> , <code>cloudwatch:GetMetricData</code> , und <code>events:ListRules</code> .	

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForS3 Restore — Neue Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Wiederherstellung ihrer Amazon S3 S3-Buckets zu gewähren: s3:CreateBucket s3:ListBucketVersion s3:ListBucket s3:GetBucketVersion s3:GetBucketLocation s3:PutBucketVersion . 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 s3:ListMultipartUploadParts .	17. Februar 2022

Änderungen	Beschreibung	Date
	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zur Verschlüsselung ihrer wiederhergestellten Amazon S3 S3-Daten zu gewähren: <code>kms:Decrypt</code> <code>kms:DescribeKey</code> , und <code>kms:GenerateDataKey</code> .	
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde hinzugefügt <code>s3:ListAllMyBuckets</code> , 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 <code>backup-gateway:ListVirtualMachines</code> , um Benutzern die Möglichkeit zu geben, eine Liste ihrer virtuellen Maschinen einzusehen und auszuwählen, welche sie einem Backup-Plan zuweisen möchten. Wurde hinzugefügt <code>backup-gateway:ListTagsForResource</code> , um Benutzern das Recht zu gewähren, die Tags für ihre virtuellen Maschinen aufzulisten.	30. November 2021

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt <code>backup-gateway:Backup</code> , um Benutzern Rechte für die Wiederherstellung ihrer virtuellen Maschinen-Backups zu gewähren. AWS Backup wurde auch hinzugefügt <code>backup-gateway:ListTagsForResource</code> , 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 <code>backup-gateway:Restore</code> , um Benutzern Rechte für die Wiederherstellung ihrer virtuellen Maschinen-Backups zu gewähren.	30. November 2021

Änderungen	Beschreibung	Date
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 virtuellen Maschinen zu gewähren: <code>„backup-gateway:AssociateGatewayToServer“</code> , <code>„backup-gateway>CreateGateway“</code> , <code>„backup-gateway>DeleteGateway“</code> , <code>„backup-gateway>DeleteHypervisor“</code> , <code>„backup-gateway:DissociateGatewayFromServer“</code> , <code>„backup-gateway:ImportHypervisorConfiguration“</code> , <code>„backup-gateway:ListGateways“</code> , <code>„backup-gateway:ListHypervisors“</code> , <code>„backup-gateway:ListTagsForResource“</code> , <code>„backup-gateway:ListVirtualMachines“</code> , <code>„backup-gateway:PutMaintenanceStartTime“</code> , <code>„backup-gateway:TagResource“</code> , <code>„backup-gateway:Test“</code>	30. November 2021

Änderungen	Beschreibung	Date
	<code>tHypervisorConfiguration ,backup-gateway:UntagResource ,backup-gateway:UpdateGatewayInformation , undbackup-gateway:UpdateHypervisor .</code>	
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die folgenden Aktionen wurden hinzugefügt, um Benutzern Berechtigungen zum Sichern ihrer virtuellen Maschinen zu gewähren: <code>backup-gateway:ListGateways</code> , <code>backup-gateway:ListHypervisors</code> , <code>backup-gateway:ListTagsForResource</code> , und <code>backup-gateway:ListVirtualMachines</code> .	30. November 2021
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Es wurde hinzugefügt <code>dynamodb:ListTagsOfResource</code> , um Benutzern die Rechte zu gewähren, Tags ihrer DynamoDB-Tabellen aufzulisten, um sie mithilfe der erweiterten DynamoDB-Backup-Funktionen zu sichern.	23. November 2021

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt dynamisch: <code>StartAwsBackupJob</code>, um Benutzern Berechtigungen zum Sichern ihrer DynamoDB-Tabellen mithilfe erweitert er Backup-Funktionen zu gewähren. Hinzugefügt dynamisch: <code>ListTagsOfResource</code>, um Benutzern Berechtigungen zum Kopieren von Tags aus ihren DynamoDB-Quellentabellen in ihre Backups zu gewähren.	23. November 2021
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	AWS Backup Es wurde hinzugefügt dynamisch: <code>RestoreTableFromAwsBackup</code>, um Benutzern Rechte zur Wiederherstellung ihrer DynamoDB-Tabellen zu gewähren, die mit den erweiterten DynamoDB-Backup-Funktionen gesichert wurden.	23. November 2021

Änderungen	Beschreibung	Date
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, <code>rds:DescribeDBSnapshots</code> weil sie <code>backup:GetRecoveryPointRestoreMetadata</code> überflüssig waren. AWS Backup brauchte nicht beides <code>backup:GetRecoveryPointRestoreMetadata</code> und <code>backup:Get*</code> als Teil von <code>AWSBackupOperatorAccess</code> . Ich AWS Backup brauchte auch nicht beides <code>rds:DescribeDBSnapshots</code> und <code>rds:describeDBSnapshots</code> als Teil von <code>AWSBackupOperatorAccess</code> .	23. November 2021

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neuen Aktionen <code>elasticfilesystem:DescribeFileSystems</code>, <code>dynamodb:ListTables</code>, <code>storagegateway:ListVolumes</code>, <code>ec2:DescribeVolumes</code>, <code>ec2:DescribeInstances</code>, und wurden hinzugefügt <code>rds:DescribeDBInstances</code>, <code>rds:DescribeDBClusters</code>, <code>fsx:DescribeFileSystems</code> 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 <code>AWSBackupAuditAccess</code>, 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

Änderungen	Beschreibung	Date
AWSServiceRolePolicyForBackupReports – Neue Richtlinie	Es wurde hinzugefügt <code>AWSServiceRolePolicyForBackupReports</code> , 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 <code>iam:CreateServiceLinkedRole</code> , 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

Änderungen	Beschreibung	Date
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Es wurde die neue Aktion <code>hinzugefügt dynamodb:DeleteBackup</code> , um die <code>DeleteRecoveryPoint</code> 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 <code>backup:GetRecoveryPointRestoreMetadata</code> wurden entfernt <code>rds:DescribeDBSnapshots</code> , weil sie überflüssig waren. AWS Backup brauchte nicht beide <code>backup:GetRecoveryPointRestoreMetadata</code> und <code>backup:Get*</code> als Teil von <code>AWSBackupOperatorAccess</code> . Also AWS Backup brauchte ich nicht beides <code>rds:DescribeDBSnapshots</code> und <code>rds:describeDBSnapshots</code> als Teil von <code>AWSBackupOperatorAccess</code> .	25. Mai 2021

Änderungen	Beschreibung	Date
AWSBackupOperatorAccess – Aktualisierung auf eine bestehende Richtlinie	Die Aktionen <code>backup:GetRecoveryPointRestoreMetadata</code> wurden entfernt, <code>trds:DescribeDBSnapshots</code>, weil sie überflüssig waren. AWS Backup brauchte nicht beides <code>backup:GetRecoveryPointRestoreMetadata</code> und <code>backup:Get*</code> als Teil von <code>AWSBackupOperatorAccess</code>. Ich AWS Backup brauchte auch nicht beides <code>trds:DescribeDBSnapshots</code> und <code>trds:describeDBSnapshots</code> als Teil von <code>AWSBackupOperatorAccess</code>.	25. Mai 2021
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt <code>fsx:TagResource</code>, um Ihnen die <code>StartRestoreJob</code> Erlaubnis zu erteilen, während des Wiederherstellungsvorgangs Tags auf FSx Amazon-Dateisysteme anzuwenden.	24. Mai 2021

Änderungen	Beschreibung	Date
AWSBackupServiceRolePolicyForRestores – Aktualisierung auf eine bestehende Richtlinie	Es wurden die neuen Aktionen hinzugefügt <code>ec2:DescribeImages</code> und <code>ec2:DescribeInstances</code> die <code>StartRestoreJob</code> Erlaubnis erteilt, Ihnen die Wiederherstellung von EC2 Amazon-Instances von Wiederherstellungspunkten zu ermöglichen.	24. Mai 2021
AWSBackupServiceRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt <code>fsx:CopyBackup</code> , um Ihnen die <code>StartCopyJob</code> Erlaubnis zu erteilen, FSx Amazon-Wiederherstellungspunkte zwischen Regionen und Konten zu kopieren.	12. April 2021
AWSBackupServiceLinkedRolePolicyForBackup – Aktualisierung auf eine bestehende Richtlinie	Die neue Aktion wurde hinzugefügt <code>fsx:CopyBackup</code> , um Ihnen die <code>StartCopyJob</code> Erlaubnis zu erteilen, FSx Amazon-Wiederherstellungspunkte zwischen Regionen und Konten zu kopieren.	12. April 2021

Änderungen	Beschreibung	Date
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 <code>kms:Decrypt</code> und <code>kms:GenerateDataKey</code> zur IAM-Rolle hinzufügen, die für die Sicherung verwendet wird.	10. März 2021

Änderungen	Beschreibung	Date
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 <code>rds:ModifyDBInstance</code> vorhanden ist, die in Ihrer Backup-Plan-Konfiguration definiert ist. Um kontinuierliche Amazon RDS-Sicherungen wiederherzustellen, müssen Sie die Berechtigung <code>rds:RestoreDBInstanceToPointInTime</code> 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 <code>rds:DescribeDBInstanceAutomatedBackups</code> API-Berechtigung in Ihre von IAM verwaltete Richtlinie aufnehmen.	10. März 2021

Änderungen	Beschreibung	Date
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 angegebene dienstbezogene Rolle `AWSServiceRoleForBackup`, um in Ihrem Namen Backups Ihrer AWS Ressourcen zu erstellen und zu löschen.

Die `AWSServiceRoleForBackup` dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `backup.amazonaws.com`

Die Berechtigungen für diese Richtlinie finden Sie [AWSBackupServiceLinkedRolePolicyforBackup](#) in 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-Managementkonsole, 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 AWSService RoleForBackup 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 Rollenbeschreibung](#) 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 AWSService RoleForBackup (Konsole) verwendet werden

1. Gehen Sie wie unter [Einen Tresor löschen](#) beschrieben vor, um all 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 AWSService RoleForBackup ()AWS CLI verwendet werden

1. Um alle 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 AWSService RoleForBackup (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 AWSService RoleForBackup 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:

- `reports.backup.amazonaws.com`

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSServiceRolePolicyForBackupReports](#) in der Referenz zu von AWS verwalteten 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-Managementkonsole, der oder der AWS API erstellen AWS CLI, AWS Backup erstellt die dienstbezogene Rolle für Sie.

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 `AWSService RoleForBackupReports` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie im [IAM-Benutzerhandbuch unter Bearbeiten einer Beschreibung einer dienstbezogenen Rolle](#).

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 `AWSService RoleForBackupReports` (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 AWSService RoleForBackupReports (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 AWSService RoleForBackupReports (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 AWSService RoleForBackupReports 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 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 `AWSServiceRoleForBackupRestoreTesting`— Stellt Backup-Berechtigungen für die Durchführung von Wiederherstellungstests bereit.

Die serviceverknüpfte Rolle `AWSServiceRoleForBackupRestoreTesting` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `restore-testing.backup.amazonaws.com`

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSServiceRolePolicyForBackupRestoreTesting](#) in der Referenz zu von AWS verwalteten 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-Managementkonsole AWS CLI, der oder der AWS API durchführen, AWS Backup erstellt die dienstbezogene Rolle für Sie.

 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 ermöglicht es Ihnen nicht, die mit dem AWSService RoleForBackupRestoreTesting Dienst verknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename 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 Rollenbeschreibung](#) 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 AWSService RoleForBackupRestoreTesting (Konsole) verwendet werden

- Informationen zum Löschen aller Wiederherstellungstestpläne finden Sie unter [Wiederherstellungstests](#).

Um AWS Backup Ressourcen zu löschen, die von `AWSServiceRoleForBackupRestoreTesting` (AWS CLI) verwendet werden

- Um Wiederherstellungstestpläne zu löschen, verwenden Sie `delete-restore-testing-plan`.

Um AWS Backup Ressourcen zu löschen, die von der `AWSServiceRoleForBackupRestoreTesting` (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 `AWSServiceRoleForBackupRestoreTesting` 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](#).

Serviceübergreifende 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 privilegiere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit dem verwirrten Stellvertreter führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS bietet Tools, mit denen Sie Ihre Daten für alle Dienste mit Dienstprinzipalen schützen können, denen Zugriff auf Ressourcen in Ihrem Konto gewährt wurde.

Wir empfehlen, die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, AWS Backup die der Ressource einen anderen Dienst gewähren. 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 Amazon SNS SNS-Themen in Ihrem Namen veröffentlichen.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `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 Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws::servicename::123456789012:*`.

Die folgende Beispielrichtlinie zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, AWS Backup um das Problem des verwirrten Stellvertreters zu vermeiden. Diese Richtlinie gewährt dem Service Principal `backup-storage.amazonaws.com` nur dann die Möglichkeit, KMS-Aktionen durchzuführen, wenn der Service Principal im Namen des Kontos 123456789012 in den Backup-Tresoren handelt: AWS

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 über das Backup-Gateway

VMware verbunden sind. AWS Backup ermöglicht Backups von Daten, die mit anderen Diensten gespeichert wurden, darunter Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon FSx für Windows File Server EC2, Amazon für Lustre, Amazon FSx für OpenZFS, Amazon FSx für NetApp ONTAP, Amazon Neptune, Amazon RDS und Amazon Redshift.

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 unter erhältlich ist. [AWS Artifact](#)

Rechtliche Bestimmungen und AWS Backup

Überblick über gesetzliche Aufbewahrungsfristen

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.

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. Gesetzliche Aufbewahrungsfristen gelten nicht für [fortlaufende](#) Backups.

Wenn eine gesetzliche Aufbewahrungsfrist erstellt wird, können dabei bestimmte Filterkriterien wie Ressourcentypen und Ressourcen berücksichtigt IDs werden. Darüber hinaus können Sie den Zeitraum für das Erstellungsdatum der Sicherungen definieren, die Sie in eine gesetzliche Aufbewahrungsfrist aufnehmen möchten.

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 eines gesetzlichen Speichers sein.

Beachten Sie, dass [AWS Backup Vault Lock](#) zwar zusätzlichen Schutz und die Unveränderlichkeit eines Tresors bietet, eine gesetzliche Aufbewahrungsfrist jedoch zusätzlichen Schutz vor dem Löschen einzelner Backups (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.

Mehrere gesetzliche Sperren

Ein Backup kann mehrere gesetzliche Aufbewahrungsfristen haben. Rechtliche Aufbewahrungsfristen und Backups stehen in einer Viele-Viele-Beziehung, was bedeutet, dass ein Backup mehr als eine gesetzliche Aufbewahrungsfrist haben kann und eine gesetzliche Aufbewahrungsfrist mehr als ein Backup umfassen kann.

Ein Backup kann nicht gelöscht werden, solange es mindestens eine gesetzliche Aufbewahrungsfrist hat. Nachdem alle gesetzlichen Aufbewahrungsfristen für ein Backup aufgehoben wurden, unterliegt es den Eigenschaften seines Aufbewahrungslbenszyklus. Behalten Sie mindestens eine gesetzliche Aufbewahrungsfrist bei, um das Löschen von Backups zu verhindern. Rechtliche Aufbewahrungsfristen können auf einen Wiederherstellungspunkt angewendet werden, der über das Aufbewahrungsdatum des Backup-Lebenszyklus hinaus aufbewahrt wird (aufgrund einer bestehenden gesetzlichen Sperre).

Für jedes Konto können maximal 50 aktive Aufbewahrungsfristen gleichzeitig bestehen.

Erstellen einer gesetzlichen Aufbewahrungsfrist

Eine gesetzliche Aufbewahrungsfrist kann zu einem bestehenden Backup (Wiederherstellungspunkt) hinzugefügt werden.

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 Aufbewahrungsfristen 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 aus.
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 Details 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 mithilfe der AWS CLI

Sie können eine gesetzliche Sperre mit dem [create-legal-hold](#)Befehl 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 sich Details zur gesetzlichen Sperre in der AWS Backup Konsole oder programmgesteuert anzeigen lassen.

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: und. [ListLegalHoldsGetLegalHold](#)

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 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 Gesetzliche Aufbewahrungsfristen (Legal holds) können Sie alle Ihre Sperren einsehen. Wenn die Freigabe erfolgreich war, wird der Status dieser Sperre als `angezeigtReleased`.

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

Malware-Schutz in AWS Backup

Das Scannen Ihrer Backups auf Malware wird von Amazon GuardDuty Malware Protection bereitgestellt. Mit Amazon GuardDuty Malware Protection for AWS Backup können Sie das Scannen von Wiederherstellungspunkten mithilfe vorhandener Backup-Workflows automatisieren oder On-Demand-Scans von zuvor erstellten Backups initiieren. Diese AWS native Lösung trägt dazu bei, dass Ihre Backups frei von potenzieller Malware sind, sodass Sie Compliance-Anforderungen erfüllen und schneller auf böswillige Vorfälle reagieren können, indem sie die Wiederherstellung sauberer Daten sicherstellen.

Eine Liste der unterstützten Ressourcentypen und Regionen finden Sie auf der [Seite zur Verfügbarkeit von Funktionen](#).

Topics

- [Integration mit Amazon GuardDuty](#)
- [Sofortige Zugriffsberechtigungen Backup](#)
- [Wie verwendet man das Scannen nach Schadsoftware](#)
- [Zugriff](#)
- [Inkrementelle oder vollständige Scans](#)
- [Überwachung Ihrer Malware-Scans](#)
- [Die Scanergebnisse verstehen](#)
- [Behebung von Scanfehlern](#)
- [Metering \(Messung\)](#)
- [Kontingente](#)
- [Schritte zur Verwendung von Konsole und CLI für Malware-Scantypen](#)

Integration mit Amazon GuardDuty

AWS Backup lässt sich in Amazon GuardDuty Malware Protection integrieren, um Bedrohungen für Ihre Wiederherstellungspunkte zu erkennen. Wenn Sie einen Malware-Scan starten, ruft er nach Abschluss jedes Backups AWS Backup automatisch die `StartMalwareScan` API GuardDuty von Amazon auf und übergibt die Details des Wiederherstellungspunkts und Ihre Anmeldeinformationen für die Scannerrolle. Amazon beginnt GuardDuty dann mit dem Lesen, Entschlüsseln und Scannen aller Dateien und Objekte innerhalb des Backups.

Wenn Amazon GuardDuty auf Ihre Backup-Daten zugreift, wird dieser Zugriff aus AWS CloudTrail Gründen der Sichtbarkeit angemeldet.

Weitere Informationen zu dieser Integration finden Sie in der [Amazon GuardDuty Malware Protection-Dokumentation](#).

Sofortige Zugriffsberechtigungen Backup

Wenn Sie Amazon GuardDuty Malware Protection for AWS Backup mit S3-Backups verwenden, GuardDuty greift Amazon über drei Methoden auf Ihre S3-Backups zu APIs: `CreateBackupAccessPoint`, `DescribeBackupAccessPoint`, und `DeleteBackupAccessPoint`.

Amazon GuardDuty verwendet `CreateBackupAccessPoint`, um auf Ihre verschlüsselten Backup-Daten zuzugreifen. Wird während des Scan-Jobs GuardDuty verwendet, `DescribeBackupAccessPoint` um zu überprüfen, ob der Access Point erfolgreich erstellt wurde. Sobald der Scan abgeschlossen ist, werden GuardDuty Aufrufe aufgerufen, `DeleteBackupAccessPoint` um ihm den Zugriff auf Ihr Backup zu entziehen.

Dieser Workflow gilt sowohl für S3-Backups als auch für EC2 /EBS-Backups, die in einem Tresor mit logischem Air-Gap gespeichert sind.

Wie verwendet man das Scannen nach Schadsoftware

Wenn Sie Amazon GuardDuty Malware Protection mit verwenden AWS Backup, können Sie Ihre Backups automatisch auf Malware scannen. Diese Integration hilft Ihnen dabei, böartigen Code in Ihren Backups zu erkennen und saubere Wiederherstellungspunkte für Wiederherstellungsvorgänge zu identifizieren.

Amazon GuardDuty Malware Protection unterstützt zwei primäre Workflows für das Scannen Ihrer Backups:

- Automatisches Scannen von Schadsoftware mithilfe von Backup-Plänen — Aktivieren Sie Malware-Scans in Backup-Plänen, um die Malware-Erkennung zu automatisieren AWS Backup. Wenn diese Option aktiviert ist, AWS Backup wird nach jedem erfolgreichen Abschluss der Sicherung automatisch ein GuardDuty Amazon-Scan initiiert. Sie können entweder das vollständige oder das inkrementelle Scannen für bestimmte Regeln für den Backup-Plan konfigurieren, die festlegen, wie oft Ihre Backups gescannt werden. Weitere Informationen zu den Scantypen finden Sie [the section called “Inkrementelle oder vollständige Scans”](#) weiter unten. AWS Backup empfiehlt, automatische Malware-Scans in Backup-Plänen zu aktivieren, um Bedrohungen nach der Erstellung des Backups proaktiv zu erkennen.
- Scans auf Anforderung — Führen Sie Scans auf Anforderung durch, um vorhandene Backups manuell zu scannen. Wählen Sie dabei zwischen vollständigen und inkrementellen Scans. AWS Backup empfiehlt, On-Demand-Scans zu verwenden, um Ihr letztes sauberes Backup zu identifizieren. Verwenden Sie beim Scannen vor einem Wiederherstellungsvorgang einen vollständigen Scan, um das gesamte Backup mit dem neuesten Bedrohungserkennungsmodell zu untersuchen.

Zugriff

Bevor Sie mit dem Schutz vor Schadsoftware beginnen, muss Ihr Konto über die erforderlichen Berechtigungen für die Vorgänge verfügen.

AWS Backup Für das Scannen nach Schadsoftware sind zwei IAM-Rollen erforderlich, um Ihre Wiederherstellungspunkte nach potenzieller Malware zu durchsuchen:

- Zunächst muss die `AWSBackupServiceRolePolicyForScans` verwaltete Richtlinie an Ihre bestehende oder neue Backup-Rolle angehängt werden. Dabei handelt es sich um dieselbe Rolle, die Sie in der Ressourcenzuweisung für Ihren Backup-Plan in der Konsole oder über die [BackupSelection API](#) finden. Diese verwaltete Richtlinie ermöglicht AWS Backup die Initiierung von Malware-Scans bei Amazon GuardDuty.
- Zweitens ist eine neue Scanner-Rolle mit einer `AWSBackupGuardDutyRolePolicyForScans` verwalteten, vertrauenswürdigen Richtlinie erforderlich. `malware-protection.guardduty.amazonaws.com` Dabei handelt es sich um dieselbe Rolle, die Sie im Bereich Malware-Schutz Ihres Backup-Plans in der Konsole oder in den Scaneinstellungen in Ihrer [BackupPlan API](#) finden. Diese Rolle wird bei der Initiierung eines Scans AWS Backup an Amazon GuardDuty übergeben und bietet Zugriff auf Backups.

Inkrementelle oder vollständige Scans

Bei Malware-Scans haben Sie die Möglichkeit, je nach Ihren Sicherheitsanforderungen und Kostenerwägungen zwischen inkrementellen und vollständigen Scans zu wählen.

Inkrementelle Scans analysieren nur die Daten, die sich zwischen dem Ziel- und dem Basiswiederherstellungspunkt geändert haben. Diese Scans sind schneller und kostengünstiger für regelmäßige Scans und eignen sich daher ideal für regelmäßige Backups, bei denen Sie neu gesicherte Daten scannen möchten.

AWS Backup führt in den folgenden Situationen einen vollständigen Scan durch, auch wenn inkrementelles Scannen ausgewählt ist:

- **Erstmalige Scans:** Der erste Scan einer Ressource ist immer ein vollständiger Scan, sodass Amazon GuardDuty einen Basiswert potenzieller Bedrohungen ermitteln kann. Nachfolgende Scans werden dann inkrementell durchgeführt.
- **Abgelaufener Basiswert:** Wenn Ihr Basiswiederherstellungspunkt vor mehr als 90 Tagen gescannt wurde, wird ein vollständiger Scan durchgeführt. Da Amazon GuardDuty Suchinformationen nur 90 Tage lang aufbewahrt, muss ein neuer Basiswert festgelegt werden, um genaue Scanergebnisse zu gewährleisten.
- **Gelöschter Basiswert:** Wenn Ihr Basiswiederherstellungspunkt gelöscht wird, bevor Ihr nächster inkrementeller Scan gestartet wird, erfolgt automatisch ein vollständiger Scan.

Bei vollständigen Scans wird der gesamte Erholungspunkt unabhängig von vorherigen Scans untersucht. Diese Scans bieten zwar eine umfassende Abdeckung, dauern jedoch länger und sind mit höheren Kosten verbunden. Sie können vollständige Scans bei Bedarf ausführen oder sie über Ihre Backup-Pläne planen. AWS Backup empfiehlt, regelmäßige vollständige Scans in Ihren Backup-Plänen in längeren Intervallen zu konfigurieren, um sicherzustellen, dass Ihre gesamten Backup-Daten regelmäßig mit dem neuesten Malware-Signaturmodell gescannt werden.

Um ein optimales Sicherheits- und Kostenmanagement zu erzielen, sollten Sie bei der Auswahl der Scantypen die Häufigkeit Ihrer Backups berücksichtigen.

Note

Das Scannen von Schadsoftware wird derzeit für kontinuierliche Amazon S3 S3-Wiederherstellungspunkte nicht unterstützt. Um kontinuierliche Amazon S3 S3-Backups zu scannen, konfigurieren Sie regelmäßige Backups für Ihre Amazon S3 S3-Ressourcen und

aktivieren Sie Malware-Scans für diese regelmäßigen Backups. Sie können eine [Kombination aus kontinuierlichen und regelmäßigen Backups](#) für Ihre Amazon S3 S3-Buckets verwenden.

 Note

Inkrementelles Scannen nach Schadsoftware wird für EC2 Amazon-Wiederherstellungspunkte in einem [Tresor mit logischem Air-Gap oder für kopierte Amazon-Wiederherstellungspunkte](#) nicht unterstützt. EC2

Überwachung Ihrer Malware-Scans

Nachdem das Scannen aktiviert wurde, GuardDuty bieten sowohl AWS Backup Amazon als auch Amazon Überwachungs- und Benachrichtigungsmechanismen, mit denen Sie Ihre Ergebnisse verfolgen können:

- **AWS Backup Konsole:** Die AWS Backup Konsole wird mit `ListScanJobs` und betrieben `DescribeScanJob` APIs. Im Bereich Malware-Schutz finden Sie eine Liste der Scanaufträge, die den Auftragsstatus und die Scanergebnisse darstellt. AWS Backup unterstützt auch eine `ListScanJobSummaries` API, ist jedoch nicht in der Konsole verfügbar.
- **AWS Backup Audit Manager:** Sie können einen Scanbericht einrichten, in dem alle AWS Backup initiierten Malware-Scanaufträge der letzten 24 Stunden angezeigt werden.
- **GuardDuty Amazon-Konsole:** Wenn Amazon Base aktiviert GuardDuty ist, können Sie Details in den Malware-Scan-Ergebnissen einsehen und Malware auf der GuardDuty Amazon-Ergebnisseite untersuchen. Sie können Informationen wie die Bedrohung und den Dateinamen, den Dateipfad, die objects/files gescannten Dateien, die gescannten Byte usw. anzeigen. Beachten Sie, dass diese detaillierten Bedrohungsinformationen nicht über AWS Backup verfügbar sind und Sie über die entsprechenden GuardDuty Amazon-Berechtigungen verfügen müssen, um diese Informationen einsehen zu können.
- **Amazon EventBridge:** AWS Backup Sowohl als auch Amazon GuardDuty senden EventBridge Ereignisse aus, sodass Backup- und Sicherheitsadministratoren synchron benachrichtigt werden können. Sie können benutzerdefinierte Regeln einrichten, um Benachrichtigungen zu erhalten, wenn die Scans abgeschlossen sind oder Malware erkannt wird.
- **AWS CloudTrail:** AWS Backup Sowohl Amazon als auch GuardDuty Amazon senden CloudTrail Ereignisse aus, sodass Sie den API-Zugriff überwachen können.

Die Scanergebnisse verstehen

Ihre Scanaufträge von AWS Backup werden einen Scanstatus und ein Scanergebnis haben.

Status scannen

Der Scanstatus gibt den Auftragsstatus an und kann folgende Werte haben:

CREATED, COMPLETED, COMPLETED_WITH_ISSUES, RUNNING, FAILED, oder CANCELED.

Es gibt mehrere Situationen, in denen Ihr Scanauftrag mit dem folgenden Status abgeschlossen wird: COMPLETED_WITH_ISSUES:

Für Amazon S3 S3-Backups gibt es size/type Objektbeschränkungen, die verhindern, dass Objekte gescannt werden. Wenn mindestens ein Objekt bei einem Scan übersprungen wird, wird der entsprechende Scanauftrag als COMPLETED_WITH_ISSUES markiert. Für Amazon EC2 /Amazon EBS-Backups gibt es size/quantity Volumenbeschränkungen, die dazu führen, dass Volumes beim Scannen übersprungen werden. Diese Situationen führen zu einem EC2 Amazon-/Amazon EBS-Backup-Job, zu dem Sie führen müssen. COMPLETED_WITH_ISSUES

Wenn Ihr Auftrag mit dem Status abgeschlossen wird COMPLETED_WITH_ISSUES und Sie weitere Informationen zu den Gründen benötigen, müssen Sie diese Informationen aus dem entsprechenden Scanauftrag über Amazon abrufen GuardDuty.

Note

Bei inkrementellen Scanaufträgen wird nur der Datenunterschied zwischen zwei Backups gescannt. Wenn also bei einem inkrementellen Scanauftrag keine der oben beschriebenen Situationen auftritt, wird er im Status beendet COMPLETE und erbt den Status nicht COMPLETED_WITH_ISSUES vom Basiswiederherstellungspunkt.

In seltenen Fällen GuardDuty kann es bei Amazon zu internen Problemen beim Scannen von Dateien und Objekten kommen, sodass Wiederholungsversuche möglicherweise erschöpft sind. In diesem Fall wird der Scanauftrag wie FAILED in AWS Backup und COMPLETED_WITH_ISSUES in Amazon angezeigt GuardDuty. Dieser Statusunterschied ermöglicht es Ihnen, die verfügbaren Scanergebnisse in Amazon einzusehen und GuardDuty gleichzeitig darauf hinzuweisen, dass nicht alle unterstützten Dateien und Objekte erfolgreich gescannt wurden.

Scan-Ergebnisse

Die Scanergebnisse geben ein aggregiertes Ergebnis von Amazon an GuardDuty und können Werte wie: `THREATS_FOUND`, oder `NO_THREATS_FOUND` haben.

Die Scanergebnisse geben an, ob an Ihren Wiederherstellungspunkten potenzielle Malware entdeckt wurde. Ein `NO_THREATS_FOUND` Status bedeutet, dass keine potenzielle Malware erkannt wurde, `THREATS_FOUND` weist aber darauf hin, dass potenzielle Malware entdeckt wurde. Detaillierte Informationen zu Bedrohungen erhalten Sie, wenn Sie über die GuardDuty Amazon-Konsole auf die vollständigen GuardDuty Ergebnisse von Amazon zugreifen oder APIs. Die Scanergebnisse sind auch in Form von EventBridge Ereignissen verfügbar, sodass Sie automatisierte Workflows einrichten können, die auf infizierte Backups reagieren.

Amazon GuardDuty bewahrt die Ergebnisse 90 Tage lang auf und verfolgt Dateien oder Objekte über inkrementelle Scans, um zu überwachen, ob Bedrohungen entfernt werden oder sich Malware-Signaturen ändern. Wenn beispielsweise in Backup 2 Malware entdeckt wird, wird das Scanergebnis angezeigt `THREATS_FOUND`. Wenn Sie auf Backup 3 einen inkrementellen Scan durchführen und dabei Backup 2 als Grundlage verwenden, bleibt das Scanergebnis erhalten, `THREATS_FOUND` es sei denn, die Bedrohung wurde aus den Daten entfernt.

Behebung von Scanfehlern

Zu den häufigsten Scanfehlern gehören unzureichende IAM-Berechtigungen, Dienstbeschränkungen und Probleme mit dem Ressourcenzugriff.

Berechtigungsfehler treten auf, wenn der Backup-Rolle die `AWSBackupServiceRolePolicyForScans` erforderlichen Berechtigungen fehlen oder die Scanner-Rolle nicht über die richtigen Vertrauensbeziehungen `AWSBackupGuardDutyRolePolicyForScans` verfügt.

Fehler beim Service Limit treten auf, wenn Sie die 150 gleichzeitigen Scans pro Konto oder 5 gleichzeitige Scans pro Ressourcentyp überschreiten. Scanaufträge bleiben so lange im `CREATED` Status, bis Kapazität verfügbar ist.

Fehler „Zugriff verweigert“ können auf verschlüsselte Wiederherstellungspunkte ohne entsprechende AWS KMS Berechtigungen oder auf gelöschte übergeordnete Wiederherstellungspunkte für inkrementelle Scans hinweisen.

Timeout-Fehler können bei sehr großen Wiederherstellungspunkten oder während hoher GuardDuty Amazon-Ladezeiten auftreten.

Überprüfen Sie zur Fehlerbehebung den Status des Scanauftrags mithilfe der `DescribeScanJob` API, überprüfen Sie die IAM-Rollenkonfigurationen, stellen Sie sicher, dass Wiederherstellungspunkte existieren und zugänglich sind, und erwägen Sie, zu vollständigen Scans zu wechseln, falls übergeordnete Referenzen für inkrementelle Scans fehlen.

Überwachen Sie Ihre gleichzeitige Nutzung von Scans und implementieren Sie Jittering in automatisierte Workflows, um zu vermeiden, dass Sie die Service-Limits überschreiten.

Metering (Messung)

Der Malware-Schutz wird von Amazon GuardDuty bereitgestellt und in Rechnung gestellt. Im Zusammenhang mit der Nutzung dieser Funktion werden Ihnen keine AWS Backup Gebühren berechnet. Die gesamte Nutzung kann unter der Abrechnung GuardDuty von Amazon eingesehen werden. Weitere Informationen finden Sie unter [GuardDuty Amazon-Preise](#).

Kontingente

AWS Backup Sowohl bei Amazon als auch GuardDuty bei Amazon gelten Kontingentbeschränkungen für Amazon GuardDuty Malware Protection for AWS Backup.

Weitere Informationen finden Sie unter [AWS Backup Kontingente](#) und [GuardDuty Amazon-Kontingente](#).

Schritte zur Verwendung von Konsole und CLI für Malware-Scantypen

In den folgenden Abschnitten werden die Schritte zur Konfiguration verschiedener Malware-Scantypen sowohl mit der Konsole als auch beschrieben AWS CLI.

Wie richte ich Malware-Scans ein

Konsole

1. Navigiere zu AWS Backup Konsole → Backup-Pläne
2. Erstellen Sie einen neuen Backup-Plan oder wählen Sie einen vorhandenen Plan
3. Schalten Sie den Malwareschutz ein
4. Wählen Sie Scanner-Rolle aus, um eine neue Scanner-Rolle auszuwählen. Stellen Sie sicher, dass sowohl die Backup-Rolle als auch die Scanner-Rolle über die entsprechenden Berechtigungen verfügen, wie unter beschrieben [the section called “Zugriff”](#).

5. Wählen Sie scannbare Ressourcentypen aus. Dadurch wird der Malware-Scan nach den von Ihnen ausgewählten Kriterien für die Ressourcenauswahl gefiltert. Wenn Sie beispielsweise Amazon EBS als scannbaren Ressourcentyp ausgewählt haben, die Ressourcenauswahl Ihres Plans jedoch Amazon EBS und Amazon S3 umfasst, werden nur Amazon EBS-Malware-Scans durchgeführt.
6. Legen Sie den Scantyp für jede Backup-Regel fest. Sie können zwischen vollständigem Scan, inkrementellem Scan und keinem Scan wählen. Die Auswahl des Scan-Typs bedeutet, dass der Scan mit der geplanten Häufigkeit durchgeführt wird, die in der zugehörigen Backup-Regel festgelegt ist.
7. Backup-Plan speichern

AWS CLI

CreateBackupPlan

Mit dem [create-backup-plan](#) Befehl können Sie einen Backup-Plan mit aktiviertem Malware-Scan erstellen.

```
aws backup create-backup-plan \  
  --region us-west-2 \  
  --cli-input-json '{  
    "BackupPlan": {  
      "BackupPlanName": "scan-initial-test-demo",  
      "Rules": [  
        {  
          "RuleName": "full",  
          "TargetBackupVaultName": "Default",  
          "ScheduleExpression": "cron(0 * * * ? *)",  
          "StartWindowMinutes": 120,  
          "CompletionWindowMinutes": 6000,  
          "Lifecycle": {  
            "DeleteAfterDays": 3,  
            "OptInToArchiveForSupportedResources": true  
          },  
          "RecoveryPointTags": {  
            "key1": "foo",  
            "key2": "foo"  
          },  
          "EnableContinuousBackup": true,  
        }  
      ]  
    }  
  }'
```

```

        "ScanActions": [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "FULL_SCAN"
            }
        ],
    },
    {
        "RuleName": "incremental",
        "TargetBackupVaultName": "Default",
        "ScheduleExpression": "cron(30 * * * ? *)",
        "StartWindowMinutes": 100,
        "CompletionWindowMinutes": 5000,
        "Lifecycle": {
            "DeleteAfterDays": 2,
            "OptInToArchiveForSupportedResources": true
        },
        "RecoveryPointTags": {
            "key1": "foo",
            "key2": "foo"
        },
        "EnableContinuousBackup": true,
        "ScanActions": [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "INCREMENTAL_SCAN"
            }
        ]
    }
],
"ScanSettings": [
    {
        "MalwareScanner": "GUARDDUTY",
        "ResourceTypes": ["EBS", "EC2", "S3"],
        "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
    }
]
}'

```

UpdateBackupPlan

Mit dem [update-backup-plan](#) Befehl können Sie einen Backup-Plan mit aktiviertem Malware-Scan aktualisieren.

```
aws backup update-backup-plan \  
  --region us-west-2 \  
  --cli-input-json '{  
    "BackupPlanId": "d1391282-68cf-4fce-93ad-e08bc5178bac",  
    "BackupPlan": {  
      "BackupPlanName": "scan-initial-test-demo",  
      "Rules":  
        [  
          {"RuleName": "full",  
            "TargetBackupVaultName": "Default",  
            "ScheduleExpression": "cron(0 * * * ? *)",  
            "StartWindowMinutes": 60,  
            "CompletionWindowMinutes": 3000,  
            "Lifecycle":  
              {  
                "DeleteAfterDays": 6,  
                "OptInToArchiveForSupportedResources": false},  
            "RecoveryPointTags":  
              {"key1": "foo",  
               "key2": "foo"},  
            "EnableContinuousBackup": false,  
            "ScanActions":  
              [  
                {"MalwareScanner": "GUARDDUTY",  
                 "ScanMode": "FULL_SCAN"}  
              ]  
          },  
          {  
            "RuleName": "incremental",  
            "TargetBackupVaultName": "Default",  
            "ScheduleExpression": "cron(30 * * * ? *)",  
            "StartWindowMinutes": 120,  
            "CompletionWindowMinutes": 6000,  
            "Lifecycle":  
              {  
                "DeleteAfterDays": 9,  
                "OptInToArchiveForSupportedResources": false},  
            "RecoveryPointTags":  
              {"key1": "foo",  
               "key2": "foo"},  
          }  
        ]  
    }  
  }'  
}
```

```

        "EnableContinuousBackup": false,
        "ScanActions":
        [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "INCREMENTAL_SCAN"
            }
        ]
    },
    "ScanSettings":
    [
        {
            "MalwareScanner": "GUARDDUTY",
            "ResourceTypes":
            ["ALL", "EBS"],
            "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
        }
    ]
}

```

Die wichtigsten Hinweise

- Der ARN-Zieleintrag ist erforderlich, bevor die Scanoptionen aktiviert werden (Konsole)
- Sowohl die Backup-IAM-Rolle als auch die Scanner-IAM-Rolle sind für alle Konfigurationen erforderlich
- Dient `aws backup list-scan-jobs` zum Anzeigen aller Scanaufträge (AWS CLI)
- Die Auswirkungen auf die Kosten variieren je nach Scantyp (inkrementell oder vollständig) und Häufigkeit

AWS CLI Die wichtigsten Hinweise

- `aws backup list-scan-jobs` Dient zum Anzeigen aller Scanaufträge (AWS CLI)
- Die Scanergebnisse sind über die `describe-recovery-point` API mit `ScanResults` Feld verfügbar

- Sowohl die Backup-IAM-Rolle als auch die Scanner-IAM-Rolle sind für alle Konfigurationen erforderlich
- Die Struktur des JSON-Backupplans umfasst ScanSettings sowohl die Planebene als auch die Regeln ScanActions

Belastbarkeit 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.

Kontingente

- [Backup](#)
- [Backup-Index und Suchkontingente](#)
- [Richtlinienkontingente](#)
- [Kontingente für Malware-Scans](#)
- [Amazon Timestream Timestream-Ressourcenkontingente](#)
- [AWS Backup Quoten für Audit Manager](#)
- [Kontingente des Testplans wiederherstellen](#)
- [AWS Backup gateway Kontingente](#)
- [Amazon EKS-Kontingente](#)
- [Logisch zugeordnete Tresorkontingente](#)
- [Verwandte Quotas](#)

Backup

Name	Standard	Anpassbar
Gesamtzahl der Tresore (Backup-Tresore und Tresore mit logischem Air-Gap) pro Region und Konto	300	Ja
Wiederherstellungspunkte pro Backup-Tresor	1 000 000	Ja
Backup-Pläne pro Region und Konto	300	Ja
Versionen pro Backup-Plan	2.000	Ja

Name	Standard	Anpassbar
Ressourcenzuweisungen pro Backup-Plan	100	Nein
Amazon S3 S3-Buckets pro Konto	100	Ja
Gleichzeitige regionsübergreifende Kopieraufträge pro Konto in der Zielregion	100 ²	Nein
Zusätzliche regionsübergreifende Kopieraufträge pro Tresor in einer Zielregion, nachdem das Limit in der Zeile über dem Eintrag erreicht wurde. ¹	5 ²	Nein
Gleichzeitige kontenübergreifende Kopien, die von derselben Ressource in dieselbe Zielregion erstellt werden können	30	Nein
Gleichzeitige Sicherungs- und Kopieraufträge pro Ressource	1	Nein
Stichwörter pro Ressourceauswahl in einer kontenübergreifenden Backup-Richtlinie	30	Nein. Fügen Sie zusätzliche Tags hinzu, indem Sie mehrere Ressourcenzuweisungen oder Backup-Pläne verwenden.
Hypervisoren	20	Nein
Rechtliche Aufbewahrungsfristen pro Konto	50	Nein

Name	Standard	Anpassbar
Verschachtelte Backup-Ebenen von Anwendungsstapeln	10	Nein

¹ Das Limit für gleichzeitige Kopieraufträge von einer Region in eine andere Region liegt bei 100 pro Konto und Region. Sobald dieses Limit erreicht ist und ein bestimmter Tresor in der Zielregion weniger als 5 gleichzeitige Kopieraufträge hat, können neue Kopieraufträge gestartet werden, bis zu einem Maximum von 5 gleichzeitig.

² Das Limit gilt nur für Ressourcentypen, die [vollständig von verwaltet werden](#). AWS Backup

Backup-Index und Suchkontingente

Name	Standard	Anpassbar
Gleichzeitige Indexierungsaufträge im Konto (die meisten) AWS-Regionen	40	Ja
Gleichzeitige Indexierung von Jobs im Rechnungswesen in Asien-Pazifik (Malaysia), Kanada (Zentral), Asien-Pazifik (Thailand) und Mexiko (Zentral). AWS-Regionen	10	Ja
Gleichzeitige Indexaufträge für jede Ressource	5	Nein
Gleichzeitiger Indizierungsauftrag auf Anfrage	1	Nein
Gleichzeitige Suchaufträge im Konto	10	
Gleichzeitige Exportaufträge	5	

Name	Standard	Anpassbar
Anzahl der im Suchauftrag enthaltenen Wiederherstellungspunkte	20	
Gleichzeitige Amazon EBS-Wiederherstellungsaufträge auf Dateiebene (die meisten) AWS-Regionen	25	
Gleichzeitige Amazon EBS-Wiederherstellungsaufträge auf Dateiebene in Asien-Pazifik (Malaysia), Kanada (Zentral), Asien-Pazifik (Thailand) und Mexiko (Zentral). AWS-Regionen	5	

Richtlinienkontingente

Name	Standard	Anpassbar
Ressourcenzuweisungen pro Backup-Plan	100	Nein
Tags in einer Ressourcenauswahl	30	Nein
Ressourcenauswahlen, die Tags in einem Plan verwenden	10	Nein
Regeln für Backup-Pläne in einem Plan	10	Nein

Name	Standard	Anpassbar
Zu einem Wiederherstellungspunkt hinzugefügte Tags	10	Nein
Aktionen pro Backup-Regel kopieren	5	Nein
Bedingungen in einer Ressourcenzuweisung in einem Backup-Plan	30	Nein

Kontingente für Malware-Scans

In der folgenden Tabelle sind die Kontingente für AWS Backup Malware-Scans mit Amazon aufgeführt GuardDuty.

Name	Standard	Anpassbar
Ausführung von Scanaufträgen pro Ressource pro Konto	5	Ja
Ausführung von Scanaufträgen pro Wiederherstellungspunkt pro Konto	1	Nein
Ausführung von Scanaufträgen pro Konto	150	Ja
Scanaufträge wurden pro Ressource und Konto erstellt	10	Nein
Basiseinschränkung für inkrementelle Scans	1	Nein

Wenn Sie das Limit für Ihre erstellten Scanaufträge pro Ressource und Konto erreichen, schlagen wir den ältesten Auftrag in der Warteschlange fehl.

Möglicherweise stoßen Sie auch auf von Amazon auferlegte Kontingente GuardDuty. Weitere Informationen finden Sie unter [GuardDuty Amazon-Kontingente](#) in der Allgemeine AWS-Referenz.

Amazon Timestream Timestream-Ressourcenkontingente

Name	Standard	Anpassbar
Gleichzeitige Timestream-Backup-Jobs pro Konto	4	Ja
Gleichzeitige Timestream-Wiederherstellungsaufträge pro Konto	1	Ja

AWS Backup Quoten für Audit Manager

Name	Standard	Anpassbar
Frameworks pro Konto pro Region	15	Ja
Kontrollen pro Konto pro Region	50	Ja
Pläne pro Konto melden	20	Ja
Frameworks pro Berichtsplan	1.000	Nein
[Anzahl der Konten] multipliziert mit [Anzahl der Regionen in einem Berichtsplan]	300	Nein
[Anzahl der Konten] multipliziert mit [Anzahl der Regionen in einem Berichtsplan] multipliziert mit [Anzahl der täglichen Tätigkeiten]	100 000	Nein

Name	Standard	Anpassbar
plus Bewertungen in einem Berichtsplan]		

Kontingente des Testplans wiederherstellen

Name	Standard	Anpassbar
Testpläne wiederherstellen	100	Nein
Tags pro Plan	50	Nein
Auswahl pro Plan	30	Nein
ARNs pro Auswahl für den Wiederherstellungstest	30	Nein
Bedingungen pro Auswahl (StringEquals sowohl als auch StringNotEquals)	30	Nein
Tresorauswahlen pro Wiederherstellungstest-Auswahl	30	Nein
Maximalwert (in Tagen) des Auswahlfensters	365 Tage	Nein
Grenzen für Startfensterstunden	Minimum: 1 Stunde; Maximum: 168 Stunden	Nein
Maximale Zeichenlänge des Namens des Wiederherstellungstestplans	50 Zeichen (alphanumerisch und Unterstriche, keine Leerzeichen)	Nein

Name	Standard	Anpassbar
Maximale Zeichenlänge des Namens der Wiederherstellungstest-Auswahl	50 Zeichen (alphanumerisch und Unterstriche, keine Leerzeichen)	Nein

Für jeden Ressourcentyp gilt eine Obergrenze für die Anzahl gleichzeitiger Wiederherstellungsaufträge, die im Rahmen eines Wiederherstellungstestplans erstellt wurden. Sobald dieses Limit erreicht ist, werden keine neuen Wiederherstellungsaufträge für diesen Ressourcentyp erstellt, bis ein Job, der sich im Status des RUNNING Übergangs zu COMPLETED befindet.

Wenn ein geplanter Wiederherstellungsauftrag aufgrund dieses Kontingents nicht gestartet wurde, führt dieser Auftrag zu einem FAILED Status mit der Statusmeldung "Restore job was unable to start within the specified start window. Try increasing your start window.". Wenn Sie einen fehlgeschlagenen Job mit dieser Statusmeldung erhalten, empfiehlt es sich, zunächst das Startfenster so zu verlängern, dass genügend Zeit vorhanden ist, damit die Jobs abgeschlossen werden können. Versuchen Sie es dann erneut mit den Aufträgen.

Beachten Sie, dass Kontingente nicht für Wiederherstellungsaufträge auf Abruf gelten, sondern für die Wiederherstellung von Aufträgen, die im Rahmen eines [Wiederherstellungstestplans](#) erstellt wurden. Für einige Ressourcentypen können Sie eine Erhöhung des Kontingentlimits beantragen.

Name	Standard	Anpassbar
Amazon Aurora	40	Ja
Amazon DocumentDB	40	Ja
Amazon DynamoDB	40	Nein
Amazon EBS	100	Ja
Amazon EC2	100	Ja
Amazon EFS	30	Ja
Amazon FSx	40	Ja

Name	Standard	Anpassbar
Amazon Neptune	40	Ja
Amazon RDS	40	Ja
Amazon S3	30	Ja

AWS Backup gateway Kontingente

Name	Standard	Anpassbar
Backup- oder Wiederherstellungsaufträge pro Gateway	4	Nein. Erstellen Sie mehr Gateways und verbinden Sie sie mit Ihrem Hypervisor.

Amazon EKS-Kontingente

Name	Standard	Anpassbar
Namespaces pro EKS-Cluster-Backup	1000	Ja
Persistente Speichersicherungen pro EKS-Cluster-Backup	1000	Ja
Stellen Sie Jobs pro EKS-Zielcluster wieder her	1	Nein
EKS Wiederherstellungsaufträge pro Konto	5	Ja

Logisch zugeordnete Tresorkontingente

Ressourcentyp	Maximale Anzahl gleichzeitiger Kopien
EC2	Das EBS-Limit für gleichzeitige Kopien gilt für alle Snapshots wird als Teil einer AMI-Kopie kopiert.
EBS	20
Aurora	20
DocumentDB	20
Neptune	20
Storage Gateway	5
FSx	5

Verwandte Quotas

Es gibt [Kontingente für eine einzelne Ressourcenzuweisung](#) in einer einzigen Backup-Regel. Sie können einen Backup-Plan mit mehreren Backup-Regeln erstellen.

Wenn Sie Backups über mehrere Konten hinweg 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 von einem Dienst festgelegt werden, AWS Backup der von einem Dienst unterstützt wird, einschließlich der folgenden:

- [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-Dateiserver](#)
- [Amazon DocumentDB](#)
- [Amazon Neptune](#)
- [Amazon Simple Storage Service](#)
- [Amazon Timestream](#)

Überwachung AWS Backup

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 Armaturenbrett](#) zugreifen.
- Amazon CloudWatch und Amazon EventBridge zur Überwachung von AWS Backup Prozessen.
 - Sie können CloudWatch damit Metriken verfolgen, Alarmer 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 mithilfe von Amazon überwachen EventBridge](#) und.

- AWS CloudTrail um 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 Armaturenbrett](#) zugreifen.

Themen

- [Übersicht über Backup-Dashboards](#)
- [Anzeigen des Auftrags-Dashboards](#)
- [Gründe für problematische Aufträge](#)
- [Abrufen von Dashboard-Daten über AWS CLI](#)

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 die Überwachung auf Organisationsebene oder von 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 Job-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, 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 den Standardschlüssel 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 ein Schlüssel 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 mithilfe von 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. Bitte beachten Sie, dass dies nur für Backup-Jobs gilt.

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](#)
- [Ereignisse im Backup-Plan](#)
- [Backup Vault-Ereignisse](#)

- [Job-Ereignisse kopieren](#)
- [Recovery Point-Ereignisse](#)
- [Ereignisse in den Regionseinstellungen](#)
- [Job-Ereignisse wiederherstellen](#)
- [Ereignisse bei der Indexierung von Wiederherstellungspunkten](#)
- [Auftragsereignisse für Malware-Scans](#)

Backup-Job-Ereignisse

Im Folgenden sind Beispielergebnisse aufgeführt.

Status

- [Status: FEHLGESCHLAGEN](#)
- [Status: ABGESCHLOSSEN](#)
- [Status: LÄUFT](#)
- [Zustand: ABGEBROCHEN](#)
- [Status: ABGELAUFEN](#)
- [Status: AUSSTEHEND](#)
- [Bundesstaat: ERSTELLT](#)

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:f59bffc-d-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffc-d-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": "NjBjOTUzZjYtYzZiNi00Njh1LWlzMTEtNWRjOWY0YTNjN2Vj",
      "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 Beispielergebnisse 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": "N2Q40TczMzEtZmY1My00N2UwLWE30DUtMjViYWYy0TUzZWY4",
  "creationDate": "2020-06-24T23:18:15.318Z",
  "state": "CREATED"
}
}
```

Backup Vault-Ereignisse

Im Folgenden sind Beispielergebnisse 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 Beispielergebnisse 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-ab60-4fbbabcbdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
    "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-ab60-4fbbabcbdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
    "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": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMtY2IwMTY4NWQ4",
      "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 die Ereignisse aufgeführt.

Status

- [COMPLETED](#)
- PARTIAL
- WIRD GELÖSCHT
- ABGELAUFEN
- VERFÜGBAR
- STOPPED
- WIRD ERSTELLT

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": "YTkzNmM0MmUtMWRhNS00Y2RkLTNmZGUtNjA5NTc4NGM1YTc5",
        "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
      },
      "lifecycle": {
        "deleteAfterDays": 100
      },
      "calculatedLifeCycle": {
        "deleteAt": "2020-10-23T21:38:31.152Z"
      }
    }
  }
}

```

Ereignisse in den Regionseinstellungen

Es folgt ein Beispiereignis.

```

{
  "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 Beispielergebnisse aufgeführt. Beachten Sie, dass Ihr Anwendungsfall eines Wiederherstellungsauftrags bestimmt, welche erforderlichen und optionalen Parameter enthalten sein müssen. Wenn Ihr Wiederherstellungsauftrag beispielsweise Teil eines Wiederherstellungstestplans ist, `restoreTestingPlanArn` ist der Parameter enthalten. Mögliche Parameter `DescribeRestoreJob` finden Sie unter.

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",
    "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",
    "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",
  "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",

```

```

    "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",
    "state": "CREATED"
  }
}

```

Ereignisse bei der Indexierung von Wiederherstellungspunkten

Im Folgenden sind Beispielergebnisse aufgeführt.

Status

- [Status: AKTIV](#)
- [Status: GELÖSCHT](#)
- [Status: FEHLGESCHLAGEN](#)

Status: AKTIV

```

{

```

```

"version":"0",
"id":"ab32977c-378d-2122-e985-fgh4596f0709",
"detail-type":"Recovery Point Index State Change",
"source":"aws.backup",
"account":"1112233445566",
"time":"2023-12-15T21:39:07Z",
"region":"us-west-2",
"resources":[
  "arn":"aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
  abcdef123456"
],
"detail":{
  "recoveryPointArn":"arn:aws:backup:us-west-2:1112233445566:recovery-
  point:abcd1234-5678-abcd-9012-abcdef123456",
  "accountId":"1112233445566",
  "indexStatus":"ACTIVE",
  "iamRoleArn":"arn:aws:iam::1112233445566:role/BackupIndexRole",
  "resourceType":"EBS",
  "backupVaultArn":"arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
  "indexCreationTime":"2025-05-25T21:38:31.152Z",
  "isIndexingContinuous":false,
  "sourceResourceArn":"arn:aws:ec2:us-west-2:1112233445566:volume/
  vol-01234567890abcdef",
  "backupCreationTime":"2023-12-15T21:38:00.000Z",
  "indexStatusMessage":"An AWS Backup recovery point index was
  successfully completed. Indexed recovery point arn : arn:aws:backup:us-
  west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
  "indexCompletionTime":"2025-05-25T21:39:05.689Z",
}
}

```

Status: GELÖSCHT

```

{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Recovery Point Index State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2023-12-15T21:39:07Z",
  "region":"us-west-2",
  "resources":[]
}

```

```

    "arn":"aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
    abcdef123456"
  ],
  "detail":{
    "recoveryPointArn":"arn:aws:backup:us-west-2:1112233445566:recovery-
    point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId":"1112233445566",
    "indexStatus":"DELETED",
    "iamRoleArn":"arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType":"EBS",
    "backupVaultArn":"arn:aws:crypto:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime":"2025-05-25T21:38:31.152Z",
    "isIndexingContinuous":false,
    "sourceResourceArn":"arn:aws:ec2:us-west-2:1112233445566:volume/
    vol-01234567890abcdef",
    "backupCreationTime":"2023-12-15T21:38:00.000Z",
    "indexStatusMessage":"An AWS Backup recovery point index was deleted.
    Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
    point:abcd1234-5678-abcd-9012-abcdef123456",
    "indexDeletionTime":"2025-05-27T22:39:05.689Z",
  }
}

```

Status: FEHLGESCHLAGEN

```

{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Recovery Point Index State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2023-12-15T21:39:07Z",
  "region":"us-west-2",
  "resources":[
    "arn":"aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
    abcdef123456"
  ],
  "detail":{
    "recoveryPointArn":"arn:aws:backup:us-west-2:1112233445566:recovery-
    point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId":"1112233445566",
    "indexStatus":"FAILED",
    "iamRoleArn":"arn:aws:iam::1112233445566:role/BackupIndexRole",
  }
}

```

```

    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index failed to create.
Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
  }
}

```

Auftragereignisse für Malware-Scans

Im Folgenden sind Beispielereignisse aufgeführt.

Status

- [Status: ERSTELLT](#)
- [Zustand: LÄUFT](#)
- [Status: ABGESCHLOSSEN](#)
- [Status: ABGESCHLOSSEN MIT PROBLEMEN](#)
- [Status: FEHLGESCHLAGEN](#)
- [Status: ABGESAGT](#)

Status: ERSTELLT

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
    abcdef123456"
  ],
  "detail": {

```

```

    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "CREATED"
}
}

```

Zustand: LÄUFT

```

{
    "version": "0",
    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2025-12-12T12:12:12Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
    ]
}

```

```

    ],
    "detail": {
      "accountId": "1112233445566",
      "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
      "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
      "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
      },
      "creationDate": "2025-12-12T12:12:00Z",
      "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
      "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
      "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
      "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
      "resourceType": "EC2",
      "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
      "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
      "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
      "malwareScanner": "GUARDDUTY",
      "state": "RUNNING"
    }
  }
}

```

Status: ABGESCHLOSSEN

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [

```

```

    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
    abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
    vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
      plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
    RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
    RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
    point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
    i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
    point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "scanResult": {
      "scanResultStatus": "THREATS_FOUND"
    },
    "state": "COMPLETED",
    "statusMessage": "An AWS Backup scan job was successful completed."
  }
}

```

Status: ABGESCHLOSSEN MIT PROBLEMEN

```

{
  "version": "0",

```



```

    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2025-12-12T12:12:12Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
      abcdef123456"
    ],
    "detail": {
      "accountId": "1112233445566",
      "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
      vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
      "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
      "completionDate": "2025-12-12T12:12:12Z",
      "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
        plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
      },
      "creationDate": "2025-12-12T12:12:00Z",
      "iamRoleArn": "arn:aws:iam::1112233445566:role/
      RoleForEc2BackupWithNoDescribeTagsPermissions",
      "scannerRoleArn": "arn:aws:iam::1112233445566:role/
      RoleForAwsBackupGuarddutyScanner",
      "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
      point:abcd1234-5678-abcd-9012-abcdef123456",
      "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
      i-0515aee7de03f58e1",
      "resourceType": "EC2",
      "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
      "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
      "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
      point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
      "malwareScanner": "GUARDDUTY",
      "scanResult": {
        "scanResultStatus": "NO_THREATS_FOUND"
      },
      "state": "COMPLETED_WITH_ISSUES",
      "statusMessage": "Scan job partially completed. View more details in Amazon
      GuardDuty"
    }
  ]
}

```

```
}
}
```

Status: FEHLGESCHLAGEN

```
{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
```

```

    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "FAILED",
    "statusMessage": "<failure reason>"
  }
}

```

Status: ABGESAGT

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
  }
}

```

```
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "CANCELED",
    "statusMessage": "Scan job was stopped by user."
  }
}
```

AWS Backup Metriken mit Amazon CloudWatch

Themen

- [CloudWatch Armaturenbrett](#)
- [Metriken mit CloudWatch](#)

CloudWatch Armaturenbrett

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 widerspiegelt. „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
Jobs	Anzahl der Backup-, Wiederherstellungs- und Kopieraufträge über jeden Status hinweg, einschließlich CREATED, PENDING, RUNNING, ABORTED, COMPLETED ,	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

Kategorie	Metriken	Beispiel-Dimensionen	Beispielanwendungsfall
	FAILED und EXPIRED. Verschiedene Auftragstypen haben unterschiedliche verfügbare Status.		Aufträge vorliegen , senden Sie eine E-Mail oder SMS über Amazon SNS oder eröffnen Sie ein Ticket damit das Entwicklungsteam dies untersuchen kann. Berichtskriterien: 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. Berichtskriterien: Ein Wert ungleich Null

Note

Der Auftragsstatus von Completed with issues ist nur für die AWS Backup Konsole spezifisch. Er kann nicht über die Konsole nachverfolgt werden CloudWatch.

Die folgende Tabelle listet alle Metriken auf, die verfügbar sind.

Metrik	Description
NumberOfBackupJobsCreated	Die Anzahl der AWS Backup erstellten Backup-Jobs.
NumberOfBackupJobsPending	Die Anzahl der Backup-Aufträge, die gleich in AWS Backup ausgeführt werden.
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 FSx Amazon-Wartungsfensters oder eines automatisierten Backup-Fensters geplant wird 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

Metrik	Description
	Ein Backup-Job wechselt vom Status CREATED in „EXPIRED“. Wenn ein Backup nicht innerhalb des Startfensters beginnen kann“.
NumberOfCopyJobsCreated	Die Anzahl der konto- und regionsübergreifenden Kopieraufträge, die AWS Backup erstellt hat.
NumberOfCopyJobsRunning	Die Anzahl der konto- und regionsübergreifenden Kopieraufträge, die derzeit in AWS Backup ausgeführt werden.
NumberOfCopyJobsCompleted	Die Anzahl der konto- und regionsübergreifenden Kopieraufträge, die AWS Backup abgeschlossen hat.
NumberOfCopyJobsFailed	Die Anzahl der konto- und regionsübergreifenden 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.

Metrik	Description
<code>NumberOfRecoveryPointsPartial</code>	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.
<code>NumberOfRecoveryPointsExpired</code>	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.
<code>NumberOfRecoveryPointsDeleting</code>	Die Anzahl der Wiederherstellungspunkte, AWS Backup die gelöscht werden.
<code>NumberOfRecoveryPointsCold</code>	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 CloudTrail](#) einen Dienst integriert, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienstdienst ausgeführt wurden. 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 Anforderung mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt 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-Managementkonsole sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter [Erstellen eines Trails für Ihr AWS-Konto](#) und [Erstellen eines Trails für eine Organisation](#) 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, Scans oder Benachrichtigungen durchführt. Diese Ereignisse werden nicht unbedingt durch die Nutzung der AWS Backup Öffentlichkeit ausgelöst APIs. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter [AWS Serviceereignisse](#).

- AssociateBackupVaultMpaApprovalTeamCompleted
- AssociateBackupVaultMpaApprovalTeamFailed
- BackupDeleted
- BackupJobCompleted
- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- CreateRestoreAccessBackupVaultFailed

- DisassociateBackupVaultMpaApprovalTeamFailed
- PutBackupVaultNotifications
- RecoveryPointCreated
- ReportJobCompleted
- ReportJobStarted
- RestoreAccessBackupVaultDeleted
- RestoreCompleted
- RestoreStarted
- RevokeRestoreAccessBackupVaultFailed
- ScanJobCompleted
- ScanJobCreated
- ScanJobFailed
- ScanJobStarted

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-00a129455bdb9d99",
        "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": "783ddddd-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 Organizations](#) Struktur verwalten. AWS Backup generiert diese CloudTrail Ereignisse in Ihrem Mitgliedskonto, wenn Sie eine AWS Organizations Backup-Richtlinie erstellen, aktualisieren oder löschen (die Backup-Pläne auf Ihre Mitgliedskonten anwendet) oder wenn es einen ungültigen Backup-Plan für Ihre Organisation gibt:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationBackupPlan`

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:ControllerCAMTestBackupVault\", \"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": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ0ThmNzRj",
    "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 gesendetInvalidOrganizationBackupPlan, 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:

- Benutzerbenachrichtigungen kann Benachrichtigungen, einschließlich CloudWatch Amazon-Alarme AWS Support, und Benachrichtigungen anderer Dienste senden.
- Amazon Simple Notification Service kann Sie über AWS Backup Ereignisse informieren.

Benutzerbenachrichtigungen und AWS Backup

AWS Backup unterstützt die Verwaltung Ihrer Backup-Benachrichtigungen von der [Benutzerbenachrichtigungen Konsole](#) aus. Mit [Benutzerbenachrichtigungen](#) können Sie den Status Ihrer Sicherungs-, Kopier- und Wiederherstellungsaufträge sowie Änderungen an Ihren Backup-Richtlinien, Tresoren, Wiederherstellungspunkten und Einstellungen im Notification Center 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, Amazon Q

Developer in Chat-Anwendungen, 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 das Beispiel einer Amazon SNS SNS-Benachrichtigung JSONs für abgeschlossene, fehlgeschlagene und abgelaufene Backup-Jobs 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 notification 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	Veranstaltung
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
Indizierung von Wiederherstellungspunkten	RECOVERY_POINT_INDEX_COMPLETED RECOVERY_POINT_INDEX_DELETED RECOVERY_POINT_INDEXING_FAILED

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.

AWS Backup für EKS unterstützt zwei zusätzliche Ereignisse:

- `EKS_RESTORE_OBJECT_FAILED` benachrichtigt Sie über alle EKS-Objekte, die während eines Wiederherstellungsauftrags nicht wiederhergestellt werden konnten.

- `EKS_RESTORE_OBJECT_SKIPPED` benachrichtigt Sie über alle EKS-Objekte, die während eines AWS Backup Wiederherstellungsauftrags übersprungen wurden.

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"}
    }
}

```

Example Beispiel: Die Indizierung des Wiederherstellungspunkts wurde 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 backup index job was completed. Indexed recovery
point arn: arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-
abcd-9012-abcdef123456",
      "Timestamp": "2025-05-25T18:46:02.788Z",
      ...
      "MessageAttributes" : {
        "EventType" :
{"Type":"String","Value":"RECOVERY_POINT_INDEXING_COMPLETED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "IndexStatus" : {"Type":"String","Value":"ACTIVE"},
        "IsIndexingContinuous" : {"Type":"String","Value":"false"},
        "RecoveryPointArn" : {"Type":"String","Value":"arn:aws:backup:us-
west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"}
      }
    }
  ]
}

```

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 nach Antworten suchen und Fragen stellen in [AWS re:Post](#).

Themen

- [Fehlerbehebung bei allgemeinen Problemen](#)
- [Fehlerbehebung beim Erstellen von Ressourcen](#)
- [Fehlerbehebung beim Löschen von Ressourcen](#)
- [Fehlerbehebung beim Wiederherstellen von Ressourcen](#)
- [Behebung von Formatierungsfehlern](#)

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 mithilfe von AWS Identity and Access Management (IAM) mit finden Sie AWS Backup unter [Zugriffskontrolle](#).

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 unter [AWS 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 Backups nicht 4 Stunden vor oder während des Wartungsfensters oder des automatischen Backup-Fensters starten (Amazon Aurora ist von dieser Einschränkung des Wartungsfensters ausgenommen). Zu diesen Zeiten geplante Snapshot-Backups schlagen fehl. Eine Ausnahme: Wenn Sie sich für einen unterstützten Service sowohl AWS Backup für Snapshot- als auch für kontinuierliche Backups entscheiden, müssen Sie sich über diese Zeitfenster keine Gedanken mehr machen, da sich 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 Ihre IAM-Rolle zu Ihrem KMS-Schlüssel 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 unter [Zugriffskontrolle](#).

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 FSx Amazon-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](#)
- [Wiederherstellung einer EC2 Amazon-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

Sie können nicht nur die Konsole verwenden, sondern auch die AWS Backup API-Aktionen und Datentypen verwenden, um die zugehörigen Ressourcen programmgesteuert zu konfigurieren und zu verwalten AWS Backup . In diesem Abschnitt werden AWS Backup -Aktionen und -Datentypen beschrieben. Sie enthält die API-Referenz für AWS Backup

AWS Backup API

- [AWS Backup Aktionen](#)
- [AWS Backup Datentypen](#)

Aktionen

Die folgenden Aktionen werden unterstützt von AWS Backup:

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)
- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)

- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)
- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)

- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)
- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)

- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)
- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)

- [UpdateTieringConfiguration](#)

Die folgenden Aktionen werden unterstützt von AWS Backup gateway:

- [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](#)

Die folgenden Aktionen werden unterstützt von AWS Backup:

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)
- [ListTagsForResource](#)
- [StartSearchJob](#)
- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

AWS Backup

Die folgenden Aktionen werden unterstützt von AWS Backup:

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)

- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)
- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)

- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)
- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)

- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)
- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)

- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)
- [UpdateTieringConfiguration](#)

AssociateBackupVaultMpaApprovalTeam

Service: AWS Backup

Ordnet ein MPA-Genehmigungsteam einem Backup-Tresor zu.

Anforderungssyntax

```
PUT /backup-vaults/backupVaultName/mpaApprovalTeam HTTP/1.1
Content-type: application/json

{
  "MpaApprovalTeamArn": "string",
  "RequesterComment": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name des Backup-Tresors, der dem MPA-Genehmigungsteam zugeordnet werden soll.

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

MpaApprovalTeamArn

Der Amazon-Ressourcenname (ARN) des MPA-Genehmigungsteams, das dem Backup-Tresor zugeordnet werden soll.

Typ: Zeichenfolge

Erforderlich: Ja

RequesterComment

Ein Kommentar des Antragstellers zur Erläuterung der Zuordnungsanfrage.

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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)

- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

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.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 Backup-Plan 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,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
```

```

        "ResourceTypes": [ "string" ]
    },
    "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
    },
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string" ],
            "ScannerRoleArn": "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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Arn

Context

CreatorRequestId

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Arn

Context

CreatorRequestId

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Arn

Context

CreatorRequestId

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 Aufbewahrung.

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 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.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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",
  "EncryptionKeyArn": "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

EncryptionKeyArn

Der ARN des vom Kunden verwalteten KMS-Schlüssels, der für die Verschlüsselung des Backup-Tresors mit logischem Air-Gap verwendet werden soll. Falls nicht angegeben, wird der Tresor mit einem AWS eigenen Schlüssel verschlüsselt, der von AWS Backup verwaltet wird.

Typ: Zeichenfolge

Erforderlich: Nein

MaxRetentionDays

Der maximale Aufbewahrungszeitraum, für den der Tresor seine Wiederherstellungspunkte beibehält.

Type: Long

Erforderlich: Ja

MinRetentionDays

Diese Einstellung gibt den Mindestaufbewahrungszeitraum an, in dem der Tresor seine Wiederherstellungspunkte beibehält.

Der akzeptierte Mindestwert beträgt 7 Tage.

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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 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 |
SCAN_JOB_REPORT

Wenn die Berichtsvorlage RESOURCE_COMPLIANCE_REPORT oder istCONTROL_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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateRestoreAccessBackupVault

Service: AWS Backup

Erstellt einen Backup-Tresor mit Wiederherstellungszugriff, der temporären Zugriff auf Wiederherstellungspunkte in einem Backup-Tresor mit logischem Air-Gap bietet, sofern die MPA-Genehmigung erforderlich ist.

Anforderungssyntax

```
PUT /restore-access-backup-vaults HTTP/1.1
Content-type: application/json
```

```
{
  "BackupVaultName": "string",
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "RequesterComment": "string",
  "SourceBackupVaultArn": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

BackupVaultName

Der Name des Backup-Tresors, der einem MPA-Genehmigungsteam zugeordnet werden soll.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

Erforderlich: Nein

BackupVaultTags

Optionale Tags, die dem Backup-Tresor mit Wiederherstellungszugriff zugewiesen werden können.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

CreatorRequestId

Eine eindeutige Zeichenfolge, die die Anfrage identifiziert und die Wiederholung fehlgeschlagener Anfragen ermöglicht, ohne dass das Risiko besteht, dass der Vorgang zweimal ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Nein

RequesterComment

Ein Kommentar, in dem der Grund für die Beantragung des Wiederherstellungszugriffs auf den Backup-Tresor erläutert wird.

Typ: Zeichenfolge

Erforderlich: Nein

SourceBackupVaultArn

Der ARN des Quell-Backup-Tresors, der die Wiederherstellungspunkte enthält, auf die temporärer Zugriff angefordert wird.

Typ: Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationDate": number,
  "RestoreAccessBackupVaultArn": "string",
  "RestoreAccessBackupVaultName": "string",
  "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.

CreationDate

>Datum und Uhrzeit der Erstellung des Backup-Tresors mit Wiederherstellungszugriff, im Unix-Format und in koordinierter Weltzeit

Typ: Zeitstempel

RestoreAccessBackupVaultArn

Der ARN, der den erstellten Backup-Tresor für den Wiederherstellungszugriff eindeutig identifiziert.

Typ: Zeichenfolge

RestoreAccessBackupVaultName

Der Name des erstellten Backup-Tresors mit Wiederherstellungszugriff.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

VaultState

Der aktuelle Status des Backup-Tresors mit Wiederherstellungszugriff.

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.

Arn

Context

CreatorRequestId

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateRestoreTestingPlan

Service: AWS Backup

Erstellt einen Testplan für die Wiederherstellung.

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.

Arn

Context

CreatorRequestId

Type

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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 geschützte Ressourcen ARNs hinzufügenProtectedResourceArns.

Es ist nicht möglich, sowohl nach geschützten Ressourcentypen ALS auch nach bestimmten Typen auszuwählen ARNs. 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 „-“ und „_“ 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 geschützte Ressourcen ARNs hinzufügen `ProtectedResourceArns`.

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.

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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateTieringConfiguration

Service: AWS Backup

Erstellt eine Tiering-Konfiguration.

Eine Tiering-Konfiguration ermöglicht die automatische Verschiebung von Backup-Daten auf eine kostengünstigere Speicherebene, die auf dem Alter der gesicherten Objekte im Backup-Tresor basiert.

Jeder Tresor kann nur eine tresorspezifische Tiering-Konfiguration haben, zusätzlich zu jeder globalen Konfiguration, die für alle Tresore gilt.

Anforderungssyntax

```
PUT /tiering-configurations HTTP/1.1
Content-type: application/json

{
  "CreatorRequestId": "string",
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ],
    "TieringConfigurationName": "string"
  },
  "TieringConfigurationTags": {
    "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 Anfrage identifiziert und die Wiederholung fehlgeschlagener Anfragen ermöglicht, ohne dass das Risiko besteht, dass der Vorgang 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

TieringConfiguration

Eine Tiering-Konfiguration muss eine von Ihnen erstellte eindeutige `TieringConfigurationName` Zeichenfolge sowie ein `BackupVaultName` UND enthalten. `ResourceSelection` Sie können optional eine `CreatorRequestId` Zeichenfolge einschließen.

Das `TieringConfigurationName` ist eine eindeutige Zeichenfolge, die dem Namen der Tiering-Konfiguration entspricht. Dieser Wert kann nach der Erstellung nicht geändert werden und darf nur aus alphanumerischen Zeichen und Unterstrichen bestehen.

Typ: [TieringConfigurationInputForCreate](#) Objekt

Erforderlich: Ja

TieringConfigurationTags

Die Tags, die der Tiering-Konfiguration zugewiesen werden sollen.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "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

Datum und Uhrzeit der Erstellung einer Tiering-Konfiguration im Unix-Format und in koordinierter 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

TieringConfigurationArn

Ein Amazon-Ressourcenname (ARN), der die erstellte Tiering-Konfiguration eindeutig identifiziert.

Typ: Zeichenfolge

TieringConfigurationName

Diese eindeutige Zeichenfolge ist der Name der Tiering-Konfiguration.

Der Name kann nach der Erstellung nicht mehr geändert werden. Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 200.

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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 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.

Context

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Tresor-Namen 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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

DeleteTieringConfiguration

Service: AWS Backup

Löscht die durch einen Tiering-Konfigurationsnamen angegebene Tiering-Konfiguration.

Anforderungssyntax

```
DELETE /tiering-configurations/tieringConfigurationName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

[tieringConfigurationName](#)

Der eindeutige Name einer Tiering-Konfiguration.

Pattern: `^[a-zA-Z0-9_]{1,200}$`

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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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",
  "BackupPlanName": "string",
  "BackupPlanVersion": "string",
  "BackupRuleCron": "string",
  "BackupRuleId": "string",
  "BackupRuleName": "string",
  "BackupRuleTimezone": "string"
},
"CreationDate": number,
"EncryptionKeyArn": "string",
"ExpectedCompletionDate": number,
"IamRoleArn": "string",
"InitiationDate": number,
"IsEncrypted": boolean,
"IsParent": boolean,
"MessageCategory": "string",
"NumberOfChildJobs": number,
"ParentJobId": "string",
"PercentDone": "string",
"RecoveryPointArn": "string",
"RecoveryPointLifecycle": {
  "DeleteAfterDays": number,
  "DeleteAfterEvent": "string",
  "MoveToColdStorageAfterDays": number,
  "OptInToArchiveForSupportedResources": boolean
},
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"StartBy": number,
"State": "string",
"StatusMessage": "string",
"VaultLockState": "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.

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 (Wiederherstellungspunkts) in Byte.

Dieser Wert kann je nach Ressourcentyp unterschiedlich dargestellt werden, AWS Backup da Dateninformationen von anderen AWS Diensten abgerufen werden. Beispielsweise kann der zurückgegebene Wert einen Wert von aufweisen 0, der vom erwarteten Wert abweichen kann.

Das erwartete Verhalten von Werten nach Ressourcentyp wird wie folgt beschrieben:

- Bei Amazon Aurora, Amazon DocumentDB und Amazon Neptune wird dieser Wert nicht aus dem Vorgang übernommen. `GetBackupJobStatus`
- Bei Amazon DynamoDB mit erweiterten Funktionen bezieht sich dieser Wert auf die Größe des Wiederherstellungspunkts (Backup).
- Amazon EC2 und Amazon EBS zeigen die als Teil dieses Werts zurückgegebene Volumengröße (bereitgestellter Speicher) an. Amazon EBS gibt keine Informationen zur Backup-Größe zurück. Die Snapshot-Größe hat denselben Wert wie die ursprüngliche Ressource, die gesichert wurde.

- Für Amazon EFS bezieht sich dieser Wert auf die Delta-Bytes, die während einer Sicherung übertragen wurden.
- Amazon FSx füllt diesen Wert nicht aus dem Vorgang GetBackupJobStatus für FSx Dateisysteme auf.
- Eine Amazon RDS-Instance wird als angezeigt0.
- Bei laufenden VMware virtuellen Maschinen wird dieser Wert AWS Backup über einen asynchronen Workflow weitergegeben, was bedeuten kann, dass dieser angezeigte Wert die tatsächliche Backup-Größe unterrepräsentiert.

Typ: 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.

Typ: 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

EncryptionKeyArn

Der Amazon-Ressourcenname (ARN) des KMS-Schlüssels, der zur Verschlüsselung des Backups verwendet wurde. Dies kann je nach Tresorkonfiguration ein vom Kunden AWS verwalteter Schlüssel oder ein verwalteter Schlüssel sein.

Typ: Zeichenfolge

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

IsEncrypted

Ein boolescher Wert, der angibt, ob das Backup verschlüsselt ist. Alle Backups in AWS Backup sind verschlüsselt, aber dieses Feld gibt aus Gründen der Transparenz den Verschlüsselungsstatus an.

Typ: Boolescher Wert

IsParent

Dies gibt den booleschen Wert zurück, dass es sich bei einem Backup-Auftrag um einen übergeordneten (zusammengesetzten) Auftrag handelt.

Typ: Boolescher Wert

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.

Typ: 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

RecoveryPointLifecycle

Gibt den Zeitraum in Tagen an, bevor ein Erholungspunkt in einen Cold Storage übergeht oder gelöscht wird.

In den Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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 auf unbestimmte Zeit beizubehalten, geben Sie `-1` für `MoveToColdStorageAfterDays` und an. `DeleteAfterDays`

Typ: [Lifecycle](#) Objekt

[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 dem angegebenen Backup 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

VaultLockState

Der Sperrstatus des Backup-Tresors. Bei Tresoren mit logischem Air-Gap gibt dies an, ob der Tresor im Compliance-Modus gesperrt ist. Gültige Werte sind LOCKED und UNLOCKED.

Typ: Zeichenfolge

VaultType

Der Typ des Backup-Tresors, in dem der Recovery Point gespeichert ist.
Gültige Werte gelten BACKUP_VAULT für standardmäßige Backup-Tresore und LOGICALLY_AIR_GAPPED_BACKUP_VAULT für Tresore mit logischem Air-Gap.

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.

Context

Type

HTTP Status Code: 500

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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",
  "EncryptionKeyType": "string",
  "LatestMpaApprovalTeamUpdate": {
```

```
    "ExpiryDate": number,
    "InitiationDate": number,
    "MpaSessionArn": "string",
    "Status": "string",
    "StatusMessage": "string"
  },
  "LockDate": number,
  "Locked": boolean,
  "MaxRetentionDays": number,
  "MinRetentionDays": number,
  "MpaApprovalTeamArn": "string",
  "MpaSessionArn": "string",
  "NumberOfRecoveryPoints": number,
  "SourceBackupVaultArn": "string",
  "VaultState": "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.

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

EncryptionKeyType

Der Typ des Verschlüsselungsschlüssels, der für den Backup-Tresor verwendet wird. Gültige Werte sind `CUSTOMER_MANAGED_KMS_KEY` für vom Kunden verwaltete Schlüssel oder `_OWNED_KMS_KEY` für Schlüssel, die dem Kunden gehören. AWS AWS

Typ: Zeichenfolge

Zulässige Werte: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

LatestMpaApprovalTeamUpdate

Informationen zum neuesten Update der Zuordnung des MPA-Genehmigungsteams für diesen Backup-Tresor.

Typ: [LatestMpaApprovalTeamUpdate](#) Objekt

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: Boolescher Wert

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 angibt, 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.

Typ: Long

[MpaApprovalTeamArn](#)

Der ARN des MPA-Genehmigungsteams, das diesem Backup-Tresor zugeordnet ist.

Typ: Zeichenfolge

[MpaSessionArn](#)

Der ARN der MPA-Sitzung, die diesem Backup-Tresor zugeordnet ist.

Typ: Zeichenfolge

[NumberOfRecoveryPoints](#)

Die Anzahl der Wiederherstellungspunkte, die in einem Backup-Tresor gespeichert sind.

Der in der Konsole angezeigte Wert für die Anzahl der Wiederherstellungspunkte kann ein Näherungswert sein. Verwenden Sie die [ListRecoveryPointsByBackupVault](#)-API, um die genaue Anzahl zu erhalten.

Typ: Long

[SourceBackupVaultArn](#)

Der ARN des Quell-Backup-Tresors, aus dem dieser Backup-Tresor mit Wiederherstellungszugriff erstellt wurde.

Typ: Zeichenfolge

[VaultState](#)

Der aktuelle Status des Tresors. ->

Typ: Zeichenfolge

Zulässige Werte: CREATING | AVAILABLE | FAILED

[VaultType](#)

Der beschriebene Tresortyp.

Typ: Zeichenfolge

Zulässige Werte: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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",
```



```

    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreatedByBackupJobId": "string",
  "CreationDate": number,
  "DestinationBackupVaultArn": "string",
  "DestinationEncryptionKeyArn": "string",
  "DestinationRecoveryPointArn": "string",
  "DestinationRecoveryPointLifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "DestinationVaultLockState": "string",
  "DestinationVaultType": "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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeFramework

Service: AWS Backup

Gibt Framework-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 2020-07-10T15:00:00.000-08:00 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 Kennzeichnungen `isCrossAccountBackupEnabled` `isMpaEnabled` („MPa“ bezieht sich auf die Genehmigung durch mehrere Parteien) und `isDelegatedAdministratorEnabled`

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.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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",
    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreationDate": number,
  "EncryptionKeyArn": "string",
  "EncryptionKeyType": "string",
  "IamRoleArn": "string",
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "InitiationDate": number,
  "IsEncrypted": boolean,
  "IsParent": boolean,
  "LastRestoreTime": number,
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "ParentRecoveryPointArn": "string",
  "RecoveryPointArn": "string",
  "ResourceArn": "string",
```

```

"ResourceName": "string",
"ResourceType": "string",
"ScanResults": [
  {
    "Findings": [ "string" ],
    "LastScanTimestamp": number,
    "MalwareScanner": "string",
    "ScanJobState": "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

EncryptionKeyType

Der Typ des Verschlüsselungsschlüssels, der für den Erholungspunkt verwendet wird. Gültige Werte sind `CUSTOMER_MANAGED_KMS_KEY` für vom Kunden verwaltete Schlüssel oder `_OWNED_KMS_KEY` für Schlüssel, die dem Kunden gehören. AWS AWS

Typ: Zeichenfolge

Zulässige Werte: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

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

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Ein Wiederherstellungspunkt mit einem Index, der den Status von `ACTIVE` hat, kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

IndexStatusMessage

Eine Zeichenfolge in Form einer ausführlichen Meldung, die den Status eines Backup-Indexes erklärt, der dem Erholungspunkt zugeordnet ist.

Typ: Zeichenfolge

InitiationDate

Datum und Uhrzeit der Initiierung des Sicherungsauftrags, mit dem dieser Wiederherstellungspunkt erstellt wurde, im Unix-Format und in koordinierter Weltzeit (UTC).

Typ: Zeitstempel

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: Boolescher Wert

IsParent

Dies gibt den booleschen Wert zurück, dass es sich bei einem Wiederherstellungspunkt um einen übergeordneten (zusammengesetzten) Auftrag handelt.

Typ: Boolescher Wert

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 mehr geändert werden, nachdem ein Backup 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}$`

[ScanResults](#)

Enthält die neuesten Scanergebnisse anhand des Wiederherstellungspunkts und umfasst derzeit `MalwareScanner`, `ScanJobState`, `Findings` und `LastScanTimestamp`

Typ: Array von [ScanResult](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 5 Elemente.

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. Weitere Informationen finden Sie unter [Status des Wiederherstellungspunkts](#) im AWS Backup Entwicklerhandbuch.

- **CREATING** Der Status gibt an, dass ein AWS Backup Job für eine Ressource initiiert wurde. Der Backup-Vorgang wurde gestartet und verarbeitet aktiv einen Backup-Job für den zugehörigen Recovery Point.
- **AVAILABLE** Der Status gibt an, dass das Backup für den Wiederherstellungspunkt erfolgreich erstellt wurde. Der Backup-Vorgang wurde ohne Probleme abgeschlossen und der Recovery Point ist jetzt einsatzbereit.
- **PARTIAL** Der Status gibt an, dass ein Verbundwiederherstellungspunkt über einen oder mehrere verschachtelte Wiederherstellungspunkte verfügt, die nicht im Backup enthalten waren.
- **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 Für Wiederherstellungspunkte von Amazon S3-, Amazon RDS- und Amazon Aurora Ressourcen tritt dieser Status auf, wenn die Aufbewahrungsdauer einer Regel für kontinuierliche Backups geändert wird.

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 EC2 STOPPED 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 | AVAILABLE | STOPPED | CREATING

[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 Wiederherstellungspunkt gespeichert ist.

Typ: Zeichenfolge

Zulässige Werte: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT | RESTORE_ACCESS_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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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,
  "BackupVaultArn": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "RestoreTestingPlanArn": "string"
  },
  "CreatedResourceArn": "string",
  "CreationDate": number,
  "DeletionStatus": "string",
  "DeletionStatusMessage": "string",
```

```
"ExpectedCompletionTimeMinutes": number,  
"IamRoleArn": "string",  
"IsParent": boolean,  
"ParentJobId": "string",  
"PercentDone": "string",  
"RecoveryPointArn": "string",  
"RecoveryPointCreationDate": number,  
"ResourceType": "string",  
"RestoreJobId": "string",  
"SourceResourceArn": "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

BackupVaultArn

Der Amazon-Ressourcenname (ARN) des Backup-Tresors, der den wiederherzustellenden Wiederherstellungspunkt enthält. Dies hilft bei der Identifizierung von Richtlinien und Berechtigungen für den Tresorzugriff.

Typ: Zeichenfolge

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.

Typ: 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

IsParent

Dies ist ein boolescher Wert, der angibt, ob es sich bei dem Wiederherstellungsauftrag um einen übergeordneten (zusammengesetzten) Wiederherstellungsauftrag handelt.

Typ: Boolescher Wert

ParentJobId

Dies ist die eindeutige Kennung des übergeordneten Wiederherstellungsauftrags für den ausgewählten Wiederherstellungsauftrag.

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

SourceResourceArn

Der Amazon-Ressourcenname (ARN) der ursprünglichen Ressource, die gesichert wurde. Dies bietet einen Überblick darüber, welche Ressource wiederhergestellt wird.

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.

Context

Type

HTTP Status Code: 500

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeScanJob

Service: AWS Backup

Gibt die Details des Scanauftrags für die angegebene ScanJob ID zurück.

Anforderungssyntax

```
GET /scan/jobs/ScanJobId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ScanJobId

Identifiziert eindeutig eine Anfrage AWS Backup zum Scannen einer Ressource.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "IamRoleArn": "string",
  "MalwareScanner": "string",
  "RecoveryPointArn": "string",
```

```

"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"ScanBaseRecoveryPointArn": "string",
"ScanId": "string",
"ScanJobId": "string",
"ScanMode": "string",
"ScannerRoleArn": "string",
"ScanResult": {
  "ScanResultStatus": "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.

AccountId

Gibt die Konto-ID zurück, der der Scanauftrag gehört.

Pattern: `^[0-9]{12}$`

Typ: Zeichenfolge

BackupVaultArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert; zum Beispiel `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 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}$`

Typ: Zeichenfolge

CompletionDate

Datum und Uhrzeit, an dem die Erstellung eines Backup-Index abgeschlossen wurde, im Unix-Format und in koordinierter 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 Scanauftrags, einschließlich des Sicherungsplans und der Regel, die den Scan initiiert haben.

Typ: [ScanJobCreator](#) Objekt

CreationDate

Datum und Uhrzeit, zu der die Erstellung eines Backup-Index abgeschlossen wurde, im Unix-Format und in koordinierter 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

IamRoleArn

Ein Amazon-Ressourcenname (ARN), der einen Backup-Tresor eindeutig identifiziert, z. B. `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

MalwareScanner

Die Scan-Engine, die für den entsprechenden Scanauftrag verwendet wurde. Derzeit wird nur GUARDUTY unterstützt.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

RecoveryPointArn

Ein ARN, der den Zielwiederherstellungspunkt für das Scannen eindeutig identifiziert.; zum Beispiel `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

ResourceArn

Ein ARN, der die Quellressource des entsprechenden Wiederherstellungspunkt-ARN eindeutig identifiziert.

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.

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Typ: Zeichenfolge

Zulässige Werte: EBS | EC2 | S3

ScanBaseRecoveryPointArn

Ein ARN, der den Basiswiederherstellungspunkt für das Scannen eindeutig identifiziert. Dieses Feld wird nur ausgefüllt, wenn ein inkrementeller Scanauftrag stattgefunden hat.

Typ: Zeichenfolge

ScanId

Die von Amazon GuardDuty für die entsprechende Scan-Job-ID-Anfrage von generierte Scan-ID AWS Backup.

Typ: Zeichenfolge

ScanJobId

Die Scanauftrags-ID, mit der die Anfrage eindeutig identifiziert wurde AWS Backup.

Typ: Zeichenfolge

ScanMode

Gibt den für den Scanauftrag verwendeten Scantyp an.

Typ: Zeichenfolge

Zulässige Werte: FULL_SCAN | INCREMENTAL_SCAN

ScannerRoleArn

Gibt die Scanner-IAM-Rolle an, für die ARN für den Scanauftrag verwendet wurde.

Typ: Zeichenfolge

ScanResult

Enthält den Wert ScanResultsStatus für den Scanauftrag und gibt den Wert NO_THREATS_FOUND für THREATS_FOUND abgeschlossene Aufträge zurück.

Typ: [ScanResultInfo](#) Objekt

State

Der aktuelle Status eines Scanauftrags.

Typ: Zeichenfolge

Zulässige Werte: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

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](#).

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DisassociateBackupVaultMpaApprovalTeam

Service: AWS Backup

Entfernt die Zuordnung zwischen einem MPA-Genehmigungsteam und einem Backup-Tresor und deaktiviert so den MPA-Genehmigungsworkflow für Wiederherstellungsvorgänge.

Anforderungssyntax

```
POST /backup-vaults/backupVaultName/mpaApprovalTeam?delete HTTP/1.1
Content-type: application/json

{
  "RequesterComment": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name des Backup-Tresors, von dem das MPA-Genehmigungsteam getrennt werden soll.

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

RequesterComment

Ein optionaler Kommentar, in dem der Grund für die Trennung des MPA-Genehmigungsteams vom Backup-Tresor erläutert wird.

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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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?  
MaxScheduledRunsPreview=MaxScheduledRunsPreview&versionId=VersionId HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupPlanId

Identifiziert einen Backup-Plan.

Erforderlich: Ja

MaxScheduledRunsPreview

Anzahl der future geplanten Backup-Läufe für die Vorschau. Wenn der Wert auf 0 gesetzt ist (Standard), ist keine Vorschau für geplante Läufe in der Antwort enthalten. Der gültige Bereich liegt zwischen 0 und 10.

Gültiger Bereich: Mindestwert 0. Der Maximalwert ist 10.

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Version IDs kann 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,
                "DeleteAfterEvent": "string",
                "MoveToColdStorageAfterDays": number,
                "OptInToArchiveForSupportedResources": boolean
              }
            }
          ],
          "EnableContinuousBackup": boolean,
          "IndexActions": [
            {
              "ResourceTypes": [ "string" ]
            }
          ],
          "Lifecycle": {
            "DeleteAfterDays": number,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ]
    }
  ],
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  }
},

```

```

    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],
    "ScannerRoleArn": "string"
  }
]
},
"BackupPlanArn": "string",
"BackupPlanId": "string",
"CreationDate": number,
"CreatorRequestId": "string",
"DeletionDate": number,
"LastExecutionDate": number,
"ScheduledRunsPreview": [
  {
    "ExecutionTime": number,
    "RuleExecutionType": "string",
    "RuleId": "string"
  }
],
"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

ScheduledRunsPreview

Liste der bevorstehenden geplanten Backup-Läufe. Nur enthalten, wenn der `MaxScheduledRunsPreview` Parameter größer als 0 ist. Enthält bis zu 10 future Backup-Ausführungen mit ihren geplanten Zeiten, Ausführungstypen und zugehörigen Regeln IDs.

Typ: Array von [ScheduledPlanExecutionMember](#)-Objekten

VersionId

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Die Version IDs 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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ],
      "EnableContinuousBackup": boolean,
      "IndexActions": [
        {
          "ResourceTypes": [ "string" ]
        }
      ],
      "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      },
      "RecoveryPointTags": {
        "string" : "string"
      },
      "RuleId": "string",
      "RuleName": "string",
      "ScanActions": [
        {
          "MalwareScanner": "string",
          "ScanMode": "string"
        }
      ],
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowMinutes": number,
      "TargetBackupVaultName": "string",

```

```

        "TargetLogicallyAirGappedBackupVaultArn": "string"
    },
    ],
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string " ],
            "ScannerRoleArn": "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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      }
    },
    "EnableContinuousBackup": boolean,
    "IndexActions": [
      {
        "ResourceTypes": [ "string" ]
      }
    ],
    "Lifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],

```

```
        "ScannerRoleArn": "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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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` | `CONTINUOUS_BACKUP_INTERRUPTED` | `RECOVERY_POINT_INDEX_COMPLETED` | `RECOVERY_POINT_INDEX_DELETED` | `RECOVERY_POINT_INDEXING_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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

GetRecoveryPointIndexDetails

Service: AWS Backup

Dieser Vorgang gibt die Metadaten und Details zurück, die für den Backup-Index spezifisch sind, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Anforderungssyntax

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index 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.

Zu den zulässigen Zeichen gehören Kleinbuchstaben, Zahlen und Bindestriche.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

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`.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
  "BackupVaultArn": "string",
  "IndexCompletionDate": number,
  "IndexCreationDate": number,
  "IndexDeletionDate": number,
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "RecoveryPointArn": "string",
  "SourceResourceArn": "string",
  "TotalItemsIndexed": 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 ARN, der den Backup-Tresor, in dem der Wiederherstellungspunktindex gespeichert ist, eindeutig identifiziert.

Beispiel, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

[IndexCompletionDate](#)

Datum und Uhrzeit, an dem die Erstellung eines Backup-Index abgeschlossen wurde, im Unix-Format und in koordinierter 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

[IndexCreationDate](#)

Datum und Uhrzeit der Erstellung eines Backup-Index im Unix-Format und in koordinierter 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

IndexDeletionDate

Datum und Uhrzeit der Löschung eines Backup-Index im Unix-Format und in koordinierter 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

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: PENDING | ACTIVE | FAILED DELETING

Ein Wiederherstellungspunkt mit einem Index, der den Status von hat, ACTIVE kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: PENDING | ACTIVE | FAILED | DELETING

IndexStatusMessage

Eine ausführliche Meldung, in der der Status eines Backup-Indexes erläutert wird, der dem Wiederherstellungspunkt zugeordnet ist.

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

SourceResourceArn

Eine Zeichenfolge mit dem Amazon-Ressourcennamen (ARN), der die Quellressource eindeutig identifiziert.

Typ: Zeichenfolge

TotalItemsIndexed

Anzahl der Elemente innerhalb des Backup-Index, die dem Wiederherstellungspunkt zugeordnet sind.

Type: Long

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

GetRestoreJobMetadata

Service: AWS Backup

Diese Anforderung 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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=RecoveryPointArn  
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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

GetRestoreTestingSelection

Service: AWS Backup

Retournen 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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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
- S3 für Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- Storage Gateway für AWS Storage Gateway
- Timestream für Amazon Timestream
- VirtualMachine für VMware virtuelle Maschinen

Typ: Zeichenfolge-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.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

GetTieringConfiguration

Service: AWS Backup

Gibt TieringConfiguration-Details für die angegebene TieringConfigurationName zurück. Die Details sind der Hauptteil einer Tiering-Konfiguration im JSON-Format, zusätzlich zu den Konfigurationsmetadaten.

Anforderungssyntax

```
GET /tiering-configurations/tieringConfigurationName HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

tieringConfigurationName

Der eindeutige Name einer Tiering-Konfiguration.

Pattern: `^[a-zA-Z0-9_]{1,200}$`

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "CreationTime": number,
    "CreatorRequestId": "string",
    "LastUpdatedTime": number,
    "ResourceSelection": [
      {
        "Resources": [ "string" ],

```

```
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
    },
    "TieringConfigurationArn": "string",
    "TieringConfigurationName": "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.

[TieringConfiguration](#)

Gibt den Hauptteil einer Tiering-Konfiguration an. Beinhaltet `TieringConfigurationName`.

Typ: [TieringConfiguration](#) 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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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&completeBefore=ByCompleteBefore  
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
- RDS für Amazon Relational Database Service
- Redshift für Amazon Redshift
- S3 für Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- Storage Gateway für AWS Storage Gateway
- Timestream für Amazon Timestream
- VirtualMachine für VMware 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",
        "BackupPlanName": "string",
        "BackupPlanVersion": "string",
        "BackupRuleCron": "string",
        "BackupRuleId": "string",
        "BackupRuleName": "string",
        "BackupRuleTimezone": "string"
      },
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "ExpectedCompletionDate": number,
      "IamRoleArn": "string",
      "InitiationDate": number,
      "IsEncrypted": boolean,
      "IsParent": boolean,
```

```

    "MessageCategory": "string",
    "ParentJobId": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointLifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "StartBy": number,
    "State": "string",
    "StatusMessage": "string",
    "VaultLockState": "string",
    "VaultType": "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.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 Löschdatum, Plannamen und Version 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

[BackupSelectionList](#)

Eine Reihe von Elementen in der Backup-Auswahlliste, die Metadaten zu jeder Ressource in der Liste enthalten.

Typ: Array von [BackupSelectionListMember](#)-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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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 |
RESTORE_ACCESS_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",
      "EncryptionKeyType": "string",
      "LockDate": number,
      "Locked": boolean,
      "MaxRetentionDays": number,
      "MinRetentionDays": number,
      "NumberOfRecoveryPoints": number,
      "VaultState": "string",
      "VaultType": "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.

BackupVaultList

Eine Reihe von Elementen der Backup-Tresor-Liste mit Tresor-Metadaten, darunter Amazon-Ressourcenname (ARN), Anzeigenname, 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.

Context

Type

HTTP-Statuscode: 400

`MissingParameterValueException`

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

`ResourceNotFoundException`

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&destinationVaultArn=ByDestinationVaultArn  
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
- RDS für Amazon Relational Database Service
- Redshift für Amazon Redshift
- S3 für Amazon Simple Storage Service (Amazon S3)

- SAP HANA on Amazon EC2 für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- Storage Gateway für AWS Storage Gateway
- Timestream für Amazon Timestream
- VirtualMachine für VMware virtuelle Maschinen

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[BySourceRecoveryPointArn](#)

Filter kopieren Jobs nach dem angegebenen Quellwiederherstellungspunkt-ARN.

[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 Anforderung zur Rückgabe der MaxResults Anzahl von Elementen gestellt wird, NextToken können Sie mehr Elemente in Ihrer Liste zurückgeben, 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

{
  "CopyJobs": [
    {
      "AccountId": "string",
```

```

    "BackupSizeInBytes": number,
    "ChildJobsInState": {
      "string" : number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "BackupPlanVersion": "string",
      "BackupRuleCron": "string",
      "BackupRuleId": "string",
      "BackupRuleName": "string",
      "BackupRuleTimezone": "string"
    },
    "CreatedByBackupJobId": "string",
    "CreationDate": number,
    "DestinationBackupVaultArn": "string",
    "DestinationEncryptionKeyArn": "string",
    "DestinationRecoveryPointArn": "string",
    "DestinationRecoveryPointLifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "DestinationVaultLockState": "string",
    "DestinationVaultType": "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.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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]{1,2}$`

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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListIndexedRecoveryPoints

Service: AWS Backup

Dieser Vorgang gibt eine Liste von Wiederherstellungspunkten zurück, denen ein Index zugeordnet ist, der zu dem angegebenen Konto gehört.

Optionale Parameter, die Sie angeben können, sind: MaxResults NextToken SourceResourceArns; CreatedBefore; CreatedAfter;; und ResourceType.

Anforderungssyntax

```
GET /indexes/recovery-point/?
createdAfter=CreatedAfter&createdBefore=CreatedBefore&indexStatus=IndexStatus&maxResults=MaxRes
HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

CreatedAfter

Gibt nur indizierte Wiederherstellungspunkte zurück, die nach dem angegebenen Datum erstellt wurden.

CreatedBefore

Gibt nur indizierte Wiederherstellungspunkte zurück, die vor dem angegebenen Datum erstellt wurden.

IndexStatus

Fügen Sie diesen Parameter hinzu, um die zurückgegebene Liste nach den angegebenen Status zu filtern.

Zulässige Werte: PENDING | ACTIVE | FAILED DELETING

Ein Wiederherstellungspunkt mit einem Index, der den Status von hat, ACTIVE kann in eine Suche aufgenommen werden.

Zulässige Werte: PENDING | ACTIVE | FAILED | DELETING

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente der Ressourcenliste.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

[NextToken](#)

Der nächste Eintrag folgt auf eine unvollständige Liste der zurückgegebenen Wiederherstellungspunkte.

Wenn beispielsweise die Rückgabe der `MaxResults` Anzahl der indizierten Wiederherstellungspunkte angefordert wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token verweist.

[ResourceType](#)

Gibt eine Liste von indizierten Wiederherstellungspunkten für die angegebenen Ressourcentypen zurück.

Zu den akzeptierten Werten gehören:

- EBS für Amazon Elastic Block Store
- S3 für Amazon Simple Storage Service (Amazon S3)

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[SourceResourceArn](#)

Eine Zeichenfolge mit dem Amazon-Ressourcennamen (ARN), der die Quellressource eindeutig identifiziert.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "IndexedRecoveryPoints": [
    {
      "BackupCreationDate": number,
      "BackupVaultArn": "string",
      "IamRoleArn": "string",
      "IndexCreationDate": number,
```



```
    "IndexStatus": "string",
    "IndexStatusMessage": "string",
    "RecoveryPointArn": "string",
    "ResourceType": "string",
    "SourceResourceArn": "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.

[IndexedRecoveryPoints](#)

Dies ist eine Liste von Wiederherstellungspunkten, denen ein Index zugeordnet ist, der zu dem angegebenen Konto gehört.

Typ: Array von [IndexedRecoveryPoint](#)-Objekten

[NextToken](#)

Der nächste Eintrag folgt auf eine unvollständige Liste der zurückgegebenen Wiederherstellungspunkte.

Wenn beispielsweise die Rückgabe der `MaxResults` Anzahl der indizierten Wiederherstellungspunkte angefordert wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, 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.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 der Tresore, 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.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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=ByCreatedAfter  
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-Ressourcenamen (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
- RDS für Amazon Relational Database Service
- Redshift für Amazon Redshift
- S3 für Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- Storage Gateway für AWS Storage Gateway

- Timestream für Amazon Timestream
- VirtualMachine für VMware 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": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CalculatedLifecycle": {
        "DeleteAt": number,
        "MoveToColdStorageAt": number
      }
    },
    ...
  ]
}
```



```

    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanName": "string",
        "BackupPlanVersion": "string",
        "BackupRuleCron": "string",
        "BackupRuleId": "string",
        "BackupRuleName": "string",
        "BackupRuleTimezone": "string"
    },
    "CreationDate": number,
    "EncryptionKeyArn": "string",
    "EncryptionKeyType": "string",
    "IamRoleArn": "string",
    "IndexStatus": "string",
    "IndexStatusMessage": "string",
    "InitiationDate": number,
    "IsEncrypted": boolean,
    "IsParent": boolean,
    "LastRestoreTime": number,
    "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListRecoveryPointsByLegalHold

Service: AWS Backup

Diese Aktion gibt den Wiederherstellungspunkt ARNs (Amazon Resource Names) zurück, der den angegebenen gesetzlichen Aufbewahrungszeitpunkt hat.

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 gesetzlichen 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListRecoveryPointsByResource

Service: AWS Backup

Die Informationen zu den Wiederherstellungspunkten des Typs, der durch den Amazon Resource Name (ARN) einer Ressource angegeben wird.

Note

Für Amazon EFS und Amazon listet diese Aktion nur Wiederherstellungspunkte auf EC2, die von erstellt wurden AWS Backup.

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: Boolescher Wert

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": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeBytes": number,
      "BackupVaultName": "string",
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "EncryptionKeyType": "string",
      "IndexStatus": "string",
      "IndexStatusMessage": "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 Recovery Points 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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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=NextToken  
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 | COMPLETED_WITH_ISSUES

Bitte beachten Sie, dass nur Scanaufträge mit dem Status abgeschlossen und mit Problemen abgeschlossen abgeschlossen werden. Bei Backup-Jobs handelt es sich um eine

Konsoleninterpretation eines Jobs, der im Status abgeschlossen abgeschlossen wird und eine Statusmeldung enthält.

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.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)

- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListRestoreAccessBackupVaults

Service: AWS Backup

Gibt eine Liste von Backup-Tresoren mit Wiederherstellungszugriff zurück, die einem angegebenen Backup-Tresor zugeordnet sind.

Anforderungssyntax

```
GET /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/?  
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name des Backup-Tresors, für den die zugehörigen Backup-Tresore mit Wiederherstellungszugriff aufgelistet werden sollen.

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

Erforderlich: Ja

MaxResults

Die maximale Anzahl von Elementen, die in der Antwort zurückgegeben werden sollen.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

NextToken

Das Paginierungstoken aus einer vorherigen Anfrage zum Abrufen der nächsten Ergebnisgruppe.

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "RestoreAccessBackupVaults": [
    {
      "ApprovalDate": number,
      "CreationDate": number,
      "LatestRevokeRequest": {
        "ExpiryDate": number,
        "InitiationDate": number,
        "MpaSessionArn": "string",
        "Status": "string",
        "StatusMessage": "string"
      },
      "RestoreAccessBackupVaultArn": "string",
      "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.

[NextToken](#)

Das Paginierungstoken, das in einer nachfolgenden Anfrage verwendet werden soll, um den nächsten Satz von Ergebnissen abzurufen.

Typ: Zeichenfolge

[RestoreAccessBackupVaults](#)

Eine Liste der Backup-Tresore mit Wiederherstellungszugriff, die dem angegebenen Backup-Tresor zugeordnet sind.

Typ: Array von [RestoreAccessBackupVaultListMember](#)-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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&parentJobId=ByParentJobId  
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.

[ByParentJobId](#)

Dies ist ein Filter, um untergeordnete (verschachtelte) Wiederherstellungsaufträge auf der Grundlage der ID des übergeordneten Wiederherstellungsauftrags aufzulisten.

[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
- RDS für Amazon Relational Database Service
- Redshift für Amazon Redshift
- S3 für Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud-Instances
- Storage Gateway für AWS Storage Gateway
- Timestream für Amazon Timestream
- VirtualMachine für VMware 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,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
```

```
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "SourceResourceArn": "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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [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=ByRecoveryPointCreationDateAfter&recoveryPointCreationDateBefore=ByRecoveryPointCreationDateBefore  
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,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
```

```
"PercentDone": "string",
"RecoveryPointArn": "string",
"RecoveryPointCreationDate": number,
"ResourceType": "string",
"RestoreJobId": "string",
"SourceResourceArn": "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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 `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/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]{1,2}$`

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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListScanJobs

Service: AWS Backup

Gibt eine Liste der vorhandenen Scanaufträge für ein authentifiziertes Konto der letzten 30 Tage zurück.

Anforderungssyntax

```
GET /scan/jobs?
```

```
ByAccountId=ByAccountId&ByBackupVaultName=ByBackupVaultName&ByCompleteAfter=ByCompleteAfter&ByC
```

```
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 Organisationsverwaltungskonto aus verwendet wird, werden beim Übergeben alle Jobs in der gesamten Organisation * zurückgegeben.

Pattern: `^[0-9]{12}$`

[ByBackupVaultName](#)

Gibt nur Scanaufträge zurück, die im angegebenen Backup-Tresor 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.

Pattern: `^[a-zA-Z0-9\-\_\.\.]{2,50}$`

[ByCompleteAfter](#)

Gibt nur Scanaufträge zurück, die nach einem im Unix-Format und koordinierten Weltzeit (UTC) angegebenen Datum abgeschlossen wurden.

[ByCompleteBefore](#)

Gibt nur Backup-Aufträge zurück, die vor einem Datum im Unix-Format und in der koordinierten Weltzeit (UTC) abgeschlossen wurden.

[ByMalwareScanner](#)

Gibt nur die Scanaufträge für den angegebenen Malware-Scanner zurück. Unterstützt derzeit nur GUARDDUTY.

Zulässige Werte: GUARDDUTY

[ByRecoveryPointArn](#)

Gibt nur die Scanaufträge zurück, die für den angegebenen Wiederherstellungspunkt ausgeführt wurden.

[ByResourceArn](#)

Gibt nur Scanaufträge zurück, die mit dem angegebenen Amazon Resource Name (ARN) der angegebenen Ressource übereinstimmen.

[ByResourceType](#)

Gibt die Wiederherstellungstest-Auswahlen nach dem angegebenen Namen des Wiederherstellungstestplans zurück.

- EBS für Amazon Elastic Block Store
- EC2 für Amazon Elastic Compute Cloud
- S3 für Amazon Simple Storage Service (Amazon S3)

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Zulässige Werte: EBS | EC2 | S3

[ByScanResultStatus](#)

Gibt nur die Scanaufträge für die angegebenen Scanergebnisse zurück:

- THREATS_FOUND
- NO_THREATS_FOUND

Zulässige Werte: NO_THREATS_FOUND | THREATS_FOUND

[ByState](#)

Gibt nur die Scanaufträge für den angegebenen Scanauftragsstatus zurück.

Zulässige Werte: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

MaxResults

Die maximale Anzahl der zurückzugebenden Elemente.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

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",
  "ScanJobs": [
    {
      "AccountId": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "IamRoleArn": "string",
      "MalwareScanner": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
```

```
"ResourceName": "string",
"ResourceType": "string",
"ScanBaseRecoveryPointArn": "string",
"ScanId": "string",
"ScanJobId": "string",
"ScanMode": "string",
"ScannerRoleArn": "string",
"ScanResult": {
  "ScanResultStatus": "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.

[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

[ScanJobs](#)

Ein Array von Strukturen, das Metadaten zu Ihren Scanaufträgen enthält, die im JSON-Format zurückgegeben wurden.

Typ: Array von [ScanJob](#)-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.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListScanJobSummaries

Service: AWS Backup

Dies ist eine Anforderung für eine Zusammenfassung der Scanaufträge, die in den letzten 30 Tagen erstellt wurden oder ausgeführt wurden.

Anforderungssyntax

```
GET /audit/scan-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MalwareScanner=MalwareScanner&MaxResults=MaxResults  
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 verwenden ANY, um die Anzahl der Jobs 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]{1,2}$`

AggregationPeriod

Der Zeitraum für die zurückgegebenen Ergebnisse.

- ONE_DAY Die tägliche Anzahl an Aufträgen für den letzten Tag.
- SEVEN_DAYS Die tägliche Anzahl an Aufträgen für die letzten 7 Tage.
- FOURTEEN_DAYS Die tägliche Anzahl an Aufträgen für die letzten 14 Tage.

Zulässige Werte: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MalwareScanner

Gibt nur die Scanaufträge für den angegebenen Malware-Scanner zurück. Derzeit MalwareScanner ist das einzige GUARDDUTY. Das Feld unterstützt aber auch ANY, und AGGREGATE_ALL.

Zulässige Werte: GUARDDUTY

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.

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.

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.

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

ScanResultStatus

Gibt nur die Scanaufträge für die angegebenen Scanergebnisse zurück.

Zulässige Werte: NO_THREATS_FOUND | THREATS_FOUND

State

Gibt nur die Scanaufträge für den angegebenen Scanauftragsstatus zurück.

Zulässige Werte: CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "NextToken": "string",
  "ScanJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MalwareScanner": "string",
      "Region": "string",
      "ResourceType": "string",
      "ScanResultStatus": "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_DAYDie tägliche Anzahl an Aufträgen für den letzten Tag.
- SEVEN_DAYSDie tägliche Anzahl an Aufträgen für die letzten 7 Tage.

- `FOURTEEN_DAYS` Die tägliche Anzahl an Aufträgen für die letzten 14 Tage.

Zulässige Werte: `'ONE_DAY'` | `'SEVEN_DAYS'` | `'FOURTEEN_DAYS'`

Typ: Zeichenfolge

[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

[ScanJobSummaries](#)

Die zusammenfassenden Informationen.

Typ: Array von [ScanJobSummary](#)-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.

Context

Type

HTTP-Statuscode: 400

`ServiceUnavailableException`

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Dieser Vorgang gibt Ergebnisse zurück, die vom Ressourcentyp abhängen, der im Wert für `resourceArn` verwendet wurde. Beispielsweise haben Wiederherstellungspunkte von Amazon DynamoDB mit erweiterten Einstellungen einen ARN (Amazon Resource Name), der mit `arn:aws:backup` beginnt. Wiederherstellungspunkte (Backups) von DynamoDB ohne aktivierte erweiterte Einstellungen haben einen ARN, der mit `arn:aws:dynamodb` beginnt.

Wenn dieser Vorgang aufgerufen wird und Sie Werte für `resourceArn` angeben, die einen anderen ARN als `arn:aws:backup` haben, kann er eine der unten aufgeführten Ausnahmen zurückgeben. Um diese Ausnahme zu verhindern, sollten Sie nur Werte angeben, die Ressourcentypen repräsentieren, die vollständig von verwaltet werden AWS Backup. Diese haben einen ARN, der beginnt mit `arn:aws:backup` und sie sind in der Tabelle [Verfügbarkeit von Funktionen nach Ressourcen](#) vermerkt.

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListTieringConfigurations

Service: AWS Backup

Gibt eine Liste von Tiering-Konfigurationen zurück.

Anforderungssyntax

```
GET /tiering-configurations/?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",
  "TieringConfigurations": [
    {
      "BackupVaultName": "string",
      "CreationTime": number,
      "LastUpdatedTime": number,
```

```
    "TieringConfigurationArn": "string",  
    "TieringConfigurationName": "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

[TieringConfigurations](#)

Ein Array von Tiering-Konfigurationen, die durch den `ListTieringConfigurations` Aufruf zurückgegeben wurden.

Typ: Array von [TieringConfigurationsListMember](#)-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.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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. Eine Liste der unterstützten Ereignisse, häufigen Anwendungsfälle und Codebeispiele finden Sie unter [Benachrichtigungsoptionen mit AWS Backup](#).

 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.

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 | CONTINUOUS_BACKUP_INTERRUPTED |
RECOVERY_POINT_INDEX_COMPLETED | RECOVERY_POINT_INDEX_DELETED |
RECOVERY_POINT_INDEXING_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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

RevokeRestoreAccessBackupVault

Service: AWS Backup

Widerruft den Zugriff auf einen Backup-Tresor mit Wiederherstellungszugriff, wodurch die Möglichkeit zur Wiederherstellung von seinen Wiederherstellungspunkten entfernt wird und der Tresor dauerhaft gelöscht wird.

Anforderungssyntax

```
DELETE /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/restoreAccessBackupVaultArn?requesterComment=RequesterComment HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

backupVaultName

Der Name des Quell-Backup-Tresors, der dem Backup-Tresor mit Wiederherstellungszugriff zugeordnet ist, der gesperrt werden soll.

Pattern: `^[a-zA-Z0-9\-\_\]{2,50}$`

Erforderlich: Ja

RequesterComment

Ein Kommentar, in dem der Grund für den Widerruf des Zugriffs auf den Backup-Tresor mit Wiederherstellungszugriff erläutert wird.

restoreAccessBackupVaultArn

Der ARN des Backup-Tresors mit Wiederherstellungszugriff, der widerrufen werden soll.

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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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",
  "Index": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "LogicallyAirGappedBackupVaultArn": "string",
  "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

Index

Fügen Sie diesen Parameter hinzu, um die Indexerstellung zu aktivieren, wenn Ihr Backup-Job einen Ressourcentyp hat, der Backup-Indizes unterstützt.

Zu den Ressourcentypen, die Backup-Indizes unterstützen, gehören:

- EBS für Amazon Elastic Block Store
- S3 für Amazon Simple Storage Service (Amazon S3)

Der Index kann einen von 2 möglichen Werten haben, entweder `ENABLED` oder `DISABLED`.

Um einen Backup-Index für einen geeigneten `ACTIVE Recovery Point` zu erstellen, der noch keinen Backup-Index hat, legen Sie den Wert auf `festENABLED`.

Um einen Backup-Index zu löschen, legen Sie den Wert auf `festDISABLED`.

Typ: Zeichenfolge

Zulässige Werte: `ENABLED` | `DISABLED`

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 Archivspeicher übertragene Backups 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 mehr geändert werden, nachdem ein Backup 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

LogicallyAirGappedBackupVaultArn

Der ARN eines Tresors mit logischem Air-Gap. Der ARN muss sich im selben Konto und in derselben Region befinden. Falls verfügbar, werden unterstützte, vollständig verwaltete Ressourcen direkt in einem Tresor mit logischem Air-Gap gesichert, während andere unterstützte Ressourcen einen temporären (kostenpflichtigen) Snapshot im Backup-Tresor erstellen und ihn dann in den Tresor mit logischem Air-Gap kopieren. Nicht unterstützte Ressourcen werden nur im angegebenen Backup-Tresor gesichert.

Typ: Zeichenfolge

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 aufRUNNING) 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: Boolescher Wert

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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Informationen darüber, wie [bei Wiederholungsversuchen Auftragsvorgänge kopiert](#) werden, finden Sie unter AWS Backup Wiederholung von Aufträgen.

Anforderungssyntax

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
  "DestinationBackupVaultArn": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "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 Erholungspunkt in einen Cold Storage übergeht oder gelöscht wird.

In den Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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; zum Beispiel `arn:aws:backup:us-east-1:123456789012:recovery-point:1B5E7-9EB0-435A-A80B-108B488B0D45`. EB3

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: Boolescher Wert

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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Ressourcename (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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

StartScanJob

Service: AWS Backup

Startet das Scannen von Aufträgen für bestimmte Ressourcen.

Anforderungssyntax

```
PUT /scan/job HTTP/1.1
Content-type: application/json

{
  "BackupVaultName": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "MalwareScanner": "string",
  "RecoveryPointArn": "string",
  "ScanBaseRecoveryPointArn": "string",
  "ScanMode": "string",
  "ScannerRoleArn": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

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.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Typ: Zeichenfolge

Erforderlich: Ja

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 `StartScanJob` 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

MalwareScanner

Gibt den Malware-Scanner an, der während des Scanauftrags verwendet wurde. Unterstützt derzeit nur `GUARDDUTY`.

Typ: Zeichenfolge

Zulässige Werte: `GUARDDUTY`

Erforderlich: Ja

RecoveryPointArn

Ein Amazon-Ressourcenname (ARN), der einen Wiederherstellungspunkt eindeutig identifiziert. Dies ist Ihr Ziel-Erholungspunkt für einen vollständigen Scan. Wenn Sie einen inkrementellen Scan ausführen, ist dies Ihr Erholungspunkt, der nach der Auswahl Ihres Basiswiederherstellungspunkts erstellt wurde.

Typ: Zeichenfolge

Erforderlich: Ja

ScanBaseRecoveryPointArn

Ein ARN, der den Basiswiederherstellungspunkt, der für das inkrementelle Scannen verwendet werden soll, eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

ScanMode

Gibt den für den Scanauftrag verwendeten Scantyp an.

Beinhaltet:

- `FULL_SCAN` scannt die gesamte Datenlinie innerhalb des Backups.
- `INCREMENTAL_SCAN` scannt den Datenunterschied zwischen dem Zielwiederherstellungspunkt und dem Basiswiederherstellungspunkt-ARN.

Typ: Zeichenfolge

Zulässige Werte: `FULL_SCAN` | `INCREMENTAL_SCAN`

Erforderlich: Ja

ScannerRoleArn

Der ARN für die IAM-Scannerrolle wurde angegeben.

Typ: Zeichenfolge

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationDate": number,
  "ScanJobId": "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.

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

ScanJobId

Identifiziert eindeutig eine Anfrage AWS Backup zur Sicherung einer Ressource.

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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 Aurora
- Amazon DocumentDB (mit MongoDB-Kompatibilität)
- Amazon FSx für Lustre
- Amazon FSx für NetApp ONTAP
- Amazon FSx für OpenZFS
- Amazon FSx für Windows-Dateiserver
- Amazon Neptune
- SAP HANA-Datenbanken auf EC2 Amazon-Instances
- Amazon RDS

Anforderungssyntax

```
POST /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
```

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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

TagResource

Service: AWS Backup

Weist einer Ressource einen Satz von Schlüssel-Wert-Paaren zu.

Anforderungssyntax

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json
```

```
{
  "Tags": {
    "string" : "string"
  }
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

resourceArn

Der ARN, der die Ressource eindeutig identifiziert.

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.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 backup sind, sind mit Tagging nicht kompatibel. TagResource und wenn UntagResource ungültig angegeben ARNs wird, wird ein Fehler angezeigt. 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
            "ResourceTypes": [ "string" ]
          }
        ],
        "Lifecycle": {
```

```

        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
}
],
"ScanSettings": [
    {
        "MalwareScanner": "string",
        "ResourceTypes": [ "string" ],
        "ScannerRoleArn": "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,
  "ScanSettings": [
    {
      "MalwareScanner": "string",
      "ResourceTypes": [ "string" ],
      "ScannerRoleArn": "string"
    }
  ],
  "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

[ScanSettings](#)

Enthält Ihre Scankonfiguration für den Backup-Plan und umfasst den Malware-Scanner, Ihre ausgewählten Ressourcen und die Scannerrolle.

Typ: Array von [ScanSetting](#)-Objekten

[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.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 2020-07-10T15:00:00.000-08:00 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.

Arn

Context

CreatorRequestId

Type

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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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](#)

Zu den Eingaben können gehören:

Ein Wert für `isCrossAccountBackupEnabled` und eine Region. Beispiel: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Ein Wert für die Genehmigung durch mehrere Parteien im Stil „Mpa“: `isMpaEnabled` Werte können wahr oder falsch sein. Beispiel: `update-global-settings --global-settings isMpaEnabled=false --region us-west-2`.

Ein Wert für die Erstellung einer mit dem Backup-Service verknüpften Rolle, formatiert als `isDelegatedAdministratorEnabled` Werte können wahr oder falsch sein. Beispiel: `update-global-settings --global-settings isDelegatedAdministratorEnabled=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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateRecoveryPointIndexSettings

Service: AWS Backup

Dieser Vorgang aktualisiert die Einstellungen eines Wiederherstellungspunktindexes.

Erforderlich: BackupVaultName RecoveryPointArn, und IAMRole Arn

Anforderungssyntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index HTTP/1.1
Content-type: application/json
```

```
{
  "IamRoleArn": "string",
  "Index": "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 - Region, in der sie erstellt wurden, eindeutig sind.

Zu den zulässigen Zeichen gehören Kleinbuchstaben, Zahlen und Bindestriche.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

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`.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

IamRoleArn

Dies gibt den ARN der IAM-Rolle an, der für diesen Vorgang verwendet wird.

Zum Beispiel `arn:aws:iam: :123456789012:role/S3Access`

Typ: Zeichenfolge

Erforderlich: Nein

Index

Der Index kann einen von 2 möglichen Werten haben, entweder `ENABLED` oder `DISABLED`.

Um einen Backup-Index für einen geeigneten ACTIVE Recovery Point zu erstellen, der noch keinen Backup-Index hat, legen Sie den Wert auf `ENABLED`.

Um einen Backup-Index zu löschen, legen Sie den Wert auf `DISABLED`.

Typ: Zeichenfolge

Zulässige Werte: `ENABLED` | `DISABLED`

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultName": "string",
  "Index": "string",
  "IndexStatus": "string",
  "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.

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}$`

Index

Der Index kann einen von 2 möglichen Werten haben, entweder `ENABLED` oder `DISABLED`.

Der Wert `ENABLED` bedeutet, dass ein Backup-Index für einen geeigneten `ACTIVE Recovery Point` erstellt wurde.

Der Wert `DISABLED` bedeutet, dass ein Backup-Index gelöscht wurde.

Typ: Zeichenfolge

Zulässige Werte: `ENABLED` | `DISABLED`

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Ein Wiederherstellungspunkt mit einem Index, der den Status `ACTIVE` hat, kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

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

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.

Context

Type

HTTP Status Code: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateRecoveryPointLifecycle

Service: AWS Backup

Legt den Übergangslbenszyklus eines Wiederherstellungspunkts fest.

Der Lebenszyklus definiert, wann eine geschützte Ressource in einen Kühltpeicher überführt wird und wann sie abläuft. AWS Backup überträgt Backups automatisch entsprechend dem von Ihnen definierten Lebenszyklus und lässt sie ablaufen.

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.

In den Archivspeicher übertragene Backups 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 mehr geändert werden, nachdem ein Backup in den Archivspeicher übertragen wurde.

Important

Wenn Ihr Lebenszyklus derzeit die Parameter `DeleteAfterDays` und `verwendetMoveToColdStorageAfterDays`, schließen Sie diese Parameter und ihre Werte ein, wenn Sie diesen Vorgang aufrufen. Wenn Sie sie nicht einbeziehen, kann dies dazu führen, dass Ihr Plan mit Nullwerten aktualisiert wird.

Dieser Vorgang unterstützt keine kontinuierlichen Backups.

Anforderungssyntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json
```

```
{
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "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 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 Backups 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 mehr geändert werden, nachdem ein Backup 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,
    "DeleteAfterEvent": "string",
    "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 Archivspeicher übertragene Backups 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 mehr geändert werden, nachdem ein Backup 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.

Context

Type

HTTP-Statuscode: 400

InvalidRequestException

Zeigt an, dass etwas mit der Eingabe für die Anforderung nicht stimmt. Beispielsweise ist ein Parameter vom falschen Typ.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 oder Amazon EC2 RDS zugewiesen wird, wird er in das Backup aufgenommen, auch wenn das Opt-In 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.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 `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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 geschützte Ressourcen ARNs oder Bedingungen 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 den Wiederherstellungstest zu aktualisieren, können Sie entweder geschützte Ressourcen ARNs oder Bedingungen verwenden, aber nicht beide. 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.

Context

Type

HTTP Status Code: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP Status Code: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP Status Code: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP Status Code: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateTieringConfiguration

Service: AWS Backup

Diese Anfrage sendet Änderungen an Ihrer angegebenen Tiering-Konfiguration. `TieringConfigurationName` kann nach der Erstellung nicht aktualisiert werden.

`ResourceSelection` kann enthalten:

- `Resources`
- `TieringDownSettingsInDays`
- `ResourceType`

Anforderungssyntax

```
PUT /tiering-configurations/tieringConfigurationName HTTP/1.1
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ]
  }
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

tieringConfigurationName

Der Name einer zu aktualisierenden Tiering-Konfiguration.

Pattern: `^[a-zA-Z0-9_]{1,200}$`

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

TieringConfiguration

Gibt den Hauptteil einer Tiering-Konfiguration an.

Typ: [TieringConfigurationInputForUpdate](#) Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "LastUpdatedTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "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

Datum und Uhrzeit der Erstellung einer Tiering-Konfiguration im Unix-Format und in koordinierter 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

LastUpdatedTime

Datum und Uhrzeit der Aktualisierung einer Tiering-Konfiguration im Unix-Format und in koordinierter Weltzeit (UTC). Der Wert von `LastUpdatedTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

[TieringConfigurationArn](#)

Ein Amazon-Ressourcenname (ARN), der die aktualisierte Tiering-Konfiguration eindeutig identifiziert.

Typ: Zeichenfolge

[TieringConfigurationName](#)

Diese eindeutige Zeichenfolge ist der Name der Tiering-Konfiguration.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9_]{1,200}$`

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.

Arn

Context

CreatorRequestId

Type

HTTP-Statuscode: 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.

Context

Type

HTTP-Statuscode: 400

InvalidParameterValueException

Zeigt an, dass etwas mit dem Wert eines Parameters nicht stimmt. Beispielsweise liegt der Wert außerhalb des zulässigen Bereichs.

Context

Type

HTTP-Statuscode: 400

LimitExceededException

Ein Limit in der Anforderung wurde überschritten, z. B. die maximale Anzahl von Elementen, die in einer Anforderung zulässig sind.

Context

Type

HTTP-Statuscode: 400

MissingParameterValueException

Zeigt an, dass ein erforderlicher Parameter fehlt.

Context

Type

HTTP-Statuscode: 400

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, ist nicht vorhanden.

Context

Type

HTTP-Statuscode: 400

ServiceUnavailableException

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

Context

Type

HTTP Status Code: 500

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

AWS Backup gateway

Die folgenden Aktionen werden unterstützt von AWS Backup gateway:

- [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 Daten 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 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-Z0-9+]{3})\|[a-zA-Z0-9+]`

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]{1,63}`

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]{1,63}`

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.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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. Die maximale Länge beträgt 180.

Pattern: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

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](#).

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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}){3}\[a-zA-Z-0-9]{3}`

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.

ErrorCode

Eine Beschreibung, warum Sie nicht über ausreichende Berechtigungen verfügen.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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}){3}[/[a-zA-Z-0-9]{3}]`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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. Die maximale Länge beträgt 180.

Pattern: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

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](#).

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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](#).

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Eigenschaftszuordnung zeigt das Verhältnis der vom Hypervisor verfügbaren Entitätseigenschaften 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})\[/code>`

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})\[/code>`

[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 von VMware Tags zu den Tags. AWS

Typ: Array von [VmwareToAwsTagMapping](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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](#).

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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.

ErrorCode

Eine Beschreibung, warum Sie nicht über ausreichende Berechtigungen verfügen.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 ihren 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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 ihren 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](#).

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

`ErrorCode`

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

`ErrorCode`

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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 [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})\[/code>`

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 [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})\[/code>`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Eigenschaftszuordnung zeigt das Verhältnis der vom Hypervisor verfügbaren Entitätseigenschaften 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 Zuordnung von Tags zu den VMware Tags an. AWS

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.

ErrorCode

Eine Beschreibung, warum Sie nicht über ausreichende Berechtigungen verfügen.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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.

ErrorCode

Eine Beschreibung, warum Sie nicht über ausreichende Berechtigungen verfügen.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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})\[/code>`

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})\[/code>`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Z0-9-]{3})\[/code>`

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})\[/code>`

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.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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. 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 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](#).

InternalServerError

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [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-Z0-9]{3}){3}\[a-zA-Z0-9]{3}`

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-]{1,63}):([0-9]{1,5}):log-group:[a-zA-Z0-9_-]{1,63}:[a-zA-Z0-9-]{1,63}`

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-]{1,100}`

Erforderlich: Nein

Password

Das aktualisierte Kennwort für den Hypervisor.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: `[!@#$%^&*~]{1,100}`

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.

ErrorCode

Eine Beschreibung, warum Sie nicht über ausreichende Berechtigungen verfügen.

HTTP Status Code: 400

ConflictException

Der Vorgang kann nicht fortgesetzt werden, da er nicht unterstützt wird.

ErrorCode

Eine Beschreibung, warum der Vorgang nicht unterstützt wird.

HTTP Status Code: 400

InternalServerErrorException

Der Vorgang war nicht erfolgreich, da ein interner Fehler aufgetreten ist. Bitte versuchen Sie es später erneut.

ErrorCode

Eine Beschreibung, welcher interne Fehler aufgetreten ist.

HTTP Status Code: 500

ResourceNotFoundException

Eine Ressource, die für die Aktion erforderlich ist, wurde nicht gefunden.

ErrorCode

Eine Beschreibung, welche Ressource nicht gefunden wurde.

HTTP Status Code: 400

ThrottlingException

TPS wurde auf den Schutz vor absichtlich oder unbeabsichtigt hohen Anforderungsvolumen beschränkt.

ErrorCode

Fehler: 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.

ErrorCode

Eine Beschreibung der Ursache des Validierungsfehlers.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

AWS Backup

Die folgenden Aktionen werden unterstützt von AWS Backup:

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)
- [ListTagsForResource](#)
- [StartSearchJob](#)

- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

GetSearchJob

Service: AWS Backup

Dieser Vorgang ruft Metadaten eines Suchauftrags ab, einschließlich seines Fortschritts.

Anforderungssyntax

```
GET /search-jobs/SearchJobIdentifier HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

SearchJobIdentifier

Erforderliche eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "CurrentSearchProgress": {
    "ItemsMatchedCount": number,
    "ItemsScannedCount": number,
    "RecoveryPointsScannedCount": number
  },
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
          {
            "Operator": "string",
```

```
        "Value": number
      }
    ],
    "FilePaths": [
      {
        "Operator": "string",
        "Value": "string"
      }
    ],
    "LastModificationTimes": [
      {
        "Operator": "string",
        "Value": number
      }
    ],
    "Sizes": [
      {
        "Operator": "string",
        "Value": number
      }
    ]
  }
],
"S3ItemFilters": [
  {
    "CreationTimes": [
      {
        "Operator": "string",
        "Value": number
      }
    ],
    "ETags": [
      {
        "Operator": "string",
        "Value": "string"
      }
    ],
    "ObjectKeys": [
      {
        "Operator": "string",
        "Value": "string"
      }
    ],
    "Sizes": [
```

```

        {
            "Operator": "string",
            "Value": number
        }
    ],
    "VersionIds": [
        {
            "Operator": "string",
            "Value": "string"
        }
    ]
}
]
},
"Name": "string",
"SearchJobArn": "string",
"SearchJobIdentifier": "string",
"SearchScope": {
    "BackupResourceArns": [ "string" ],
    "BackupResourceCreationTime": {
        "CreatedAfter": number,
        "CreatedBefore": number
    },
    "BackupResourceTags": {
        "string" : "string"
    },
    "BackupResourceTypes": [ "string" ],
    "SourceResourceArns": [ "string" ]
},
"SearchScopeSummary": {
    "TotalItemsToScanCount": number,
    "TotalRecoveryPointsToScanCount": number
},
"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.

CompletionTime

Das Datum und die Uhrzeit, zu der ein Suchauftrag abgeschlossen wurde, im Unix-Format und in koordinierter 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

CreationTime

Datum und Uhrzeit der Erstellung eines Suchauftrags im Unix-Format und in koordinierter 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

CurrentSearchProgress

Gibt Zahlen zurück, die für `BackupsScannedCount` `ItemsScanned`, und stehen `ItemsMatched`.

Typ: [CurrentSearchProgress](#) Objekt

EncryptionKeyArn

Der Verschlüsselungsschlüssel für den angegebenen Suchauftrag.

Beispiel: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Typ: Zeichenfolge

ItemFilters

Elementfilter stellen alle Eigenschaften des Eingabeelements dar, die bei der Erstellung der Suche angegeben wurden.

Typ: [ItemFilters](#) Objekt

Name

Der Name des angegebenen Suchauftrags wurde zurückgegeben.

Typ: Zeichenfolge

SearchJobArn

Die eindeutige Zeichenfolge, die den Amazon-Ressourcennamen (ARN) des angegebenen Suchauftrags identifiziert.

Typ: Zeichenfolge

[SearchJobIdentifier](#)

Die eindeutige Zeichenfolge, die den angegebenen Suchauftrag identifiziert.

Typ: Zeichenfolge

[SearchScope](#)

Der Suchbereich umfasst alle Backup-Eigenschaften, die in eine Suche eingegeben werden.

Typ: [SearchScope](#) Objekt

[SearchScopeSummary](#)

Es wurde eine Zusammenfassung des angegebenen Suchauftragsbereichs zurückgegeben, einschließlich:

- TotalBackupsToScanCount, die Anzahl der bei der Suche zurückgegebenen Wiederherstellungspunkte.
- TotalItemsToScanCount, die Anzahl der bei der Suche zurückgegebenen Elemente.

Typ: [SearchScopeSummary](#) Objekt

[Status](#)

Der aktuelle Status des angegebenen Suchauftrags.

Ein Suchauftrag kann einen der folgenden Status haben: RUNNING;;COMPLETED;STOPPED; FAILEDTIMED_OUT; oder EXPIRED.

Typ: Zeichenfolge

Zulässige Werte: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[StatusMessage](#)

Für einen Suchauftrag mit dem Status ERRORRED oder dem Status von COMPLETED Aufträgen mit Problemen wird eine Statusmeldung zurückgegeben.

Beispielsweise kann in einer Meldung angegeben werden, dass eine Suche Wiederherstellungspunkte enthielt, die aufgrund eines Berechtigungsproblems nicht gescannt werden konnten.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

GetSearchResultExportJob

Service: AWS Backup

Dieser Vorgang ruft die Metadaten eines Exportauftrags ab.

Ein Exportauftrag ist ein Vorgang, der die Ergebnisse eines Suchauftrags an einen angegebenen S3-Bucket in einer CSV-Datei überträgt.

Ein Exportauftrag ermöglicht es Ihnen, die Ergebnisse einer Suche über die für den Suchauftrag geplante Aufbewahrungsdauer von 7 Tagen hinaus aufzubewahren.

Anforderungssyntax

```
GET /export-search-jobs/ExportJobIdentifier HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ExportJobIdentifier

Dies ist die eindeutige Zeichenfolge, die einen bestimmten Exportauftrag identifiziert.

Für diesen Vorgang erforderlich.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "ExportJobArn": "string",
  "ExportJobIdentifier": "string",
  "ExportSpecification": { ... },
```

```
"SearchJobArn": "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.

[CompletionTime](#)

Datum und Uhrzeit des Abschlusses eines Exportauftrags im Unix-Format und in koordinierter 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

[CreationTime](#)

Datum und Uhrzeit der Erstellung eines Exportauftrags im Unix-Format und in koordinierter 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

[ExportJobArn](#)

Der eindeutige Amazon-Ressourcenname (ARN), der den Exportauftrag eindeutig identifiziert.

Typ: Zeichenfolge

[ExportJobIdentifier](#)

Dies ist die eindeutige Zeichenfolge, die den angegebenen Exportauftrag identifiziert.

Typ: Zeichenfolge

[ExportSpecification](#)

Die Exportspezifikation besteht aus dem Ziel-S3-Bucket, in den die Suchergebnisse exportiert wurden, sowie dem Zielpräfix.

Typ: [ExportSpecification](#) Objekt

Hinweis: Dieses Objekt ist eine Union. Nur ein Mitglied dieses Objekts kann angegeben oder zurückgegeben werden.

SearchJobArn

Die eindeutige Zeichenfolge, die den Amazon-Ressourcennamen (ARN) des angegebenen Suchauftrags identifiziert.

Typ: Zeichenfolge

Status

Dies ist der aktuelle Status des Exportauftrags.

Typ: Zeichenfolge

Zulässige Werte: RUNNING | FAILED | COMPLETED

StatusMessage

Eine Statusmeldung ist eine Zeichenfolge, die für einen Suchauftrag mit dem Status zurückgegeben wird. FAILED, zusammen mit Schritten zur Behebung und zum erneuten Versuch des Vorgangs.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und versuchen Sie dann erneut, die Anfrage zu starten.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListSearchJobBackups

Service: AWS Backup

Dieser Vorgang gibt eine Liste aller Backups (Wiederherstellungspunkte) in einem paginierten Format zurück, die im Suchauftrag enthalten waren.

Wenn bei einer Suche kein erwartetes Backup in den Ergebnissen angezeigt wird, können Sie diesen Vorgang aufrufen, um alle in der Suche enthaltenen Backups anzuzeigen. Alle Backups, die nicht aufgenommen wurden, weil sie aufgrund eines Berechtigungsproblems einen FAILED Status haben, werden zusammen mit einer Statusmeldung angezeigt.

Nur Wiederherstellungspunkte mit einem Backup-Index mit dem Status von ACTIVE werden in die Suchergebnisse aufgenommen. Wenn der Index einen anderen Status hat, wird sein Status zusammen mit einer Statusmeldung angezeigt.

Anforderungssyntax

```
GET /search-jobs/SearchJobIdentifier/backups?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

Der nächste Eintrag folgt auf eine unvollständige Liste der zurückgegebenen Backups, die in einem Suchauftrag enthalten waren.

Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Backups gestellt wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token zeigt.

SearchJobIdentifier

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "BackupCreationTime": number,
      "BackupResourceArn": "string",
      "IndexCreationTime": number,
      "ResourceType": "string",
      "SourceResourceArn": "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

Das nächste Element, das auf eine unvollständige Liste der zurückgegebenen Backups folgt, die in einem Suchauftrag enthalten sind.

Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Backups gestellt wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token zeigt.

Typ: Zeichenfolge

Results

Die Wiederherstellungspunkte haben die Ergebnisse eines Suchauftrags zurückgegeben

Typ: Array von [SearchJobBackupsResult](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListSearchJobResults

Service: AWS Backup

Dieser Vorgang gibt eine Liste eines angegebenen Suchauftrags zurück.

Anforderungssyntax

```
GET /search-jobs/SearchJobIdentifier/search-results?  
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, das auf eine unvollständige Liste der zurückgegebenen Suchauftragsergebnisse folgt.

Wenn beispielsweise eine Anfrage zur Rückgabe der `MaxResults` Anzahl von Suchauftragsergebnissen gestellt wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token zeigt.

SearchJobIdentifier

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "Results": [
    { ... }
  ]
}
```

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](#)

Der nächste Eintrag nach einer unvollständigen Liste von Suchauftragsergebnissen.

Wenn beispielsweise die Rückgabe der `MaxResults` Anzahl von Backups angefordert wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit dem Speicherort, auf den das nächste Token verweist.

Typ: Zeichenfolge

[Results](#)

Die Ergebnisse bestehen entweder aus `EBSResultItem` oder `S3ResultItem`.

Typ: Array von [ResultItem](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Einschränkung der Anforderung nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListSearchJobs

Service: AWS Backup

Dieser Vorgang gibt eine Liste von Suchaufträgen zurück, die zu einem Konto gehören.

Anforderungssyntax

```
GET /search-jobs?MaxResults=MaxResults&NextToken=NextToken&Status=ByStatus HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

[ByStatus](#)

Fügen Sie diesen Parameter hinzu, um die Liste nach dem Status des Suchauftrags zu filtern.

Zulässige Werte: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[MaxResults](#)

Die maximale Anzahl der zurückzugebenden Elemente der Ressourcenliste.

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 1 000.

[NextToken](#)

Das nächste Element, das auf eine unvollständige Liste zurückgegebener Suchaufträge folgt.

Wenn beispielsweise die Rückgabe der `MaxResults` Anzahl von Backups angefordert wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, 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",
```

```
"SearchJobs": [  
  {  
    "CompletionTime": number,  
    "CreationTime": number,  
    "Name": "string",  
    "SearchJobArn": "string",  
    "SearchJobIdentifier": "string",  
    "SearchScopeSummary": {  
      "TotalItemsToScanCount": number,  
      "TotalRecoveryPointsToScanCount": number  
    },  
    "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](#)

Das nächste Element, das auf eine unvollständige Liste zurückgegebener Backups folgt, die in einem Suchauftrag enthalten waren.

Wenn beispielsweise die Rückgabe der `MaxResults` Anzahl von Backups angefordert wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token zeigt.

Typ: Zeichenfolge

[SearchJobs](#)

Die Suchaufträge in der Liste, mit Details zu den zurückgegebenen Suchaufträgen.

Typ: Array von [SearchJobSummary](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListSearchResultExportJobs

Service: AWS Backup

Dieser Vorgang exportiert die Suchergebnisse eines Suchauftrags in einen angegebenen Ziel-S3-Bucket.

Anforderungssyntax

```
GET /export-search-jobs?  
MaxResults=MaxResults&NextToken=NextToken&SearchJobIdentifier=SearchJobIdentifier&Status=Status  
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

Der nächste Eintrag folgt auf eine unvollständige Liste der zurückgegebenen Backups, die in einem Suchauftrag enthalten sind.

Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Backups gestellt wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit der Position, auf die das nächste Token zeigt.

SearchJobIdentifier

Die eindeutige Zeichenfolge, die den Suchauftrag angibt.

Status

Die Suchaufträge, die in den Exportauftrag aufgenommen werden sollen, können mithilfe dieses Parameters gefiltert werden.

Zulässige Werte: `RUNNING` | `FAILED` | `COMPLETED`

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "ExportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ExportJobArn": "string",
      "ExportJobIdentifier": "string",
      "SearchJobArn": "string",
      "Status": "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.

[ExportJobs](#)

Der Vorgang gibt die enthaltenen Exportaufträge zurück.

Typ: Array von [ExportJobSummary](#)-Objekten

[NextToken](#)

Der nächste Eintrag folgt auf eine unvollständige Liste der zurückgegebenen Backups, die in einem Suchauftrag enthalten sind.

Wenn beispielsweise eine Anforderung zur Rückgabe der `MaxResults` Anzahl von Backups gestellt wird, `NextToken` können Sie mehr Elemente in Ihrer Liste zurückgeben, beginnend mit 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](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ServiceQuotaExceededException

Die Anfrage wurde aufgrund der Überschreitung der zulässigen Kontingentgrenzen abgelehnt.
message

Diese Anfrage war nicht erfolgreich, da ein Dienstkontingent die Grenzwerte überschritten hat.

quotaCode

Dies ist der Code, der für den Kontingenttyp spezifisch ist.

resourceId

Kennung der Ressource.

resourceType

Typ der Ressource.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

HTTP-Statuscode: 402

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.
message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListTagsForResource

Service: AWS Backup

Diese Operation gibt die Tags für einen Ressourcentyp zurück.

Anforderungssyntax

```
GET /tags/ResourceArn HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ResourceArn

Der Amazon-Ressourcenname (ARN), der die Ressource eindeutig identifiziert. >

Erforderlich: Ja

Anforderungstext

Der Anforderung besitzt keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "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.

Tags

Liste der von der Operation zurückgegebenen 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](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

StartSearchJob

Service: AWS Backup

Dieser Vorgang erstellt einen Suchauftrag, der Wiederherstellungspunkte, gefiltert nach, SearchScope und Elemente, nach denen gefiltert wurde, zurückgibt ItemFilters.

Sie können optional ClientToken, EncryptionKeyArn, Name und and/or Tags angeben.

Anforderungssyntax

```
PUT /search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "FilePaths": [
          {
            "Operator": "string",
            "Value": "string"
          }
        ],
        "LastModificationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "Sizes": [
          {
            "Operator": "string",
            "Value": number
          }
        ]
      }
    ]
  }
}
```

```

    }
  ],
  "S3ItemFilters": [
    {
      "CreationTimes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "ETags": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "ObjectKeys": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "Sizes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "VersionIds": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ]
    }
  ]
},
"Name": "string",
"SearchScope": {
  "BackupResourceArns": [ "string" ],
  "BackupResourceCreationTime": {
    "CreatedAfter": number,
    "CreatedBefore": number
  }
},

```



```
"BackupResourceTags": {
  "string" : "string"
},
"BackupResourceTypes": [ "string" ],
"SourceResourceArns": [ "string" ]
},
"Tags": {
  "string" : "string"
}
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ClientToken

Fügen Sie diesen Parameter hinzu, um mehrere identische Aufrufe für Idempotenz zuzulassen.

Ein Client-Token ist 8 Stunden lang gültig, nachdem die erste Anfrage, die es verwendet, abgeschlossen wurde. Nach Ablauf dieser Zeit wird jede Anfrage mit demselben Token als neue Anfrage behandelt.

Typ: Zeichenfolge

Erforderlich: Nein

EncryptionKeyArn

Der Verschlüsselungsschlüssel für den angegebenen Suchauftrag.

Typ: Zeichenfolge

Erforderlich: Nein

ItemFilters

Elementfilter stellen alle Eigenschaften des Eingabeelements dar, die bei der Erstellung der Suche angegeben wurden.

Enthält entweder EBSItem Filter oder S3 ItemFilters

Typ: [ItemFilters](#) Objekt

Erforderlich: Nein

Name

Fügen Sie alphanumerische Zeichen ein, um einen Namen für diesen Suchauftrag zu erstellen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 500 Zeichen.

Erforderlich: Nein

SearchScope

Dieses Objekt kann BackupResourceTypes,, BackupResourceArns, und enthalten BackupResourceCreationTime BackupResourceTags, SourceResourceArns um die vom Suchauftrag zurückgegebenen Wiederherstellungspunkte zu filtern.

Typ: [SearchScope](#) Objekt

Erforderlich: Ja

Tags

Liste der von der Operation zurückgegebenen Tags.

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "SearchJobArn": "string",
  "SearchJobIdentifier": "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](#)

Datum und Uhrzeit der Erstellung eines Jobs im Unix-Format und in koordinierter 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

[SearchJobArn](#)

Die eindeutige Zeichenfolge, die den Amazon-Ressourcennamen (ARN) des angegebenen Suchauftrags identifiziert.

Typ: Zeichenfolge

[SearchJobIdentifier](#)

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

ConflictException

Diese Ausnahme tritt auf, wenn ein Konflikt mit einem vorherigen erfolgreichen Vorgang erkannt wird. Dies tritt im Allgemeinen auf, wenn der vorherige Vorgang keine Zeit hatte, sich an den Host zu übertragen, der die aktuelle Anforderung bedient.

Ein erneuter Versuch (mit entsprechender Backoff-Logik) ist die empfohlene Reaktion auf diese Ausnahme.

message

Das Aktualisieren oder Löschen einer Ressource kann zu einem inkonsistenten Zustand führen.

resourceId

Kennung der betroffenen Ressource.

resourceType

Typ der betroffenen Ressource.

HTTP-Statuscode: 409

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ServiceQuotaExceededException

Die Anfrage wurde aufgrund der Überschreitung der zulässigen Kontingentgrenzen abgelehnt.

message

Diese Anfrage war nicht erfolgreich, da ein Dienstkontingent die Grenzwerte überschritten hat.

quotaCode

Dies ist der Code, der für den Kontingenttyp spezifisch ist.

resourceId

Kennung der Ressource.

resourceType

Typ der Ressource.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

HTTP-Statuscode: 402

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

StartSearchResultExportJob

Service: AWS Backup

Dieser Vorgang startet einen Job, um die Ergebnisse des Suchauftrags in einen bestimmten S3-Bucket zu exportieren.

Anforderungssyntax

```
PUT /export-search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "ExportSpecification": { ... },
  "RoleArn": "string",
  "SearchJobIdentifier": "string",
  "Tags": {
    "string" : "string"
  }
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

ClientToken

Fügen Sie diesen Parameter hinzu, um mehrere identische Aufrufe zur Feststellung von Idempotenz zu ermöglichen.

Ein Client-Token ist 8 Stunden lang gültig, nachdem die erste Anfrage, die es verwendet, abgeschlossen wurde. Nach Ablauf dieser Zeit wird jede Anfrage mit demselben Token als neue Anfrage behandelt.

Typ: Zeichenfolge

Erforderlich: Nein

[ExportSpecification](#)

Diese Spezifikation enthält eine erforderliche Zeichenfolge des Ziel-Buckets. Optional können Sie das Zielpräfix angeben.

Typ: [ExportSpecification](#) Objekt

Hinweis: Dieses Objekt ist eine Union. Nur ein Mitglied dieses Objekts kann angegeben oder zurückgegeben werden.

Erforderlich: Ja

[RoleArn](#)

Dieser Parameter gibt den Rollen-ARN an, der zum Starten der Exportaufträge für Suchergebnisse verwendet wird.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 20. Maximale Länge beträgt 2048 Zeichen.

Pattern: `arn:(?:aws|aws-cn|aws-us-gov):iam::[a-z0-9-]+:role/(.+)`

Erforderlich: Nein

[SearchJobIdentifier](#)

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Typ: Zeichenfolge

Erforderlich: Ja

[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

Antwortsyntax

HTTP/1.1 200


```
Content-type: application/json

{
  "ExportJobArn": "string",
  "ExportJobIdentifier": "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.

[ExportJobArn](#)

Dies ist der eindeutige ARN (Amazon Resource Name), der zu dem neuen Exportauftrag gehört.

Typ: Zeichenfolge

[ExportJobIdentifier](#)

Dies ist die eindeutige Kennung, die den neuen Exportauftrag spezifiziert.

Typ: Zeichenfolge

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

ConflictException

Diese Ausnahme tritt auf, wenn ein Konflikt mit einem vorherigen erfolgreichen Vorgang erkannt wird. Dies tritt im Allgemeinen auf, wenn der vorherige Vorgang keine Zeit hatte, sich an den Host zu übertragen, der die aktuelle Anforderung bedient.

Ein erneuter Versuch (mit entsprechender Backoff-Logik) ist die empfohlene Reaktion auf diese Ausnahme.

message

Das Aktualisieren oder Löschen einer Ressource kann zu einem inkonsistenten Zustand führen.

resourceId

Kennung der betroffenen Ressource.

resourceType

Typ der betroffenen Ressource.

HTTP-Statuscode: 409

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ServiceQuotaExceededException

Die Anfrage wurde aufgrund der Überschreitung der zulässigen Kontingentgrenzen abgelehnt.

message

Diese Anfrage war nicht erfolgreich, da ein Dienstkontingent die Grenzwerte überschritten hat.

quotaCode

Dies ist der Code, der für den Kontingenttyp spezifisch ist.

resourceId

Kennung der Ressource.

resourceType

Typ der Ressource.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

HTTP-Statuscode: 402

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

StopSearchJob

Service: AWS Backup

Dieser Vorgang beendet einen Suchauftrag.

Nur ein Suchauftrag mit dem Status von RUNNING kann gestoppt werden.

Anforderungssyntax

```
PUT /search-jobs/SearchJobIdentifier/actions/cancel HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

SearchJobIdentifier

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

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](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

ConflictException

Diese Ausnahme tritt auf, wenn ein Konflikt mit einem vorherigen erfolgreichen Vorgang erkannt wird. Dies tritt im Allgemeinen auf, wenn der vorherige Vorgang keine Zeit hatte, sich an den Host zu übertragen, der die aktuelle Anforderung bedient.

Ein erneuter Versuch (mit entsprechender Backoff-Logik) ist die empfohlene Reaktion auf diese Ausnahme.

message

Das Aktualisieren oder Löschen einer Ressource kann zu einem inkonsistenten Zustand führen.

resourceId

Kennung der betroffenen Ressource.

resourceType

Typ der betroffenen Ressource.

HTTP-Statuscode: 409

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

TagResource

Service: AWS Backup

Bei diesem Vorgang werden der von Ihnen angegebenen Ressource Tags zugewiesen.

Anforderungssyntax

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json
```

```
{
  "Tags": {
    "string" : "string"
  }
}
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ResourceArn

Der Amazon-Ressourcenname (ARN), der die Ressource eindeutig identifiziert.

Dies ist die Ressource, die die angegebenen Tags haben wird.

Erforderlich: Ja

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Tags

Erforderliche Tags, die aufgenommen werden müssen. 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: 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](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und versuchen Sie dann erneut, die Anfrage zu starten.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [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 für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UntagResource

Service: AWS Backup

Dieser Vorgang entfernt Tags aus der angegebenen Ressource.

Anforderungssyntax

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

URI-Anfrageparameter

Die Anforderung verwendet die folgenden URI-Parameter.

ResourceArn

Der Amazon-Ressourcenname (ARN), der die Ressource, von der Sie Tags entfernen möchten, eindeutig identifiziert.

Erforderlich: Ja

TagKeys

Dieser erforderliche Parameter enthält die Tag-Schlüssel, die Sie aus der Quelle entfernen möchten.

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](#).

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

message

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP Status Code: 403

InternalServerErrorException

Es ist ein interner Serverfehler aufgetreten. Wiederholen Sie Ihre Anforderung.

message

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

HTTP Status Code: 500

ResourceNotFoundException

Die Ressource wurde für diese Anfrage nicht gefunden.

Vergewissern Sie sich, dass die Ressourceninformationen, wie z. B. der ARN oder der Typ, korrekt und vorhanden sind, und wiederholen Sie dann die Anfrage.

message

Die Anfrage verweist auf eine Ressource, die nicht existiert.

resourceId

Hypothetischer Identifier der betroffenen Ressource.

resourceType

Hypothetischer Typ der betroffenen Ressource.

HTTP Status Code: 404

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

message

Die Anfrage war aufgrund der Drosselung der Anfrage nicht erfolgreich.

quotaCode

Dies ist der eindeutige Code für den ursprünglichen Dienst mit dem Kontingent.

retryAfterSeconds

Versuchen Sie den Anruf nach einigen Sekunden erneut.

serviceCode

Dies ist der eindeutige Code für den ursprünglichen Dienst.

HTTP-Statuscode: 429

ValidationException

Die Eingabe erfüllt nicht die von einem Dienst angegebenen Einschränkungen.

message

Die Eingabe erfüllt nicht die von einem Amazon-Service angegebenen Einschränkungen.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [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 für Kotlin](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

Datentypen

Die folgenden Datentypen werden unterstützt von AWS Backup:

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)
- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)
- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)

- [Framework](#)
- [FrameworkControl](#)
- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)
- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)
- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)

- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)
- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)
- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)
- [TieringConfigurationsListMember](#)

Die folgenden Datentypen werden unterstützt von AWS Backup gateway:

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)
- [VmwareToAwsTagMapping](#)

Die folgenden Datentypen werden unterstützt von AWS Backup:

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)
- [SearchScopeSummary](#)
- [StringCondition](#)
- [TimeCondition](#)

AWS Backup

Die folgenden Datentypen werden unterstützt von AWS Backup:

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)

- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)
- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)
- [Framework](#)
- [FrameworkControl](#)
- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)

- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)
- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)
- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)
- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)

- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)
- [TieringConfigurationsListMember](#)

AdvancedBackupSetting

Service: AWS Backup

Die Backup-Optionen für jeden Ressourcentyp.

Inhalt

BackupOptions

Gibt die Backup-Option für eine ausgewählte Ressource an. Diese Option ist für Windows VSS-Backup-Jobs und S3-Backups 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.

Legen Sie für S3-Backups fest, ob ACLs von der Sicherung ausgeschlossen oder "S3BackupObjectTags": "disabled" Objekt-Tags von der Sicherung ausgeschlossen werden sollen. "S3BackupACLs": "disabled" Standardmäßig sind ACLs sowohl Objekt-Tags als auch Objekt-Tags in S3-Backups enthalten.

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 EC2 Amazon-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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AggregatedScanResult

Service: AWS Backup

Enthält aggregierte Scanergebnisse aus mehreren Scanvorgängen und bietet eine Zusammenfassung des Scanstatus und der Ergebnisse.

Inhalt

FailedScan

Ein boolescher Wert, der angibt, ob einer der aggregierten Scans fehlgeschlagen ist.

Typ: Boolesch

Erforderlich: Nein

Findings

Eine Reihe von Ergebnissen, die bei allen aggregierten Scans entdeckt wurden.

Typ: Zeichenfolgen-Array

Zulässige Werte: MALWARE

Erforderlich: Nein

LastComputed

Der Zeitstempel, zu dem das aggregierte Scanergebnis zuletzt berechnet wurde, im Unix-Format und in koordinierter Weltzeit (UTC).

Typ: Zeitstempel

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen 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 (Wiederherstellungspunkts) in Byte.

Dieser Wert kann je nach Ressourcentyp unterschiedlich dargestellt werden, AWS Backup da Dateninformationen von anderen AWS Diensten abgerufen werden. Beispielsweise kann der zurückgegebene Wert einen Wert von aufweisen `0`, der vom erwarteten Wert abweichen kann.

Das erwartete Verhalten von Werten nach Ressourcentyp wird wie folgt beschrieben:

- Bei Amazon Aurora, Amazon DocumentDB und Amazon Neptune wird dieser Wert nicht aus dem Vorgang übernommen. `GetBackupJobStatus`
- Bei Amazon DynamoDB mit erweiterten Funktionen bezieht sich dieser Wert auf die Größe des Wiederherstellungspunkts (Backup).
- Amazon EC2 und Amazon EBS zeigen die als Teil dieses Werts zurückgegebene Volumengröße (bereitgestellter Speicher) an. Amazon EBS gibt keine Informationen zur Backup-Größe zurück. Die Snapshot-Größe hat denselben Wert wie die ursprüngliche Ressource, die gesichert wurde.
- Für Amazon EFS bezieht sich dieser Wert auf die Delta-Bytes, die während einer Sicherung übertragen wurden.
- Amazon FSx füllt diesen Wert nicht aus dem Vorgang `GetBackupJobStatus` für FSx Dateisysteme auf.
- Eine Amazon RDS-Instance wird als `angezeigt0`.
- Bei laufenden VMware virtuellen Maschinen wird dieser Wert AWS Backup über einen asynchronen Workflow weitergegeben, was bedeuten kann, dass dieser angezeigte Wert die tatsächliche Backup-Größe unterrepräsentiert.

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

EncryptionKeyArn

Der Amazon-Ressourcenname (ARN) des KMS-Schlüssels, der zur Verschlüsselung des Backups verwendet wurde. Dies kann je nach Tresorkonfiguration ein vom Kunden AWS verwalteter Schlüssel oder ein verwalteter Schlüssel sein.

Typ: Zeichenfolge

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. Beispiel, `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

IsEncrypted

Ein boolescher Wert, der angibt, ob das Backup verschlüsselt ist. Alle Backups in AWS Backup sind verschlüsselt, aber dieses Feld gibt aus Gründen der Transparenz den Verschlüsselungsstatus an.

Typ: Boolesch

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

RecoveryPointLifecycle

Gibt den Zeitraum in Tagen an, bevor ein Erholungspunkt in einen Cold Storage übergeht oder gelöscht wird.

In den Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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

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 gesichert werden soll, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) - Datenbank. Für Windows Volume Shadow Copy Service (VSS) -Backups ist Amazon EC2 der einzige unterstützte Ressourcentyp.

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

VaultLockState

Der Sperrstatus des Backup-Tresors. Bei Tresoren mit logischem Air-Gap gibt dies an, ob der Tresor im Compliance-Modus gesperrt ist. Gültige Werte sind `LOCKED` und `UNLOCKED`.

Typ: Zeichenfolge

Erforderlich: Nein

VaultType

Der Typ des Backup-Tresors, in dem der Recovery Point gespeichert ist. Gültige Werte gelten `BACKUP_VAULT` für standardmäßige Backup-Tresore und `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` für Tresore mit logischem Air-Gap.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BackupJobSummary

Bedienung: AWS Backup

Dies ist eine Zusammenfassung der Aufträge, die in den letzten 30 Tagen erstellt oder ausgeführt wurden.

Die zurückgesendete 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

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenategorie 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 einer der sprachspezifischen Sprachen 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. Darf nur alphanumerische Zeichen oder '-' '_' enthalten. Sonderzeichen.

Wenn dies in der Konsole festgelegt ist, kann es 1 bis 50 Zeichen enthalten. Wenn dies über CLI oder API festgelegt ist, kann es 1 bis 200 Zeichen enthalten.

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

ScanSettings

Enthält Ihre Scankonfiguration für den Backup-Plan und umfasst den Malware-Scanner, Ihre ausgewählten Ressourcen und die Scannerrolle.

Typ: Array von [ScanSetting](#)-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen 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

ScanSettings

Enthält Ihre Scankonfiguration für die Backup-Regel und umfasst den Malware-Scanner sowie den Scanmodus „Vollständig“ oder „Inkrementell“.

Typ: Array von [ScanSetting](#)-Objekten

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BackupPlansListMember

Bedienung: 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. Die Version IDs kann nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BackupPlanTemplatesListMember

Bedienung: 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 einer der sprachspezifischen Sprachen 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

IndexActions

IndexActions ist ein Array, mit dem Sie angeben, wie Backup-Daten indexiert werden sollen.

Jedes Backup BackupRule kann 0 oder 1 haben IndexAction, da jedem Backup bis zu einem Index zugeordnet sein kann.

Innerhalb des Arrays ist ResourceType. Für jeden wird nur einer akzeptiert BackupRule.

Typ: Array von [IndexAction](#)-Objekten

Erforderlich: Nein

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 Archivspeicher übertragene Backups 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 mehr geändert werden, nachdem ein Backup 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

ScanActions

Enthält Ihre Scankonfiguration für die Backup-Regel und umfasst den Malware-Scanner sowie den Scanmodus „Vollständig“ oder „Inkrementell“.

Typ: Array von [ScanAction](#)-Objekten

Erforderlich: Nein

ScheduleExpression

Ein Cron-Ausdruck in UTC, der angibt, wann ein AWS Backup Backup-Job initiiert wird. Wenn kein CRON-Ausdruck angegeben wird, AWS Backup wird der Standardausdruck verwendet.

`cron(0 5 ? * * *)`

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 aufRUNNING) oder bis sich der Jobstatus auf ändert EXPIRED (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Type: Long

Erforderlich: Nein

TargetLogicallyAirGappedBackupVaultArn

Der ARN eines Tresors mit logischem Air-Gap. ARN muss sich im selben Konto und in derselben Region befinden. Falls verfügbar, werden unterstützte, vollständig verwaltete Ressourcen direkt in einem Tresor mit logischem Air-Gap gesichert, während andere unterstützte Ressourcen einen temporären (kostenpflichtigen) Snapshot im Backup-Tresor erstellen und ihn dann in den Tresor mit logischem Air-Gap kopieren. Nicht unterstützte Ressourcen werden nur im angegebenen Backup-Tresor gesichert.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs 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

IndexActions

IndexAction In jedem Backup kann es bis zu einen geben BackupRule, da jedem Backup 0 oder 1 Backup-Index zugeordnet sein kann.

Innerhalb des Arrays befindet sich ResourceTypes. Für jeden wird nur ein Ressourcentyp akzeptiert BackupRule. Zulässige Werte:

- EBS für Amazon Elastic Block Store
- S3 für Amazon Simple Storage Service (Amazon S3)

Typ: Array von [IndexAction](#)-Objekten

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 Archivspeicher übertragene Backups 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 „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

ScanActions

Enthält Ihre Scankonfiguration für die Backup-Regel und umfasst den Malware-Scanner sowie den Scanmodus „Vollständig“ oder „Inkrementell“.

Typ: Array von [ScanAction](#)-Objekten

Erforderlich: Nein

ScheduleExpression

Ein CRON-Ausdruck in UTC, der angibt, wann ein AWS Backup Backup-Job initiiert wird. Wenn kein CRON-Ausdruck angegeben wird, AWS Backup wird der Standardausdruck verwendet.

```
cron(0 5 ? * * *)
```

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 aufRUNNING) oder bis sich der Jobstatus auf ändert EXPIRED (was voraussichtlich nach Ablauf der Startzeit der Fall sein wird).

Type: Long

Erforderlich: Nein

TargetLogicallyAirGappedBackupVaultArn

Der ARN eines Tresors mit logischem Air-Gap. Der ARN muss sich im selben Konto und in derselben Region befinden. Falls verfügbar, werden unterstützte, vollständig verwaltete Ressourcen direkt in einem Tresor mit logischem Air-Gap gesichert, während andere unterstützte Ressourcen einen temporären (kostenpflichtigen) Snapshot im Backup-Tresor erstellen und ihn dann in den Tresor mit logischem Air-Gap kopieren. Nicht unterstützte Ressourcen werden nur im angegebenen Backup-Tresor gesichert.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BackupSelection

Bedienung: 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. Beispiel, `"StringEquals": { "ConditionKey": "aws:ResourceTag/backup", "ConditionValue": "daily" }`.

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

Es wird empfohlen, den Conditions Parameter anstelle dieses Parameters zu verwenden.

Die Bedingungen, die Sie definieren, um Ihren Backup-Plänen mithilfe von Tags Ressourcen zuzuweisen. Beispiel, "StringEquals": { "ConditionKey": "backup", "ConditionValue": "daily"}.

ListOfTags unterstützt nur StringEquals. Bei Bedingungsoperatoren wird zwischen Groß- und Kleinschreibung unterschieden.

Wenn Sie mehrere Bedingungen angeben, entsprechen die Ressourcen weitgehend allen 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 ist 500 ohne Platzhalter 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 ist 500 ohne Platzhalter 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 angeben ARNs, stimmen die Ressourcen weitgehend mit der ARNs (OR-Logik) überein.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BackupSelectionsListMember

Bedienung: 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 einer der sprachspezifischen Sprachen 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

EncryptionKeyType

Der Typ des Verschlüsselungsschlüssels, der für den Backup-Tresor verwendet wird. Gültige Werte sind `CUSTOMER_MANAGED_KMS_KEY` für vom Kunden verwaltete Schlüssel oder `_OWNED_KMS_KEY` für Schlüssel, die dem Kunden gehören. AWS AWS

Typ: Zeichenfolge

Zulässige Werte: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Erforderlich: Nein

LockDate

Datum und Uhrzeit, an dem die Vault Lock-Konfiguration unveränderlich wird, d. h. sie kann nicht geändert oder gelöscht werden. AWS Backup

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

VaultState

Der aktuelle Status des Tresors.

Typ: Zeichenfolge

Zulässige Werte: CREATING | AVAILABLE | FAILED

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 |
RESTORE_ACCESS_BACKUP_VAULT

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CalculatedLifecycle

Bedienung: 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 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.

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Condition

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ConditionParameter

Bedienung: 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. Beispiel, `"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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Conditions

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ControllInputParameter

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ControlScope

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CopyAction

Bedienung: 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 Erholungspunkt in einen Kaltspeicher 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

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs 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

CreatedByBackupJobId

Die ID des Sicherungsauftrags, der diesen Kopierauftrag initiiert hat. Gilt nur für geplante Kopieraufträge und automatische Kopieraufträge in einen Tresor mit logischem Air-Gap.

Typ: Zeichenfolge

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

DestinationEncryptionKeyArn

Der Amazon-Ressourcenname (ARN) des KMS-Schlüssels, der zur Verschlüsselung des kopierten Backups im Zieltresor verwendet wurde. Dabei kann es sich um einen vom Kunden verwalteten Schlüssel oder um einen AWS verwalteten Schlüssel handeln.

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

DestinationRecoveryPointLifecycle

Gibt den Zeitraum in Tagen an, bevor ein Wiederherstellungspunkt in einen Cold Storage übergeht oder gelöscht wird.

In den Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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

`DestinationVaultLockState`

Der Sperrstatus des Ziel-Backup-Tresors. Bei Tresoren mit logischem Air-Gap gibt dies an, ob der Tresor im Compliance-Modus gesperrt ist. Gültige Werte sind `LOCKED` und `UNLOCKED`.

Typ: Zeichenfolge

Erforderlich: Nein

`DestinationVaultType`

Der Typ des Ziel-Backup-Tresors, in dem der kopierte Recovery Point gespeichert ist. Gültige Werte gelten `BACKUP_VAULT` für Standard-Backup-Tresore und `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` für Tresore mit logischem Air-Gap.

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 [Zeichenketten finden Sie unter Überwachung](#).

MessageCategory

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 einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [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, 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

MessageCategory

Dieser Parameter gibt die Anzahl der Aufträge für die angegebene Nachrichtenategorie 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DateRange

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Framework

Bedienung: 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 2020-07-10T15:00:00.000-08:00 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FrameworkControl

Bedienung: 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 Geltungsbereichen für Steuerung 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 einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

IndexAction

Bedienung: AWS Backup

Dies ist ein optionales Array innerhalb eines BackupRule.

IndexAction besteht aus einem ResourceTypes.

Inhalt

ResourceTypes

0 oder 1 Indexaktion wird für jede Aktion akzeptiert BackupRule.

Zulässige Werte:

- EBS für Amazon Elastic Block Store
- S3 für Amazon Simple Storage Service (Amazon S3)

Typ: Zeichenfolgen-Array

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IndexedRecoveryPoint

Bedienung: AWS Backup

Dies ist ein Wiederherstellungspunkt, dem ein Backup-Index zugeordnet ist.

Nur Wiederherstellungspunkte mit einem Backup-Index können in eine Suche einbezogen werden.

Inhalt

BackupCreationDate

Datum und Uhrzeit der Erstellung eines Backups im Unix-Format und in koordinierter 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

BackupVaultArn

Ein ARN, der den Backup-Tresor, in dem der Wiederherstellungspunktindex gespeichert ist, eindeutig identifiziert.

Beispiel, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Typ: Zeichenfolge

Erforderlich: Nein

IamRoleArn

Dies gibt den ARN der IAM-Rolle an, der für diesen Vorgang verwendet wird.

Zum Beispiel `arn:aws:iam: :123456789012:role/S3Access`

Typ: Zeichenfolge

Erforderlich: Nein

IndexCreationDate

Datum und Uhrzeit der Erstellung eines Backup-Index im Unix-Format und in koordinierter 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

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: PENDING | ACTIVE | FAILED | DELETING

Ein Wiederherstellungspunkt mit einem Index, der den Status von hat, ACTIVE kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: PENDING | ACTIVE | FAILED | DELETING

Erforderlich: Nein

IndexStatusMessage

Eine Zeichenfolge in Form einer ausführlichen Meldung, die den Status eines Backup-Indexes erklärt, der dem Erholungspunkt zugeordnet ist.

Typ: Zeichenfolge

Erforderlich: Nein

RecoveryPointArn

Ein ARN, das einen Wiederherstellungspunkt eindeutig identifiziert; zum Beispiel
`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der Ressourcentyp des indizierten Wiederherstellungspunkts.

- EBS für Amazon Elastic Block Store
- S3 für Amazon Simple Storage Service (Amazon S3)

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

SourceResourceArn

Eine Zeichenfolge mit dem Amazon-Ressourcennamen (ARN), der die Quellressource eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

KeyValue

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LatestMpaApprovalTeamUpdate

Service: AWS Backup

Enthält Informationen über das neueste Update einer Vereinigung von MPA-Genehmigungsteams.

Inhalt

ExpiryDate

Datum und Uhrzeit, zu dem das Update des MPA-Genehmigungsteams abläuft.

Typ: Zeitstempel

Erforderlich: Nein

InitiationDate

Datum und Uhrzeit, an dem das Update des MPA-Genehmigungsteams eingeleitet wurde.

Typ: Zeitstempel

Erforderlich: Nein

MpaSessionArn

Der ARN der MPA-Sitzung, die mit diesem Update verknüpft ist.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Der aktuelle Status der Aktualisierung des MPA-Genehmigungsteams.

Typ: Zeichenfolge

Zulässige Werte: PENDING | APPROVED | FAILED

Erforderlich: Nein

StatusMessage

Eine Nachricht, die den aktuellen Status der Aktualisierung des MPA-Genehmigungsteams beschreibt.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LatestRevokeRequest

Service: AWS Backup

Enthält Informationen über die letzte Anfrage zum Widerruf des Zugriffs auf einen Backup-Tresor.

Inhalt

ExpiryDate

Datum und Uhrzeit, zu dem die Widerrufsanzforderung abläuft.

Typ: Zeitstempel

Erforderlich: Nein

InitiationDate

Datum und Uhrzeit der Initiierung der Widerrufsanzforderung.

Typ: Zeitstempel

Erforderlich: Nein

MpaSessionArn

Der ARN der MPA-Sitzung, die dieser Widerrufsanzforderung zugeordnet ist.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Der aktuelle Status der Widerrufsanzforderung.

Typ: Zeichenfolge

Zulässige Werte: PENDING | FAILED

Erforderlich: Nein

StatusMessage

Eine Nachricht, die den aktuellen Status der Widerrufsanzforderung beschreibt.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LegalHold

Bedienung: 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 gefiltert werden IDs.

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 gesetzlich vorgeschriebenen Speichers, zum Beispiel `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 einer der sprachspezifischen Sprachen 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 Archivspeicher übertragene Backups müssen mindestens 90 Tage lang im Archivspeicher 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`

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

`DeleteAfterEvent`

Das Ereignis, nach dem ein Erholungspunkt gelöscht wird. Ein Wiederherstellungspunkt mit beiden `DeleteAfterDays` und `DeleteAfterEvent` wird gelöscht, je nachdem, welche Bedingung zuerst erfüllt ist. Als Eingabe nicht gültig.

Typ: Zeichenfolge

Zulässige Werte: `DELETE_AFTER_COPY`

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ProtectedResource

Bedienung: 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 Volume Shadow Copy Service (VSS) -Backups ist Amazon EC2 der einzige unterstützte Ressourcentyp.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ProtectedResourceConditions

Bedienung: AWS Backup

Die Bedingungen, die Sie für Ressourcen in Ihrem Wiederherstellungstestplan mithilfe von Tags definieren.

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 einer der sprachspezifischen Sprachen 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

AggregatedScanResult

Enthält die neuesten Scanergebnisse anhand des Wiederherstellungspunkts und umfasst `derzeitFailedScan`, `Findings`, `LastComputed`.

Typ: [AggregatedScanResult](#) Objekt

Erforderlich: Nein

BackupSizeInBytes

Die Größe eines Backups in Byte

Typ: 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

Die ID einer Ressource innerhalb einer zusammengesetzten Gruppe, z. B. eines verschachtelten (untergeordneten) Wiederherstellungspunkts, der zu einem zusammengesetzten (übergeordneten) Stapel 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

EncryptionKeyType

Der Typ des Verschlüsselungsschlüssels, der für den Erholungspunkt verwendet wird. Gültige Werte sind `CUSTOMER_MANAGED_KMS_KEY` für vom Kunden verwaltete Schlüssel oder `_OWNED_KMS_KEY` für Schlüssel, die dem Kunden gehören. AWS AWS

Typ: Zeichenfolge

Zulässige Werte: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

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

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Ein Wiederherstellungspunkt mit einem Index, der den Status von `PENDING` hat, `ACTIVE` kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: PENDING | ACTIVE | FAILED | DELETING

Erforderlich: Nein

IndexStatusMessage

Eine Zeichenfolge in Form einer ausführlichen Meldung, die den Status eines Backup-Indexes erklärt, der dem Erholungspunkt zugeordnet ist.

Typ: Zeichenfolge

Erforderlich: Nein

InitiationDate

Datum und Uhrzeit der Initiierung des Sicherungsauftrags, mit dem dieser Wiederherstellungspunkt erstellt wurde, im Unix-Format und in koordinierter Weltzeit (UTC).

Typ: Zeitstempel

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 Archivspeicher übertragene Backups 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 mehr geändert werden, nachdem ein Backup 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 Volume Shadow Copy Service (VSS) -Backups ist Amazon EC2 der einzige unterstützte Ressourcentyp.

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 | AVAILABLE | STOPPED | CREATING

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 | RESTORE_ACCESS_BACKUP_VAULT

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen 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

AggregatedScanResult

Enthält die neuesten Scanergebnisse anhand des Wiederherstellungspunkts und umfasst derzeitFailedScan,Findings,LastComputed.

Typ: [AggregatedScanResult](#) Objekt

Erforderlich: Nein

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

EncryptionKeyType

Der Typ des Verschlüsselungsschlüssels, der für den Erholungspunkt verwendet wird. Gültige Werte sind `CUSTOMER_MANAGED_KMS_KEY` für vom Kunden verwaltete Schlüssel oder `_OWNED_KMS_KEY` für Schlüssel, die dem Kunden gehören. AWS AWS

Typ: Zeichenfolge

Zulässige Werte: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Erforderlich: Nein

IndexStatus

Dies ist der aktuelle Status für den Backup-Index, der dem angegebenen Wiederherstellungspunkt zugeordnet ist.

Die Status sind: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Ein Wiederherstellungspunkt mit einem Index, der den Status von `ACTIVE` hat, kann in eine Suche aufgenommen werden.

Typ: Zeichenfolge

Zulässige Werte: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Erforderlich: Nein

IndexStatusMessage

Eine Zeichenfolge in Form einer ausführlichen Meldung, die den Status eines Backup-Indexes erklärt, der dem Erholungspunkt zugeordnet ist.

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 zu dem angegebenen Backup gehört.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Ein Statuscode, der den Status des Wiederherstellungspunkts angibt.

Typ: Zeichenfolge

Zulässige Werte: COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

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 |
RESTORE_ACCESS_BACKUP_VAULT

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen 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

BackupPlanName

Der Name des Backup-Plans, mit dem dieser Wiederherstellungspunkt erstellt wurde. Dies bietet einen für Menschen lesbaren Kontext darüber, welcher Backup-Plan für den Backup-Job verantwortlich war.

Typ: Zeichenfolge

Erforderlich: Nein

BackupPlanVersion

Version IDs sind eindeutige, zufällig generierte, Unicode- und UTF-8-kodierte Zeichenketten, die maximal 1.024 Byte lang sind. Sie können nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Nein

BackupRuleCron

Der Cron-Ausdruck, der den Zeitplan für die Backup-Regel definiert. Dies zeigt die Häufigkeit und den Zeitpunkt an, zu dem Backups automatisch ausgelöst 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

BackupRuleName

Der Name der Backup-Regel innerhalb des Backup-Plans, mit der dieser Wiederherstellungspunkt erstellt wurde. Auf diese Weise können Sie ermitteln, welche spezifische Regel den Backup-Job ausgelöst hat.

Typ: Zeichenfolge

Erforderlich: Nein

BackupRuleTimezone

Die Zeitzone, die für den Zeitplan der Backup-Regel verwendet wurde. Dies bietet einen Kontext dafür, wann Backups in der angegebenen Zeitzone ausgeführt werden sollen.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

RecoveryPointMember

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RecoveryPointSelection

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportDeliveryChannel

Bedienung: 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: CSVJSON, 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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

ReportDestination

Bedienung: 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportJob

Bedienung: 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. Der Berichtsauftrag IDs kann 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportPlan

Bedienung: 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 istCONTROL_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 einer der sprachspezifischen Sprachen 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 |  
SCAN_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 in einem Bericht behandelt werden.

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ResourceSelection

Service: AWS Backup

Dies enthält Metadaten zur Ressourcenauswahl für Tiering-Konfigurationen.

Sie können bis zu 5 verschiedene Ressourcenauswahlen pro Tiering-Konfiguration angeben. Daten, die auf eine kostengünstigere Stufe verschoben wurden, verbleiben dort, bis sie gelöscht werden (unidirektionaler Übergang).

Inhalt

Resources

Ein Zeichenkettenarray, das entweder die zugehörigen Ressourcen oder einen Platzhalter * zur Angabe aller Ressourcen enthält. ARNs Sie können bis zu 100 spezifische Ressourcen pro Tiering-Konfiguration angeben.

Typ: Zeichenfolgen-Array

Erforderlich: Ja

ResourceType

Der AWS Ressourcentyp, zum Beispiel S3 für Amazon S3. Bei Tiering-Konfigurationen ist dies derzeit beschränkt auf S3.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Ja

TieringDownSettingsInDays

Gibt an, wie viele Tage nach der Erstellung in einem Backup-Tresor ein Objekt auf die kostengünstige Warm-Storage-Stufe umgestellt werden kann. Muss eine positive Ganzzahl zwischen 60 und 36500 Tagen sein.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 60. Der Höchstwert ist 36500.

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreAccessBackupVaultListMember

Service: AWS Backup

Enthält Informationen über einen Backup-Tresor mit Wiederherstellungszugriff.

Inhalt

ApprovalDate

Datum und Uhrzeit der Genehmigung des Backup-Tresors mit Wiederherstellungszugriff.

Typ: Zeitstempel

Erforderlich: Nein

CreationDate

Datum und Uhrzeit der Erstellung des Backup-Tresors mit Wiederherstellungszugriff.

Typ: Zeitstempel

Erforderlich: Nein

LatestRevokeRequest

Informationen über die letzte Anfrage zum Widerruf des Zugriffs auf diesen Backup-Tresor.

Typ: [LatestRevokeRequest](#) Objekt

Erforderlich: Nein

RestoreAccessBackupVaultArn

Der ARN des Backup-Tresors mit Wiederherstellungszugriff.

Typ: Zeichenfolge

Erforderlich: Nein

VaultState

Der aktuelle Status des Backup-Tresors mit Wiederherstellungszugriff.

Typ: Zeichenfolge

Zulässige Werte: CREATING | AVAILABLE | FAILED

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreJobCreator

Bedienung: 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 einer der sprachspezifischen Sprachen 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

BackupVaultArn

Der Amazon-Ressourcenname (ARN) des Backup-Tresors, der den wiederherzustellenden Wiederherstellungspunkt enthält. Dies hilft bei der Identifizierung von Richtlinien und Berechtigungen für den Tresorzugriff.

Typ: Zeichenfolge

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.

Typ: Long

Erforderlich: Nein

IamRoleArn

Die IAM-Rolle ARN, die zur Erstellung 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, ob es sich bei dem Wiederherstellungsauftrag um einen übergeordneten (zusammengesetzten) Wiederherstellungsauftrag handelt.

Typ: Boolesch

Erforderlich: Nein

ParentJobId

Dies ist die eindeutige Kennung des übergeordneten Wiederherstellungsauftrags für den ausgewählten Wiederherstellungsauftrag.

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 Volume Shadow Copy Service (VSS) -Backups ist Amazon EC2 der einzige unterstützte Ressourcentyp.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

RestoreJobId

Identifiziert den Auftrag, der einen Wiederherstellungspunkt wiederherstellt, eindeutig.

Typ: Zeichenfolge

Erforderlich: Nein

SourceResourceArn

Der Amazon-Ressourcenname (ARN) der ursprünglichen Ressource, die gesichert wurde. Dies bietet einen Überblick darüber, welche Ressource wiederhergestellt wird.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Ein Statuscode, der den Status des Auftrags angibt, der von AWS Backup der 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 einer der sprachspezifischen Sprachen 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 Resource Type, 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingPlanForCreate

Bedienung: 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 einen bestimmten Platzhalter. 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-Tresore angeben möchten ARNs , 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. Wenn kein CRON-Ausdruck angegeben wird, AWS Backup wird der Standardausdruck `cron(0 5 ? * * *)` verwendet.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingPlanForGet

Bedienung: 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 Testplans für die Wiederherstellung.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird. Wenn kein CRON-Ausdruck angegeben wird, AWS Backup wird der Standardausdruck `cron(0 5 ? * * *)` verwendet.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingPlanForList

Bedienung: 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 Testplans für die Wiederherstellung.

Typ: Zeichenfolge

Erforderlich: Ja

ScheduleExpression

Ein CRON-Ausdruck in der angegebenen Zeitzone, wenn ein Wiederherstellungstestplan ausgeführt wird. Wenn kein CRON-Ausdruck angegeben wird, AWS Backup wird der Standardausdruck `cron(0 5 ? * * *)` verwendet.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingPlanForUpdate

Bedienung: 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. Wenn kein CRON-Ausdruck angegeben ist, AWS Backup wird der Standardausdruck verwendet. `cron(0 5 ? * * *)`

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingRecoveryPointSelection

Bedienung: 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 einen bestimmten Platzhalter. 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-Tresore angeben möchten ARNs , 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 Selektoren 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 ein bestimmter ARNs oder ARN-Wildcard-Ersatz ["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; 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.

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 einer der sprachspezifischen Sprachen 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 geschützte Ressourcen hinzufügen ARNs . ProtectedResourceArns

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.

Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

Typ: Zeichenfolge

Erforderlich: Ja

ProtectedResourceArns

Jede geschützte Ressource kann nach ihren spezifischen Eigenschaften gefiltert werden ARNs, z. B. `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` oder nach einem Platzhalter: `ProtectedResourceArns: ["*"]`, aber nicht nach beiden.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

ProtectedResourceConditions

Wenn Sie den Platzhalter hinzugefügt haben `ProtectedResourceArns`, können Sie Ressourcenbedingungen einbeziehen, wie z. `ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }] }`

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 (0 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 einer der sprachspezifischen Sprachen 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.

Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

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 einen bestimmten Platzhalter angeben ARNs, z. B. `ProtectedResourceArns: ["arn:aws:...","arn:aws:..."]` oder Sie können einen Platzhalter angeben: `ProtectedResourceArns: ["*"]`, aber nicht beide.

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs 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.

Der Name enthält nur alphanumerische Zeichen und Unterstriche. Die maximale Länge beträgt 50.

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RestoreTestingSelectionForUpdate

Bedienung: 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 bestimmte Liste hinzufügen ARNs, z. B. `ProtectedResourceArns`: `["arn:aws:...","arn:aws:..."]` oder Sie können einen Platzhalter angeben: `ProtectedResourceArns`: `["*"]`, aber nicht beide.

Typ: Zeichenfolgen-Array

Erforderlich: Nein

ProtectedResourceConditions

Die Bedingungen, die Sie für Ressourcen in Ihrem Wiederherstellungstestplan mithilfe von Tags definieren.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanAction

Service: AWS Backup

Definiert eine Scanaktion, die den zu verwendenden Malware-Scanner und den zu verwendenden Scanmodus festlegt.

Inhalt

MalwareScanner

Der Malware-Scanner, der für die Scanaktion verwendet werden soll. Derzeit wird nur GUARDDUTY unterstützt.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

Erforderlich: Nein

ScanMode

Der Scanmodus, der für die Scanaktion verwendet werden soll.

Zulässige Werte: FULL_SCAN | INCREMENTAL_SCAN.

Typ: Zeichenfolge

Zulässige Werte: FULL_SCAN | INCREMENTAL_SCAN

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanJob

Service: AWS Backup

Enthält Metadaten zu einem Scanauftrag, einschließlich Informationen über den Scanvorgang, die Ergebnisse und die zugehörigen Ressourcen.

Inhalt

AccountId

Die Konto-ID, der der Scanauftrag gehört.

Typ: Zeichenfolge

Erforderlich: Ja

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: Ja

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

Erforderlich: Ja

CreatedBy

Enthält identifizierende Informationen über die Erstellung eines Scanauftrags.

Typ: [ScanJobCreator](#) Objekt

Erforderlich: Ja

CreationDate

Datum und Uhrzeit der Erstellung eines Scanauftrags im Unix-Format und in koordinierter 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: Ja

IamRoleArn

Gibt den ARN der IAM-Rolle an, der zur Erstellung des Scanauftrags verwendet wurde; zum Beispiel `arn:aws:iam::123456789012:role/S3Access`.

Typ: Zeichenfolge

Erforderlich: Ja

MalwareScanner

Die für den Scanauftrag verwendete Scan-Engine. Derzeit wird nur GUARDDUTY unterstützt.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

Erforderlich: Ja

RecoveryPointArn

Ein ARN, der den gescannten Wiederherstellungspunkt eindeutig identifiziert; zum Beispiel `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Typ: Zeichenfolge

Erforderlich: Ja

ResourceArn

Ein ARN, der die Quellressource des gescannten Wiederherstellungspunkts eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Ja

ResourceName

Der nicht eindeutige Name der Ressource, die zu der angegebenen Sicherung gehört.

Typ: Zeichenfolge

Erforderlich: Ja

ResourceType

Der Typ der AWS Ressource, die gescannt wird, z. B. ein Amazon Elastic Block Store (Amazon EBS) -Volume oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank.

Typ: Zeichenfolge

Zulässige Werte: EBS | EC2 | S3

Erforderlich: Ja

ScanJobId

Die eindeutige Kennung, die die Scan-Job-Anfrage identifiziert. AWS Backup

Typ: Zeichenfolge

Erforderlich: Ja

ScanMode

Gibt den für den Scanauftrag verwendeten Scantyp an.

Beinhaltet:

FULL_SCAN scannt die gesamte Datenlinie innerhalb des Backups.

INCREMENTAL_SCAN scannt den Datenunterschied zwischen dem Zielwiederherstellungspunkt und dem Basiswiederherstellungspunkt-ARN.

Typ: Zeichenfolge

Zulässige Werte: FULL_SCAN | INCREMENTAL_SCAN

Erforderlich: Ja

ScannerRoleArn

Gibt den ARN der Scanner-IAM-Rolle an, der für den Scanauftrag verwendet wird.

Typ: Zeichenfolge

Erforderlich: Ja

CompletionDate

Datum und Uhrzeit der Fertigstellung eines Scanauftrags im Unix-Format und in koordinierter Weltzeit (Coordinated Universal Time, 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

ScanBaseRecoveryPointArn

Ein ARN, der den Basiswiederherstellungspunkt für das Scannen eindeutig identifiziert. Dieses Feld wird aufgefüllt, wenn ein inkrementeller Scanauftrag stattgefunden hat.

Typ: Zeichenfolge

Erforderlich: Nein

ScanId

Die vom Malware-Scanner für den entsprechenden Scanauftrag generierte Scan-ID.

Typ: Zeichenfolge

Erforderlich: Nein

ScanResult

Enthält Informationen zu den Suchergebnissen, einschließlich des Status der beim Scannen gefundenen Bedrohungen.

Typ: [ScanResultInfo](#) Objekt

Erforderlich: Nein

State

Der aktuelle Status des Scanauftrags.

Gültige Werte: CREATED | RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Typ: Zeichenfolge

Zulässige Werte: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

Erforderlich: Nein

StatusMessage

Eine ausführliche Meldung, in der der Status des Scanauftrags erläutert wird.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanJobCreator

Service: AWS Backup

Enthält identifizierende Informationen über die Erstellung eines Scanauftrags, einschließlich des Sicherungsplans und der Regel, die den Scan initiiert hat.

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: Ja

BackupPlanId

Die ID des Backup-Plans.

Typ: Zeichenfolge

Erforderlich: Ja

BackupPlanVersion

Eindeutige, zufällig generierte Unicode- und UTF-8-kodierte Zeichenfolgen, die maximal 1.024 Bytes lang sind. Die Version IDs kann nicht bearbeitet werden.

Typ: Zeichenfolge

Erforderlich: Ja

BackupRuleId

Identifiziert eindeutig die Backup-Regel, die den Scan-Job initiiert hat.

Typ: Zeichenfolge

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanJobSummary

Service: AWS Backup

Enthält zusammenfassende Informationen zu Scanaufträgen, einschließlich Anzahl und Metadaten für einen bestimmten Zeitraum und bestimmte Kriterien.

Inhalt

AccountId

Die Konto-ID, der die in dieser Zusammenfassung enthaltenen Scanaufträge gehören.

Typ: Zeichenfolge

Pattern: `^[0-9]{12}$`

Erforderlich: Nein

Count

Die Anzahl der Scanaufträge, die den angegebenen Kriterien entsprechen.

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

MalwareScanner

Gibt den Malware-Scanner an, der während des Scanauftrags verwendet wurde. Unterstützt derzeit nur GUARDDUTY.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

Erforderlich: Nein

Region

Die AWS Region, in der die Scanaufträge ausgeführt wurden.

Typ: Zeichenfolge

Erforderlich: Nein

ResourceType

Der AWS Ressourcentyp für die in dieser Zusammenfassung enthaltenen Scanaufträge.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

ScanResultStatus

Der Status der Scanergebnisse für die in dieser Zusammenfassung enthaltenen Scanaufträge.

Zulässige Werte: THREATS_FOUND | NO_THREATS_FOUND.

Typ: Zeichenfolge

Zulässige Werte: NO_THREATS_FOUND | THREATS_FOUND

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

Der Status der in dieser Zusammenfassung enthaltenen Scanaufträge.

Gültige Werte: CREATED RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Typ: Zeichenfolge

Zulässige Werte: CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanResult

Service: AWS Backup

Enthält die Ergebnisse eines Sicherheitsscans, einschließlich Scannerinformationen, Scanstatus und aller gefundenen Ergebnisse.

Inhalt

Findings

Eine Reihe von Ergebnissen, die während des Scans entdeckt wurden.

Typ: Zeichenfolgen-Array

Zulässige Werte: MALWARE

Erforderlich: Nein

LastScanTimestamp

Der Zeitstempel, wann der letzte Scan durchgeführt wurde, im Unix-Format und in koordinierter Weltzeit (UTC).

Typ: Zeitstempel

Erforderlich: Nein

MalwareScanner

Der Malware-Scanner, mit dem der Scan durchgeführt wurde. Derzeit wird nur GUARDDUTY unterstützt.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

Erforderlich: Nein

ScanJobState

Der endgültige Status des Scanauftrags.

Zulässige Werte: COMPLETED | FAILED | CANCELED.

Typ: Zeichenfolge

Zulässige Werte: COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanResultInfo

Service: AWS Backup

Enthält Informationen über die Ergebnisse eines Scanauftrags.

Inhalt

ScanResultStatus

Der Status der Scanergebnisse.

Zulässige Werte: THREATS_FOUND | NO_THREATS_FOUND.

Typ: Zeichenfolge

Zulässige Werte: NO_THREATS_FOUND | THREATS_FOUND

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScanSetting

Service: AWS Backup

Enthält Konfigurationseinstellungen für Malware-Scans, einschließlich des Scannertyps, der Zielressourcentypen und der Scannerrolle.

Inhalt

MalwareScanner

Der Malware-Scanner, der für das Scannen verwendet werden soll. Derzeit wird nur GUARDDUTY unterstützt.

Typ: Zeichenfolge

Zulässige Werte: GUARDDUTY

Erforderlich: Nein

ResourceTypes

Eine Reihe von Ressourcentypen, die auf Malware gescannt werden sollen.

Typ: Zeichenfolge-Array

Pattern: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erforderlich: Nein

ScannerRoleArn

Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die der Scanner für den Zugriff auf Ressourcen verwendet, `arn:aws:iam::123456789012:role/ScannerRole` z. B..

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ScheduledPlanExecutionMember

Service: AWS Backup

Enthält Informationen zur Ausführung eines geplanten Sicherungsplans, einschließlich der Ausführungszeit, des Regeltyps und der zugehörigen Regel-ID.

Inhalt

ExecutionTime

Der Zeitstempel, zu dem die Ausführung des Backups geplant ist, im Unix-Format und in koordinierter Weltzeit (UTC). Der Wert ist auf Millisekunden genau.

Typ: Zeitstempel

Erforderlich: Nein

RuleExecutionType

Die Art der Ausführung der Backup-Regel. Gültige Werte sind `CONTINUOUS` (point-in-time Wiederherstellung), `SNAPSHOTS` (Snapshot-Backups) oder `CONTINUOUS_AND_SNAPSHOTS` (beide Typen zusammen).

Typ: Zeichenfolge

Zulässige Werte: `CONTINUOUS` | `SNAPSHOTS` | `CONTINUOUS_AND_SNAPSHOTS`

Erforderlich: Nein

RuleId

Die eindeutige Kennung der Backup-Regel, die zur geplanten Zeit ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TieringConfiguration

Service: AWS Backup

Dies enthält Metadaten zu einer Tiering-Konfiguration.

Inhalt

BackupVaultName

Der Name des Backup-Tresors, für den die Tiering-Konfiguration gilt. Wird für alle Backup-Tresore verwendet*.

Typ: Zeichenfolge

Pattern: `^(\\*|[a-zA-Z0-9\\-\\_]){2,50})$`

Erforderlich: Ja

ResourceSelection

Eine Reihe von Ressourcenauswahlobjekten, die angeben, welche Ressourcen in der Tiering-Konfiguration enthalten sind und welche Tiering-Einstellungen sie haben.

Typ: Array von [ResourceSelection](#)-Objekten

Erforderlich: Ja

TieringConfigurationName

Der eindeutige Name der Tiering-Konfiguration. Dieser Wert kann nach der Erstellung nicht geändert werden und darf nur aus alphanumerischen Zeichen und Unterstrichen bestehen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9_]{1,200}$`

Erforderlich: Ja

CreationTime

Datum und Uhrzeit der Erstellung einer Tiering-Konfiguration im Unix-Format und in koordinierter 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

CreatorRequestId

Dies ist eine eindeutige Zeichenfolge, die die Anfrage identifiziert und die Wiederholung fehlgeschlagener Anfragen ermöglicht, ohne dass das Risiko besteht, dass der Vorgang zweimal ausgeführt wird.

Typ: Zeichenfolge

Erforderlich: Nein

LastUpdatedTime

Datum und Uhrzeit der Aktualisierung einer Tiering-Konfiguration im Unix-Format und in koordinierter Weltzeit (UTC). Der Wert von LastUpdatedTime ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

TieringConfigurationArn

Ein Amazon-Ressourcenname (ARN), der die Tiering-Konfiguration eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TieringConfigurationInputForCreate

Service: AWS Backup

Dies enthält Metadaten zu einer Tiering-Konfiguration für Erstellungsvorgänge.

Inhalt

BackupVaultName

Der Name des Backup-Tresors, für den die Tiering-Konfiguration gilt. Wird für alle Backup-Tresore verwendet*.

Typ: Zeichenfolge

Pattern: `^(\\*|[a-zA-Z0-9\\-\\_]){2,50}$`

Erforderlich: Ja

ResourceSelection

Eine Reihe von Ressourcenauswahlobjekten, die angeben, welche Ressourcen in der Tiering-Konfiguration enthalten sind und welche Tiering-Einstellungen sie haben.

Typ: Array von [ResourceSelection](#)-Objekten

Erforderlich: Ja

TieringConfigurationName

Der eindeutige Name der Tiering-Konfiguration. Dieser Wert kann nach der Erstellung nicht geändert werden und darf nur aus alphanumerischen Zeichen und Unterstrichen bestehen.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9_]{1,200}$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TieringConfigurationInputForUpdate

Service: AWS Backup

Dies enthält Metadaten zu einer Tiering-Konfiguration für Aktualisierungsvorgänge.

Inhalt

BackupVaultName

Der Name des Backup-Tresors, für den die Tiering-Konfiguration gilt. Wird für alle Backup-Tresore verwendet*.

Typ: Zeichenfolge

Pattern: `^(\\*|[a-zA-Z0-9\\-\\_]){2,50})$`

Erforderlich: Ja

ResourceSelection

Eine Reihe von Ressourcenauswahlobjekten, die angeben, welche Ressourcen in der Tiering-Konfiguration enthalten sind und welche Tiering-Einstellungen sie haben.

Typ: Array von [ResourceSelection](#)-Objekten

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TieringConfigurationsListMember

Service: AWS Backup

Dies enthält Metadaten zu einer Tiering-Konfiguration, die in einer Liste zurückgegeben werden.

Inhalt

BackupVaultName

Der Name des Backup-Tresors, für den die Tiering-Konfiguration gilt. Wird für alle Backup-Tresore verwendet*.

Typ: Zeichenfolge

Pattern: `^(\\*|[a-zA-Z0-9\\-\\_]){2,50})$`

Erforderlich: Nein

CreationTime

Datum und Uhrzeit der Erstellung einer Tiering-Konfiguration im Unix-Format und in koordinierter Weltzeit (Coordinated Universal Time, 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

LastUpdatedTime

Datum und Uhrzeit der Aktualisierung einer Tiering-Konfiguration im Unix-Format und in koordinierter Weltzeit (UTC). Der Wert von `LastUpdatedTime` ist auf Millisekunden genau. Der Wert 1516925490.087 steht beispielsweise für Freitag, 26. Januar 2018, 12:11:30,087 Uhr.

Typ: Zeitstempel

Erforderlich: Nein

TieringConfigurationArn

Ein Amazon-Ressourcenname (ARN), der die Tiering-Konfiguration eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

TieringConfigurationName

Der eindeutige Name der Tiering-Konfiguration.

Typ: Zeichenfolge

Pattern: `^[a-zA-Z0-9_]{1,200}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AWS Backup gateway

Die folgenden Datentypen werden unterstützt von AWS Backup gateway:

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)
- [VmwareToAwsTagMapping](#)

BandwidthRateLimitInterval

Bedienung: 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 Bandbreitenbegrenzungintervalls 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 einer der sprachspezifischen Sprachen 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})\[/code>`

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 zuletzt 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 einer der sprachspezifischen Sprachen 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})\[/code>`

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 einer der sprachspezifischen Sprachen 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})\[/code>`

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 einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [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})\[/code>`

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-]{3})?:([0-9-]{3})?:(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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MaintenanceStartTime

Bedienung: 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 einer der sprachspezifischen Sprachen 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.

Zulässige Zeichen sind UTF-8-Buchstaben, Zahlen und die folgenden Zeichen: + - =. _ : /.

Leerzeichen sind in Tag-Werten nicht erlaubt.

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 einer der sprachspezifischen Sprachen 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-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

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 einer der sprachspezifischen Sprachen 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 ihren 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-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

VmwareTag

Bedienung: AWS Backup gateway

Ein VMware Tag ist ein Tag, der an eine bestimmte virtuelle Maschine angehängt ist. 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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VmwareToAwsTagMapping

Service: AWS Backup gateway

Dadurch wird die Zuordnung von 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: `(?!aws:)[\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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AWS Backup

Die folgenden Datentypen werden unterstützt von AWS Backup:

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)

- [SearchScopeSummary](#)
- [StringCondition](#)
- [TimeCondition](#)

BackupCreationTimeFilter

Bedienung: AWS Backup

Dies filtert nach Wiederherstellungspunkten innerhalb der CreatedBefore Zeitstempel CreatedAfter und.

Inhalt

CreatedAfter

Dieser Zeitstempel beinhaltet Wiederherstellungspunkte, die erst nach der angegebenen Zeit erstellt wurden.

Typ: Zeitstempel

Erforderlich: Nein

CreatedBefore

Dieser Zeitstempel beinhaltet Wiederherstellungspunkte, die nur vor dem angegebenen Zeitpunkt erstellt wurden.

Typ: Zeitstempel

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CurrentSearchProgress

Bedienung: AWS Backup

Dies enthält Informationsergebnisse, die aus einem Suchauftrag abgerufen wurden, der möglicherweise noch nicht abgeschlossen wurde.

Inhalt

ItemsMatchedCount

Diese Zahl ist die Summe aller Elemente, die den Elementfiltern eines laufenden Suchauftrags entsprechen.

Type: Long

Erforderlich: Nein

ItemsScannedCount

Diese Zahl ist die Summe aller Elemente, die bisher während eines Suchauftrags gescannt wurden.

Type: Long

Erforderlich: Nein

RecoveryPointsScannedCount

Diese Zahl ist die Summe aller Backups, die bisher während eines Suchauftrags gescannt wurden.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

EBSItemFilter

Bedienung: AWS Backup

Dies enthält Arrays von Objekten, zu denen CreationTimes Zeitbedingungsobjekte, FilePaths Zeichenkettenobjekte, LastModificationTimes Zeitbedingungsobjekte gehören können,

Inhalt

CreationTimes

Sie können 1 bis 10 Werte angeben.

Wenn einer enthalten ist, geben die Ergebnisse nur übereinstimmende Elemente zurück.

Wenn mehr als ein Element enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der enthaltenen Werte entsprechen.

Typ: Array von [TimeCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

FilePaths

Sie können 1 bis 10 Werte angeben.

Wenn ein Dateipfad enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Dateipfad entsprechen.

Wenn mehr als ein Dateipfad enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Dateipfade entsprechen.

Typ: Array von [StringCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

LastModificationTimes

Sie können 1 bis 10 Werte angeben.

Wenn einer enthalten ist, geben die Ergebnisse nur übereinstimmende Elemente zurück.

Wenn mehr als ein Element enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der enthaltenen Werte entsprechen.

Typ: Array von [TimeCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

Sizes

Sie können 1 bis 10 Werte angeben.

Wenn einer enthalten ist, geben die Ergebnisse nur übereinstimmende Elemente zurück.

Wenn mehr als ein Element enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der enthaltenen Werte entsprechen.

Typ: Array von [LongCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EBSResultItem

Bedienung: AWS Backup

Dies sind die Elemente, die in den Ergebnissen einer Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Inhalt

BackupResourceArn

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für den Amazon-Ressourcennamen (ARN) von Wiederherstellungspunkten übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultName

Der Name des Backup-Tresors.

Typ: Zeichenfolge

Erforderlich: Nein

CreationTime

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für Erstellungszeiten übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeitstempel

Erforderlich: Nein

FilePath

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für Dateipfade übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeichenfolge

Erforderlich: Nein

FileSize

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für Dateigrößen übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Type: Long

Erforderlich: Nein

FileSystemIdentifier

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für Dateisysteme übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeichenfolge

Erforderlich: Nein

LastModifiedTime

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für die Uhrzeit der letzten Änderung übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeitstempel

Erforderlich: Nein

SourceResourceArn

Dies sind ein oder mehrere Elemente in den Ergebnissen, die mit Werten für den Amazon-Ressourcennamen (ARN) der Quellressourcen übereinstimmen, die bei der Suche nach Amazon EBS-Backup-Metadaten zurückgegeben wurden.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExportJobSummary

Bedienung: AWS Backup

Dies ist die Zusammenfassung eines Exportauftrags.

Inhalt

ExportJobIdentifier

Dies ist die eindeutige Zeichenfolge, die einen bestimmten Exportauftrag identifiziert.

Typ: Zeichenfolge

Erforderlich: Ja

CompletionTime

Dies ist ein Zeitstempel für den Zeitpunkt, zu dem der Exportauftrag abgeschlossen wurde.

Typ: Zeitstempel

Erforderlich: Nein

CreationTime

Dies ist ein Zeitstempel für den Zeitpunkt, zu dem der Exportauftrag erstellt wurde.

Typ: Zeitstempel

Erforderlich: Nein

ExportJobArn

Dies ist der eindeutige ARN (Amazon Resource Name), der zu dem neuen Exportauftrag gehört.

Typ: Zeichenfolge

Erforderlich: Nein

SearchJobArn

Die eindeutige Zeichenfolge, die den Amazon-Ressourcennamen (ARN) des angegebenen Suchauftrags identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Der Status des Exportauftrags ist einer der folgenden:

CREATED;RUNNING;FAILED; oderCOMPLETED.

Typ: Zeichenfolge

Zulässige Werte: RUNNING | FAILED | COMPLETED

Erforderlich: Nein

StatusMessage

Eine Statusmeldung ist eine Zeichenfolge, die für einen Exportauftrag zurückgegeben wird.

Eine Statusmeldung ist für jeden Status enthalten, bei dem es sich nicht um einen Status COMPLETED ohne Probleme handelt.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExportSpecification

Bedienung: AWS Backup

Dies enthält das Objekt der Exportspezifikation.

Inhalt

Important

Bei diesem Datentyp handelt es sich um einen UNION-Datentyp, sodass nur eines der folgenden Elemente angegeben werden kann, wenn es verwendet oder zurückgegeben wird.

s3ExportSpecification

Dies gibt den Amazon S3-Ziel-Bucket für den Exportauftrag an. Und falls enthalten, gibt es auch das Zielpräfix an.

Typ: [S3ExportSpecification](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ItemFilters

Bedienung: AWS Backup

Elementfilter stellen alle Eigenschaften des Eingabeelements dar, die bei der Erstellung der Suche angegeben wurden.

Enthält entweder EBSItem Filter oder S3 ItemFilters

Inhalt

EBSItemFilters

Dieses Array kann Objekte CreationTimes, FilePaths LastModificationTimes, oder Sizes enthalten.

Typ: Array von [EBSItemFilter](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

S3ItemFilters

Dieses Array kann CreationTimes,, ETags ObjectKeys, Sizes oder VersionIds Objekte enthalten.

Typ: Array von [S3ItemFilter](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LongCondition

Bedienung: AWS Backup

Die lange Bedingung enthält eine Value und kann optional eine enthaltenOperator.

Inhalt

Value

Der Wert eines Elements, das in einem der Suchelementfilter enthalten ist.

Type: Long

Erforderlich: Ja

Operator

Eine Zeichenfolge, die definiert, welche Werte zurückgegeben werden.

Wenn dies enthalten ist, vermeiden Sie Kombinationen von Operatoren, die alle möglichen Werte zurückgeben. Wenn Sie beispielsweise beide angeben EQUALS_TO und NOT_EQUALS_TO einen Wert von angeben, 4 werden alle Werte zurückgegeben.

Typ: Zeichenfolge

Zulässige Werte: EQUALS_TO | NOT_EQUALS_TO | LESS_THAN_EQUAL_TO | GREATER_THAN_EQUAL_TO

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ResultItem

Bedienung: AWS Backup

Dies ist ein Objekt, das das Element darstellt, das in den Ergebnissen einer Suche nach einem bestimmten Ressourcentyp zurückgegeben wurde.

Inhalt

Important

Bei diesem Datentyp handelt es sich um einen UNION-Datentyp, sodass nur eines der folgenden Elemente angegeben werden kann, wenn es verwendet oder zurückgegeben wird.

EBSResultItem

Dies sind Artikel, die in den Suchergebnissen einer Amazon EBS-Suche zurückgegeben wurden.

Typ: [EBSResultItem](#) Objekt

Erforderlich: Nein

S3ResultItem

Dies sind Artikel, die in den Suchergebnissen einer Amazon S3-Suche zurückgegeben wurden.

Typ: [S3ResultItem](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

S3ExportSpecification

Bedienung: AWS Backup

Diese Spezifikation enthält eine erforderliche Zeichenfolge für den Ziel-Bucket. Optional können Sie das Zielpräfix angeben.

Inhalt

DestinationBucket

Dies gibt den Amazon S3-Ziel-Bucket für den Exportauftrag an.

Typ: Zeichenfolge

Erforderlich: Ja

DestinationPrefix

Dies gibt das Präfix für den Amazon S3-Ziel-Bucket für den Exportauftrag an.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

S3ItemFilter

Bedienung: AWS Backup

Dies enthält Arrays von Objekten, zu denen Größen ObjectKeys, CreationTimes VersionIds, und/oder ETags gehören können.

Inhalt

CreationTimes

Sie können 1 bis 10 Werte angeben.

Wenn ein Wert enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Wert entsprechen.

Wenn mehr als ein Wert enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Werte entsprechen.

Typ: Array von [TimeCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

ETags

Sie können 1 bis 10 Werte angeben.

Wenn ein Wert enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Wert entsprechen.

Wenn mehr als ein Wert enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Werte entsprechen.

Typ: Array von [StringCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

ObjectKeys

Sie können 1 bis 10 Werte angeben.

Wenn ein Wert enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Wert entsprechen.

Wenn mehr als ein Wert enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Werte entsprechen.

Typ: Array von [StringCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

Sizes

Sie können 1 bis 10 Werte angeben.

Wenn ein Wert enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Wert entsprechen.

Wenn mehr als ein Wert enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Werte entsprechen.

Typ: Array von [LongCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

VersionIds

Sie können 1 bis 10 Werte angeben.

Wenn ein Wert enthalten ist, geben die Ergebnisse nur Elemente zurück, die dem Wert entsprechen.

Wenn mehr als ein Wert enthalten ist, geben die Ergebnisse alle Elemente zurück, die einem der Werte entsprechen.

Typ: Array von [StringCondition](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 10 Elemente.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

S3ResultItem

Bedienung: AWS Backup

Dies sind die Elemente, die in den Ergebnissen einer Suche nach Amazon S3 S3-Backup-Metadaten zurückgegeben wurden.

Inhalt

BackupResourceArn

Dies sind Elemente in den zurückgegebenen Ergebnissen, die mit der Eingabe von Amazon Resource Names (ARN) für den Wiederherstellungspunkt bei der Suche nach Amazon S3 S3-Backup-Metadaten übereinstimmen.

Typ: Zeichenfolge

Erforderlich: Nein

BackupVaultName

Der Name des Backup-Tresors.

Typ: Zeichenfolge

Erforderlich: Nein

CreationTime

Dabei handelt es sich um ein oder mehrere Elemente in den zurückgegebenen Ergebnissen, die mit Werten für die bei der Suche nach Amazon S3 S3-Backup-Metadaten eingegebenen Werten für die Zeit der Artikelerstellung übereinstimmen.

Typ: Zeitstempel

Erforderlich: Nein

ETag

Dies sind ein oder mehrere Elemente in den zurückgegebenen Ergebnissen, die mit Werten übereinstimmen, die bei der Suche nach Amazon S3 S3-Backup-Metadaten ETags eingegeben wurden.

Typ: Zeichenfolge

Erforderlich: Nein

ObjectKey

Dies ist ein oder mehrere Elemente, die in den Ergebnissen einer Suche nach Amazon S3 S3-Backup-Metadaten zurückgegeben wurden, die den für den Objektschlüssel eingegebenen Werten entsprechen.

Typ: Zeichenfolge

Erforderlich: Nein

ObjectSize

Dies sind Elemente in den zurückgegebenen Ergebnissen, die mit Werten für Objektgröße (n) übereinstimmen, die bei der Suche nach Amazon S3 S3-Backup-Metadaten eingegeben wurden.

Type: Long

Erforderlich: Nein

SourceResourceArn

Dies sind Elemente in den zurückgegebenen Ergebnissen, die mit der Quelleingabe von Amazon Resource Names (ARN) bei der Suche nach Amazon S3 S3-Backup-Metadaten übereinstimmen.

Typ: Zeichenfolge

Erforderlich: Nein

VersionId

Dies sind ein oder mehrere Elemente in den zurückgegebenen Ergebnissen, die Werten für die IDs Versionseingabe während einer Suche nach Amazon S3 S3-Backup-Metadaten entsprechen.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SearchJobBackupsResult

Bedienung: AWS Backup

Dies enthält die Informationen zu Wiederherstellungspunkten, die in den Ergebnissen eines Suchauftrags zurückgegeben wurden.

Inhalt

BackupCreationTime

Dies ist die Erstellungszeit des Backups (Wiederherstellungspunkts).

Typ: Zeitstempel

Erforderlich: Nein

BackupResourceArn

Der Amazon-Ressourcenname (ARN), der die Backup-Ressourcen eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

IndexCreationTime

Dies ist die Erstellungszeit des Backup-Index.

Typ: Zeitstempel

Erforderlich: Nein

ResourceType

Dies ist der Ressourcentyp der Suche.

Typ: Zeichenfolge

Zulässige Werte: S3 | EBS

Erforderlich: Nein

SourceResourceArn

Der Amazon-Ressourcenname (ARN), der die Quellressourcen eindeutig identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Dies ist der Status des Backup-Ergebnisses des Suchauftrags.

Typ: Zeichenfolge

Zulässige Werte: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

Erforderlich: Nein

StatusMessage

Dies ist die Statusmeldung, die in den Ergebnissen enthalten ist.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SearchJobSummary

Bedienung: AWS Backup

Dies sind Informationen, die sich auf einen Suchauftrag beziehen.

Inhalt

CompletionTime

Dies ist die Fertigstellungszeit des Suchauftrags.

Typ: Zeitstempel

Erforderlich: Nein

CreationTime

Dies ist die Erstellungszeit des Suchauftrags.

Typ: Zeitstempel

Erforderlich: Nein

Name

Dies ist der Name des Suchauftrags.

Typ: Zeichenfolge

Erforderlich: Nein

SearchJobArn

Die eindeutige Zeichenfolge, die den Amazon-Ressourcennamen (ARN) des angegebenen Suchauftrags identifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

SearchJobIdentifier

Die eindeutige Zeichenfolge, die den Suchauftrag spezifiziert.

Typ: Zeichenfolge

Erforderlich: Nein

SearchScopeSummary

Es wurde eine Zusammenfassung des angegebenen Suchauftragsbereichs zurückgegeben, einschließlich:

- TotalBackupsToScanCount, die Anzahl der bei der Suche zurückgegebenen Wiederherstellungspunkte.
- TotalItemsToScanCount, die Anzahl der bei der Suche zurückgegebenen Elemente.

Typ: [SearchScopeSummary](#) Objekt

Erforderlich: Nein

Status

Dies ist der Status des Suchauftrags.

Typ: Zeichenfolge

Zulässige Werte: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

Erforderlich: Nein

StatusMessage

Für einen Suchauftrag mit dem Status ERRORERD oder dem Status von COMPLETED Aufträgen mit Problemen wird eine Statusmeldung zurückgegeben.

Beispielsweise kann in einer Meldung angegeben werden, dass eine Suche Wiederherstellungspunkte enthielt, die aufgrund eines Berechtigungsproblems nicht gescannt werden konnten.

Typ: Zeichenfolge

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SearchScope

Bedienung: AWS Backup

Der Suchbereich umfasst alle Backup-Eigenschaften, die in eine Suche eingegeben werden.

Inhalt

BackupResourceTypes

Die in einer Suche enthaltenen Ressourcentypen.

Zu den geeigneten Ressourcentypen gehören S3 und EBS.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Feste Anzahl von 1 Element.

Zulässige Werte: S3 | EBS

Erforderlich: Ja

BackupResourceArns

Der Amazon-Ressourcenname (ARN), der die Backup-Ressourcen eindeutig identifiziert.

Typ: Zeichenfolge-Array

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

BackupResourceCreationTime

Dies ist der Zeitpunkt, zu dem eine Backup-Ressource erstellt wurde.

Typ: [BackupCreationTimeFilter](#) Objekt

Erforderlich: Nein

BackupResourceTags

Dies sind ein oder mehrere Tags auf dem Backup (Wiederherstellungspunkt).

Typ: Abbildung einer Zeichenfolge auf eine Zeichenfolge

Erforderlich: Nein

SourceResourceArns

Der Amazon-Ressourcenname (ARN), der die Quellressourcen eindeutig identifiziert.

Typ: Zeichenfolge-Array

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SearchScopeSummary

Bedienung: AWS Backup

Die Zusammenfassung des angegebenen Suchauftragsbereichs, einschließlich:

- TotalBackupsToScanCount, die Anzahl der bei der Suche zurückgegebenen Wiederherstellungspunkte.
- TotalItemsToScanCount, die Anzahl der bei der Suche zurückgegebenen Elemente.

Inhalt

TotalItemsToScanCount

Dies ist die Gesamtzahl der Elemente, die bei einer Suche gescannt werden.

Type: Long

Erforderlich: Nein

TotalRecoveryPointsToScanCount

Dies ist die Gesamtzahl der Backups, die bei einer Suche gescannt werden.

Typ: Ganzzahl

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

StringCondition

Bedienung: AWS Backup

Dies enthält den Wert der Zeichenfolge und kann einen oder mehrere Operatoren enthalten.

Inhalt

Value

Der Wert der Zeichenfolge.

Typ: Zeichenfolge

Erforderlich: Ja

Operator

Eine Zeichenfolge, die definiert, welche Werte zurückgegeben werden.

Wenn dies enthalten ist, vermeiden Sie Kombinationen von Operatoren, die alle möglichen Werte zurückgeben. Wenn Sie beispielsweise beide angeben `EQUALS_TO` und `NOT_EQUALS_TO` einen Wert von angeben, 4 werden alle Werte zurückgegeben.

Typ: Zeichenfolge

Zulässige Werte: `EQUALS_TO` | `NOT_EQUALS_TO` | `CONTAINS` | `DOES_NOT_CONTAIN` | `BEGINS_WITH` | `ENDS_WITH` | `DOES_NOT_BEGIN_WITH` | `DOES_NOT_END_WITH`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TimeCondition

Bedienung: AWS Backup

Eine Zeitbedingung bezeichnet eine Erstellungszeit, eine Uhrzeit der letzten Änderung oder eine andere Uhrzeit.

Inhalt

Value

Dies ist der Zeitstempelwert der Zeitbedingung.

Typ: Zeitstempel

Erforderlich: Ja

Operator

Eine Zeichenfolge, die definiert, welche Werte zurückgegeben werden.

Wenn dies enthalten ist, vermeiden Sie Kombinationen von Operatoren, die alle möglichen Werte zurückgeben. Wenn Sie beispielsweise beide angeben `EQUALS_TO` und `NOT_EQUALS_TO` einen Wert von angeben, 4 werden alle Werte zurückgegeben.

Typ: Zeichenfolge

Zulässige Werte: `EQUALS_TO` | `NOT_EQUALS_TO` | `LESS_THAN_EQUAL_TO` | `GREATER_THAN_EQUAL_TO`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen 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 zu Signature Version 4 finden Sie unter [Signieren von AWS API-Anfragen](#) im IAM-Benutzerhandbuch.

Action

Die auszuführende Aktion.

Typ: Zeichenfolge

Erforderlich: Ja

Version

Die API-Version, für die die Anfrage geschrieben wurde, ausgedrückt im Format YYYY-MM-DD.

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 im IAM-Benutzerhandbuch unter [Erstellen einer signierten AWS API-Anfrage](#).

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'SSMSS'Z') sein. Beispielsweise ist die folgende Datums- und Uhrzeitangabe 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-Grundformat angegeben ist, X-Amz-Date ist dies nicht erforderlich. Wenn verwendet X-Amz-Date wird, überschreibt er immer den Wert des Date-Headers. Weitere Informationen finden Sie unter [Elemente einer AWS API-Anforderungssignatur](#) im IAM-Benutzerhandbuch.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Security-Token

Das temporäre Sicherheitstoken, das durch einen Aufruf 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 Sicherheitsanmeldedaten von verwenden AWS STS, müssen Sie das Sicherheitstoken angeben.

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 werden die Fehler aufgeführt, die bei den API-Aktionen aller AWS Dienste häufig 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 angegebene AWS Zugriffsschlüssel-ID ist in unseren Aufzeichnungen nicht vorhanden.

HTTP Status Code: 403

NotAuthorized

Sie haben keine Berechtigung zum Ausführen dieser Aktion.

HTTP Status Code: 400

OptInRequired

Für die AWS Zugriffsschlüssel-ID ist ein Abonnement für den Dienst erforderlich.

HTTP Status Code: 403

RequestExpired

Die Anfrage erreichte den Service mehr als 15 Minuten nach dem Datumsstempel auf der Anfrage oder mehr als 15 Minuten nach dem Ablaufdatum der Anfrage (z. B. bei vorsignierter Anfrage URLs), oder der Datumsstempel auf der Anfrage liegt mehr als 15 Minuten in der future.

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 Dienst angegebenen Einschränkungen.

HTTP Status Code: 400

Dokumenthistorie für AWS Backup

- API-Version: 19. November 2025
- Letzte Aktualisierung der Dokumentation: 19. November 2025

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.

Änderungen	Beschreibung	Date
GuardDuty Amazon-Malware-Schutz für AWS Backup	Amazon GuardDuty Malware Protection unterstützt jetzt EBS AWS Backup- und S3-Backups und erweitert die Funktionen zur EC2 Malware-Erkennung auf diese. Weitere Informationen finden Sie auf der Produktdetailseite von .	19. November 2025
Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupGuardDutyRolePolicyForScans _AWS verwaltete Richtlinie hinzugefügt. Weitere Informationen finden Sie unter Verwaltete Richtlinien für AWS Backup.	19. November 2025
Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupServiceRolePolicyForScans AWS verwaltete Richtlinie hinzugefügt.	19. November 2025

Änderungen	Beschreibung	Date
	Weitere Informationen finden Sie unter Verwaltete Richtlinien für AWS Backup .	
Aktualisierung der verwalteten Richtlinien	AWS Backup den folgenden AWS verwalteten Richtlinien wurden zusätzliche Berechtigungen hinzugefügt: • AWSBackupFullAccess • AWSBackupOperatorAccess Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	19. November 2025
Backup-Tiering	AWS Backup führt eine kostengünstige Warm-Storage-Stufe für Amazon S3 S3-Backup-Daten ein. Weitere Informationen finden Sie unter Backup-Tiering.	18. November 2025

Änderungen	Beschreibung	Date
Primäre Backups zu logischen Air-Gapped Vaults	Logisch bedingte Air-Gap-Depots werden jetzt als primäres Backup-Ziel unterstützt. Diese Erweiterung ermöglicht es Kunden, die Sicherheits- und Wiederherstellungsvorteile logischer Air-Gap-Tresore zu nutzen und gleichzeitig nur eine einzige Sicherungskopie zu verwalten, wodurch die Speicher- und Betriebskosten gesenkt werden. Bisher konnten in Tresoren mit logischem Air-Gap nur Kopien vorhandener Backups gespeichert werden. Weitere Informationen finden Sie unter Primäre Backups in Tresoren mit logischem Air-Gap.	17. November 2025
AWS Backup Unterstützung für Amazon Elastic Kubernetes Service Cluster	AWS Backup unterstützt jetzt Amazon EKS-Cluster. Kunden können Backups erstellen und Wiederherstellungspunkte für Amazon EKS-Cluster und die zugehörigen Ressourcen wiederherstellen. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Ressourcen und Aktualisierungen verwaltet er Richtlinien für AWS Backup.	10. November 2025

Änderungen	Beschreibung	Date
Aktualisierung der verwalteten Richtlinien	AWS Backup den folgenden AWS verwalteten Richtlinien wurden zusätzliche Berechtigungen hinzugefügt: • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForRestores Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	10. November 2025
Logischer Air-Gap-Vault-Support für vom Kunden verwaltete Schlüssel AWS KMS	Tresore mit logischem Air-Gap unterstützen jetzt die Verschlüsselung mit vom Kunden verwalteten Schlüsseln. AWS KMS Weitere Informationen finden Sie unter Tresor mit logischem Air-Gap.	6. November 2025

Änderungen	Beschreibung	Date
Unterstützung für das regionsübergreifende und kontoübergreifende Kopieren von Snapshots	Amazon RDS, Aurora, DocumentDB und Neptune unterstützen jetzt regionsübergreifendes und kontoübergreifendes Kopieren von Snapshots in einer einzigen Aktion. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Ressourcen.	23. Oktober 2025
AWS Backup Erweiterung der regionalen Unterstützung für Aurora DSQL	Aurora DSQL-Backup- und Wiederherstellungsunterstützung ist jetzt in Europa (Frankfurt) verfügbar. Weitere Informationen finden Sie unter Unterstützte Dienste nach Region und Aurora DSQL-Backups.	22. Oktober 2025
AWS Backup Regionale Expansion	AWS Backup, zusammen mit vielen seiner Funktionen, ist jetzt im asiatisch-pazifischen Raum (Neuseeland) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	29. September 2025

Änderungen	Beschreibung	Date
Unterstützung für optionale Amazon S3 S3-Backups ACLs und Object-Tags	AWS Backup unterstützt jetzt den optionalen Ausschluss von Amazon S3 ACLs und Objekt-Tags, sodass Kunden dazu beitragen können, die Backup-Kosten zu senken. Weitere Informationen finden Sie unter Amazon-S3-Backups.	9. September 2025
Aktualisierung der verwalteten Richtlinien	AWS Backup den folgenden AWS verwalteten Richtlinien wurden zusätzliche Berechtigungen hinzugefügt: • AWSBackupServiceLinkedRolePolicyForBackup Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	9. September 2025

Änderungen	Beschreibung	Date
AWS Backup Audit Manager Regionale Expansion	AWS Backup Regions- und kontenübergreifende Berichte von Audit Manager sind jetzt zusätzlich verfügbar AWS-Regionen, darunter Asien-Pazifik (Hyderabad), Asien-Pazifik (Jakarta), Asien-Pazifik (Melbourne), Europa (Spanien), Europa (Zürich) und Naher Osten (VAE). Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen von AWS-Region und Berichtspläne erstellen.	5. September 2025
Verbesserte AWS Backup Unterstützung für Amazon Aurora DSQL Multi-Region-Wiederherstellung	AWS Backup Benutzer können jetzt Aurora DSQL-Cluster mit mehreren Regionen über die AWS Backup Konsole oder über AWS Backup die CLI wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Aurora DSQL-Clusters mit mehreren Regionen.	29. Juli 2025

Änderungen	Beschreibung	Date
Aktualisierung der verwalteten Richtlinien	AWS Backup den folgenden AWS verwalteten Richtlinien wurden zusätzliche Berechtigungen hinzugefügt: • AWSBackupServiceRolePolicyForRestore Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	29. Juli 2025
AWS Backup Unterstützung für Amazon Aurora DSQL Multiregion Restore zusätzlich AWS-Regionen	AWS Backup unterstützt jetzt zusätzlich Aurora DSQL Multi-Region Restore. AWS-Regionen Weitere Informationen finden Sie unter Wiederherstellen eines Aurora DSQL-Clusters mit mehreren Regionen und Unterstützte Dienste nach Region.	3. Juli 2025

Änderungen	Beschreibung	Date
AWS Backup Merkmal Regionale Expansion	AWS Backup fügt Unterstützung für konto- und regionsübergreifendes Kopieren von Amazon S3 S3-Backups innerhalb AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) hinzu. AWS-Regionen Weitere Informationen finden Sie unter Amazon S3 S3-Backups und Backup und Tag-Kopie.	26. Juni 2025
AWS Backup Unterstützung für Amazon Aurora DSQL im asiatisch-pazifischen Raum (Seoul)	AWS Backup unterstützt jetzt Aurora DSQL im asiatisch-pazifischen Raum (Seoul). Weitere Informationen finden Sie unter Unterstützte Dienste nach Regionen.	26. Juni 2025

Änderungen	Beschreibung	Date
AWS Backup Unterstützung für die Genehmigung durch mehrere Parteien	AWS Backup unterstützt jetzt die optionale Integration von Tresoren mit logischem Air-Gap zur Verwendung der Genehmigung durch mehrere Parteien. Diese Funktion ist derzeit für Konten im Osten der USA (Nord-Virginia) verfügbar. Weitere Informationen finden Sie unter: • Genehmigung durch mehrere Parteien für Tresore mit logischem Air-Gap Benutzerhandbuch für die Genehmigung durch mehrere Parteien	17. Juni 2025
AWS verwaltetes Richtlini enupdate	AWS Backup der AWS verwalteten Richtlinie wurden neue Berechtigungen hinzugefügt AWSBackup FullAccess . Weitere Informationen und spezifische Berechtigungsänderungen finden Sie unter Richtlini enaktualisierungen.	17. Juni 2025

Änderungen	Beschreibung	Date
AWS Backup Audit Manager Regionale Expansion	AWS Backup Audit Manager ist jetzt zusätzlich verfügbar AWS-Regionen, darunter: • Asien-Pazifik (Hyderabad) • Asien-Pazifik (Jakarta) • Asien-Pazifik (Melbourne) • Europa (Spain) • Europa (Zürich) • Naher Osten (VAE) Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Region und Backup Audit Manager.	16. Juni 2025
AWS Backup Regionale Expansion	AWS Backup ist zusammen mit vielen seiner Funktionen jetzt im asiatisch-pazifischen Raum (Taipeh) verfügbar AWS-Region. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Regionen und Unterstützte Dienste nach Regionen.	6. Juni 2025

Änderungen	Beschreibung	Date
Backup-Index-Benachrichtigung und Unterstützung bei Ereignissen	AWS Backup startet Unterstützung für Amazon Simple Notification Service-Benachrichtigungen und EventBridge Amazon-Ereignisse für Backup-Indizes. AWS Backup Unterstützung für Benachrichtigungs-Backup-Indizes ist in allen AWS kommerziellen und GovCloud Regionen verfügbar, in denen Backup-Indizes, SNS und. unterstützt werden. EventBridge Weitere Informationen finden Sie unter Benutzerbenachrichtigungen Konsole, Konsole und Suche und EventBridge Index für Backups.	3. Juni 2025

Änderungen	Beschreibung	Date
Zusätzliche Funktionen für Amazon EC2 Restore	Die Volumenkonfigurationen können während eines Wiederherstellungsauftrags angepasst werden. Sie können benutzerdefinierte Einstellungen für an ein Amazon EC2 AMI angehängte Amazon EBS-Volumes angeben, einschließlich der Wiederherstellungsmetadaten für Blockgerätezuordnungen. Weitere Informationen finden Sie unter Amazon wiederherstellen EC2 mit AWS CLI und im Amazon Elastic Compute Cloud-Benutzerhandbuch.	28. Mai 2025
AWS Backup Unterstützung für Amazon Aurora DSQL-Cluster	AWS Backup bietet jetzt die Integration mit Aurora DSQL in mehreren AWS-Regionen. Kunden können Backups erstellen und Wiederherstellungspunkte für Aurora DSQL-Cluster mit einer oder mehreren Regionen wiederherstellen. Weitere Informationen finden Sie unter Amazon Aurora DSQL-Wiederherstellung, Funktionsverfügbarkeit nach Ressource und Cluster in Aurora DSQL verwalten mit dem AWS CLI	27. Mai 2025

Änderungen	Beschreibung	Date
Aktualisierung der verwalteten Richtlinien	AWS Backup zusätzliche Berechtigungen für die folgenden AWS verwalteten Richtlinien hinzugefügt: AWSBackupFullAccess, AWSBackupOperatorAccess, AWSBackupServiceLinkedRolePolicyForBackup, AWSBackupServiceRolePolicyForBackup, und AWSBackupServiceRolePolicyForRestores. Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	27. Mai 2025
AWS Backup Funktion Regionale Expansion	AWS Backup Die Suche ist jetzt in Asien-Pazifik (Thailand), Mexiko (Zentral), AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) verfügbar. AWS-Regionen Weitere Informationen erhalten Sie unter Verfügbarkeit der Funktionen von AWS-Region und Backup-Suche.	22. April 2025

Änderungen	Beschreibung	Date
AWS Backup Unterstützung für serverlose Amazon Redshift Redshift-Namespaces	Kunden haben jetzt die Möglichkeit, manuelle Redshift Serverless-Snapshot-Backups AWS Backup zu erstellen und auf Redshift Serverless-Namespaces wiederherzustellen. Weitere Informationen finden Sie unter Serverlose Backups von Amazon Redshift.	31. März 2025
Aktualisierung der verwalteten Richtlinien	AWS Backup den folgenden AWS verwalteten Richtlinien wurden zusätzliche Berechtigungen hinzugefügt: • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForRestore Weitere Informationen finden Sie unter Verwaltete Richtlinienaktualisierungen für AWS Backup.	31. März 2025

Änderungen	Beschreibung	Date
AWS Backup unterstützter Service Regionale Expansion	AWS Backup Unterstützung FSx für OpenZFS ist jetzt in den folgenden Bereichen verfügbar: AWS-Regionen • USA West (Nordkalifornien) • Afrika (Kapstadt) • Asien-Pazifik (Hyderabad) • Asien-Pazifik (Jakarta) • Asien-Pazifik (Osaka) • Europa (Milan) • Europa (Paris) • Europa (Spain) • Europa (Zürich) • Israel (Tel Aviv) • Middle East (Bahrain) • Naher Osten (VAE) • Südamerika (São Paulo) Weitere Informationen finden Sie unter Unterstützte Dienste von. AWS-Regionen	12. März 2025

Änderungen	Beschreibung	Date
Erweiterung der Tresor-Ressourcen mit logischem Air-Gap	Wiederherstellungspunkte (Backups) von FSx Lustre-, FSx Windows File Server- und OpenZFS-Ressourcen können jetzt in FSx einen Tresor mit logischem Air-Gapped kopiert werden. Weitere Informationen finden Sie unter: • Logischer Air-Gapped Vault • Feature-Verfügbarkeit nach Ressource	12. März 2025
Neue verwaltete Richtlinie AWS	AWS Backup hat eine neue AWS verwaltete Richtlinie hinzugefügt: AWSBackupSearchOperatorAccess. Weitere Informationen finden Sie AWSBackupSearchOperatorAccess im AWS Managed Policy Guide.	27. Februar 2025
AWS Backup Regionale Expansion	AWS Backup, zusammen mit vielen seiner Funktionen, ist jetzt in Mexiko (Zentral) verfügbar AWS-Region. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	21. Januar 2025

Änderungen	Beschreibung	Date
AWS Backup Regionale Expansion	AWS Backup, zusammen mit vielen seiner Funktionen, ist jetzt im asiatisch-pazifischen Raum (Thailand) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	14. Januar 2025
Aktualisierte von AWS verwaltete Richtlinien	AWS Backup hat die Berechtigung <code>rds:AddTagsToResource</code> zur verwalteten Richtlinie hinzugefügt <code>AWSBackupServiceLinkedRolePolicyForBackup</code>. AWS Backup hat die Berechtigungen <code>rds:CreateTenantDatabase</code> und <code>rds>DeleteTenantDatabase</code> zur Richtlinie hinzugefügt <code>AWSBackupServiceRolePolicyForRestores</code>. Weitere Informationen finden Sie unter Richtlinienaktualisierungen.	8. Januar 2025

Änderungen	Beschreibung	Date
Support für IPv6	AWS Backup unterstützt jetzt beide Internetprotokolle Version 6 (IPv6) und IPv4. Weitere Informationen zu Dual-Stack-Funktionen und Endpunkten finden Sie unter AWS Backup Netzwerk.	18. Dezember 2024
AWS Backup unterstützter Service Regionale Expansion	AWS Backup Unterstützung für Amazon Timestream ist jetzt in AWS GovCloud (US-West) verfügbar. Weitere Informationen finden Sie unter Unterstützte Services von AWS-Regionen und Amazon Timestream Timestream-Backups.	18. Dezember 2024
Suchfunktion hinzugefügt	AWS Backup führt die Option ein, Ihre Backup-Metadaten nach Eigenschaften auf Elementebene zu durchsuchen, um Wiederherstellungspunkte und andere Dateien oder Objekte zu finden, die Sie wiederherstellen möchten. Weitere Informationen finden Sie unter Backup-Suche.	17. Dezember 2024

Änderungen	Beschreibung	Date
Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupServiceRolePolicyForItemResources AWS verwaltete Richtlinie hinzugefügt. Weitere Informationen finden Sie unter Verwaltete Richtlinien für AWS Backup.	17. Dezember 2024
Eine neue AWS verwaltete Richtlinie wurde hinzugefügt	AWS Backup hat die AWSBackupServiceRolePolicyForIndexing AWS verwaltete Richtlinie hinzugefügt. Weitere Informationen finden Sie unter Verwaltete Richtlinien für AWS Backup.	17. Dezember 2024
AWS Backup Funktion Regionale Expansion	Eine kontenübergreifende Verwaltung zur Überwachung von Sicherungs-, Kopier- und Wiederherstellungsaufträgen AWS Backup sowie zur AWS Organizations Integration ist jetzt auch dort verfügbar , AWS-Regionen wo eine Anmeldung erforderlich ist. Weitere Informationen finden Sie unter Verfügbarkeit von Features nach Region.	12. Dezember 2024

Änderungen	Beschreibung	Date
AWS Backup unterstützter Service, Regionale Expansion	AWS Backup Unterstützung für Amazon Timestream ist jetzt im asiatisch-pazifischen Raum (Mumbai) verfügbar. Weitere Informationen finden Sie unter Unterstützte Services von AWS-Regionen und Amazon Timestream Timestream-Backups.	22. November 2024
Zusätzliche Funktionen für die Amazon S3 S3-Wiederherstellung	AWS Backup bietet zusätzliche Flexibilität bei der Wiederherstellung von S3-Backups. Sie können jetzt zusätzliche Versionen von Objekten wiederherstellen, einschließlich der Wiederherstellung aller Versionen. Weitere Informationen finden Sie unter S3-Daten wiederherstellen mit AWS Backup.	21. November 2024

Änderungen	Beschreibung	Date
AWS Backup Funktion Regionale Expansion	AWS Backup Kunden können jetzt regionsübergreifende Kopien von Amazon Neptune Neptune-Backups in mehr Regionen erstellen, darunter Afrika (Kapstadt), Asien-Pazifik (Jakarta) und Asien-Pazifik (Osaka). Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Regionen und Erstellen von Sicherungskopien in allen Regionen. AWS-Regionen	13. November. 2024
Erweiterung des Kopiervorgangs über mehrere Regionen	Regionsübergreifendes Kopieren von Amazon S3 S3-Backups wird jetzt dort unterstützt AWS-Regionen , wo eine Anmeldung erforderlich ist. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen von. AWS-Region	13. November 2024
AWS Backup Audit Manager Regionale Expansion	AWS Backup Audit Manager ist jetzt im AWS-Region asiatisch-pazifischen Raum (Osaka) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach Region und Backup Audit Manager.	29. Oktober 2024

Änderungen	Beschreibung	Date
AWS Backup jetzt in der Region Asien-Pazifik (Malaysia) erhältlich	Backup und Wiederherstellung für viele Ressourcentypen sind jetzt im AWS-Region asiatisch-pazifischen Raum (Malaysia) 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.	10. Oktober 2024
AWS Backup Audit Manager Manager-Steuerung für Tresor mit logischem Air-Gap	AWS Backup Audit Manager bietet jetzt die Kontrollressourcen in einem Tresor mit logischem Air-Gap an, um zu überwachen, ob Ressourcen innerhalb des angegebenen Zeitrahmens in einen Tresor mit logischem Air-Gap kopiert wurden. Weitere Informationen erhalten Sie unter Steuerelemente und Abhilfemaßnahmen und Prüfung eines Wiederherstellungstests.	12. September 2024

Änderungen	Beschreibung	Date
AWS Backup Merkmal Regionale Expansion	AWS Backup Kunden können jetzt regionsübergreifende Kopien von Amazon Neptune Neptune-Backups in mehr Regionen erstellen, darunter Asien-Pazifik (Hongkong), Israel (Tel Aviv), Naher Osten (Bahrain) und Naher Osten (VAE). Weitere Informationen finden Sie unter Verfügbarkeit der Funktionen nach Regionen und Erstellen von Sicherungskopien in allen Regionen. AWS-Regionen	29. August. 2024
AWS Backup unterstützt regionsübergreifendes, kontoübergreifendes Kopieren für SAP HANA-Datenbanken	Benutzer, die SAP HANA-Datenbanken auf EC2 Amazon-Instances gesichert haben, können jetzt Snapshots von vollständigen Backups in andere Regionen und andere Konten kopieren. Weitere Informationen finden Sie unter SAP HANA-Datenbanken auf EC2 Amazon-Instances.	20. August 2024

Änderungen	Beschreibung	Date
AWS Backup bietet jetzt eine neue Art von sicherem Tresor	AWS Backup hat einen sekundären Tresortyp zum Speichern von Backup-Kopien eingeführt. Tresore mit logischem Air-Gap bieten erweiterte Sicherheitsfunktionen sowie die Möglichkeit, den Tresorzugriff mit Konten gemeinsam zu nutzen. AWS RAM Weitere Informationen finden Sie unter Tresor mit logischem Air-Gapped.	7. August 2024
AWS Backup Merkmal Regionale Expansion	AWS Backup Unterstützung für Amazon Simple Storage Service (Amazon S3) ist jetzt in Kanada West (Calgary) verfügbar. Kunden können jetzt Ressourcen in der Region Kanada West (Calgary) sichern und wiederherstellen. Weitere Informationen zur Verfügbarkeit von AWS Backup Amazon S3 in der Region finden Sie unter Unterstützte Services von AWS-Region.	27. Juni 2024
Logischer Air-Gap-Tresor-Vorschauverschluss	Logischerweise wurde die Vault-Vorschau mit Air-Gaps beendet.	27. Juni 2024

Änderungen	Beschreibung	Date
AWS Backup Merkmal Regionale Expansion	AWS Backup Die Unterstützung der Amazon EBS-Snapshots-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 • AWSBackupServiceRolePolicyForS3 Backup • AWSBackupServiceLinkedRolePolicyForBackup Weitere Informationen finden Sie unter Richtlinienaktualisierungen.	17. Mai 2024

Änderungen	Beschreibung	Date
AWS Backup jetzt erhältlich in der Region Kanada West (Calgary)	Backup und Wiederherstellung für viele Ressourcentypen sind jetzt in AWS-Region Kanada 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, AWSServiceRolePolicyForBackupRestoreTesting indem 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

Änderungen	Beschreibung	Date
Backup- und Wiederherstellungsunterstützung FSx für ONTAP-Volumes FlexGroup	AWS Backup unterstützt jetzt in den meisten Fällen die Sicherung und Wiederherstellung von FSx FlexGroup ONTAP-Volumes. AWS-Regionen Weitere Informationen finden Sie unter Wiederherstellen eines FSx Amazon-Datensystems.	10. Januar 2024
Unterstützung für SAP-HANA-HA-Backup und -Wiederherstellung	AWS Backup bietet jetzt Unterstützung für SAP HANA-Hochverfügbarkeitsdatenbanken auf Amazon EC2 Backup and Restore. Weitere Informationen finden Sie unter EC2 Backups von SAP HANA auf Amazon und Wiederherstellen eines SAP HANA-Hochverfügbarkeitssystems.	21. Dezember 2023

Änderungen	Beschreibung	Date
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 erhalten 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 for Cold StorageLebenszyklus und Speicherstufen, und Erstellen Sie einen Backup-Plan.	8. November 2023

Änderungen	Beschreibung	Date
Einführung zu Wiederherstellungstests	AWS Backup führt Wiederherstellungstests ein, die eine automatische und regelmäßige Bewertung der Durchführbarkeit der Wiederherstellung sowie die Möglichkeit bieten, die Dauer von Wiederherstellungsaufträgen zu überwachen. Weitere Informationen finden Sie unter Wiederherstellungstests.	8. November 2023

Änderungen	Beschreibung	Date
Aktualisierte von AWS verwaltete Richtlinien	AWS Backup hat die Berechtigungen <code>ec2:DescribeSnapshotTierStatus</code> und <code>ec2:ModifySnapshotTier</code> zu den verwalteten Richtlinien hinzugefügt <code>AWSBackupServiceRolePolicyForBackups</code> und <code>AWSBackupServiceLinkedRolePolicyForBackup</code> . AWS Backup hat auch die Berechtigungen <code>ec2:DescribeSnapshotTierStatus</code> und <code>ec2:RestoreSnapshotTier</code> die verwaltet e Richtlinie hinzugefügt <code>AWSBackupServiceRolePolicyForRestores</code> . 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

Änderungen	Beschreibung	Date
Es wurde eine Weitergabe-Rollenberechtigung hinzugefügt, um Wiederherstellungstests zu unterstützen.	AWS Backup <code>restore-testing.backup.amazonaws.com</code> zu <code>IamPassRolePermissions</code> und <code>IamCreateServiceLinkedRolePermissions</code> hinzugefügt. Dieser Zusatz ist erforderlich AWS Backup , um Wiederherstellungstests im Auftrag von Kunden durchzuführen.	8. November 2023

Änderungen	Beschreibung	Date
Es wurde eine neue serviceverknüpfte Rolle hinzugefügt	AWS Backup hat die neue dienstbezogene Rolle mit dem Namen hinzugefügt <u>AWSServiceRoleForBackupRestoreTesting</u>, die Backup-Berechtigungen für die Durchführung von Wiederherstellungstests bereitstellt. Diese neue <u>dienstbezogene Rolle</u> bietet AWS Backup die für die Durchführung von Wiederherstellungstests erforderlichen Berechtigungen. Die Berechtigungen umfassen die Aktionen <code>list</code>, <code>read</code>, <code>and write</code> für die folgenden Dienste, die in Wiederherstellungstests aufgenommen werden sollen: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon, Amazon EFS EC2, FSx für Lustre, für Windows File Server, FSx für ONTAP, FSx für OpenZFS, Amazon Neptune, Amazon RDS und Amazon S3.	8. November 2023

Änderungen	Beschreibung	Date
Neues Job-Metrik-Dashboard in der Konsole AWS Backup	In der AWS Backup Konsole wird jetzt ein Job-Dashboard angezeigt, das die Überwachung des Backup-Zustands im großen 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 -Konsole-Dashboards.	15. November 2023

Änderungen	Beschreibung	Date
Support für verschachtelte Stack-Backups	AWS Backup hat seine Unterstützung für Backups von 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 Point-in-time Backups und Wiederherstellungen von Amazon Aurora	AWS Backup unterstützt jetzt kontinuierliche point-in-time Backups und Wiederherstellungen (PITR) für Aurora-Ressourcen. Weitere Informationen finden Sie unter Kontinuierliche Backups und Point-in-time Wiederherstellung.	07. September 2023

Änderungen	Beschreibung	Date
CloudFormation Stacks unterstützen den Ausschluss von Ressourcen	AWS Backup unterstützt jetzt die Option, ausgewählte Ressourcen von Ihrem CloudFormation Stack auszuschließen. Weitere Informationen finden Sie unter 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 erhältlich in der Region Israel (Tel Aviv)	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

Änderungen	Beschreibung	Date
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 Backups prüfen und Berichte mit AWS Backup Audit Manager erstellen , Mit Auditberichten arbeiten und Delegierter Administrator .	16. 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
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

Änderungen	Beschreibung	Date
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
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

Änderungen	Beschreibung	Date
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
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

Änderungen	Beschreibung	Date
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
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

Änderungen	Beschreibung	Date
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
Erweiterte Unterstützung für regionsübergreifendes Kopieren AWS Backup	Regionsübergreifende Backups von Amazon EFS- und DynamoDB-Ressourcen können jetzt in den folgenden Regionen durchgeführt werden: Asien-Pazifik (Jakarta), Naher Osten (Bahrain), Asien-Pazifik (Hongkong), Afrika (Kapstadt) und Europa (Mailand). VMware	28. April 2023

Änderungen	Beschreibung	Date
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
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

Änderungen	Beschreibung	Date
SAP HANA-Datenbanken auf EC2 Amazon-Instances Backup und wiederherstellen	AWS Backup bietet jetzt in den meisten Regionen die Möglichkeit, SAP HANA-Datenbanken, die auf EC2 Amazon-Instances laufen, zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Backup von SAP HANA-Datenbanken auf EC2 Amazon-Instances.	17. April 2023
AWS Backup jetzt in den Regionen Europa (Spanien), Europa (Zürich) und Asien-Pazifik (Hyderabad) erhältlich	AWS Backup Die Unterstützung wurde auf neue Regionen ausgeweitet, darunter Europa (Spanien), Europa (Zürich) und Asien-Pazifik (Hyderabad). Unterstützte Ressourcen können in diesen Regionen gesichert und wiederhergestellt werden. Weitere Informationen finden Sie unter Verfügbarkeit von Funktionen nach AWS Regionen.	13. April 2023

Änderungen	Beschreibung	Date
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:DescribeComplianceByConfigRule durch eine Wildcard-Ressource ersetzt. Weitere Informationen finden Sie unter Richtlinien-Updates für AWS Backup .	11. April 2023
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

Änderungen	Beschreibung	Date
Verbesserung des inkrementellen Backups virtueller Maschinen	VMware Backups von virtuellen Maschinen (VMs), 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
AWS Backup Unterstützung für mehrere Netzwerkadapter	AWS Backup Gateway unterstützt jetzt die Konfiguration mehrerer Netzwerkadapter Weitere Informationen zur Konfiguration Ihrer Netzwerkadapter finden Sie unter Konfiguration Ihres Gateways für mehrere NICs VMware im AWS Backup Entwicklerhandbuch.	08. März 2023

Änderungen	Beschreibung	Date
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 Supported VMs im AWS Backup Developer Guide.	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

Änderungen	Beschreibung	Date
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). Weitere Informationen finden Sie unter Erstellen von Backup-Kopien über AWS-Regionen hinweg.	21. Dezember 2022

Änderungen	Beschreibung	Date
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. Um diese Funktion zu unterstützen, AWS Backup hat das Unternehmen verwaltete Richtlinien erstellt und aktualisiert, darunter <code>AWSBackupFullAccess</code> und <code>AWSBackupOperatorAccess</code>. Weitere Informationen finden Sie unter Bandbreitendrosselung des Backup-Gateways.	15. Dezember 2022

Änderungen	Beschreibung	Date
Unterstützung für VMware Backup-Gateway-Tags	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 <code>AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync</code>, darunter <code>AWSBackupFullAccess</code>, und <code>AWSBackupOperatorAccess</code>. 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

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
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 Vorschauversion von SAP HANA auf EC2 Amazon-Instances. Zur Unterstützung dieser Vorversion AWS Backup hat das Unternehmen Richtlinienaktualisierungen und neue AWS verwaltete Richtlinien für diese Funktionen bereitgestellt.	20. November 2022

Änderungen	Beschreibung	Date
Auf EC2 Amazon-Instances wiederherstellen VMware	AWS Backup bietet jetzt die Möglichkeit, virtuelle Maschinen auf EC2 Amazon-Instances wiederherzustellen , zusätzlich zur Möglichkeit, Maschinen in EBS VMware, VMware Cloud on AWS und VMware Cloud on AWS Outposts wiederherzustellen. Weitere Informationen finden Sie in der Dokumentation zur Verwendung der AWS Backup Konsole zum Wiederherstellen von Wiederherstellungspunkten 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 Unveränderlichkeit zu gewährleisten. Erfahren Sie mehr unter AWS Backup Vault Lock.	4. Oktober 2022

Änderungen	Beschreibung	Date
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-EB S-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

Änderungen	Beschreibung	Date
AWS Backup Audit Manager bietet zusätzliche Kontrollunterstützung FSx für ONTAP	AWS Backup Audit Manager bietet jetzt zusätzliche Steuerelemente zur Unterstützung der Überwachung und Prüfung FSx von ONTAP-Volumen, einschließlich Backup-Ressourcen, die in mindestens einem Backup-Plan enthalten sind und der zuletzt erstellte Wiederherstellungspunkt. Weitere Informationen finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe.	22. Juli 2022
AWS Backup fügt Unterstützung 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 Wiederherstellung 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

Änderungen	Beschreibung	Date
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 (virtuellen privaten Netzwerken) zu helfen.	14. Juni 2022

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
AWS Backup Audit Manager bietet zusätzliche Kontrollunterstützung für Storage Gateway	Backup Audit Manager bietet jetzt Unterstützung für die Compliance-Kontrolle Durch Backup-Pläne geschützt e Backup-Ressourcen für Storage-Gateway-Ressourcentypen. Weitere Informationen finden Sie unter AWS Backup Audit Manager – Kontrollen und Abhilfe .	25. Mai 2022
Support für Amazon FSx für OpenZFS	AWS Backup bietet jetzt zusätzliche Datenschutzverwaltung für das Sichern und Wiederherstellen von FSx OpenZFS-Dateisystemen.	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 Audit Manager – Kontrollen und Abhilfe .	11. Mai 2022

Änderungen	Beschreibung	Date
Amazon wird FSx jetzt in der Region Asien-Pazifik (Osaka) unterstützt	AWS Backup bietet jetzt Backups von Amazon FSx in der Region Asien-Pazifik (Osaka) sowie regionsübergreifende Kopien in und aus der Region Asien-Pazifik (Osaka) an.	26. April 2022
Support für Amazon FSx for Lustre Persistent_2	AWS Backup bietet jetzt allgemeine Unterstützung 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, Wiederherstellung auf Festplattenebene und Unterstützung für VMware . 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

Änderungen	Beschreibung	Date
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 erhalten Sie unter AWS Backup und AWS PrivateLink .	28. Februar 2022

Änderungen	Beschreibung	Date
Unterstützung für Amazon Simple Storage Service (Amazon S3)	Die allgemeine Verfügbarkeit 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 China 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
Support für VMware virtuelle Maschinen (VMs)	Sie können es jetzt verwenden AWS Backup , um automatische Backups zu erstellen VMware VMs. Weitere Informationen finden Sie unter Backups virtueller Maschinen .	30. November 2021

Änderungen	Beschreibung	Date
Unterstützung für erweitertes DynamoDB-Backup	Sie können jetzt die folgenden Funktionen für alle neuen DynamoDB-Tabellensicherungen verwenden AWS Backup , die Sie erstellen: Cold Storage Tiering, Cost Allocation Tagging, regionsübergreifendes Kopieren, kontoübergreifendes Kopieren, unabhängige Verschlüsselung und Kopieren von Tags aus DynamoDB-Quellentabellen. Weitere Informationen finden Sie Erweitertes DynamoDB-Backup im Amazon DynamoDB Developer Guide und unter Using AWS Backup with DynamoDB .	23. November 2021
Support bei der Verbesserung der AWS Backup Ressourcenzuweisung in AWS China Regionen	AWS Backup Die Verbesserung der Ressourcenzuweisung 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

Änderungen	Beschreibung	Date
Einführung der Verbesserung der AWS Backup Ressourcenzuweisung	Die Verbesserung der Zuweisung von Backup-Ressourcen bietet Ihnen zusätzliche, detaillierte Kontrollen und neue optimierte Prozesse für die Bereitstellung von Backup-Plänen, die Hunderttausende von Ressourcen schützen. AWS Verwenden Sie dieses Feature, um Ihre Geschwindigkeit, 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

Änderungen	Beschreibung	Date
Support für AWS Backup Vault Lock in AWS China 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

Änderungen	Beschreibung	Date
CloudFormation Unterstützung für AWS Backup Audit Manager	Mit 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 für die Einhaltung Ihrer definierten Kontrollen im Laufe der Zeit dienen. Weitere Informationen finden Sie unter Backup-Audit und Berichte mit AWS Backup Audit Manager .	24. August 2021

Änderungen	Beschreibung	Date
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 EC2 Amazon-Instances schützen, erstellt standardmäßig mehrvolumige AWS Backup , absturzsichere Backups aller Amazon EBS-Volumes, die an jede Amazon-Instance angehängt sind. EC2 Weitere Informationen finden Sie unter Erstellen eines absturzkonsistenten Amazon-EBS-Multi-Volume-Backup .	14. Juni 2021

Änderungen	Beschreibung	Date
Zusätzliche Support für Amazon FSx AWS-Regionen	Sie können es jetzt AWS Backup zum Schutz Ihrer FSx Amazon-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 Allgemeinen AWS -Referenz.	15. April 2021
Support für regionsübergreifende und FSx kontoübergreifende Amazon-Backups	Sie können es jetzt verwenden AWS Backup , um FSx Amazon-Backups zwischen Konten AWS-Regionen zu kopieren. Weitere Informationen finden Sie unter Erstellen einer Backup-Kopie. Wenn Sie vom Kunden verwaltete Richtlinien verwenden, sollten Sie die neue Berechtigung <code>fsx:CopyBackup</code> hinzufügen, um zu verhindern, dass bestehende Backup-Aufträge fehlschlagen. Informationen zu dieser Genehmigung finden Sie in der letzten Erklärung in der FSx Amazon-Backup-Richtlinie unter Vom Kunden verwaltete Richtlinien.	12. April 2021

Änderungen	Beschreibung	Date
Unterstützung für Kostenzuordnung-Tags für Amazon-EFS-Backups	Sie können jetzt Kostenzuordnung-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 Kostenzuordnung-Tags .	7. April 2021
FedRAMP-High-Autorisierung	AWS Backup ist jetzt autorisiert, FedRAMP High-Workloads zu unterstützen. Weitere Informationen finden Sie unter AWS -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 werden Storage Gateway, Amazon FSx und kontenübergreifendes Backup in dieser Region AWS Backup derzeit nicht unterstützt. Weitere Informationen finden Sie unter AWS Backup -Endpunkte und -Kontingente in der Allgemeinen AWS -Referenz.	25. März 2021

Änderungen	Beschreibung	Date
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 S-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

Änderungen	Beschreibung	Date
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 kontoübergreifenden 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
Support für das Sichern und Wiederherstellen von FSx Amazon-Dateisystemen	Sie können es jetzt AWS Backup zum Sichern von FSx Amazon-Dateisystemen verwenden. Weitere Informationen finden Sie unter Arbeiten mit FSx Amazon-Dateisystemen .	9. November 2020

Änderungen	Beschreibung	Date
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 EC2 Amazon-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

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
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
Support für die Sicherung von EC2 Amazon-Instances und zusätzliche Unterstützung für regionsübergreifendes Backup	Sie können jetzt ganze EC2 Amazon-Instances sichern und auch Ressourcen kopieren AWS-Regionen. 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.