aws

Benutzer-Leitfaden

Amazon EBS



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

Amazon EBS: Benutzer-Leitfaden

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

Die Handelsmarken und die 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 Amazon EBS? 1
Features von Amazon EBS 1
Zugehörige Services 2
Zugreifen auf Amazon EBS 3
Preisgestaltung 4
Für Amazon EBS einrichten 5
Melden Sie sich für eine an AWS-Konto 5
(Optional) Erstellen und verwenden Sie einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung 5
(Optional) Aktivieren Sie die Blockierung des öffentlichen Zugriffs für Amazon EBS-Snapshots 6
EBS-Datenträger 8
Features und Vorteile 9
Datenverfügbarkeit 9
Datenpersistenz 10
Datenverschlüsselung 11
Datensicherheit 11
-Snapshots 12
Flexibilität 13
EBS-Volume-Typen 13
Volumes für Solid-State-Laufwerke (SSD) 13
Volumes für Festplattenlaufwerke (HDD) 16
Volumes der vorherigen Generation 17
Allzweck-SSD-Volumes 18
Bereitgestellte IOPS-SSD-Volumes 23
Durchsatzoptimierte HDD- und Cold-HDD-Volumes 27
EBS-Volumenbeschränkungen 38
Speicherkapazität 39
Service-Einschränkungen 39
Partitionierungsschemata 40
Datenblockgrößen 41
EBS-Volumes und NVMe 44
Ordnen Sie Volumes Gerätenamen zu 45
I/O Timeout für den Betrieb 49

Abort command 50
Lebenszyklus eines Volumens 51
Ein Volume erstellen 53
Einen Band teilen 58
Kopieren Sie ein Volume 64
Ein Volume an die Instance anhängen 72
Anfügen eines Volumes an mehrere Instances 74
Verfügbarmachen eines Volumes für die Verwendung 84
Anzeigen von Volumendetails 99
Ändern Sie ein Volume 106
Trennen eines Volumes von einer Instance 133
Löschen eines Volumes 138
Ersetzen eines Volumes 139
Statusüberprüfungen 143
Volumenereignisse 146
Arbeiten mit einem beeinträchtigten Volume 148
Auto-enable I/O 152
Fehlertests 154
Verfügbare Experimente 154
Überlegungen 154
Unterbrechen Sie die I/O Fehlereinleitung 155
Latenzinjektion 157
EBS-Snapshots 161
Funktionsweise von Snapshots 162
Snapshot-Lebenszyklus 166
Erstellen von -Snapshots 167
-Snapshot-Informationen anzeigen 174
Kopieren eines -Snapshots 178
Teilen Sie einen Snapshot 193
Archivieren von Snapshots 201
Löschen eines Snapshots 238
Schnelle Snapshot-Wiederherstellung 243
Überlegungen 244
Preise und Fakturierung 245
Guthaben zum Erstellen eines Volumes 245
Konfigurieren Sie die schnelle Snapshot-Wiederherstellung 247

Überprüfen Sie den Status der schnellen Snapshot-Wiederherstellung 250
Anzeigen von Volumes, die mithilfe der schnellen Snapshot-Wiederherstellung wiederhergestellt wurden 252
Snapshot Lock 253
Konzepte 254
Überlegungen 257
Kontrollieren des Zugriffs 258
Sperren eines Snapshots 262
Entsperren eines Snapshots 265
Einstellungen der Snapshot-Sperre aktualisieren 265
Überwachen Sie die Snapshot 267
Blockieren des öffentlichen Zugriffs auf Snaphots 270
IAM-Berechtigungen 272
Konfigurieren von Block Public Access 273
Die Einstellung „Öffentlichen Zugriff blockieren“ anzeigen 277
Öffentlichen Zugriff deaktivieren 280
Überwachen, blockieren Sie den öffentlichen Zugriff 283
Lokale Schnappschüsse auf Outposts 285
Häufig gestellte Fragen 285
Voraussetzungen 288
Überlegungen 75
Zugriffssteuerung mit IAM 289
Arbeiten mit lokale Snapshots 291
Lokale Schnappschüsse in lokalen Zonen 297
Häufig gestellte Fragen 285
Überlegungen 75
Zugriffssteuerung mit IAM 300
EBS-Verschlüsselung 305
So funktioniert die EBS-Verschlüsselung 305
So funktioniert die EBS-Verschlüsselung bei verschlüsseltem Snapshot 306
So funktioniert die EBS-Verschlüsselung bei unverschlüsseltem Snapshot 307
Auswirkung von unbrauchbaren KMS-Schlüsseln auf Datenschlüssel 307
Lokale Zonen, Außenposten und Wellenlängenzonen 308
Local Zones 308
Außenposten und Wellenlängenzonen 309
Voraussetzungen 309

Unterstützte Volume-Typen 310
Unterstützte Instance-Typen 310
Berechtigungen für --Benutzer 310
Berechtigungen für Instances 311
Aktivieren Sie standardmäßig die Verschlüsselung 313
Standard-Verschlüsselungsschlüssel 317
Verschlüsseln von EBS-Ressourcen 318
Verschlüsseln eines leeren Volumes bei der Erstellung 318
Verschlüsseln unverschlüsselter Ressourcen 319
KMS-Schlüssel rotieren 319
Beispiele 320
Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung nicht aktiviert) 321
Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung aktiviert) 322
Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung nicht aktiviert) 322
Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung aktiviert) .. 323
Re-encrypt ein verschlüsseltes Volume 323
Re-encrypt ein verschlüsselter Snapshot 324
Migrieren von Daten zwischen verschlüsselten und unverschlüsselten Volumes 325
Verschlüsselungsergebnisse 325
EBS-Leistung 330
Tipps zur Amazon EBS-Leistung 330
Verwenden Sie Instanzen EBS-optimized 331
Konfigurieren Sie die Instanzbandbreite 331
Informationen zum Berechnen der Leistung 331
Informationen zum Workload 331
Berücksichtigen der Leistungseinbußen, die beim Initialisieren von Volumes aus Snapshots auftreten 331
Faktoren, die die HDD-Leistung beeinträchtigen können 332
Erhöhen Sie den Read-Ahead-Wert für Workloads mit hohem Durchsatz und leseintensiven Workloads auf st1 und sc1 (Nur Linux-Instanzen) 332
Verwenden Sie einen modernen Linux-Kernel (Nur Linux-Instanzen) 333
Verwenden von RAID 0 zur maximalen Nutzung der Instance-Ressourcen 334
Überwachen Sie die Leistung des Amazon EBS-Volumes 334

EBS-Optimierung ... 334
Initialisieren von Volumes ... 335
Verwenden Sie eine von Amazon EBS bereitgestellte Rate für die Volumeninitialisierung ... 336
Verwenden Sie einen Snapshot, der für die schnelle Snapshot-Wiederherstellung aktiviert ist ... 342
Initialisieren Sie die Volumes manuell ... 342
Überwachen Sie die Initialisierung des Volumes ... 347
Konfigurierbare Gewichtung der Instanz-Bandbreite ... 352
I/O Eigenschaften und Überwachung ... 353
E/A\Sek ... 354
Länge und Latenz der Volume-Warteschlange ... 355
I/O Grenzwerte für Größe und Volumen beim Durchsatz ... 356
Überwachen Sie die Eigenschaften I/O mit CloudWatch ... 357
Überwachen Sie Leistungsstatistiken in Echtzeit I/O ... 359
Zugehörige Ressourcen ... 359
RAID-Konfiguration ... 359
RAID-Konfigurationsoptionen ... 360
Erstellen Sie ein RAID 0-Array ... 361
Erstellen von Snapshots von Volumes in einem RAID-Array ... 370
Durchführen von Benchmark-Tests für EBS-Volumes ... 371
Einrichten Ihrer Instance ... 371
Installieren von Benchmark-Tools ... 373
Auswählen der Volume-Warteschlangenlänge ... 375
Deaktivieren C-states ... 375
Durchführen von Benchmark-Tests ... 377
Amazon Data Lifecycle Manager ... 381
Kontingente ... 382
Funktionsweise ... 382
Richtlinien ... 382
Zeitpläne von Richtlinien ... 384
Target resource Tags (Zielressourcen-Tags (Markierungen)) ... 385
-Snapshots ... 385
EBS-backed AMIs ... 386
Amazon-Data-Lifecycle-Manager-Tags ... 386
Standardrichtlinien im Vergleich zu benutzerdefinierten Richtlinien ... 387
Vergleich der EBS-Snapshot-Richtlinien ... 387

EBS-backed Vergleich der AMI-Richtlinien ... 390
Erstellen Sie Standardrichtlinien ... 392
Überlegungen zu Standardrichtlinien ... 392
Erstellen Sie eine Standardrichtlinie für Amazon EBS-Snapshots ... 393
Erstellen Sie eine Standardrichtlinie für AMIs EBS-backed ... 397
Aktivieren Sie die Standardrichtlinien für alle Konten und Regionen ... 401
Erstellen Sie eine benutzerdefinierte Richtlinie für Snapshots ... 406
Erstellen einer Snapshot-Lebenszyklusrichtlinie ... 407
Überlegungen zu Snapshot-Lebenszyklusrichtlinien ... 424
Weitere Ressourcen ... 430
Automatisieren Sie anwendungskonsistente Snapshots ... 430
Andere Anwendungsfälle für Vor- und Nach-Skripte ... 468
Funktionsweise von Vor- und Nach-Skripten ... 477
Identifizieren Sie Snapshots, die mit Pre- und Post-Skripten erstellt wurden ... 480
Überwachen Sie Pre- und Post-Skripte ... 481
Erstellen Sie eine benutzerdefinierte Richtlinie für AMIs ... 482
Erstellen einer AMI-Lebenszyklusrichtlinie ... 482
Überlegungen zu AMI-Lebenszyklusrichtlinien ... 489
Weitere Ressourcen ... 493
Kontoübergreifende Snapshot-Kopien automatisieren ... 493
Kontoübergreifende Richtlinien für Snapshot-Kopierrichtlinien ... 494
Festlegen von Snapshot-Beschreibungsfiltern ... 506
Überlegungen zu Richtlinien für das kontoübergreifende Kopieren von Snapshots ... 507
Weitere Ressourcen ... 508
Richtlinien ändern ... 508
Löschen von Richtlinien ... 511
Kontrollieren des Zugriffs ... 513
AWS verwaltete Richtlinien ... 515
IAM-Servicerollen ... 524
Überwachen Sie die Richtlinien ... 531
Konsole und AWS CLI ... 531
Überwachen Sie Richtlinien mithilfe von EventBridge ... 532
Überwachen Sie Richtlinien mithilfe von CloudWatch ... 534
Protokollieren von AWS CloudTrail-API-Aufrufen mithilfe von ... 549
Service-Endpunkte ... 553
IPv4-Endpunkte ... 554

Dual-stack (IPv4 und IPv6) -Endpunkte ... 554
FIPS-Endpunkte ... 555
Angeben von Endpunkten ... 555
Schnittstellen-VPC-Endpunkte ... 556
Überlegungen zu Amazon EBS-VPC-Endpunkten ... 556
Erstellen Sie einen Schnittstellen-VPC-Endpunkt für Amazon EBS ... 557
Fehlerbehebung ... 557
Fehler: Die `Rolle mit dem Namen ist bereits vorhanden` ... 557
AWS Backup für Amazon EBS ... 559
Amazon EBS Direct-APIs ... 560
Preisgestaltung ... 561
Preise für APIs ... 561
Netzwerkkosten ... 561
Konzepte ... 562
-Snapshots ... 562
Blöcke ... 562
Blockindizes ... 563
Block-Tokens ... 563
Prüfsumme ... 563
Verschlüsselung ... 563
API-Aktionen ... 563
Signatur, Version 4, Signierung ... 564
Kontrollieren des Zugriffs ... 565
Lesen von Snapshots ... 570
Liste der Blöcke in einem Snapshot ... 571
Liste der Blöcke, die sich zwischen zwei Snapshots unterscheiden ... 574
Abrufen von Blockdaten aus einem Snapshot ... 578
Schreiben von Snapshots ... 579
Starten eines Snapshots ... 580
Einfügen von Daten in einen Snapshot ... 582
Abschluss eines Snapshots ... 584
Verschlüsselungsergebnisse ... 585
Verschlüsselungsergebnisse: unverschlüsselter übergeordneter Snapshot ... 586
Verschlüsselungsergebnisse: verschlüsselter übergeordneter Snapshot ... 587
Verschlüsselungsergebnisse: kein übergeordneter Snapshot ... 588
Validieren Sie Snapshot-Daten ... 589

Stellen Sie Idempotenz sicher ... 590
Wiederholungsversuche ... 591
Optimieren der Leistung ... 595
Service-Endpunkte ... 596
IPv4-Endpunkte ... 596
Dual-stack Endpunkte (IPv4 und IPv6) ... 597
FIPS-Endpunkte ... 598
Angeben von Endpunkten ... 598
SDK-Codebeispiele ... 600
StartSnapshot ... 600
PutSnapshotBlock ... 601
CompleteSnapshot ... 602
Schnittstellen-VPC-Endpunkte ... 603
Überlegungen zu VPC-Endpunkten für EBS-Direct-APIs ... 603
Erstellen eines Schnittstellen-VPC-Endpunkts für EBS-Direct-APIs ... 604
CloudTrail protokolliert ... 605
EBS Direct APIs, Daten, Ereignisse in CloudTrail ... 607
Verwaltungsereignisse für direkte EBS-APIs in CloudTrail ... 607
Beispiele für Ereignisse mit EBS Direct APIs ... 550
Häufig gestellte Fragen ... 614
Papierkorb ... 617
Unterstützte Ressourcen ... 618
Funktionsweise ... 619
Überlegungen ... 620
Kontingente ... 624
Zugehörige Services ... 625
Preisgestaltung ... 625
Kontrollieren des Zugriffs ... 626
Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln ... 626
Berechtigungen zum Arbeiten mit Ressourcen im Papierkorb ... 628
Bedingungsschlüssel für den Papierkorb ... 628
Aufbewahrungsregel erstellen ... 631
Aufbewahrungsregel aktualisieren ... 636
Aufbewahrungsregel sperren ... 638
Aufbewahrungsregel entsperren ... 640
Zuweisen von Tags zu Aufbewahrungsregeln ... 641

Anzeigen von Tags für Aufbewahrungsregeln ... 642
Entfernen von Tags von Aufbewahrungsregeln ... 643
Löschen Sie die Aufbewahrungsregeln ... 644
Gelöschte Schnappschüsse wiederherstellen ... 645
Berechtigungen zum Arbeiten mit Snapshots im Papierkorb ... 646
Anzeigen von Snapshots im Papierkorb ... 647
Wiederherstellen von Snapshots aus dem Papierkorb ... 648
Gelöschte Volumes wiederherstellen ... 650
Berechtigungen für die Arbeit mit Volumes im Papierkorb ... 650
Volumes im Papierkorb anzeigen ... 652
Stellen Sie Volumes aus dem Papierkorb wieder her ... 653
Gelöschte AMIs wiederherstellen ... 654
Berechtigungen zum Arbeiten mit AMIs im Papierkorb ... 655
Anzeigen von AMIs im Papierkorb ... 656
Wiederherstellen von AMIs aus dem Papierkorb ... 658
Überwachen Sie mit EventBridge ... 659
RuleLocked ... 660
RuleChangeAttempted ... 660
RuleUnlockScheduled ... 661
RuleUnlockingNotice ... 662
RuleUnlocked ... 662
Überwachen Sie mit CloudTrail ... 663
Informationen zum Papierkorb finden Sie unter CloudTrail ... 549
Auswerten der Papierkorb-Protokolldateieinträge ... 665
Service-Endpunkte ... 678
IPv4-Endpunkte ... 596
Dual-stack (IPv4 und IPv6) Endpunkte ... 679
FIPS-Endpunkte ... 679
Angeben von Endpunkten ... 680
Verwenden Sie Schnittstellen-VPC-Endpunkte ... 681
Erstellen Sie einen Schnittstellen-VPC-Endpunkt für den Papierkorb ... 681
Erstellen Sie eine VPC-Endpunktrichtlinie für den Papierkorb ... 681
Sicherheit ... 683
Datenschutz ... 683
Datensicherheit bei Amazon EBS ... 685
Verschlüsselung bei Speicherung und Übertragung ... 685

KMS-Schlüsselverwaltung ... 685
Identity and Access Management ... 686
Zielgruppe ... 687
Authentifizierung mit Identitäten ... 687
Verwalten des Zugriffs mit Richtlinien ... 689
Wie funktioniert EBS mit IAM ... 690
IAM-Beispielrichtlinien ... 696
Fehlerbehebung ... 716
Compliance-Validierung ... 718
Datenstabilität ... 718
Überwachen ... 720
Amazon CloudWatch ... 721
Metriken für Amazon-EBS-Volumes ... 721
Metriken für Amazon EBS-Snapshots ... 749
Metriken für Nitro-Instances ... 749
Metriken für die schnelle Snapshot-Wiederherstellung ... 755
Diagramme der Amazon-EC2-Konsole ... 756
Amazon EventBridge ... 758
EBS-Volume-Ereignisse ... 759
Ereignis zur Initialisierung des EBS-Volumes ... 765
Ereignisse der EBS-Volume-Änderung ... 766
EBS-Snapshot-Ereignisse ... 766
Archivereignisse von EBS-Snapshots ... 775
EBS – schnelle Snapshot-Wiederherstellungsereignisse ... 775
Verwenden AWS Lambda um Ereignisse zu verarbeiten EventBridge ... 776
Detaillierte Leistungsstatistiken von EBS ... 780
Statistiken ... 781
Auf die Statistiken zugreifen ... 783
Amazon GuardDuty ... 785
Fakturierungs- und Nutzungsberichte ... 786
-Snapshots ... 786
Volume-Speicher ... 787
Bereitgestellte Leistung ... 788
Direkte EBS-APIs ... 789
Schnelle Snapshot-Wiederherstellung (FSR) ... 790
Inventarisieren Sie Ihre EBS-Volumes ... 790

Datenträger 791
I/O Leistung 793
Inhalt Ihrer EBS-Datenvolumes 794
-Snapshots 795
Inhalt Ihrer EBS-Snapshots 795
Kontingente 797
Dokumentverlauf 813
..... dcccxxvi

Was ist Amazon Elastic Block Store?

Amazon Elastic Block Store (Amazon EBS) bietet skalierbare, leistungsstarke Blockspeicherressourcen, die mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwendet werden können. Mit Amazon Elastic Block Store können Sie die folgenden Blockspeicherressourcen erstellen und verwalten:

- Amazon EBS-Volumes – Dies sind Speichervolumes, die Sie Amazon-EC2-Instances zuordnen. Nachdem Sie ein Volume an eine Instance angehängt haben, können Sie es auf dieselbe Weise verwenden, wie Sie eine an einen Computer angeschlossene lokale Festplatte verwenden würden, beispielsweise um Dateien zu speichern oder Anwendungen zu installieren.
- Amazon-EBS-Snapshots – Dies sind zeitpunktgenaue Backups von Amazon-EBS-Volumes, die unabhängig vom Volume selbst bestehen bleiben. Sie können Snapshots erstellen, um die Daten auf Ihren Amazon-EBS-Volumes zu sichern. Sie können dann jederzeit neue Volumes aus diesen Snapshots wiederherstellen.

Themen

- Features von Amazon EBS
- Zugehörige Services
- Zugreifen auf Amazon EBS
- Preisgestaltung

Features von Amazon EBS

Amazon EBS bietet die folgenden Funktionen und Vorteile:

- Mehrere Volume-Typen — Amazon EBS bietet mehrere Volume-Typen, mit denen Sie die Speicherleistung und die Kosten für eine Vielzahl von Anwendungen optimieren können. Volumetypen werden in zwei Hauptkategorien unterteilt: SSD-backed Speicher für transaktionale Workloads und HDD-backed Speicher für durchsatzintensive Workloads.
- Skalierbarkeit — Sie können Amazon EBS-Volumes mit Kapazitäts- und Leistungsspezifikationen erstellen, die Ihren Anforderungen entsprechen. Wenn sich Ihre Anforderungen ändern, können Sie Elastic Volumes-Operationen verwenden, um die Kapazität dynamisch zu erhöhen oder die Leistung ohne Ausfallzeiten zu optimieren.

- Sicherung und Wiederherstellung — Verwenden Sie Amazon EBS-Snapshots, um die auf Ihren Volumes gespeicherten Daten zu sichern. Sie können diese Snapshots dann verwenden, um Volumes sofort wiederherzustellen oder Daten zwischen AWS Konten, AWS Regionen oder Availability Zones zu migrieren.
- Datenschutz — Verwenden Sie die Amazon EBS-Verschlüsselung, um Ihre Amazon EBS-Volumes und Amazon EBS-Snapshots zu verschlüsseln. Verschlüsselungsvorgänge finden auf den Servern statt, die Amazon EC2-Instances hosten. Dadurch wird die Sicherheit sowohl der Daten im Ruhezustand als auch der Daten bei der Übertragung zwischen einer Instance und dem zugehörigen Volume sowie nachfolgenden Snapshots gewährleistet.
- Datenverfügbarkeit und Beständigkeit — io2 Block Express-Volumes bieten eine Zuverlässigkeit von 99,999% bei einer jährlichen Ausfallrate von 0,001%. Andere Datenträgertypen bieten eine Haltbarkeit von 99,8% bis 99,9% bei einer jährlichen Ausfallrate von 0,1% bis 0,2%. Darüber hinaus werden Volumendaten automatisch auf mehrere Server in einer Availability Zone repliziert, um Datenverlust durch den Ausfall einer einzelnen Komponente zu verhindern.
- Datenarchivierung — EBS Snapshots Archive bietet eine kostengünstige Speicherebene für die Archivierung vollständiger Point-in-Time-Kopien von EBS-Snapshots. Verwenden Sie Archive, wenn Sie Snapshots aus behördlichen Gründen, zur Einhaltung gesetzlicher Vorschriften oder zu zukünftigen Projektveröffentlichungen mindestens 90 Tage lang aufbewahren müssen.

Zugehörige Services

Amazon EBS arbeitet mit den folgenden Diensten zusammen:

- Amazon Elastic Compute Cloud — Ein Service, mit dem Sie virtuelle Maschinen (Amazon EC2-Instances) in der AWS Cloud starten und verwalten können. Sie können EBS-Volumes an diese Instances anhängen und sie auf die gleiche Weise verwenden, wie Sie eine lokale Festplatte verwenden würden, beispielsweise um Dateien zu speichern oder Anwendungen zu installieren. Weitere Informationen finden Sie unter Was ist Amazon EC2?
- AWS Key Management Service— Ein verwalteter Dienst, mit dem Sie kryptografische Schlüssel erstellen und verwalten können. Sie können AWS KMS kryptografische Schlüssel verwenden, um die auf Ihren Amazon EBS-Volumes und in Ihren Amazon EBS-Snapshots gespeicherten Daten zu verschlüsseln. Weitere Informationen finden Sie unter So verwendet Amazon EBS. AWS KMS
- Amazon Data Lifecycle Manager — Ein verwalteter Service, der die Erstellung, Aufbewahrung und Löschung von EBS-Snapshots und AMIs automatisiert. EBS-backed Sie können Amazon Data Lifecycle Manager verwenden, um Backups für Ihre Amazon EBS-Volumes und Amazon EC2-

Instances zu automatisieren. Weitere Informationen finden Sie unter Automatisieren Sie Backups mit Amazon Data Lifecycle Manager.

- Direkte EBS-APIs — Ein Service, mit dem Sie EBS-Snapshots erstellen, Daten direkt in Ihre Snapshots schreiben, Daten aus Ihren Snapshots lesen und die Unterschiede oder Änderungen zwischen zwei Snapshots identifizieren können. Weitere Informationen finden Sie unter Verwenden von EBS-Direct-APIs für den Zugriff auf den Inhalt eines EBS-Snapshots.
- Papierkorb — Ein Datenwiederherstellungsdienst, mit dem Sie versehentlich gelöschte EBS-Snapshots und AMIs wiederherstellen können. EBS-backed Weitere Informationen finden Sie unter Papierkorb.

Zugreifen auf Amazon EBS

Sie können Ihre Amazon EBS-Ressourcen mithilfe der folgenden Schnittstellen erstellen und verwalten:

Amazon EC2-Konsole

Eine Weboberfläche zum Erstellen und Verwalten von Volumes und Snapshots. Wenn Sie sich für ein AWS Konto angemeldet haben, können Sie unter auf die Amazon EC2-Konsole zugreifen. https://console.aws.amazon.com/ec2/

AWS Command Line Interface

Ein Befehlszeilentool, mit dem Sie Amazon EBS-Ressourcen mithilfe von Befehlen in Ihrer Befehlszeilen-Shell verwalten können. Es wird auf Windows, Mac und Linux unterstützt. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch und in den ec2-Befehlen. https://docs.aws.amazon.com/cli/latest/reference/ec2/

AWS -Tools für PowerShell

Eine Reihe von PowerShell Modulen, die es Ihnen ermöglichen, Operationen auf Ihren Amazon EBS-Ressourcen von der PowerShell Befehlszeile aus zu skripten. Weitere Informationen finden Sie im AWS -Tools für PowerShell Benutzerhandbuch und in der AWS -Tools für PowerShell Cmdlet-Referenz.

CloudFormation

Ein vollständig verwalteter AWS Dienst, mit dem Sie wiederverwendbare JSON- oder YAML-Vorlagen erstellen können, die Ihre AWS Ressourcen beschreiben. Anschließend werden diese

Ressourcen für Sie bereitgestellt und konfiguriert. Weitere Informationen finden Sie im AWS CloudFormation -Benutzerhandbuch.

Amazon EC2-Abfrage-API

Die Amazon EC2-Abfrage-API stellt HTTP- oder HTTPS-Anfragen bereit, die das HTTP-Verb `GET` oder `POST` und einen benannten Abfrageparameter verwenden. `Action` Weitere Informationen finden Sie in der Amazon EC2-API-Referenz.

AWS SDKs

Language-specific APIs, mit denen Sie Anwendungen erstellen können, die in AWS Dienste integriert sind. AWS SDKs sind für viele gängige Programmiersprachen verfügbar. Weitere Informationen finden Sie unter Tools, auf AWS denen Sie aufbauen können.

Preisgestaltung

Bei Amazon EBS bezahlen Sie nur für das, was Sie tatsächlich nutzen. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Für Amazon EBS einrichten

Führen Sie die Aufgaben in diesem Abschnitt aus, um sich für die Arbeit mit Amazon EBS-Ressourcen einzurichten.

Aufgaben

- Melden Sie sich für eine an AWS-Konto
- (Optional) Erstellen und verwenden Sie einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung
- (Optional) Aktivieren Sie die Blockierung des öffentlichen Zugriffs für Amazon EBS-Snapshots

Melden Sie sich für eine an AWS-Konto

Um damit zu beginnen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen einer AWS-Konto finden Sie AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch unter Erste Schritte mit einer.

(Optional) Erstellen und verwenden Sie einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung

Die Amazon EBS-Verschlüsselung ist eine Verschlüsselungslösung, die AWS KMS kryptografische Schlüssel verwendet, um Ihre Amazon EBS-Volumes und Amazon EBS-Snapshots zu verschlüsseln. Amazon EBS erstellt automatisch einen eindeutigen AWS verwalteten KMS-Schlüssel für die Amazon EBS-Verschlüsselung in jeder Region. Der KMS-Schlüssel hat den Alias `aws/ebs`. Sie können den Standard-KMS-Schlüssel nicht rotieren oder seine Berechtigungen verwalten. Für mehr Flexibilität und Kontrolle über den KMS-Schlüssel, der für die Amazon EBS-Verschlüsselung verwendet wird, könnten Sie erwägen, einen vom Kunden verwalteten Schlüssel zu erstellen und zu verwenden.

Um einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung zu erstellen und zu verwenden

1. Erstellen Sie einen KMS-Schlüssel für die symmetrische Verschlüsselung.
2. Wählen Sie den KMS-Schlüssel als Standard-KMS-Schlüssel für die Amazon EBS-Verschlüsselung aus.

3. Erteilen Sie Benutzern die Erlaubnis, den KMS-Schlüssel für die Amazon EBS-Verschlüsselung zu verwenden.

(Optional) Aktivieren Sie die Blockierung des öffentlichen Zugriffs für Amazon EBS-Snapshots

Um zu verhindern, dass Ihre Snapshots öffentlich freigegeben werden, können Sie das Blockieren des öffentlichen Zugriffs auf Snapshots aktivieren. Nachdem Sie das Blockieren des öffentlichen Zugriffs auf Snapshots in einer Region aktiviert haben, wird jeder Versuch, Snapshots in dieser Region öffentlich freizugeben, automatisch blockiert. Dies hilft Ihnen dabei, die Sicherheit Ihrer Snapshots zu verbessern und Ihre Snapshot-Daten vor unbefugtem oder unbeabsichtigtem Zugriff zu schützen.

Weitere Informationen finden Sie unter Sperren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots.

Console

So aktivieren Sie das Blockieren des öffentlichen Zugriffs für Snapshots

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard aus und wählen Sie dann unter Kontoattribute (auf der rechten Seite) Datenschutz und Sicherheit.
3. Wählen Sie im Abschnitt Blockieren des öffentlichen Zugriffs auf EBS-Snapshots die Option Verwalten.
4. Wählen Sie Öffentlichen Zugriff blockieren und anschließend eine der folgenden Optionen:
   - Blockieren des gesamten öffentlichen Zugriffs – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
   - Blockieren der neuen öffentlichen Freigabe – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.
5. Wählen Sie Aktualisieren aus.

AWS CLI

So aktivieren Sie das Blockieren des öffentlichen Zugriffs für Snapshots

Verwenden Sie den Befehl enable-snapshot-block-public-access. Geben Sie für `--state` einen der folgenden Werte an:

- `block-all-sharing` – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
- `block-new-sharing` – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

```
aws ec2 enable-snapshot-block-public-access --state block-new-sharing
```

PowerShell

So aktivieren Sie das Blockieren des öffentlichen Zugriffs für Snapshots

Verwenden Sie das cmdlet Enable-EC2SnapshotBlockPublicAccess. Geben Sie für `-State` einen der folgenden Werte an:

- `block-all-sharing` – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
- `block-new-sharing` – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

```
Enable-EC2SnapshotBlockPublicAccess -State block-new-sharing
```

Amazon EBS-Volumes

Ein Amazon EBS-Volume ist ein robustes Speichergerät auf Blockebene, das Sie Ihren Instances anfügen können. Nachdem Sie einer Instance ein Volume angefügt haben, können Sie es wie eine echte Festplatte verwenden. EBS-Volumes sind flexibel. Bei Volumes der aktuellen Generation, die Instance-Typen der aktuellen Generation zugeordnet sind, können Sie die Größe dynamisch erhöhen, die bereitgestellte IOPS-Kapazität modifizieren und den Volume-Typ für aktive bzw. produktive Volumes ändern.

Sie können EBS-Volumes als primären Speicher für Daten verwenden, die häufige aktualisiert werden müssen, z. B. als Systemlaufwerk für eine Instance oder als Speicher für eine Datenbankanwendung. Außerdem können Sie sie für durchsatzintensive Anwendungen verwenden, die fortlaufend Datenträgerscans durchführen. EBS-Volumes bleiben unabhängig von der Betriebsdauer einer einzelnen EC2-Instance erhalten.

Sie können mehrere EBS-Volumes an eine einzelne Instance anfügen. Volume und Instance müssen sich in derselben Availability Zone befinden. Je nach Volume und Instance-Typ können Sie Multi-Attach damit ein Volume auf mehreren Instances gleichzeitig mounten.

Amazon EBS bietet die folgenden Volume-Typen: Allzweck-SSD (`gp2` und `gp3`), Bereitgestellte IOPS-SSD (`io1` und `io2`), durchsatzoptimierte HDD (`st1`), Cold-HDD (`sc1`) und Magnetfestplatte (`standard`). Diese unterscheiden sich bei den Leistungsmerkmalen und im Preis, sodass Sie die Speicherleistung und -kosten an die Anforderungen Ihrer Anwendungen anpassen können. Weitere Informationen finden Sie unter Amazon EBS-Volume-Typen.

Ihr Konto hat ein Limit für den gesamten Speicherplatz, der Ihnen zur Verfügung steht. Weitere Informationen zu diesen Limits und dazu, wie Sie eine Erhöhung dieser Limits anfordern können, finden Sie unter Endpunkte und Kontingente von Amazon EBS.

Ein verwaltetes EBS-Volume wird von einem Serviceanbieter wie Amazon EKS Auto Mode verwaltet. Sie können die Einstellungen eines verwalteten EBS-Volumes nicht direkt ändern. Verwaltete EBS-Volumes werden durch einen Wahr-Wert im Feld Verwaltet identifiziert. Weitere Informationen finden Sie unter Von Amazon EC2 verwaltete Instances.

Weitere Informationen zu Preisen finden Sie unter Amazon EBS-Preise.

Inhalt

- Funktionen und Vorteile von Amazon EBS-Volumes

- Amazon EBS-Volume-Typen
- Einschränkungen für Amazon-EBS-Volumes
- Amazon-EBS-Volumes und NVMe
- Lebenszyklus von Amazon EBS-Volumes
- Ersetzen Sie ein Amazon EBS-Volume mithilfe eines Snapshots
- Statusüberprüfungen des Amazon EBS-Volumes
- Fehlertests auf Amazon EBS

Funktionen und Vorteile von Amazon EBS-Volumes

EBS-Volumes bieten Vorteile, die von Instance-Speicher-Volumes nicht bereitgestellt werden.

Vorteile

- Datenverfügbarkeit
- Datenpersistenz
- Datenverschlüsselung
- Datensicherheit
- -Snapshots
- Flexibilität

Datenverfügbarkeit

Wenn Sie ein Amazon EBS-Volume erstellen, wird es in automatisch in seiner Availability Zone repliziert. Beim Ausfall irgendeiner Hardwarekomponente lässt sich dadurch ein Datenverlust verhindern. Sie können ein EBS-Volume jeder EC2-Instance in derselben Availability Zone zuweisen. Nach dem Anfügen eines Volumes erscheint es als natives Blockgerät ähnlich einer Festplatte oder einem anderen physischen Gerät. Zu diesem Zeitpunkt kann die Instance mit dem Volume wie mit einem lokalen Laufwerk interagieren. Sie können eine Verbindung zur Instance herstellen und das EBS-Volume mit einem Dateisystem formatieren, z. B. `Ext4` für eine Linux-Instance oder `NTFS` für eine Windows-Instance, und dann Anwendungen installieren.

Wenn Sie mehrere Volumes an ein von Ihnen benanntes Gerät anschließen, können Sie Daten auf die Volumes verteilen, um die Durchsatzleistung zu erhöhen I/O .

Sie können `io2` EBS-Volumes an `io1` bis zu 16 Nitro-based Instances anhängen. Weitere Informationen finden Sie unter Hängen Sie ein EBS-Volume mit mehreren EC2-Instances an Multi-Attach. Im Gegensatz dazu können Sie einer einzelnen Instance ein EBS-Volume zuweisen.

Sie können Überwachungsdaten für Ihre EBS-Volumes, einschließlich Root-Geräte-Volumes für EBS-backed Instances, ohne zusätzliche Kosten abrufen. Weitere Informationen zur Überwachung von Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS. Informationen zum Verfolgen des Status Ihrer Volumes finden Sie unter EventBridge Amazon-Ereignisse für Amazon EBS.

Datenpersistenz

EBS-Volumes sind Speicher außerhalb der Instances. Sie bestehen unabhängig von der Instance. Sie bezahlen so lange für die Nutzung des Volumes, wie die Daten bestehen.

EBS-Volumes, die an eine aktive Instance angefügt sind, können automatisch mit intakten Daten von der Instance getrennt werden, wenn die Instance beendet wird. Deaktivieren Sie hierzu das Kontrollkästchen Delete on Termination (Bei Beenden löschen), wenn Sie EBS-Volumes für Ihre Instance auf der EC2-Konsole konfigurieren. Das Volume kann dann einer neuen Instance hinzugefügt werden, sodass Sie schnell erneut auf die Daten zugreifen können. Wenn das Kontrollkästchen für Delete on Termination (Bei Beenden löschen) aktiviert ist, werden die Volumes bei der Beendigung der EC2-Instance gelöscht. Wenn Sie eine EBS-backed Instance verwenden, können Sie diese Instance anhalten und neu starten, ohne dass dies Auswirkungen auf die auf dem angehängten Volume gespeicherten Daten hat. Das Volume bleibt während des Neustarts angefügt. Dies ermöglicht Ihnen, Daten auf dem Volume unbegrenzt zu verarbeiten und zu speichern. Dabei werden die Verarbeitungs- und Speicherressourcen nur dann genutzt, wenn dies erforderlich ist. Die Daten bleiben auf dem Volume bestehen, bis es explizit gelöscht wird. Der physische Blockspeicher, der von gelöschten EBS-Volumes verwendet wird, wird mit Nullen oder kryptografisch pseudozufälligen Daten überschrieben, bevor er einem neuen Volume zugewiesen wird. Falls Sie mit vertraulichen Daten arbeiten, sollten Sie diese Daten manuell verschlüsseln oder auf einem mit Amazon EBS-Verschlüsselung geschützten Volume speichern. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung.

Standardmäßig wird das EBS-Stamm-Volume, das beim Start einer Instance erstellt und ihr angefügt wird, beim Beenden dieser Instance gelöscht. Sie können dieses Verhalten ändern, indem Sie beim Start der Instance den Wert des Flag `DeleteOnTermination` in `false` ändern. Die Änderung dieses Werts sorgt dafür, dass das Volume auch nach dem Beenden der Instance weiterhin besteht. Damit können Sie das Volume einer anderen Instance anfügen.

Standardmäßig werden zusätzliche EBS-Volumes, die beim Start einer Instance erstellt und ihr angefügt werden, beim Beenden dieser Instance gelöscht. Sie können dieses Verhalten ändern, indem Sie beim Start der Instance den Wert des Flag `DeleteOnTermination` in `true` ändern. Dieser geänderte Wert führt zur Löschung des Volume, wenn die Instance beendet wird.

Datenverschlüsselung

Mit dem Feature Amazon EBS-Verschlüsselung erstellen Sie verschlüsselte EBS-Volumes für einfache Datenverschlüsselung. Alle EBS-Volume-Typen unterstützen Verschlüsselung. Sie können verschlüsselte EBS-Volumes verwenden, um eine Vielzahl von Verschlüsselungsanforderungen für Daten und Anwendungen im Ruhezustand zu erfüllen. regulated/audited Die Amazon EBS-Verschlüsselung verwendet 256-Bit-Algorithmen des Advanced Encryption Standard () AES-256 und eine wichtige Infrastruktur. Amazon-managed Die Verschlüsselung findet auf dem Server statt, auf dem die EC2-Instance gehostet wird, während die Daten zwischen der EC2-Instance und dem Amazon EBS-Speicher verschoben werden. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung.

Die Amazon EBS-Verschlüsselung wird AWS KMS keys bei der Erstellung verschlüsselter Volumes und aller Snapshots verwendet, die aus Ihren verschlüsselten Volumes erstellt wurden. Wenn Sie zum ersten Mal ein verschlüsseltes EBS-Volume in einer Region erstellen, wird automatisch ein standardmäßiger AWS verwalteter KMS-Schlüssel für Sie erstellt. Dieser Schlüssel wird für die Amazon EBS-Verschlüsselung verwendet, sofern Sie keinen vom Kunden verwalteten Schlüssel erstellen und verwenden. Wenn Sie Ihren eigenen, vom Kunden verwalteten Schlüssel erstellen, haben Sie mehr Flexibilität. Sie können beispielsweise Zugriffskontrollen erstellen, rotieren, deaktivieren, definieren und die zum Schutz Ihrer Daten verwendeten Verschlüsselungsschlüssel überprüfen. Weitere Informationen finden Sie im AWS Key Management Service -Entwicklerhandbuch.

Datensicherheit

Amazon-EBS-Volumes werden Ihnen als unformatierte Blockgeräte präsentiert. Diese logischen Geräte werden in der EBS-Infrastruktur erstellt und der Amazon-EBS-Service stellt sicher, dass die Geräte vor jeder (Wieder-)Verwendung durch einen Kunden logisch leer sind (d. h. die Rohblöcke werden auf Null gesetzt oder enthalten kryptografische pseudozufällige Daten).

Wenn Prozeduren erfordern, dass alle Daten mit einer bestimmten Methode gelöscht werden, entweder nach oder vor der Verwendung (oder beidem), wie z. B. in DoD 5220.22-M (National Industrial Security Program Operating Manual) oder NIST 800-88 (Guidelines for Media Sanitization),

ist das in Amazon EBS entsprechend möglich. Diese Aktivität auf Blockebene wird auf die zugrunde liegenden Speichermedien im Amazon EBS-Service übertragen.

-Snapshots

Mit Amazon EBS können Sie Snapshots (Backups) aller EBS-Volumes erstellen und eine Kopie der in dem Volume enthaltenen Daten an Amazon S3 übertragen, wo sie redundant in mehreren Availability Zones gespeichert werden. Das Volume muss nicht an eine laufende Instance angefügt werden, um einen Snapshot zu erstellen. Während Daten auf ein Volume geschrieben werden, können Sie periodisch Snapshots des Volumes erstellen, um sie als Grundlage für neue Volumes oder für das Daten-Backup zu verwenden. Aus diesen Snapshots können Sie mehrere neue EBS-Volumes erstellen oder Volumes über Availability Zones hinweg verschieben. Snapshots von verschlüsselten EBS-Volumes werden automatisch verschlüsselt.

Wird aus einem Snapshot ein neues Volume erstellt, stellt dieses eine exakte Kopie des ursprünglichen Volume zum Zeitpunkt der Erstellung des Snapshot dar. Aus verschlüsselten Snapshots erstellte EBS-Volumes werden automatisch verschlüsselt. Indem Sie dabei optional eine andere Availability Zone angeben, können Sie diese Funktionalität dazu nutzen, ein Duplikat eines Volume in dieser Zone zu erstellen. Die Schnappschüsse können mit bestimmten AWS Konten geteilt oder veröffentlicht werden. Für die Erstellung von Snapshots werden Ihnen in Amazon S3 Gebühren abhängig von der Größe des Quell-Volumes berechnet. Nachfolgende Snapshots desselben Volumes sind inkrementelle Snapshots. Diese enthalten nur geänderte und neue Daten, die seit der Erstellung des letzten Snapshots auf das Volume geschrieben wurden, und Ihnen werden nur für diese geänderten und neuen Daten berechnet.

Snapshots sind inkrementelle Backups, d. h., dass nur die Blöcke des Volumes gespeichert werden, die sich seit dem letzten Snapshot geändert haben. Angenommen, Sie verfügen über ein Volume mit 100 GiB Daten, aber nur 5 GiB haben sich seit dem letzten Snapshot geändert, dann werden nur die geänderten 5 GiB auf Amazon S3 gespeichert. Snapshots werden zwar inkrementell gespeichert, der Löschvorgang von Snapshots ist jedoch so konzipiert, dass Sie nur den aktuellen Snapshot beibehalten müssen.

Um die Kategorisierung und Verwaltung der Volumes und Snapshots zu vereinfachen, können Sie sie mit Metadaten Ihrer Wahl markieren.

Zum automatischen Backup Ihrer Volumes können Sie Amazon Data Lifecycle Manager oder AWS Backup verwenden.

Flexibilität

An EBS-Volumes können Konfigurationsänderungen vorgenommen werden, während das Volume in der Produktionsumgebung aktiv ist. Sie können Art und Größe des Volumes sowie die IOPS-Kapazität ohne Serviceunterbrechung ändern. Weitere Informationen finden Sie unter Ändern Sie ein Amazon EBS-Volume mithilfe von Elastic Volumes-Vorgängen.

Amazon EBS-Volume-Typen

Amazon EBS bietet die folgenden Volume-Typen, die sich bei den Leistungsmerkmalen und im Preis unterscheiden, sodass Sie die Speicherleistung und -kosten an die Anforderungen Ihrer Anwendungen anpassen können.

> **Important**
>
> Es gibt mehrere Faktoren, die die Leistung von EBS-Volumes beeinflussen können, z. B. die Instanzkonfiguration, die I/O Eigenschaften und die Arbeitslastanforderung. Verwenden Sie für EBS optimierte Instances, um die auf einem EBS-Volume bereitgestellten IOPS vollständig zu nutzen. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-optimized.html Weitere Informationen zur optimalen Nutzung von EBS-Volumes finden Sie unter Leistung des Amazon EBS-Volumes.

Weitere Informationen zu Preisen finden Sie unter Amazon EBS-Preise.

Volume-Typen

- Volumes für Solid-State-Laufwerke (SSD)
- Volumes für Festplattenlaufwerke (HDD)
- Volumes der vorherigen Generation

Volumes für Solid-State-Laufwerke (SSD)

SSD-backed Volumes sind für transaktionale Workloads mit häufigen read/write Vorgängen und geringer I/O Größe optimiert, bei denen das dominierende Leistungsattribut IOPS ist. SSD-backed Zu den Volume-Typen gehören Allzweck-SSD und Provisioned IOPS SSD. Im Folgenden finden Sie eine Zusammenfassung der Anwendungsfälle und Eigenschaften von SSD-backed Volumes.

	Amazon EBS-SSD-Volumes für allgemeine Zwecke		Von Amazon EBS bereitgestellte IOPS-SSD-Volumes	
Volume-Typ	gp3[6]	gp2	io2Express blockieren	io1
Haltbarkeit	99,8% - 99,9% Haltbarkeit (0,1% - 0,2% jährliche Ausfallrate)		99,999% Haltbarkeit (0,001% jährliche Ausfallrate)	99,8% - 99,9% Haltbarkeit (0,1% - 0,2% jährliche Ausfallrate)
Anwendungsfälle	• Transaktionale Workloads • Virtuelle Desktops • Medium-sized, Einzelinstanzdatenbanken • Low-latency interaktive Anwendungen • Start-Volumes • Entwicklungs- und Testumgebungen		Workloads, die Folgendes erfordern: • Konsistente Latenz unter einer Millisekunde mit einer durchschnittlichen Latenz von unter 500 Mikrosekunden 5 • Dauerhafte IOPS-Leistung • Mehr als 80.000 IOPS oder 2.000 Durchsatz MiB/s	• Workloads, die eine anhaltende IOPS-Leistung oder mehr als 16 000-IOPS erfordern • I/O-intensive Datenbank-Workloads
Volume-Größe	1 GiB - 64 TiB	1 GiB – 16 TiB	4 GiB – 64 TiB	4 GiB – 16 TiB
Max. IOPS	80.000 (325,6 KiB 4) I/O	16.000 (16 KiB 4) I/O	256.000 (316 KiB I/O 4)	64.000 (16 KiB 4) I/O

	Amazon EBS-SSD-Volumes für allgemeine Zwecke		Von Amazon EBS bereitgestellte IOPS-SSD-Volumes	
Maximaler Durchsatz	2.000 MiB/s	250 MiB/s [1]	4.000 MiB/s	1.000 MiB/s [2]
Amazon EBS Multi-attach	Nicht unterstützt		Unterstützt	
NVMe-Reservierungen	Nicht unterstützt		Unterstützt	Unterstützt
Startvolume	Unterstützt			

[1] Die Durchsatzgrenze liegt je nach Volumengröße zwischen 128 MiB/s und 250 MiB/s. Weitere Informationen finden Sie unter `GP2-Volumen-Leistung`. Volumes, die vor dem 3. Dezember 2018 erstellt und die seit der Erstellung nicht geändert wurden, erreichen möglicherweise nicht die volle Leistung, es sei denn, Sie ändern das Volume.

[2] Um einen maximalen Durchsatz von 1.000 zu erreichen MiB/s, muss das Volume mit 64.000 IOPS bereitgestellt und an eine Instance angehängt werden. Nitro-based Volumes, die vor dem 6. Dezember 2017 erstellt und die seit der Erstellung nicht geändert wurden, erreichen möglicherweise nicht die volle Leistung, es sei denn, Sie ändern das Volume.

[3] Nitro-based Instances unterstützen Volumes, die mit bis zu 256.000 IOPS bereitgestellt werden. Andere Instance-Typen können an Volumes angehängt werden, die mit bis zu 64 000 IOPS bereitgestellt werden, können aber nur bis zu 32 000 IOPS erreichen.

[4] Stellt die I/O Größe dar, die erforderlich ist, um die maximale IOPS innerhalb der Durchsatzgrenze des Volumes zu erreichen.

[5] `io2` Block Express-Volumes sind so konzipiert, dass sie bei I/O 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten.

[6] Auf Outposts unterstützen gp3-Volumes Größen bis zu 16 TiB, IOPS bis zu 16.000 und einen Durchsatz von bis zu 1.000. MiB/s

Weitere Informationen zu den SSD-backed Volume-Typen finden Sie unter den folgenden Links:

- Amazon EBS-SSD-Volumes für allgemeine Zwecke
- Von Amazon EBS bereitgestellte IOPS-SSD-Volumes

Volumes für Festplattenlaufwerke (HDD)

HDD-backed Volumes sind für große Streaming-Workloads optimiert, bei denen das dominierende Leistungsattribut der Durchsatz ist. Zu den HDD-Volume-Typen gehören Durchsatzoptimierte HDD und Cold-HDD. Im Folgenden finden Sie eine Zusammenfassung der Anwendungsfälle und Eigenschaften von HDD-backed Volumes.

	Durchsatzoptimierte HDD-Volumes	Cold-HDD-Volumes
Volume-Typ	`st1`	`sc1`
Haltbarkeit	99,8% - 99,9% Haltbarkeit (0,1% - 0,2% jährliche Ausfallrate)	
Anwendungsfälle	• Big Data • Data Warehouses • Protokollverarbeitung	• Throughput-oriented Speicher für Daten, auf die selten zugegriffen wird • Szenarien, in denen niedrigste Speicherkosten wichtig sind
Volume-Größe	125 GiB – 16 TiB	
Max. IOPS pro Volume (1 MiB) I/O	500	250
Max. Durchsatz pro Volume	500 MiB/s	250 MiB/s
Amazon EBS Multi-attach	Nicht unterstützt	

	Durchsatzoptimierte HDD-Volumes	Cold-HDD-Volumes
Startvolume	Nicht unterstützt	

Weitere Informationen zu Festplattenlaufwerken (HDD) finden Sie unter Amazon EBS-Volumes: Durchsatzoptimierte HDD- und Cold HDD-Volumes.

Volumes der vorherigen Generation

Magnetische (`standard`) Volumes sind Volumes früherer Generationen, die von magnetischen Laufwerken gestützt werden. Sie können für Workloads mit kleinen Datensätzen verwenden werden, bei denen selten auf Daten zugegriffen wird und die Leistung nicht von vorrangiger Bedeutung ist. Diese Volumes bieten durchschnittlich ca. 100 I/O-Vorgänge pro Sekunde und einer Spitzenleistung bis zu Hunderten IOPS. Ihre Größe kann 1 GiB bis 1 TiB betragen.

> **Tip**
>
> Magnetfestplatten sind ein Volume-Typ der vorherigen Generation. Wenn Sie eine höhere Leistung oder Leistungskonstanz benötigen, als die Volumes der vorherigen Generation bieten können, empfehlen wir, einen der Volume-Typen der aktuellen Generation zu verwenden.

Die folgende Tabelle beschreibt EBS-Volume-Typen der früheren Generation.

	Magnetic
Volume-Typ	`standard`
Anwendungsfälle	Workloads mit seltenem Datenzugriff
Volume-Größe	1 TiB GiB-1
Max. IOPS pro Volume	40 – 200
Max. Durchsatz pro Volume	40—90 MiB/s
Startvolume	Unterstützt

Amazon EBS-SSD-Volumes für allgemeine Zwecke

Allzweck-SSD-Volumes (gp2 und gp3) werden von Solid-State-Laufwerken (SSDs) unterstützt. Diese bieten ein günstiges Preis-Leistungs-Verhältnis für ein breites Spektrum an Transaktions-Workloads. Dazu gehören virtuelle Desktops, mittelgroße Einzel-Instance-Datenbanken, latenzempfindliche interaktive Anwendungen, Entwicklungs- und Testumgebungen sowie Boot-Volumes. Wir empfehlen diese Volumes für die meisten Workloads.

Amazon EBS bietet die folgenden Arten von Allzweck-SSD-Volumes an:

Typen

- Allzweck-SSD-Volumes (gp3)
- Allzweck-SSD-Volumes (gp2)

Allzweck-SSD-Volumes (gp3)

Allzweck-SSD-Volumes (gp3) sind die neueste Generation von Allzweck-SSD-Volumes und das kostengünstigste SSD-Volume, das von Amazon EBS angeboten wird. Dieser Volume-Typ trägt dazu bei, für die meisten Anwendungen das richtige Preis-Leistungs-Verhältnis bereitzustellen. Außerdem können Sie die Volume-Leistung unabhängig von der Volume-Größe skalieren. Das bedeutet, dass Sie die erforderliche Leistung bereitstellen können, ohne zusätzliche Blockspeicherkapazität bereitstellen zu müssen. Darüber hinaus bieten gp3-Volumes einen um 20 % niedrigeren Preis pro GiB als Allzweck-SSD-Volumes (gp2).

gp3-Volumes bieten eine Latenz im einstelligen Millisekundenbereich und eine Datenträgerbeständigkeit von 99,8 bis 99,9 Prozent bei einer jährlichen Ausfallrate (AFR) von nicht mehr als 0,2 Prozent, was einem Maximum von zwei Volumenausfällen pro 1.000 laufenden Volumes über einen Zeitraum von einem Jahr entspricht. AWS konzipiert GP3-Volumes so, dass sie in 99 Prozent der Fälle die von ihnen bereitgestellte Leistung bereitstellen.

> **Tip**
>
> Für latenzempfindliche Workloads empfehlen wir die Verwendung von io2 Block Express-Volumes. `io2` Block Express-Volumes sind so konzipiert, dass sie bei 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten. I/O `io2` Block Express-Volumes bieten im Vergleich zu Allzweck-Volumes auch eine bessere Ausreißerlatenz, wodurch die Häufigkeit von I/Os Überschreitungen von 800 Mikrosekunden um mehr als das

Zehnfache reduziert wird. Weitere Informationen finden Sie unter Bereitgestellte IOPS SSD (io2) Block Express-Volumes .

Inhalt

- gp3-Volume-Leistung
- gp3-Volume-Größe
- Migrieren von gp2 zu gp3

gp3-Volume-Leistung

> **Tip**
>
> gp3-Volumes verwenden keine Burst-Leistung. Diese können unbegrenzt ihre volle bereitgestellte IOPS- und Durchsatzleistung aufrechterhalten.

IOPS-Leistung

gp3-Volumes liefern eine konsistente Basis-IOPS-Leistung von 3 000 IOPS, die im Speicherpreis enthalten ist. Sie können zusätzliche IOPS (bis zu einem Maximum von 80.000) gegen Aufpreis in einem Verhältnis von 500 IOPS pro GiB Volumegröße bereitstellen. Maximale IOPS können für Volumes ab 160 GiB bereitgestellt werden (500 IOPS pro GiB × 160 GiB = 80.000 IOPS).

Durchsatzleistung

GP3-Volumes bieten eine konsistente Basisdurchsatzleistung von 125 MiB/s, die im Speicherpreis enthalten ist. Sie können zusätzlichen Durchsatz (bis zu einem Maximum von 2.000 MiB/s) gegen eine zusätzliche Gebühr in einem Verhältnis von 0,25 MiB/s pro bereitgestellter IOPS bereitstellen. Der maximale Durchsatz kann mit 8.000 IOPS oder höher und 16 GiB oder mehr (8.000 IOPS × 0,25 pro IOPS = 2.000) bereitgestellt werden. MiB/s MiB/s

> **Note**
>
> Auf Outposts unterstützen gp3-Volumes Größen bis zu 16 TiB, IOPS bis zu 16.000 und einen Durchsatz von bis zu 1.000. MiB/s

gp3-Volume-Größe

Ein GP3-Volume kann eine Größe zwischen 1 GiB und 64 TiB haben.

Migrieren von gp2 zu gp3

Wenn Sie derzeit gp2-Volumes verwenden, können Sie Ihre Volumes mithilfe von Ändern Sie ein Amazon EBS-Volume mithilfe von Elastic Volumes-Vorgängen-Vorgängen zu gp3 migrieren. Sie können Vorgänge von Amazon EBS Elastic Volumes verwenden, um den Volume-Typ, die IOPS und den Durchsatz Ihrer vorhandenen Volumes zu ändern, ohne Ihre Amazon-EC2-Instances zu unterbrechen. Wenn Sie die Konsole verwenden, um ein Volume oder ein AMI aus einem Snapshot zu erstellen, ist Allzweck-SSD gp3 die Standardauswahl für den Volume-Typ. In anderen Fällen ist gp2 die Standardauswahl. In diesen Fällen können Sie gp3 als Datenträgertyp auswählen, anstatt gp2 zu verwenden.

Um herauszufinden, wie viel Sie durch die Migration Ihrer gp2-Volumes zu gp3 sparen können, verwenden Sie den Migrations-Kostenrechner für Amazon EBS gp2 zu gp3.

Allzweck-SSD-Volumes (gp2)

Diese bieten kostengünstigen Speicherplatz, der sich ideal für eine breite Palette von transaktionalen Workloads eignet. Bei gp2-Volumes skaliert die Leistung mit der Größe des Volumes.

> **Tip**
>
> gp3-Volumes sind die neueste Generation von Allzweck-SSD-Volumes. Sie bieten eine vorhersehbarere Leistungsskalierung und Preise, die bis zu 20 Prozent niedriger sind als gp2-Volumes. Weitere Informationen finden Sie unter Allzweck-SSD-Volumes (gp3).
> Um herauszufinden, wie viel Sie durch die Migration Ihrer gp2-Volumes zu gp3 sparen können, verwenden Sie den Migrations-Kostenrechner für Amazon EBS gp2 zu gp3.

gp2Volumes bieten eine Latenz im einstelligen Millisekundenbereich und eine Datenträgerbeständigkeit von 99,8 bis 99,9 Prozent bei einer jährlichen Ausfallrate (AFR) von nicht mehr als 0,2 Prozent, was einem Maximum von zwei Volumenausfällen pro 1.000 laufenden Volumes über einen Zeitraum von einem Jahr entspricht. AWS konzipiert gp2 Volumes so, dass sie in 99 Prozent der Fälle die von ihnen bereitgestellte Leistung bereitstellen.

Inhalt

- GP2-Volumen-Leistung
- GP2-Volumegröße

GP2-Volumen-Leistung

IOPS-Leistung

Die Baseline-IOPS-Leistung skaliert linear zwischen einem Minimum von 100 und einem Maximum von 16 000 bei einer Rate von 3 IOPS pro GiB der Volume-Größe. Die IOPS-Leistung wird wie folgt bereitgestellt:

- Volumes mit 33,33 GiB und kleiner werden mit mindestens 100 IOPS bereitgestellt.
- Volumes mit mehr als 33,33 GiB werden mit 3 IOPS pro GiB Volume-Größe bis zum Maximum von 16 000 IOPS bereitgestellt, das bei 5 334 GiB (3 x 5 334) erreicht wird.
- Volumes mit 5 334 GiB und mehr werden mit 16 000 IOPS bereitgestellt.

gp2-Volumes, die kleiner als 1 TiB sind (und mit weniger als 3 000 IOPS bereitgestellt werden), können auf 3 000 IOPS ansteigen, wenn sie über einen längeren Zeitraum benötigt werden. Die Fähigkeit eines Volumes, zu explodieren, hängt von den I/O Credits ab. Wenn die I/O Nachfrage die Grundleistung übersteigt, verbraucht das Volume I/O Credits, um das erforderliche Leistungsniveau (bis zu 3.000 IOPS) zu erreichen. Beim Burst-Betrieb werden keine I/O Credits angesammelt, sondern sie werden mit der Rate an IOPS ausgegeben, die über dem IOPS-Ausgangswert verbraucht wird (Ausgabenrate = Burst-IOPS — Baseline-IOPS). Je mehr I/O Credits ein Volume angesammelt hat, desto länger kann es seine Burst-Performance aufrechterhalten. Sie können die Burst-Dauer wie folgt berechnen:

$$\text{Burst duration} = \frac{\text{(I/O credit balance)}}{\text{(Burst IOPS) - (Baseline IOPS)}}$$

Wenn die I/O Nachfrage auf das Ausgangsleistungsniveau oder darunter fällt, beginnt das Volume, 3 I/O I/O Credits pro GiB Volume-Größe pro Sekunde zu sammeln. Für Volumes gilt ein I/O Limit von 5,4 Millionen I/O Credits, was ausreicht, um die maximale Burst-Performance von 3.000 IOPS mindestens 30 Minuten lang aufrechtzuerhalten.

> **Note**
>
> Jedes Volume erhält ein anfängliches I/O Guthaben von 5,4 Millionen I/O Credits, was einen schnellen ersten Startzyklus für Startvolumes und ein gutes Bootstrapping-Erlebnis für andere Anwendungen ermöglicht.

In der folgenden Tabelle sind beispielhafte Volume-Größen und die zugehörige Basisleistung des Volumes, die Burst-Dauer (wenn Sie mit 5,4 Millionen I/O Credits beginnen) und die Zeit aufgeführt, die benötigt wird, um ein leeres I/O Guthaben wieder aufzufüllen.

Volume-Größe (GiB)	Basisleistung (IOPS)	Burst-Dauer bei 3 000 IOPS (Sekunden)	Zeit zum Auffüllen des leeren Guthabens (Sekunden)
1 bis 33,33	100	1,862	54,000
100	300	2000	18.000
334 (Mindestgröße für maximalen Durchsatz)	1.002	2.703	5.389
750	2.250	7.200	2.400
1.000	3.000	N/A*	N/A*
5 334 (Mindestgröße für max. IOPS) und größer	16,000	N/A*	N/A*

* Wenn die Basisleistung des Volumes die maximale Burst-Leistung übersteigt, wird das Guthaben nie verbraucht.

Sie können das I/O Guthaben für ein Volume mithilfe der Amazon `BurstBalance` EBS-Metrik in Amazon überwachen. CloudWatch Diese Metrik zeigt den Prozentsatz der gp2 verbleibenden I/O Credits. Weitere Informationen finden Sie unter I/O Eigenschaften und Überwachung von Amazon EBS. Sie einen Alarm einstellen, der Sie benachrichtigt, wenn der `BurstBalance`-Wert auf ein bestimmtes Niveau fällt. Weitere Informationen finden Sie unter CloudWatch Alarme erstellen.

Durchsatzleistung

gp2Volumes bieten einen Durchsatz zwischen 128 MiB/s und 250 MiB/s, abhängig von der Volume-Größe. Die Durchsatzleistung wird wie folgt bereitgestellt:

- Volumes mit einer Größe von 170 GiB und weniger bieten einen maximalen Durchsatz von 128 MiB/s.
- Bei Volumes, die größer als 170 GiB, aber kleiner als 334 GiB sind, kann ein Burst auf einen maximalen Durchsatz von 250 GiB erreicht MiB/s werden.
- Volumes mit 334 GiB und mehr liefern 250 GiB MiB/s.

Der Durchsatz für ein gp2 Volumen kann mithilfe der folgenden Formel bis zur Durchsatzgrenze von 250 berechnet werden MiB/s:

```
Throughput in MiB/s = IOPS performance × I/O size in KiB / 1,024
```

GP2-Volumegröße

gp2-Volumes verfügen über Größen von 1 GiB bis 16 TiB. Beachten Sie, dass die Volume-Leistung linear mit der Volume-Größe skaliert.

Von Amazon EBS bereitgestellte IOPS-SSD-Volumes

Bereitgestellte IOPS-SSD-Volumes werden durch Solid-State-Laufwerke (SSDs) gestützt. Es handelt sich um Amazon EBS-Speichervolumes mit der höchsten Leistung, die für kritische und durchsatzintensive Workloads konzipiert wurden IOPS-intensive, die eine geringe Latenz erfordern. SSD-Volumes mit bereitgestellten IOPS liefern in 99,9 % der Zeit über ihre bereitgestellte IOPS-Leistung.

Amazon EBS bietet drei Arten von SSD-Volumes mit bereitgestellten IOPS:

- Bereitgestellte IOPS SSD (io2) Block Express-Volumes
- Bereitgestellte IOPS-SSD-Volumes (io1)

Bereitgestellte IOPS SSD (io2) Block Express-Volumes

io2-Block-Express-Volumes sind die nächste Generation der Amazon-EBS-Speicher-Serverarchitektur. Es wurde entwickelt, um die Leistungsanforderungen der anspruchsvollsten I/

O intensiven Anwendungen zu erfüllen, die auf Instances ausgeführt werden, die auf dem Nitro-System basieren. Mit der höchsten Haltbarkeit und niedrigsten Latenz ist Block Express ideal für die Ausführung leistungsintensiver, unternehmenskritischer Workloads wie Oracle, SAP HANA, Microsoft SQL Server und SAS Analytics.

Die Block-Express-Architektur erhöht die Leistung und Skalierung von `io2`-Volumes. Block Express-Server kommunizieren mit Nitro-based Instanzen mithilfe des Netzwerkprotokolls Scalable Reliable Datagram (SRD). Diese Schnittstelle ist in der Nitro-Karte implementiert, die für die Amazon I/O EBS-Funktion auf der Host-Hardware der Instance vorgesehen ist. Sie minimiert I/O Verzögerungen und Latenzschwankungen (Netzwerk-Jitter) und sorgt so für eine schnellere und konsistentere Leistung Ihrer Anwendungen.

`io2`-Block-Express-Volumes sind so konzipiert, dass sie eine Volume-Haltbarkeit von 99,999 % bei einer jährlichen Ausfallrate (AFR) von nicht mehr als 0,001 % bieten, was einem einzigen Volume-Ausfall pro 100 000 ausgeführten Volumes über einen Zeitraum von einem Jahr entspricht. `io2` Block Express-Volumes eignen sich für Workloads, die von einem einzigen Volume profitieren, das eine konsistente Latenz von unter einer Millisekunde bietet und höhere IOPS- und Durchsatzraten als GP3-Volumes unterstützt.

Wenn `io2` Block Express-Volumes an Nitro-based Instanzen angeschlossen sind, sind sie so konzipiert, dass sie bei 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten. I/O `io2` Block Express-Volumes bieten im Vergleich zu Allzweck-Volumes auch eine bessere Ausreißerlatenz, wodurch die Häufigkeit von I/Os Überschreitungen von 800 Mikrosekunden um mehr als das Zehnfache reduziert wird.

Themen

- Überlegungen
- Leistung

Überlegungen

- `io2`Block Express-Volumes sind in allen AWS Regionen verfügbar, einschließlich der AWS GovCloud (US) Regionen Regionen und China.
- Stand 30. April 2025 sind alle neuen und zuvor erstellten `io2` Volumes `io2` Block Express-Volumes.

- Nitro-based Instances unterstützen Volumes, die mit bis zu 256.000 IOPS bereitgestellt werden. Andere Instance-Typen können an Volumes angehängt werden, die mit bis zu 64 000 IOPS bereitgestellt werden, können aber nur bis zu 32 000 IOPS erreichen.

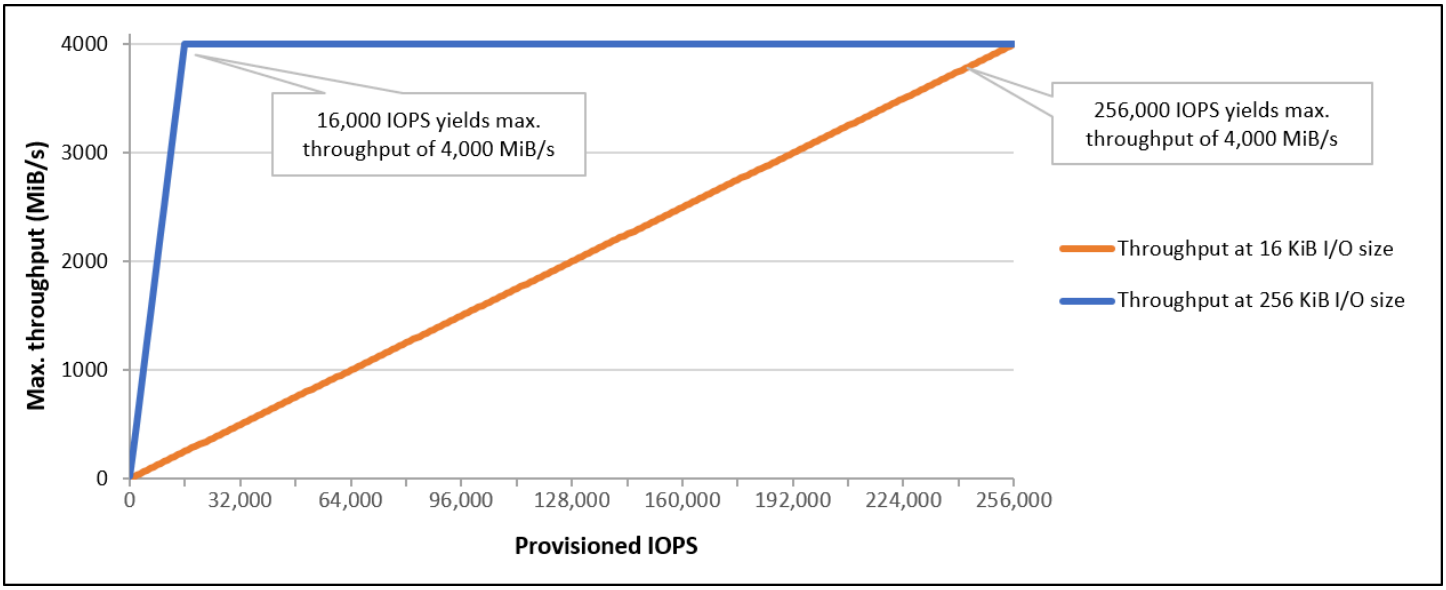
Leistung

`io2`Block Express-Volumes weisen die folgenden Eigenschaften auf:

- Durchschnittliche Latenz unter 500 Mikrosekunden bei einer Größe von 16 KiB I/O . Bessere Ausreißerlatenz im Vergleich zu Allzweck-Volumes, wodurch die Häufigkeit von I/Os Überschreitungen von 800 Mikrosekunden um mehr als das Zehnfache reduziert wird.
- Speicherkapazität bis zu 64 TiB (65.536 GiB).
- Bereitgestellte IOPS bis zu 256.000, mit einem Verhältnis von 1. 000:1. IOPS:GiB Maximale IOPS können mit Volumes ab einer Größe von 256 GiB (1 000 IOPS × 256 GiB = 256 000 IOPS) bereitgestellt werden.

> **Note**
>
> Mit Instances können Sie bis zu 256.000 IOPS erreichen. Nitro-based In anderen Instanzen können Sie bis zu 32.000 IOPS erreichen.

- Volumendurchsatz bis zu 4.000. MiB/s Der Durchsatz skaliert proportional mit einer Rate von 0,256 MiB/s pro bereitgestellter IOPS. Der maximale Durchsatz kann bei 16 000 IOPS oder höher erreicht werden.



Bereitgestellte IOPS-SSD-Volumes (io1)

Die bereitgestellten IOPS-SSD (`io1`) -Volumes sind so konzipiert, dass sie die Anforderungen von I/O-intensive Workloads, insbesondere Datenbank-Workloads, erfüllen, bei denen es auf Speicherleistung und Konsistenz ankommt. Bereitgestellte IOPS-SSD-Volumes verwenden eine konsistente IOPS-Rate, die Sie beim Erstellen des Volumes angeben. Amazon EBS stellt die Leistung 99,9 Prozent der Zeit bereit.

`io1`-Volumes sind so konzipiert, dass sie eine Volume-Haltbarkeit von 99,8 % bis 99,9 % bei einer jährlichen Ausfallrate (AFR) von nicht mehr als 0,2 % bieten, was maximal zwei Volume-Ausfällen pro 1 000 ausgeführten Volumes über einen Zeitraum von einem Jahr entspricht.

`io1`-Volumes sind für alle Amazon-EC2-Instance-Typen verfügbar.

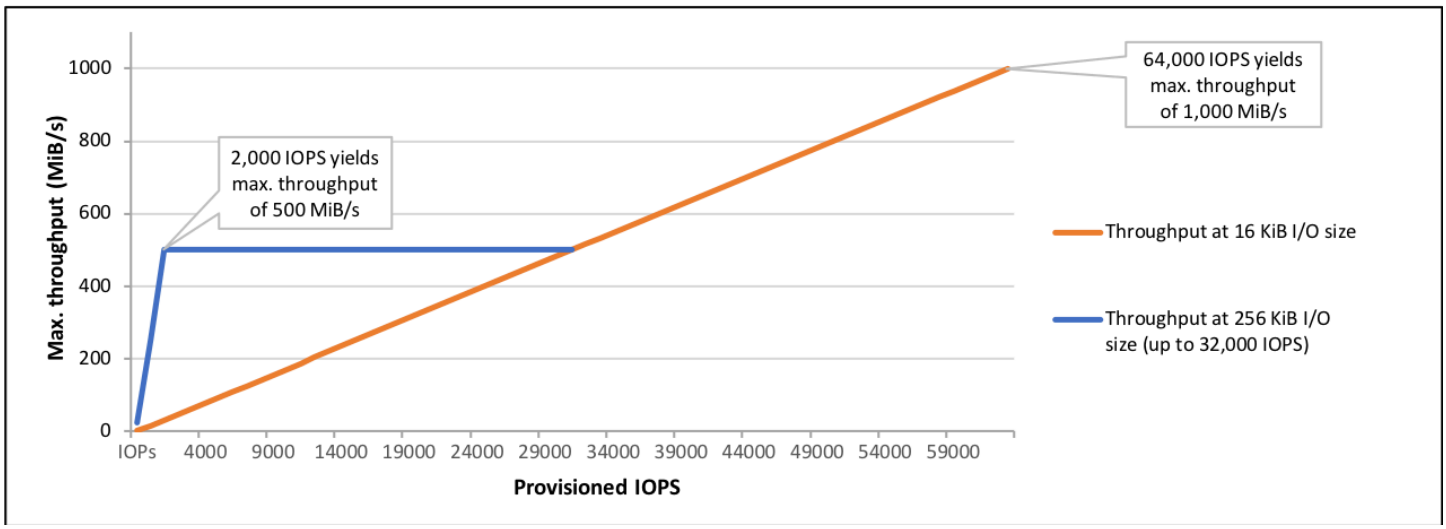
Leistung

`io1`-Volumes können eine Größe von 4 GiB bis 16 TiB aufweisen und Sie können von 100 IOPS bis zu 64 000 IOPS pro Volume bereitstellen. Das maximale Verhältnis von bereitgestellten IOPS zur angeforderten Volume-Größe (in GiB) liegt bei 50 zu 1. Beispielsweise können mit einem 100-GiB-`io1`-Volume bis zu 5 000 IOPS bereitgestellt werden.

Die maximalen IOPS können für Volumes ab 1 280 GiB (50 × 1 280 GiB = 64 000 IOPS) bereitgestellt werden.

- `io1`Volumes, die mit bis zu 32.000 IOPS bereitgestellt werden, unterstützen eine maximale I/O Größe von 256 KiB und bieten einen Durchsatz von bis zu 500. MiB/s Bei maximaler I/O Größe wird der Spitzendurchsatz bei 2.000 IOPS erreicht.
- `io1`-Volumes mit mehr als 32 000 IOPS (bis zu einem Maximum von 64 000 IOPS) führen zu einer linearen Erhöhung des Durchsatzes mit einer Rate von 16 KiB pro bereitgestellter IOPS. Beispielsweise kann ein Volume, das mit 48.000 IOPS bereitgestellt wird, einen Durchsatz MiB/s von bis zu 750 pro bereitgestellter IOPS unterstützen (16 KiB pro bereitgestellter IOPS × 48.000 bereitgestellte IOPS = 750). MiB/s
- Um den maximalen Durchsatz von 1.000 zu erreichen MiB/s, muss ein Volume mit 64.000 IOPS bereitgestellt werden (16 KiB pro bereitgestellten IOPS × 64.000 bereitgestellten IOPS = 1.000). MiB/s
- Sie können nur auf Instances bis zu 64.000 IOPS erreichen. Nitro-based In anderen Instanzen können Sie bis zu 32.000 IOPS erreichen.

Diese Leistungsmerkmale werden im folgenden Diagramm veranschaulicht:



Ihre Erfahrung pro I/O Latenz hängt von den bereitgestellten IOPS und Ihrem Workload-Profil ab. Für ein optimales I/O Latenzerlebnis sollten Sie sicherstellen, dass Sie IOPS bereitstellen, die dem I/O Profil Ihrer Arbeitslast entsprechen.

Amazon EBS-Volumes: Durchsatzoptimierte HDD- und Cold HDD-Volumes

Die von Amazon EBS bereitgestellten HDD-backed Volumes fallen in die folgenden Kategorien:

- Durchsatzoptimierte HDD – eine kostengünstige HDD für häufig aufgerufene, durchsatzintensive Workloads

- Cold HDD — Die kostengünstigste Festplatte, die für Workloads entwickelt wurde, auf die seltener zugegriffen wird.

Themen

- Einschränkungen beim Durchsatz pro Instance
- Durchsatzoptimierte HDD-Volumes
- Cold-HDD-Volumes
- Überlegungen in Bezug auf die Leistung bei Verwendung von HDD-Volumes
- Überwachen der Burst Bucket-Menge für Volumes

Einschränkungen beim Durchsatz pro Instance

Der Durchsatz für `st1`- und `sc1`-Volumes wird immer durch den kleineren der folgenden Werte bestimmt:

- Durchsatzlimits des Volumes
- Durchsatzlimits der Instance

Wie bei allen Amazon EBS-Volumes empfehlen wir, eine geeignete EBS-optimized EC2-Instance auszuwählen, um Netzwerkengpässe zu vermeiden.

Durchsatzoptimierte HDD-Volumes

Durchsatzoptimierte HDD-Volumes (`st1`) bieten kostengünstigen Magnetfestplattenspeicher, bei dem die Leistung durch den Durchsatz anstatt die IOPS definiert wird. Dieser Volume-Typ eignet sich für große, sequenzielle Workloads wie Amazon EMR, ETL, Data Warehouses und die Protokollverarbeitung. Startbare `st1`-Volumes werden nicht unterstützt.

Durchsatzoptimierte HDD-Volumes (`st1`) ähneln zwar Cold-HDD-Volumes (`sc1`), sind aber auf Daten ausgelegt, auf die häufig zugegriffen wird.

> **Note**
>
> Dieser Volume-Typ ist für Workloads mit großen, sequentiellen Workloads optimiert. Wir empfehlen Kunden mit Workloads I/O, die kleine, zufällige Nutzung von oder ausführen. I/O Amazon EBS-SSD-Volumes für allgemeine Zwecke Von Amazon EBS bereitgestellte IOPS-

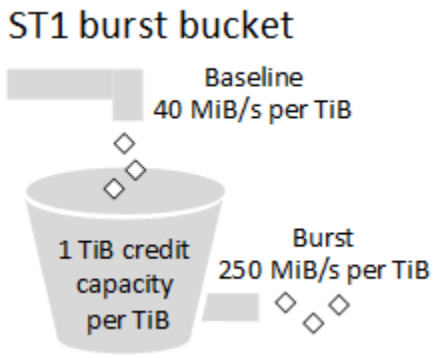
SSD-Volumes Weitere Informationen finden Sie unter Ineffizienz von Small auf der Festplatte read/writes.

Durchsatzoptimierte HDD (`st1`) -Volumes, die an EBS-optimized Instances angeschlossen sind, sind so konzipiert, dass sie eine gleichbleibende Leistung bieten und in 99 Prozent der Fälle in einem bestimmten Jahr mindestens 90 Prozent der erwarteten Durchsatzleistung liefern.

Durchsatzguthaben und Maximalleistung

Wie `gp2`, verwendet auch `st1` ein Burst-Bucket-Modell für die Leistung. Die Volumegröße bestimmt den Basisdurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der das Volume Durchsatzguthaben sammelt. Die Volumegröße bestimmt auch den Spitzendurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der Sie verfügbares Guthaben verbrauchen können. Größere Volumes haben einen höheren Basis- und Spitzendurchsatz. Je mehr Credits Ihr Volume hat, desto länger kann es I/O im Burst-Modus betrieben werden.

Im folgenden Diagramm wird das Burst-Bucket-Verhalten für `st1` dargestellt.



Der verfügbare Durchsatz eines `st1`-Volumes unterliegt Durchsatz- und Durchsatzguthabengrenzen und wird durch die folgende Formel ausgedrückt:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Bei einem `st1` 1-TB-Volume ist der Burst-Durchsatz auf 250 begrenzt MiB/s, der Bucket füllt sich bei 40 MiB/s Credits mit Credits und kann bis zu 1 TiB-worth Credits aufnehmen.

Bei größeren Volumes werden diese Grenzwerte linear skaliert, wobei der Durchsatz auf maximal 500 begrenzt ist. MiB/s Wenn der Bucket aufgebraucht ist, wird der Durchsatz auf die Ausgangsrate von 40 pro TiB begrenzt. MiB/s

Bei Volumengrößen zwischen 0,125 TiB und 16 TiB variiert der Basisdurchsatz zwischen 5 MiB/s und einer Obergrenze von 500 MiB/s, die bei 12,5 TiB wie folgt erreicht wird:

```
            40 MiB/s
12.5 TiB × ---------- = 500 MiB/s
             1 TiB
```

Der Burst-Durchsatz variiert zwischen 31 MiB/s und einer Obergrenze von 500 MiB/s, die bei 2 TiB wie folgt erreicht wird:

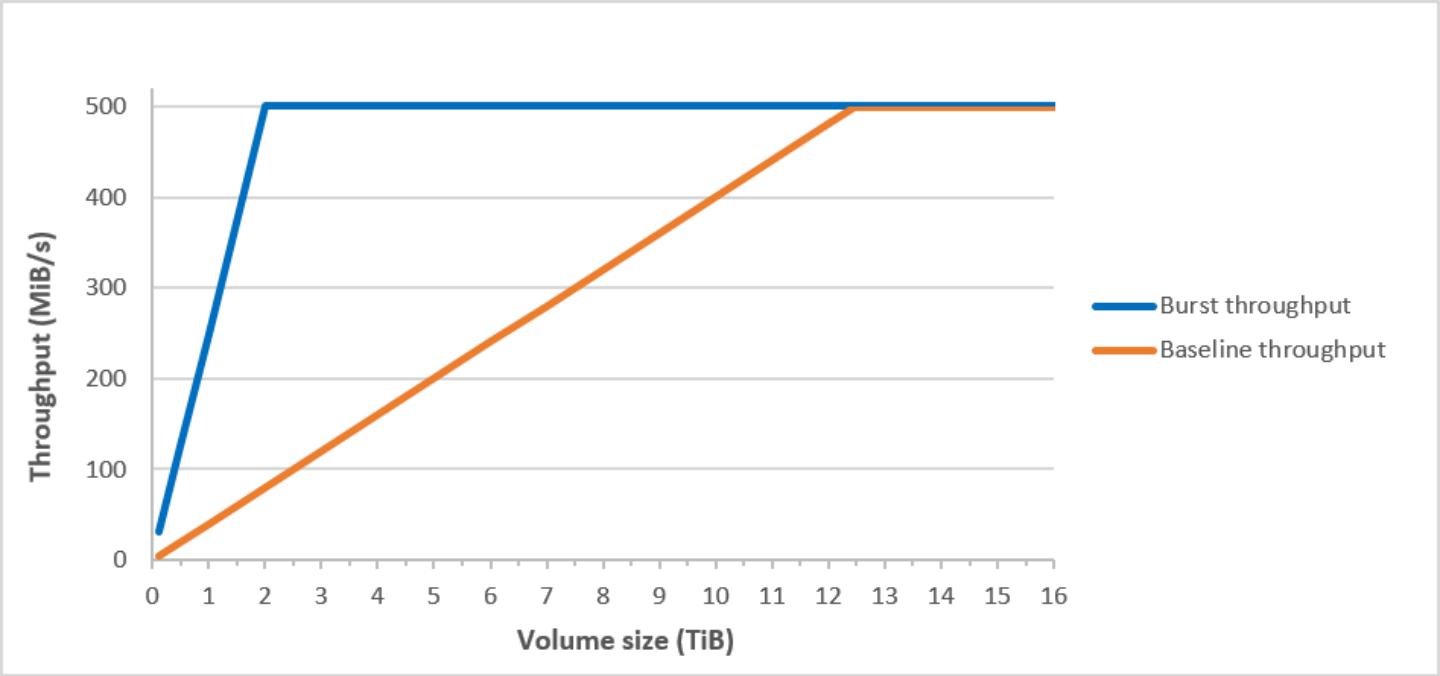
```
         250 MiB/s
2 TiB × ---------- = 500 MiB/s
          1 TiB
```

Die folgende Tabelle gibt den vollständigen Bereich von Basis- und Spitzendurchsatzwerten für `st1`.

Volumegröße (TiB)	ST1-Basisdurchsatz () MiB/s	ST1-Burst-Durchsatz () MiB/s
0.125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500

Volumegröße (TiB)	ST1-Basisdurchsatz () MiB/s	ST1-Burst-Durchsatz () MiB/s
11	440	500
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

Das folgende Diagramm stellt die Tabellenwerte dar:



> **Note**
>
> Wenn Sie einen Snapshot eines durchsatzoptimierten HDD-Volumes (`st1`) erstellen, kann die Leistung bis auf den Basiswert des Volumes abfallen, während der Snapshot generiert wird.

Informationen zur Verwendung von CloudWatch Metriken und Alarmen zur Überwachung Ihres Burst-Bucket-Guthabens finden Sie unterÜberwachen der Burst Bucket-Menge für Volumes.

Cold-HDD-Volumes

Cold-HDD-Volumes (`sc1`) bieten kostengünstigen Magnetfestplattenspeicher, bei dem die Leistung durch den Durchsatz anstatt die IOPS definiert wird. Mit einem niedrigeren Durchsatzlimit als `st1` ist `sc1` ideal für große, sequenzielle Workloads für selten verwendete Daten. Wenn Sie nur selten auf Ihre Daten zugreifen müssen und Kosten sparen möchten, bietet `sc1` kostengünstige Blockspeicherung. Startbare `sc1`-Volumes werden nicht unterstützt.

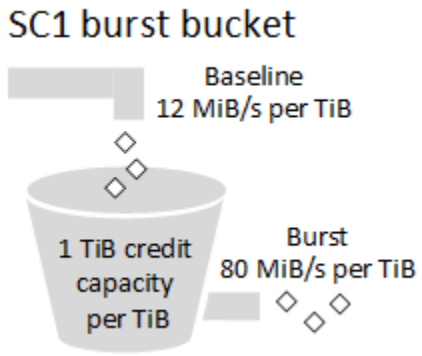
Cold-HDD-Volumes (`sc1`) ähneln zwar durchsatzoptimierten HDD-Volumes (`st1`), sind aber auf Daten ausgelegt, auf die selten zugegriffen wird.

> **Note**
>
> Dieser Volume-Typ ist für Workloads mit großen I/O, sequentiellen Workloads optimiert. Wir empfehlen Kunden mit Workloads, die kleine, zufällige I/O Nutzung durchführen. Amazon EBS-SSD-Volumes für allgemeine Zwecke Von Amazon EBS bereitgestellte IOPS-SSD-Volumes Weitere Informationen finden Sie unter Ineffizienz von Small auf der Festplatte read/writes.

Cold HDD (`sc1`) -Volumes, die an EBS-optimized Instances angeschlossen sind, sind so konzipiert, dass sie eine gleichbleibende Leistung bieten und in 99 Prozent der Fälle in einem bestimmten Jahr mindestens 90 Prozent der erwarteten Durchsatzleistung liefern.

Durchsatzguthaben und Maximalleistung

Wie `gp2`, verwendet auch `sc1` ein Burst-Bucket-Modell für die Leistung. Die Volumegröße bestimmt den Basisdurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der das Volume Durchsatzguthaben sammelt. Die Volumegröße bestimmt auch den Spitzendurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der Sie verfügbares Guthaben verbrauchen können. Größere Volumes haben einen höheren Basis- und Spitzendurchsatz. Je mehr Credits Ihr Volume hat, desto länger kann es I/O im Burst-Modus betrieben werden.



Der verfügbare Durchsatz eines `sc1`-Volumes unterliegt Durchsatz- und Durchsatzguthabengrenzen und wird durch die folgende Formel ausgedrückt:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Bei einem `sc1` 1-TB-Volume ist der Burst-Durchsatz auf 80 begrenzt MiB/s, der Bucket füllt sich bei 12 MiB/s Credits mit Credits und kann bis zu 1 TiB-worth Credits aufnehmen.

Bei größeren Volumes werden diese Grenzwerte linear skaliert, wobei der Durchsatz auf maximal 250 begrenzt ist. MiB/s Wenn der Bucket aufgebraucht ist, wird der Durchsatz auf die Ausgangsrate von 12 pro TiB begrenzt. MiB/s

Bei Volumengrößen zwischen 0,125 TiB und 16 TiB variiert der Basisdurchsatz zwischen 1,5 und einem Maximum von 192 MiB/s. MiB/s Dieser Wert wird bei 16 TiB wie folgt erreicht:

```
           12 MiB/s
16 TiB × ---------- = 192 MiB/s
            1 TiB
```

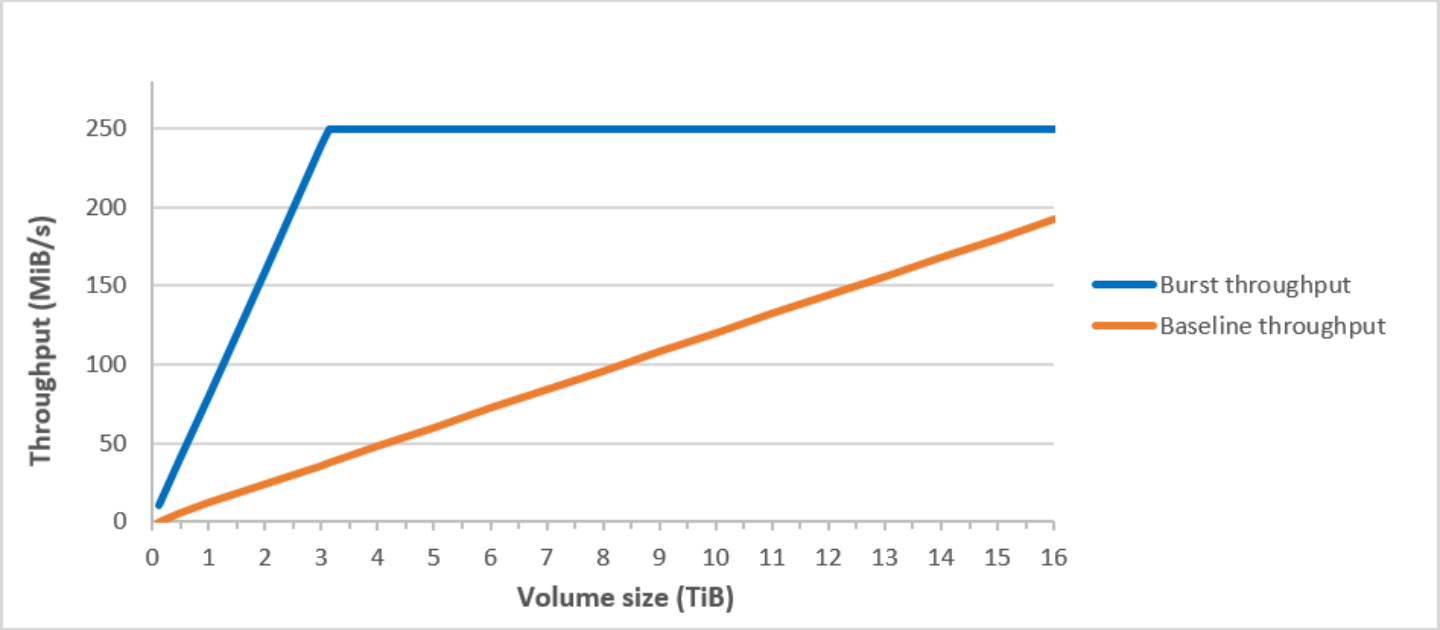
Der Burst-Durchsatz variiert zwischen 10 MiB/s und einer Obergrenze von 250 MiB/s, was bei 3,125 TiB wie folgt erreicht wird:

```
             80 MiB/s
3.125 TiB × ----------- = 250 MiB/s
              1 TiB
```

Die folgende Tabelle gibt den vollständigen Bereich von Basis- und Spitzendurchsatzwerten für a `sc1`:

Volumegröße (TiB)	SC1-Basisdurchsatz () MiB/s	SC1-Burst-Durchsatz () MiB/s
0.125	1.5	10
0,5	6	40
1	12	80
2	24	160
3	36	240
3,125	37,5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

Das folgende Diagramm stellt die Tabellenwerte dar:



> **Note**
>
> Wenn Sie einen Snapshot eines Cold-HDD-Volumes (`sc1`) erstellen, kann die Leistung bis auf den Basiswert des Volumes abfallen, während der Snapshot generiert wird.

Informationen zur Verwendung von CloudWatch Metriken und Alarmen zur Überwachung Ihres Burst-Bucket-Guthabens finden Sie unterÜberwachen der Burst Bucket-Menge für Volumes.

Überlegungen in Bezug auf die Leistung bei Verwendung von HDD-Volumes

Für optimale Durchsatzergebnisse bei der Verwendung von HDD-Volumes berücksichtigen Sie bei der Planung Ihrer Workloads folgende Punkte.

Vergleich von durchsatzoptimierter HDD und Cold-HDD

Die Bucketgrößen von `st1` und `sc1` variieren je nach Volumegröße und ein voller Bucket enthält genügend Token für eine vollständige Volumeüberprüfung. Bei größeren `st1`- und `sc1`-Volumes dauert die Volume-Überprüfung jedoch aufgrund von Durchsatzbeschränkungen pro Instance und pro Volume länger. An kleinere Instances angefügte Volumes sind auf den Durchsatz pro Instance anstatt der Durchsatzlimits von `st1` oder `sc1` begrenzt.

Beide `st1` `sc1` sind auf eine konstante Leistung von 90 Prozent des Burst-Durchsatzes in 99 Prozent der Fälle ausgelegt. Non-compliant Die Zeiträume sind ungefähr gleichmäßig verteilt und zielen auf 99 Prozent des erwarteten Gesamtdurchsatzes pro Stunde ab.

Im Allgemeinen werden Überprüfungszeiten mit dieser Formel ausgedrückt:

```
 Volume size
------------ = Scan time
 Throughput
```

Beispiel: Bei Berücksichtigung der garantierten Leistungskonsistenz und anderer Optimierungen kann ein `st1`-Kunde mit einem 5-TiB-Volume erwarten, dass eine vollständige Volume-Überprüfung in 2,91 bis 3,27 Stunden abgeschlossen wird.

- Optimale Scan-Zeit

```
   5 TiB            5 TiB
----------- = ------------------ = 10,486 seconds = 2.91 hours
 500 MiB/s     0.00047684 TiB/s
```

- Maximale Scan-Zeit

```
  2.91 hours
-------------- = 3.27 hours
 (0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time
```

Entsprechend kann ein `sc1`-Kunde mit einem 5-TiB-Volume erwarten, dass eine vollständige Volume-Überprüfung in 5,83 bis 6,54 Stunden abgeschlossen wird.

- Optimale Scan-Zeit

```
   5 TiB             5 TiB
----------- = ------------------- = 20972 seconds = 5.83 hours
 250 MiB/s     0.000238418 TiB/s
```

- Maximale Scan-Zeit

```
  5.83 hours
-------------- = 6.54 hours
 (0.90)(0.99)
```

Die folgende Tabelle zeigt ideale Überprüfungszeiten für Volumes verschiedener Größen; dabei wird von vollen Buckets und ausreichendem Instance-Durchsatz ausgegangen.

Volumegröße (TiB)	ST1-Überprüfungszeit bei Spitzenleistung (Stunden)*	SC1-Überprüfungszeit bei Spitzenleistung (Stunden)*
1	1,17	3,64
2	1,17	3,64
3	1,75	3,64
4	2,33	4,66
5	2,91	5,83
6	3,50	6,99
7	4,08	8,16
8	4,66	9,32
9	5,24	10,49
10	5,83	11,65
11	6,41	12,82
12	6,99	13,98
13	7,57	15,15
14	8,16	16,31
15	8,74	17,48
16	9,32	18,64

* Bei diesen Scanzeiten wird von einer durchschnittlichen Warteschlangentiefe (auf die nächste ganze Zahl gerundet) von vier oder mehr ausgegangen, wenn 1 MiB sequentiell ausgeführt wird. I/O

Wenn Sie eine durchsatzorientierte Arbeitslast haben, bei der Scans schnell abgeschlossen werden müssen (bis zu 500 MiB/s) oder mehrere vollständige Volumenscans pro Tag erforderlich sind, sollten Sie daher Folgendes verwenden. `st1` Wenn Sie die Kosten optimieren, relativ selten auf Ihre Daten zugegriffen wird und Sie nicht mehr als 250 MiB/s Scanleistung benötigen, verwenden Sie diese Option. `sc1`

Ineffizienz von Small auf der Festplatte read/writes

Das Leistungsmodell für `st1` und `sc1` Volumes ist für sequentielle I/Os Arbeitslasten optimiert und begünstigt Workloads mit hohem Durchsatz. Es bietet eine akzeptable Leistung bei Workloads mit gemischten IOPS- und Durchsatzraten und verhindert Workloads mit kleinen, zufälligen Arbeitslasten. I/O

Beispielsweise gilt eine I/O Anforderung von 1 MiB oder weniger als 1 MiB-Guthaben. I/O Wenn sie jedoch sequentiell I/Os sind, werden sie zu I/O 1-MiB-Blöcken zusammengeführt und zählen nur als 1 MiB-Guthaben. I/O

Überwachen der Burst Bucket-Menge für Volumes

Sie können das Burst-Bucket-Level `st1` und die `sc1` Volumes mithilfe der Amazon `BurstBalance` EBS-Metrik überwachen, die bei Amazon verfügbar ist. CloudWatch Diese Metrik zeigt die Durchsatzgutschriften für `st1` und `sc1`, die im Burst-Bucket verbleiben. Weitere Informationen zur `BurstBalance` Metrik und zu anderen Metriken im Zusammenhang I/O mit diesem Thema finden Sie unterI/O Eigenschaften und Überwachung von Amazon EBS. CloudWatch ermöglicht es Ihnen auch, einen Alarm einzustellen, der Sie benachrichtigt, wenn der `BurstBalance` Wert einen bestimmten Wert unterschreitet. Weitere Informationen finden Sie unter CloudWatch Alarme https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html erstellen.

Einschränkungen für Amazon-EBS-Volumes

Die Größe eines Amazon EBS-Volumes wird durch die Physik und Arithmetik der Blockdatenspeicherung sowie durch die Implementierungsentscheidungen der Betriebssystem- und Dateisystemdesigner eingeschränkt. AWS legt zusätzliche Beschränkungen für die Volume-Größe fest, um die Zuverlässigkeit seiner Dienste zu gewährleisten.

In den folgenden Abschnitten werden die wichtigsten Faktoren beschrieben, die die nutzbare Größe eines EBS-Volumes begrenzen. Zudem werden Empfehlungen für die Konfiguration Ihrer EBS-Volumes geboten.

Inhalt

- Speicherkapazität
- Service-Einschränkungen
- Partitionierungsschemata
- Datenblockgrößen

Speicherkapazität

Die folgende Tabelle fasst die theoretischen und implementierten Speicherkapazitäten für die am häufigsten verwendeten Systeme auf Amazon EBS zusammen, ausgehend von einer Blockgröße von 4 096 Bytes.

Partitionierungsschema	Max. adressierbare Blöcke	Theoretische max. Größe (Blöcke x Blockgröße)	Ext4-Implementierung – max. Größe*	XFS-Implementierung – max. Größe**	NTFS-Implementierung – max. Größe	Max. von EBS unterstützt
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB	1 EiB = 1024^2 TiB (50 TiB zertifiziert auf RHEL7)	500 TiB (zertifiziert auf RHEL7)	256 TiB	64 TiB †

* Ext4 Howto und Was sind die Datei- und Systemgrößenbeschränkungen für Red Hat Enterprise Linux?

** Was sind die Datei- und Systemgrößenbeschränkungen für Red Hat Enterprise Linux?

† `io2` Block Express-Volumes unterstützen für GPT-Partitionen bis zu 64 TiB. Weitere Informationen finden Sie unter Bereitgestellte IOPS SSD (io2) Block Express-Volumes .

Service-Einschränkungen

Amazon EBS abstrahiert den massiv verteilten Speicher eines Rechenzentrums zu virtuellen Festplattenlaufwerken. Für ein auf einer EC2-Instance installiertes Betriebssystem erscheint

ein verbundenes EBS-Volume wie eine physische Festplatte mit 512-Byte-Festplattensektoren. Das Betriebssystem verwaltet die Zuweisung der Datenblöcke (oder Cluster) zu diesen virtuellen Sektoren über seine Speicherverwaltungsvorrichtungen. Die Zuweisung geschieht im Einklang mit einem Volume-Partitionierungsschema, etwa einem Master Boot Record (MBR) oder einer GUID-Partitionstabelle (GPT) und innerhalb der Kapazität des installierten Dateisystems (ext4, NTFS u. dgl.).

EBS berücksichtigt nicht die in den virtuellen Festplattensektoren enthaltenen Daten, sondern sichert lediglich die Integrität der Sektoren. Das bedeutet, dass AWS Aktionen und Betriebssystemaktionen unabhängig voneinander sind. Wenn Sie eine Volume-Größe auswählen, achten Sie auf die Kapazitäten und Einschränkungen beider, wie in den folgenden Fällen:

- EBS unterstützt derzeit eine maximale Volume-Größe von 64 TiB. Dies bedeutet, dass Sie eine EBS-Volume von bis zu 64 TiB erstellen können, ob das Betriebssystem aber diese gesamte Kapazität erkennt, hängt von dessen eigenen Eigenschaften und von der Partitionierung des Volumes ab.
- Startvolumes müssen entweder das MBR- oder das GPT-Partitionierungsschema verwenden. Das AMI, von dem aus Sie eine Instance starten, bestimmt den Startmodus und anschließend das für das Startvolume verwendete Partitionsschema.

  Bei MBR sind Startvolumes auf eine Größe von 2 TiB begrenzt.

  Mit GPT können Startvolumes bis zu 64 TiB groß sein, wenn sie mit GRUB2 (Linux) oder dem UEFI-Startmodus (Windows) verwendet werden.

  Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.
- Non-boot Volumes mit einer Größe von 2 TiB (2048 GiB) oder größer müssen eine GPT-Partitionstabelle verwenden, um auf das gesamte Volume zugreifen zu können.

Partitionierungsschemata

Neben anderen Auswirkungen legt das Partitionierungsschema fest, wie viele logische Blöcke in einem einzelnen Volume logisch adressiert werden können. Weitere Informationen finden Sie unter Datenblockgrößen. Die gängigen Partitionierungs-Schemata sind Master Boot Record (MBR) und GUID-Partitionstabelle (GPT). Die wichtigsten Unterschiede zwischen diesen Schemata können wie folgt zusammengefasst werden.

MBR

MBR verwendet eine 32-Bit-Datenstruktur zum Speichern von Blockadressen. Dies bedeutet, dass jedem Datenblock einer von 2^{32} möglichen Ganzzahlen zugewiesen wird. Die maximal adressierbare Größe eines Volumes ergibt sich über die folgende Formel:

$$2^{32} \times \text{Block size}$$

Die Blockgröße für MBR-Volumes ist konventionell auf 512 Bytes begrenzt. Daher gilt:

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

Technische Workarounds zur Erhöhung dieser 2 TiB-Grenze für MBR-Volumes haben sich in der Branche nicht allgemein durchgesetzt. Daher erkennen Linux und Windows niemals, dass ein MBR-Volume größer als 2 TiB ist, auch wenn sich AWS herausstellt, dass es größer ist.

GPT

GPT verwendet eine 64-Bit-Datenstruktur zum Speichern von Blockadressen. Dies bedeutet, dass jedem Datenblock einer von 2^{64} möglichen Ganzzahlen zugewiesen wird. Die maximal adressierbare Größe eines Volumes ergibt sich über die folgende Formel:

$$2^{64} \times \text{Block size}$$

Die Blockgröße bei GPT-Volumes ist gewöhnlich 4 096 Bytes. Daher gilt:

$$\begin{aligned} & 2^{64} \times 4{,}096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{70} \times 2^{6} \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

Real-world Computersysteme unterstützen nichts, was diesem theoretischen Maximum nahe kommt. Die implementierte Dateisystemgröße ist derzeit auf 50 TiB für ext4 und 256 TiB für NTFS begrenzt.

Datenblockgrößen

Die Datenspeicherung auf einer modernen Festplatte wird über die logische Blockadressierung verwaltet, eine Abstraktionsebene, die dem Betriebssystem ermöglicht, Daten in logischen Blöcken zu lesen und zu schreiben, ohne viel über die zugrunde liegende Hardware wissen zu müssen.

Das Betriebssystem ist darauf angewiesen, dass das Speichergerät die Blöcke seinen physischen Sektoren zuordnet, und liest und schreibt Daten auf die Festplatte, wobei Datenblöcke verwendet werden, die ein Vielfaches der Sektorgröße sind.

Amazon EBS kündigt dem Betriebssystem entweder 512-Byte- oder 4.096-Byte (4 KiB) physische Sektoren an, abhängig von den folgenden Faktoren:

1. Der Amazon EC2-Instance-Typ
2. Das Betriebssystem
3. Die NVMe-Treiberversion

Amazon EBS bewirbt physische Sektoren mit 4 KiB nur, wenn alle Faktoren dies unterstützen. Wenn einer dieser Sektoren keine physischen Sektoren mit 4 KiB unterstützt, bewirbt Amazon EBS physische Sektoren mit 512 Byte.

Unterstützung für Amazon EC2-Instance-Typen

Die folgende Tabelle zeigt die Sektorgrößen, die Amazon EBS für die verschiedenen Amazon EC2-Instance-Typen ankündigt.

Instance-Typ	Linux	Windows
Alle Instance-Typen Xen-based	Amazon EBS bewirbt immer physische 512-Byte-Sektoren	
A1 | C5 | C5a | C5ad | C5d | C5n | C6g | C6gd | DL1 | D3 | D3en | G4ad | G4dn | G5 | G5g | I3 | I3en | Inf1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | P3dn | P4d | P4de | R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | T3 | T3a | T4g | | | | | | x2Gd | X2ieZn | VT1 | Z1d U-12tb1 U-18tb1 U-24tb1 U-3tb1 U-6tb1 U-9tb1	Amazon EBS bewirbt immer physische 512-Byte-Sektoren	Amazon EBS bewirbt physische Sektoren mit 512 Byte oder 4 KiB 1

Instance-Typ	Linux	Windows
Nitro-based Alle anderen Instanzen	Amazon EBS bewirbt physische Sektoren mit 512 Byte oder 4 KiB 1	

[1] Hängt von der Betriebssystemunterstützung ab. Lesen Sie den folgenden Abschnitt.

Unterstützung des Betriebssystems

Die folgende Tabelle enthält Beispielbetriebssysteme und die entsprechenden physischen Sektorgrößen, die von Amazon EBS angekündigt werden. Diese Liste ist nicht vollständig. Wir empfehlen Ihnen, die von Amazon EBS angegebene physische Sektorgröße in Ihrem Betriebssystem zu überprüfen.

Betriebssystem	Größe des angegebenen physischen Sektors
• Amazon Linux mit Kernelversion 4.14 und früher • RHEL 7.9 und früher • Ubuntu 20.04 und früher • Windows 7/Windows Server 2008 und früher	512 Byte
• Amazon Linux mit Kernel-Version 5.3 und höher • RHEL8.8 und später • Ubuntu 22.04 und später • Windows 8/Windows Server 2012 und später 1	4 KiB

1 Stellen Sie für Windows-Workloads sicher, dass Sie die neueste Version der AWS NVMe-Treiber verwenden. Amazon EBS bewirbt physische Sektoren mit einer Kapazität von 4 KiB mit der AWS NVMe-Treiberversion 1.4.1 und höher.

Non-default Blockgrößen

Die branchenübliche Standardgröße für logische Datenblöcke beträgt derzeit 4 KiB. Da bestimmte Workloads von einer geringeren oder höheren Blockgröße profitieren, unterstützen Dateisysteme Nicht-Standard-Blockgrößen, die bei der Formatierung festgelegt werden können. Szenarien, in denen nicht standardmäßige Blockgrößen verwendet werden sollten (z. B. Optimierungen), sind nicht Gegenstand dieses Themas, aber die Wahl der Blockgröße hat Konsequenzen für die Speicherkapazität des Volumes. Die folgende Tabelle zeigt die theoretische Speicherkapazität als Funktion der Blockgröße. Beachten Sie jedoch, dass die EBS-imposed Begrenzung der Volume-Größe (64 TiB für io2 Block Express) derzeit der maximalen Größe entspricht, die durch 16-KiB-Datenblöcke aktiviert wird.

Blockgröße	Max. Volume-Größe
4 KiB (Standard)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (Maximum)	256 TiB

Amazon-EBS-Volumes und NVMe

Amazon EBS-Volumes werden als NVMe-Blockgeräte auf Amazon EC2-Instances bereitgestellt, die auf dem Nitro-System basieren. AWS Um die Leistung und Funktionen von Amazon EBS-Volumes, die als NVMe-Blockgeräte verfügbar sind, voll ausschöpfen zu können, muss auf der EC2-Instance der NVMe-Treiber installiert sein. AWS Auf allen AWS Windows- und Linux-AMIs der aktuellen Generation ist der AWS NVMe-Treiber standardmäßig installiert.

Wenn Sie ein AMI verwenden, das nicht über den AWS NVMe-Treiber verfügt, können Sie ihn manuell installieren. Weitere Informationen finden Sie unter AWS NVMe-Treiber im Amazon EC2-Benutzerhandbuch.

Linux-Instances

Die Gerätenamen lauten `/dev/nvme0n1`/`dev/nvme1n1`, und so weiter. Die Gerätenamen, die Sie in einer Blockgerätezuordnung angeben, werden durch NVMe-Gerätenamen () erse (`/dev/nvme[0-26]n1`). Der Blockgerät-Treiber kann NVMe-Gerätenamen in einer anderen Reihenfolge zuweisen, als Sie es für die Volumes in der Blockgerät-Zuweisung angegeben haben.

Windows-Instances

Wenn Sie Ihrer Instance ein Volume anfügen, geben Sie einen Gerätenamen für das Volume mit an. Dieser Gerätename wird von Amazon EC2 verwendet. Der Blockgerätetreiber für die Instance weist beim Mounten des Volumes den tatsächlichen Volume-Namen zu, und der zugewiesene Name kann sich von dem Namen unterscheiden, den Amazon EC2 verwendet.

Inhalt

- Ordnen Sie Amazon EBS-Volumes NVMe-Gerätenamen zu
- Timeout bei I/O NVMe-Vorgängen für Amazon EBS-Volumes
- NVMe Abbrechen Befehl für Amazon EBS-Volumes

Ordnen Sie Amazon EBS-Volumes NVMe-Gerätenamen zu

EBS verwendet I/O Single-Root-Virtualisierung (SR-IOV), um Volume-Anhänge auf Nitro-based Instances bereitzustellen, die die NVMe-Spezifikation verwenden. Diese Geräte benötigen Standard-NVMe-Treiber auf dem Betriebssystem. Diese Treiber erkennen die angefügten Geräte in der Regel beim Instance-Start und erstellen Geräteknoten basierend auf der Reihenfolge, in der die Geräte reagieren, und nicht darauf, wie die Geräte in der Blockgerät-Zuweisung angegeben sind.

Linux-Instances

<y>Unter Linux folgen NVMe-Gerätenamen dem Muster`/dev/nvme<x>n<y>`, wobei <x>die Aufzählungsreihenfolge und für EBS der Wert 1 ist. Gelegentlich können Geräte bei nachfolgenden Instance-Starts auf die Erkennung in einer anderen Reihenfolge reagieren, was dazu führt, dass sich der Gerätename ändert. Darüber hinaus kann der Gerätename, der vom Blockgerät-Treiber zugewiesen wird, von dem in der Blockgerät-Zuweisung angegebenen Namen abweichen.

Wir empfehlen Ihnen, für Ihre EBS-Volumes innerhalb Ihrer Instance stabile IDs zu verwenden, wie beispielsweise eine der folgenden:

- Zum Nitro-based Beispiel werden die Blockgerätezuordnungen, die in der Amazon EC2-Konsole angegeben werden, wenn Sie ein EBS-Volume anschließen oder während `AttachVolume`

oder `RunInstances` API-Aufrufen, im herstellerspezifischen Datenfeld der NVMe-Controller-Identifikation erfasst. Mit Amazon Linux-AMIs ab der Version 2017.09.01 stellen wir eine `udev`-Regel zur Verfügung, die diese Daten liest und einen symbolischen Link zur Blockgerät-Zuweisung erstellt.

- Die EBS-Volume-ID und der Einhängepunkt sind zwischen Instance-Statusänderungen stabil. Der NVMe-Gerätename kann sich je nach Reihenfolge ändern, in der die Geräte während des Instance-Starts reagieren. Wir empfehlen die Verwendung der EBS-Volume-ID und des Einhängepunkts zur konsistenten Geräteerkennung.
- Bei NVMe EBS-Volumes ist die EBS-Volume-ID als Seriennummer in der Gerätekennung festgelegt. Verwenden Sie den Befehl `lsblk -o +SERIAL`, um die Seriennummer aufzulisten.
- Das Format des NVMe-Gerätenamens kann je nachdem, ob das EBS-Volume während oder nach dem Start der Instance angeschlossen wurde, variieren. NVMe-Gerätenamen für Volumes, die nach dem Instance-Start verbunden sind, umfassen das `/dev/`-Präfix, während NVMe-Gerätenamen für Volumes, die während des Instance-Starts verbunden sind, das `/dev/`Präfix nicht einschließen.
  - Verwenden Sie für Amazon Linux- oder FreeBSD-AMI den Befehl für einen konsistenten NVMe-Gerätenamen. `sudo ebsnvme-id /dev/nvme0n1 -u`
  - Verwenden Sie für andere Verteilungen den Befehl `sudo nvme id-ctrl -V /dev/nvme0n1`, um den NVMe-Gerätenamen zu ermitteln. Möglicherweise müssen Sie die Befehlsoption angeben. `--vendor-specific`
- Beim Formatieren eines Geräts wird eine UUID erzeugt, die für die gesamte Lebensdauer des Dateisystems erhalten bleibt. Gleichzeitig kann eine Gerätebezeichnung angegeben werden. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung Und Von falschem Volume starten.

Amazon Linux-AMIs

Mit Amazon Linux-AMI 2017.09.01 oder höher (inklusive Amazon Linux 2) können Sie den Befehl ebsnvme-id wie folgt ausführen, um den NVMe-Gerätenamen einer Volume-ID zuzuordnen und umgekehrt:

Das folgende Beispiel zeigt den Befehl und die Ausgabe für ein Volume, das beim Instance-Start verbunden ist. Beachten Sie, dass der Name des NVMe-Gerätenamens nicht das `/dev/`-Präfix einschließt.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
```

```
Volume ID: vol-01324f611e2463981
sda
```

Das folgende Beispiel zeigt den Befehl und die Ausgabe eines Volumes, der nach dem Instance-Start verbunden ist. Beachten Sie, dass der NVMe-Gerätename das `/dev/`-Präfix einschließt.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux erstellt auch eine symbolische Verknüpfung vom Gerätenamen in der Blockgerätezuordnung (zum Beispiel `/dev/sdf`) zum NVMe-Gerätenamen.

FreeBSD-AMIs

Ab FreeBSD 12.2-RELEASE können Sie den Befehl ebsnvme-id wie oben gezeigt ausführen. Übergeben Sie entweder den Namen des NVMe-Geräts (z. B. `nvme0`) oder des Festplattengeräts (z. B. `nvd0` oder `nda0`). FreeBSD erstellt auch symbolische Links zu den Festplattengeräten (zum Beispiel `/dev/aws/disk/ebs/`*`volume_id`*).

Andere Linux-AMIs

Mit einer Kernel-Version von 4.2 oder höher können Sie den Befehl nvme id-ctrl wie folgt ausführen, um ein NVMe-Gerät einer Volume-ID zuzuordnen. Installieren Sie zunächst das NVMe-Befehlszeilenpaket, `nvme-cli`, unter Verwendung der Paketverwaltungstools für Ihre Linux-Distribution. Hinweise zum Download und zur Installation anderer Verteilungen finden Sie in der für Ihre Verteilung spezifischen Dokumentation.

Im folgenden Beispiel werden Volume-ID und NVMe-Gerätename für ein Volume abgerufen, das beim Instance-Start angehängt wurde. Beachten Sie, dass der Name des NVMe-Gerätenamens nicht das `/dev/`-Präfix einschließt. Der Gerätename ist über die für den Anbieter des NVMe-Controllers spezifische Extension (Bytes 384:4095 der Controller-ID) verfügbar:

```
[ec2-user ~]$ sudo nvme id-ctrl -V /dev/nvme0n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
```

```
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

Im folgenden Beispiel werden Volume-ID und NVMe-Gerätename für ein Volume abgerufen, das nach dem Instance-Start angeschlossen wurde. Beachten Sie, dass der NVMe-Gerätename das `/dev/`-Präfix einschließt.

```
[ec2-user ~]$ sudo nvme id-ctrl -V /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

Der Befehl lsblk führt die verfügbaren Geräte und, falls vorhanden, ihre Mountingpunkte auf. Damit können Sie bestimmen, welchen Gerätenamen Sie verwenden müssen. In diesem Beispiel ist `/dev/nvme0n1p1` als Root-Gerät gemountet, und `/dev/nvme1n1` ist angefügt, aber nicht gemountet.

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:3   0  100G  0 disk
nvme0n1       259:0   0    8G  0 disk
  nvme0n1p1   259:1   0    8G  0 part /
  nvme0n1p128 259:2   0    1M  0 part
```

Windows-Instances

Sie können den Befehl **`ebsnvme-id`** ausführen, um die NVMe-Geräte-Datenträgernummer einer EBS-Volume-ID und einem Gerätenamen zuzuordnen. Alle EBS-NVMe-Geräte sind standardmäßig aufgezählt. Sie können eine Datenträgernummer zum Aufzählen von Informationen zu einem bestimmten Gerät übergeben. Das `ebsnvme-id` Tool ist in den neuesten AWS Windows Server-AMIs enthalten, die sich unter befinden. `C:\ProgramData\Amazon\Tools`

Ab dem AWS NVMe-Treiberpaket wird `1.5.0,` die neueste Version des `ebsnvme-id` Tools vom Treiberpaket installiert. Die neueste Version ist nur im Treiberpaket verfügbar. Der eigenständige Download-Link für das `ebsnvme-id`-Tool erhält keine Updates mehr. Die letzte über den eigenständigen Link verfügbare Version ist `1.1.0`, die Sie über den Link ebsnvme-id.zip

herunterladen und den Inhalt in Ihre Amazon-EC2-Instance extrahieren können, um Zugriff auf `ebsnvme-id.exe` zu erhalten.

```
PS C:\ProgramData\Amazon\Tools> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb

Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

```
PS C:\ProgramData\Amazon\Tools> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

Timeout bei I/O NVMe-Vorgängen für Amazon EBS-Volumes

Die meisten Betriebssysteme geben einen Timeout für I/O Operationen an, die an NVMe-Geräte gesendet werden.

Linux-Instances

Unter Linux verwenden EBS-Volumes, die an Nitro-based Instances angehängt sind, den Standard-NVMe-Treiber, der vom Betriebssystem bereitgestellt wird. Die meisten Betriebssysteme geben einen Timeout für I/O Operationen an, die an NVMe-Geräte übertragen werden. Das Standard-Timeout beträgt 30 Sekunden und kann mit dem Boot-Parameter `nvme_core.io_timeout` geändert werden. Bei den meisten Linux-Kerneln vor Version 4.6 lautet dieser Parameter `nvme.io_timeout`.

Wenn die I/O Latenz den Wert dieses Timeout-Parameters überschreitet, schlägt der Linux-NVMe-Treiber fehl I/O und gibt einen Fehler an das Dateisystem oder die Anwendung zurück. Je nach I/O Vorgang kann Ihr Dateisystem oder Ihre Anwendung den Fehler erneut versuchen. In einigen Fällen kann es vorkommen, dass Ihr Dateisystem als schreibgeschützt wieder gemountet wird.

Für eine Erfahrung, die mit der bei an Xen-Instances angefügten EBS-Volumen vergleichbar ist, sollte für `nvme_core.io_timeout` der höchstmögliche Wert festgelegt werden. Für aktuellen Kernel ist der Höchstwert 4294967295, während für frühere Kernels maximal 255. Abhängig von der Linux-Version ist das Timeout möglicherweise bereits auf den unterstützten Höchstwert festgelegt. Beispiel: Für Amazon Linux AMI 2017.09.01 und höher ist als Timeout standardmäßig 4294967295 festgelegt.

Sie können den Maximalwert für Ihre Linux-Distribution überprüfen, indem Sie einen höheren Wert als den vorgeschlagenen Maximalwert in `/sys/module/nvme_core/parameters/io_timeout` eintragen und nach dem Fehler Numerical result out of range (Numerisches Ergebnis außerhalb des Bereichs) suchen, wenn Sie versuchen, die Datei zu speichern.

Windows-Instances

Unter Windows beträgt das Standard-Timeout 60 Sekunden und das Maximum 255 Sekunden. Die `TimeoutValue`-Festplattenklasseneinstellung kann mit dem unter Registry-Einträge für SCSI Miniport-Treiber beschriebenen Verfahren geändert werden.

NVMe Abbrechen Befehl für Amazon EBS-Volumes

Der `Abort` Befehl ist ein NVMe-Admin-Befehl, der ausgegeben wird, um einen bestimmten Befehl zu beenden, der zuvor an den Controller gesendet wurde. Dieser Befehl wird in der Regel vom Gerätetreiber an Speichergeräte ausgegeben, die den Schwellenwert für das I/O Betriebs-Timeout überschritten haben.

Amazon EC2-Instance-Typen, die den `Abort` Befehl standardmäßig unterstützen, beenden einen bestimmten Befehl, der zuvor an den Controller gesendet wurde, wenn ein `Abort` Befehl an angehängte Amazon EBS-Volumes ausgegeben wird. Amazon EC2-Instances, die den `Abort` Befehl nicht unterstützen, ergreifen keine Maßnahmen, wenn ein `Abort` Befehl an angehängte Amazon EBS-Volumes ausgegeben wird.

Der `Abort` Befehl wird unterstützt mit:

- Amazon EBS-Geräte mit NVMe-Geräteversion 1.4 oder höher.
- Alle Amazon EC2-Instances, mit Ausnahme der Xen-based Instance-Typen und der folgenden Nitro-based Instance-Typen:

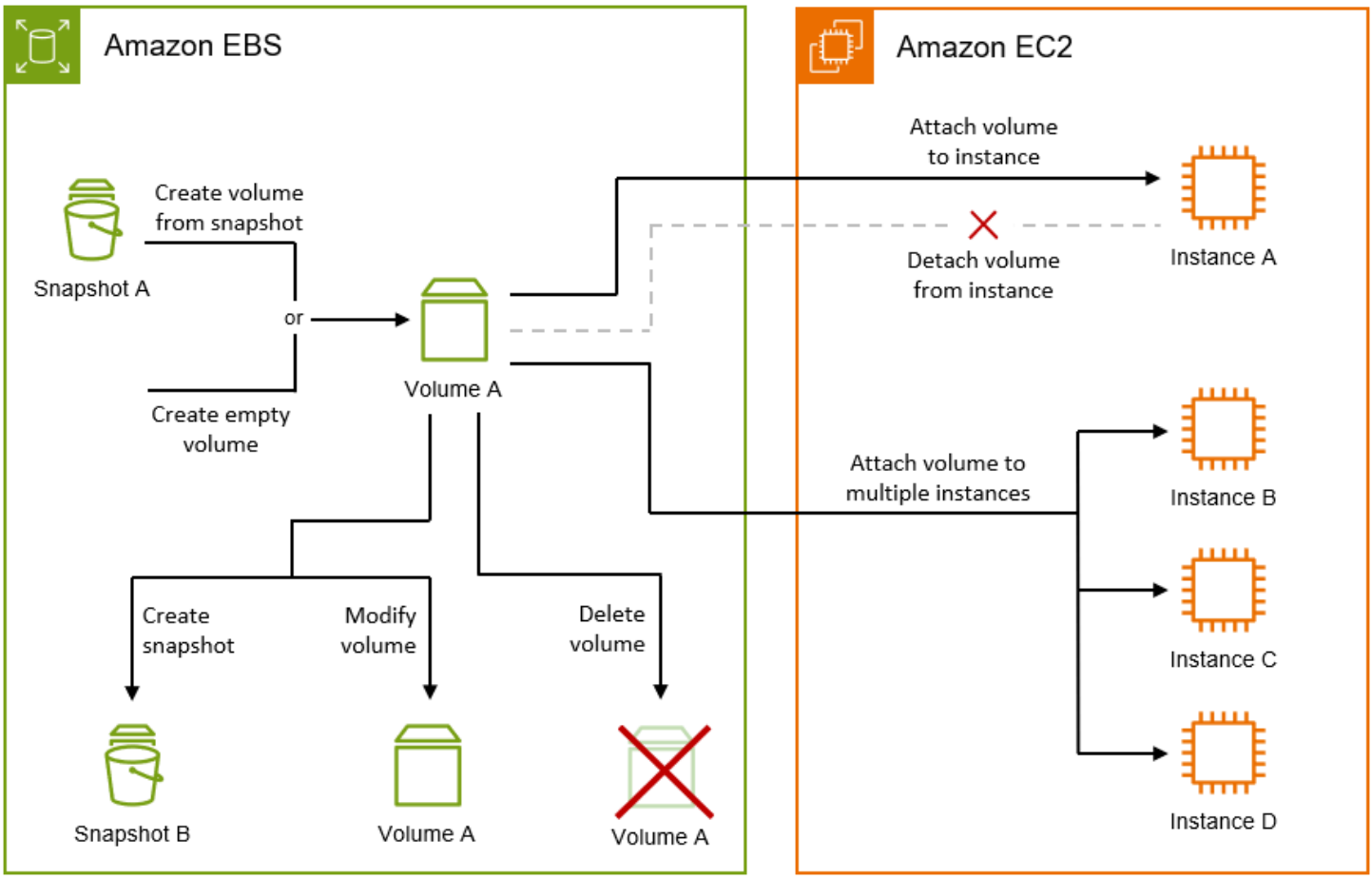
- Allgemeiner Zweck: A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g
- Computeroptimiert: C5 | c5a | C5ad | C5d | C5n | C6g | C6gd
- Speicheroptimiert: R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | | | | | | x2GD | X2ieZn | Z1d U-12tb1 U-18tb1 U-24tb1 U-3tb1 U-6tb1 U-9tb1
- Optimierte Speicherleistung: D3 | D3en | I3en
- Beschleunigtes Rechnen: DL1 | G4ad | G4dn | G5 | G5G | Inf1 | P3dn | P4d | P4de | VT1

Weitere Informationen finden Sie im Abschnitt 5.1-Befehl der NVM Express Base Specification. Abort https://nvmexpress.org/wp-content/uploads/NVM-Express-1_4-2019.06.10-Ratified.pdf

Lebenszyklus von Amazon EBS-Volumes

Der Lebenszyklus eines Amazon EBS-Volumes beginnt mit dem Erstellungsprozess. Sie können ein Volume aus einem Amazon EBS-Snapshot erstellen oder Sie können ein leeres Volume erstellen. Bevor Sie Ihr Volume verwenden können, müssen Sie es an eine oder mehrere Amazon EC2-Instances anhängen, die sich in derselben Availability Zone wie das Volume befinden. Sie können mehrere Volumes an eine Instance anhängen. Bei Bedarf können Sie ein Volume von einer Instance trennen und es dann an eine andere Instance anhängen. Wenn sich Ihre Speicheranforderungen ändern, können Sie die Größe oder Leistung des Volumes jederzeit ändern. Sie können Point-in-Time-Backups Ihrer Volumes erstellen, indem Sie Amazon EBS-Snapshots erstellen. Wenn Sie ein Volume nicht mehr benötigen, können Sie es löschen, damit die damit verbundenen Speicherkosten nicht mehr anfallen.

Die folgende Abbildung zeigt Aktionen, die Sie im Rahmen des Volume-Lebenszyklus an Ihren Volumes ausführen können. Es gibt auch Aufgaben, die Sie ausführen, indem Sie eine Verbindung zur Instance herstellen und einen Betriebssystembefehl ausführen. Zum Beispiel das Formatieren des Volumes, das Mounten des Volumes, das Verwalten von Partitionen und das Anzeigen des freien Speicherplatzes.



Aufgaben

- Erstellen Sie ein Amazon EBS-Volume
- Teilen Sie ein Volume
- Kopieren Sie ein Amazon EBS-Volume
- Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an
- Hängen Sie ein EBS-Volume mit mehreren EC2-Instances an Multi-Attach
- Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung
- Anzeigen von Informationen über ein Amazon EBS-Volume
- Ändern Sie ein Amazon EBS-Volume mithilfe von Elastic Volumes-Vorgängen
- Trennen Sie ein Amazon EBS-Volume von einer Amazon EC2-Instance
- Löschen eines Amazon EBS-Volumes

Erstellen Sie ein Amazon EBS-Volume

Sie können ein Amazon-EBS-Volume erstellen und dann an jede EC2-Instance in derselben Availability Zone anfügen.

Sie können entweder ein leeres Volume oder ein Volume aus einem Amazon EBS-Snapshot erstellen. Wenn Sie ein Volume aus einem Snapshot erstellen, ist das Volume zunächst ein exaktes Replikat des Volumes, das zur Erstellung dieses Snapshots verwendet wurde.

Initialisierung des Datenträgers

Wenn Sie ein Volume aus einem Snapshot erstellen, müssen die Speicherblöcke aus dem Snapshot von Amazon S3 heruntergeladen und auf das Volume geschrieben werden, bevor Sie darauf zugreifen können. Dieser Vorgang wird als Volume-Initialisierung bezeichnet. Während dieser Zeit kommt es auf dem Volume zu einer erhöhten I/O Latenz. Die volle Leistung des Datenträgers wird erst erreicht, nachdem alle Speicherblöcke heruntergeladen und auf das Volume geschrieben wurden.

Die standardmäßige Initialisierungsrate des Volumes schwankt während des Initialisierungsprozesses, wodurch die Fertigstellungszeiten unvorhersehbar werden können.

Um die mit der Volume-Initialisierung verbundenen Leistungseinbußen zu minimieren, können Sie eine Amazon EBS-Provisioned Rate für die Volume-Initialisierung (Volume-Initialisierungsrate) oder die schnelle Snapshot-Wiederherstellung verwenden. Weitere Informationen finden Sie unter Initialisieren von Volumes Amazon EBS.

Volume-Verschlüsselung

Der Verschlüsselungsstatus des Volumes hängt davon ab, ob Ihr Konto standardmäßig für die Verschlüsselung aktiviert ist, und vom Verschlüsselungsstatus des Snapshots, falls Sie einen verwenden möchten. In der folgenden Tabelle werden die möglichen Verschlüsselungsergebnisse zusammengefasst.

Standardmäßige Verschlüsselung	Snapshot verwendet?	Ergebnis der Volumenverschlüsselung	Hinweis
Disabled	Nein	Optionale Verschlüsselung	Wenn Sie die Verschlüsselung aktivieren, können Sie den zu verwendenden

Standardmäßige Verschlüsselung	Snapshot verwendet?	Ergebnis der Volumenverschlüsselung	Hinweis
			KMS-Schlüssel angeben. Wenn Sie die Verschlüsselung aktivieren, aber keinen KMS-Schlüssel angeben, wird das Von AWS verwalteter Schlüssel (`aws/ebs`) verwendet.
Disabled	Ja, unverschlüsselt	Optionale Verschlüsselung	Wenn Sie die Verschlüsselung aktivieren, können Sie den zu verwendenden KMS-Schlüssel angeben. Wenn Sie die Verschlüsselung aktivieren, aber keinen KMS-Schlüssel angeben, wird das Von AWS verwalteter Schlüssel (`aws/ebs`) verwendet.
Disabled	Ja, verschlüsselt	Automatische Verschlüsselung	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird das Volume mit demselben KMS-Schlüssel wie der Quell-Snapshot verschlüsselt.
Aktiviert	Nein	Automatische Verschlüsselung	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird der standardmäßig für die Verschlüsselung angegebene Schlüssel verwendet.
Aktiviert	Ja, unverschlüsselt	Automatische Verschlüsselung	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird der standardmäßig für die Verschlüsselung angegebene Schlüssel verwendet.

Standardr äßige Verschlüs selung	Snapshot verwendet?	Ergebnis der Volumenve rschlüsselung	Hinweis
Aktiviert	Ja, verschlüsselt	Automatische Verschlüsselung	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird das Volume mit demselben Schlüssel wie der Quell-Snapshot (Konsole) oder mit dem standardmäßig für die Verschlüs selung angegebenen Schlüssel (CLI/API) verschlüsselt.

Weitere Überlegungen

- Volumes müssen an Instances in derselben Availability Zone angehängt werden.
- Volumes sind erst einsatzbereit, wenn sie den `available` Status erreicht haben.
- Wenn Sie ein Volume mithilfe der Konsole erstellen, `gp3` ist dies der Standard-Volume-Typ. Für die Befehlszeilentools `gp2` ist API und SDK der Standard-Volume-Typ.
- Um ein Volume mit einer Instance zu verwenden, die auf einem Outpost läuft, müssen Sie das Volume auf demselben Outpost wie die Instance erstellen.
- Wenn Sie ein Volume für die Verwendung mit einer Windows-Instance erstellen und es größer als 2048 GiB ist, stellen Sie sicher, dass Sie das Volume für die Verwendung von GPT-Partitionstabellen konfigurieren. Weitere Informationen finden Sie unter Einschränkungen für Amazon-EBS-Volumes und Windows-Unterstützung für Festplatten mit mehr als 2 TB. .
- Volumes werden auch indirekt durch das Starten einer Amazon EC2-Instance erstellt. Entweder das AMI, mit dem die Instance gestartet wurde, oder die Instance-Startanforderung selbst könnte Blockgerätezuordnungen für Amazon EBS-Volumes enthalten. Weitere Informationen finden Sie unter Gerätezuordnungen blockieren.

Console

So erstellen Sie ein Volume

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes und dann Create volume aus.
3. (nur für Outpost Kunden) Geben Sie für Outpost ARN den ARN des Volumes ein, AWS Outpost auf dem das Volume erstellt werden soll.
4. Wählen Sie für Volume-Typ den Typ des zu erstellenden Volumes aus. Weitere Informationen zu den verfügbaren Volume-Typen finden Sie unterAmazon EBS-Volume-Typen.
5. Geben Sie als Größe die Größe des Volumes in GiB ein. Weitere Informationen finden Sie unter Einschränkungen für Amazon-EBS-Volumes.
6. (Nur für *io1*io2*, und *gp3* nur) Geben Sie für IOPS die maximale Anzahl von input/output Vorgängen pro Sekunde (IOPS) ein, die das Volume bereitstellen soll.
7. (*gp3*Nur) Geben Sie für Durchsatz den Durchsatz ein, den das Volume bieten soll, in. MiB/s
8. Wählen Sie unter Availability Zone die Availability Zone aus, in der das Volume erstellt werden soll.
9. Führen Sie für die Snapshot-ID einen der folgenden Schritte aus:
   - Um ein leeres Volume zu erstellen, behalten Sie den Standardwert bei (Erstellen Sie kein Volume aus einem Snapshot).
   - Um das Volume aus einem Snapshot zu erstellen, wählen Sie den Snapshot aus, den Sie verwenden möchten.
10. Wenn Sie einen Snapshot ausgewählt haben, können Sie für die Volume-Initialisierungsrate optional die Volume-Initialisierungsrate angeben MiB/s, in der die Snapshot-Blöcke nach der Erstellung von Amazon S3 auf das Volume heruntergeladen werden sollen. Weitere Informationen finden Sie unter Verwenden Sie eine von Amazon EBS bereitgestellte Rate für die Volumeninitialisierung. Um die Standard-Initialisierungsrate oder die schnelle Snapshot-Wiederherstellung zu verwenden (sofern sie für den ausgewählten Snapshot aktiviert ist), geben Sie keine Rate an.
11. (*io1*und *io2* nur) Um das Volume für Amazon EBS zu aktivieren Multi-Attach, wählen Sie Aktivieren aus. Multi-Attach Weitere Informationen finden Sie unter Hängen Sie ein EBS-Volume mit mehreren EC2-Instances an Multi-Attach.
12. Legen Sie den Verschlüsselungsstatus für das Volume fest.

- Wenn Ihr Konto standardmäßig für die Verschlüsselung aktiviert ist, erfolgt die Verschlüsselung automatisch und kann nicht deaktiviert werden.
- Wenn Sie einen verschlüsselten Snapshot ausgewählt haben, erfolgt die Verschlüsselung automatisch und kann nicht deaktiviert werden.
- Wenn Ihr Konto standardmäßig nicht für die Verschlüsselung aktiviert ist und Sie einen unverschlüsselten Snapshot auswählen oder keinen Snapshot auswählen, ist die Verschlüsselung optional.

13. (Optional) Um dem Volume benutzerdefinierte Tags zuzuweisen, wählen Sie im Abschnitt Tags die Option Tag hinzufügen aus und geben Sie dann ein Tag-Schlüssel-Wert-Paar ein.
14. Wählen Sie Create Volume (Volume erstellen) aus.
15. Um das Volume zu verwenden, warten Sie, bis es den `available` Status erreicht hat, und hängen Sie es dann an eine Amazon EC2-Instance in derselben Availability Zone an. Weitere Informationen finden Sie unter Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.

AWS CLI

So erstellen Sie ein Volume

Verwenden Sie den Befehl create-volume. Im folgenden Beispiel wird ein leeres gp3-Volume mit einer Größe von 100 GiB in der angegebenen Availability Zone erstellt.

```
aws ec2 create-volume \
    --volume-type gp3 \
    --size 100 \
    --availability-zone us-east-1a
```

PowerShell

So erstellen Sie ein Volume

Verwenden Sie das cmdlet New-EC2Volume. Im folgenden Beispiel wird ein leeres GP3-Volume mit einer Größe von 100 GiB in der angegebenen Availability Zone erstellt.

```
New-EC2Volume `
    -VolumeType gp3 `
    -Size 100 `
```

```
    -AvailabilityZone us-east-1a
```

Teilen Sie ein Volume

Sie können AWS Resource Access Manager (AWS RAM) verwenden, um Amazon EBS-Volumes für andere AWS Konten freizugeben. Nachdem Sie ein Volume gemeinsam genutzt haben, können nutzende Konten die Volume-Informationen einsehen und Kopien des gemeinsam genutzten Volumes in derselben Availability Zone erstellen. Weitere Informationen zum Erstellen von Kopien finden Sie unterKopieren Sie ein Amazon EBS-Volume. Benutzerkonten können keine Snapshots eines gemeinsam genutzten Volumes anhängen, ändern, löschen oder erstellen.

Sie können beispielsweise Produktionsvolumes mit Entwicklungskonten teilen, um Testumgebungen mit aktuellen Produktionsdaten zu aktualisieren und gleichzeitig die Isolierung auf Kontoebene aufrechtzuerhalten.

Sie können Volumes gemeinsam nutzen, die:

- Unverschlüsselt
- Verschlüsselt mit einem vom Kunden verwalteten Schlüssel

Sie können keine Volumes teilen, die mit dem standardmäßigen AWS verwalteten Schlüssel für Amazon EBS verschlüsselt sind.

Inhalt

- Berechtigungen
- Teilen Sie ein Volume
- Geteilte Volumes anzeigen
- Überlegungen zur gemeinsamen Nutzung von Volumes
- Überwachen Sie die Freigabeaktivitäten
- Geteilte Volumes und Papierkorb
- Preisgestaltung

Berechtigungen

Wenn Sie eine Ressourcenfreigabe für gemeinsam genutzte Volumes erstellen, müssen Sie der Ressourcenfreigabe verwaltete Berechtigungen zuordnen. Die verwalteten Berechtigungen

bestimmen, welche Aktionen nutzende Konten auf den gemeinsam genutzten Volumes in der Ressourcenfreigabe ausführen können. AWS RAM bietet die folgenden AWS verwalteten Berechtigungen:

- AWSRAMDefaultPermissionEBSVolume(Standard) — Erteilt nutzenden Konten die Erlaubnis, Volumeninformationen einzusehen.
- AWSRAMPermissionEBSVolumeCopyAccess— Erteilt Benutzerkonten die Erlaubnis, Volumeninformationen einzusehen und Kopien des gemeinsam genutzten Volumes zu erstellen.

Alternativ können Sie eine vom Kunden verwaltete Berechtigung für den `ec2:Volume` Ressourcentyp erstellen. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Erstellen und Verwenden von vom Kunden verwalteten Berechtigungen.

Teilen Sie ein Volume

Verwenden Sie eine der folgenden Methoden, um ein Amazon EBS-Volume gemeinsam zu nutzen.

Console

Um ein Volume zu teilen

1. Öffnen Sie die Amazon Elastic Compute Cloud-Konsole unterhttps://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus und wählen Sie dann Actions, Share volume aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um das Volume einer vorhandenen Ressourcenfreigabe hinzuzufügen, wählen Sie die Ressourcenfreigabe aus.
   - Um eine neue Ressourcenfreigabe zu erstellen, wählen Sie Neue Ressourcenfreigabe erstellen. Dadurch wird die AWS RAM Konsole geöffnet, in der Sie den Share konfigurieren.
5. Fügen Sie für Principals die Konten hinzu, mit denen Sie das Volume teilen möchten. Sie können einzelne Konto-IDs, Organisationseinheiten (OUs) oder Ihre gesamte Organisation hinzufügen.
6. Wählen Sie für Verwaltete Berechtigungen eine der folgenden Optionen aus:

- AWSRAMDefaultPermissionEBSVolume(Standard) — Benutzerkonten können nur Volumenmetadaten anzeigen.
- AWSRAMPermissionEBSVolumeCopyAccess— Benutzerkonten können Volumenmetadaten einsehen und Kopien des gemeinsam genutzten Volumes erstellen.
- Eine vom Kunden verwaltete Berechtigung, die Sie für den `ec2:Volume` Ressourcentyp erstellt haben.

7. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

AWS CLI

Verwenden Sie den Befehl create-resource-share. Geben Sie den Volume-ARN, das verbrauchende Konto und den Berechtigungs-ARN an. Rufen Sie https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-volumes.html describe-volumes auf, um den Volume-ARN zu finden. Die Antwort enthält das `VolumeArn` Feld für jedes Volume.

Im folgenden Beispiel wird eine gemeinsam genutzte Ressource erstellt, bei der das Volumen `vol-1234567890abcdef0` mit dem Konto gemeinsam genutzt wird`222222222222`, und die `AWSRAMPermissionEBSVolumeCopyAccess` verwaltete Berechtigung wird zugewiesen:

```
aws ram create-resource-share \
--name my-volume-share \
--resource-arns arn:aws:ec2:us-east-1:111111111111:volume/vol-1234567890abcdef0 \
--principals 222222222222 \
--permission-arns arn:aws:ram::aws:permission/AWSRAMPermissionEBSVolumeCopyAccess \
--region us-east-1
```

Wenn Sie mit der Standardberechtigung (`AWSRAMDefaultPermissionEBSVolume`nur Beschreibung) teilen möchten, lassen Sie den `--permission-arns` Parameter weg:

```
aws ram create-resource-share \
--name my-volume-share \
--resource-arns arn:aws:ec2:us-east-1:111111111111:volume/vol-1234567890abcdef0 \
--principals 222222222222 \
--region us-east-1
```

Weitere Informationen zu Ressourcenfreigaben finden Sie im AWS RAM Benutzerhandbuch unter Erstellen einer Ressourcenfreigabe.

Geteilte Volumes anzeigen

Nachdem Sie die Ressourcenfreigabe erstellt haben, erhalten die angegebenen Konten eine Einladung. Konten außerhalb Ihrer Organisation AWS Organizations müssen die Einladung annehmen, bevor sie auf gemeinsam genutzte Volumes zugreifen können. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Annehmen und Ablehnen von Einladungen zur gemeinsamen Nutzung von Ressourcen.

Sie können sich die Volumes ansehen, die mit Ihrem Konto geteilt werden, indem Sie eine der folgenden Methoden verwenden.

Console

Um geteilte Volumes anzuzeigen

1. Öffnen Sie die Amazon Elastic Compute Cloud-Konsole unterhttps://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie den voreingestellten Filter Für mich freigegeben, um alle Volumes anzuzeigen, die mit Ihrem Konto geteilt wurden.
   - Wählen Sie „Filter hinzufügen“, „Inhaber-ID“ und geben Sie dann die ID des Sharing-Kontos ein.

Bei geteilten Volumes wird die gemeinsame Konto-ID in der Spalte Besitzer-ID angezeigt.

AWS CLI

Verwenden Sie den Befehl describe-volumes zusammen mit dem `owner-id` Filter, um Volumes anzuzeigen, die von einem bestimmten Konto für Sie freigegeben wurden.

```
aws ec2 describe-volumes \
--filters Name=owner-id,Values=111111111111 \
--region us-east-1
```

Geteilte Volumes enthalten das `OwnerId` Feld in der Antwort, in dem die ID des gemeinsamen Kontos angezeigt wird.

Überlegungen zur gemeinsamen Nutzung von Volumes

Beachten Sie Folgendes, wenn Sie Volumes mit anderen Konten teilen.

- Sie können unverschlüsselte Volumes und Volumes, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt wurden, gemeinsam nutzen. Sie können keine Volumes teilen, die mit dem standardmäßigen AWS verwalteten Schlüssel für Amazon EBS verschlüsselt sind.
- Um ein Volume gemeinsam nutzen zu können, muss das Konto des Volume-Besitzers über die `kms:DescribeKey` Berechtigung für den standardmäßigen Amazon EBS-Verschlüsselungsschlüssel verfügen. Dies ist für alle Volumes erforderlich, einschließlich unverschlüsselter Volumes, da der Service den Verschlüsselungsstatus des Volumes während des Freigabevorgangs überprüft.
- Um ein Volume, das mit einem vom Kunden verwalteten Schlüssel verschlüsselt wurde, gemeinsam nutzen zu können, müssen Sie den KMS-Schlüssel auch mit dem Konto teilen, das die Daten verwendet. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service - Entwicklerhandbuch.
- Um Kopien eines gemeinsam genutzten verschlüsselten Volumes zu erstellen, benötigt das nutzende Konto `kms:CreateGrant` `kms:GenerateDataKeykms:GenerateDataKeyWithoutPlaintext`,`kms:ReEncrypt*`, und `kms:Decrypt` auf dem KMS-Schlüssel.
- Benutzerkonten können keine Snapshots eines gemeinsam genutzten Volumes anhängen, ändern, löschen oder erstellen. Sie können nur Volume-Metadaten einsehen und Kopien erstellen.
- Auf einem gemeinsam genutzten Volume kann jeweils nur ein Kopiervorgang ausgeführt werden, und zwar für alle Konten, mit denen das Volume gemeinsam genutzt wird. Zusätzliche Kopieranforderungen geben einen Fehler zurück, bis der aktuelle Vorgang abgeschlossen ist.
- Die Namen der Availability Zones (z. B.`us-east-1a`) sind verschiedenen physischen Standorten in verschiedenen AWS Konten zugeordnet. Verwenden Sie Availability Zone-IDs (wie`use1-az1`), um in allen Konten denselben physischen Standort zu identifizieren. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Availability Zone-IDs für Ihre AWS Ressourcen.
- Durch das Entfernen eines Volumes aus einer Ressourcenfreigabe werden laufende Kopiervorgänge nicht abgebrochen.
- Durch das Löschen des Quell-Volumes werden laufende Kopiervorgänge nicht abgebrochen.

Überwachen Sie die Freigabeaktivitäten

AWS CloudTrail API-Protokollierung

Alle API-Aufrufe zum Teilen und Kopieren von Volume sind angemeldet AWS CloudTrail. `CopyVolumes` API-Aufrufe werden sowohl für das Konto, das die Kopie initiiert hat, als auch für das Konto des Volume-Besitzers protokolliert. Weitere Informationen finden Sie unter Protokollieren von Amazon Elastic Compute Cloud-API-Aufrufen mit AWS CloudTrail.

EventBridge Amazon-Benachrichtigungen

Amazon EBS sendet EventBridge Amazon-Ereignisse, wenn kontoübergreifende Kopiervorgänge abgeschlossen sind. Sowohl der Besitzer des Volumes als auch das Konto, das das Laufwerk nutzt, erhalten das Ereignis. Für Ereignisse mit Volumenkopie wird der Detailtyp `EBS Volume Notification` mit dem Eventnamen verwendet`sharedVolumeCopy`. Das Ereignis umfasst die Volume-ID, den Abschlussstatus (`completed`oder`failed`) und einen Zeitstempel.

Um Benachrichtigungen einzurichten, erstellen Sie eine EventBridge Amazon-Regel, die `EBS Volume Notification` Ereignissen den Namen des `sharedVolumeCopy` Ereignisses zuordnet. Weitere Informationen finden Sie unter EventBridge Amazon-Ereignisse für Amazon EBS.

Geteilte Volumes und Papierkorb

Wenn Sie eine Aufbewahrungsregel für den Papierkorb haben, die für Volumes gilt, wird das geteilte Volume durch Löschen in den Papierkorb verschoben. Das Volume verbleibt während des gesamten Aufbewahrungszeitraums in seinen AWS RAM Ressourcenanteilen. Wenn Sie das Volume aus dem Papierkorb wiederherstellen, können Sie über dieselben Ressourcenfreigaben darauf zugreifen, zu denen es vor dem Löschen gehörte.

Beachten Sie das folgende Verhalten bei der gemeinsamen Nutzung von Ressourcen für ein Volume, das sich im Papierkorb befindet:

- Wenn Sie ein Konto aus der Ressourcenfreigabe entfernt haben, während sich das Volume im Papierkorb befand, gewährt Ihnen das Wiederherstellen des Volumes nicht erneut Zugriff auf dieses Konto.
- Wenn Sie der Ressourcenfreigabe ein Konto hinzugefügt haben, während sich das Volume im Papierkorb befand, hat dieses Konto nach der Wiederherstellung Zugriff auf das Volume.

Nachdem Sie ein Volume aus dem Papierkorb wiederhergestellt haben, überprüfen Sie anhand Ihrer Ressourcenfreigaben in der Konsole, ob nur die AWS RAM dafür vorgesehenen Konten Zugriff haben.

Preisgestaltung

Für die gemeinsame Nutzung von Volumes fallen keine Kosten an. AWS RAM Das Konto, das eine Kopie erstellt, zahlt die Gebühr für Volumenkopien und die regulären Amazon EBS-Volumengebühren für das neue Volume. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Kopieren Sie ein Amazon EBS-Volume

Eine Volumenkopie ist eine absturzkonsistente Point-in-Time-Kopie des Quell-Volumes. Sie umfasst alle Datenblöcke, die zu Beginn der Initialisierung der Volumenkopie auf das Quell-Volume geschrieben wurden. Die Volumenkopie erhält ihre eigene eindeutige Volume-ID. Volumenkopien werden sofort erstellt und können an eine Amazon EC2-Instance angehängt werden, sobald diese den `available` Status erreicht hat. Mithilfe von Volumenkopien können Sie Ihre Produktionsdaten schnell für Test- und Entwicklungsumgebungen kopieren.

Sie können auch Kopien von Volumes erstellen, die Ihnen von anderen AWS Konten zur Verfügung gestellt wurden. Um ein Volume von einem anderen Konto zu kopieren, muss das Quell-Volume über AWS Resource Access Manager (AWS RAM) mit Ihnen geteilt werden. Weitere Informationen finden Sie unter Teilen Sie ein Volume.

Initialisierung

Volumenkopien werden nach der Erstellung initialisiert. Bei der Initialisierung werden die Datenblöcke vom Quell-Volume kopiert und im Hintergrund auf die Volume-Kopie geschrieben. Das Volume verbleibt im `initializing` Zustand, bis die Initialisierung abgeschlossen ist.

Leistung während der Initialisierung

Kopiervorgänge wirken sich nicht auf die Leistung des Quell-Volumes aus. Sie können das Quellvolume während des Kopiervorgangs normal weiterverwenden. Auf kopierte Volumes kann sofort zugegriffen werden, ohne darauf warten zu müssen, dass die Daten vom Quellvolume kopiert werden. Volumenkopien bieten sofortigen Zugriff auf Daten mit einer Latenz im einstelligen Millisekundenbereich. Die tatsächliche Latenz kann jedoch je nach Volume-Typ variieren. Während der Initialisierung bietet die Volumenkopie eine Grundleistung, die dem niedrigsten der folgenden drei Werte entspricht:

- 3.000 input/output Operationen pro Sekunde (IOPS) und 125 MiB/s
- Die bereitgestellte Leistung für das Quell-Volume
- Die bereitgestellte Leistung für die Volumenkopie

Die Volumenkopie kann die Ausgangsleistung übertreffen, wenn die folgenden Kriterien erfüllt sind:

1. Sowohl das Quellvolume als auch die Volumenkopie sind mit mehr als 3.000 IOPS pro Sekunde und 125 ausgestattet. MiB/s
2. Das Quell-Volume hat eine ungenutzte Leistungskapazität (die betriebene Leistung ist geringer als die bereitgestellte Leistung).

Wenn das Quell-Volume beispielsweise mit 10.000 IOPS bereitgestellt wird und Ihre Arbeitslast derzeit nur 5.000 IOPS ausmacht und die Volumenkopie mit 10.000 IOPS bereitgestellt wird, kann die Volumenkopie bei der Initialisierung eine Leistung erzielen, die höher ist als die Basisleistung von 3.000 IOPS, indem die ungenutzten 5.000 IOPS des Quell-Volumes verwendet werden.

Dauer der Initialisierung

Die Zeit, die für die Initialisierung einer Volumenkopie benötigt wird, hängt von der Größe der Blockdaten ab, die zum Zeitpunkt der Erstellung der Volumenkopie auf das Quellvolume geschrieben wurden. Volumenkopien werden nach bestem Bemühen initialisiert, wobei die folgenden allgemeinen Richtlinien eingehalten werden. Für die ersten 1 TiB an Datenblöcken dauert die Volume-Initialisierung bis zu 6 Stunden. Für jedes weitere 1 TiB an Datenblöcken bis zu 16 TiB dauert die Initialisierung 1,2 Stunden pro TiB. Bei geschriebenen Daten, die größer als 16 TiB sind, dauert die Initialisierung 24 Stunden.

Überwachen Sie den Fortschritt der Initialisierung

Sie können den Initialisierungsfortschritt mit dem Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-volume-status.html AWS CLI describe-volume-status oder mit Amazon überwachen. EventBridge Weitere Informationen finden Sie unter Überwachen Sie den Status der Amazon EBS-Volume-Initialisierung.

Verschlüsselung

Wenn Sie ein Volume kopieren, hängt die Verschlüsselung der Kopie vom Verschlüsselungsstatus des Quell-Volumes, der Standardeinstellung für die Verschlüsselung Ihres Kontos und den `KmsKeyId` Parametern `Encrypted` und ab, die Sie in der Kopieranforderung angeben.

Unverschlüsselte Quell-Volumes

Wenn das Quellvolume unverschlüsselt ist und die Verschlüsselung für Ihr Konto standardmäßig deaktiviert ist, ist die Kopie unverschlüsselt. Sie können die Kopie verschlüsseln, indem Sie den Parameter auf `Encrypted` setzen. `true` Wenn Sie keinen angeben KMS key, wird der standardmäßige Amazon EBS-Verschlüsselungsschlüssel Ihres Kontos verwendet.

Wenn das Quellvolume unverschlüsselt ist und die Verschlüsselung für Ihr Konto standardmäßig aktiviert ist, wird die Kopie automatisch verschlüsselt. Wenn Sie keinen angeben KMS key, wird der standardmäßige Amazon EBS-Verschlüsselungsschlüssel Ihres Kontos verwendet.

Verschlüsselte Quell-Volumes

Wenn das Quellvolume verschlüsselt ist, ist die Kopie immer verschlüsselt. Sie können keine unverschlüsselte Kopie von einem verschlüsselten Quellvolume erstellen.

Bei Kopien mit demselben Konto verwendet die Kopie standardmäßig denselben KMS-Schlüssel wie das Quellvolume. Sie können einen anderen vom Kunden verwalteten Schlüssel angeben, um die Kopie erneut zu verschlüsseln.

Bei kontoübergreifenden Kopien verwendet die Kopie standardmäßig den Amazon EBS-Standardverschlüsselungsschlüssel Ihres Kontos. Sie können im Parameter einen anderen vom `KmsKeyId` Kunden verwalteten Schlüssel angeben. Sie können den KMS-Schlüssel des Quellkontos verwenden, um die Volumenkopie zu verschlüsseln, wenn dieser Schlüssel mit Ihrem Konto geteilt wurde.

Cross-account Anforderungen an die Verschlüsselung

Um ein gemeinsam genutztes Volume zu kopieren, das mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, muss der Besitzer des Volumes den KMS-Schlüssel mit Ihrem Konto teilen. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Zulassen der Verwendung von a KMS key durch Benutzer mit anderen Konten.

Volumes, die mit dem standardmäßigen AWS verwalteten Schlüssel für Amazon EBS verschlüsselt wurden, können nicht für mehrere Konten gemeinsam genutzt oder kopiert werden.

Verschlüsselungsergebnisse

Unverschlüsselte Quell-Volumes

Standardmäßige Verschlüsselung	Sie geben eine an KMS key	Ergebnis
Disabled	Nein	Die Kopie ist unverschlüsselt
Disabled	Ja	Mit dem angegebenen Schlüssel verschlüsselte Kopie
Aktiviert	Nein	Kopieren Sie verschlüsselt mit dem standardmäßigen Amazon EBS-Verschlüsselungsschlüssel Ihres Kontos
Aktiviert	Ja	Mit dem angegebenen Schlüssel verschlüsselt kopieren

Verschlüsselte Quellvolumes (gleiches Konto)

Sie geben eine an KMS key	Ergebnis
Nein	Mit demselben Schlüssel wie das Quellvolume verschlüsselt kopieren
Ja	Kopiert erneut verschlüsselt mit dem angegebenen Schlüssel

Verschlüsselte Quellvolumes (kontoübergreifend)

Sie geben eine an KMS key	Ergebnis
Nein	Kopieren Sie verschlüsselt mit dem standardmäßigen Amazon EBS-Verschlüsselungsschlüssel Ihres Kontos

Sie geben eine an KMS key	Ergebnis
Ja	Mit dem angegebenen Schlüssel verschlüsselt kopieren

Cross-account Kopien verwenden standardmäßig niemals den KMS-Schlüssel des Quellkontos wieder. Wenn Sie einen Schlüssel aus dem Quellkonto verwenden möchten, muss er mit Ihrem Konto geteilt werden.

Überlegungen

- Eine Volumenkopie erfasst einen absturzkonsistenten Zustand des Quell-Volumes zu einem bestimmten Zeitpunkt. Sie enthält nur die Daten, die zum Zeitpunkt der Kopieranforderung auf das Volume geschrieben wurden. Daten, die von Anwendungen oder dem Betriebssystem zwischengespeichert wurden, sind nicht enthalten. Um anwendungskonsistente Kopien zu erhalten, pausieren Sie Schreibvorgänge auf das Volume oder schalten Sie die Anwendung aus, bevor Sie die Kopie erstellen. Verwenden Sie bei Datenbanken den entsprechenden Mechanismus, um verschmutzte Seiten zu löschen und einzufrieren I/O (z. B. unter Linux oder VSS `fsfreeze` unter Windows). Sie können den Schreibvorgang fortsetzen, nachdem die Kopieranforderung zurückgegeben wurde.
- Sie können jeweils nur eine Volumenkopie von einem Quellvolume erstellen. Sie können nachfolgende Kopien desselben Quell-Volumes nur erstellen, wenn die vorherige Volumenkopie vollständig initialisiert wurde.
- Pro Region können maximal 5 Volumenkopien in Bearbeitung sein. Wenn Sie dieses Kontingent überschreiten, erhalten Sie die `CopyVolumesLimitExceeded` Fehlermeldung. Sie können bei https://docs.aws.amazon.com/servicequotas/latest/userguide/request-quota-increase.html Bedarf eine Kontingenterhöhung beantragen.
- Die Volumenkopie muss in derselben Availability Zone wie das Quell-Volume erstellt werden.
- Die Größe der Volumenkopie muss gleich oder größer als die Größe des Quell-Volumes sein.
- Sie können eine Volumenkopie nicht kopieren, während sie erstellt oder initialisiert wird.
- Um eine Volumenkopie zu erstellen, muss sich das Quell-Volume im `in-use` Zustand `available` OR befinden, und Volumenänderungen müssen den `optimizing` Status `completed` OR aufweisen.

- Für Volumenkopien gelten dieselben Konto- und regionalen Speicher- und IOPS-Kontingente wie für reguläre Amazon EBS-Volumes. Weitere Informationen finden Sie unter Amazon EBS Kontingente.
- Wenn Sie das Quell-Volume löschen, während der Kopiervorgang ausgeführt wird, wird der Kopiervorgang trotzdem abgeschlossen.
- Dem Quellvolume zugewiesene Tags werden der Volumenkopie nicht zugewiesen.
- Sie können keine Kopien von Volumes auf Outposts oder in Wavelength Zones erstellen.

Preisgestaltung

Wenn Sie eine Kopie eines Quell-Volumes erstellen, wird Ihnen der Kopiervorgang in Rechnung gestellt. Die Gebühr für den Kopiervorgang basiert auf der Größe der Datenblöcke, die zum Zeitpunkt der Kopiererstellung auf das Quellvolume geschrieben wurden. Das neu erstellte Volume wird auf die gleiche Weise wie jedes andere Amazon EBS-Volume berechnet. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Kopieren Sie ein Volume

Verwenden Sie eine der folgenden Methoden, um ein Amazon EBS-Volume zu kopieren.

Console

Um ein Volume zu kopieren

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das zu kopierende Volume aus und wählen Sie Aktionen, Volume kopieren.
4. Wählen Sie unter Datenträgertyp den Datenträgertyp für die Kopie aus. Der Standard-Volumetyp ist gp3.
5. Geben Sie für Größe die Größe der Volumenkopie in GiBs ein. Die Größe muss gleich oder größer als die Größe des Quellvolumes sein.
6. (*io1*, *io2*, und *gp3* nur) Geben Sie für IOPS die maximale Anzahl von input/output Vorgängen pro Sekunde (IOPS) für die Volumenkopie ein.
7. (*gp3*nur) Geben Sie für Durchsatz den Durchsatz für die Volumenkopie in ein. MiB/s
8. (*io1*und *io2* nur) Um die Volumenkopie für Amazon EBS zu aktivieren Multi-Attach, wählen Sie Aktivieren Multi-Attach aus.

9. Bei Verschlüsselung hängt die Standardeinstellung vom Quell-Volume und Ihren Kontoeinstellungen ab. Bei Kopien desselben Kontos erbt die Kopie den Verschlüsselungsschlüssel des Quell-Volumes. Für kontoübergreifende Kopien wird der standardmäßige Amazon EBS-Verschlüsselungsschlüssel Ihres Kontos verwendet. Sie können einen anderen vom Kunden verwalteten Schlüssel wählen.
10. (Optional) Um der Volumenkopie benutzerdefinierte Schlagworte zuzuweisen, wählen Sie im Abschnitt Schlagworte die Option Tag hinzufügen aus und geben Sie dann ein Tag-Schlüssel-Wert-Paar ein.
11. Wählen Sie „Volume kopieren“.
12. Das kopierte Volume wechselt in den `creating` Zustand und wechselt dann `available` kurz danach in den Zustand. Sie können es dann an eine Amazon EC2-Instance in derselben Availability Zone anhängen.

AWS CLI

Um ein Volume zu kopieren

Verwenden Sie den Befehl copy-volumes.

Im folgenden Beispiel wird eine Volumekopie von `vol-01234567890abcdef` mit dem `gp3` Datenträgertyp, einer Größe von `100` GiB und einem Durchsatz von erstellt. `250` MiB/s

```
aws ec2 copy-volumes \
--source-volume-id vol-01234567890abcdef \
--volume-type gp3 \
--size 100 \
--throughput 250
```

Um ein unverschlüsseltes Volume während des Kopierens zu verschlüsseln

Verwenden Sie den Befehl copy-volumes mit den Parametern und. `--encrypted` `--kms-key-id`

```
aws ec2 copy-volumes \
--source-volume-id vol-01234567890abcdef \
--encrypted \
--kms-key-id alias/my-key
```

Um mit einem anderen, vom Kunden verwalteten Schlüssel erneut zu verschlüsseln

Verwenden Sie den Befehl copy-volumes mit dem `--kms-key-id` Parameter, um einen anderen Schlüssel anzugeben.

```
aws ec2 copy-volumes \
--source-volume-id vol-01234567890abcdef \
--kms-key-id arn:aws:kms:us-east-1:222222222222:key/abcd1234-a123-456a-a12b-a123b4cd56ef
```

PowerShell

Um ein Volume zu kopieren

Verwenden Sie das cmdlet Copy-EC2Volume.

Im folgenden Beispiel wird eine Volumekopie von `vol-01234567890abcdef` mit dem `gp3` Datenträgertyp, einer Größe von `100` GiB und einem Durchsatz von erstellt `250` MiB/s.

```
Copy-EC2Volume `
-SourceVolumeId vol-01234567890abcdef `
-VolumeType gp3 `
-Size 100 `
-Throughput 250
```

Um ein unverschlüsseltes Volume während des Kopierens zu verschlüsseln

Verwenden Sie das Copy-EC2Volume Cmdlet mit den Parametern und. `-Encrypted` `-KmsKeyId`

```
Copy-EC2Volume `
-SourceVolumeId vol-01234567890abcdef `
-Encrypted $true `
-KmsKeyId "alias/my-key"
```

Um mit einem anderen, vom Kunden verwalteten Schlüssel erneut zu verschlüsseln

Verwenden Sie das Copy-EC2Volume Cmdlet mit dem `-KmsKeyId` Parameter, um einen anderen Schlüssel anzugeben.

```
Copy-EC2Volume `
```

```
-SourceVolumeId vol-01234567890abcdef `
-KmsKeyId "arn:aws:kms:us-east-1:222222222222:key/abcd1234-a123-456a-a12b-
a123b4cd56ef"
```

Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an

Sie können ein verfügbares EBS-Volume an eine oder mehrere Ihrer Instances anfügen, die sich in derselben Availability Zone wie das Volume befindet.

Informationen zum Hinzufügen von EBS-Volumes zu Ihrer Instance beim Start finden Sie unter Instance Block Device Mapping.

Überlegungen

- Die maximale Anzahl von Amazon EBS-Volumes, die Sie an eine Instance anhängen können, hängt vom Instance-Typ ab. Wenn Sie das Limit für Volume-Anhänge für einen Instance-Typ überschreiten, schlägt die Anhangsanforderung mit dem `AttachmentLimitExceeded` Fehler fehl. Weitere Informationen finden Sie unter Volumenlimits für Instanzen.
- Sie können Volumes nur an Instances anhängen, die sich in derselben Availability Zone befinden.
- Multi-Attach aktivierte Volumes können an bis zu 16 Instances angehängt werden. Weitere Informationen finden Sie unter Hängen Sie ein EBS-Volume mit mehreren EC2-Instances an Multi-Attach.
- Wenn das Volume einen AWS Marketplace Produktcode hat:
  - Sie können es nur an eine gestoppte Instanz anhängen.
  - Sie müssen den AWS Marketplace Code abonniert haben, der sich auf dem Volume befindet.
  - Die Konfiguration der Instanz, wie z. B. ihr Typ und ihr Betriebssystem, muss diesen speziellen AWS Marketplace Code unterstützen. Beispielsweise können Sie nicht ein Volume von einer Windows-Instance trennen und an eine Linux-Instance anfügen.
  - AWS Marketplace Codes werden vom Volume auf die Instanz kopiert.
- Dieser von Ihnen angegebene Gerätename wird von Amazon EC2 verwendet. Der Blockgerätetreiber kann das Gerät mit einem Gerätenamen mounten, der sich von dem von Ihnen angegebenen unterscheidet. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon EC2-Instances.
- In einigen Fällen kann ein anderes Volume als das Volume verwendet werden, das an die Instance angehängt ist `/dev/xvda` oder das Root-Volume für die Instance werden `/dev/sda` kann. Dies

kann passieren, wenn Sie das Root-Volume einer anderen Instance oder ein Volume, das aus dem Snapshot eines Root-Volumes erstellt wurde, an eine Instance mit einem vorhandenen Root-Volume anhängen. Weitere Informationen finden Sie unter Vom falschen Volume starten.

- Einige Instance-Typen unterstützen mehr als eine EBS-Karte. Sie können die EBS-Karte für das Volume auswählen, an das angehängt werden soll, indem Sie den EBS-Kartenindex angeben. Informationen zu Instances, die mehrere EBS-Karten unterstützen, finden Sie unter EBS-Karten.
  - Ihr Root-Volume muss an den EBS-Kartenindex angehängt sein. `0`
  - Für Instances, die mehrere EBS-Karten unterstützen: Wenn Sie den EBS-Kartenindex nicht angeben, wird Ihr Volume an den EBS-Kartenindex angehängt. `0`
  - Bei der Konfiguration Ihrer EC2-Instances für Hochleistungs-Workloads ist es wichtig, die EBS-Volumes auf der Grundlage der Leistungsanforderungen auf die EBS-Karten auszubalancieren, um zu vermeiden, dass bei einer der EBS-Karten Leistungseinschränkungen auftreten.
  - Das Limit für Volume-Attachments für einen Instance-Typ ist gleichmäßig auf jede EBS-Karte verteilt. Beispielsweise kann auf einer EC2-Instance, die 128 Volume-Anhänge mit 2 EBS-Karten unterstützt, jede EBS-Karte bis zu Volume-Anhänge unterstützen. 64 Wenn Sie das Limit für EBS-Kartenanhänge überschreiten, schlägt die Anfrage mit dem Fehler fehl. `CardAttachmentLimitExceeded`

Console

Um ein EBS-Volume an eine Instance anzuhängen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das anzufügende Volume aus und wählen Sie dann Actions (Aktionen), Attach Volume (Volume anfügen) aus.
4. Geben Sie für Instance die ID der Instance ein oder wählen Sie die Instance aus der Liste der Optionen aus.
5. Führen Sie für den Gerätenamen einen der folgenden Schritte aus:
   - Wählen Sie für ein Root-Volume den erforderlichen Gerätenamen aus dem Abschnitt Reserviert für Root-Volume der Liste aus. In der Regel `/dev/sda1` oder je nach AMI `/dev/xvda` für Linux-Instances oder `/dev/sda1` für Windows-Instances.
   - Wählen Sie für Daten-Volumes einen verfügbaren Gerätenamen aus dem Abschnitt Für Daten-Volumes empfohlen der Liste aus.

- Um einen benutzerdefinierten Gerätenamen zu verwenden, wählen Sie Benutzerdefinierten Gerätenamen angeben aus und geben Sie dann den zu verwendenden Gerätenamen ein.

6. Wählen Sie Attach volume (Volume anfügen) aus.
7. Stellen Sie eine Verbindung mit Ihrer Instance her und mounten Sie das Volume. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

AWS CLI

Um ein EBS-Volume an eine Instance anzuhängen

Verwenden Sie den Befehl attach-volume. Im folgenden Beispiel wird das angegebene Volume unter Verwendung des angegebenen Gerätenamens an die angegebene Instance angehängt.

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --device /dev/sdf
```

PowerShell

Um ein EBS-Volume an eine Instance anzuhängen

Verwenden Sie das cmdlet Add-EC2Volume. Im folgenden Beispiel wird das angegebene Volume unter Verwendung des angegebenen Gerätenamens an die angegebene Instance angehängt.

```
Add-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -InstanceId i-1234567890abcdef0 `
    -Device /dev/sdf
```

Hängen Sie ein EBS-Volume mit mehreren EC2-Instances an Multi-Attach

Amazon EBS Multi-Attach ermöglicht es Ihnen, ein einzelnes bereitgestelltes IOPS-SSD-Volume (`io1`oder`io2`) an mehrere Instances anzuhängen, die sich in derselben Availability Zone befinden. Sie können mehrere Multi-Attach aktivierte Volumes an eine Instance oder eine Gruppe von Instances anhängen. Jede Instance, an die das Volume angehängt ist, hat volle Lese- und

Schreibberechtigungen für das gemeinsam genutzte Volume. Multi-Attacherleichtert es Ihnen, eine höhere Anwendungsverfügbarkeit in Anwendungen zu erreichen, die gleichzeitige Schreibvorgänge verwalten.

Preise und Fakturierung

Für die Nutzung von Amazon EBS Multi-Attach fallen keine zusätzlichen Gebühren an. Ihnen werden die Standardgebühren berechnet, die für Bereitgestellte IOPS-SSD-Volumes (`io1` und `io2`) gelten. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Inhalt

- Überlegungen und Einschränkungen
- Leistung für Multi-Attach Amazon EBS-Volumes
- Für ein Amazon Multi-Attach EBS-Volume aktivieren
- Multi-Attach Für ein Amazon EBS-Volume deaktivieren
- Verwenden Sie NVMe-Reservierungen mit Multi-Attach aktivierten Amazon EBS-Volumes

Überlegungen und Einschränkungen

- Multi-Attach aktivierte Volumes können an bis zu 16 Instances angehängt werden, die auf dem Nitro-System basieren und sich in derselben Availability Zone befinden.
- Unterstützung für Multi-Attach aktivierte Linux-Instanzen `io1` und `io2` Volumes. Windows-Instanzen unterstützen nur Multi-Attach aktivierte `io2` Volumes.
- Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Weitere Informationen finden Sie unter Volumenbeschränkungen für Instanzen.
- Multi-Attach wird ausschließlich auf bereitgestellten IOPS-SSD-Volumes (`io1`und`io2`) unterstützt.
- Multi-Attach for `io1` volumes ist in allen Regionen verfügbar, die Unterstützung bieten. `io1`

  Multi-Attach for `io2` ist in allen Regionen verfügbar, die Unterstützung bieten`io2`.

> **Note**
>
> Für eine bessere Leistung, Konsistenz und Langlebigkeit bei geringeren Kosten empfehlen wir die Verwendung von `io2`-Volumes.

- Standard-Dateisysteme wie XFS und EXT4 sind nicht für den gleichzeitigen Zugriff von mehreren Servern wie EC2-Instances ausgelegt. Sie sollten ein geclustertes Dateisystem verwenden, um sicherzustellen, dass Ihre Daten für Ihre Produktionsworkloads robust und zuverlässig sind.
- Multi-Attach aktiviert `io1` und `io2` Volumes unterstützen I/O Fencing. I/O Fencing-Protokolle steuern den Schreibzugriff in einer gemeinsam genutzten Speicherumgebung, um die Datenkonsistenz aufrechtzuerhalten. Ihre Anwendungen müssen die Schreibreihenfolge für die angefügten Instances bereitstellen, um die Datenkonsistenz zu wahren. Weitere Informationen finden Sie unter Verwenden Sie NVMe-Reservierungen mit Multi-Attach aktivierten Amazon EBS-Volumes.
- Multi-Attach aktivierte Volumes können nicht als Startvolumes erstellt werden.
- Multi-Attach aktivierte Volumes können einer Blockgerätezuordnung pro Instanz zugeordnet werden.
- Multi-Attach kann beim Start der Instance weder über die Amazon EC2-Konsole noch über die RunInstances API aktiviert werden.
- Multi-Attach aktivierte Volumes, bei denen ein Problem auf der Amazon EBS-Infrastrukturebene auftritt, sind für alle angeschlossenen Instances nicht verfügbar. Probleme auf der Amazon EC2- oder der Netzwerkebene können sich nur auf einige angefügte Instances auswirken.
- Die folgende Tabelle zeigt die Unterstützung für Volumenänderungen für Multi-Attach aktivierte `io2` Volumes `io1` und Volumes nach der Erstellung.

	`io2`-Volumes	**`io1`**-Volumes
Volume-Typ ändern	✓ **	✓ **
Volume-Größe ändern	✓	✓
Ändern von bereitgestellten IOPS	✓	✓
Aktivieren Multi-Attach	✓ *	✓ *

	io2-Volumes	**io1**-Volumes
Deaktiviert Multi-Attach	✓ *	✓ *

* Sie können das Volume nicht aktivieren oder deaktivieren, Multi-Attach solange das Volume an eine Instance angeschlossen ist.

** Die Änderung des Volumetyps für Multi-Attach aktivierte Volumes wird nur zwischen `io1` und `io2` in beide Richtungen unterstützt, auch wenn das Volume angeschlossen ist. Andere Änderungen des Volumetyps werden nicht unterstützt.

- Multi-Attach aktivierte Volumes werden beim Beenden der Instanz gelöscht, wenn die zuletzt angehängte Instanz beendet wird und wenn diese Instanz so konfiguriert ist, dass das Volume beim Beenden gelöscht wird. Wenn das Volume an mehrere Instances angefügt ist, die unterschiedliche Einstellungen für die Löschung bei Beendigung in den Volume-Blockgerät-Zuweisungen haben, bestimmt die Einstellung für die Blockgerät-Zuweisung der letzten angefügten Instance das Löschverhalten bei Beendigung.

  Um ein vorhersehbares Löschverhalten bei Beendigung zu gewährleisten, aktivieren oder deaktivieren Sie das Löschen bei Beendigung für alle Instances, an die das Volume angefügt ist. Weitere Informationen finden Sie unter Daten beibehalten, wenn eine Instanz beendet wird.
- Sie können ein Multi-Attach aktiviertes Volume mithilfe der CloudWatch Metriken für Amazon EBS-Volumes überwachen. Die Daten werden über alle angefügten Instances aggregiert. Metriken für einzelne angefügte Instances können nicht überwacht werden. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS.

Leistung für Multi-Attach Amazon EBS-Volumes

Jede angefügte Instance kann ihre maximale IOPS-Leistung bis zur maximalen bereitgestellten Leistung des Volumes steigern. Die Gesamtleistung aller angefügten Instances darf jedoch die maximale bereitgestellte Leistung des Volumes nicht überschreiten. Wenn der Bedarf der angefügten Instances nach IOPS höher ist als die Provisioned IOPS des Volumes, überschreitet das Volume die bereitgestellte Leistung nicht.

Angenommen, Sie erstellen ein `io2` Multi-Attach aktiviertes Volume mit `80,000` bereitgestellten IOPS und hängen es an eine `m7g.large` Instance an, die bis zu IOPS unterstützt, und an eine

`r7g.12xlarge` Instance, die bis zu `40,000` IOPS unterstützt. `60,000` Jede Instance kann ihre maximalen IOPS steuern, da sie weniger als die bereitgestellten IOPS des Volumes `80,000` sind. Wenn jedoch beide Instanzen gleichzeitig I/O auf das Volume zugreifen, dürfen ihre kombinierten IOPS die für das Volume bereitgestellte IOPS-Leistung nicht überschreiten. `80,000`

Um eine gleichbleibende Leistung zu erzielen, empfiehlt es sich, die von den angeschlossenen Instances I/O ausgehenden Berechnungen auf die Sektoren eines Multi-Attach aktivierten Volumes abzugleichen.

Weitere Informationen zur IOPS-Leistung für die Amazon EC2-Instance-Typen finden Sie unter Für Amazon EBS optimierte Instance-Typen im Amazon EC2-Benutzerhandbuch.

Für ein Amazon Multi-Attach EBS-Volume aktivieren

Multi-Attach aktivierte Volumes können auf die gleiche Weise verwaltet werden wie jedes andere Amazon EBS-Volume. Um die Multi-Attach Funktion nutzen zu können, müssen Sie sie jedoch für das Volume aktivieren.

Wenn Sie ein neues Volume erstellen, Multi-Attach ist standardmäßig deaktiviert. Sie können es aktivieren Multi-Attach , wenn Sie ein Volume erstellen.

Sie können auch Multi-Attach für `io2` Volumes `io1` und Volumes nach der Erstellung aktivieren, allerdings nur, wenn sie keiner Instanz zugeordnet sind.

Nach der Aktivierung Multi-Attach für ein Volume können Sie das Volume auf dieselbe Weise an eine Instance anhängen, wie Sie jedes andere EBS-Volume anhängen. Weitere Informationen finden Sie unter Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.

Console

Zur Aktivierung Multi-Attach während der Volume-Erstellung

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie Create Volume (Volume erstellen) aus.
4. Wählen Sie für Volumen-Typ die Option Bereitgestellte IOPS-SSD (**`io1`**) oder Bereitgestellte IOPS-SSD (**`io2`**) aus.
5. Wählen Sie für Größe und IOPS die erforderliche Volume-Größe und die Anzahl der bereitzustellenden IOPS aus.

6. Wählen Sie für Availability Zone dieselbe Availability Zone aus, in der sich die Instances befinden.
7. Wählen Sie für Amazon EBS die Option Multi-Attach Enable Multi-Attach aus.
8. (Optional) Wählen Sie für Snapshot-ID den Snapshot aus, aus dem das Volume erstellt werden soll.
9. Legen Sie den Verschlüsselungsstatus für das Volume fest.

   Wenn der ausgewählte Snapshot verschlüsselt ist oder Ihr Konto für die standardmäßige Verschlüsselung aktiviert ist, wird die Verschlüsselung automatisch aktiviert und Sie können sie nicht deaktivieren. Sie können den KMS-Schlüssel für die Verschlüsselung des Volumes auswählen.

   Wenn der ausgewählte Snapshot unverschlüsselt und Ihr Konto standardmäßig nicht für die Verschlüsselung aktiviert ist, ist die Verschlüsselung optional. Um das Volume zu verschlüsseln, wählen Sie für Encryption (Verschlüsselung) die Option Encrypt this volume (Dieses Volume verschlüsseln) und wählen Sie dann den KMS-Schlüssel aus, der zum Verschlüsseln des Volumes verwendet werden soll.

   Sie können verschlüsselte Volumes nur an Instances anfügen, die die Amazon-EBS-Verschlüsselung unterstützen. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung.
10. (Optional) Um dem Volume benutzerdefinierte Tags zuzuweisen, wählen Sie im Abschnitt Tags die Option Tag hinzufügen aus und geben Sie dann ein Tag-Schlüssel/Wert-Paar ein.
11. Wählen Sie Create Volume (Volume erstellen) aus.

Um es nach der Erstellung zu aktivieren Multi-Attach

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus und wählen Sie dann Actions (Aktionen), Modify Volume (Volume ändern) aus.
4. Wählen Sie für Amazon EBS die Option Multi-Attach Enable Multi-Attach aus.
5. Wählen Sie Ändern aus.

AWS CLI

Zur Aktivierung Multi-Attach während der Volumenerstellung

Verwenden Sie den Befehl create-volume mit der `--multi-attach-enabled` Option.

```
aws ec2 create-volume \
    --volume-type io2 \
    --multi-attach-enabled \
    --size 100 \
    --iops 2000 \
    --region us-west-2 \
    --availability-zone us-west-2b
```

Um es nach der Erstellung zu aktivieren Multi-Attach

Verwenden Sie den Befehl modify-volume mit der Option. `--multi-attach-enabled`

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --multi-attach-enabled
```

PowerShell

Zur Aktivierung während der Volumenerstellung Multi-Attach

Verwenden Sie das New-EC2Volume Cmdlet mit dem `-MultiAttachEnabled` Parameter.

```
New-EC2Volume `
    -VolumeType io2 `
    -MultiAttachEnabled $true `
    -Size 100 `
    -Iops 2000 `
    -Region us-west-2 `
    -AvailabilityZone us-west-2b
```

Um es nach der Erstellung zu aktivieren Multi-Attach

Verwenden Sie das Edit-EC2Volume Cmdlet mit dem `-MultiAttachEnabled` Parameter.

```
Edit-EC2Volume `
```

```
    -VolumeId vol-01234567890abcdef `
    -MultiAttachEnabled $true
```

Multi-Attach Für ein Amazon EBS-Volume deaktivieren

Sie können Multi-Attach die Option für ein `io1` `io2` OR-Volume nur deaktivieren, wenn es nicht an eine Instance angehängt ist.

Console

Zur Deaktivierung Multi-Attach nach der Erstellung

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus und wählen Sie dann Actions (Aktionen), Modify Volume (Volume ändern) aus.
4. Deaktivieren Sie für Amazon EBS Multi-Attach die Option Aktivieren Multi-Attach.
5. Wählen Sie Ändern aus.

AWS CLI

Um es nach der Erstellung zu deaktivieren Multi-Attach

Verwenden Sie den Befehl modify-volume mit der Option. `-no-multi-attach-enabled`

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --no-multi-attach-enabled
```

PowerShell

Zum Deaktivieren nach der Erstellung Multi-Attach

Verwenden Sie das Edit-EC2Volume Cmdlet mit dem `-MultiAttachEnabled` Parameter.

```
Edit-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -MultiAttachEnabled $false
```

Verwenden Sie NVMe-Reservierungen mit Multi-Attach aktivierten Amazon EBS-Volumes

Multi-Attach aktiviert `io1` und `io2` Volumes unterstützen NVMe-Reservierungen. Dabei handelt es sich um eine Reihe von Storage-Fencing-Protokollen nach Industriestandard. Mit diesen Protokollen können Sie Reservierungen erstellen und verwalten, die den Zugriff mehrerer Instances auf ein gemeinsam genutztes Volume steuern und koordinieren. Anwendungen für gemeinsam genutzten Speicher verwenden Reservierungen, um sicherzustellen, dass die Daten konsistent bleiben.

Inhalt

- Voraussetzungen
- Unterstützung für NVMe-Reservierungen aktivieren
- Unterstützte NVMe-Reservierungsbefehle
- Preisgestaltung

Voraussetzungen

NVMe-Reservierungen werden unterstützt, wenn `io2` Volumes Multi-Attach aktiviert `io1` sind. Multi-Attach aktivierte Volumes können nur an Instanzen angehängt werden, die auf dem Nitro-System erstellt wurden.

NVMe-Reservierungen werden unter den folgenden Betriebssystemen unterstützt:

- SUSE Linux Enterprise 12 SP3 und höher
- RHEL 8.3 und höher
- Amazon-Linux-2 und höher
- Windows Server 2016 und höher

> **Note**
>
> Für unterstützte Windows Server-AMIs vom Jahr 2023.09.13 und höher sind die erforderlichen NVMe-Treiber enthalten. Für frühere AMIs müssen Sie auf die NVMe-Treiberversion 1.5.0 oder höher aktualisieren. Weitere Informationen finden Sie unter AWS NVMe-Treiber.

Wenn Sie EC2Launch v2 zur Initialisierung Ihrer Festplatten verwenden, müssen Sie ein Upgrade auf Version 2.0.1521 oder höher durchführen. Weitere Informationen finden Sie unter Verwenden des EC2Launch v2-Agenten.

Unterstützung für NVMe-Reservierungen aktivieren

Die Unterstützung für NVMe-Reservierungen ist standardmäßig für alle aktivierten `io2` Volumes Multi-Attach aktiviert, die nach dem 18. September 2023 erstellt wurden, und für alle Multi-Attach aktivierten **`io1`** Volumes, die nach dem 1. Oktober 2026 erstellt wurden.

Um die Unterstützung für NVMe-Reservierungen für vorhandene `io2` Volumes zu aktivieren, die vor dem 18. September 2023 erstellt wurden, oder für bestehende `io1` Volumes, die vor dem 1. Oktober 2026 erstellt wurden, müssen Sie alle Instanzen vom Volume trennen und dann die erforderlichen Instances erneut anfügen. Für alle Anhänge, die nach dem Trennen aller Instances erstellt wurden, sind NVMe-Reservierungen aktiviert.

Unterstützte NVMe-Reservierungsbefehle

Amazon EBS unterstützt die folgenden NVMe-Reservierungsbefehle:

Reservierungsregister

Registriert einen Reservierungsschlüssel, hebt die Registrierung auf oder ersetzt ihn. Ein Registrierungsschlüssel wird verwendet, um eine Instance zu identifizieren und zu authentifizieren. Durch die Registrierung eines Reservierungsschlüssels bei einem Volume wird eine Verbindung zwischen der Instance und dem Volume hergestellt. Sie müssen die Instance bei dem Volume registrieren, bevor diese Instance eine Reservierung erwerben kann.

Reservierung: Erwerben

Erwirbt eine Reservierung auf einem Volume, macht einer Reservierung auf einem Namespace zuvor und bricht eine Reservierung auf einem Volume ab. Die folgenden Reservierungstypen können erworben werden:

- Exklusive Reservierung schreiben
- Exklusive Zugangsreservierung
- Exklusiv schreiben – Reservierung nur für Registranten
- Exklusiver Zugang – Reservierung nur für Registranten
- Exklusiv schreiben – Reservierung für alle Registranten
- Exklusiver Zugang – Reservierung für alle Registranten

Freigabe der Reservierung

Gibt eine Reservierung für einen Band frei oder löscht sie.

Reservierungsbericht

Beschreibt den Registrierungs- und Reservierungsstatus eines Bandes.

Preisgestaltung

Für die Aktivierung und Verwendung fallen keine zusätzlichen Kosten an. Multi-Attach

Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung

Nachdem Sie ein Amazon EBS-Volume an Ihre Instance angehängt haben, wird es als Blockgerät angezeigt. Sie können das Volume mit einem beliebigen Dateisystem formatieren und dann mounten. Nachdem Sie das EBS-Volume für die Verwendung verfügbar gemacht haben, können Sie mit den gleichen Methoden darauf zugreifen, wie auf jedes andere Volume. Alle in dieses Dateisystem geschriebenen Daten werden auf das EBS-Volume geschrieben und sind für Anwendungen, die das Gerät verwenden, transparent.

Sie können Snapshots Ihres EBS-Volumes zu Backup-Zwecken erstellen oder als Basis für die Erstellung eines weiteren Volumes verwenden. Weitere Informationen finden Sie unter Amazon EBS-Snapshots.

Wenn das EBS-Volume, das Sie zur Verwendung vorbereiten, größer als 2 TiB ist, müssen Sie ein GPT-Partitionierungsschema verwenden, um auf das gesamte Volume zuzugreifen. Weitere Informationen finden Sie unter Einschränkungen für Amazon-EBS-Volumes.

Linux-Instances

Formatieren und Mounten eines verknüpften Volumes

Angenommen, Sie haben eine EC2-Instance mit einem EBS-Volume für das Root-Gerät, `/dev/xvda`, und Sie haben soeben ein leeres EBS-Volume mithilfe von `/dev/sdf` mit der Instance verknüpft. Gehen Sie wie folgt vor, damit das neu verknüpfte Volume verwendet werden kann.

So formatieren und mounten Sie ein EBS-Volume unter Linux

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu Ihrer Linux-Instance her.

2. Das Gerät kann mit einer Instance mit einem anderen als dem von Ihnen in der Blockgerät-Zuweisung angegeben Namen verknüpft werden. Weitere Informationen finden Sie unter Gerätenamen auf Linux-Instances. Verwenden Sie den Befehl lsblk, um Ihre verfügbaren Datenträger und (ggf.) deren Mounting-Punkte anzuzeigen, damit Sie anhand dieser Informationen den richtigen Gerätenamen ermitteln können. Die Ausgabe von lsblk entfernt das Präfix `/dev/` aus vollständigen Gerätepfaden.

   Im Folgenden finden Sie eine Beispielausgabe für eine Instance, die auf dem Nitro-System basiert und EBS-Volumes als NVMe-Blockgeräte verfügbar macht. Das Root-Gerät ist `/dev/nvme0n1`, das zwei Partitionen mit den Namen `nvme0n1p1` und `nvme0n1p128` hat. Das verknüpfte Volume ist `/dev/nvme1n1`, das keine Partitionen hat und noch nicht gemountet ist.

   ```
   [ec2-user ~]$ lsblk
   NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme1n1       259:0    0  10G  0 disk
   nvme0n1       259:1    0   8G  0 disk
   -nvme0n1p1    259:2    0   8G  0 part /
   -nvme0n1p128  259:3    0   1M  0 part
   ```

   Nachstehend finden Sie eine Beispielausgabe für eine T2-Instance. Das Root-Gerät ist `/dev/xvda`, die eine Partition mit dem Namen `xvda1` hat. Das verknüpfte Volume ist `/dev/xvdf`, das keine Partitionen hat und noch nicht gemountet ist.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   -xvda1  202:1    0    8G  0 part /
   xvdf    202:80   0   10G  0 disk
   ```

3. Stellen Sie fest, ob es ein Dateisystem auf dem Volume gibt. Neue Volumes sind unformatierte Blockgeräte. Sie müssen ein Dateisystem auf ihnen erstellen, bevor Sie sie mounten und verwenden können. Auf Volumes, die aus Snapshots erstellt wurden, ist wahrscheinlich bereits ein Dateisystem vorhanden. Wenn Sie ein dann weiteres Dateisystem erstellen, werden bei diesem Vorgang Ihre Daten überschrieben.

   Verwenden Sie eine oder beide der folgenden Methoden, um festzustellen, ob auf dem Volume ein Dateisystem vorhanden ist:

- Verwenden Sie den Befehl file -s, um Informationen zu einem speziellen Gerät zu erhalten, z. B. den zugehörigen Dateisystemtyp. Wenn die Ausgabe einfach `data` anzeigt, so wie in der folgenden Beispielausgabe, ist auf dem Gerät kein Dateisystem vorhanden.

  ```
  [ec2-user ~]$ sudo file -s /dev/xvdf
  /dev/xvdf: data
  ```

  Wenn das Gerät ein Dateisystem hat, zeigt der Befehl Informationen zum Dateisystemtyp an. In der folgenden Ausgabe ist beispielsweise ein Root-Gerät mit XFS-Dateisystem zu sehen.

  ```
  [ec2-user ~]$ sudo file -s /dev/xvda1
  /dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
  ```

- Verwenden Sie den lsblk -f-Befehl, um Informationen über alle an die Instance angehängten Geräte zu erhalten.

  ```
  [ec2-user ~]$ sudo lsblk -f
  ```

  Die folgende Ausgabe zeigt beispielsweise, dass drei Geräte an die Instances —, `nvme1n1`, `nvme0n1` und `nvme2n1` angeschlossen sind. In der ersten Spalte werden die Geräte und ihre Partitionen aufgeführt. Die Spalte `FSTYPE` zeigt den Dateisystemtyp für jedes Gerät. Wenn die Spalte für ein bestimmtes Gerät leer ist, bedeutet dies, dass das Gerät kein Dateisystem hat. In diesem Fall sind das Gerät `nvme1n1` und Partition `nvme0n1p1` auf Gerät `nvme0n1` beide mit dem XFS-Dateisystem formatiert, während das Gerät `nvme2n1` und Partition `nvme0n1p128` auf Gerät `nvme0n1` keine Dateisysteme haben.

  ```
  NAME  FSTYPE LABEL UUID      MOUNTPOINT
  nvme1n1         xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
  nvme0n1
  ##nvme0n1p1 xfs     / 90e29211-2de8-4967-b0fb-16f51a6e464c         /
  ##nvme0n1p128
  nvme2n1
  ```

Wenn die Ausgabe dieser Befehle zeigt, dass auf dem Gerät kein Dateisystem vorhanden ist, müssen Sie eines erstellen.

4. (Bedingt) Wenn Sie im vorherigen Schritt festgestellt haben, dass es ein Dateisystem auf dem Gerät gibt, überspringen Sie diesen Schritt. Wenn Sie ein leeres Volume haben, erstellen Sie mit dem Befehl mkfs -t ein Dateisystem auf dem Volume.

   > **Warning**
   >
   > Verwenden Sie diesen Befehl nicht, wenn Sie ein Volume mounten, auf dem sich bereits Daten befinden (z. B. ein Volume, das aus einem Snapshot erstellt wurde). Andernfalls formatieren Sie das Volume und löschen die vorhandenen Daten.

   ```
   [ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
   ```

   Wenn Sie die Fehlermeldung erhalten, dass `mkfs.xfs` nicht gefunden wurde, können Sie mit folgendem Befehl die XFS-Tools installieren und anschließend den vorherigen Befehl wiederholen:

   ```
   [ec2-user ~]$ sudo yum install xfsprogs
   ```

5. Erstellen Sie mit dem Befehl mkdir das Mountingpunkt-Verzeichnis für das Volume. Der Mounting-Punkt ist die Position des Volumes in der Dateisystemstruktur und wo nach dem Mounten des Volumes Dateien gelesen und geschrieben werden. Im folgenden Beispiel wird ein Verzeichnis mit dem Namen erstell `/data`.

   ```
   [ec2-user ~]$ sudo mkdir /data
   ```

6. Mounten Sie das Volume oder die Partition in das Mountingpunkt-Verzeichnis, das Sie im vorherigen Schritt erstellt haben.

   Wenn das Volume keine Partitionen hat, verwenden Sie den folgenden Befehl und geben Sie den Gerätenamen an, um das gesamte Volume zu mounten.

   ```
   [ec2-user ~]$ sudo mount /dev/xvdf /data
   ```

   Wenn das Volume Partitionen hat, verwenden Sie den folgenden Befehl und geben Sie den Partitionsnamen an, um eine Partition zu mounten.

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /data
```

7. Überprüfen Sie die Dateiberechtigungen Ihrer Volumebereitstellung, um sicherzustellen, dass Ihre Benutzer und Anwendungen auf das Volume schreiben können. Weitere Informationen zu Dateiberechtigungen finden Sie unter Dateisicherheit im Linux-Dokumentationsprojekt.
8. Der Mountingpunkt wird nach dem Neustarten der Instance nicht automatisch beibehalten. Um dieses EBS-Volume nach dem Neustart automatisch zu mounten, folgen Sie dem nächsten Verfahren.

Automatisches Mounten eines verknüpften Volumes nach dem Neustart

Um ein verknüpftes EBS-Volume bei jedem Neustart des Systems zu mounten, fügen Sie der Datei `/etc/fstab` einen Eintrag für das Gerät hinzu.

Sie können den Gerätenamen, z. B. `/dev/xvdf`, in `/etc/fstab` verwenden, empfohlen wird jedoch die Verwendung des 128-Bit-UUID (Universally Unique Identifier) des Geräts. Die Gerätenamen können geändert werden, aber der UUID bleibt während der gesamten Nutzungsdauer der Partition bestehen. Durch Verwenden des UUID reduzieren Sie das Risiko, dass das System nach einer Neukonfiguration der Hardware nicht mehr gestartet werden kann. Weitere Informationen finden Sie unter Ordnen Sie Amazon EBS-Volumes NVMe-Gerätenamen zu.

So mounten Sie ein verknüpftes Volume nach dem Neustart automatisch

1. (Optional) Erstellen Sie ein Backup der Datei `/etc/fstab` für den Fall, dass Sie diese Datei beim Bearbeiten versehentlich beschädigen oder löschen.

   ```
   [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
   ```

2. Verwenden Sie den Befehl blkid, um den UUID des Geräts zu finden. Notieren Sie sich die UUID des Geräts, das Sie nach dem Neustart mounten möchten. Sie werden sie im folgenden Schritt brauchen.

   Der folgende Befehl zeigt beispielsweise, dass zwei Geräte an der Instance gemountet sind und die UUIDs für beide Geräte angezeigt werden.

   ```
   [ec2-user ~]$ sudo blkid
   /dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
    PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
   ```

```
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

Verwenden Sie für Ubuntu 18.04 den lsblk-Befehl.

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. Öffnen Sie die Datei `/etc/fstab` mit einem Texteditor Ihrer Wahl, z. B. nano oder vim.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. Fügen Sie der Datei `/etc/fstab` den folgenden Eintrag hinzu, um das Gerät am angegebenen Mountingpunkt zu mounten. Die Felder sind der UUID-Wert, der vom Befehl blkid (oder lsblk für Ubuntu 18.04) zurückgegeben wurde, der Mountingpunkt, das Dateisystem und die empfohlenen Mountingoptionen für das Dateisystem. Um weitere Informationen zu den erforderlichen Feldern zu erhalten, führen Sie `man fstab` aus, um das fstab-Handbuch zu öffnen.

   Im folgenden Beispiel wird das Gerät mit der UUID am Bereitstellungspunkt gemountet `/data` und `aebf131c-6957-451e-8d34-ec978d9581ae` das Dateisystem verwendet. `xfs` Es verwendet auch die Flags und`defaults`. `nofail` Es gibt `0` an, dass verhindert werden soll, dass das Dateisystem gedumpt wird, und gibt an, dass es sich nicht 2 um ein Root-Gerät handelt.

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae  /data  xfs  defaults,nofail  0  2
```

> **Note**
>
> Wenn Sie Ihre Instance jemals booten, ohne dass dieses Volume verknüpft ist (z. B. nachdem das Volume zu einer anderen Instances verschoben wurde), ermöglicht die Mountingoption `nofail` das Starten der Instance, auch wenn beim Mounten des Volumes Probleme auftreten. Unter Debian-Derivaten wie Ubuntu-Versionen vor 16.04 muss außerdem die Mount-Option `nobootwait` hinzugefügt werden.

5. Um zu prüfen, ob der Eintrag funktioniert, führen Sie die folgenden Befehle aus, um das Mounting des Geräts aufzuheben und dann alle Dateisysteme in `/etc/fstab` zu mounten. Wenn es keine Fehler gibt, ist die `/etc/fstab`-Datei in Ordnung und das Dateisystem wird nach dem Neustart automatisch gemountet.

```
[ec2-user ~]$ sudo umount /data
```

```
[ec2-user ~]$ sudo mount -a
```

Wenn Sie eine Fehlermeldung erhalten, beheben Sie die Fehler in der Datei.

> **Warning**
>
> Fehler in der Datei `/etc/fstab` können dazu führen, dass ein System nicht mehr gestartet werden kann. Fahren Sie das System nicht herunter, wenn Fehler in der Datei `/etc/fstab` auftreten.

Wenn Sie nicht sicher sind, wie Fehler `/etc/fstab` korrigiert werden, und Sie im ersten Schritt dieses Verfahren eine Backup-Datei erstellt haben, können Sie mit dem folgenden Befehl eine Wiederherstellung aus Ihrer Backup-Datei durchführen.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

Windows-Instances

Verwenden Sie eine der folgenden Methoden, um ein Volume auf einer Windows-Instanz verfügbar zu machen.

PowerShell

Um alle EBS-Volumes mit Raw-Partitionen für die Verwendung mit Windows verfügbar zu machen PowerShell

1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu Ihrer Windows-Instance her.
2. Öffnen Sie in der Taskleiste das Startmenü und wählen Sie Windows PowerShell.
3. Verwenden Sie die bereitgestellte Reihe von PowerShell Windows-Befehlen in der geöffneten PowerShell Eingabeaufforderung. Das Skript führt standardmäßig die folgenden Aktionen aus:

    1. Stoppt den ShellHWDetection-Service.
    2. Führt Festplatten auf, bei denen der Partitionsstil roh ist.

3. Erstellt eine neue Partition über die maximale Größe, die der Datenträger und der Partitionstyp unterstützen.
4. Weist einen verfügbaren Laufwerkbuchstaben zu.
5. Formatiert das Dateisystem als NTFS mit der angegebenen Dateisystembezeichnung.
6. Startet den ShellHWDetection-Service erneut.

```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
 -PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
Start-Service -Name ShellHWDetection
```

DiskPart command line tool

Um ein EBS-Volume für die Verwendung mit dem DiskPart Befehlszeilentool verfügbar zu machen

1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu Ihrer Windows-Instance her.
2. Bestimmen Sie die Datenträgernummer, die Sie verfügbar machen möchten:
   1. Öffnen Sie das Startmenü und wählen Sie Windows aus PowerShell.
   2. Verwenden Sie das `Get-Disk`-Cmdlet zum Abrufen einer Liste verfügbarer Festplatten.
   3. Notieren Sie sich in der Befehlsausgabe die Zahl entsprechend des Datenträgers, den Sie verfügbar machen.
3. Erstellen Sie eine Skriptdatei, um DiskPart Befehle auszuführen:
   1. Öffnen Sie das Startmenü und wählen Sie den Datei-Explorer aus.
   2. Navigieren Sie zu einem Verzeichnis wie z. B. C:\, um die Skriptdatei zu speichern.
   3. Wählen Sie (mit der rechten Maustaste) eine leere Stelle im Ordner, um das Dialogfeld zu öffnen, positionieren Sie den Cursor über Neu, um das Kontextmenü aufzurufen, und wählen Sie dann Textdokument.
   4. Benennen Sie die Textdatei mit `diskpart.txt`.
4. Fügen Sie die folgenden Befehle zur Skriptdatei hinzu. Möglicherweise müssen Sie die Datenträgernummer, den Partitionstyp, die Volume-Bezeichnung und den Laufwerksbuchstaben ändern. Das Skript führt standardmäßig die folgenden Aktionen aus:

1. Wählt Datenträger 1 zum Ändern aus.
2. Konfiguriert das Volume für die Verwendung der MBR-Partitionsstruktur (Master Boot Record).
3. Formatiert das Volume als NTFS-Volume.
4. Legt die Volume-Bezeichnung fest.
5. Weist dem Volume einen Laufwerksbuchstaben zu.

> **Warning**
>
> Wenn Sie ein Volume mounten, auf dem bereits Daten vorhanden sind, achten Sie darauf, das Volume nicht neu zu formatieren, da andernfalls die vorhandenen Daten gelöscht werden.

```
select disk 1
attributes disk clear readonly
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

Weitere Informationen finden Sie unter DiskPart Syntax und Parameter.

5. Öffnen Sie eine Befehlszeile, navigieren Sie zu dem Ordner, in dem sich das Skript befindet, und führen Sie den folgenden Befehl aus, um ein Volume zur Verwendung auf dem angegebenen Datenträger verfügbar zu machen:

```
C:\> diskpart /s diskpart.txt
```

Disk Management utility

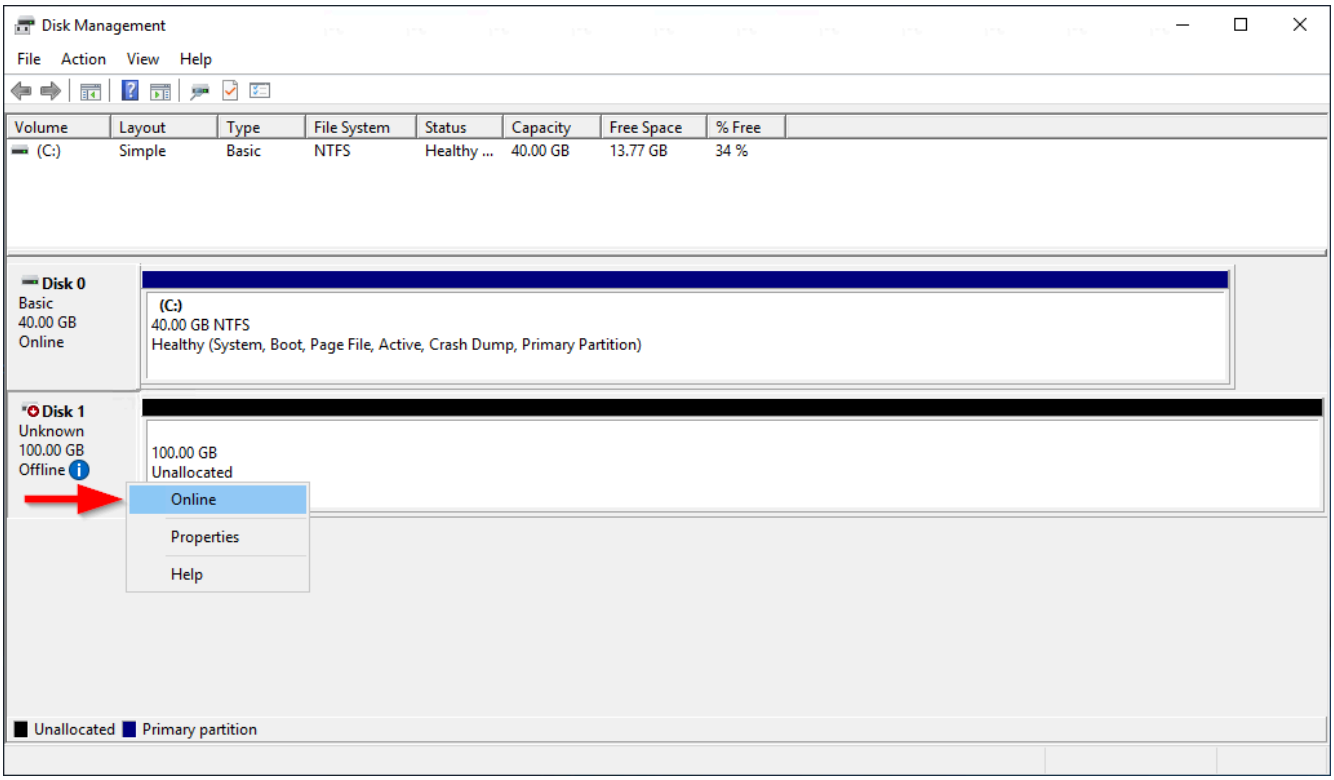
EBS-Volume mit dem Dienstprogramm für die Datenträgerverwaltung verfügbar machen

1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu Ihrer Windows-Instanz her.

2. Starten Sie das Dienstprogramm für die Datenträgerverwaltung. Öffnen Sie in der Taskleiste das Kontextmenü (Rechtsklick) für das Windows-Logo und wählen Sie Datenträgerverwaltung aus.

> **Note**
>
> Wählen Sie unter Windows Server 2008 die Optionen Start, Administrative Tools (Verwaltungstools), Computer Mangement (Computer-Verwaltung) und Disk Management (Datenträgerverwaltung) aus.

3. Bringen Sie das Volume online. Öffnen Sie im unteren Bereich das Kontextmenü (Rechtsklick) im linken Bereich für den Datenträger des EBS-Volume. Klicken Sie auf Online.



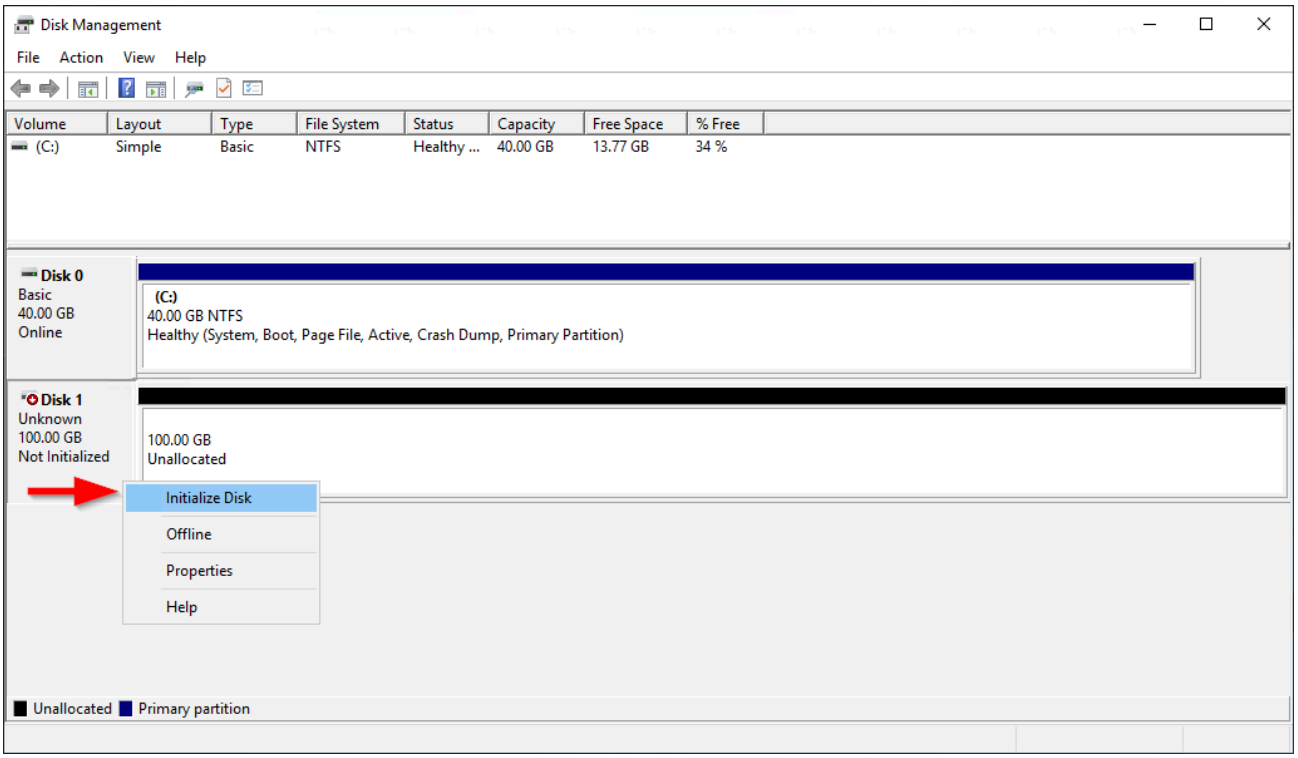
4. (Bedingt) Wenn der Datenträger nicht initialisiert ist, müssen Sie ihn initialisieren, bevor Sie ihn verwenden können. Wenn der Datenträger bereits initialisiert wurde, überspringen Sie diesen Schritt.

> **Warning**
>
> Wenn Sie ein Volume mounten, auf dem bereits Daten vorhanden sind (z. B. einen öffentlichen Datensatz oder ein Volume, das aus einem Snapshot erstellt

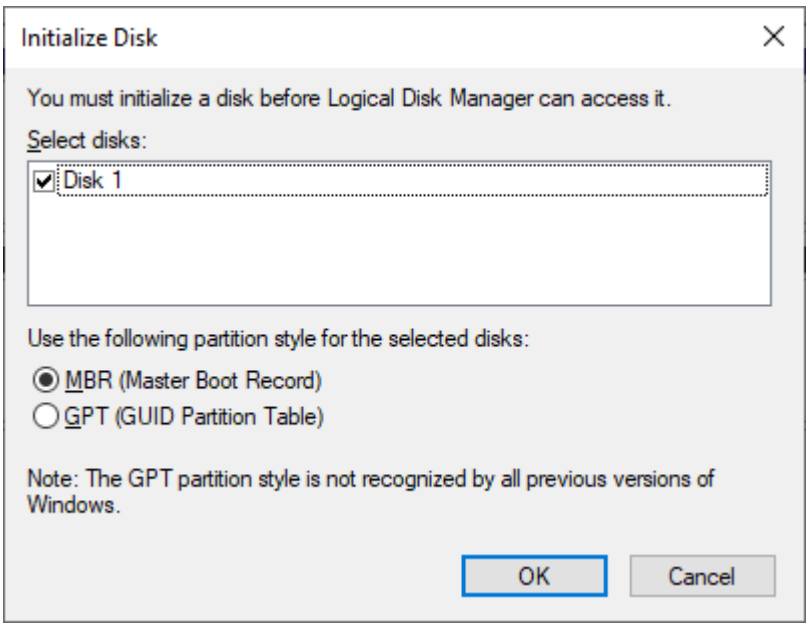
wurde), achten Sie darauf, das Volume nicht neu zu formatieren, da andernfalls die vorhandenen Daten gelöscht werden.

Wenn der Datenträger nicht initialisiert ist, initialisieren Sie ihn folgendermaßen:

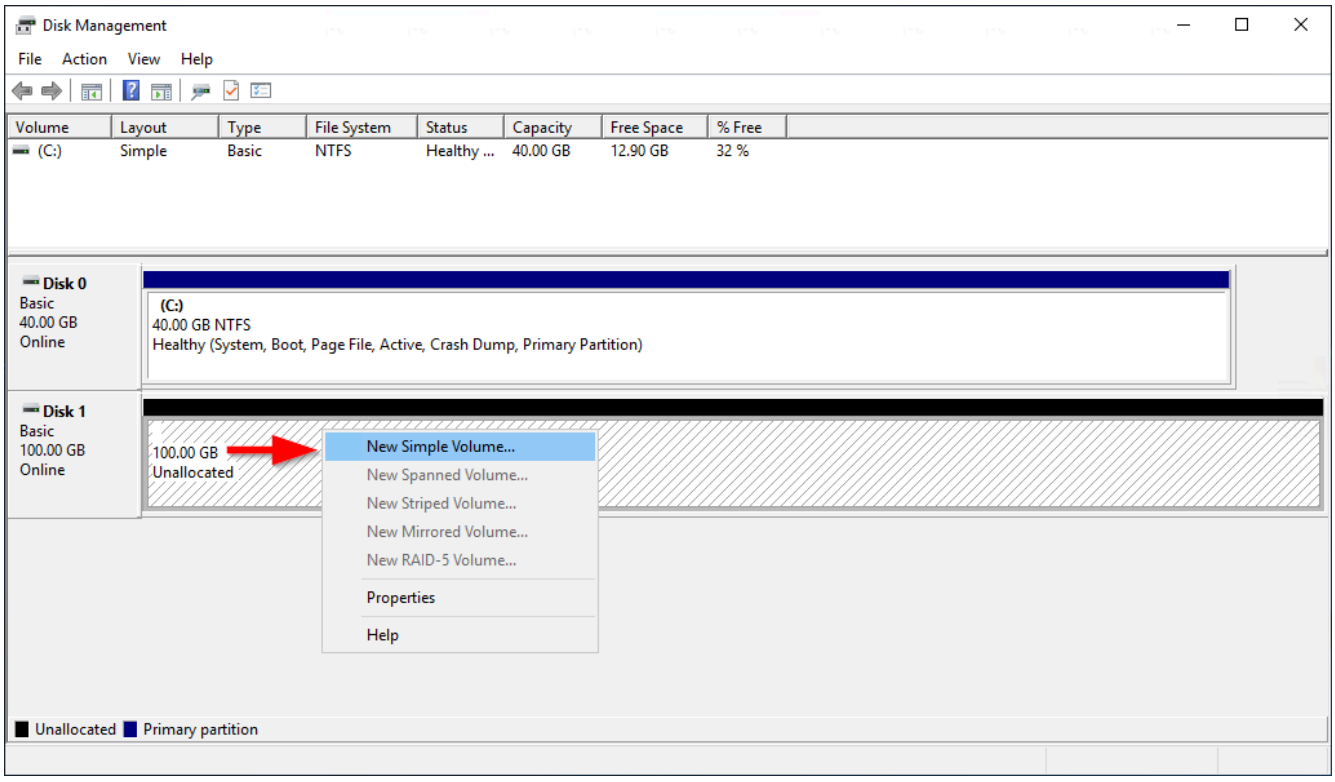
1. Öffnen Sie im linken Bereich das Kontextmenü (Rechtsklick) für den Datenträger und wählen Sie Datenträgerinitialisierung aus.



2. Wählen Sie im Dialogfeld Datenträgerinitialisierung einen Partitionsstil und danach OK aus.



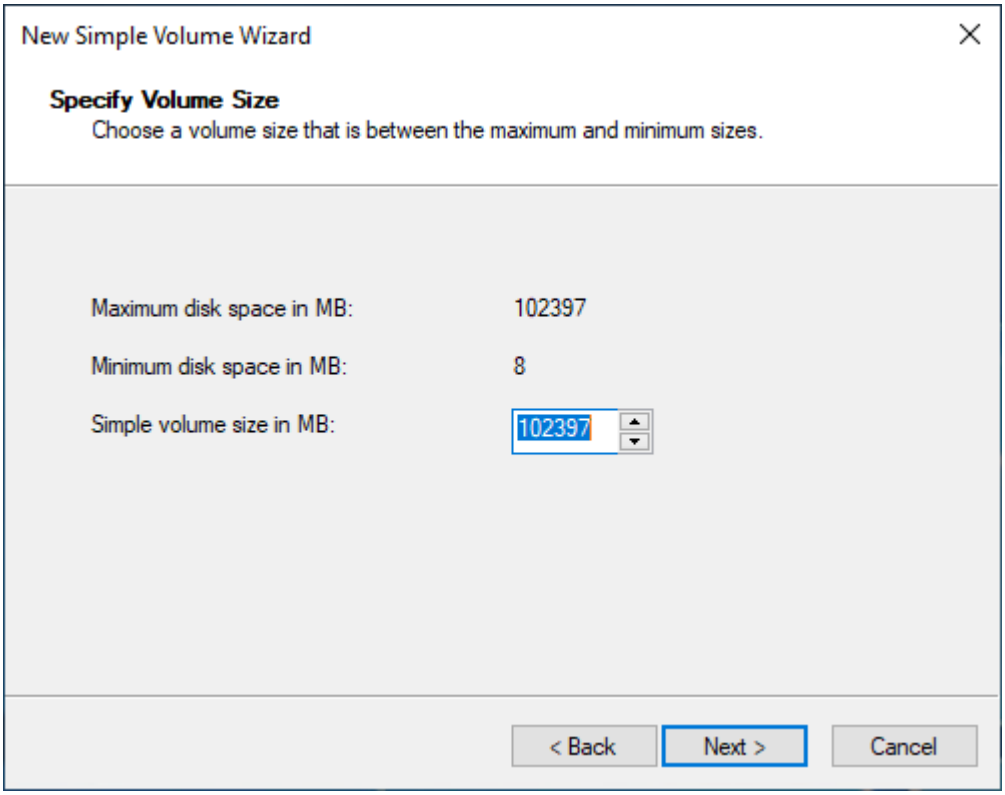
5. Öffnen Sie im rechten Bereich das Kontextmenü (Rechtsklick) für den Datenträger und wählen Sie Neues einfaches Volume aus.



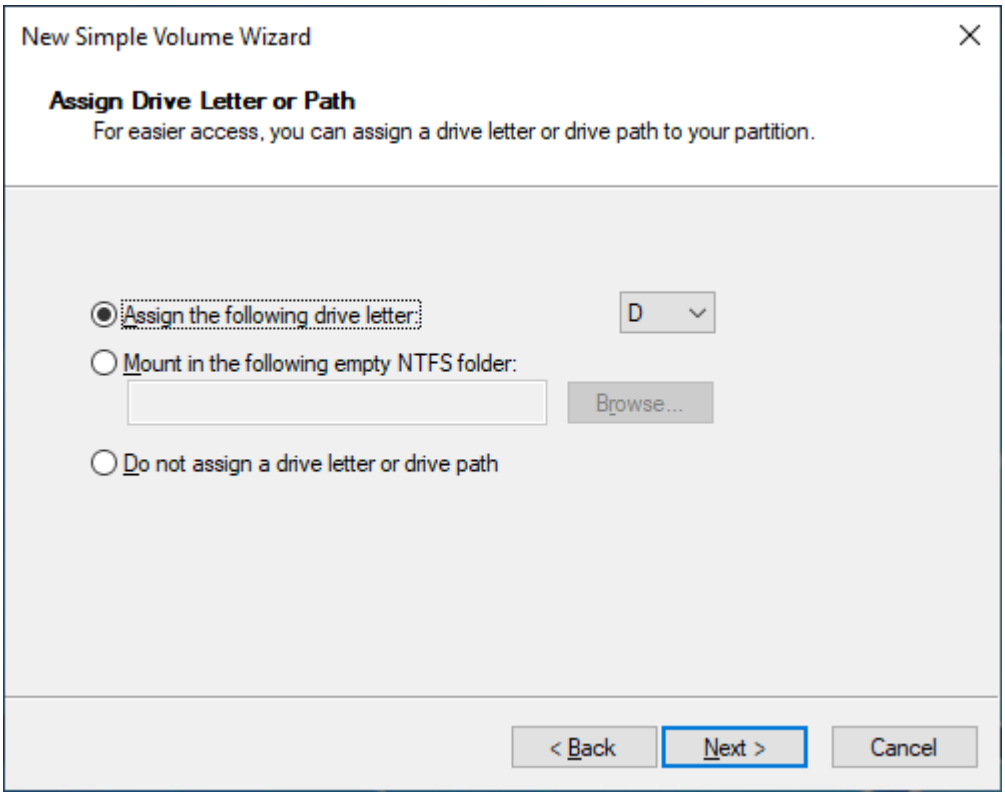
6. Wählen Sie im Assistenten zum Erstellen neuer einfacher Volumes die Option Weiter aus.



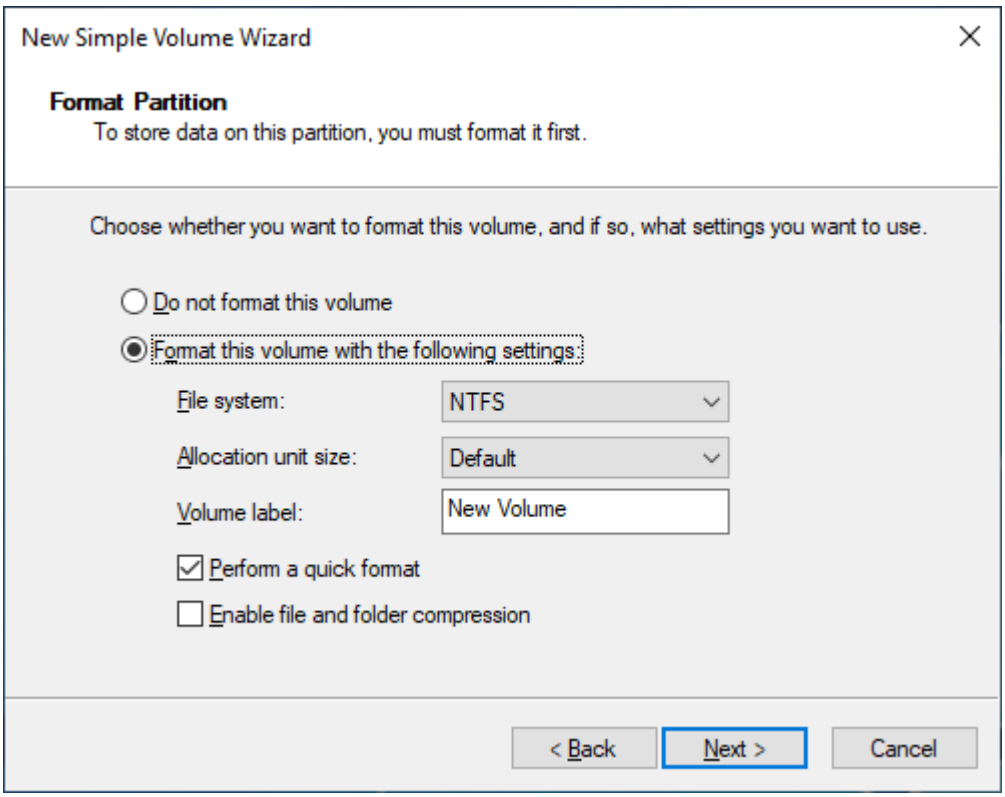
7. Wenn Sie den Standardmaximalwert ändern möchten, geben Sie die Größe des einfachen Volumes in MB an und klicken Sie danach auf Weiter.



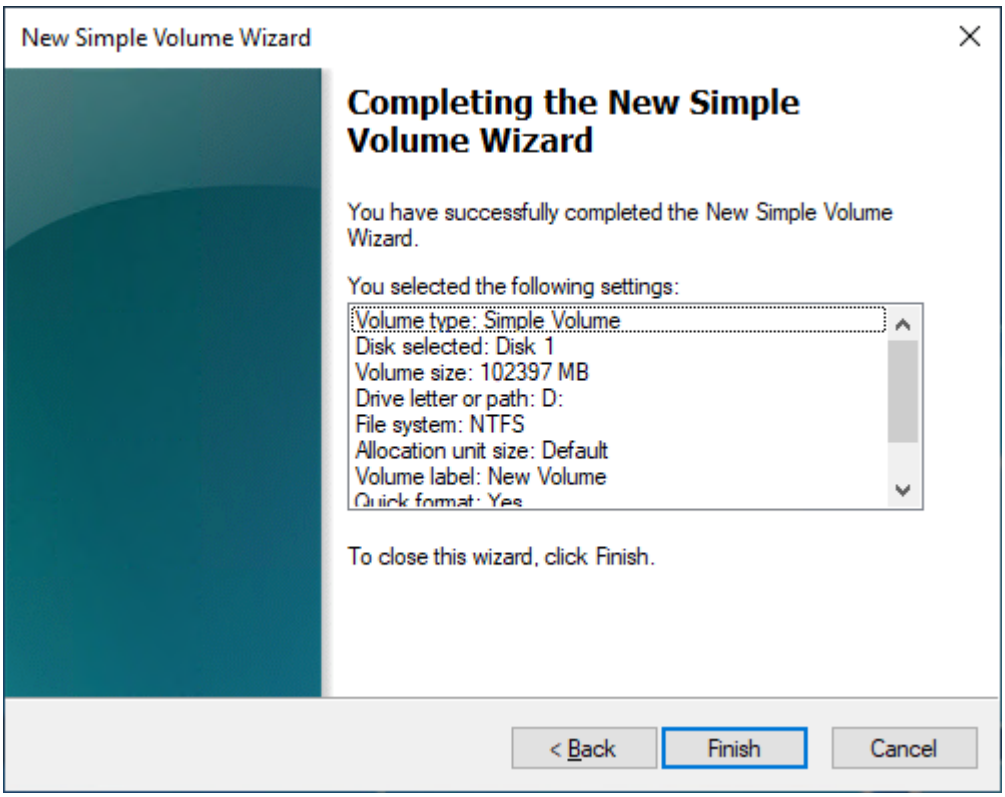
8. Geben Sie ggf. einen bevorzugten Laufwerksbuchstaben im Dropdown Folgenden Laufwerkbuchstaben zuweisen an und wählen Sie dann Weiter aus.



9. Geben Sie eine Volumebezeichnung ein, passen Sie die Standardeinstellungen nach Bedarf an und wählen Sie dann Weiter aus.



10. Überprüfen Sie die Einstellungen und wählen Sie anschließend Fertig stellen aus, um die Änderungen anzuwenden und den Assistenten zum Erstellen neuer einfacher Volumes zu schließen.



Anzeigen von Informationen über ein Amazon EBS-Volume

Sie können beschreibende Informationen zu Ihren EBS-Volumes anzeigen. Sie können beispielsweise Informationen über alle Volumes in einer bestimmten Region oder detaillierte Informationen zu einem einzelnen Volume anzeigen, einschließlich dessen Größe, Volume-Typ, ob das Volume verschlüsselt ist, welcher KMS-Schlüssel zum Verschlüsseln des Volumes verwendet wurde und der spezifischen Instance, an die das Volume angehängt ist.

Sie können zusätzliche Informationen, wie etwa den verfügbaren Speicherplatz, über EBS-Volumes vom Betriebssystem auf der Instance erhalten.

Inhalt

- Anzeigen von Volume-Informationen
- Angaben zur Lautstärke
- Anzeigen von Volumemetriken
- Anzeigen von freiem Festplattenspeicher

Anzeigen von Volume-Informationen

Sie können Informationen zu Ihren EBS-Volumes anzeigen.

Console

Um Informationen zu einem Volume anzuzeigen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Um die Liste zu reduzieren, können Sie die Volumes mithilfe von Tags und Volume-Attributen filtern. Wählen Sie das Filterfeld aus, wählen Sie ein Tag oder ein Volume-Attribut aus und wählen Sie dann den Filterwert aus.
4. Um weitere Informationen zu einem Volume anzuzeigen, wählen Sie seine ID.

So zeigen Sie die EBS-Volumes an, die einer Instance zugeordnet sind

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Auf der Registerkarte Speicher listet der Abschnitt Blockgerät die Volumes auf, die an die Instance angefügt sind. Um Informationen zu einem bestimmten Volume anzuzeigen, wählen Sie seine ID in der Spalte Volume-ID aus.

Amazon EC2 Global View

Sie können Amazon EC2 Global View verwenden, um Ihre Volumes in allen Regionen anzuzeigen, für die Ihr AWS Konto aktiviert ist.

Um eine Zusammenfassung Ihrer EBS-Volumes in allen Regionen zu erhalten

1. Öffnen Sie die Amazon EC2 Global View-Konsole unter. https://console.aws.amazon.com/ec2globalview/home
2. Überprüfen Sie auf der Registerkarte Regions-Explorer unter Zusammenfassung die Anzahl der Ressourcen für Volumes, einschließlich der Anzahl der Volumes und der Anzahl der Regionen. Wählen Sie den unterstrichenen Text aus, um zu sehen, wie sich die Volumenzahl auf die Regionen verteilt.

3. Wählen Sie auf der Registerkarte Globale Suche den Client-Filter Ressourcentyp = Volume aus. Sie können die Ergebnisse weiter filtern, indem Sie eine Region oder ein Tag angeben.

AWS CLI

So zeigen Sie Informationen zu einem EBS-Volume an

Verwenden Sie den Befehl describe-volumes. Im folgenden Beispiel werden die Volumes in der aktuellen Region gezählt.

```
aws ec2 describe-volumes --query "length(Volumes[*])"
```

Das folgende Beispiel listet die Volumes auf, die an die angegebene Instance angehängt sind.

```
aws ec2 describe-volumes \
    --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0" \
    --query Volumes[*].VolumeId \
    --output text
```

Das folgende Beispiel beschreibt das angegebene Volume.

```
aws ec2 describe-volumes --volume-ids vol-01234567890abcdef
```

Es folgt eine Beispielausgabe.

```
{
    "Volumes": [
        {
            "Iops": 3000,
            "VolumeType": "gp3",
            "MultiAttachEnabled": false,
            "Throughput": 125,
            "Operator": {
                "Managed": false
            },
            "VolumeId": "vol-01234567890abcdef",
            "Size": 8,
            "SnapshotId": "snap-0abcdef1234567890",
            "AvailabilityZone": "us-west-2b",
            "State": "in-use",
```

```
            "CreateTime": "2024-05-17T23:23:00.400000+00:00",
            "Attachments": [
                {
                    "DeleteOnTermination": true,
                    "VolumeId": "vol-01234567890abcdef",
                    "InstanceId": "i-1234567890abcdef0",
                    "Device": "/dev/xvda",
                    "State": "attached",
                    "AttachTime": "2024-05-17T23:23:00+00:00"
                }
            ],
            "Encrypted": false
        }
    ]
}
```

PowerShell

So zeigen Sie Informationen zu einem EBS-Volume an

Verwenden Sie das cmdlet Get-EC2Volume. Im folgenden Beispiel werden die Volumen in der aktuellen Region gezählt.

```
(Get-EC2Volume).Count
```

Das folgende Beispiel listet die Volumes auf, die an die angegebene Instance angehängt sind.

```
(Get-EC2Volume `
    -Filters @{Name="attachment.instance-id";Values="i-1234567890abcdef0"}).VolumeId
```

Das folgende Beispiel beschreibt das angegebene Volume.

```
Get-EC2Volume -VolumeId vol-01234567890abcdef
```

Es folgt eine Beispielausgabe.

```
Attachments        : {i-1234567890abcdef0}
AvailabilityZone   : us-west-2b
CreateTime         : 5/17/2024 11:23:00 PM
Encrypted          : False
```

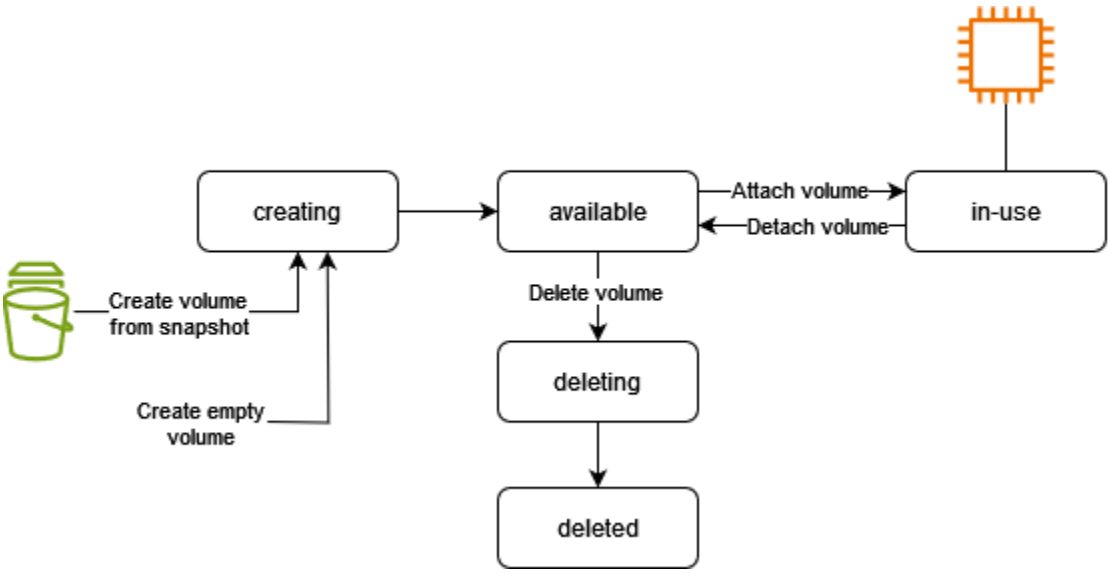
```
FastRestored       : False
Iops               : 3000
KmsKeyId           :
MultiAttachEnabled : False
Operator           : Amazon.EC2.Model.OperatorResponse
OutpostArn         :
Size               : 8
SnapshotId         : snap-0abcdef1234567890
SseType            :
State              : in-use
Tags               : {}
Throughput         : 125
VolumeId           : vol-01234567890abcdef
VolumeType         : gp3
```

Angaben zur Lautstärke

Der Volume-Status beschreibt die Verfügbarkeit eines Amazon EBS-Volumes. Sie können den Volume-Status in der Spalte State auf der Seite Volumes in der Konsole oder mithilfe des Befehls describe-volumes AWS CLI anzeigen.

Ein Amazon EBS-Volume durchläuft vom Moment seiner Erstellung bis zu seinem Löschen verschiedene Status.

Die folgende Abbildung zeigt die Übergänge zwischen den Volumenzuständen. Sie können ein Volume aus einem Amazon EBS-Snapshot erstellen oder ein leeres Volume erstellen. Wenn Sie ein Volume erstellen, wechselt es in den `creating` Status. Nachdem das Volume betriebsbereit ist, wechselt es in den `available` Status. Sie können ein verfügbares Volume an eine Instance anhängen, die sich in derselben Availability Zone wie das Volume befindet. Sie müssen das Volume trennen, bevor Sie es an eine andere Instance anhängen oder löschen können. Sie können ein Volume löschen, wenn Sie es nicht mehr benötigen.



In der folgenden Tabelle sind die Volume-Status zusammengefasst.

Status	Description
`creating`	Das Volume wird erstellt.
`available`	Das Volume ist keiner Instance zugeordnet.
`in-use`	Das Volume ist einer Instance zugeordnet.
`deleting`	Das Volume wird gelöscht.
`deleted`	Das Volume ist gelöscht.
`error`	Die Ihrem EBS-Volume zugrunde liegende Hardware ist ausgefallen, und die mit dem Volume verbundenen Daten sind nicht wiederherstellbar. Informationen zur Wiederherstellung des Volumes oder zur Wiederherstellung der Daten auf dem Volume finden Sie unter Warum hat mein EBS-Volume den Status „Fehler“? .

Anzeigen von Volumemetriken

Zusätzliche Informationen zu Ihren EBS-Volumes erhalten Sie von Amazon CloudWatch. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS.

Anzeigen von freiem Festplattenspeicher

Sie können zusätzliche Informationen, wie etwa den verfügbaren Speicherplatz, über EBS-Volumes vom Betriebssystem auf der Instance erhalten.

Linux-Instances

Verwenden Sie den df -hT Befehl und geben Sie den Gerätenamen an:

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

Windows-Instances

Sie können den freien Speicherplatz anzeigen, indem Sie den Datei-Explorer öffnen und Dieser PC auswählen.

Sie können den freien Speicherplatz auch mithilfe des folgenden `dir`-Befehls und durch Überprüfen der letzten Zeile der Ausgabe anzeigen:

```
C:\> dir C:
 Volume in drive C has no label.
 Volume Serial Number is 68C3-8081

 Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  18,113,662,976 bytes free
```

Sie können den freien Speicherplatz auch anhand des folgenden `fsutil`-Befehls anzeigen:

```
C:\> fsutil volume diskfree C:
Total # of free bytes        : 18113204224
Total # of bytes             : 32210153472
Total # of avail free bytes  : 18113204224
```

> **Tip**
>
> Sie können den CloudWatch Agenten auch verwenden, um Messwerte zur Speicherplatznutzung von einer Amazon EC2-Instance zu erfassen, ohne eine Verbindung zur Instance herzustellen. Weitere Informationen finden Sie unter Erstellen der CloudWatch Agenten-Konfigurationsdatei und Installieren des CloudWatch Agenten im CloudWatch Amazon-Benutzerhandbuch. Wenn Sie die Speicherplatznutzung für mehrere Instances überwachen müssen, können Sie den CloudWatch Agenten auf diesen Instances mithilfe von Systems Manager installieren und konfigurieren. Weitere Informationen finden Sie unter Installieren des CloudWatch Agenten mithilfe des Systems Manager.

Ändern Sie ein Amazon EBS-Volume mithilfe von Elastic Volumes-Vorgängen

Mit Amazon EBS-Elastic Volumes können die Volume-Größe erhöhen, den Volume-Typ ändern oder die Performance Ihrer EBS-Volumes anpassen. Wenn Ihre Instance Elastic Volumes unterstützt, müssen Sie das Volume nicht trennen oder die Instance neu starten. Auf diese Weise können Sie Ihre Anwendung verwenden, während die Änderungen wirksam werden.

Für das Ändern der Konfiguration eines Volumes fallen keine Kosten an. Nachdem Sie eine Volume-Änderung vorgenommen haben, wird Ihnen der neue Volume-Konfigurationspreis berechnet. Weitere Informationen finden Sie in der Amazon EBS-Preisliste.

Inhalt

- Überlegungen
- Einschränkungen
- Anforderungen für Änderungen an Amazon EBS-Volumes
- Änderungen am Amazon EBS-Volume anfordern
- Überwachen Sie den Fortschritt der Änderungen am Amazon EBS-Volume

- Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben

Überlegungen

- Nachdem Sie eine Volumenänderung initiiert haben, müssen Sie warten, bis diese Änderung den `completed` Status erreicht hat, bevor Sie eine weitere Änderung für dasselbe Volume vornehmen können. Sie können ein Volume innerhalb von 24 Stunden bis zu viermal ändern, sofern sich das Volume im `available` Status `in-use` Oder befindet und alle vorherigen Änderungen für dieses Volume ebenfalls gültig sind`completed`. Wenn Sie dieses Limit überschreiten, erhalten Sie eine Fehlermeldung, die angibt, wann Sie Ihre nächste Änderung vornehmen können.
- Volumenänderungen werden nach bestem Wissen und Gewissen durchgeführt. Je nach angeforderter Volume-Konfiguration kann es zwischen einigen Minuten und einigen Stunden dauern, bis sie abgeschlossen sind. In der Regel kann es bis zu sechs Stunden dauern, bis ein 1-TiB-Volume geändert wird. Die Zeit skaliert jedoch nicht immer linear mit der Volumengröße — ein größeres Volumen nimmt möglicherweise weniger Zeit in Anspruch, und ein kleineres Volumen kann mehr Zeit in Anspruch nehmen.
- Größenzunahmen werden wirksam, sobald die Volumenänderung den `optimizing` Status erreicht hat, was in der Regel einige Sekunden dauert.
- Die Änderungszeit wird für Volumes erhöht, die nicht vollständig initialisiert sind. Weitere Informationen finden Sie unter Initialisieren Sie die Volumes nach der Erstellung manuell.
- Wenn Sie den Volume-Typ von `gp2` auf ändern, `gp3` ohne IOPS oder Durchsatzleistung anzugeben, stellt Amazon EBS automatisch die Leistung bereit. Es verwendet entweder die äquivalente Leistung des `gp2` Quell-Volumes oder die `gp3` Basisleistung, je nachdem, welcher Wert höher ist.

  Wenn Sie beispielsweise ein `gp2` 500-GiB-Volume mit 250 MiB/s Durchsatz und 1500 IOPS `gp3` ohne Angabe von IOPS oder Durchsatzleistung ändern, stellt Amazon EBS das Volume automatisch mit 3000 IOPS (`gp3`Basis-IOPS) und 250 MiB/s (entsprechend dem `gp3` Quell-Volume-Durchsatz) bereit. `gp2`
- Wenn Sie beim Ändern eines EBS-Volumes eine Fehlermeldung erhalten oder wenn Sie versuchen, ein EBS Volume zu ändern, das an einen Instance-Typ einer älteren Generation angefügt ist, müssen Sie einen der folgenden Schritte ausführen:
  - Nicht-Stamm-Volume: Trennen Sie das Volume von der Instance, führen Sie die Änderungen durch und fügen Sie das Volume dann wieder an.

- Stamm-Volume: Halten Sie die Instance an, nehmen Sie die Änderungen vor und führen Sie einen Neustart der Instance durch.

Einschränkungen

- Nachdem Sie eine Volume-Änderungsanforderung gesendet haben, können Sie sie nicht stornieren.
- Sie müssen das Volume vergrößern. Sie können die Volumengröße nicht verringern. Sie können jedoch ein kleineres Volume erstellen und dann Ihre Daten mithilfe eines Tools auf Anwendungsebene wie rsync (Linux-Instances) oder robocopy (Windows-Instances) dorthin migrieren.
- Es gibt Grenzen für den maximalen aggregierten Speicher, der über Volumenänderungen angefordert werden kann. Weitere Informationen finden Sie unter Amazon-EBS-Service-Quotas in der Allgemeine Amazon Web Services-Referenz.
- Die neue Volume-Größe darf die unterstützte Kapazität des Dateisystems und des Partitionierungsschemas nicht überschreiten. Weitere Informationen finden Sie unter Einschränkungen für Amazon-EBS-Volumes.
- Wenn Sie den Volume-Typ nicht ändern, müssen die Volume-Größe und die Leistungsänderungen innerhalb der Grenzen des aktuellen Volume-Typs liegen. Wenn Sie den Volume-Typ ändern, müssen die Änderungen an Volume-Größe und Leistung innerhalb der Grenzen des Zieldatenvolumes liegen. Weitere Informationen finden Sie unter Amazon EBS-Volume-Typen.
- Nitro-based Instances unterstützen Volumes, die mit bis zu 256.000 IOPS bereitgestellt werden. Andere Instance-Typen können an Volumes angehängt werden, die mit bis zu 64 000 IOPS bereitgestellt werden, können aber nur bis zu 32 000 IOPS erreichen.
- Bei Multi-Attach aktivierten Volumes können Sie den Volume-Typ zwischen `io1` und `io2` in beide Richtungen ändern, auch wenn das Volume angeschlossen ist. Andere Änderungen des Volumetyps werden nicht unterstützt.

  Wenn Sie den Volumetyp zwischen `io1` und `io2` für ein Multi-Attach aktiviertes Volume ändern, wird der Aktivierungsstatus für NVMe-Reservierungen auf den Ziel-Volume-Typ übertragen.
- Ein Root-Volume vom Typ `io1`, `io2`, `gp2`, `gp3` oder `standard` kann nicht zu einem `st1`- oder `sc1`-Volume geändert werden, auch wenn es von der Instance getrennt ist.
- Wenn das Volume vor dem 3. November 2016 23:40 UTC angefügt wurde, müssen Sie die Elastic Volumes-Unterstützung initialisieren. Weitere Informationen finden Sie unter Initializing Elastic Volumes Support.

- `m3.medium`-Instances unterstützen zwar Volume-Änderungen vollständig, `m3.large`-, `m3.xlarge`- und `m3.2xlarge`-Instances unterstützen jedoch möglicherweise nicht alle Features zur Volume-Änderung.

Anforderungen für Änderungen an Amazon EBS-Volumes

Bei der Änderung eines Amazon EBS-Volumes gelten die folgenden Anforderungen und Einschränkungen. Weitere Informationen über die allgemeinen Anforderungen für EBS-Volumes finden Sie unter Einschränkungen für Amazon-EBS-Volumes.

Themen

- Unterstützte Instance-Typen
- Betriebssystem

Unterstützte Instance-Typen

Elastic Volumes werden auf den folgenden Instances unterstützt:

- Alle Instances der aktuellen Generation
- Die folgenden Instances der vorherigen Generation: C1, C3, C4, G2, I2, M1, M3, M4, R3 und R4

Wenn Ihr Instance-Typ Elastic Volumes nicht unterstützt, finden Sie weitere Informationen unter Ändern eines EBS-Volumes, wenn Elastic Volumes nicht unterstützt wird.

Betriebssystem

Es gelten die folgenden Betriebssystemanforderungen:

Linux

Linux-AMIs erfordern eine GUID-Partitionstabelle (GPT) und GRUB 2 für Boot-Volumes mit 2 TiB (2 048 GiB) oder größer. Viele Linux-AMIs verwenden heute noch immer das MBR-Partitionierungsschema, das nur Boot-Volumes bis 2 TiB unterstützt. Wenn Ihre Instance nicht mit einem Boot-Volume von mehr als 2 TiB startet, ist das von Ihnen verwendete AMI möglicherweise auf eine Startvolumegröße von weniger als 2 TiB beschränkt. Non-boot Für Volumes gilt diese Beschränkung für Linux-Instances nicht.

Bevor Sie versuchen, die Größe eines Boot-Volumes auf über 2 TiB zu erhöhen, können Sie ermitteln, ob das Volume die MBR- oder die GPT-Partitionierung verwendet. Führen Sie hierzu den folgenden Befehl auf Ihrer Instance aus:

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

Eine Amazon Linux-Instance mit GPT-Partitionierung gibt folgende Informationen zurück:

```
GPT fdisk (gdisk) version 0.8.10

  Partition table scan:
    MBR: protective
    BSD: not present
    APM: not present
    GPT: present

  Found valid GPT with protective MBR; using GPT.
```

Eine SUSE-Instance mit MBR-Partitionierung gibt folgende Informationen zurück:

```
GPT fdisk (gdisk) version 0.8.8

  Partition table scan:
    MBR: MBR only
    BSD: not present
    APM: not present
    GPT: not present
```

Windows

Standardmäßig initialisiert Windows Volumes mit einer Master Boot Record (MBR) Partitionierungstabelle. Da MBR nur Volumes unter 2 TiB (2.048 GiB) unterstützt, verhindert Windows die Änderung der Größe von MBR-Volumes über diese Grenze hinaus. In einem solchen Fall ist die Option Extend Volume (Volume erweitern) im Windows-Disk Management (Datenträgerverwaltung)-Hilfsprogramm deaktiviert. Wenn Sie AWS-Managementkonsole oder verwenden AWS CLI , um ein MBR-partitioned Volume zu erstellen, das die Größenbeschränkung überschreitet, kann Windows den zusätzlichen Speicherplatz nicht erkennen oder verwenden.

Um diese Begrenzung zu umgehen, können Sie ein neues, größeres >Volume mit einer GUID-Partitionierungstabelle (GPT) erstellen und die Daten von dem ursprünglichen MBR-Volume darauf kopieren.

So erstellen Sie ein GPT-Volume:

1. Erstellen Sie ein neues, leeres Volume mit der gewünschten Größe in der Availability Zone der EC2-Instance, und verbinden Sie es mit Ihrer Instance.

   > **Note**
   >
   > Das neue Volume darf nicht aus einem Snapshot wiederhergestellt sein.

2. Melden Sie sich bei Ihrem Windows-System an, und öffnen Sie Disk Management (diskmgmt.exe).
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für die neue Festplatte, und wählen Sie Online aus.
4. Wählen Sie im Fenster Initialize Disk die neue Festplatte und dann GPT (GUID Partition Table), OK.
5. Kopieren Sie nach dem Abschluss der Initialisierung mit einem Tool wie robocopy oder teracopy die Daten von dem ursprünglichen Volume zu dem neuen Volume.
6. Ändern Sie unter Disk Management die Laufwerkbuchstaben zu den benötigten Werten, und nehmen Sie das alte Volume offline.
7. Trennen Sie in der Amazon EC2-Konsole das alte Volume von der Instance, starten Sie die Instance neu, um ihre korrekte Funktion zu prüfen, und löschen Sie das alte Volume.

Änderungen am Amazon EBS-Volume anfordern

Mit Elastic Volumes können Sie die Größe dynamisch erhöhen, die Leistung erhöhen oder verringern und den Volume-Typ Ihrer Amazon-EBS-Volumes ändern, ohne sie zu trennen.

Prozessübersicht

1. (Optional) Bevor Sie ein Volume mit wichtigen Daten ändern, besteht eine bewährte Methode darin, einen Snapshot des betroffenen Volumes anzulegen, falls Sie Ihre Änderungen rückgängig machen möchten. Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots.
2. Fordern Sie die Volume-Änderung an.
3. Überwachen Sie den Fortschritt der Volume-Änderung. Weitere Informationen finden Sie unter Überwachen Sie den Fortschritt der Änderungen am Amazon EBS-Volume.

4. Wenn die Größe des Volumes geändert wurde, müssen Sie das Dateisystem des Volumes erweitern, um die größere Speicherkapazität nutzen zu können. Weitere Informationen finden Sie unter Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben.

Inhalt

- Ändern eines EBS-Volumes mit Elastic Volumes
- Ändern eines EBS-Volumes, wenn Elastic Volumes nicht unterstützt wird
- Initialisieren des Elastic-Volumes-Supports (falls erforderlich)

Ändern eines EBS-Volumes mit Elastic Volumes

Bevor Sie beginnen, sollten Sie Folgendes beachten:

- Überlegungen
- Einschränkungen
- Voraussetzungen

Console

Um ein EBS-Volume zu ändern

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus, das Sie ändern möchten, und wählen Sie dann Aktionen, Volume ändern aus.
4. Auf dem Bildschirm Volume ändern werden die Volume-ID und die aktuelle Konfiguration des Volumes einschließlich Typ, Größe, IOPS und Durchsatz angezeigt. Stellen Sie die neuen Konfigurationswerte wie folgt ein:
   - Wenn Sie den Typ ändern möchten, wählen Sie einen Wert für Volume-Typ aus.
   - Um die Größe zu ändern, geben Sie einen neuen Wert für Größe ein.
   - (Nur `gp3`, `io1`, und `io2`) Um den IOPS zu ändern, geben Sie einen neuen Wert für IOPS ein.
   - (Nur `gp3`) Um den Durchsatz zu ändern, geben Sie einen neuen Wert für Durchsatz ein.

5. Wenn Sie mit dem Ändern der Volume-Einstellungen fertig sind, wählen Sie Modify (Ändern) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ändern aus.
6. Wenn Sie die Größe Ihres Volumes erhöht haben, müssen Sie auch die Partition des Volumes erweitern, um die zusätzliche Speicherkapazität zu nutzen. Weitere Informationen finden Sie unter Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben.
7. (Nur Windows-Instanzen) Wenn Sie die Größe eines NVMe-Volumes auf einer Instance erhöhen, die nicht über die AWS NVMe-Treiber verfügt, müssen Sie die Instance neu starten, damit Windows die neue Volume-Größe erkennen kann. Weitere Informationen zur Installation der AWS NVMe-Treiber finden Sie unter AWS NVMe-Treiber.

AWS CLI

Um ein EBS-Volume zu ändern

Verwenden Sie den Befehl modify-volume. Wenn Sie beispielsweise über ein Volume des Typs gp2 mit einer Größe von 100 GiB verfügen, ändert das folgende Beispiel dessen Konfiguration in ein Volume des Typs `io1` mit 10.000 IOPS und einer Größe von 200 GiB.

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --volume-type io1 \
    --iops 10000 \
    --size 200
```

Es folgt eine Beispielausgabe.

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-01234567890abcdef",
        "TargetIops": 10000,
        "StartTime": "2022-01-19T22:21:02.959Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
    }
```

```
}
```

Wenn Sie die Größe Ihres Volumes erhöht haben, müssen Sie auch die Partition des Volumes erweitern, um die zusätzliche Speicherkapazität zu nutzen. Weitere Informationen finden Sie unter Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben.

PowerShell

Um ein EBS-Volume zu ändern

Verwenden Sie das cmdlet Edit-EC2Volume. Wenn Sie beispielsweise ein Volume vom Typ gp2 mit einer Größe von 100 GiB haben, ändert das folgende Beispiel seine Konfiguration in ein Volume des Typs `io1` mit 10.000 IOPS und einer Größe von 200 GiB.

```
Edit-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -VolumeType io1 `
    -Iops 10000 `
    -Size 200
```

Wenn Sie die Größe Ihres Volumes erhöht haben, müssen Sie auch die Partition des Volumes erweitern, um die zusätzliche Speicherkapazität zu nutzen. Weitere Informationen finden Sie unter Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben.

Ändern eines EBS-Volumes, wenn Elastic Volumes nicht unterstützt wird

Wenn Sie einen unterstützten Instance-Typ verwenden, können Sie mit Elastic Volumes die Größe, Leistung und den Volume-Typ Ihrer Amazon EBS-Volumes dynamisch ändern, ohne sie zu trennen.

Wenn Sie Elastic Volumes nicht verwenden, aber das Stamm-Volume (Boot-Volume) ändern müssen, halten Sie die Instance an, ändern Sie das Volume und starten Sie die Instance dann neu.

Nachdem die Instance gestartet wurde, können Sie die Größe des Dateisystems überprüfen, um herauszufinden, ob Ihre Instance den größeren Volume-Speicherplatz erkennt. Verwenden Sie unter Linux den df -h Befehl, um die Größe des Dateisystems zu überprüfen.

```
[ec2-user ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
```

```
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

Wenn die angezeigte Größe nicht der Größe Ihres kürzlich erweiterten Volumes entspricht, müssen Sie das Dateisystem Ihres Geräts erweitern, sodass die Instance den neu verfügbaren Speicherplatz nutzen kann. Weitere Informationen finden Sie unter Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben.

Bei Windows-Instanzen müssen Sie das Volume möglicherweise online schalten, um es verwenden zu können. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung. Es ist nicht erforderlich, das Volume neu zu formatieren.

Initialisieren des Elastic-Volumes-Supports (falls erforderlich)

Bevor Sie ein Volume ändern können, das vor dem 3. November 2016 23:40 UTC mit einer Instance verbunden wurde, müssen Sie die Unterstützung der Volume-Änderung durch eine der folgenden Maßnahmen initialisieren:

- Volume trennen und wieder anfügen
- Starten und Stoppen der Instance

Console

Um festzustellen, ob Ihre Instances bereit sind

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie das Show/Hide Spaltensymbol (das Zahnrad). Wählen Sie die Attributspalte Startzeit und dann Bestätigen aus.
4. Sortieren Sie die Liste der Instances nach der Spalte Launch Time. Wählen Sie für jede Instance, die vor dem Stichtag gestartet wurde, die Registerkarte Speicher und überprüfen Sie in der Spalte Anhangszeit, wann die Volumes angehängt wurden.

AWS CLI

Um festzustellen, ob Ihre Instances bereit sind

Mit dem folgenden describe-instances-Befehl können Sie bestimmen, ob das Volume vor dem 3. November 2016 23:40 UTC angefügt wurde.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" \
    --output text
```

Die erste Zeile der Ausgabe für jede Instance zeigt deren ID und ob sie vor dem Stichdatum gestartet wurde (True oder False). In einer oder mehreren weiteren Zeilen wird angezeigt, ob jedes EBS-Volume vor dem Stichdatum angefügt wurde (True oder False). In der folgenden Beispielausgabe müssen Sie die Volume-Änderung für die erste Instance initialisieren, da sie vor dem Stichdatum gestartet und ihr Root-Volume ebenfalls davor angefügt wurde. Die anderen Instances sind bereit, da Sie nach dem Stichdatum gestartet wurden.

```
i-e905622e              True
True
i-719f99a8              False
True
i-006b02c1b78381e57     False
False
False
i-e3d172ed              False
True
```

PowerShell

Um festzustellen, ob eine Instance bereit ist

Verwenden Sie das Get-EC2Instance Cmdlet, um zu ermitteln, ob ein Volume vor dem 3. November 2016, 23:40 UTC, angehängt wurde.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
     Format-Table @{Name="VolumeId";Expression={$_.Ebs.VolumeId}}, `
                  @{Name="AttachTime";Expression={$_.Ebs.AttachTime}}
```

Es folgt eine Beispielausgabe.

```
VolumeId              AttachTime
--------              ----------
vol-0b243c8d927752d2b 3/23/2020 12:21:14 AM
```

```
vol-043eadbeb4a8387c3 9/5/2020 7:39:22 PM
vol-0c3f0c4e55c082753 4/23/2019 4:07:40 PM
```

Überwachen Sie den Fortschritt der Änderungen am Amazon EBS-Volume

Wenn Sie ein EBS-Volume ändern, durchläuft es eine Reihe von Zuständen. Das Volume tritt in den Zustand `modifying`, `optimizing` und schließlich in den Zustand `completed` ein. An diesem Punkt ist das Volume bereit für weitere Änderungen.

Während sich das Volume im Status `optimizing` befindet, liegt die Leistung Ihres Volumes zwischen den Spezifikationen der Quell- und Zielkonfiguration. Die vorübergehende Leistung des Volumes ist nicht geringer als die des Quell-Volumes. Wenn Sie ein IOPS-Downgrade durchführen, ist die vorübergehende Leistung des Volumes nicht geringer als die des Ziel-Volumes.

Die Volume-Änderungen werden wie folgt wirksam:

- Größenerhöhungen werden wirksam, sobald die Volumenänderung den `optimizing` Status erreicht hat, was normalerweise einige Sekunden dauert.
- Je nach angeforderter Volume-Konfiguration kann es zwischen einigen Minuten und einigen Stunden dauern, bis Leistungsänderungen (IOPS und Durchsatz) abgeschlossen sind. In der Regel kann die Migration eines voll genutzten 1-TB-Volumes auf eine neue Leistungskonfiguration etwa 6 Stunden dauern. In einigen Fällen kann es mehr als 24 Stunden dauern, bis eine neue Leistungskonfiguration wirksam wird, z. B. wenn das Volume nicht vollständig initialisiert wurde.

Die möglichen Volume-Status sind: `creating`, `available`, `in-use`, `deleting`, `deleted` und `error`.

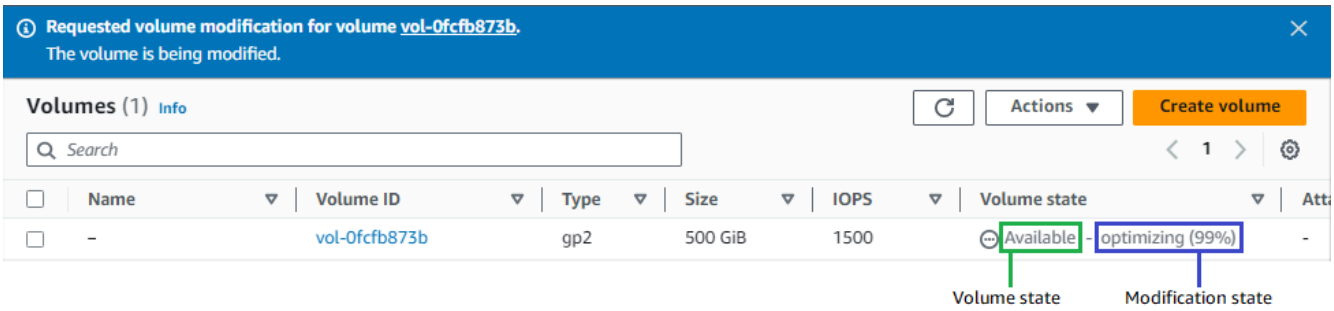
Die möglichen Änderungsstatus sind `modifying`, `optimizing` und `completed`.

Console

Um den Fortschritt einer Änderung zu überwachen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus.
4. Die Spalte „Volumenstatus“ und das Feld „Volumenstatus“ auf der Registerkarte „Details“ enthalten Informationen im folgenden Format: *`Volume state`* - *`Modification state`*

(*Modification progress*%). Das folgende Image zeigt den Status des Volumes und der Volume-Änderung.



Nach Abschluss der Änderung wird nur der Volume-Status angezeigt. Der Änderungsstatus und der Fortschritt werden nicht mehr angezeigt.

Alternativ können Sie Amazon verwenden, EventBridge um eine Benachrichtigungsregel für Ereignisse zu erstellen, die sich an der Lautstärke ändern. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge.

AWS CLI

Um den Fortschritt einer Änderung zu überwachen

Verwenden Sie den Befehl describe-volumes-modifications, um den Fortschritt einer oder mehrerer Volume-Änderungen anzuzeigen. Im folgenden Beispiel werden die Volume-Änderungen für zwei Volumes beschrieben.

```
aws ec2 describe-volumes-modifications \
    --volume-ids vol-1111111111111111 vol-2222222222222222
```

In der folgenden Beispielausgabe befinden sich die Volume-Änderungen immer noch im Status `modifying`. Fortschritt wird als Prozentsatz gemeldet.

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
            "ModificationState": "modifying",
            "VolumeId": "vol-1111111111111111",
            "TargetIops": 10000,
```

```
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-2222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

Im nächsten Beispiel werden alle Volumes mit einem Änderungsstatus von `optimizing` oder `completed` beschrieben und die Ergebnisse so gefiltert und formatiert, dass nur Änderungen angezeigt werden, die am oder nach dem 1. Februar 2017 veranlasst wurden:

```
aws ec2 describe-volumes-modifications \
    --filters Name=modification-state,Values="optimizing","completed" \
    --query "VolumesModifications[?StartTime>='2017-02-01'].
{ID:VolumeId,STATE:ModificationState}"
```

Es folgt eine Beispielausgabe mit Informationen über zwei Volumes:

```
[
    {
        "STATE": "optimizing",
        "ID": "vol-06397e7a0eEXAMPLE"
    },
    {
        "STATE": "completed",
        "ID": "vol-ba74e18c2aEXAMPLE"
    }
]
```

PowerShell

Um den Fortschritt einer Änderung zu überwachen

Verwenden Sie das cmdlet Get-EC2VolumeModification. Im folgenden Beispiel werden die Volume-Änderungen für zwei Volumes beschrieben.

```
Get-EC2VolumeModification `
    -VolumeId vol-1111111111111111 vol-2222222222222222
```

> **Note**
>
> In seltenen Fällen kann ein vorübergehender AWS Fehler zu einem `failed` Zustand führen. Dies ist kein Hinweis auf den Zustand des Volumes. Er weist lediglich darauf hin, dass bei der Änderung des Volumes ein Fehler aufgetreten ist. Wenn dieser Fall eintritt, sollten Sie erneut versuchen, die Volume-Änderung vorzunehmen.

Erweitern Sie das Dateisystem, nachdem Sie die Größe eines Amazon EBS-Volumes geändert haben

Nachdem Sie die Größe eines EBS-Volumes erhöht haben, müssen Sie die Partition und das Dateisystem auf die neue, größere Größe erweitern. Sie können dies tun, sobald der Datenträger in den `optimizing`-Status übergeht.

Bevor Sie beginnen

- Erstellen Sie einen Snapshot des Volumes, falls Sie Ihre Änderungen rückgängig machen müssen. Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots.
- Vergewissern Sie sich, dass die Volume-Änderung erfolgreich war und dass es sich im Status `optimizing` oder `completed` befindet. Weitere Informationen finden Sie unter Überwachen Sie den Fortschritt der Änderungen am Amazon EBS-Volume.
- Stellen Sie sicher, dass das Volume an die Instance angehängt ist und dass es formatiert und gemountet ist. Weitere Informationen finden Sie unter Formatieren und Mounten eines verknüpften Volumes.
- (Nur Linux-Instances) Wenn Sie logische Volumes auf dem Amazon EBS-Volume verwenden, müssen Sie Logical Volume Manager (LVM) verwenden, um das logische Volume zu erweitern.

Anweisungen dazu finden Sie im Abschnitt LV erweitern im Artikel Wie verwende ich LVM, um ein logisches Volume auf der Partition eines EBS-Volumes zu erstellen? .

Linux-Instances

> **Note**
>
> Die folgenden Anweisungen führen Sie durch den Prozess der Erweiterung der XFS - und Ext4-Dateisysteme für Linux. Informationen zur Erweiterung eines anderen Dateisystems finden Sie in der zugehörigen Dokumentation.

Bevor Sie ein Dateisystem unter Linux erweitern können, müssen Sie die Partition erweitern, falls Ihr Volume eine solche hat.

Erweitern des Dateisystems von EBS-Volumes

Verwenden Sie das folgende Verfahren, um das Dateisystem für ein größenverändertes Volume zu erweitern.

Beachten Sie, dass die Geräte- und Partitionsnamen für Xen-Instanzen und Instanzen, die auf dem Nitro-System erstellt wurden, unterschiedlich sind. Um festzustellen, ob es sich bei Ihrer Instance um einen Xen-based oder handelt Nitro-based, lesen Sie den Amazon EC2-Hypervisor-Typ.

So erweitern Sie das Dateisystem von EBS-Volumes

1. Verbinden Sie sich mit der Instance.
2. Passen Sie bei Bedarf die Größe der Partition an. Gehen Sie hierzu wie folgt vor:
   a. Prüfen Sie, ob das Volume über eine Partition verfügt. Verwenden Sie den Befehl lsblk.

      Nitro instance example

      In der folgenden Beispielausgabe hat das Root-Volume (`nvme0n1`) zwei Partitionen (`nvme0n1p1` und `nvme0n1p128`), während das zusätzliche Volume (`nvme1n1`) keine Partitionen hat.

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
```

```
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

In der folgenden Beispielausgabe hat das Stamm-Volume (`xvda`) eine Partition (`xvda1`), während das zusätzliche Volume (`xvdf`) keine Partition hat.

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

- Wenn das Volume eine Partition hat, fahren Sie mit dem nächsten Schritt (2b) fort.
- Wenn das Volume keine Partitionen hat, überspringen Sie die Schritte 2b, 2c und 2d und fahren Sie mit Schritt 3 fort.

> **Tipp zur Problembehebung**
>
> Wenn Sie das Volume in der Befehlsausgabe nicht sehen, stellen Sie sicher, dass das Volume an die Instance ??? angehängt ist und dass es formatiert und gemountet ist.

b. Prüfen Sie, ob die Partition erweitert werden muss. In der lsblk-Befehlsausgabe aus dem vorherigen Schritt, vergleichen Sie die Partitionsgröße und die Volume-Größe.

- Wenn die Partitionsgröße kleiner als die Volume-Größe ist, fahren Sie mit dem nächsten Schritt (2c) fort.
- Wenn die Partitionsgröße der Volume-Größe entspricht, muss die Partition nicht erweitert werden. Überspringen Sie die Schritte 2c und 2d und fahren Sie mit Schritt 3 fort.

> **Tipp zur Problembehebung**
>
> Wenn das Volume immer noch die ursprüngliche Größe aufweist, bestätigen Sie, dass die Volume-Änderung erfolgreich war.

c. Erweitern Sie die Partition. Verwenden Sie den growpart Befehl und geben Sie den Gerätenamen und die Partitionsnummer an.

Nitro instance example

Die Partitionsnummer ist die Zahl nach demp. Zum Beispiel lautet `nvme0n1p1` die Partitionsnummer`1`. Denn `nvme0n1p128` die Partitionsnummer lautet`128`.

Verwenden Sie den folgenden Befehl`nvme0n1p1`, um eine Partition mit dem Namen zu erweitern.

> **Important**
>
> Beachten Sie das Leerzeichen zwischen dem Gerätenamen (`nvme0n1`) und der Partitionsnummer (1).

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Xen instance example

Die Partitionsnummer ist die Zahl nach dem Gerätenamen. Zum Beispiel lautet `xvda1` die Partitionsnummer`1`. Denn `xvda128` die Partitionsnummer lautet`128`.

Verwenden Sie den folgenden Befehl`xvda1`, um eine Partition mit dem Namen zu erweitern.

> **Important**
>
> Beachten Sie das Leerzeichen zwischen dem Gerätenamen (`xvda`) und der Partitionsnummer (1).

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

Tipps zur Problembehebung

- `mkdir: cannot create directory ‘/tmp/growpart.31171’: No space left on device FAILED: failed to make temp dir`: Zeigt an, dass auf dem Volume nicht genügend freier Speicherplatz vorhanden ist, damit Growpart das temporäre Verzeichnis erstellen kann, das für die Größenänderung benötigt wird. Geben Sie etwas Speicherplatz frei und versuchen Sie es dann erneut.
- `must supply partition-number`: Zeigt an, dass Sie eine falsche Partition angegeben haben. Verwenden Sie den lsblk Befehl, um den Partitionsnamen zu bestätigen, und stellen Sie sicher, dass Sie ein Leerzeichen zwischen dem Gerätenamen und der Partitionsnummer eingeben.
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown`: Zeigt an, dass die Partition bereits das gesamte Volume erweitert und nicht erweitert werden kann. Bestätigen Sie, dass die Volume-Änderung erfolgreich war.

d. Stellen Sie sicher, dass die Partition erweitert wurde. Verwenden Sie den Befehl lsblk. Die Partitionsgröße sollte jetzt der Volume-Größe entsprechen.

Nitro instance example

Die folgende Beispielausgabe zeigt, dass sowohl die Volumes (`nvme0n1`) als auch die Partition (`nvme0n1p1`) die gleiche Größe (`16 GB`) haben.

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0  16G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

Die folgende Beispielausgabe zeigt, dass sowohl die Volumes (`xvda`) als auch die Partition (`xvda1`) die gleiche Größe (`16 GB`) haben.

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. Erweitern Sie das Dateisystem.

   a. Ermitteln Sie den Namen, die Größe, den Typ und den Mount-Punkt für das Dateisystem, das Sie erweitern müssen. Verwenden Sie den lsblk -f Befehl df -hT oder.

   Nitro instance example

   Die folgende Beispielausgabe für den df -hT Befehl zeigt, dass das `/dev/nvme0n1p1` Dateisystem 8 GB groß ist, dass sein Typ und sein Bereitstellungspunkt lauten`/`. `xfs`

   ```
   [ec2-user ~]$ df -hT
   Filesystem      Type  Size  Used Avail Use% Mounted on
   /dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
   /dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
   ...
   ```

   Xen instance example

   Die folgende Beispielausgabe für den df -hT Befehl zeigt, dass das `/dev/xvda1` Dateisystem 8 GB groß ist, dass es `ext4` den Typ und den Bereitstellungspunkt hat`/`.

   ```
   [ec2-user ~]$ df -hT
   Filesystem      Type   Size    Used   Avail   Use%   Mounted on
   /dev/xvda1      ext4   8.0G    1.9G   6.2G    24%    /
   /dev/xvdf1      xfs    24.0G   45M    8.0G    1%     /data
   ...
   ```

   - Wenn die Dateisystemgröße kleiner als die Volumegröße ist, fahren Sie mit dem nächsten Schritt (3b) fort.

- Wenn die Dateisystemgröße der Volumegröße entspricht, muss sie nicht erweitert werden. Überspringen Sie in diesem Fall die verbleibenden Schritte - die Partition und das Dateisystem wurden auf die neue Volumegröße erweitert.

b. Die Befehle zum Erweitern des Dateisystems unterscheiden sich je nach Dateisystemtyp. Wählen Sie den folgenden richtigen Befehl basierend auf dem Dateisystemtyp, den Sie sich im vorherigen Schritt notiert haben.

- [XFS-Dateisystem] Verwenden Sie den xfs_growfs-Befehl und geben Sie den Mount-Punkt des Dateisystems an, den Sie im vorherigen Schritt notiert haben.

  Nitro and Xen instance example

  Um beispielsweise ein auf `/` gemountetes Dateisystem zu erweitern, verwenden Sie den folgenden Befehl.

  ```
  [ec2-user ~]$ sudo xfs_growfs -d /
  ```

  Tipps zur Problembehebung

  - `xfs_growfs: /data is not a mounted XFS filesystem`: Zeigt an, dass Sie den falschen Mount-Punkt angegeben haben oder dass das Dateisystem nicht XFS ist. Verwenden Sie den df -hT-Befehl, um den Mount-Punkt und den Dateisystemtyp zu überprüfen.
  - `data size unchanged, skipping`: Zeigt an, dass das Dateisystem bereits das gesamte Volume erweitert. Wenn das Volume keine Partitionen hat, bestätigen Sie, dass die Volume-Änderung erfolgreich war. Wenn das Volume Partitionen enthält, stellen Sie sicher, dass die Partition wie in Schritt 2 beschrieben erweitert wurde.

- [Ext4-Dateisystem] Verwenden Sie den resize2fs-Befehl und geben Sie den Namen des Dateisystems ein, das Sie sich im vorherigen Schritt notiert haben.

  Nitro instance example

  Um beispielsweise ein gemountetes Dateisystem mit dem Namen `/dev/nvme0n1p1` zu erweitern, verwenden Sie den folgenden Befehl.

```
[ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
```

Xen instance example

Um beispielsweise ein gemountetes Dateisystem mit dem Namen `/dev/xvda1` zu erweitern, verwenden Sie den folgenden Befehl.

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
```

Tipps zur Problembehebung

- `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1`: Zeigt an, dass das Dateisystem nicht Ext4 ist. Verwenden Sie den df -hT-Befehl, um den Systemtyp der Datei zu überprüfen.
- `open: No such file or directory while opening /dev/xvdb1`: Zeigt an, dass Sie eine falsche Partition angegeben haben. Verwenden Sie den df -hT-Befehl, um die Partition zu überprüfen.
- `The filesystem is already 3932160 blocks long. Nothing to do!`: Zeigt an, dass das Dateisystem bereits das gesamte Volume erweitert. Wenn das Volume keine Partitionen hat, bestätigen Sie, dass die Volume-Änderung erfolgreich war. Wenn das Volume Partitionen enthält, stellen Sie sicher, dass die Partition wie in Schritt 2 beschrieben erweitert wurde.

- [Anderes Dateisystem] Weitere Anweisungen finden Sie in der Dokumentation zu Ihrem Dateisystems.

c. Stellen Sie sicher, dass das Dateisystem erweitert wurde. Verwenden Sie den df -hT-Befehl und bestätigen Sie, dass die Größe des Dateisystems der Volume-Größe entspricht.

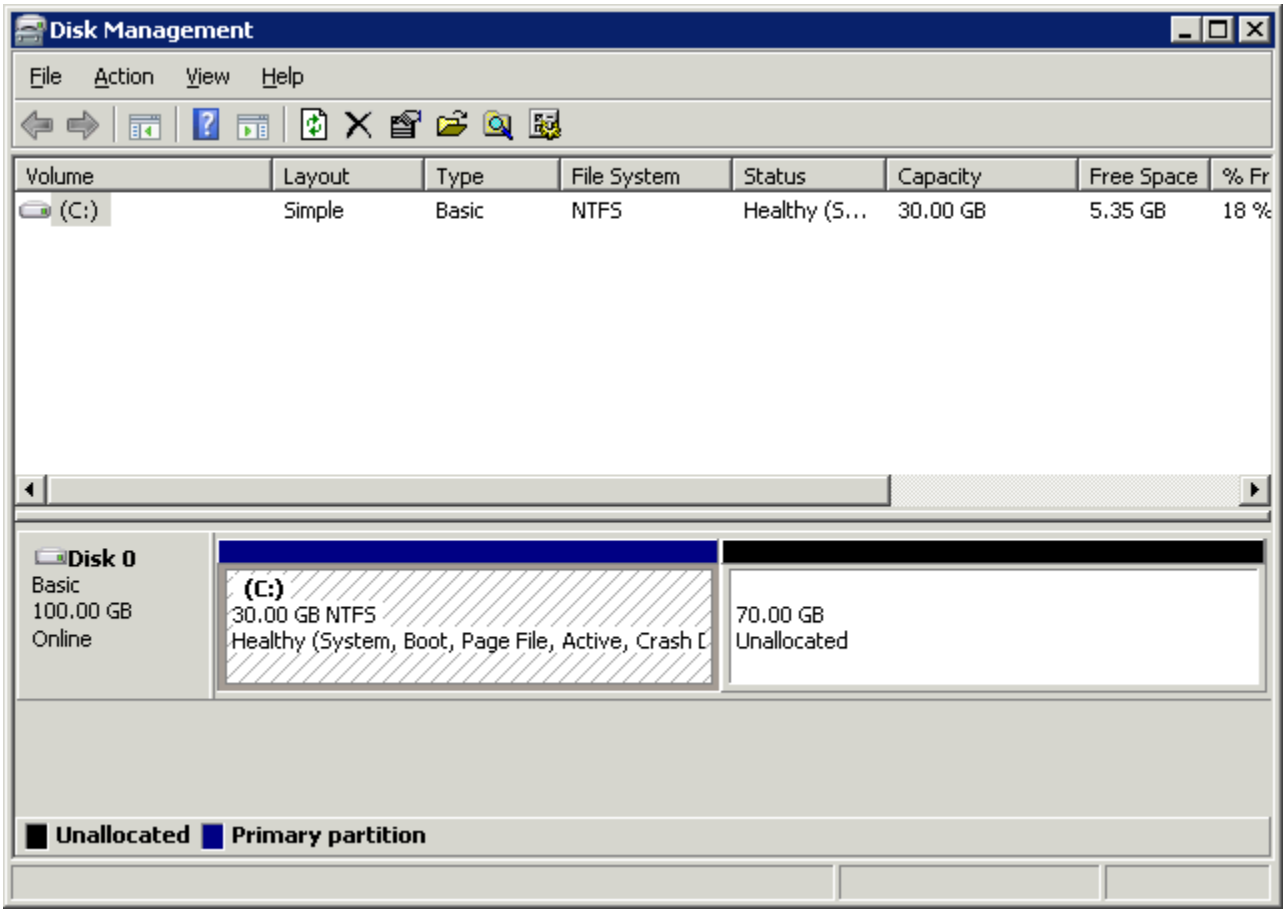
Windows-Instances

Verwenden Sie eine der folgenden Methoden, um das Dateisystem auf einer Windows-Instanz zu erweitern.

Disk Management utility

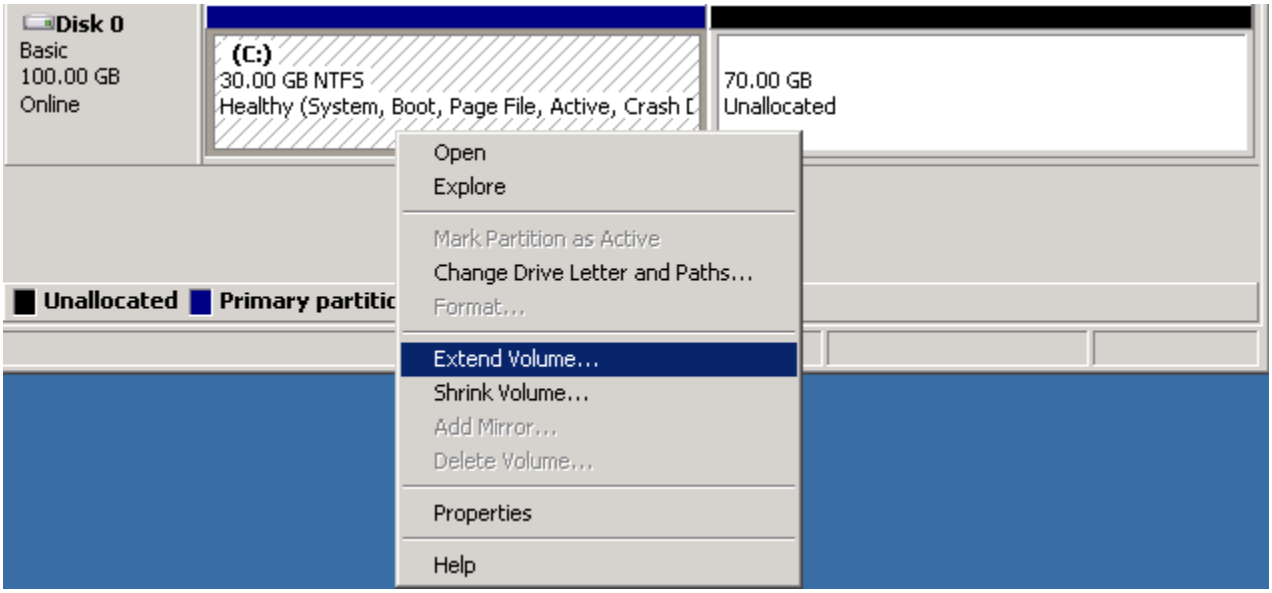
So erweitern Sie ein Dateisystem mithilfe der Datenträgerverwaltung

1. Bevor Sie ein Dateisystem mit wichtigen Daten ändern, ist eine bewährte Methode das Anlegen eines Snapshots des entsprechenden Volumes, falls Sie Ihre Änderungen rückgängig machen möchten. Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots.
2. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an.
3. Geben Sie im Dialogfeld Ausführen diskmgmt.msc ein und drücken Sie die Eingabetaste. Das Dienstprogramm „Datenträgerverwaltung“ wird geöffnet.

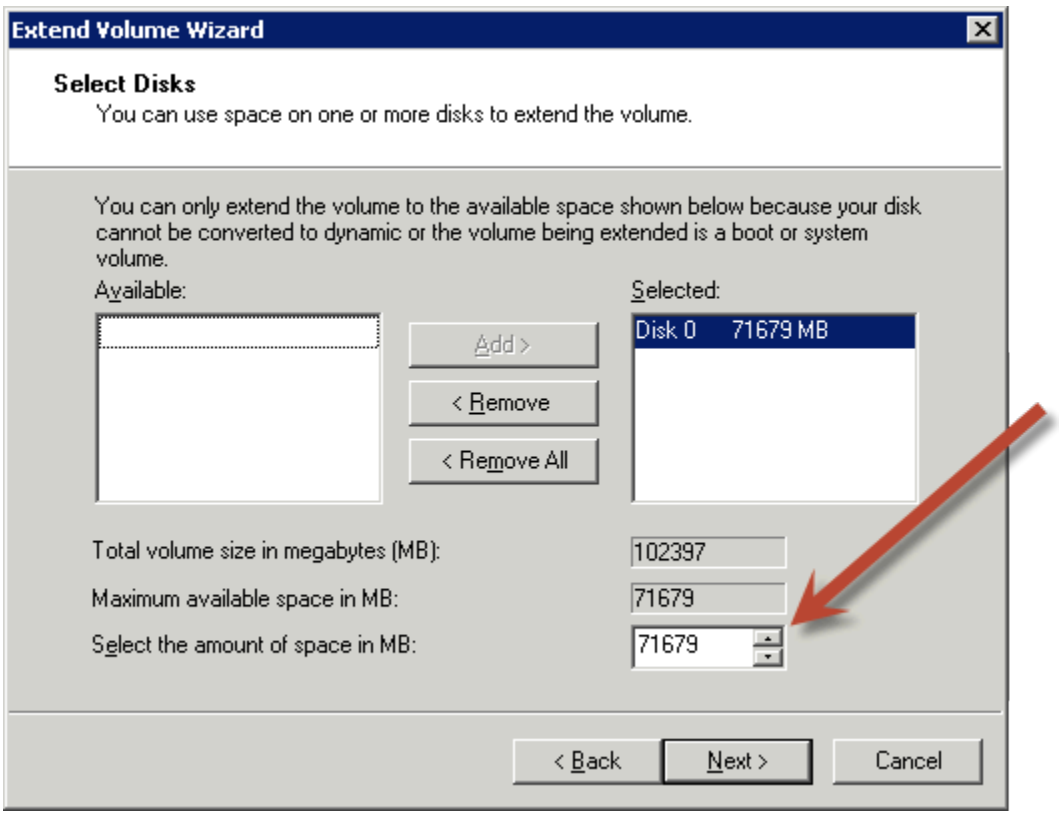


4. Wählen Sie im Menü Datenträgerverwaltung die Option Aktion und anschließend Datenträger neu einlesen aus.
5. Öffnen Sie das Kontextmenü (rechte Maustaste) für den erweiterten Datenträger und wählen Sie dann Volume erweitern aus.

> **Note**
>
> Extend Volume (Volume erweitern) ist möglicherweise deaktiviert (ausgegraut), wenn:
>
> - Der nicht zugewiesene Speicherplatz befindet sich nicht neben dem Laufwerk. Der nicht zugewiesene Speicherplatz muss sich neben der rechten Seite des Laufwerks befinden, das Sie erweitern möchten.
> - Das Volume verwendet den Master Boot Record (MBR)-Partitionsstil und ist bereits 2 TB groß. Volumes, die MBR verwenden, dürfen nicht mehr als 2 TB groß sein.



6. Wählen Sie im Assistenten Volume erweitern die Option Weiter. Geben Sie unter Speicherplatz in MB: die Anzahl der Megabytes ein, um die Sie das Volume erweitern möchten. Im Allgemeinen geben Sie den maximal verfügbaren Speicherplatz an. Der hervorgehobene Text unter Ausgewählt gibt die Menge des hinzugefügten Speicherplatzes und nicht die abschließende Größe des Volumes an. Schließen Sie den Assistenten ab.



7. Wenn Sie die Größe eines NVMe-Volumes auf einer Instance erhöhen, die nicht über den AWS -NVMe-Treiber verfügt, müssen Sie die Instance neu starten, damit Windows die neue Volume-Größe sehen kann. Weitere Informationen zur Installation des AWS NVMe-Treibers finden Sie unter AWS NVMe-Treiber.

PowerShell

Verwenden Sie das folgende Verfahren, um ein Windows-Dateisystem mithilfe von zu erweitern. PowerShell

Um ein Dateisystem zu erweitern mit PowerShell

1. Bevor Sie ein Dateisystem mit wichtigen Daten ändern, ist eine bewährte Methode das Anlegen eines Snapshots des entsprechenden Volumes, falls Sie Ihre Änderungen rückgängig machen möchten. Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots.
2. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an.
3. PowerShell Als Administrator ausführen.

4. Führen Sie den `Get-Partition` Befehl aus. PowerShell gibt die entsprechende Partitionsnummer für jede Partition, den Laufwerksbuchstaben, den Offset, die Größe und den Typ zurück. Beachten Sie den Laufwerksbuchstaben der zu erweiternden Partition.
5. Führen Sie den folgenden Befehl aus, um den Datenträger erneut zu scannen:

   ```
   "rescan" | diskpart
   ```

6. Führen Sie den folgenden Befehl aus und verwenden Sie anstelle von den Laufwerksbuchstaben, den Sie in Schritt 4 notiert haben**<drive-letter>**. PowerShell gibt die Mindest- und Höchstgröße der zulässigen Partition in Byte zurück.

   ```
   Get-PartitionSupportedSize -DriveLetter <drive-letter>
   ```

7. Wenn Sie die Partition auf eine bestimmte Größe erweitern möchten, führen Sie den folgenden Befehl aus und geben Sie anstelle von **<size>** die neue Größe des Volumes ein. Sie können die Größe in `KB`, `MB` und `GB`, z. B. `50GB`, eingeben.

   ```
   Resize-Partition -DriveLetter <drive-letter> -Size <size>
   ```

   Führen Sie den folgenden Befehl aus, um die Partition auf die maximal verfügbare Größe zu erweitern.

   ```
   Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize
    -DriveLetter <drive-letter>).SizeMax
   ```

   Die folgenden PowerShell Befehle zeigen den vollständigen Befehls- und Antwortablauf für die Erweiterung eines Dateisystems auf eine bestimmte Größe.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     8 MB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-------      -------
8388608 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS
```

Die folgenden PowerShell Befehle zeigen den vollständigen Befehls- und Antwortablauf für die Erweiterung eines Dateisystems auf die maximal verfügbare Größe.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

 SizeMin      SizeMax
 -------      -------
59047936 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                    100 GB IFS
```

Trennen Sie ein Amazon EBS-Volume von einer Amazon EC2-Instance

Sie müssen ein Amazon-Elastic-Block-Store(Amazon EBS)-Volume von einer Instance trennen, bevor Sie es an eine andere Instance anhängen oder löschen können. Das Trennen eines Volumes wirkt sich nicht auf die Daten auf dem Volume aus.

Themen

- Überlegungen
- Unmounten und Trennen eines Volumes

- Fehlerbehebung

Überlegungen

- Sie können ein Amazon EBS-Volume explizit oder durch Beenden der Instance von einer Instance trennen. Wenn die Instance jedoch ausgeführt wird, müssen Sie zuerst das Mounting des Volumes in der Instance aufheben.
- Wenn ein EBS-Volume das Root-Gerät einer Instance ist, müssen Sie die Instance anhalten, bevor das Volume getrennt werden kann.
- Sie können ein getrenntes Volume (dessen Mounting nicht aufgehoben wurde) erneut anfügen, es erhält jedoch möglicherweise nicht denselben Mounting-Punkt. Wenn es Schreibzugriffe auf das sich in Bearbeitung befindliche Volume gab, als es abgetrennt wurde, sind die Daten auf dem Volume möglicherweise nicht synchronisiert.
- Nachdem Sie ein Volume getrennt haben, wird Ihnen weiterhin der Volume-Speicher in Rechnung gestellt, solange die Speichermenge das Limit des AWS kostenlosen Kontingents überschreitet. Sie müssen ein Volume löschen, damit keine weiteren Gebühren anfallen. Weitere Informationen finden Sie unter Löschen eines Amazon EBS-Volumes.

Unmounten und Trennen eines Volumes

Gehen Sie wie folgt vor, um ein Volume von einer Instance zu trennen und das Mounten aufzuheben: Dies kann nützlich sein, wenn Sie das Volume an eine andere Instance anhängen müssen oder wenn Sie das Volume löschen müssen.

Schritte

- Schritt 1: Aufheben der Bereitstellung des Volumes
- Schritt 2: Trennen des Volumes von der Instance
- Schritt 3: (Nur Windows-Instanzen) Deinstallieren Sie die Standorte der Offline-Geräte

Schritt 1: Aufheben der Bereitstellung des Volumes

Linux-Instances

Verwenden Sie in Ihrer Linux-Instance den folgenden Befehl, um das Mounting des Geräts `/dev/sdh` aufzuheben.

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

Windows-Instances

Heben Sie auf Ihrer Windows-Instance das Mounten des Volumes wie folgt auf.

1. Starten Sie das Dienstprogramm für die Datenträgerverwaltung.
   - (Windows Server 2012 und höher) Klicken Sie auf der Taskleiste auf das Windows-Logo (klicken Sie mit der rechten Maustaste) und wählen Sie Datenträgerverwaltung.
   - (Windows Server 2008) Wählen Sie die Optionen Start, Administrative Tools (Verwaltungstools), Computer Management (Computer-Verwaltung) und Disk Management (Datenträgerverwaltung) aus.
2. Wählen Sie das Laufwerk aus (klicken Sie z. B. mit der rechten Maustaste auf Laufwerk 1) und wählen Sie dann Offline. Warten Sie, bis der Datenträgerstatus in Offline geändert wurde, bevor Sie die Amazon EC2-Konsole öffnen.

Schritt 2: Trennen des Volumes von der Instance

Verwenden Sie eine der folgenden Methoden, um das Volume von der Instance zu trennen:

Console

So trennen Sie ein EBS-Volume

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus.
4. Wählen Sie „Aktionen“, „Volume trennen“.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Trennen.

AWS CLI

Um ein EBS-Volume von einer Instance zu trennen

Verwenden Sie nach dem Aushängen des Volumes den Befehl detach-volume.

```
aws ec2 detach-volume --volume-id vol-01234567890abcdef
```

PowerShell

Um ein EBS-Volume von einer Instance zu trennen

Verwenden Sie das Cmdlet, nachdem Sie die Bereitstellung des Volumes aufgehoben haben. Dismount-EC2Volume

```
Dismount-EC2Volume -VolumeId vol-01234567890abcdef
```

Schritt 3: (Nur Windows-Instanzen) Deinstallieren Sie die Standorte der Offline-Geräte

Wenn Sie das Mounten eines Volumes von einer Instance aufheben und von dieser trennen, kennzeichnet Windows den Gerätestandort als offline. Der Gerätestandort bleibt nach dem Neustart, Stoppen und Neustarten der Instance offline. Wenn Sie die Instance neu starten, kann Windows eines der verbleibenden Volumes auf den Offline-Geräte-Standort mounten. Dies führt dazu, dass das Volume in Windows nicht verfügbar ist. Gehen Sie wie folgt vor, um dies zu verhindern und sicherzustellen, dass alle Volumes beim nächsten Start von Windows an die Standorte der Online-Geräte angeschlossen sind:

1. Öffnen Sie auf der Instance den Geräte-Manager.
2. Wählen Sie im Geräte-Manager Ansicht, Versteckte Geräte anzeigen aus.
3. Erweitern Sie in der Geräteliste den Knoten Speichercontroller .

   Die Gerätestandorte, an denen die abgetrennten Volumes gemountet wurden, heißen `AWS NVMe Elastic Block Storage Adapter` und sollten ausgegraut erscheinen.
4. Wählen Sie (mit der rechten Maustaste) jeden ausgegrauten Gerätestandort mit einem Namen aus`AWS NVMe Elastic Block Storage Adapter`, wählen Sie Gerät deinstallieren und dann Deinstallieren aus.

   > **Important**
   >
   > Aktivieren Sie nicht das Kontrollkästchen Treibersoftware für dieses Gerät löschen.

Fehlerbehebung

Nachfolgend finden Sie Probleme, die beim Trennen von Volumes häufig auftreten, sowie Informationen zu deren Behebung.

> **Note**
>
> Erstellen Sie einen Snapshot Ihres Volumes, bevor Sie sein Mounting aufheben, um Datenverlusten vorzubeugen. Die erzwungene Trennung eines hängengebliebenen Volumes kann das Dateisystem oder die darin enthaltenen Daten beschädigen oder dazu führen, dass ein neues Volume mit demselben Gerätenamen erst angefügt werden kann, wenn Sie die Instance neu starten.

- Wenn beim Trennen eines Volumes über die Amazon EC2-Konsole Probleme auftreten, kann der CLI-Befehl describe-volumes hilfreich beim Diagnostizieren des Problems sein. Weitere Informationen finden Sie unter describe-volumes.
- Wenn Ihr Volume den Status `detaching` beibehält, können Sie die Trennung erzwingen, indem Sie Force Detach (Trennung erzwingen) wählen. Verwenden Sie diese Option nur als letztes Mittel, um ein Volume von einer ausgefallenen Instance zu trennen oder wenn Sie ein Volume trennen, das Sie anschließend löschen möchten. Die Instance erhält keine Gelegenheit, die Caches oder Metadaten des Dateisystems zu löschen. Wenn Sie diese Option verwenden, müssen Sie eine Überprüfung und Reparatur des Dateisystems durchführen.
- Wenn Sie innerhalb weniger Minuten mehrfach versucht haben, die Trennung des Volumes zu erzwingen, sie jedoch weiterhin den Status `detaching`aufweist, können Sie eine Anfrage im AWS re:Post stellen. Um schneller eine Lösung zu erhalten, geben Sie die Volume-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben.
- Wenn Sie versuchen, ein noch gemountetes Volume zu trennen, kann das Volume während des Trennungsversuchs im Status `busy` hängenbleiben. Die folgende Ausgabe des Befehls describe-volumes zeigt ein Beispiel dieses Zustands:

```
"Volumes": [
    {
        "AvailabilityZone": "us-west-2b",
        "Attachments": [
            {
                "AttachTime": "2022-07-21T23:44:52.000Z",
                "InstanceId": "i-1234567890abcdef0",
                "VolumeId": "vol-01234567890abcdef",
                "State": "busy",
                "DeleteOnTermination": false,
                "Device": "/dev/sdf"
            }
```

```
        ...
    }
]
```

Wenn dieser Status auftritt, kann sich das Trennen auf unbestimmte Zeit verzögern, bis Sie das Mounting des Volumes aufheben, die Trennung erzwingen, die Instance neu starten oder alle drei dieser Schritte durchführen.

Löschen eines Amazon EBS-Volumes

Wenn Sie ein Amazon EBS-Volume nicht mehr benötigen, können Sie es löschen. Nach dem Löschen sind die Daten weg und das Volume kann nicht an eine Instance angefügt werden. Sie können vor dem Löschen einen Snapshot des Volumes speichern, mit dem Sie das Volume später wiederherstellen können.

Sie können ein Volume nicht löschen, wenn es an eine Instance angefügt ist. Um ein Volume zu löschen, müssen Sie es zuerst trennen. Weitere Informationen finden Sie unter Trennen Sie ein Amazon EBS-Volume von einer Amazon EC2-Instance.

Wenn Sie ein Volume löschen, das einer Aufbewahrungsregel für den Papierkorb entspricht, wird das Volume im Papierkorb aufbewahrt und nicht sofort gelöscht. Weitere Informationen finden Sie unter Papierkorb.

Console

Um ein EBS-Volume zu löschen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus. Stellen Sie sicher, dass sich das Volume im Status Verfügbar befindet.
4. Wählen Sie „Aktionen“, „Volume löschen“.

   Wenn diese Option deaktiviert ist, ist das Volume an eine Instanz angehängt und kann nicht gelöscht werden.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Delete (Löschen) aus.

AWS CLI

Um zu überprüfen, ob ein EBS-Volume verwendet wird

Verwenden Sie den Befehl describe-volumes. Wenn das Volume verwendet wird, lautet `in-use` der Status. Andernfalls ist es `available`.

```
aws ec2 describe-volumes \
    --volume-id vol-01234567890abcdef \
    --query Volumes[*].State \
    --output text
```

Um ein EBS-Volume zu löschen

Verwenden Sie den Befehl delete-volume.

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

PowerShell

Um zu überprüfen, ob ein EBS-Volume verwendet wird

Verwenden Sie das cmdlet Get-EC2Volume. Wenn das Volume verwendet wird, lautet `in-use` der Status. Andernfalls ist es `available`.

```
(Get-EC2Volume `
    -VolumeId vol-01234567890abcdef).State.Value
```

Um ein EBS-Volume zu löschen

Verwenden Sie das cmdlet Remove-EC2Volume.

```
Remove-EC2Volume -VolumeId vol-01234567890abcdef
```

Ersetzen Sie ein Amazon EBS-Volume mithilfe eines Snapshots

Amazon EBS-Snapshots werden wegen ihrer Geschwindigkeit, Bequemlichkeit und geringen Kosten auf Amazon EC2 als Backup-Tool bevorzugt. Wenn Sie ein Volume aus einem Snapshot erstellen,

stellen Sie seinen Status zu einem bestimmten Zeitpunkt wieder her, wobei die bis zu diesem Zeitpunkt gespeicherten Daten intakt sind. Durch das Anfügen eines aus einem Snapshot erstellten Volumes an eine Instance können Sie Daten in mehreren Regionen duplizieren, Testumgebungen erstellen, ein beschädigtes Produktionsvolume vollständig ersetzen oder bestimmte Dateien und Verzeichnisse abrufen und zu einem anderen angefügten Volume übertragen. Weitere Informationen finden Sie unter Amazon EBS-Snapshots.

Sie können eines der folgenden Verfahren nutzen, um ein Amazon-EBS-Volume durch ein anderes Volume ersetzen, das aus einem vorherigen Snapshot dieses Volumes erstellt wurde.

Anforderung

Sie müssen Ihr Volume in derselben Availability Zone wie die Instance erstellen. Volumes müssen an Instances in derselben Availability Zone angehängt werden.

Console

So ersetzen Sie ein Volume

1. Erstellen Sie ein Volume aus dem Snapshot und notieren Sie sich die ID des neuen Volumes. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.
2. Wählen Sie auf der Seite „Instances“ die Instance aus, für die das Volume ersetzt werden soll, und notieren Sie die Instance-ID.

   Lassen Sie die Instance ausgewählt und wählen Sie die Registerkarte Speicher. Suchen Sie im Abschnitt Blockgeräte das zu ersetzende Volume und notieren Sie den Gerätenamen für das Volume (z. B. `/dev/sda1`).
3. Wählen Sie auf der Registerkarte Speicher die Volume-ID aus, heben Sie dann die Bereitstellung auf und trennen Sie das Volume von der Instance.
4. Wählen Sie das neue Volume aus, das Sie in Schritt 1 erstellt haben, und wählen Sie Aktionen, Volume anfügen.

   Geben Sie für Instance und Gerätename die Instance-ID und den Gerätenamen ein, die Sie in Schritt 2 notiert haben, und wählen Sie dann Volume anfügen.
5. Stellen Sie eine Verbindung mit Ihrer Instance her und spielen Sie das Volume auf. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

AWS CLI

So ersetzen Sie ein Volume

1. Erstellen Sie ein neues Volume aus dem Snapshot. Verwenden Sie den Befehl create-volume mit der Option. `--snapshot-id` Geben Sie für `--availability-zone` dieselbe Availability Zone wie für die Instance an. Notieren Sie sich die ID des neuen Volumes in der Ausgabe.

```
aws ec2 create-volume \
    --volume-type gp3 \
    --snapshot-id snap-0abcdef1234567890 \
    --availability-zone us-east-1a
```

2. Ermittelt den Gerätenamen des zu ersetzenden Volumes. Verwenden Sie den Befehl describe-instances. Geben Sie für `--instance-ids` die ID der Instance an, für die das Volume ersetzt werden soll. Notieren Sie sich den Gerätenamen und die Volume-ID des zu ersetzenden Volumes.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BlockDeviceMappings
```

3. Trennen Sie das zu ersetzende Volume von der Instance. Verwenden Sie den Befehl detach-volume.

```
aws ec2 detach-volume --volume-id vol-xxxxxxxxxxxxxxxxx
```

4. Fügen Sie das Ersatz-Volume der Instance an. Verwenden Sie den Befehl attach-volume. Geben Sie für `--volume-id` die ID des Ersatz-Volumes an. Geben Sie für die ID der Instanz an`--instance-id`, an die das Volume angehängt werden soll. Geben Sie für `--device` denselben Gerätenamen an, den Sie zuvor notiert haben.

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --device /dev/sdf
```

5. Stellen Sie eine Verbindung mit Ihrer Instance her und spielen Sie das Volume auf. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

PowerShell

So ersetzen Sie ein Volume

1. Erstellen Sie ein neues Volume aus dem Snapshot. Verwenden Sie das New-EC2Volume Cmdlet mit der `-SnapshotId` Option. Geben Sie für `-AvailabilityZone` dieselbe Availability Zone wie für die Instance an. Notieren Sie sich die ID des neuen Volumes in der Ausgabe.

```
New-EC2Volume `
    -VolumeType gp3 `
    -SnapshotId snap-0abcdef1234567890 `
    -AvailabilityZone us-east-1a
```

2. Ermittelt den Gerätenamen des zu ersetzenden Volumes. Verwenden Sie das cmdlet Get-EC2Instance. Geben Sie für `-InstanceId` die ID der Instance an, für die das Volume ersetzt werden soll. Notieren Sie sich den Gerätenamen und die Volume-ID des zu ersetzenden Volumes.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
     Format-Table DeviceName, @{Name="VolumeId";Expression={$_.Ebs.VolumeId}}
```

3. Trennen Sie das zu ersetzende Volume von der Instance. Verwenden Sie das cmdlet Dismount-EC2Volume.

```
DismountEC2Volume -VolumeId vol-xxxxxxxxxxxxxxxxx
```

4. Fügen Sie das Ersatz-Volume der Instance an. Verwenden Sie das cmdlet Add-EC2Volume. Geben Sie für `-VolumeId` die ID des Ersatz-Volumes an. Geben Sie für die ID der Instanz an`-InstanceId`, an die das Volume angehängt werden soll. Geben Sie für `-Device` denselben Gerätenamen an, den Sie zuvor notiert haben.

```
Add-EC2Volume`
    -VolumeId vol-01234567890abcdef `
    -InstanceId i-1234567890abcdef0 `
```

```
    -Device /dev/sdf
```

5. Stellen Sie eine Verbindung mit Ihrer Instance her und spielen Sie das Volume auf. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

Statusüberprüfungen des Amazon EBS-Volumes

Volume-Statusprüfungen erlauben Ihnen, mögliche Inkonsistenzen in den Daten auf einem Amazon EBS-Volume besser zu verstehen, nachzuverfolgen und zu verwalten. Diese Prüfungen bieten Ihnen die Informationen, die Sie benötigen, um zu bestimmen, ob Ihre Amazon EBS-Volumes beeinträchtigt sind, und um Ihnen kontrollieren zu helfen, wie ein potenziell inkonsistentes Volume bearbeitet wird.

Volume-Statusprüfungen sind automatisierte Tests, die alle 5 Minuten ausgeführt werden und den Status „Bestanden“ oder „Nicht bestanden“ zurückgeben. Wenn alle Prüfungen bestanden wurden, ist der Status des Volumes ok. Wenn eine Prüfung nicht bestanden wird, ist der Status des Volumes `impaired`. Wenn der Status `insufficient-data` ist, sind die Prüfungen bei dem Volume möglicherweise noch in Bearbeitung. Sie können die Ergebnisse von Volume-Statusprüfungen anzeigen, um beeinträchtigte Volumes zu identifizieren und die notwendigen Maßnahmen zu ergreifen.

Wenn Amazon EBS feststellt, dass die Daten eines Volumes potenziell inkonsistent sind, werden standardmäßig alle angeschlossenen EC2-Instances für das Volume deaktiviert I/O , wodurch Datenbeschädigungen verhindert werden. Nach der Deaktivierung schlägt die nächste Überprüfung des Volume-Status fehl, und der Volume-Status I/O lautet. `impaired` Darüber hinaus wird ein Ereignis angezeigt, das Sie darüber informiert, dass das Laufwerk deaktiviert I/O ist und dass Sie die Beeinträchtigung des Volumens beheben können, indem Sie das Volume wieder einschalten. I/O EBS wartet, bis Sie die Option aktivieren, I/O um Ihnen die Möglichkeit zu geben, zu entscheiden, ob Sie Ihre Instances weiterhin das Volume verwenden lassen oder ob Sie eine Konsistenzprüfung mit einem Befehl wie fsck (Linux-Instances) oder chkdsk (Windows-Instances) ausführen möchten, bevor Sie dies tun.

> **Note**
>
> Der Volume-Status basiert auf den Volume-Statusprüfungen und gibt nicht den Volume-Zustand wieder. Daher gibt der Volume-Status nicht an, dass sich Volumes im `error` Status

befinden (z. B. wenn ein Volume nicht akzeptiert werden kann). I/O Informationen zum Volume-Status finden Sie unter Angaben zur Lautstärke.

Wenn die Konsistenz eines bestimmten Volumes kein Problem darstellt und Sie es vorziehen, dass das Volume sofort verfügbar gemacht wird, wenn es beeinträchtigt ist, können Sie das Standardverhalten außer Kraft setzen, indem Sie das Volume so konfigurieren, dass es automatisch aktiviert I/O wird. Wenn Sie das Auto-Enable IO-Volume-Attribut (`autoEnableIO`in der API) aktivieren, wird der Status des Volumes weiterhin geprüft. Darüber hinaus wird ein Ereignis angezeigt, das Sie darüber informiert, dass das Volume als potenziell inkonsistent eingestuft wurde, dass es jedoch automatisch aktiviert I/O wurde. Somit können Sie die Konsistenz des Volumes überprüfen oder es zu einem späteren Zeitpunkt ersetzen.

Bei der I/O Leistungsstatusüberprüfung wird die tatsächliche Leistung eines Volumes mit der erwarteten Leistung eines Volumes verglichen. Sie warnt Sie, wenn das Volume unter den Erwartungen liegt. Diese Statusprüfung ist nur für SSD-Volumes mit bereitgestellten IOPS (`io1` und `io2`) und Allzweck-SSD-Volumes (`gp3`) verfügbar, die einer Instance angefügt sind. Die Statusprüfung ist nicht gültig für Allzweck-SSD- (`gp2`), durchsatzoptimierte HDD- (`st1`), Cold-HDD- (`sc1`) und Magnetfestplatten-Volumes (`standard`). Die I/O Leistungsstatusüberprüfung wird einmal pro Minute durchgeführt und CloudWatch erfasst diese Daten alle 5 Minuten. Ab dem Zeitpunkt, an dem Sie ein `io1` `io2` OR-Volume an eine Instance anhängen, kann es bis zu 5 Minuten dauern, bis die Statusüberprüfung den I/O Leistungsstatus meldet.

Important

Bei der Initialisierung bereitgestellter IOPS-SSD-Volumes, die anhand von Snapshots wiederhergestellt wurden, kann die Leistung des Volumes unter 50 Prozent des erwarteten Werts fallen, wodurch für das Volume ein `warning` Status in der I/O Leistungsstatusprüfung angezeigt wird. Dies ist normal. Sie können den Status `warning` bei Bereitgestellte IOPS-SSD-Volumes bei der Initialisierung ignorieren. Weitere Informationen finden Sie unter Initialisieren Sie die Volumes nach der Erstellung manuell.

In der folgenden Tabelle sind die Status für Amazon EBS-Volumes aufgeführt.

Volume-Status	I/O Status aktiviert	I/O Leistungsstatus (**io1io2**, und nur **gp3** Volumes)
ok	Aktiviert (I/O Aktiviert oder I/O Auto-Enabled)	Normal (Volume-Leistung ist wie erwartet)
warning	Aktiviert (I/O Aktiviert oder I/O Auto-Enabled)	Schwach (Volume-Leistung liegt unter den Erwartungen) Sehr schwach (Volume-L eistung liegt weit unter den Erwartungen)
impaired	Aktiviert (I/O Aktiviert oder I/O Auto-Enabled) Deaktiviert (Das Volume ist offline und wartet auf die Wiederherstellung oder wartet darauf, dass Sie es aktivieren I/O)	Blockiert (Volume-Leistung ist stark beeinträchtigt) Nicht verfügbar (I/O Leistung kann nicht ermittelt werden, da deaktiviert I/O ist)
insufficient-data	Aktiviert (I/O Aktiviert oder I/O Auto-Enabled) Unzureichende Daten	Unzureichende Daten

Console

Anzeigen der Statusprüfungen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.

   Die Spalte Volume Status (Volume-Status) zeigt jeweils den Betriebszustand eines Volumes an.
3. Um die Statusdetails eines bestimmten Volumes anzuzeigen, wählen Sie es im Raster aus und wählen Sie die Registerkarte Status Checks (Statusprüfungen).

4. Informationen zu einem Volume mit nicht bestandener Statusprüfung (der Status lautet `impaired`) finden Sie unter Arbeiten Sie mit einem beeinträchtigten Amazon EBS-Volume.

Alternativ dazu können Sie Events (Ereignisse) im Navigator auswählen, um alle Ereignisse für Ihre Instances und Volumes anzuzeigen. Weitere Informationen finden Sie unter Amazon EBS-Volumenereignisse.

AWS CLI

Anzeigen der Informationen zum Volumenstatus

Verwenden Sie den Befehl describe-volume-status .

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

Verwenden Sie das folgende Beispiel, um unzulängliche Lautstärken zu identifizieren.

```
aws ec2 describe-volume-status --filters Name=volume-status.status,Values=impaired
```

PowerShell

Anzeigen der Informationen zum Volumenstatus

Verwenden Sie das cmdlet Get-EC2VolumeStatus.

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

Identifizieren Sie anhand des folgenden Beispiels eine beeinträchtigte Lautstärke.

```
Get-EC2VolumeStatus -Filter @{Name="volume-status.status"; Values="impaired"}
```

Amazon EBS-Volumenereignisse

Wenn Amazon EBS feststellt, dass die Daten eines Volumes potenziell inkonsistent sind, werden alle angeschlossenen EC2-Instances standardmäßig für das Volume deaktiviert I/O . Dies hat zur Folge, dass die Statusprüfung des Volumes nicht bestanden und ein Volume-Statusereignis erstellt wird, das die Ursache des Ausfalls anzeigt.

Um die automatische Aktivierung I/O auf einem Volume mit potenziellen Dateninkonsistenzen durchzuführen, ändern Sie die Einstellung des Auto-Enabled IO-Volume-Attributs (in der API). `autoEnableIO` Weitere Informationen zum Ändern dieses Attributs finden Sie unter Arbeiten Sie mit einem beeinträchtigten Amazon EBS-Volume.

Jedes Ereignis umfasst eine Startzeit, die den Zeitpunkt angibt, zu dem das Ereignis eingetreten ist, und eine Dauer, die angibt, wie I/O lange das Volume deaktiviert war. Die Endzeit wird dem Ereignis hinzugefügt, wenn I/O das Volume aktiviert ist.

Ereignisse mit dem Status des Laufwerks

`Awaiting Action: Enable IO`

Volumendaten sind möglicherweise inkonsistent. I/O ist für das Volume deaktiviert, bis Sie es explizit aktivieren. Die Beschreibung des Ereignisses ändert sich in, IO Enabled nachdem Sie es explizit aktiviert haben I/O.

`IO Enabled`

I/O Operationen wurden für dieses Volume explizit aktiviert.

`IO Auto-Enabled`

I/O Operationen wurden auf diesem Volume automatisch aktiviert, nachdem ein Ereignis eingetreten war. Wir empfehlen, dass Sie die Daten auf Inkonsistenzen überprüfen, bevor Sie sie weiterhin verwenden.

`Normal`

Nur für `io1`-, `io2`- und `gp3`-Volumes. Volume-Leistung ist wie erwartet.

`Degraded`

Nur für `io1`-, `io2`- und `gp3`-Volumes. Volume-Leistung liegt unter den Erwartungen.

`Severely Degraded`

Nur für `io1`-, `io2`- und `gp3`-Volumes. Volume-Leistung liegt weit unter den Erwartungen.

`Stalled`

Nur für `io1`-, `io2`- und `gp3`-Volumes. Volume-Leistung ist stark beeinträchtigt.

Wenn Sie ein Volume haben, auf dem I/O es deaktiviert ist, finden Sie weitere Informationen unterArbeiten Sie mit einem beeinträchtigten Amazon EBS-Volume. Wenn Sie ein Volume

haben, dessen I/O Leistung unter dem Normalwert liegt, kann es sich um einen vorübergehenden Zustand handeln, der auf eine von Ihnen ergriffene Aktion zurückzuführen ist (z. B. Erstellen eines Snapshots eines Volumes bei Spitzenauslastung, Ausführen des Volumes auf einer Instance, die die erforderliche I/O Bandbreite nicht unterstützt, erstmaliger Zugriff auf Daten auf dem Volume usw.).

Console

Anzeigen der Ereignisse für Ihre Volumes

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events. Es werden alle Instances und Volumes aufgelistet, die Ereignisse haben.
3. Sie können das Ergebnis auch nach Volume filtern, damit nur der Status von Volumes angezeigt wird. Sie können auch nach bestimmten Statustypen filtern.
4. Wählen Sie ein Volume aus, um sein Ereignis anzuzeigen.

AWS CLI

Anzeigen der Ereignisse für Ihre Volumes

Verwenden Sie den Befehl describe-volume-status .

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

PowerShell

Anzeigen der Ereignisse für Ihre Volumes

Verwenden Sie das cmdlet Get-EC2VolumeStatus.

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

Arbeiten Sie mit einem beeinträchtigten Amazon EBS-Volume

Verwenden Sie die folgenden Optionen, wenn ein Volume beeinträchtigt ist, weil die Daten des Volumes möglicherweise inkonsistent sind.

Optionen

- Option 1: Durchführen einer Konsistenzprüfung bei dem Volume, das an die Instance angefügt ist
- Option 2: Durchführen einer Konsistenzprüfung bei dem Volume mithilfe einer anderen Instance
- Option 3: Löschen des Volumes, wenn Sie es nicht mehr benötigen

Option 1: Durchführen einer Konsistenzprüfung bei dem Volume, das an die Instance angefügt ist

Die einfachste Option besteht darin, das Volume zu aktivieren I/O und dann eine Datenkonsistenzprüfung durchzuführen, während das Volume noch mit seiner Amazon EC2-Instance verbunden ist.

So führen Sie eine Konsistenzprüfung bei dem angefügten Volume durch

1. Beenden Sie die Nutzung des Volumes durch Anwendungen.
2. I/O Auf dem Volume aktivieren. Verwenden Sie eine der folgenden Methoden:

   Console

   Um es I/O für ein Volume zu aktivieren

   1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im Navigationsbereich die Option Events.
   3. Wählen Sie das Volume aus.
   4. Wählen Sie Aktionen, I/O aktivieren.

   AWS CLI

   Um ein Volume I/O zu aktivieren

   Verwenden Sie den Befehl enable-volume-io.

   ```
   aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
   ```

   PowerShell

   Um ein Volume I/O zu aktivieren

   Verwenden Sie das cmdlet Enable-EC2VolumeIO.

```
Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
```

3. Überprüfen Sie die Daten auf dem Volume.

   a. Führen Sie den Befehl fsck (Linux-Instanzen) oder chkdsk (Windows-Instanzen) aus.

   b. (Optional) Überprüfen Sie verfügbare Anwendungen oder Systemprotokolle auf relevante Fehlermeldungen.

   c. Wenn die Lautstärke länger als 20 Minuten lang beeinträchtigt ist, können Sie sich an das AWS Support Center wenden. Wählen Sie Troubleshoot (Fehlerbehebung) und anschließend im Dialogfeld Troubleshoot Status Checks (Fehlerbehebung bei Statusprüfungen) die Option Contact Support (Support kontaktieren) aus, um einen Supportfall zu eröffnen.

Option 2: Durchführen einer Konsistenzprüfung bei dem Volume mithilfe einer anderen Instance

Wenden Sie das folgende Verfahren an, um das Volume außerhalb Ihrer Produktionsumgebung zu überprüfen.

> **Important**
>
> Dieses Verfahren kann dazu führen, I/Os dass Schreibvorgänge verloren gehen, die bei der Deaktivierung des Volumes I/O unterbrochen wurden.

So führen Sie eine Konsistenzprüfung bei einem isolierten Volume durch

1. Beenden Sie die Nutzung des Volumes durch Anwendungen.
2. Trennen Sie das Volume von der Instance. Weitere Informationen finden Sie unter Trennen Sie ein Amazon EBS-Volume von einer Amazon EC2-Instance.
3. I/O Auf dem Volume aktivieren. Verwenden Sie eine der folgenden Methoden:

   Console

   Um es I/O für ein Volume zu aktivieren

   1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie das Volume aus, dessen Zuordnung Sie im vorherigen Schritt aufgehoben haben.
4. Wählen Sie Aktionen, I/O aktivieren.

AWS CLI

Um ein Volume I/O zu aktivieren

Verwenden Sie den Befehl enable-volume-io.

```
aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
```

PowerShell

Um ein Volume I/O zu aktivieren

Verwenden Sie das cmdlet Enable-EC2VolumeIO.

```
Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
```

4. Fügen Sie das EBS-Volume an eine andere Instance an. Weitere Informationen finden Sie unter Starten Sie Ihre Instance und Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.
5. Überprüfen Sie die Daten auf dem Volume.
   a. Führen Sie den Befehl fsck (Linux-Instances) oder chkdsk (Windows-Instances) aus.
   b. (Optional) Überprüfen Sie verfügbare Anwendungen oder Systemprotokolle auf relevante Fehlermeldungen.
   c. Wenn die Lautstärke länger als 20 Minuten lang beeinträchtigt ist, können Sie sich an das AWS Support Center wenden. Wählen Sie Troubleshoot und anschließend im Dialogfeld für die Fehlersuche die Option Contact Support aus, um einen Supportfall zu eröffnen.

Option 3: Löschen des Volumes, wenn Sie es nicht mehr benötigen

Wenn Sie das Volume aus Ihrer Umgebung entfernen möchten, löschen Sie es einfach. Informationen zum Löschen von Volumes finden Sie unter Löschen eines Amazon EBS-Volumes.

Wenn Sie einen kürzlichen Snapshot haben, mit dem die Daten auf dem Volume gesichert sind, können Sie aus dem Snapshot ein neues Volume erstellen. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.

Auto-enable I/O für beeinträchtigte Amazon EBS-Volumes

Wenn Amazon EBS feststellt, dass die Daten eines Volumes potenziell inkonsistent sind, werden standardmäßig alle angeschlossenen EC2-Instances für das Volume deaktiviert I/O . Dies hat zur Folge, dass die Statusprüfung des Volumes nicht bestanden und ein Volume-Statusereignis erstellt wird, das die Ursache des Ausfalls anzeigt. Wenn die Konsistenz eines bestimmten Volumes kein Problem darstellt und Sie es vorziehen, dass das Volume sofort verfügbar gemacht wird, wenn es beeinträchtigt ist, können Sie das Standardverhalten außer Kraft setzen, indem Sie das Volume so konfigurieren, dass es automatisch aktiviert wird. I/O Wenn Sie das Auto-Enabled I/O-Volume-Attribut (`autoEnableIO`in der API) aktivieren, wird die I/O Verbindung zwischen dem Volume und der Instance automatisch wieder aktiviert und die Statusüberprüfung des Volumes wird erfolgreich abgeschlossen. Darüber hinaus wird ein Ereignis angezeigt, das Sie darüber informiert, dass sich das Volume in einem potenziell inkonsistenten Zustand befand, es jedoch automatisch aktiviert I/O wurde. Wenn dieses Ereignis auftritt, sollten Sie die Konsistenz des Volumes überprüfen und es nötigenfalls ersetzen. Weitere Informationen finden Sie unter Amazon EBS-Volumenereignisse.

Console

So zeigen Sie das Auto-Enabled IO-Attribut eines Volumes an

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus und klicken Sie auf Status Checks (Statusprüfungen).

   Das Auto-enabled I/O Feld zeigt die aktuelle Einstellung (Aktiviert oder Deaktiviert) für das ausgewählte Volume an.

Um das Auto-Enabled IO-Attribut eines Volumes zu ändern

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus und wählen Sie Aktionen, Verwaltung automatisch aktiviert I/O.

4. Um die automatische Aktivierung I/O bei eingeschränkter Lautstärke durchzuführen, aktivieren Sie das Kontrollkästchen Auto-enable I/O Für eingeschränkte Lautstärke. Um das Feature zu deaktivieren, deaktivieren Sie das Kontrollkästchen.
5. Wählen Sie Aktualisieren aus.

AWS CLI

Anzeigen des Attributs AutoEnableIO eines Volumes

Verwenden Sie den Befehl describe-volume-attribute.

```
aws ec2 describe-volume-attribute \
    --attribute autoEnableIO \
    --volume-id vol-01234567890abcdef
```

Es folgt eine Beispielausgabe.

```
{
    "AutoEnableIO": {
        "Value": true
    },
    "VolumeId": "vol-01234567890abcdef"
}
```

So ändern Sie das autoEnableIO-Attribut eines Volumes

Verwenden Sie den Befehl modify-volume-attribute.

```
aws ec2 modify-volume-attribute \
    --auto-enable-io \
    --volume-id vol-01234567890abcdef
```

PowerShell

Anzeigen des Attributs AutoEnableIO eines Volumes

Verwenden Sie das cmdlet Get-EC2VolumeAttribute.

```
(Get-EC2VolumeAttribute `
    -Attribute autoEnableIO `
```

```
    -VolumeId vol-01234567890abcdef).AutoEnableIO
```

Es folgt eine Beispielausgabe.

```
True
```

So ändern Sie das autoEnableIO-Attribut eines Volumes

Verwenden Sie das cmdlet Edit-EC2VolumeAttribute.

```
Edit-EC2VolumeAttribute `
    -AutoEnableIO $true `
    -VolumeId vol-01234567890abcdef
```

Fehlertests auf Amazon EBS

AWS Fault Injection Service (AWS FIS) ist ein vollständig verwalteter Service, der Sie bei der Durchführung von Fehlerinjektionsexperimenten an Ihren AWS Workloads unterstützt. Mit aktivierten EBS-Aktionen können Sie testen AWS FIS, wie Ihre Anwendungen auf Speicherfehler reagieren, die zu I/O Unterbrechungen und Leistungseinbußen auf Ihren Volumes führen können. In dieser kontrollierten Testumgebung können Sie beobachten, wie Ihre Anwendungen auf Störungen reagieren, sodass Sie Schwachstellen in Ihrer Architektur identifizieren und die allgemeine Widerstandsfähigkeit Ihrer Anwendungen verbessern können. Mithilfe der I/O Aktionen Pause und Latency Injection können Sie Ihre Überwachungs- und Wiederherstellungsmechanismen wie CloudWatch Amazon-Alarme und Failover-Workflows testen und die Widerstandsfähigkeit Ihrer unternehmenskritischen Anwendungen gegenüber Speicherfehlern verbessern. Weitere Informationen dazu finden Sie im AWS FIS Benutzerhandbuch. AWS Fault Injection Service

Verfügbare Experimente

Amazon EBS unterstützt derzeit zwei AWS FIS Fehlerinjektionen:

- Unterbrechen Sie die I/O Fehlereinleitung
- Latenzinjektion

Überlegungen

Beachten Sie die folgenden Überlegungen:

- Alle Amazon EBS-Volumetypen werden unterstützt. Sowohl Root-Volumes als auch Datenvolumes werden unterstützt. Instance-Speicher-Volumes werden nicht unterstützt.
- Volumes müssen an Nitro-based EC2-Instances angehängt werden.
- Je nach Dauer nehmen Ihre Volumes nach Abschluss des Experiments ihre ursprüngliche I/O Leistung wieder auf. Sie können ein laufendes Experiment auch beenden, bevor es abgeschlossen ist. Alternativ können Sie eine Stoppbedingung erstellen, um das Experiment zu beenden, wenn es einen Schwellenwert erreicht, den Sie in einem CloudWatch Alarm definiert haben.
- Sie können es AWS FIS mit Multi-Attach aktivierten Lautsprechern verwenden. Alle angehängten Instanzen sind betroffen. Sie können kein bestimmtes Volume-Instance-Attachment für Experimente auswählen.
- FIS ist derzeit in Local Zones, Outposts oder Wavelength Zones nicht verfügbar.
- Sie können bis zu 5 Volumes in derselben Availability Zone gleichzeitig testen, wenn Sie Volume-ARNs in der Konsole angeben.
- Sie können es nicht AWS FIS mit Volumes verwenden, die in einerOutpost, in einer AWS Wavelength Zone oder in einer lokalen Zone erstellt wurden.

Unterbrechen Sie die I/O Fehlereinleitung

Verwenden Sie AWS Fault Injection Service und die I/O Aktion Pause, um I/O zwischen einem Amazon EBS-Volume und den Instances, an die es angehängt ist, vorübergehend anzuhalten, um zu testen, wie Ihre Workloads mit Unterbrechungen umgehen. I/O

Weitere Informationen AWS FIS dazu finden Sie im AWS Fault Injection Service Benutzerhandbuch.

Überlegungen

Beachten Sie beim Anhalten der Lautstärke die folgenden Überlegungen: I/O

- Pause I/O wird auf allen Nitro-based Instance-Typen unterstützt.
- Legen Sie zum Testen der Timeout-Konfiguration Ihres Betriebssystems die Testdauer gleich oder größer als den für `nvme_core.io_timeout` angegebenen Wert fest. Weitere Informationen finden Sie unter Timeout bei I/O NVMe-Vorgängen für Amazon EBS-Volumes.
- Wenn Sie I/O zu einem Volume fahren, das I/O angehalten wurde, passiert Folgendes:
  - Der Status des Volumes wechselt innerhalb von 120 Sekunden zu `impaired`. Weitere Informationen finden Sie unter Statusüberprüfungen des Amazon EBS-Volumes.

- Die CloudWatch Metrik für gibt `VolumeStalledIOCheck` an, `1` ob die Lautstärke länger I/O als 60 Sekunden angehalten wurde. Weitere Informationen finden Sie unter Metriken für Amazon-EBS-Volumes.
- Die CloudWatch Metriken für die Länge der Warteschlange (`VolumeQueueLength`) sind ungleich Null. Alle Warnungen oder Überwachungen sollten auf eine Warteschlangentiefe ungleich Null überwachen.
- Die CloudWatch Metriken für `VolumeReadOps` oder `VolumeWriteOps` werden sein`0`, was darauf hinweist, dass das Volume nicht mehr verarbeitet I/O wird.

Sie können ein einfaches Experiment von der Amazon EC2-Konsole aus durchführen, oder Sie können komplexere Experimente mithilfe der AWS FIS Konsole durchführen. Weitere Informationen zur Durchführung fortgeschrittener Experimente mit der AWS FIS Konsole finden Sie unter Tutorials AWS FIS im AWS Fault Injection Service Benutzerhandbuch.

So führen Sie ein einfaches Experiment mit der Amazon-EC2-Konsole durch

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie die Lautstärke aus, für die Sie pausieren möchten, I/O und wählen Sie „Aktionen“, „Fehlerinjektion“ und „Lautstärke anhalten I/O“.
4. Geben Sie unter Dauer die Dauer ein, für die I/O zwischen dem Volume und den Instances eine Pause eingelegt werden soll. Das Feld neben der Dropdown-Liste „Dauer“ zeigt die Dauer im ISO-8601-Format an.
5. Wählen Sie im Abschnitt Servicezugriff die IAM-Servicerolle aus, die Sie für AWS FIS die Durchführung des Experiments übernehmen möchten. Sie können entweder die Standardrolle verwenden oder eine vorhandene Rolle, die Sie erstellt haben. Weitere Informationen finden Sie unter Erstellen einer IAM-Rolle für AWS FIS -Experimente.
6. Wählen Sie Lautstärke I/O anhalten. Wenn Sie dazu aufgefordert werden, geben Sie `start` in das Bestätigungsfeld ein und wählen Sie Experiment starten.
7. Überwachen Sie den Fortschritt und die Auswirkungen Ihres Experiments. Weitere Informationen finden Sie unter Überwachung von AWS FIS im AWS FIS -Benutzerhandbuch.

Latenzinjektion

Verwenden Sie die Aktion Latency Injection (`aws:ebs:volume-io-latency`) in AWS FIS , um eine erhöhte I/O Latenz auf Ihren Amazon EBS-Volumes zu simulieren und zu testen, wie Ihre Anwendungen auf eine Verschlechterung der Speicherleistung reagieren. Mit dieser Aktion können Sie den Latenzwert angeben, der injiziert werden soll, sowie den Prozentsatz I/O , in dem sich dies auf das Zielvolume auswirkt. Mit AWS FIS können Sie vorkonfigurierte Vorlagen für Latenzexperimente verwenden, um mit dem Testen verschiedener I/O Latenzmuster zu beginnen, die bei Speicherfehlern auftreten können. Diese Vorlagen sind als erste Reihe von Szenarien konzipiert, die Sie verwenden können, um Ihre Anwendungen zu unterbrechen und die Stabilität zu testen. Sie sind nicht dafür konzipiert, alle Arten von Auswirkungen abzudecken, denen Ihre Anwendungen in der realen Welt ausgesetzt sein können. Wir empfehlen Ihnen, sie so anzupassen, dass Sie je nach den Leistungsanforderungen Ihrer Anwendungen mehrere verschiedene Tests ausführen können. Sie können die verfügbaren Vorlagen anpassen oder neue Versuchsvorlagen erstellen, um sie auf Ihre anwendungsspezifischen Anforderungen hin zu testen.

Pre-configured Vorlagen für Latenzexperimente

Amazon EBS stellt die folgenden Vorlagen für Latenzexperimente über die EBS-Konsole und die AWS FIS Szenariobibliothek bereit. Sie können diese Vorlagen direkt auf Ihren Ziel-Volumes verwenden, um ein Latenzinjektionsexperiment durchzuführen.

- Anhaltende Latenz — Simuliert eine konstante Latenz. Dieses Experiment verwendet eine Latenzinjektion und hat eine Gesamtdauer von 15 Minuten. Dieses Experiment simuliert eine anhaltende Latenz bei 50 Prozent des Lesens I/O und 100 Prozent des Schreibens I/O: 500 ms für 15 Minuten.
- Steigende Latenz — Simuliert eine schrittweise Erhöhung der Latenz. Dieses Experiment verwendet fünf Latenzinjektionsaktionen und hat eine Gesamtdauer von 15 Minuten. In diesem Experiment wird ein allmählicher Anstieg der Latenz bei 10 Prozent des Lesens I/O und 25 Prozent des Schreibens simuliert I/O: 50 ms für 3 Minuten, 200 ms für 3 Minuten, 700 ms für 3 Minuten, 1 Sekunde für 3 Minuten und 15 Sekunden für 3 Minuten.
- Intermittierende Latenz — Simuliert starke intermittierende Latenzspitzen mit dazwischen liegenden Erholungsphasen. Dieses Experiment verwendet drei Latenzinjektionsaktionen und hat eine Gesamtdauer von 15 Minuten. Bei diesem Experiment werden drei Latenzspitzen bei 0,1 Prozent der Lese- und Schreibvorgänge simuliert I/O: eine 30-Sekunden-Spitze, die eine Minute andauert, eine 10-Sekunden-Spitze, die 2 Minuten anhält, und eine 20-Sekunden-Spitze, die 2 Minuten andauert. Zwischen den einzelnen Latenzspitzen gibt es Erholungsphasen von 5 Minuten.

- Abnehmende Latenz — Simuliert eine allmählich abnehmende Latenz. Dieses Experiment verwendet fünf Latenzinjektionsaktionen und hat eine Gesamtdauer von 15 Minuten. In diesem Experiment wird eine allmähliche Verringerung der Latenz bei 10 Prozent der Lese I/O - und Schreibvorgänge simuliert I/O: 20 Sekunden für 3 Minuten, 5 Sekunden für 3 Minuten, 900 ms für 3 Minuten, 300 ms für 3 Minuten und 40 ms für 3 Minuten.

Passen Sie vorkonfigurierte Szenarien an

Sie passen die oben genannten vorkonfigurierten Vorlagen an oder erstellen Ihre eigenen neuen Versuchsvorlagen mithilfe der folgenden anpassbaren Parameter.

- `readIOPercentage`— Prozentsatz der I/O Lesevorgänge, bei denen Latenz erzeugt wird. Dies ist der Prozentsatz aller I/O Lesevorgänge auf dem Volume, die von der Aktion betroffen sein werden.

  Bereich: Min. 0,1%, Max. 100%
- `readIOLatencyMilliseconds`— Umfang der Latenz, die bei I/O Lesevorgängen injiziert wird. Dies ist der Latenzwert, der I/O während des Experiments für den angegebenen Prozentsatz der Lesevorgänge beobachtet wird.

  Bereich: Min. 1 ms (io2)/10 ms (nicht io2), Max. 60 Sekunden
- `writeIOPercentage`— Prozentsatz der I/O Schreibvorgänge, bei denen Latenz erzeugt wird. Dies ist der Prozentsatz aller I/O Schreibvorgänge auf dem Volume, die von der Aktion betroffen sein werden.

  Bereich: Min. 0,1%, Max. 100%
- `writeIOLatencyMilliseconds`— Umfang der Latenz, die bei I/O Schreibvorgängen injiziert wird. Dies ist der Latenzwert, der bei dem angegebenen Prozentsatz der Schreibvorgänge I/O während des Experiments beobachtet wird.

  Bereich: Min. 1 ms (io2)/10 ms (nicht io2), max. 60 Sekunden
- `duration`— Dauer, für die die Latenz auf Basis des ausgewählten Prozentsatzes berechnet wird. I/O

  Bereich: Min. 1 Sekunde, Max. 12 Stunden

Überwachung der Latenzinjektion

Sie können die Auswirkungen auf die Leistung Ihrer Volumes auf folgende Weise überwachen:

- Verwenden Sie Metriken zur durchschnittlichen Latenz CloudWatch , um die durchschnittliche I/O Latenz pro Minute zu ermitteln. Weitere Informationen finden Sie unter Überwachen Sie Ihre EBS-Volumes mit. CloudWatch
- Verwenden Sie die detaillierten EBS-Leistungsstatistiken NVMe-CLI, die über CloudWatch Agent und Prometheus verfügbar sind, um die durchschnittliche Latenz pro Sekunde zu ermitteln. I/O Die detaillierten Metriken enthalten auch I/O Latenzhistogramme, anhand derer Sie die Latenzvarianz auf Ihren Volumes analysieren können. Weitere Informationen finden Sie unter Detaillierte NVMe-Leistungsstatistiken.
- Verwenden Sie die Statusüberprüfungen des Amazon EBS-Volumes. Wenn Sie I/O Latenz eingeben, wechselt der Status des Volumes in den `warning` Status.

Überlegungen

Beachten Sie Folgendes, wenn Sie die EBS-Latenzinjektion verwenden:

- Die Latenzinjektion wird auf allen Nitro-based Instance-Typen unterstützt, mit Ausnahme von: P4d, P5, P5e, Trn2u, G6, G6f, Gr6, Gr6f, M8i,, R8i,, i8GE und. M8i-flex C8i-flex R8i-flex Mac-m4pro Mac-m4
- Möglicherweise stellen Sie eine Abweichung von bis zu 5 Prozent zwischen dem im Experiment angegebenen Latenzwert und der daraus resultierenden beobachteten Latenz fest.
- Wenn Sie nur eine sehr kleine Anzahl von I/O Vorgängen ausführen, entspricht der in den Aktionsparametern I/O angegebene Prozentsatz der Operationen möglicherweise nicht dem tatsächlichen Prozentsatz der von der Aktion I/O betroffenen Operationen.

Um ein Latenzinjektionsexperiment auf einem Amazon EBS-Volume durchzuführen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie die Volumes aus, auf denen das Experiment ausgeführt werden soll, und wählen Sie Actions, Resilience Testing, Inject Volume I/O Latency aus.

   Die AWS Fault Injection Service Konsole wird geöffnet.
4. Wählen Sie im Fenster Experiment erstellen den Typ des auszuführenden Experiments aus: Intermittierend, Zunehmend , Anhaltend oder Abnehmend.
5. Wählen Sie für die IAM-Rollenauswahl die Option Neue Rolle erstellen aus, um eine neue Rolle zu erstellen, mit der die Experimente in Ihrem Namen durchgeführt AWS FIS werden.

Wählen Sie alternativ eine vorhandene IAM-Rolle verwenden aus, wenn Sie zuvor eine IAM-Rolle mit den erforderlichen Berechtigungen erstellt haben.

6. Im Abschnitt Kostenvoranschlag erhalten Sie eine Schätzung der Kosten für die Durchführung des Experiments. Mit wird Ihnen pro Minute AWS FIS, die eine Aktion von Anfang bis Ende ausgeführt wird, auf der Grundlage der Anzahl der Zielkonten für Ihr Experiment in Rechnung gestellt.
7. Wählen Sie Start Experiment (Experiment starten) aus.

Amazon EBS-Snapshots

Sie können die auf Ihren Amazon-EBS-Volumes gespeicherten Daten sichern, indem Sie zeitpunktbezogene Kopien erstellen, die als Amazon EBS-Snapshots bezeichnet werden. Ein Snapshot ist eine inkrementelle Sicherung, es werden also nur die Blöcke auf dem Volume gespeichert, die seit dem letzten Snapshot geändert wurden. Hierdurch wird die zum Erstellen des Snapshots erforderliche Zeit verringert und es werden Speicherkosten eingespart, weil keine Datenduplikate angelegt werden.

> **Important**
>
> AWS erstellt nicht automatisch eine Sicherungskopie der auf Ihren EBS-Volumes gespeicherten Daten. Aus Gründen der Datenstabilität und Notfallwiederherstellung liegt es in Ihrer Verantwortung, regelmäßige EBS-Snapshots zu erstellen oder die automatische Snapshot-Erstellung mithilfe von Automatisieren Sie Backups mit Amazon Data Lifecycle Manager oder AWS Backup einzurichten.

Snapshots werden in Amazon S3 in S3-Buckets gespeichert, auf die Sie nicht direkt zugreifen können. Sie können Snapshots manuell mit der Amazon-EC2-Konsole oder der Amazon-EC2-API erstellen. Sie können nicht über die Amazon-S3-Konsole oder die Amazon-S3-API auf Ihre Snapshots zugreifen.

Snapshot-Daten werden automatisch in alle Availability Zones der Region repliziert. Dies sorgt für eine hohe Verfügbarkeit und Beständigkeit der Snapshot-Daten und ermöglicht Ihnen die Wiederherstellung von Volumes in allen Availability Zones dieser Region.

Jeder Snapshot enthält alle erforderlichen Informationen für die Wiederherstellung Ihrer Daten (ab dem Erstellungszeitpunkt des Snapshots) auf einem neuen EBS-Volume. Wenn Sie ein EBS-Volume anhand eines Snapshots erstellen, startet das neue Volume als identische Kopie des Volumes, das für den Snapshot verwendet wurde.

Weitere Informationen finden Sie auf der Produktseite zu Amazon-EBS-Snapshots.

Snapshot-Ereignisse

Sie können den Status Ihrer EBS-Snapshots über Ereignisse verfolgen. CloudWatch Weitere Informationen finden Sie unter EBS-Snapshot-Ereignisse.

Snapshot-Preise

Die Gebühren für Ihre Snapshots basieren auf der Menge der gespeicherten Daten. Da Snapshots inkrementell sind, verringert das Löschen eines Snapshots möglicherweise die Datenspeicherkosten nicht. Daten, auf die ausschließlich von einem Snapshot verwiesen wird, werden entfernt, wenn dieser Snapshot gelöscht wird, aber Daten, auf die von anderen Snapshots verwiesen wird, bleiben erhalten. Weitere Informationen finden Sie unter Amazon Elastic Block Store-Volumes und -Snapshots im Benutzerhandbuch für AWS Billing .

Inhalt

- So funktionieren Amazon EBS-Snapshots
- Lebenszyklus eines Amazon EBS-Snapshots
- Schnelle Amazon EBS-Snapshot-Wiederherstellung
- Amazon-EBS-Snapshot-Sperre
- Sperren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots
- Lokale Amazon-EBS-Snapshots auf Outposts
- Lokale Schnappschüsse in lokalen Zonen

So funktionieren Amazon EBS-Snapshots

Der erste Snapshot, den Sie aus einem Volume erstellen, ist immer ein vollständiger Snapshot. Es enthält alle Datenblöcke, die zum Zeitpunkt der Snapshot-Erstellung auf das Volume geschrieben wurden. Nachfolgende Snapshots desselben Volumes sind inkrementelle Snapshots. Diese enthalten nur geänderte und neue Datenblöcke, die seit der Erstellung des letzten Snapshots auf das Volume geschrieben wurden

Die Größe eines vollständigen Snapshots wird durch die Größe der zu sichernden Daten bestimmt, nicht durch die Größe des Quell-Volumes. Ebenso werden die mit einem vollständigen Snapshot verbundenen Speicherkosten von der Größe des Snapshots und nicht von der Größe des Quell-Volumes bestimmt. Beispielsweise erstellen Sie den ersten Snapshot eines `200 GiB`-Amazon-EBS-Volumes, das nur `50 GiB` an Daten enthält. Dies führt zu einem vollständigen Snapshot mit einer Größe von `50 GiB`, und Ihnen wird `50 GiB` Snapshot-Speicher in Rechnung gestellt.

In ähnlicher Weise werden die Größe und die Speicherkosten eines inkrementellen Snapshots durch die Größe aller Daten bestimmt, die seit der Erstellung des vorherigen Snapshots auf das Volume geschrieben wurden. Wenn Sie das vorherige Beispiel fortsetzen und nach dem Ändern `20 GiB` von

Daten und Hinzufügen von Daten einen zweiten Snapshot desselben 200 GiB Volumes erstellen, hat 10 GiB der inkrementelle Snapshot die Größe. 30 GiB Dieser zusätzliche 30 GiB Snapshot-Speicher wird Ihnen dann in Rechnung gestellt.

Weitere Informationen zu Snapshot-Preisen finden Sie unter Amazon-EBS-Preise.

> **Important**
>
> Wenn Sie einen inkrementellen Snapshot archivieren, wird dieser in einen vollständigen Snapshot umgewandelt, der alle Blöcke enthält, die zum Zeitpunkt der Erstellung des Snapshots auf das Volume geschrieben wurden. Anschließend wird es zur Stufe von Amazon EBS Snapshots Archive verschoben. Snapshots im Archivstufe werden zu einem anderen Preis abgerechnet als Snapshots im Standardstufe. Weitere Informationen finden Sie unter Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots.

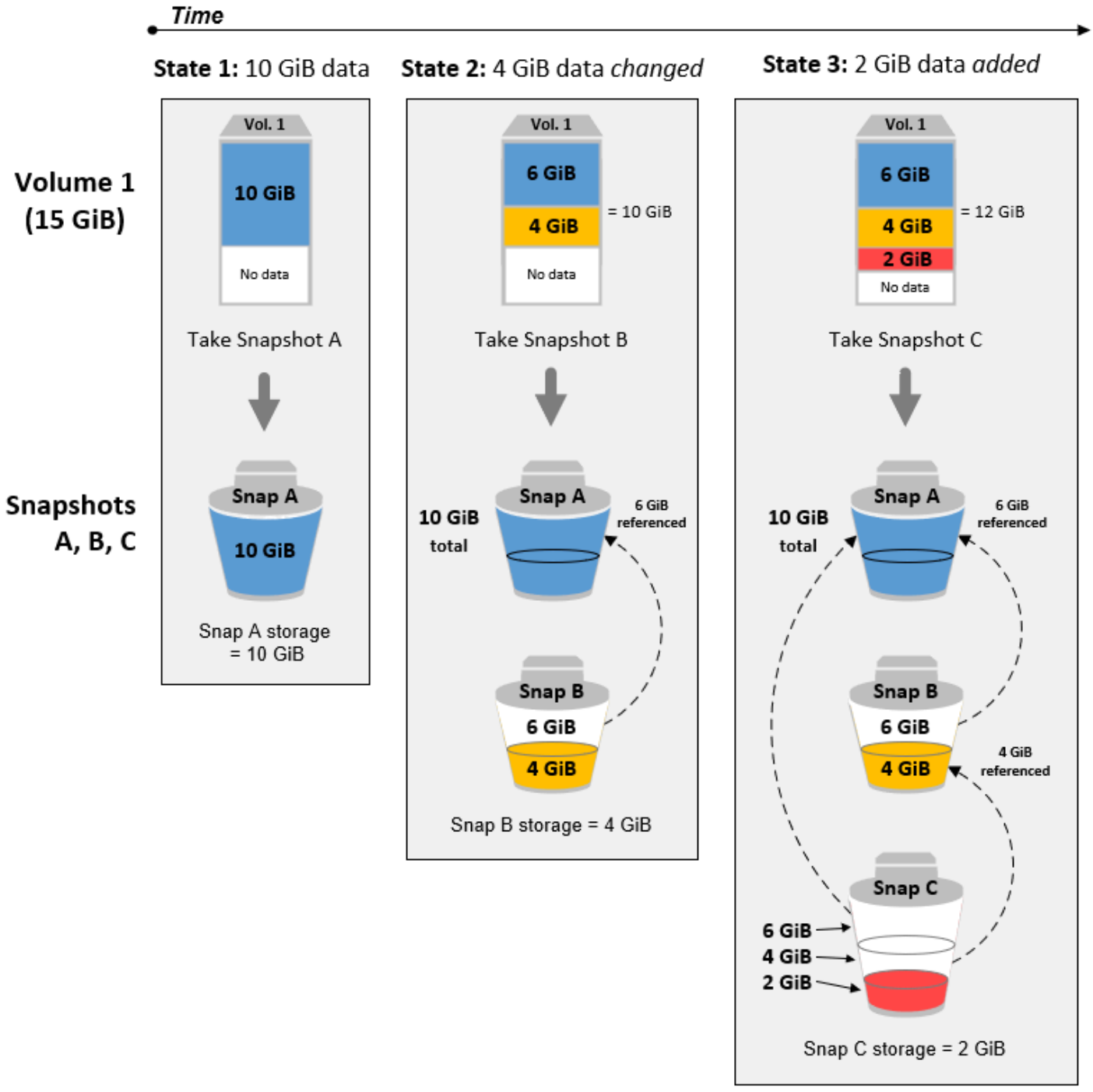
In den folgenden Abschnitten wird gezeigt, wie ein EBS-Snapshot den Status eines Volumes zu einem bestimmten Zeitpunkt erfasst und wie nachfolgende Snapshots eines sich ändernden Volumes einen Verlauf dieser Änderungen erstellen.

Mehrere Snapshots desselben Volumes

Das Diagramm in diesem Abschnitt zeigt Volume 1, das 15 GiB groß ist, zu drei verschiedenen Zeitpunkten. Von jedem dieser drei Volume-Status wurde ein Snapshot angelegt. Das Diagramm zeigt insbesondere Folgendes:

- In Status 1 verfügt das Volume über 10 GiB an Daten. Snap A der erste Snapshot des Volumes. Snap A ist ein vollständiger Snapshot, und die gesamten 10 GiB an Daten werden gesichert.
- In Status 2 verfügt das Volume weiterhin über 10 GiB an Daten, aber nur 4 GiB haben sich geändert, nachdem Snap A erstellt wurde. Snap B ist ein inkrementeller Snapshot. Es müssen nur die 4 GiB gesichert werden, die sich geändert haben. Die übrigen 6 GiB an unveränderten Daten, die bereits in Snap A gesichert sind, werden referenziert von Snap B, anstatt erneut gesichert zu werden. Dies ist durch den gestrichelten Pfeil dargestellt.
- In Status 3 wurden dem Volume 2 GiB an Daten hinzugefügt, sodass es jetzt insgesamt über 12 GiB verfügt, nachdem Snap B erstellt wurde. Snap B ist ein inkrementeller Snapshot. Es müssen nur die 2 GiB gesichert werden, die nach der Erstellung von Snap B hinzugefügt wurden. Wie durch die gestrichelten Pfeile dargestellt, verweist Snap C auch auf die 4 GiB an Daten, die in Snap B gespeichert sind, und auf die 6 GiB an Daten, die in Snap A gespeichert sind.

- Der erforderliche Gesamtspeicher für die drei Snapshots beträgt insgesamt 16 `GiB`. Dies entspricht 10 GB für Snap A, 4 GB für Snap B und 2 GB für Snap C.



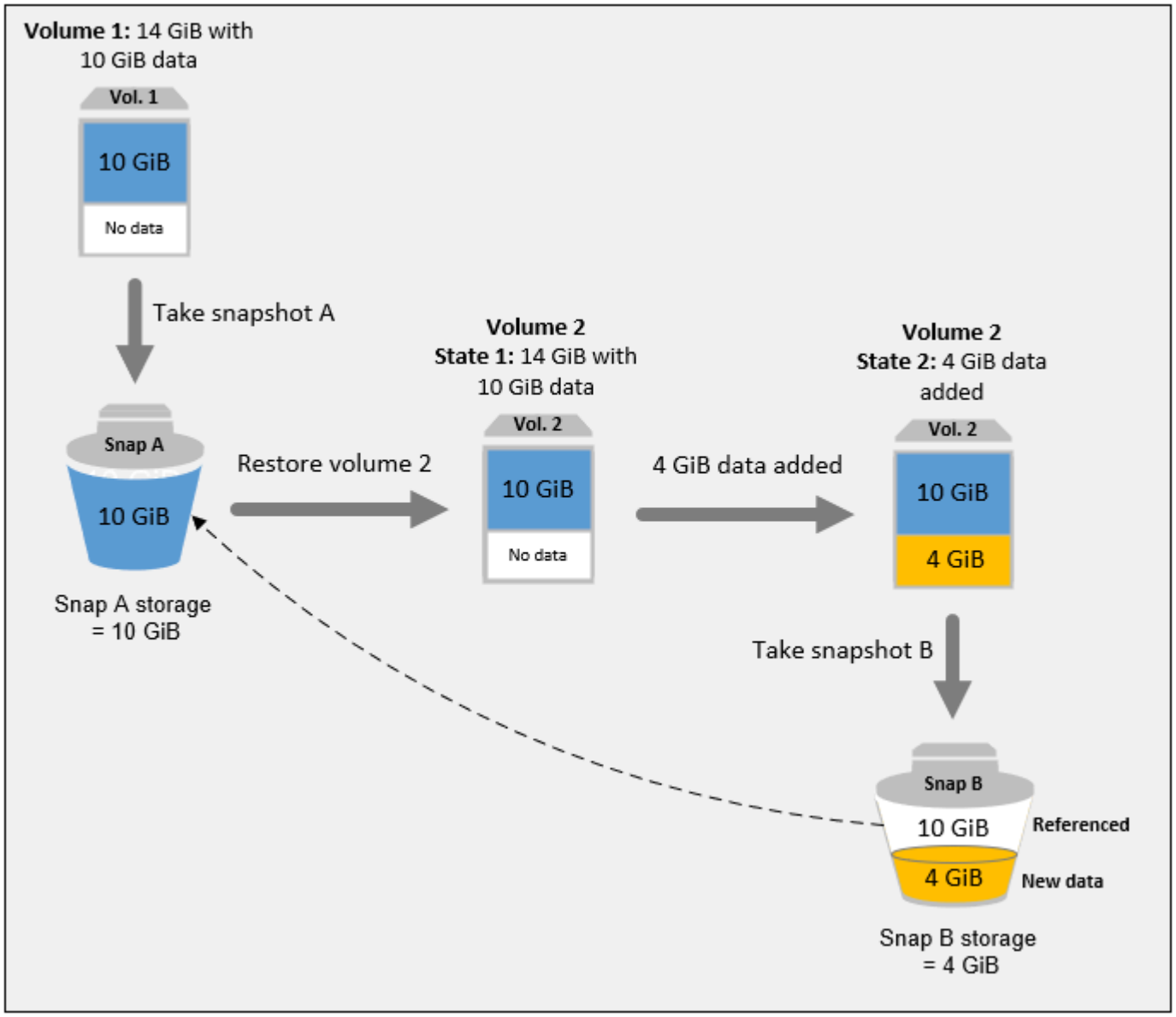
Inkrementelle Snapshots verschiedener Volumes

Das Diagramm in diesem Abschnitt zeigt, wie inkrementelle Snapshots von verschiedenen Volumes aufgenommen werden können.

1. Volume 1, das groß `14 GiB` ist, enthält `10 GiB` an Daten. Da Snap A der erste Snapshot des Volumes ist, handelt es sich um einen vollständigen Snapshot, und die gesamten `10 GiB` an Daten werden gesichert.
2. Vol 2 wird aus Snap A erstellt, daher ist es ein genaues Replikat von Vol 1 zum Zeitpunkt der Erstellung des Snapshots.
3. Im Laufe der Zeit werden `4 GiB` Daten zu Vol 2 hinzugefügt und die Gesamtgröße der Daten beträgt `14 GiB`.
4. Snap B wird aus Vol 2 erstellt. Für Snap B werden nur die `4 GiB` an Daten gesichert, die hinzugefügt wurden, nachdem das Volume aus Snap A erstellt wurde. Die übrigen `10 GiB` an unveränderten Daten, die bereits in Snap A gesichert sind, werden von Snap B referenziert, anstatt erneut gesichert zu werden.

   Snap B ist ein inkrementeller Snapshot von Snap A, obwohl er aus einem anderen Volume erstellt wurde.

> **Important**
>
> Das Diagramm geht davon aus, dass Sie Vol 1 und Snap A besitzen und dass Vol 2 mit demselben KMS-Schlüssel wie Vol 1 verschlüsselt ist. Wenn Band 1 einem anderen AWS Konto gehört und dieses Konto Snap A übernommen und mit dir geteilt hat, dann wäre Snap B ein vollständiger Snapshot. Oder wenn Vol 2 mit einem anderen KMS-Schlüssel verschlüsselt wurde als Vol 1, dann würde es sich bei Snap B um einen vollständigen Snapshot handeln.



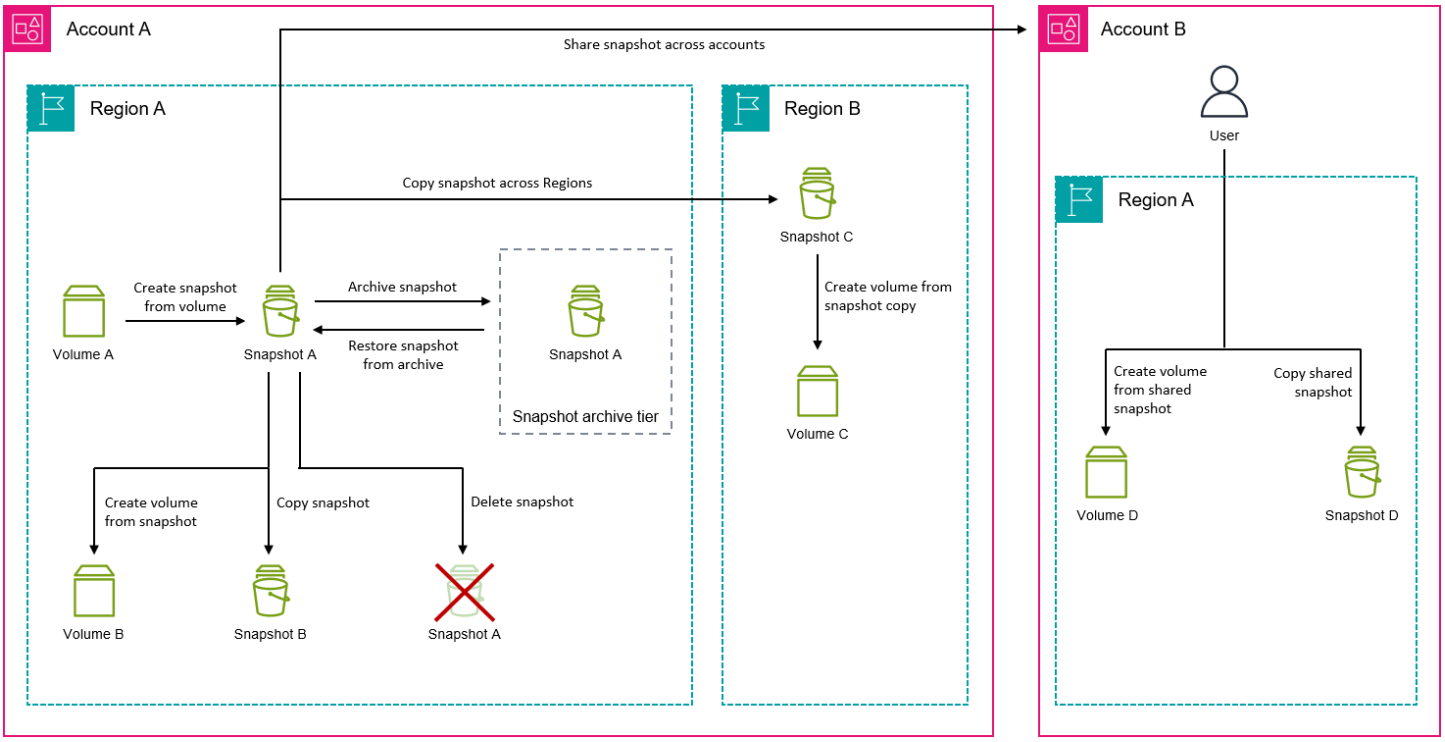
Weitere Informationen dazu, wie Daten beim Löschen eines Snapshots verwaltet werden, erhalten Sie unter Löschen eines Amazon EBS-Snapshots.

Lebenszyklus eines Amazon EBS-Snapshots

Der Lebenszyklus eines Amazon EBS-Snapshots beginnt mit dem Erstellungsprozess. Sie erstellen Snapshots aus Amazon EBS-Volumes. Sie können Snapshots verwenden, um neue Amazon EBS-Volumes wiederherzustellen. Sie können Kopien von Snapshots entweder in derselben Region oder in verschiedenen Regionen erstellen. Sie können Schnappschüsse mit anderen teilen AWS-Konten, entweder öffentlich oder privat. Diese Konten können Volumes aus den geteilten Snapshots wiederherstellen oder sie können Kopien der geteilten Snapshots in ihrem eigenen Konto erstellen.

Wenn Sie keinen sofortigen Zugriff auf einen Snapshot benötigen, können Sie ihn archivieren, um Speicherkosten zu sparen.

Die folgende Abbildung zeigt Aktionen, die Sie im Rahmen des Snapshot-Lebenszyklus an Ihren Snapshots ausführen können.



Aufgaben

- Erstellen von Amazon EBS-Snapshots
- Amazon EBS-Snapshot-Informationen anzeigen
- Kopieren Sie einen Amazon EBS-Snapshot
- Teilen Sie einen Amazon EBS-Snapshot mit anderen AWS Konten
- Archivieren von Amazon EBS-Snapshots
- Löschen eines Amazon EBS-Snapshots

Erstellen von Amazon EBS-Snapshots

Sie können einen Amazon EBS-Snapshot eines Amazon EBS-Volumes erstellen, um ein Point-in-Time-Backup dieses Volumes zu erstellen. Sie können entweder Snapshots einzelner Amazon EBS-Volumes erstellen, oder Sie können Snapshots mehrerer Volumes aller oder einer Teilmenge der an eine Amazon EC2-Instance angehängten Volumes erstellen.

Die Snapshot-Erstellung erfolgt asynchron. Der Snapshot wird sofort erstellt, er bleibt jedoch so lange `pending` erhalten, bis alle Daten an Amazon S3 übertragen wurden. Dieser Vorgang kann je nach Anzahl der geänderten Blöcke auf dem Volume mehrere Stunden in Anspruch nehmen. Sie können das Volume während dieser Zeit weiter verwenden, ohne dass dies Auswirkungen auf den Snapshot hat. Der Snapshot enthält nur die Daten, die zum Zeitpunkt der Anforderung des Snapshots auf das Volume geschrieben wurden. Er enthält keine Daten, die von Anwendungen oder dem Betriebssystem zwischengespeichert wurden.

> **Tip**
>
> Um sicherzustellen, dass die Snapshots konsistent und vollständig sind, empfehlen wir, die Schreibvorgänge auf das Volume anzuhalten, bevor Sie den Snapshot erstellen. Wenn Sie Schreibvorgänge auf das Volume nicht unterbrechen können, empfehlen wir Ihnen, die Bereitstellung des Volumes von der Instance aus aufzuheben, bevor Sie den Snapshot erstellen. Sie können die Schreibvorgänge erneut bereitstellen und fortsetzen, sobald der Snapshot den Status erreicht hat. `pending`
>
> Wenn Sie einen Snapshot eines Volumes erstellen, das als Root-Gerät für eine Amazon EC2-Instance dient, empfehlen wir Ihnen, die Instance anzuhalten, bevor Sie den Snapshot erstellen.

Inhalt

- Snapshot-Verschlüsselung
- Snapshot-Ziele
- Automatisierung von Snapshots
- Überlegungen zum Erstellen von Snapshots
- Erstellen Sie einen Snapshot eines EBS-Volumes
- Erstellen Sie EBS-Snapshots mit mehreren Volumes aus einer EC2-Instance

Snapshot-Verschlüsselung

Ein Snapshot erhält automatisch denselben Verschlüsselungsstatus wie das Volume, aus dem er erstellt wurde. Snapshots, die aus unverschlüsselten Volumes erstellt wurden, sind nicht verschlüsselt. Snapshots, die aus verschlüsselten Volumes erstellt wurden, werden automatisch mit demselben KMS-Schlüssel wie das Volume verschlüsselt.

> **Tip**
>
> Wenn Sie einen verschlüsselten Snapshot von einem unverschlüsselten Volume erstellen müssen, erstellen Sie zuerst den unverschlüsselten Snapshot des Volumes und dann eine verschlüsselte Kopie dieses Snapshots.

Snapshot-Ziele

Der Standort der Quellressource (Volume oder Instance) bestimmt, wo Sie Snapshots erstellen können.

- Wenn sich die Quellressource in einer Region befindet, müssen Sie Snapshots in derselben Region wie die Quellressource erstellen.
- Wenn sich die Quellressource in einer lokalen Zone befindet, können Sie Snapshots in derselben lokalen Zone oder in der übergeordneten Region erstellen. Weitere Informationen finden Sie unter Lokale Schnappschüsse in lokalen Zonen.
- Wenn sich die Quellressource in einer befindetOutpost, können Sie Snapshots in derselben Outpost oder in der übergeordneten Region erstellen. Weitere Informationen finden Sie unter Lokale Amazon-EBS-Snapshots auf Outposts.

Automatisierung von Snapshots

Sie können die Erstellung von Snapshots mit Amazon Data Lifecycle Manager und AWS Backup automatisieren.

Überlegungen zum Erstellen von Snapshots

- Wir empfehlen, keine Snapshots von Volumes zu erstellen, die an Amazon EC2-Instances angehängt sind, die sich im Ruhezustand befinden oder für die der Ruhezustand aktiviert ist. Weitere Informationen finden Sie unter So funktioniert der Ruhezustand von Amazon EC2-Instances.
- Sie können zwar einen Snapshot eines Volumes erstellen, während sich ein früherer Snapshot dieses Volumes im `pending` Status befindet, aber wenn mehrere Snapshots für dasselbe Volume im `pending` Status sind, kann dies zu einer verringerten Volume-Leistung führen, bis die Snapshots abgeschlossen sind.

- Die Anzahl der Snapshots, die Sie im `pending` Status haben können, und die Anzahl der gleichzeitigen Snapshots, die Sie pro Volume-Typ anfordern können, ist begrenzt. Weitere Informationen finden Sie unter Kontingente für Amazon EBS. Wenn Sie eines dieser Kontingente überschreiten, warten Sie, bis die aktuellen Snapshots abgeschlossen sind, und versuchen Sie es dann erneut.

Erstellen Sie einen Snapshot eines EBS-Volumes

Sie können einen einzelnen Snapshot eines einzelnen Volumes erstellen. Verwenden Sie alternativ Amazon Data Lifecycle Manager oder, um die Snapshot-Erstellung zu automatisieren AWS Backup. Verwenden Sie Snapshots mehrerer Volumes, um Snapshots aller Volumes für eine EC2-Instance zu erstellen.

Console

So erstellen Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Snapshots, Snapshot erstellen.
3. Wählen Sie für Resource type (Ressourcentyp) die Option Volume aus.
4. Wählen Sie für Volume-ID das Volume aus, von dem der Snapshot erstellt werden soll. Das Feld Verschlüsselung gibt den Verschlüsselungsstatus des Volumes und des resultierenden Snapshots an. Es kann nicht geändert werden.
5. (Optional) Geben Sie unter Beschreibung eine kurze Beschreibung für den Snapshot ein.
6. Wenn sich das Volume in einer Outpost oder in einer lokalen Zone befindet, wird das Snapshot-Zielfeld angezeigt. Führen Sie eine der folgenden Aktionen aus:
   - Wenn sich das Volume in einer lokalen Zone befindet, wählen Sie Lokale Zone, um den Snapshot in derselben lokalen Zone zu erstellen, oder wählen Sie AWS Region, um den Snapshot in der übergeordneten Region der lokalen Zone zu erstellen.
   - Wenn sich das Volume auf einer befindetOutpost, wählen Sie AWS Outpost, um den Snapshot auf derselben zu erstellenOutpost, oder wählen Sie AWS Region, um den Snapshot in der übergeordneten Region von zu erstellenOutpost.

> **Note**
>
> Wenn sich das Volume in einer Region befindet, wird das Snapshot-Ziel nicht angezeigt. Der Snapshot wird automatisch in derselben Region wie das Volume erstellt.

7. (Optional) Um dem Snapshot benutzerdefinierte Tags zuzuweisen, wählen Sie im Abschnitt „Tags“ die Option „Tag hinzufügen“ aus und geben Sie dann das Schlüssel-Wert-Paar ein. Sie können bis zu 50 Tags hinzufügen.
8. Wählen Sie Snapshot erstellen aus.

AWS CLI

So erstellen Sie einen Snapshot

Verwenden Sie den Befehl create-snapshot .

```
aws ec2 create-snapshot  \
    --volume-id vol-01234567890abcdef \
    --description "Snapshot of the root volume for i-1234567890abcdef0"
```

PowerShell

So erstellen Sie einen Snapshot

Verwenden Sie das cmdlet New-EC2Snapshot.

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "Snapshot of the root volume for i-1234567890abcdef0"
```

Erstellen Sie EBS-Snapshots mit mehreren Volumes aus einer EC2-Instance

Wenn Sie Snapshots mit mehreren Volumes aus einer Amazon EC2-Instance erstellen, erstellt Amazon EBS standardmäßig Snapshots aller Amazon EBS-Volumes, die an die Instance angehängt sind. Sie können jedoch wählen, ob Sie das Root-Volume oder bei Bedarf bestimmte Datenvolumes ausschließen möchten.

> **Tip**
>
> Wir empfehlen, dass Sie Ihre Snapshots mit mehreren Volumes taggen, damit Sie sie leicht identifizieren und gemeinsam verwalten können. Sie können auch die Tags von den Quell-Volumes in die entsprechenden Snapshots kopieren, um die Snapshot-Metadaten wie Zugriffsrichtlinien, Anhangsinformationen und Kostenzuweisung an das Quell-Volume anzupassen.

Überlegungen für Snapshots mit mehreren Volumes

- Wenn alle Snapshots erfolgreich abgeschlossen wurden, `succeeded` wird ein `createSnapshots` CloudWatch Ereignis mit dem Ergebnis von an Ihr Konto gesendet. AWS Wenn ein Snapshot im Snapshot-Set mit mehreren Volumes ausfällt, wechseln alle anderen Snapshots in den `error` Status und ein `createSnapshots` CloudWatch Ereignis mit dem Ergebnis von `failed` wird an Ihr Konto gesendet. Weitere Informationen finden Sie unter Snapshots erstellen (createSnapshots).
- Multi-volume Snapshots unterstützen bis zu 128 Amazon EBS-Volumes, die an eine Instance angehängt sind, einschließlich des Root-Volumes und bis zu 127 Datenvolumes.
- Jeder Snapshot im Snapshot-Set mit mehreren Volumes ist ein einzelner Snapshot, der auf dieselbe Weise wie ein einzelner Snapshot verwendet werden kann und dieselben Funktionen unterstützt.
- Sie können mithilfe von Befehlsdokumenten anwendungskonsistente Snapshots aller Amazon EBS-Volumes erstellen, die an eine Amazon EC2-Windows-Instance angehängt sind. AWS Systems Manager

Console

Um Snapshots mit mehreren Volumes zu erstellen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Snapshots, Snapshot erstellen.
3. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.
4. (Optional) Geben Sie unter Beschreibung eine kurze Beschreibung für die Snapshots ein. Diese Beschreibung wird auf alle Snapshots angewendet.
5. Wenn sich die Instance in einer Outpost oder in einer lokalen Zone befindet, wird das Snapshot-Zielfeld angezeigt. Führen Sie eine der folgenden Aktionen aus:

- Wenn sich die Instanz in einer lokalen Zone befindet, wählen Sie Local Zone, um die Snapshots in derselben lokalen Zone zu erstellen, oder wählen Sie AWS Region, um die Snapshots in der übergeordneten Region der lokalen Zone zu erstellen.
- Wenn sich die Instanz auf einer befindetOutpost, wählen Sie AWS Outpost, um die Snapshots auf derselben zu erstellenOutpost, oder wählen Sie AWS Region, um die Snapshots in der übergeordneten Region von zu erstellen. Outpost

> **Note**
>
> Wenn sich die Instanz in einer Region befindet, wird das Snapshot-Ziel nicht angezeigt. Der Snapshot wird automatisch in derselben Region wie die Instanz erstellt.

6. (Optional) Um das Root-Volume der Instanz auszuschließen, wählen Sie Root-Volume ausschließen aus.
7. (Optional) Um Datenvolumen auszuschließen, wählen Sie Bestimmte Datenvolumes ausschließen aus. Der Abschnitt Attached data volumes (Zugeordnete Data-Volumes) listet alle Data-Volumes auf, die derzeit an die ausgewählte Instance angefügt sind.

   Wählen Sie die auszuschließenden Datenmengen aus. Nur Volumes, die nicht ausgewählt werden, werden in den Multi-Volume-Snapshot-Set aufgenommen.
8. (Optional) Um Tags automatisch von den Quell-Volumes auf die entsprechenden Snapshots zu kopieren, wählen Sie unter Tags vom Quell-Volume kopieren die Option Tags kopieren aus.
9. (Optional) Um den Snapshots zusätzliche benutzerdefinierte Tags zuzuweisen, wählen Sie im Abschnitt „Tags“ die Option „Tag hinzufügen“ aus und geben Sie dann das Schlüssel-Wert-Paar ein. Sie können bis zu 50 Tags hinzufügen.
10. Wählen Sie Snapshot erstellen aus.

AWS CLI

Um Schnappschüsse mit mehreren Volumes zu erstellen

Verwenden Sie den Befehl create-snapshots.

```
aws ec2 create-snapshots \
```

```
    --instance-specification InstanceId=i-1234567890abcdef0 \
    --description "from a multi-volume snapshot of i-1234567890abcdef0"
```

Um das Root-Volume auszuschließen, fügen Sie der Option Folgendes hinzu. `--instance-specification`

```
ExcludeBootVolume=true
```

Um ein Datenvolume auszuschließen, fügen Sie der `--instance-specification` Option Folgendes hinzu.

```
ExcludeDataVolumeIds=vol-01234567890abcdef
```

PowerShell

Um Snapshots mit mehreren Volumes zu erstellen

Verwenden Sie das cmdlet New-EC2SnapshotBatch.

```
New-EC2SnapshotBatch `
    -InstanceSpecification_InstanceId i-1234567890abcdef0 `
    -Description "from a multi-volume snapshot of i-1234567890abcdef0"
```

Um das Root-Volume auszuschließen, fügen Sie den folgenden Parameter hinzu.

```
-InstanceSpecification_ExcludeBootVolume $true
```

Um Datenvolumen auszuschließen, fügen Sie den folgenden Parameter hinzu.

```
-InstanceSpecification_ExcludeDataVolumes "vol-01234567890abcdef"
```

Amazon EBS-Snapshot-Informationen anzeigen

Sie können detaillierte Informationen zu Ihren Snapshots anzeigen.

Console

So zeigen Sie Snapshot-Informationen an

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Um nur Snapshots anzuzeigen, die Ihnen gehören, wählen Sie in der oberen linken Ecke des Bildschirms Eigentum von mir. Sie können die Snapshot-Liste auch mithilfe von Tags und anderen Snapshot-Attributen filtern. Wählen Sie im Feld Filter das Attributfeld aus und wählen Sie dann den Attributwert aus oder geben Sie ihn ein. Um beispielsweise nur verschlüsselte Snapshots anzuzeigen, wählen Sie Verschlüsselung aus und geben dann `true` ein.
4. Wenn Sie weitere Informationen zu einem bestimmten Snapshot sehen möchten, wählen Sie seine ID in der Liste aus.

> **Note**
>
> Das Feld Vollständige Snapshot-Größe zeigt die volle Größe des Snapshots in Byte an. Dies ist nicht die inkrementelle Größe des Snapshots. Stattdessen stellt es die Größe aller Blöcke dar, die zum Zeitpunkt der Erstellung des Snapshots auf das Quell-Volume geschrieben wurden.
> Das Feld Volume Size zeigt die Größe des EBS-Volumes an, das aus dem Snapshot erstellt wird, sofern keine andere Größe angegeben ist.

AWS CLI

Um Snapshot-Informationen anzuzeigen

Verwenden Sie den Befehl describe-snapshots.

Example Beispiel 1: Filtern anhand von Tags (Markierungen)

Das folgende Beispiel beschreibt die Snapshots mit dem Tag stack=PRODUCTION.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example Beispiel 2: Filtern anhand des Volumes

Das folgende Beispiel beschreibt die Snapshots, die auf dem angegebenen Volume erstellt wurden.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example Beispiel 3: Filtern anhand des Snapshot-Alters

Sie können JMESPath verwenden, um Ergebnisse mithilfe von Ausdrücken zu filtern. Mit dem folgenden Befehl werden beispielsweise die IDs aller Snapshots angezeigt, die von Ihrem Konto vor dem angegebenen Datum erstellt wurden. Wenn Sie den Eigentümer nicht angeben, enthalten die Ergebnisse alle öffentlichen Snapshots.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

Der folgende Befehl zeigt die IDs aller Snapshots an, die im angegebenen Datumsbereich erstellt wurden.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
    --output text
```

PowerShell

Um Snapshot-Informationen anzuzeigen

Verwenden Sie das cmdlet Get-EC2Snapshot.

Beispiel 1: Beschreiben Sie einen Snapshot

Das folgende -Beispiel beschreibt den angegebenen Snapshot.

```
Get-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

Beispiel 2: Filtern anhand des Volumes

Das folgende Beispiel beschreibt die Snapshots, die auf dem angegebenen Volume erstellt wurden.

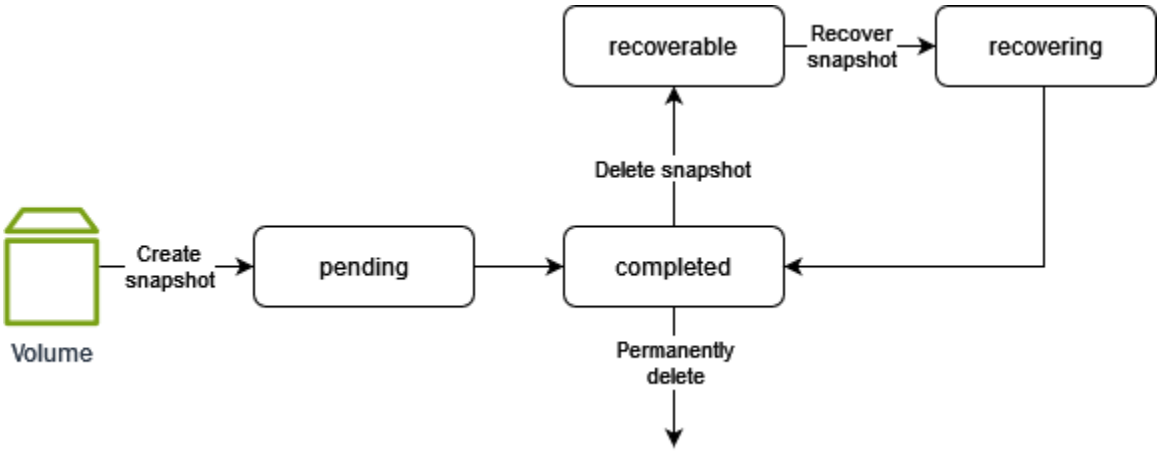
```
Get-EC2Snapshot`
```

```
    -Filter @{Name="volume-id"; Values="vol-01234567890abcdef"}
```

Snapshot-Status

Ein Amazon EBS-Snapshot durchläuft vom Moment seiner Erstellung bis zu seiner endgültigen Löschung verschiedene Status.

Die folgende Abbildung zeigt die Übergänge zwischen den Snapshot-Zuständen. Wenn Sie einen Snapshot erstellen, wechselt er in den `pending` Status. Nachdem der Snapshot einsatzbereit ist, wechselt er in den `completed` Status. Wenn Sie entschieden haben, dass Sie einen Snapshot nicht mehr benötigen, können Sie ihn löschen. Wenn Sie einen Snapshot löschen, der einer Aufbewahrungsregel für den Papierkorb entspricht, wird er im Papierkorb aufbewahrt und wechselt in den `recoverable` Status. Wenn Sie einen Snapshot aus dem Papierkorb wiederherstellen, wechselt er in den `recovering` Status und dann in den Status. `completed` Andernfalls wird er dauerhaft gelöscht.



In der folgenden Tabelle sind die Snapshot-Status zusammengefasst.

Status	Description
`pending`	Der Snapshot-Erstellungsprozess ist noch nicht abgeschlossen. Ein Snapshot kann nicht verwendet werden, solange er sich im `pending` Status befindet.
`completed`	Der Snapshot-Erstellungsvorgang ist abgeschlossen und der Snapshot ist einsatzbereit.

Status	Description
`recoverable`	Der Snapshot befindet sich derzeit im Papierkorb. Um den Snapshot verwenden zu können, müssen Sie ihn zuerst aus dem Papierkorb wiederherstellen.
`recovering`	Der Snapshot wird gerade aus dem Papierkorb wiederhergestellt. Nachdem der Snapshot wiederhergestellt wurde, wechselt er in den `completed` Status und ist einsatzbereit.
`error`	Der Snapshot-Erstellungsvorgang ist fehlgeschlagen. Ein Snapshot kann nicht verwendet werden, wenn er sich im `error` Status befindet.

Kopieren Sie einen Amazon EBS-Snapshot

Nachdem Sie einen Snapshot erstellt haben und dieser den `completed` Status erreicht hat, können Sie eine Kopie davon erstellen. Die Snapshot-Kopie ist eine exakte Kopie des Originals, hat jedoch eine eindeutige Ressourcen-ID. Sie können Schnappschüsse, deren Eigentümer Sie sind, und Schnappschüsse, die mit Ihnen geteilt wurden, privat oder öffentlich kopieren. Für die folgenden Anwendungsfälle müssen Sie möglicherweise einen Snapshot kopieren:

- Geografische Erweiterung — Sie müssen Ihre Anwendungen in einer neuen Region starten.
- Migration — Sie müssen eine Anwendung an ein neues Ziel verschieben, um eine bessere Verfügbarkeit zu gewährleisten oder die Kosten zu minimieren.
- Notfallwiederherstellung — Aus Gründen der Datenredundanz müssen Sie Ihre Daten und Protokolle in sekundären Regionen sichern.
- Verschlüsselung — Sie müssen einen zuvor unverschlüsselten Snapshot verschlüsseln oder einen verschlüsselten Snapshot mit einem anderen KMS-Schlüssel erneut verschlüsseln.
- Einen geteilten Snapshot kopieren — Sie müssen einen Snapshot kopieren, der mit Ihnen geteilt wird.
- Anforderungen an die Aufbewahrung und Prüfung von Daten — Sie müssen verschlüsselte Snapshots von einem AWS Konto auf ein anderes kopieren, um Daten für Prüfungen oder

Datenaufbewahrungszwecke aufzubewahren. Wenn Sie ein anderes Konto verwenden, sind Sie geschützt, falls Ihr AWS Hauptkonto gefährdet ist.

Um Snapshots mehrerer Volumes zu kopieren, identifizieren Sie alle Snapshots, die Teil dieses Sets sind, anhand der Tags, die Sie bei der Erstellung zugewiesen haben, und kopieren Sie sie dann einzeln.

Weitere Informationen zum Kopieren von Amazon RDS-Snapshots erhalten Sie unter Kopieren eines DB-Snapshots im Amazon RDS-Benutzerhandbuch.

Preisgestaltung

Preisinformationen zum Kopieren von Snapshots finden Sie unter Amazon EBS-Preise.

Inhalt

- Überlegungen zum Kopieren von Snapshots
- Ziele für Snapshot-Kopien
- Inkrementelles Kopieren von Snapshots
- Time-based Kopien für Amazon EBS-Snapshots und AMIs EBS-backed
- Verschlüsselung und Kopieren von Snapshots
- Kopieren eines -Snapshots

Überlegungen zum Kopieren von Snapshots

- Sie können VM AWS Marketplace Import/Export - und Storage Gateway-Snapshots kopieren, aber Sie müssen sicherstellen, dass der Snapshot in der Zielregion unterstützt wird.
- Es gibt ein Limit an `20` gleichzeitigen Snapshot-Kopieranforderungen pro Ziel. Wenn Sie diese Quote überschreiten, erhalten Sie einen `ResourceLimitExceeded`-Fehler. Wenn dieser Fehler angezeigt wird, warten Sie, bis eine oder mehrere der Kopieranfragen abgeschlossen sind, bevor Sie eine neue Snapshot-Kopieranforderung stellen.
- User-defined Tags werden nicht vom Quell-Snapshot in die Snapshot-Kopie kopiert. Sie können während oder nach dem Kopiervorgang benutzerdefinierte Tags (Markierungen) hinzufügen.
- Snapshots, die durch einen Snapshot-Kopiervorgang erstellt werden, haben eine zufällige Volume-ID, wie z. B. `vol-ffff` oder `vol-ffffffff`. Diese zufälligen Volume-IDs sollten nicht für andere Zwecke verwendet werden.

- Resource-level Die für den Snapshot-Kopiervorgang angegebenen Berechtigungen können für die Snapshot-Kopie und den Quell-Snapshot gelten. Ein Beispiel finden Sie unter Beispiel: Kopieren von Snapshots.
- Wenn Sie einen Snapshot kopieren, der für die schnelle Snapshot-Wiederherstellung aktiviert ist, wird die Snapshot-Kopie nicht automatisch für die schnelle Snapshot-Wiederherstellung aktiviert. Sie müssen die schnelle Snapshot-Wiederherstellung für die Snapshot-Kopie explizit aktivieren.
- Wenn Sie einen Snapshot kopieren und mit einem neuen KMS-Schlüssel verschlüsseln, wird eine vollständige (nicht inkrementelle) Kopie erstellt. Dies führt zu zusätzlichen Lagerkosten.
- Wenn Sie einen Snapshot in eine neue Region kopieren, wird eine vollständige (nicht inkrementelle) Kopie erstellt. Dies führt zu zusätzlichen Lagerkosten.
- Wenn Sie externe oder regionsübergreifende Datenübertragungen verwenden, fallen zusätzliche https://aws.amazon.com/ebs/pricing/ EC2-Datenübertragungsgebühren an. Wenn Sie nach der Initiierung Snapshots löschen, werden Ihnen weiterhin die bereits übertragenen Daten in Rechnung gestellt.

Ziele für Snapshot-Kopien

Der Speicherort des Quell-Snapshots bestimmt, ob Sie ihn kopieren können oder nicht.

- Wenn sich der Quell-Snapshot in einer Region befindet, können Sie ihn innerhalb dieser Region, in eine andere Region, in eine dieser Region Outpost zugeordnete Region oder in eine lokale Zone in dieser Region kopieren.
- Wenn sich der Quell-Snapshot in einer lokalen Zone befindet, können Sie ihn innerhalb derselben lokalen Zone, in eine andere lokale Zone in derselben Zonengruppe oder in die übergeordnete Region dieser lokalen Zone kopieren.
- Wenn sich der Quell-Snapshot auf einem befindetOutpost, können Sie ihn nicht kopieren.

Inkrementelles Kopieren von Snapshots

Snapshot-Kopiervorgänge innerhalb desselben Kontos und derselben Region, die denselben KMS-Schlüssel verwenden, sind immer inkrementelle Kopien. Wenn Sie die Snapshot-Kopie jedoch mit einem anderen KMS-Schlüssel verschlüsseln, handelt es sich bei der Kopie um eine vollständige Kopie.

Wenn Sie einen Snapshot über Regionen oder Konten hinweg kopieren, handelt es sich bei der Kopie um eine inkrementelle Kopie, wenn die folgenden Bedingungen erfüllt sind:

- Der Snapshot wurde zuvor in die Zielregion oder das Konto kopiert.
- Die aktuelle Snapshot-Kopie ist in der Zielregion oder im Konto noch vorhanden.
- Die neueste Snapshot-Kopie wurde nicht archiviert.
- Alle Kopien des Snapshots in der Zielregion oder im Konto sind entweder unverschlüsselt oder wurden mit demselben KMS-Schlüssel verschlüsselt.

> **Tip**
>
> Wir empfehlen, Ihre Snapshot-Kopien mit der Volume-ID und der Erstellungszeit zu taggen, damit Sie den Überblick über die neueste Snapshot-Kopie eines Volumes in der Zielregion oder im Zielkonto behalten können.

Um festzustellen, ob Ihre Snapshot-Kopien inkrementell sind, überprüfen Sie das CopySnapshot-Ereignis CloudWatch .

Time-based Kopien für Amazon EBS-Snapshots und AMIs EBS-backed

Time-based Kopien können Ihnen dabei helfen, Compliance- oder Geschäftsanforderungen für die Datenreplikation zu erfüllen, indem sie sicherstellen, dass Ihre EBS-Snapshots und EBS-backed AMIs innerhalb und zwischen AWS Regionen innerhalb eines bestimmten Zeitrahmens kopiert werden. Time-based Kopien können Backup-Administratoren auch dabei helfen, strenge Disaster Recovery-Anforderungen (Recovery Point Objectives und Recovery Time Objectives) zu erfüllen. Außerdem verbessern sie die Agilität bei der Entwicklung, da vorhersehbare Kopierzeiten für Snapshots und AMIs gewährleistet werden. EBS-backed

Bei zeitbasierten Snapshot- und EBS-backed AMI-Kopiervorgängen geben Sie eine Abschlussdauer zwischen 15 Minuten und 48 Stunden an, in der die Kopie abgeschlossen sein soll. Die Abschlussdauer muss in Schritten von 15 Minuten angegeben werden.

Themen

- Kontingente
- Legen Sie Ihre Abschlussdauer fest
- Überlegungen
- Überwachen
- Preise und Fakturierung

Kontingente

Die folgenden Kontingente gelten für zeitbasierte Snapshot- und EBS-backed AMI-Kopiervorgänge:

Kontingent	Description	Kontingentwert	Einstellbar
Durchsatzquote für Snapshot-Kopiervorgänge	Der maximale Durchsatz, der durch einen einzelnen zeitbasierten Snapshot-Kopiervorgang erreicht werden kann. **Note** Bei AMI-Kopiervorgängen gilt das Kontingent für jeden einzelnen Snapshot, der dem AMI zugeordnet ist.	500 MiB/s	Nein
Kontingent für den kumulativen Kopierdurchsatz von	Der maximale kumulative Durchsatz, der durch gleichzeitige zeitbasierte Snapshot-Kopiervorgänge zwischen einer Quell- und einer Zielregion erreicht werden kann.	2.000 MiB/s	Ja

Kontingent	Description	Kontingentwert	Einstellbar
	Note Bei AMI-Kopierv orgänge n wird jeder einzelne Snapshot, der dem AMI zugeordnet ist, auf das Kontingent angerechnet.		

Wenn Sie einen zeitbasierten Snapshot-Kopiervorgang starten, geben Sie eine Abschlussdauer an. Der von der Anforderung verwendete Durchsatz wird durch die Größe der Snapshot-Daten und die angeforderte Abschlussdauer bestimmt. Wenn Sie beispielsweise einen Snapshot mit 225.000 MiB (0,214 TiB) an Daten kopieren und eine Abschlussdauer von 15 Minuten anfordern, beträgt der Durchsatz 250 MiB/s (225.000 MiB ÷ 15 Minuten = 250). MiB/s

Wenn Sie einen zeitbasierten AMI-Kopiervorgang starten, gilt die von Ihnen angegebene Abschlussdauer für jeden Snapshot, der dem AMI zugeordnet ist. Da jeder Snapshot eine andere Größe haben kann, wird jeder Snapshot mit einem anderen Durchsatz kopiert, um sicherzustellen, dass alle Snapshots innerhalb der Abschlussdauer kopiert werden. Angenommen, Sie haben ein AMI mit den folgenden zugehörigen Snapshots:

- Snapshot 1:200.000 MiB
- Schnappschuss 2:500.000 MiB
- Schnappschuss 3:450.000 MiB

Wenn Sie eine zeitbasierte Kopie für dieses AMI initiieren und eine Abschlussdauer von 60 Minuten angeben, verwendet die Anforderung den folgenden Durchsatz:

- Snapshot 1:55,56 MiB/s (200.000 MiB ÷ 60 Minuten = 55,56) MiB/s
- Schnappschuss 2:138,89 MiB/s (500.000 MiB ÷ 60 Minuten = 138,89) MiB/s

- Schnappschuss 3:125 MiB/s (450.000 MiB ÷ 60 Minuten = 125) MiB/s

Das bedeutet, dass die Anforderung 319,45 MiB/s Ihres kumulativen Snapshot-Kopierdurchsatzes verbraucht, um sicherzustellen, dass der Kopiervorgang in 60 Minuten abgeschlossen ist.

Wenn Sie eine zeitbasierte Snapshot- oder EBS-backed AMI-Kopieranforderung initiieren und Ihr verfügbares kumulatives Snapshot-Kopierdurchsatzkontingent wie folgt lautet:

- größer oder gleich der erforderlichen Durchsatzrate, wird die Kopie innerhalb der angeforderten Abschlussdauer abgeschlossen.
- weniger als die erforderliche Durchsatzrate, aber größer als Null, die Anfrage ist erfolgreich, aber es dauert länger als von Ihnen angefordert. Der Kopiervorgang wird mit Ihrem verfügbaren Durchsatzkontingent abgeschlossen.
- Null (Kontingent erreicht), die Anfrage schlägt fehl.

Legen Sie Ihre Abschlussdauer fest

Die Mindestdauer, die Sie für einen zeitbasierten Snapshot- oder EBS-backed AMI-Kopiervorgang anfordern können, beträgt 15 Minuten, und die maximale Abschlussdauer, die Sie anfordern können, beträgt 48 Stunden. Die Abschlussdauer muss in Schritten von 15 Minuten angegeben werden.

Gleichzeitige zeitbasierte Snapshot-Kopiervorgänge

Sie können zeitbasierte Snapshot-Kopiervorgänge gleichzeitig zwischen derselben Quell- und Zielregion ausführen, sofern der kombinierte Durchsatz aller gleichzeitigen Vorgänge innerhalb Ihres kumulativen Snapshot-Kopierdurchsatzkontingents liegt (standardmäßig 2.000). MiB/s

Um zu ermitteln, ob Sie die erforderliche Abschlussdauer für Ihre vorhandenen Snapshots erreichen können, teilen Sie die Gesamtgröße aller Snapshots durch die erforderliche Abschlussdauer, um die erforderliche Durchsatzrate zu ermitteln.

> **Tip**
>
> Wenn Sie die genaue Größe der Daten in Ihren Snapshots nicht kennen, können Sie stattdessen die gesamte Snapshot-Größe als Proxy verwenden. Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-snapshots.html AWS CLI describe-snapshots, um die volle Snapshot-Größe abzurufen.

```
required throughput rate = combined snapshot size ÷ required completion duration
```

Wenn die erforderliche Durchsatzrate unter Ihrem kumulativen Snapshot-Kopierdurchsatzkontingent liegt, können Sie die erforderliche Abschlussdauer erreichen. Wenn die erforderliche Durchsatzrate höher ist als Ihr kumulatives Durchsatzkontingent für Snapshot-Kopien, empfehlen wir Ihnen, eine Kontingenterhöhung anzufordern, die mindestens 10% über Ihrer erforderlichen Durchsatzrate liegt.

> **Tip**
>
> Die Amazon EC2-Konsole bietet einen Rechner, mit dem Sie überprüfen können, wie viele Snapshot-Daten Sie in einem bestimmten Zeitraum zwischen zwei Regionen kopiert haben, und die erreichbare Mindestdauer für die Fertigstellung, die Sie für diese Datenmenge erreichen können, basierend auf einem bestimmten kumulativen Snapshot-Kopierdurchsatzkontingent. Der Rechner verwendet die `SnapshotCopyBytesTransferred` CloudWatch Metrik, um Daten zu berechnen, die über einen Zeitraum zwischen zwei Regionen kopiert wurden. Um den Rechner zu öffnen, wählen Sie im Navigationsbereich der Amazon EC2-Konsole Snapshots und dann Aktionen , Kopierdauerrechner starten aus.
> Die Berechnung der Snapshot-Kopierdauer wird für Local Zones und AWS Outposts Wavelength Zones nicht unterstützt.

Individuelle zeitbasierte Snapshot-Kopiervorgänge

Sie können die Mindestdauer für den Abschluss eines einzelnen zeitbasierten Snapshot-Kopiervorgangs berechnen, indem Sie die Größe der Snapshot-Daten durch das Durchsatzkontingent des Snapshot-Kopiervorgangs (500 MiB/s) dividieren.

> **Tip**
>
> Wenn Sie die genaue Größe der Daten in Ihren Snapshots nicht kennen, können Sie stattdessen die gesamte Snapshot-Größe als Proxy verwenden. Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-snapshots.html AWS CLI describe-snapshots, um die volle Snapshot-Größe abzurufen.

```
minimum completion duration = Max(15 minutes, (snapshot data size ÷ 500 MiB/s)
```

Beispielsweise beträgt die Mindestdauer für die Fertigstellung eines Snapshots mit 900.000 MiB an Daten 30 Minuten.

```
minimum completion duration = Max(15 minutes, (900,000 MiB ÷ 500 MiB/s)
= Max(15 minutes, 30 minutes)
= 30 minutes
```

Time-based AMI-Kopiervorgänge

Wenn Sie einen zeitbasierten AMI-Kopiervorgang für ein EBS-backed AMI mit einem einzelnen zugehörigen Snapshot initiieren, verhält er sich genauso wie ein einzelner zeitbasierter Snapshot-Kopiervorgang, und es gelten dieselben Durchsatzbeschränkungen.

Wenn Sie einen zeitbasierten AMI-Kopiervorgang für ein EBS-backed AMI mit mehreren zugehörigen Snapshots initiieren, verhält er sich genauso wie gleichzeitige zeitbasierte Snapshot-Kopiervorgänge, und es gelten dieselben Durchsatzbeschränkungen. Jeder zugehörige Snapshot führt zu einer separaten Snapshot-Kopieranforderung, die jeweils zu Ihrem kumulativen Durchsatzkontingent für Snapshot-Kopien beiträgt. Die von Ihnen angegebene Abschlussdauer gilt für jeden zugehörigen Snapshot.

Überlegungen

- Sie können zeitbasierte Snapshot- und EBS-backed AMI-Kopiervorgänge initiieren, wenn Sie Snapshots innerhalb derselben Region kopieren oder wenn Sie Snapshots regionsübergreifend kopieren.
- Wenn Sie zwei zeitbasierte Kopiervorgänge für denselben Snapshot oder dasselbe AMI starten, beginnt die Abschlussdauer des zweiten Kopiervorgangs erst, nachdem der erste Kopiervorgang abgeschlossen ist.
- Time-based Kopiervorgänge und die Berechnung der Snapshot-Kopierdauer werden mit AWS Outposts Local Zones und Wavelength Zones nicht unterstützt.

Überwachen

Sie können den Fortschritt zeitbasierter Snapshot- und EBS-backed AMI-Kopiervorgänge mithilfe der Amazon EC2-Konsole und der überwachen. AWS CLI Wählen Sie in der Konsole den Snapshot aus und überprüfen Sie dann auf der Registerkarte Details das Feld Progress. Untersuchen Sie mit dem AWS CLI das `Progress` Ausgabeelement in der Befehlsantwort „describe-snapshots“.

Sie können überprüfen, ob ein zeitbasierter Snapshot- oder EBS-backed AMI-Kopiervorgang innerhalb der angeforderten Abschlussdauer abgeschlossen wurde, indem Sie den Unterschied zwischen den Zeiten „Gestartet“ und „Abgeschlossen“ in der Konsole oder `StartTime` in der Antwort überprüfen. `CompletionTime` `describe-snapshots`

Sie können das `copySnapshot` EventBridge Amazon-Ereignis auch verwenden, um das Ergebnis zeitbasierter Kopiervorgänge zu überwachen. Das Ereignis gibt an, ob der Vorgang abgeschlossen wurde und ob die angeforderte Abschlussdauer eingehalten wurde. Wenn die Abschlussdauer nicht eingehalten wurde, enthält das Ereignis weitere Informationen zur Ursache. Weitere Informationen finden Sie unter EBS-Snapshot-Ereignisse.

Preise und Fakturierung

> **Note**
>
> Ähnlich wie bei standardmäßigen Snapshot-Kopiervorgängen wird beim Kopieren eines Snapshots in eine neue Region eine vollständige (nicht inkrementelle) Kopie erstellt, was zu zusätzlichen Speicherkosten führt. Nachfolgende Kopien desselben Snapshots sind inkrementell. Wenn Sie externe oder regionsübergreifende Datenübertragungen verwenden, fallen außerdem zusätzliche Amazon EC2-Datenübertragungsgebühren an.

Für zeitbasierte Snapshot- und EBS-backed AMI-Kopiervorgänge fallen zusätzliche Gebühren an. Time-based Kopiervorgänge werden mit einer Rate berechnet, die auf der angeforderten Abschlussdauer pro GiB kopierter Snapshot-Daten basiert. Die festen Tarife lauten wie folgt:

> **Note**
>
> Die Dauer der Fertigstellung muss in Schritten von 15 Minuten angegeben werden. Die Mindestdauer für die Fertigstellung beträgt 15 Minuten und die Höchstdauer 48 Stunden.

- 15 Minuten — 0,020 USD pro GiB an Daten
- 30 Minuten und 45 Minuten — 0,018 USD pro GiB an Daten
- 1 Stunde bis 1 Stunde 45 Minuten — 0,016 USD pro GiB an Daten
- 2 Stunden bis 3 Stunden 45 Minuten — 0,014 USD pro GiB an Daten
- 4 Stunden bis 7 Stunden 45 Minuten — 0,012 USD pro GiB an Daten
- 8 Stunden bis 15 Stunden 45 Minuten — 0,010 USD pro GiB an Daten

- 16 Stunden oder mehr — 0,005 USD pro GiB an Daten

Wenn Sie beispielsweise einen Snapshot mit 3.000 GiB an Daten mit einer Bearbeitungsdauer von 8 Stunden kopieren, werden Ihnen 30$ (0,010$ x 3.000 GiB) in Rechnung gestellt.

Wenn Sie einen zeitbasierten Kopiervorgang initiieren, die angeforderte Abschlussdauer jedoch nicht eingehalten wird, weil Sie ein Kontingent überschritten haben, wird Ihnen die tatsächliche Abschlussdauer und nicht die angeforderte Abschlussdauer in Rechnung gestellt. Wenn Sie beispielsweise eine Bearbeitungsdauer von 1 Stunde anfordern, der Vorgang jedoch in 2 Stunden abgeschlossen ist, wird Ihnen der Tarif für die zweistündige Bearbeitungsdauer in Rechnung gestellt.

Wenn Amazon EBS die angeforderte Abschlussdauer nicht einhalten kann oder wenn eine Anfrage aufgrund von serviceseitigen Problemen storniert wird, werden Ihnen die zusätzlichen Gebühren für den zeitbasierten Snapshot-Kopiervorgang nicht in Rechnung gestellt.

Wenn Sie die Snapshot-Kopie löschen, während der zeitbasierte Snapshot-Kopiervorgang noch läuft, werden Ihnen die bis zu diesem Zeitpunkt kopierten Daten mit der Rate in Rechnung gestellt, die der angegebenen Abschlussdauer entspricht.

Verschlüsselung und Kopieren von Snapshots

> **Note**
>
> Die serverseitige Verschlüsselung von Amazon S3 (256-Bit-AES) schützt die Daten eines Snapshots während der Übertragung bei einem Kopiervorgang.

Sie können eine verschlüsselte Snapshot-Kopie eines unverschlüsselten Quell-Snapshots erstellen. Und Sie können eine Snapshot-Kopie mit einem KMS-Schlüssel verschlüsseln, der sich vom Quell-Snapshot unterscheidet. Das Ändern des Verschlüsselungsstatus einer Snapshot-Kopie während eines Kopiervorgangs kann jedoch zu einer vollständigen (nicht inkrementellen) Kopie führen, was zu höheren Datenübertragungs- und Speicherkosten führen kann.

> **Tip**
>
> Wenn Sie einen verschlüsselten Snapshot verwenden, der für Sie freigegeben ist, empfehlen wir, den Snapshot erneut zu verschlüsseln, indem Sie ihn kopieren und einen KMS-Schlüssel verwenden, den Sie besitzen. Dies schützt Sie, falls der ursprüngliche KMS-Schlüssel kompromittiert wird oder wenn der Besitzer Ihren Zugriff widerruft, was dazu führen könnte,

dass Sie den Zugriff auf den Snapshot und alle verschlüsselten Volumes, die Sie daraus erstellt haben, verlieren.

Berechtigungen für das Kopieren verschlüsselter Schnappschüsse

Um einen verschlüsselten Snapshot zu kopieren, muss Ihr Benutzer über die folgenden Berechtigungen verfügen, um die Amazon-EBS-Verschlüsselung verwenden zu können.

- • `kms:DescribeKey`
  - `kms:CreateGrant`
  - `kms:GenerateDataKey`
  - `kms:GenerateDataKeyWithoutPlaintext`
  - `kms:ReEncrypt`
  - `kms:Decrypt`
- Um einen verschlüsselten Snapshot zu kopieren, der von einem anderen AWS Konto aus geteilt wird, müssen Sie über die Berechtigungen verfügen, den vom Kunden verwalteten Schlüssel zu verwenden, der zum Verschlüsseln des Snapshots verwendet wurde. Weitere Informationen finden Sie unter Teilen Sie den KMS-Schlüssel, der zum Verschlüsseln eines gemeinsam genutzten Amazon EBS-Snapshots verwendet wird.

Verschlüsselungsergebnisse für Snapshot-Kopien

In der folgenden Tabelle werden die Verschlüsselungsergebnisse beschrieben, wenn Sie Snapshots kopieren, deren Eigentümer Sie sind, und Snapshots, die mit Ihnen geteilt werden.

Standardverschlüsselung für die Zielregion	Quell-Snapshot	Ergebnis der Verschlüsselung der Snapshot-Kopie	Hinweis
Disabled	Unverschlüsselt	Optionale Verschlüsselung	Wenn Sie die Kopie verschlüsseln, können Sie den zu verwendenden KMS-Schlüssel angeben. Wenn Sie die Kopie verschlüsseln, aber keinen KMS-Schlüssel angeben, wird

Standardverschlüsselung für die Zielregion	Quell-Snapshot	Ergebnis der Verschlüsselung der Snapshot-Kopie	Hinweis
			standardmäßig der für die Verschlüsselung angegebene Schlüssel verwendet.
Disabled	Verschlüsselt	Automatisch verschlüsselt	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird das Von AWS verwalteter Schlüssel (`aws/ebs`) verwendet.
Aktiviert	Unverschlüsselt	Automatisch verschlüsselt	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird der standardmäßig für die Verschlüsselung angegebene Schlüssel verwendet.
Aktiviert	Verschlüsselt	Automatisch verschlüsselt	Sie können den zu verwendenden KMS-Schlüssel angeben. Wenn Sie keinen KMS-Schlüssel angeben, wird der standardmäßig für die Verschlüsselung angegebene Schlüssel verwendet.

Kopieren eines -Snapshots

Sie können Schnappschüsse von einer Region in eine andere kopieren. Sie können einen unverschlüsselten Snapshot in einen verschlüsselten Snapshot kopieren. Wenn Sie jedoch versuchen, einen verschlüsselten Snapshot zu kopieren, ohne über die Berechtigungen zur Verwendung des Verschlüsselungsschlüssels zu verfügen, schlägt der Vorgang im Hintergrund fehl und die Snapshot-Kopie erhält die Statusmeldung „Auf die angegebene Schlüssel-ID kann nicht zugegriffen werden“.

Console

So kopieren Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den zu kopierenden Snapshot aus und wählen Sie dann Aktionen, Snapshot kopieren.
4. Geben Sie für Beschreibung eine kurze Beschreibung für die Snapshot-Kopie ein.

   Standardmäßig enthält die Beschreibung Informationen zum Quell-Snapshot, damit Sie eine Kopie vom Original unterscheiden können.
5. Geben Sie das Ziel für die Snapshot-Kopie an.

   - Um den Snapshot in dieselbe Region oder in eine andere Region zu kopieren, wählen Sie AWS Region und dann die Zielregion aus.
   - Um den Snapshot in eine lokale Zone zu kopieren, wählen Sie AWS Lokale Zone und dann die lokale Zielzone aus.
   - (nur für Outpost Kunden) Um den Snapshot in eine zu kopierenOutpost, wählen Sie den ARN des Ziels aus AWS Outpost und geben Sie ihn einOutpost.
6. Wenn die Snapshot-Kopie innerhalb eines bestimmten Zeitrahmens abgeschlossen werden muss, wählen Sie Zeitbasierte Kopie aktivieren aus. Geben Sie für die Abschlussdauer die erforderliche Abschlussdauer in Schritten von 15 Minuten ein. Weitere Informationen finden Sie unter Time-based Kopien für Amazon EBS-Snapshots und AMIs EBS-backed.

   Wenn Sie nicht möchten, dass die Snapshot-Kopie in einem bestimmten Zeitraum abgeschlossen wird, aktivieren Sie das zeitbasierte Kopieren nicht. In diesem Fall wird die Snapshot-Kopie nach bestem Bemühen abgeschlossen.
7. (nur für Outpost Kunden) Um die Snapshot-Kopie auf einem Outpost in der ausgewählten Region zu erstellen, wählen Sie als Snapshot-Ziel aus AWS Outpost, und geben Sie dann für Outpost Ziel-ARN den ARN des ein, in den Outpost der Snapshot kopiert werden soll. Das Snapshot-Zielfeld wird nur angezeigt, wenn Sie einen Snapshot-Zielort haben und sich Outpost in der ausgewählten Region befinden.
8. Geben Sie den Verschlüsselungsstatus für die Snapshot-Kopie an.

   Wenn der Quell-Snapshot verschlüsselt ist oder Ihr Konto standardmäßig für die Verschlüsselung aktiviert ist, wird die Snapshot-Kopie automatisch verschlüsselt.

Wenn der Quell-Snapshot unverschlüsselt ist und Ihr Konto standardmäßig nicht für die Verschlüsselung aktiviert ist, ist die Verschlüsselung optional.

9. Wählen Sie Snapshot kopieren aus.

AWS CLI

Um einen Snapshot in eine andere Region zu kopieren

Verwenden Sie den Befehl copy-snapshot. Das folgende Beispiel kopiert den angegebenen Snapshot von der Quellregion in die aktuelle Region, die durch die `--region` Option angegeben wird.

```
aws ec2 copy-snapshot \
    --source-snapshot-id snap-0abcdef1234567890 \
    --source-region us-east-1 \
    --region us-west-2
```

Um einen unverschlüsselten Snapshot in einen verschlüsselten Snapshot zu kopieren

Verwenden Sie den Befehl copy-snapshot. Das folgende Beispiel kopiert den angegebenen unverschlüsselten Snapshot von der Quellregion in die aktuelle Region und verschlüsselt den neuen Snapshot mit dem angegebenen KMS-Schlüssel.

```
aws ec2 copy-snapshot \
    --source-snapshot-id snap-0abcdef1234567890 \
    --source-region us-east-1 \
    --encrypted \
    --kms-key-id alias/my-kms-key
```

PowerShell

Um einen Snapshot in eine andere Region zu kopieren

Verwenden Sie das cmdlet Copy-EC2Snapshot. Das folgende Beispiel kopiert den angegebenen Snapshot von der Quellregion in die aktuelle Region, die durch die `--region` Option angegeben wird.

```
Copy-EC2Snapshot `
    -SourceSnapshotId snap-0abcdef1234567890 `
    -SourceRegion us-east-1 `
```

```
    -Region us-west-2
```

Um einen unverschlüsselten Snapshot in einen verschlüsselten Snapshot zu kopieren

Verwenden Sie das cmdlet Copy-EC2Snapshot. Das folgende Beispiel kopiert den angegebenen unverschlüsselten Snapshot von der Quellregion in die aktuelle Region und verschlüsselt den neuen Snapshot mit dem angegebenen KMS-Schlüssel.

```
Copy-EC2Snapshot `
    -SourceSnapshotId snap-0abcdef1234567890 `
    -SourceRegion us-east-1 `
    -Encrypted $true `
    -KmsKeyId alias/my-kms-key
```

Teilen Sie einen Amazon EBS-Snapshot mit anderen AWS Konten

Sie können die Berechtigungen eines Snapshots ändern, wenn Sie ihn für andere AWS -Konten freigeben möchten. Sie können Snapshots öffentlich mit allen anderen AWS Konten teilen, oder Sie können sie privat mit einzelnen AWS Konten teilen, die Sie angeben. Benutzer, die Sie autorisiert haben, können die von Ihnen freigegebenen Snapshots zur Erstellung ihrer eigenen EBS-Volumes verwenden, während Ihr Original-Snapshot davon unberührt bleibt.

> **Important**
>
> Wenn Sie einen Snapshot freigeben, erteilen Sie anderen Zugriff auf sämtliche Daten dieses Snapshots. Geben Sie Snapshots mit all Ihren Snapshot-Daten nur für Personen frei, denen Sie vertrauen.

Um das öffentliche Teilen von Schnappschüssen zu verhindern, können Sie Folgendes aktivieren. Sperren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots

Themen

- Vor der Freigabe eines Snapshots
- Teilen Sie einen Snapshot
- Teilen Sie den KMS-Schlüssel, der zum Verschlüsseln eines gemeinsam genutzten Amazon EBS-Snapshots verwendet wird
- Verwenden Sie Amazon EBS-Snapshots, die mit Ihnen geteilt werden

- Festlegen der Verwendung von Snapshots, die Sie freigeben

Vor der Freigabe eines Snapshots

Für die Freigabe von Snapshots gelten die folgenden Dinge:

- Wenn das Blockieren des öffentlichen Zugriffs auf Snapshots für die Region aktiviert ist, werden Versuche, Snapshots öffentlich freizugeben, blockiert. Snapshots können weiterhin privat freigegeben werden.
- Snapshots sind auf die Region beschränkt, in der sie erstellt wurden. Um einen Snapshot in einer anderen Region freizugeben, kopieren Sie den Snapshot in die Region und geben dann die Kopie frei. Weitere Informationen finden Sie unter Kopieren Sie einen Amazon EBS-Snapshot.
- Sie können keine Snapshots freigeben, die mit dem standardmäßigen Von AWS verwalteter Schlüssel verschlüsselt sind. Sie können nur Snapshots freigeben, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Weitere Informationen finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.
- Sie können nur unverschlüsselte Snapshots öffentlich freigeben.
- Wenn Sie einen verschlüsselten Snapshot freigeben, müssen Sie auch den vom Kunden verwalteten Schlüssel freigeben, mit dem der Snapshot verschlüsselt wurde. Weitere Informationen finden Sie unter Teilen Sie den KMS-Schlüssel, der zum Verschlüsseln eines gemeinsam genutzten Amazon EBS-Snapshots verwendet wird.

Teilen Sie einen Snapshot

Sie können einen Snapshot öffentlich oder mit bestimmten AWS Konten teilen.

Console

So geben Sie einen Snapshot frei:

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den freizugebenden Snapshot aus und wählen Sie dann Aktionen, Berechtigungen ändern.
4. Legen Sie die Berechtigungen für den Snapshot fest. Aktuelle Einstellung gibt die aktuellen Freigabeberechtigungen des Snapshots an.

- Um den Snapshot öffentlich mit allen AWS Konten zu teilen, wählen Sie Öffentlich.
- Um den Snapshot privat mit bestimmten AWS Konten zu teilen, wählen Sie Privat. Wählen Sie dann im Abschnitt Konten teilen die Option Konto hinzufügen aus und geben Sie die 12-stellige ID (ohne Bindestriche) des Kontos ein, für das Sie den Snapshot freigeben möchten.

5. Wählen Sie Änderungen speichern aus.

AWS CLI

Die Berechtigungen für einen Snapshot angegeben sind mit dem `createVolumePermission`-Attribut des Snapshots. Wenn Sie einen Snapshot öffentlich zu machen, legen Sie die Gruppe `all` an. Um einen Snapshot mit einem bestimmten AWS Konto zu teilen, geben Sie dem Benutzer die ID des AWS Kontos an.

So geben Sie einen Snapshot öffentlich frei:

Verwenden Sie den Befehl modify-snapshot-attribute.

Legen Sie für `--attribute` die Option `createVolumePermission` fest. Legen Sie für `--operation-type` die Option `add` fest. Legen Sie für `--group-names` die Option `all` fest.

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission \
    --operation-type add \
    --group-names all
```

So geben Sie einen Snapshot privat frei:

Verwenden Sie den Befehl modify-snapshot-attribute.

Legen Sie für `--attribute` die Option `createVolumePermission` fest. Legen Sie für `--operation-type` die Option `add` fest. Geben Sie für `--user-ids` die 12-stelligen IDs der AWS Konten an, mit denen die Snapshots geteilt werden sollen.

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission \
    --operation-type add \
    --user-ids 123456789012 111122223333
```

PowerShell

Die Berechtigungen für einen Snapshot angegeben sind mit dem `createVolumePermission`-Attribut des Snapshots. Wenn Sie einen Snapshot öffentlich zu machen, legen Sie die Gruppe `all` an. Um einen Snapshot mit einem bestimmten AWS Konto zu teilen, geben Sie für den Benutzer die ID des AWS Kontos ein.

So geben Sie einen Snapshot öffentlich frei:

Verwenden Sie das cmdlet Edit-EC2SnapshotAttribute.

Legen Sie für `-Attribute` die Option `CreateVolumePermission` fest. Legen Sie für `-OperationType` die Option `Add` fest. Legen Sie für `-GroupName` die Option `all` fest.

```
Edit-EC2SnapshotAttribute `
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute CreateVolumePermission `
    -OperationType Add `
    -GroupName all
```

So geben Sie einen Snapshot privat frei:

Verwenden Sie das cmdlet Edit-EC2SnapshotAttribute.

Legen Sie für `-Attribute` die Option `CreateVolumePermission` fest. Legen Sie für `-OperationType` die Option `Add` fest. Geben Sie für `UserId` die 12-stelligen IDs der AWS Konten an, mit denen die Snapshots geteilt werden sollen.

```
Edit-EC2SnapshotAttribute `
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute CreateVolumePermission `
    -OperationType Add `
    -UserId 123456789012 111122223333
```

Teilen Sie den KMS-Schlüssel, der zum Verschlüsseln eines gemeinsam genutzten Amazon EBS-Snapshots verwendet wird

Wenn Sie einen verschlüsselten Snapshot freigeben, müssen Sie auch den vom Kunden verwalteten Schlüssel freigeben, mit dem der Snapshot verschlüsselt wurde. Sie können kontenübergreifende

Berechtigungen auf einen vom Kunden verwalteten Schlüssel entweder bei dessen Erstellung oder zu einem späteren Zeitpunkt anwenden.

Benutzer Ihres freigegebenen vom Kunden verwalteten Schlüssels, die auf verschlüsselte Snapshots zugreifen, müssen Berechtigungen erhalten, um die folgenden Aktionen für den Schlüssel durchzuführen:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn der Zuschuss im Namen des Benutzers von einem AWS Dienst erstellt wird.

Weitere Informationen über die Kontrolle des Zugriffs auf vom Kunden verwaltete Schlüssel finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im AWS Key Management Service - Entwicklerhandbuch.

Um den vom Kunden verwalteten Schlüssel gemeinsam zu nutzen, verwenden Sie den AWS KMS Konsole

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Customer managed keys (Vom Kunden verwaltete Schlüssel).

4. Wählen Sie in der Spalte Alias den Alias (Textlink) des vom Kunden verwalteten Schlüssels aus, mit dem Sie den Snapshot verschlüsselt haben. Die Schlüsseldetails werden auf einer neuen Seite geöffnet.
5. Im Abschnitt Key policy (Schlüsselrichtlinie) wird entweder die Richtlinienansicht oder die Standardansicht angezeigt. In der Richtlinienansicht wird das wichtige Richtliniendokument angezeigt. In der Standardansicht werden Abschnitte für Key administrators (Schlüsseladministratoren), Key deletion (Schlüssellöschung), Key Use (Schlüsselverwendung) und Other AWS accounts angezeigt. Die Standardansicht wird angezeigt, wenn Sie die Richtlinie in der Konsole erstellt und nicht angepasst haben. Wenn die Standardansicht nicht verfügbar ist, müssen Sie die Richtlinie in der Richtlinienansicht manuell bearbeiten. Weitere Informationen finden Sie unter Anzeigen einer Schlüsselrichtlinie (Konsole) im AWS Key Management Service - Entwicklerhandbuch.

   Verwenden Sie entweder die Richtlinienansicht oder die Standardansicht, je nachdem, auf welche Ansicht Sie zugreifen können, um der Richtlinie eine oder mehrere AWS Konto-IDs hinzuzufügen. Gehen Sie wie folgt vor:

   - (Richtlinienansicht) Wählen Sie Edit (Bearbeiten) aus. Fügen Sie den folgenden Anweisungen eine oder mehrere AWS Konto-IDs hinzu: `"Allow use of the key"` und`"Allow attachment of persistent resources"`. Wählen Sie Änderungen speichern aus. Im folgenden Beispiel `444455556666` wird die AWS Konto-ID zur Richtlinie hinzugefügt.

     ```
     {
       "Sid": "Allow use of the key",
       "Effect": "Allow",
       "Principal": {"AWS": [
         "arn:aws:iam::111122223333:user/KeyUser",
         "arn:aws:iam::444455556666:root"
       ]},
       "Action": [
         "kms:Encrypt",
         "kms:Decrypt",
         "kms:ReEncrypt*",
         "kms:GenerateDataKey*",
         "kms:DescribeKey"
       ],
       "Resource": "*"
     },
     {
     ```

```
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- (Standardansicht) Scrollen Sie nach unten zu Andere AWS Konten. Wählen Sie Weitere AWS Konten hinzufügen und geben Sie die AWS Konto-ID ein, wenn Sie dazu aufgefordert werden. Um ein weiteres Konto hinzuzufügen, wählen Sie Weiteres AWS Konto hinzufügen und geben Sie die AWS Konto-ID ein. Wenn Sie alle AWS -Konten hinzugefügt haben, wählen Sie Save Changes (Änderungen speichern) aus.

Verwenden Sie Amazon EBS-Snapshots, die mit Ihnen geteilt werden

So verwenden Sie einen freigegebenen, unverschlüsselten Snapshot:

Suchen Sie den freigegebenen Snapshot nach der ID oder der Beschreibung. Sie können diesen Snapshot so wie alle anderen Snapshots verwenden, deren Eigentümer Sie in Ihrem Konto sind. Sie können beispielsweise ein Volume aus dem Snapshot erstellen oder ihn in eine andere Region kopieren.

So verwenden Sie einen freigegebenen, verschlüsselten Snapshot:

Suchen Sie den freigegebenen Snapshot nach der ID oder der Beschreibung. Erstellen Sie eine Kopie des freigegebenen Snapshots in Ihrem Konto und verschlüsseln Sie die Kopie mit einem KMS-Schlüssel, dessen Eigentümer Sie sind. Anschließend können Sie die Kopie verwenden, um Volumes zu erstellen oder sie in andere Regionen kopieren.

Console

Um Snapshot-Berechtigungen einzusehen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus.
4. Wenn der Filter mir gehört, gehört der Snapshot diesem Konto. Wenn es sich bei dem Filter um Private Snapshots handelt, gehört der Snapshot entweder diesem Konto oder ist speziell für dieses Konto freigegeben. Wählen Sie einen Snapshot aus und überprüfen Sie auf der Registerkarte Details, ob der Eigentümer dieses Konto oder ein anderes Konto angibt.

AWS CLI

Um Snapshot-Berechtigungen einzusehen

Verwenden Sie den Befehl describe-snapshot-attribute, um die Snapshot-Berechtigungen für den angegebenen Snapshot abzurufen.

```
aws ec2 describe-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateVolumePermissions": [
        {
            "UserId": "111122223333"
        }
    ]
}
```

PowerShell

Um Snapshot-Berechtigungen anzuzeigen

Verwenden Sie das cmdlet Get-EC2SnapshotAttribute.

```
(Get-EC2SnapshotAttribute `
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute createVolumePermission).CreateVolumePermissions
```

Es folgt eine Beispielausgabe.

```
Group UserId
----- ------
      111122223333
```

Festlegen der Verwendung von Snapshots, die Sie freigeben

Sie können AWS CloudTrail damit überwachen, ob ein Snapshot, den Sie mit anderen geteilt haben, kopiert oder zur Erstellung eines Volumes verwendet wird. Die folgenden Ereignisse werden protokolliert CloudTrail , wenn eine Aktion für einen Snapshot ausgeführt wird, den Sie geteilt haben:

- SharedSnapshotCopyInitiated— Ein geteilter Snapshot wird kopiert.
- SharedSnapshotVolumeCreated— Ein gemeinsam genutzter Snapshot wird verwendet, um ein Volume zu erstellen.

Weitere Informationen zur Verwendung CloudTrail finden Sie unter Amazon EC2- und Amazon EBS-API-Aufrufe protokollieren mit. AWS CloudTrail

Archivieren von Amazon EBS-Snapshots

Amazon EBS Snapshots Archive ist eine Speicherebene, die Sie für eine kostengünstige und langfristige Speicherung Ihrer selten aufgerufenen Snapshots verwenden können, die nicht oft oder schnell abgerufen werden müssen.

Wenn Sie einen Snapshot erstellen, wird er standardmäßig auf der Standardstufe für Amazon EBS-Snapshots (Standardstufe) gespeichert. Snapshots, die auf der Standardstufe gespeichert sind, sind inkrementell. Das bedeutet, dass nur die Blöcke auf dem Volume gespeichert werden, die sich nach Ihrem letzten Snapshot geändert haben.

Wenn Sie einen Snapshot archivieren, wird der inkrementelle Snapshot in einen vollständigen Snapshot konvertiert und von der Standardstufe zur Stufe von Amazon EBS Snapshots Archive (Archivstufe) verschoben. Vollständige Snapshots umfassen alle Blöcke, die zum Zeitpunkt der Snapshot-Erstellung auf das Volume geschrieben wurden.

Wenn Sie auf einen archivierten Snapshot zugreifen müssen, können Sie ihn von der Archivstufe auf die Standardstufe wiederherstellen und ihn dann genau wie andere Snapshots in Ihrem Konto verwenden.

Amazon EBS Snapshots Archive bietet bis zu 75 Prozent niedrigere Snapshot-Speicherkosten für Snapshots, die Sie 90 Tage oder länger speichern möchten und auf die Sie selten zugreifen müssen.

Einige typische Anwendungsfälle:

- Archivieren des einzigen Snapshots eines Volumes (z. B. Snapshots bei Projektende)
- Archivieren vollständiger inkrementeller Point-in-Time-Snapshots aus Compliance-Gründen
- Archivieren monatlicher, vierteljährlicher oder jährlicher inkrementeller Snapshots

Themen

- Kontingente
- Überlegungen und Einschränkungen bei der Archivierung von Amazon EBS-Snapshots
- Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots
- Richtlinien und bewährte Methoden für die Archivierung von Amazon EBS-Snapshots
- Erforderliche IAM-Berechtigungen für die Archivierung von Amazon EBS-Snapshots
- Archivieren Sie einen Amazon EBS-Snapshot
- Stellen Sie einen archivierten Amazon EBS-Snapshot wieder her
- Ändern Sie den Wiederherstellungszeitraum für einen vorübergehend wiederhergestellten Amazon EBS-Snapshot
- Archivierte Amazon EBS-Snapshots anzeigen
- Überwachen Sie die Amazon EBS-Snapshot-Archivierung mithilfe von Events CloudWatch

Kontingente

In diesem Abschnitt werden die Standardkontingente für archivierte und in Bearbeitung befindliche Snapshots beschrieben.

Kontingent	Standardkontingent			
Archivierte Snapshots	25			

Kontingent	Standardkontingent			
pro Volume				
Gleichzeitig aktive Snapshot-Archive pro Konto	25			
Gleichzeitig aktive Snapshot-Wiederherstellungen pro Konto	5			

Wenn Sie mehr als die Standardlimits benötigen, füllen Sie das Support Center https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-ebs Create-Fallformular aus, um eine Limiterhöhung zu beantragen.

Überlegungen und Einschränkungen bei der Archivierung von Amazon EBS-Snapshots

Beachten Sie bei der Archivierung von Amazon EBS-Snapshots Folgendes.

Überlegungen

- Der minimale Archivzeitraum beträgt 90 Tage. Wenn Sie einen archivierten Snapshot vor Ablauf des minimalen Archivzeitraums von 90 Tagen löschen oder dauerhaft wiederherstellen, werden Ihnen die verbleibenden Tage auf der Archivstufe in Rechnung gestellt (auf die nächste Stunde

gerundet). Weitere Informationen finden Sie unter Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots.

- Je nach Größe des Snapshots kann es bis zu 72 Stunden dauern, bis ein archivierter Snapshot von der Archivstufe auf die Standardstufe wiederhergestellt wird.
- Archivierte Snapshots sind immer vollständige Snapshots. Ein vollständiger Snapshot enthält alle Blöcke, die zum Zeitpunkt der Erstellung des Snapshots auf das Volume geschrieben wurden. Der vollständige Snapshot ist wahrscheinlich größer als der inkrementelle Snapshot, auf dessen Grundlage er erstellt wurde. Wenn Sie jedoch nur einen Snapshot eines Volumes auf der Standard-Ebene haben, entspricht die Größe des gesamten Snapshots auf der Archivebene der Größe des Snapshots auf der Standard-Ebene. Dies liegt daran, dass der erste Snapshot eines Volumes immer ein vollständiger Snapshot ist. Verwenden Sie den Befehl describe-snapshots, um die volle AWS CLI Snapshot-Größe abzurufen.
- Die Archivierung wird für monatliche, vierteljährliche oder jährliche Snapshots empfohlen. Die Archivierung täglicher schrittweiser Snapshots eines einzelnen Volumes kann im Vergleich zur Aufbewahrung im Standard-Tier zu höheren Kosten führen.
- Wenn ein Snapshot archiviert wird, werden die Daten des Snapshots, auf die andere Snapshots in der Snapshot-Lineage verweisen, auf der Standardstufe gespeichert. Die Daten- und Speicherkosten für die referenzierten Daten, die auf der Standardstufe gespeichert werden, werden dem nächsten Snapshot in der Lineage zugeordnet. Dadurch ist sichergestellt, dass nachfolgende Snapshots in der Lineage nicht von der Archivierung betroffen sind.
- Wenn Sie einen archivierten Snapshot löschen, der einer Aufbewahrungsregel für den Papierkorb entspricht, wird der archivierte Snapshot so lange im Papierkorb aufbewahrt, wie es gemäß Aufbewahrungsregel definiert ist. Um den Snapshot verwenden zu können, müssen Sie ihn zuerst aus dem Papierkorb wiederherstellen und dann aus der Archivstufe wiederherstellen. Weitere Informationen finden Sie unter Papierkorb und. Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots
- Sie können einen archivierten Snapshot nicht in einer Blockgerät-Zuweisung oder zur Erstellung eines Amazon EBS-Volumes verwenden.
- Sie können Schnappschüsse archivieren AWS-Backup-Konsole, die AWS Backup mit den APIs oder Befehlszeilentools erstellt wurden. Weitere Informationen finden Sie unter Erstellen eines Backup-Plans im Entwicklerhandbuch für AWS Backup

Einschränkungen

- Sie können nur Snapshots archivieren, die den Status `completed` haben.

- Sie können nur Snapshots archivieren, deren Eigentümer Sie in Ihrem Konto sind. Um einen für Sie freigegebenen Snapshot zu archivieren, kopieren Sie zuerst den Snapshot in Ihr Konto und archivieren Sie dann die Snapshot-Kopie.
- Bevor Sie einen archivierten Snapshot verwenden können, müssen Sie ihn zuerst auf der Standardstufe wiederherstellen. Die Wiederherstellung auf die Standardstufe ist erforderlich, um aus dem Snapshot mithilfe des `CreateVolume` und den API-Operationen `RunInstances` ein Volume zu erstellen und einen Snapshot freizugeben oder zu kopieren. Weitere Informationen finden Sie unter Stellen Sie einen archivierten Amazon EBS-Snapshot wieder her.
- Sie können einen Snapshot, der einem oder mehreren AMIs zugeordnet ist, nur archivieren, wenn alle zugehörigen AMIs deaktiviert sind. Weitere Informationen finden Sie unter Ein AMI https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/disable-an-ami.html deaktivieren.
- Sie können ein deaktiviertes AMI nicht aktivieren, wenn die zugehörigen Snapshots vorübergehend wiederhergestellt werden. Alle zugehörigen Snapshots müssen dauerhaft wiederhergestellt werden, bevor Sie das AMI aktivieren können.
- Sie können den Snapshot-Archivierungs- oder Snapshot-Wiederherstellungsvorgang nicht abbrechen, nachdem er gestartet wurde.
- Sie können archivierte Snapshots nicht freigeben. Wenn Sie einen Snapshot archivieren, den Sie für andere Konten freigegeben haben, haben die Konten, für die der Snapshot freigegeben nach der Archivierung des Snapshots keinen Zugriff mehr darauf.
- Sie können archivierte Snapshots nicht kopieren. Damit Sie einen archivierten Snapshot kopieren können, müssen Sie ihn zuerst wiederherstellen.
- Sie können die schnelle Snapshot-Wiederherstellung nicht für archivierte Snapshots aktivieren. Die schnelle Snapshot-Wiederherstellung wird automatisch deaktiviert, wenn ein Snapshot archiviert wird. Damit Sie die schnelle Snapshot-Wiederherstellung verwenden können, müssen Sie sie nach dem Wiederherstellen des Snapshots manuell aktivieren.

Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots

Archivierte Snapshots werden mit einem Preis von 0,0125 USD pro Person in Rechnung gestellt. GB-month Wenn Sie beispielsweise einen 100-GiB-Snapshot archivieren, werden Ihnen 1,25 USD (100 GiB * 0,0125 USD) pro Monat in Rechnung gestellt.

Snapshot-Wiederherstellungen werden mit einem Satz von 0,03 USD pro GB an wiederhergestellten Daten abgerechnet. Wenn Sie beispielsweise einen 100-GiB-Snapshot von der Archivstufe wiederherstellen, werden Ihnen einmalig 3 USD (100 GiB * 0,03 USD) in Rechnung gestellt.

Nachdem der Snapshot auf der Standardstufe wiederhergestellt wurde, wird der Snapshot zum Standardtarif für Snapshots in Höhe von 0,05 USD pro Snapshot in Rechnung gestellt. GB-month

Weitere Informationen finden Sie unter Amazon EBS – Preise.

Abrechnung für den minimalen Archivzeitraum

Der minimale Archivzeitraum beträgt 90 Tage. Wenn Sie einen archivierten Snapshot vor Ablauf des minimalen Archivzeitraums von 90 Tagen löschen oder dauerhaft wiederherstellen, wird Ihnen für die verbleibenden Tage eine anteilige Gebühr in Höhe der Speichergebühr für die Archivstufe in Rechnung gestellt (auf die nächste Stunde gerundet). Wenn Sie beispielsweise einen archivierten Snapshot nach 40 Tagen löschen oder dauerhaft wiederherstellen, werden Ihnen die verbleibenden 50 Tage des minimalen Archivzeitraums in Rechnung gestellt.

> **Note**
>
> Für die vorübergehende Wiederherstellung eines archivierten Snapshots vor Ablauf des minimalen Archivzeitraums von 90 Tagen fällt diese Gebühr nicht an.

Temporäre Wiederherstellungen

Wenn Sie einen Snapshot vorübergehend wiederherstellen, wird der Snapshot von der Archivstufe auf die Standardstufe wiederhergestellt und eine Kopie des Snapshots verbleibt auf der Archivstufe. Für die Dauer des temporären Wiederherstellungszeitraums werden Ihnen sowohl der Snapshot auf der Standardstufe als auch die Snapshot-Kopie auf der Archivstufe in Rechnung gestellt. Wenn der vorübergehend wiederhergestellte Snapshot aus der Standardstufe entfernt wird, wird Ihnen dieser nicht mehr in Rechnung gestellt. Ihnen wird dann nur noch der Snapshot auf der Archivstufe in Rechnung gestellt.

Dauerhafte Wiederherstellungen

Wenn Sie einen Snapshot dauerhaft wiederherstellen, wird der Snapshot von der Archivstufe auf die Standardstufe wiederhergestellt und der Snapshot wird aus der Archivstufe gelöscht. Der Snapshot wird Ihnen nur auf der Standardstufe in Rechnung gestellt.

Löschen von Snapshots

Wenn Sie einen Snapshot löschen, während er archiviert wird, werden Ihnen die Snapshot-Daten in Rechnung gestellt, die bereits auf die Archivstufe verschoben wurden. Für diese

Daten gilt ein minimaler Archivzeitraum von 90 Tagen und sie werden nach der Löschung entsprechend abgerechnet. Wenn Sie beispielsweise einen 100-GiB-Snapshot archivieren und den Snapshot löschen, nachdem nur 40 GiB archiviert wurden, werden Ihnen 1,50 USD für den Mindestarchivierungszeitraum von 90 Tagen für die 40 GiB, die bereits archiviert wurden, in Rechnung gestellt (0,0125 USD pro GB-month * 40 GB * (90 Tage* 24 Stunden)/(24 hours/day * 30-Tage-Monat).

Wenn Sie einen Snapshot löschen, während er von der Archivstufe wiederhergestellt wird, wird Ihnen die Snapshot-Wiederherstellung für die volle Größe des Snapshots (Snapshot-Größe * 0,03 USD) in Rechnung gestellt. Wenn Sie beispielsweise einen 100-GiB-Snapshot von der Archivstufe wiederherstellen und den Snapshot löschen, bevor die Snapshot-Wiederherstellung abgeschlossen ist, werden Ihnen 3 USD (100 GiB-Snapshotgröße * 0,03 USD) in Rechnung gestellt.

Papierkorb

Archivierte Snapshots werden mit dem Satz für archivierte Snapshots abgerechnet, während sie sich im Papierkorb befinden. Für archivierte Snapshots, die sich im Papierkorb befinden, gilt der minimale Archivzeitraum von 90 Tagen und sie werden entsprechend abgerechnet, wenn sie vor Ablauf des minimalen Archivzeitraums im Papierkorb gelöscht werden. Mit anderen Worten: Wenn ein archivierter Snapshot vor dem Mindestzeitraum von 90 Tagen durch eine Aufbewahrungsregel aus dem Papierkorb gelöscht wird, werden Ihnen die verbleibenden Tage in Rechnung gestellt.

Wenn Sie einen Snapshot löschen, der einer Aufbewahrungsregel entspricht, während der Snapshot archiviert wird, wird der archivierte Snapshot so lange im Papierkorb aufbewahrt, wie es gemäß Aufbewahrungsregel definiert ist. Er wird zum Satz für archivierte Snapshots abgerechnet.

Wenn Sie einen Snapshot löschen, der einer Aufbewahrungsregel entspricht, während der Snapshot wiederhergestellt wird, wird der wiederhergestellte Snapshot für den Rest des Aufbewahrungszeitraums im Papierkorb gespeichert und mit dem standardmäßigen Satz für Snapshots abgerechnet. Damit Sie den wiederhergestellten Snapshot verwenden können, müssen Sie ihn zuerst aus dem Papierkorb wiederherstellen.

Weitere Informationen finden Sie unter Papierkorb. ???

Kostenverfolgung

Archivierte Snapshots werden im AWS Cost and Usage Report mit derselben Ressourcen-ID und demselben Amazon-Ressourcennamen (ARN) angezeigt. Weitere Informationen finden Sie im AWS Cost and Usage Report -Benutzerhandbuch.

Sie können die folgenden Nutzungstypen verwenden, um die damit verbundenen Kosten zu identifizieren:

- `SnapshotArchiveStorage` – Gebühr für die monatliche Datenspeicherung
- `SnapshotArchiveRetrieval` – Einmalige Gebühr für Snapshot-Wiederherstellungen
- `SnapshotArchiveEarlyDelete` – Gebühr für das Löschen oder dauerhafte Wiederherstellen eines Snapshots vor Ablauf des minimalen Archivzeitraums (90 Tage)

Richtlinien und bewährte Methoden für die Archivierung von Amazon EBS-Snapshots

In diesem Abschnitt finden Sie einige Richtlinien und bewährte Methoden zum Archivieren von Snapshots.

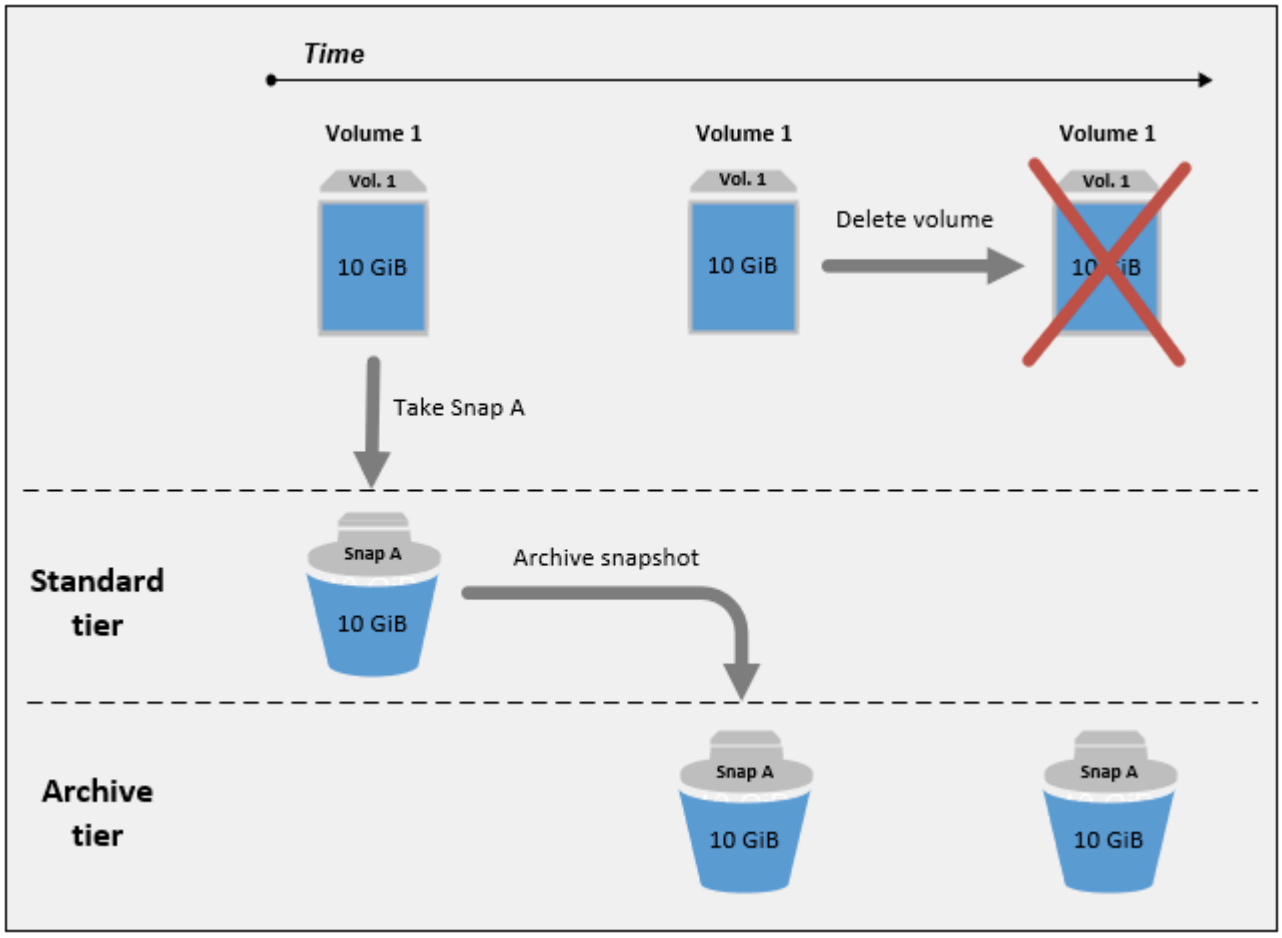
Themen

- Archivieren des einzigen Snapshots eines Volumes
- Archivieren inkrementeller Snapshots eines einzelnen Volumes
- Archivieren von vollständigen Snapshots aus Compliance-Gründen
- Ermitteln der Verringerung der Speicherkosten auf Standardstufe

Archivieren des einzigen Snapshots eines Volumes

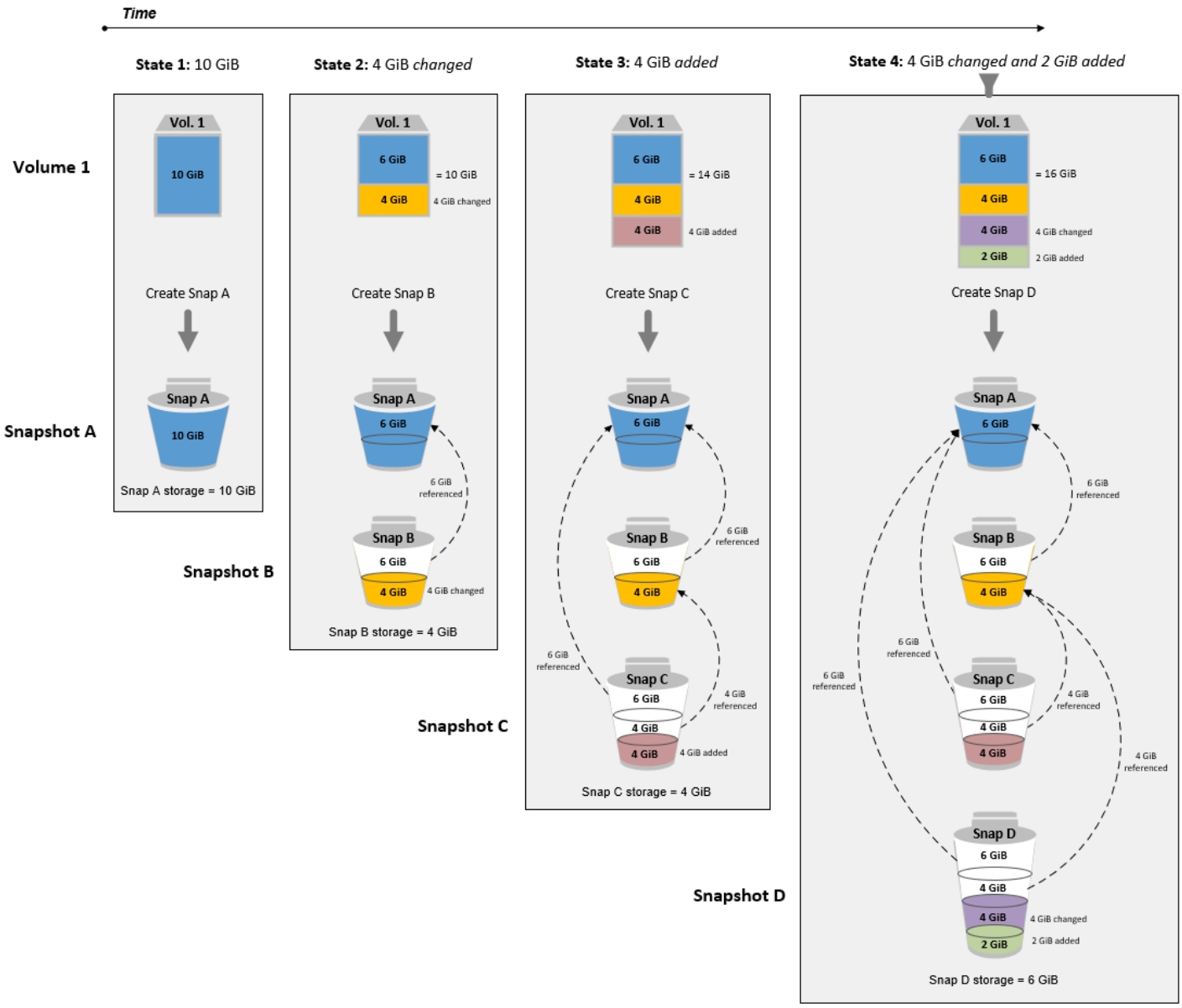
Wenn Sie nur einen Snapshot eines Volumes besitzen, hat der Snapshot immer die gleiche Größe wie die Blöcke, die zum Zeitpunkt der Erstellung des Snapshots auf dem Volume geschrieben waren. Wenn Sie einen solchen Snapshot archivieren, wird er auf der Standardstufe in einen vollständigen Snapshot mit der entsprechenden Größe konvertiert und von der Standardstufe auf die Archivstufe verschoben.

Durch das Archivieren dieser Snapshots können Sie die Speicherkosten verringern. Wenn Sie das Quellvolume nicht mehr benötigen, können Sie das Volume löschen, um die Speicherkosten weiter zu senken.



Archivieren inkrementeller Snapshots eines einzelnen Volumes

Wenn Sie einen inkrementellen Snapshot archivieren, wird der Snapshot in einen vollständigen Snapshot konvertiert und auf die Archivstufe verschoben. Wenn Sie beispielsweise im folgenden Image Snap B archivieren, wird der Snapshot in einen vollständigen Snapshot mit einer Größe von 10 GiB konvertiert und auf die Archivstufe verschoben. Wenn Sie Snap C archivieren, beträgt die Größe des vollständigen Snapshots auf der Archivstufe 14 GiB.



Wenn Sie Snapshots archivieren, um Ihre Speicherkosten auf der Standardstufe zu senken, sollten Sie nicht den ersten Snapshot einer Reihe inkrementeller Snapshots archivieren. Nachfolgende Snapshots in der Snapshot-Lineage verweisen auf diese Snapshots. In den meisten Fällen hat das Archivieren dieser Snapshots keine Verringerung der Speicherkosten zur Folge.

> **Note**
>
> Der letzte Snapshot in einer Reihe inkrementeller Snapshots sollte nicht archiviert werden. Der letzte Snapshot ist der neueste Snapshot eines Volumes. Sie benötigen diesen Snapshot

auf der Standardstufe, wenn Sie Volumes daraus erstellen möchten, weil ein Volume beschädigt wurde oder nicht mehr verfügbar ist.

Wenn Sie einen Snapshot archivieren, der Daten enthält, auf die ein nachfolgender Snapshot in der Lineage verweist, werden der Datenspeicher und die Speicherkosten für die referenzierten Daten dem späteren Snapshot in der Lineage zugeordnet. In diesem Fall führt die Archivierung des Snapshots nicht zu einer Verringerung der Datenspeicher- oder Speicherkosten. Wenn Sie beispielsweise Snap B archivieren (wie in dem vorherigen Image dargestellt), werden dessen 4 GiB an Daten Snap C zugeordnet. In diesem Fall erhöhen sich Ihre Gesamtspeicherkosten, da Ihnen Speicherkosten für die vollständige Version von Snap B auf der Archivstufe entstehen. Ihre Speicherkosten für die Standardstufe bleiben unverändert.

Wenn Sie Snap C archivieren, verringert sich Ihr Speicher auf der Standardstufe um 4 GiB, da die Daten nicht von anderen Snapshots später in der Lineage referenziert werden. Gleichzeitig erhöht sich Ihr Speicher auf Archivstufe um 14 GiB erhöht, da der Snapshot in einen vollständigen Snapshot konvertiert wird.

Archivieren von vollständigen Snapshots aus Compliance-Gründen

Möglicherweise müssen Sie aus Compliance-Gründen monatlich, vierteljährlich oder jährlich vollständige Backups von Volumes erstellen. Für diese Backups benötigen Sie möglicherweise eigenständige Snapshots ohne Rückwärts- oder Vorwärtsverweise auf andere Snapshots in der Snapshot-Lineage. Snapshots, die mit dem EBS-Snapshots-Archiv archiviert wurden, sind vollständige Snapshots und enthalten keine Verweise auf andere Snapshots in der Lineage. Darüber hinaus müssen Sie diese Snapshots wahrscheinlich aus Compliance-Gründen mehrere Jahre lang aufbewahren. Mit dem EBS-Snapshots-Archiv lassen sich diese vollständigen Snapshots kostengünstig zur langfristigen Aufbewahrung archivieren.

Ermitteln der Verringerung der Speicherkosten auf Standardstufe

Wenn Sie einen inkrementellen Snapshot archivieren möchten, um Ihre Speicherkosten zu senken, sollten Sie die Größe des vollständigen Snapshots auf der Archivstufe und die Verringerung des Speichers auf der Standardstufe berücksichtigen. In diesem Abschnitt wird erklärt, wie Sie hierzu vorgehen.

> **Important**
>
> Die Daten in den API-Antworten sind zum Zeitpunkt, an dem die APIs aufgerufen werden, genau. API-Antworten können abweichen, da sich die mit einem Snapshot verbundenen Daten aufgrund von Änderungen an der Snapshot-Lineage ändern.

Wenn Sie die Verringerung des Datenspeichers und der Speicherkosten auf der Standardstufe ermitteln möchten, gehen Sie nachfolgend beschrieben vor.

1. Überprüfen Sie für den Snapshot, den Sie archivieren möchten, die volle Snapshot-Größe und das Quell-Volume, aus dem er erstellt wurde. Verwenden Sie den Befehl describe-snapshots und geben Sie für die ID des Snapshots an`--snapshot-id`, den Sie archivieren möchten.

   ```
   $ aws ec2 describe-snapshots --snapshot-id snapshot_id
   ```

   Der `FullSnapshotSizeInBytes` Antwortwert gibt die volle Snapshot-Größe in Byte an, und der `VolumeId` Antwortwert gibt die ID des Quell-Volumes an.

   Beim folgenden Befehl werden beispielsweise Informationen zum Snapshot `snap-09c9114207084f0d9` zurückgegeben.

   ```
   $ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
   ```

   Die folgende Beispielausgabe zeigt, dass die gesamte Snapshot-Größe `5678912341` Byte (5,28 GiB) beträgt, und das Quell-Volume ist es. `vol-0f3e2c292c52b85c3`

   ```
   {
       "Snapshots": [
           {
               "Description": "",
               "Tags": [],
               "Encrypted": false,
               "VolumeId": "vol-0f3e2c292c52b85c3",
               "State": "completed",
               "VolumeSize": 8,
               "StartTime": "2021-11-16T08:29:49.840Z",
               "Progress": "100%",
               "OwnerId": "123456789012",
   ```

```
            "FullSnapshotSizeInBytes" : "5678912341",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

2. Suchen Sie alle Snapshots, die aus dem Quellvolume erstellt wurden. Verwenden Sie den Befehl describe-snapshots. Geben Sie den Filter `volume-id` und die Volume-ID aus dem vorherigen Schritt als Filterwert an.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

Beim folgenden Befehl werden beispielsweise alle Snapshots zurückgegeben, die aus Volume `vol-0f3e2c292c52b85c3` erstellt wurden.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
 Values=vol-0f3e2c292c52b85c3"
```

Die folgende Befehlsausgabe gibt an, dass drei Snapshots aus Volume `vol-0f3e2c292c52b85c3` erstellt wurden.

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-08ca60083f86816b0"
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
```

```
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

3. Sortieren Sie die Snapshots anhand der Ausgabe des vorherigen Befehls nach ihrer Erstellungszeit, vom ältesten zum neuesten. Der `StartTime`-Antwortparameter für jeden Snapshot gibt seine Erstellungszeit im UTC-Zeitformat an.

   Beispielsweise sehen die im vorherigen Schritt zurückgegebenen Snapshots, sortiert nach Erstellungszeit, vom ältesten zum neuesten, wie folgt aus:

   1. `snap-08ca60083f86816b0`(ältester — vor dem Snapshot erstellt, den Sie archivieren möchten)
   2. `snap-09c9114207084f0d9` (der zu archivierende Snapshot)
   3. `snap-024f49fe8dd853fa8` (neuestes – erstellt nach dem Snapshot, den Sie archivieren möchten)

4. Identifizieren Sie die Snapshots, die unmittelbar vor und nach dem Snapshot erstellt wurden, den Sie archivieren möchten. In diesem Fall möchten Sie Snapshot `snap-09c9114207084f0d9` archivieren, den zweiten inkrementellen Snapshot, der in den drei Snapshots erstellt wurde. Snapshot `snap-08ca60083f86816b0` wurde unmittelbar zuvor erstellt und Snapshot `snap-024f49fe8dd853fa8` wurde unmittelbar danach erstellt.

5. Ermitteln Sie die nicht referenzierten Daten im Snapshot, den Sie archivieren möchten. Suchen Sie zuerst die Blöcke, die sich zwischen dem Snapshot, der unmittelbar vor dem zu

archivierenden Snapshot erstellt wurde, und dem zu archivierenden Snapshot unterscheiden. Verwenden Sie den Befehl list-changed-blocks. Geben Sie für `--first-snapshot-id` die ID des Snapshots an, der unmittelbar vor dem Snapshot erstellt wurde, den Sie archivieren möchten. Geben Sie für `--second-snapshot-id` die ID des Snapshots an, den Sie archivieren möchten.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
snapshot-id snapshot_to_archive
```

Der folgende Befehl zeigt beispielsweise die Blockindizes für die Blöcke an, die sich zwischen Snapshot `snap-08ca60083f86816b0` (dem Snapshot, der vor dem zu archivierenden Snapshot erstellt wurde) und Snapshot `snap-09c9114207084f0d9` (dem Snapshot, den Sie archivieren möchten) unterscheiden.

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
snapshot-id snap-09c9114207084f0d9
```

Im Folgenden wird die Befehlsausgabe dargestellt, bei der einige Blöcke weggelassen werden.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy
+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue+cRwUqF",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
```

```
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
            "BlockIndex": 13174
        },
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
```

```
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

Verwenden Sie als Nächstes denselben Befehl, um Blöcke zu finden, die sich zwischen dem zu archivierenden Snapshot und dem Snapshot, der unmittelbar danach erstellt wurde, unterscheiden. Geben Sie für `--first-snapshot-id` die ID des Snapshots an, den Sie archivieren möchten. Geben Sie für `--second-snapshot-id` die ID des Snapshots an, der unmittelbar nach dem Snapshot erstellt wurde, den Sie archivieren möchten.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after
```

Der folgende Befehl zeigt beispielsweise die Blockindizes der Blöcke an, die sich zwischen Snapshot `snap-09c9114207084f0d9` (der Snapshot, den Sie archivieren möchten) und Snapshot `snap-024f49fe8dd853fa8` (der nach dem Snapshot, den Sie archivieren möchten, erstellte Snapshot) unterscheiden.

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8
```

Im Folgenden wird die Befehlsausgabe dargestellt, bei der einige Blöcke weggelassen werden.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
```

```
            "BlockIndex": 5
        },
        {
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
            "BlockIndex": 13193
        },
```

```
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```

6. Vergleichen Sie die Ausgabe, die im vorherigen Schritt von beiden Befehlen zurückgegeben wurde. Wenn in beiden Befehlsausgaben derselbe Blockindex angezeigt wird, enthält der Block nicht referenzierte Daten.

   Die Befehlsausgabe im vorherigen Schritt zeigt beispielsweise an, dass die Blöcke 4, 5, 13 und 14 für Snapshot `snap-09c9114207084f0d9` eindeutig sind und dass sie nicht von anderen Snapshots in der Snapshot-Lineage referenziert werden.

   Um die Reduzierung des Standardstufenspeichers zu ermitteln, multiplizieren Sie die Anzahl der Blöcke, die in beiden Befehlsausgaben angezeigt werden, mit 512 KiB (Snapshot-Blockgröße).

   Wenn beispielsweise in beiden Befehlsausgaben 9 950 Blockindizes angezeigt werden, bedeutet dies, dass Sie den Standardstufenspeicher um rund 4,85 GiB verringern (9 950 Blöcke * 512 KiB = 4,85 GiB).

7. Bestimmen Sie die Speicherkosten für die Speicherung der nicht referenzierten Blöcke auf der Standardstufe für 90 Tage. Vergleichen Sie diesen Wert mit den Kosten für die Speicherung des vollständigen Snapshots, wie in Schritt 1 beschrieben, auf der Archivebene. Sie können Ihre Kosteneinsparungen ermitteln, indem Sie die Werte vergleichen. Dies gilt jedoch nur, wenn Sie den vollständigen Snapshot nicht während des Mindestzeitraums von 90 Tagen aus der Archivstufe wiederherstellen. Weitere Informationen finden Sie unter Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots.

Erforderliche IAM-Berechtigungen für die Archivierung von Amazon EBS-Snapshots

Standardmäßig verfügen Benutzer nicht über die Berechtigung zur Verwendung der Snapshot-Archivierung. Damit Benutzer die Snapshot-Archivierung verwenden können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Verwendung bestimmter Ressourcen und API-Aktionen gewähren. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Zur Verwendung der Snapshot-Archivierung müssen Benutzer über die folgenden Berechtigungen verfügen.

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

Konsolenbenutzer benötigen möglicherweise zusätzliche Berechtigungen wie `ec2:DescribeSnapshots`.

Zum Archivieren und Wiederherstellen verschlüsselter Snapshots sind die folgenden zusätzlichen AWS KMS Berechtigungen erforderlich.

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die IAM-Benutzern die Berechtigung zum Archivieren, Wiederherstellen und Anzeigen verschlüsselter und unverschlüsselter Snapshots gewährt. Es umfasst die `ec2:DescribeSnapshots`-Berechtigung für Konsolenbenutzer. Werden einige Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn die Gewährung im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

JSON

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

```
        "Action": [
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Archivieren Sie einen Amazon EBS-Snapshot

Sie können jeden Snapshot archivieren, der den Status `completed` hat und dessen Eigentümer Sie in Ihrem Konto sind. Sie können keine Snapshots archivieren, die den Status `pending` oder

`error` haben oder für Sie freigegeben sind. Weitere Informationen finden Sie unter Überlegungen und Einschränkungen bei der Archivierung von Amazon EBS-Snapshots.

Wenn der Snapshot mit einem oder mehreren AMIs verknüpft ist, müssen Sie zuerst die verknüpften AMIs deaktivieren, bevor Sie den Snapshot archivieren können. Weitere Informationen finden Sie unter Ein AMI https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/disable-an-ami.html deaktivieren.

Archivierte Snapshots behalten ihre Snapshot-ID, ihren Verschlüsselungsstatus, ihre AWS Identity and Access Management (IAM) -Berechtigungen, Eigentümerinformationen und Ressourcen-Tags. Die schnelle Snapshot-Wiederherstellung und die Snapshot-Freigabe werden jedoch automatisch deaktiviert, nachdem der Snapshot archiviert wurde.

Sie können den Snapshot weiterhin verwenden, während die Archivierung in Bearbeitung ist. Sobald der Snapshot-Ebenen-Status den `archival-complete`-Status hat, können Sie den Snapshot nicht mehr verwenden.

Console

So archivieren Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie in der Liste der Snapshots den zu archivierenden Snapshot aus und wählen Sie dann Aktionen, Snapshot archivieren.
4. Wählen Sie zur Bestätigung Snapshot archivieren.

AWS CLI

So archivieren Sie einen Snapshot

Verwenden Sie den Befehl modify-snapshot-tier AWS CLI . Geben Sie für `--snapshot-id` die ID des zu archivierenden Snapshots an. Legen Sie für `--storage-tier` die Option `archive` fest.

```
aws ec2 modify-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --storage-tier archive
```

Es folgt eine Beispielausgabe. Der `TieringStartTime` Antwortparameter gibt das Datum und die Uhrzeit an, zu denen der Archivierungsvorgang gestartet wurde, im UTC-Zeitformat (). YYYY-MM-DDTHH:MM:SSZ

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

PowerShell

So archivieren Sie einen Snapshot

Verwenden Sie das cmdlet Edit-EC2SnapshotTier. Im folgenden Beispiel für wird der angegebene Snapshot archiviert.

```
Edit-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -StorageTier "archive"
```

Stellen Sie einen archivierten Amazon EBS-Snapshot wieder her

Bevor Sie einen archivierten Snapshot verwenden können, müssen Sie ihn zuerst auf der Standardstufe wiederherstellen. Beim wiederhergestellten Snapshot sind die Snapshot-ID, der Verschlüsselungsstatus, die IAM-Berechtigungen, Eigentümerinformationen und Ressourcen-Tags genau wie vor der Archivierung. Nachdem der Snapshot wiederhergestellt wurde, können Sie ihn genauso verwenden wie jeden anderen Snapshot in Ihrem Konto. Der wiederhergestellte Snapshot ist immer ein vollständiger Snapshot.

Wenn Sie einen Snapshot wiederherstellen, können Sie ihn permanent oder temporär wiederherstellen.

Wenn Sie einen Snapshot permanent wiederherstellen, wird der Snapshot dauerhaft von der Archivstufe auf die Standardstufe verschoben. Der Snapshot bleibt wiederhergestellt und für die Verwendung bereit, bis Sie ihn manuell erneut archivieren oder manuell löschen. Wenn Sie einen Snapshot permanent wiederherstellen, wird er aus der Archivstufe entfernt.

Wenn Sie einen Snapshot temporär wiederherstellen, wird er für einen von Ihnen angegebenen Wiederherstellungszeitraum von der Archivstufe auf die Standardstufe kopiert. Der Snapshot

bleibt nur für die Dauer des Wiederherstellungszeitraums wiederhergestellt und kann nur in dieser Zeit verwendet werden. Während des Wiederherstellungszeitraums verbleibt eine Kopie des Snapshots auf der Archivstufe. Nach Ablauf des Zeitraums wird der Snapshot automatisch aus der Standardstufe entfernt. Während des Wiederherstellungszeitraums können Sie den Wiederherstellungszeitraum jederzeit verlängern oder verkürzen oder den Wiederherstellungstyp zu „Permanent“ ändern. Weitere Informationen finden Sie unter Ändern Sie den Wiederherstellungszeitraum für einen vorübergehend wiederhergestellten Amazon EBS-Snapshot.

Wenn Sie Snapshots wiederherstellen, die einem deaktivierten AMI zugeordnet sind, und Sie beabsichtigen, dieses AMI zu verwenden, müssen Sie zuerst alle zugehörigen Snapshots dauerhaft wiederherstellen und dann ein deaktiviertes AMI erneut aktivieren, bevor Sie es verwenden können. Sie können ein AMI nicht aktivieren, wenn die zugehörigen Snapshots vorübergehend wiederhergestellt werden. Verwenden Sie den folgenden Befehl, um alle Snapshots zu finden, die einem AMI zugeordnet sind.

```
aws ec2 describe-images --image-id ami_id \
  --query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

Console

So stellen Sie einen Snapshot aus dem Archiv wieder her:

Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.

1. Wählen Sie im Navigationsbereich die Option Snapshots.
2. Wählen Sie in der Liste der Snapshots den wiederherzustellenden archivierten Snapshot aus, und wählen Sie dann Aktionen, Snapshot aus Archiv wiederherstellen.
3. Geben Sie den Typ der durchzuführenden Wiederherstellung an. Führen Sie für Wiederherstellungstyp eine der folgenden Aktionen aus:
   - Um den Snapshot dauerhaft wiederherzustellen, wählen Sie Permanent.
   - Um den Snapshot vorübergehend wiederherzustellen, wählen Sie Temporary (Temporär) und geben Sie dann für Temporary restore period (Temporärer Wiederherstellungszeitraum) die Anzahl der Tage ein, für die der Snapshot wiederhergestellt werden soll.
4. Wählen Sie zur Bestätigung Snapshot wiederherstellen.

AWS CLI

So stellen Sie einen archivierten Snapshot dauerhaft wieder her:

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-tier.html AWS CLI restore-snapshot-tier mit der Option. `--permanent-restore` Geben Sie für `--snapshot-id` die ID des wiederherzustellenden Snapshots an.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --permanent-restore
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "IsPermanentRestore": true
}
```

So stellen Sie einen archivierten Snapshot temporär wieder her:

Verwenden Sie den AWS CLI Befehl restore-snapshot-tier. Lassen Sie die `--permanent-restore`-Option weg. Geben Sie für die Anzahl der Tage an`--temporary-restore-days`, für die der Snapshot wiederhergestellt werden soll. Der zulässige Bereich liegt zwischen 1 und 180 Tagen. Wenn Sie keinen Wert angeben, ist der Standardwert 1 Tag.

Im folgenden Beispiel wird der angegebene Snapshot vorübergehend für einen Wiederherstellungszeitraum von 5 Tagen wiederhergestellt.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --temporary-restore-days 5
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

PowerShell

So stellen Sie einen archivierten Snapshot dauerhaft wieder her:

Verwenden Sie das cmdlet Restore-EC2SnapshotTier.

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -PermanentRestore $true
```

So stellen Sie einen archivierten Snapshot temporär wieder her:

Verwenden Sie das cmdlet Restore-EC2SnapshotTier.

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -TemporaryRestoreDays 5
```

Ändern Sie den Wiederherstellungszeitraum für einen vorübergehend wiederhergestellten Amazon EBS-Snapshot

Wenn Sie einen Snapshot temporär wiederherstellen, müssen Sie die Anzahl der Tage angeben, für die der Snapshot in Ihrem Konto wiederhergestellt bleiben soll. Nach Ablauf des Wiederherstellungszeitraums wird der Snapshot automatisch aus der Standardstufe entfernt.

Sie können den Wiederherstellungszeitraum eines temporär wiederhergestellten Snapshots jederzeit ändern.

Sie können den Wiederherstellungszeitraum verlängern oder verkürzen oder den Wiederherstellungstyp von „Temporär“ zu „Permanent“ ändern.

Wenn Sie den Wiederherstellungszeitraum ändern, gilt der neue Wiederherstellungszeitraum ab dem aktuellen Datum. Wenn Sie beispielsweise einen neuen Wiederherstellungszeitraum von 5 Tagen angeben, bleibt der Snapshot ab dem aktuellen Datum fünf Tage lang wiederhergestellt.

> **Note**
>
> Sie können eine temporäre Wiederherstellung vorzeitig beenden, indem Sie den Wiederherstellungszeitraum auf 1 Tag festlegen.

Wenn Sie den Wiederherstellungstyp von „Temporär“ zu „Permanent“ ändern, wird die Snapshot-Kopie aus der Archivstufe gelöscht und der Snapshot bleibt in Ihrem Konto verfügbar, bis Sie ihn manuell erneut archivieren oder löschen.

Console

So ändern Sie den Wiederherstellungszeitraum oder den Wiederherstellungstyp:

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie in der Liste der Snapshots den Snapshot aus, den Sie zuvor temporär wiederhergestellt haben, und wählen Sie dann Aktionen, Snapshot aus Archiv wiederherstellen.
4. Führen Sie für Wiederherstellungstyp eine der folgenden Aktionen aus:
   - Um den Wiederherstellungstyp von „Temporär“ in „Permanent“ zu ändern, wählen Sie Permanent aus.
   - Um den Wiederherstellungszeitraum zu verlängern oder zu verkürzen, behalten Sie Temporary (Temporär) bei, und geben Sie dann für Temporary restore period (Temporärer Wiederherstellungszeitraum) den neuen Wiederherstellungszeitraum in Tagen ein.
5. Wählen Sie zur Bestätigung Snapshot wiederherstellen.

AWS CLI

So ändern Sie den Wiederherstellungszeitraum oder den Wiederherstellungstyp:

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-tier.html restore-snapshot-tier. Geben Sie für `--snapshot-id` die ID des Snapshots an, den Sie zuvor temporär wiederhergestellt haben. Um den Wiederherstellungstyp von „Temporär“ in „Permanent“ zu ändern, geben Sie `--permanent-restore` an und lassen Sie `--temporary-restore-days` weg. Um den Wiederherstellungszeitraum zu verlängern oder zu verkürzen, lassen Sie `--permanent-restore` weg und geben Sie für `--temporary-restore-days` den neuen Wiederherstellungszeitraum in Tagen an.

Beispiel: Verlängern oder Verkürzen des Wiederherstellungszeitraums

Mit dem folgenden Befehl wird der Wiederherstellungszeitraum für den angegebenen Snapshot auf Tage geändert. `10`

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --temporary-restore-days 10
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

Beispiel: Ändern des Wiederherstellungstyps in „Permanent“

Mit dem folgenden Befehl wird der Wiederherstellungstyp für den angegebenen Snapshot von temporär zu permanent geändert.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --permanent-restore
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "IsPermanentRestore": true
}
```

PowerShell

So ändern Sie den Wiederherstellungszeitraum oder den Wiederherstellungstyp:

Verwenden Sie das cmdlet Restore-EC2SnapshotTier. Geben Sie für `-SnapshotId` die ID des Snapshots an, den Sie zuvor temporär wiederhergestellt haben. Um den Wiederherstellungstyp von „Temporär“ in „Permanent“ zu ändern, geben Sie `-PermanentRestore` an und lassen Sie `-TemporaryRestoreDays` weg. Um den Wiederherstellungszeitraum zu verlängern oder zu verkürzen, lassen Sie `-PermanentRestore` weg und geben Sie für `-TemporaryRestoreDays` den neuen Wiederherstellungszeitraum in Tagen an.

Beispiel: Verlängern oder Verkürzen des Wiederherstellungszeitraums

Mit dem folgenden Befehl wird der Wiederherstellungszeitraum für den angegebenen Snapshot auf `10` Tage geändert.

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -TemporaryRestoreDays 10
```

Beispiel: Ändern des Wiederherstellungstyps in „Permanent“

Mit dem folgenden Befehl wird der Wiederherstellungstyp für den angegebenen Snapshot von temporär zu permanent geändert.

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -PermanentRestore $true
```

Archivierte Amazon EBS-Snapshots anzeigen

Console

So zeigen Sie Informationen zur Speicherebene für einen Snapshot an:

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie in der Liste der Snapshots den Snapshot aus und wählen Sie die Registerkarte Speicher-Kontingent.

   Die Registerkarte enthält die folgenden Informationen:

   - Last tier change started on (Letzte Stufenänderung begann am) – Das Datum und die Uhrzeit, zu der die letzte Archivierung oder Wiederherstellung gestartet wurde.
   - Tier change progress (Fortschritt der Stufenänderung) – Prozentangabe für den Fortschritt der letzten Archivierungs- oder Wiederherstellungsaktion.
   - Speicher-Kontingent – Die Speicherebene des Snapshots. Immer `archive` für archivierte Snapshots und `standard` für Snapshots, die auf der Standardstufe gespeichert sind, einschließlich temporär wiederhergestellter Snapshots.
   - Tiering status (Stufenstatus) – Der Status der letzten Archivierungs- oder Wiederherstellungsaktion.

- Archive completed on (Archiv abgeschlossen am) – Das Datum und die Uhrzeit, zu der das Archiv abgeschlossen wurde.
- Temporary restore expires on (Ablauf der temporären Wiederherstellung) – Das Datum und die Uhrzeit, zu der ein temporär wiederhergestellter Snapshot abläuft.

AWS CLI

So zeigen Sie Archivinformationen zu einem archivierten Snapshot an:

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-snapshot-tier-status.html describe-snapshot-tier-status. Geben Sie den `snapshot-id`-Filter und für den Filterwert die Snapshot-ID an. Alternativ können Sie den Filter weglassen, um alle archivierten Snapshots anzuzeigen.

```
--filters "Name=snapshot-id, Values=snapshot_id"
```

Die Ausgabe enthält die folgenden Antwortparameter:

- `Status` – Der Status des Snapshots. Immer `completed` für archivierte Snapshots. Es können nur Snapshots archiviert werden, die den Status `completed` haben.
- `LastTieringStartTime`— Datum und Uhrzeit, zu denen der Archivierungsvorgang gestartet wurde, im UTC-Zeitformat (). YYYY-MM-DDTHH:MM:SSZ
- `LastTieringOperationState` – Der aktuelle Status des Archivierungsvorgangs. Beispiele für mögliche Statusangaben: `archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- `LastTieringProgress` – Der Fortschritt des Snapshot-Archivierungsvorgangs in Prozent.
- `StorageTier` – Die Speicherebene für den Snapshot. Immer `archive` für archivierte Snapshots und `standard` für Snapshots, die auf der Standardstufe gespeichert sind, einschließlich temporär wiederhergestellter Snapshots.
- `ArchivalCompleteTime`— Datum und Uhrzeit des Abschlusses des Archivierungsvorgangs im UTC-Zeitformat ()YYYY-MM-DDTHH:MM:SSZ.

Beispiel: Beschreiben Sie einen Snapshot

Im folgenden Beispiel werden Informationen zum angegebenen Snapshot angezeigt.

```
aws ec2 describe-snapshot-tier-status \
    --filters "Name=snapshot-id, Values=snap-0abcdef1234567890"
```

Es folgt eine Beispielausgabe.

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcdef",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-0abcdef1234567890",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

So zeigen Sie archivierte und Standardstufen-Snapshots an:

Verwenden Sie den Befehl describe-snapshots. Geben Sie für `--snapshot-ids` die ID des Snapshots an.

```
aws ec2 describe-snapshots --snapshot-ids snap-0abcdef1234567890
```

Es folgt eine Beispielausgabe. Der Antwortparameter `StorageTier` gibt an, ob der Snapshot derzeit archiviert ist. `archive` bedeutet, dass der Snapshot derzeit archiviert und auf der Archivstufe gespeichert ist, und `standard` gibt an, dass der Snapshot derzeit nicht archiviert ist und dass er auf der Standardstufe gespeichert ist.

In der folgenden Beispielausgabe ist nur `Snap A` archiviert. `Snap B` und `Snap C` sind nicht archiviert.

Außerdem wird der Antwortparameter `RestoreExpiryTime` nur für Snapshots zurückgegeben, die temporär aus dem Archiv wiederhergestellt werden. Er zeigt an, wann temporär

wiederhergestellte Snapshots automatisch aus der Standardstufe entfernt werden sollen. Es wird nicht für Snapshots zurückgegeben, die permanent wiederhergestellt werden.

Im folgenden Beispiel wird die Ausgabe vorübergehend wiederhergestellt und am 19.09.2021 T21:00:00.000Z (19. September 2021 um 21:00 Uhr UTC) automatisch aus der Standardstufe entfernt. `Snap C`


```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
```

```
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
}
```

So zeigen Sie nur Snapshots an, die auf der Archiv- oder Standardstufe gespeichert sind

Verwenden Sie den Befehl describe-snapshots. Schließen Sie die `--filter` Option zusammen mit dem Filternamen ein. `storage-tier` Geben Sie für den Filterwert entweder `archive` oder an`standard`. Im folgenden Beispiel werden nur archivierte Snapshots angezeigt.

```
aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

PowerShell

So zeigen Sie Archivinformationen zu einem archivierten Snapshot an

Verwenden Sie das cmdlet Get-EC2SnapshotTierStatus.

```
Get-EC2SnapshotTierStatus `
    -Filter @{Name="snapshot-id"; Values="snap-0abcdef1234567890"}
```

So zeigen Sie archivierte und Standardstufen-Snapshots an:

Verwenden Sie das cmdlet Get-EC2Snapshot.

```
Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890
```

So zeigen Sie nur Snapshots an, die auf der Archiv- oder Standardstufe gespeichert sind

Verwenden Sie das cmdlet Get-EC2Snapshot. Im folgenden Beispiel werden nur archivierte Snapshots angezeigt.

```
Get-EC2Snapshot `
    -Filter @{Name="storage-tier"; Values="archive"}
```

Überwachen Sie die Amazon EBS-Snapshot-Archivierung mithilfe von Events CloudWatch

Amazon EBS sendet Ereignisse im Zusammenhang mit Snapshot-Archivierungsaktionen aus. Sie können Amazon CloudWatch Events verwenden AWS Lambda , um Ereignisbenachrichtigungen programmgesteuert zu verarbeiten. Ereignisse werden auf bestmögliche Weise ausgegeben. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Die folgenden Ereignisse sind verfügbar:

- `archiveSnapshot` – Wird ausgegeben, wenn eine Snapshot-Archivierungsaktion erfolgreich ist oder fehlschlägt.

  Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine Snapshot-Archivierungsaktion erfolgreich ausgeführt wird.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

  Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine Snapshot-Archivierungsaktion fehlschlägt.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `permanentRestoreSnapshot` – Wird ausgegeben, wenn eine permanente Wiederherstellungsaktion erfolgreich ist oder fehlschlägt.

  Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine permanente Wiederherstellungsaktion erfolgreich ausgeführt wird.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
```

```
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine permanente Wiederherstellungsaktion fehlschlägt.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `temporaryRestoreSnapshot` – Wird ausgegeben, wenn eine temporäre Wiederherstellungsaktion erfolgreich ist oder fehlschlägt.

  Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine temporäre Wiederherstellungsaktion erfolgreich ausgeführt wird.

```
{
```

```
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

Nachstehend finden Sie ein Beispiel für ein Ereignis, das ausgegeben wird, wenn eine temporäre Wiederherstellungsaktion fehlschlägt.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
```

```
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `restoreExpiry` – Wird ausgegeben, wenn der Wiederherstellungszeitraum für einen temporär wiederhergestellten Snapshot abläuft.

  Im Folgenden wird ein -Beispiel gezeigt.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

Löschen eines Amazon EBS-Snapshots

Wenn Sie einen Amazon EBS-Snapshot eines Volumes nicht mehr benötigen, können Sie ihn löschen. Das Löschen eines Snapshots hat keine Auswirkungen auf das Volume. Das Löschen eines Volumes hat keine Auswirklungen auf die Snapshots, die von diesem Volume erstellt wurden.

Themen

- Überlegungen zum Löschen von Snapshots
- So funktioniert das Löschen inkrementeller Snapshots
- Löschen eines Snapshots
- Löschen Sie Snapshots mit mehreren Volumes

Überlegungen zum Löschen von Snapshots

Für das Löschen von Snapshots gelten die folgenden Überlegungen:

- Sie können einen Snapshot des Stammgeräts eines EBS-Volumes, das von einem registrierten AMI verwendet wird, nicht löschen. Diese Überlegung gilt auch dann, wenn das registrierte AMI veraltet oder deaktiviert ist. Sie müssen die Registrierung des AMI zunächst aufheben, bevor Sie den Snapshot löschen können. Weitere Informationen finden Sie unter Abmelden Ihres AMI.
- Sie können einen Snapshot, der vom AWS Backup Service mithilfe von Amazon EC2 verwaltet wird, nicht löschen. Verwenden Sie stattdessen, AWS Backup um die entsprechenden Wiederherstellungspunkte im Backup-Tresor zu löschen. Weitere Informationen finden Sie unter Löschen von Backups im AWS Backup Entwickler-Leitfaden.
- Sie können Snapshots manuell erstellen, beibehalten und löschen oder Amazon Data Lifecycle Manager Ihre Snapshots für Sie verwalten lassen. Weitere Informationen finden Sie unter Amazon Data Lifecycle Manager.
- Sie können zwar einen Snapshot löschen, der noch in Bearbeitung ist, aber der Snapshot muss fertiggestellt sein, bevor der Löschvorgang wirksam wird. Das könnte eine lange Zeit dauern. Wenn Sie zudem Ihre Beschränkung für gleichzeitige Snapshots erreicht haben und versuchen, einen weiteren Snapshot zu erstellen, wird u. U. der Fehler `ConcurrentSnapshotLimitExceeded` ausgegeben. Weitere Informationen finden Sie in den Servicekontingenten für Amazon EBS im Allgemeine Amazon Web Services-Referenz.
- Wenn Sie einen Snapshot löschen, der einer Aufbewahrungsregel für den Papierkorb entspricht, wird der Snapshot im Papierkorb aufbewahrt und nicht sofort gelöscht. Weitere Informationen finden Sie unter Papierkorb.
- Sie können keine Snapshots löschen, die mit deaktivierten EBS-backed AMIs verknüpft sind. Weitere Informationen finden Sie unter AMI https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/disable-an-ami.html deaktivieren.
- Sie können keine Schnappschüsse löschen, die mit Ihnen geteilt wurden.
- Wenn Sie einen geteilten Snapshot löschen, dessen Eigentümer Sie sind, verlieren alle Konten, mit denen der Snapshot geteilt wurde, den Zugriff darauf.

So funktioniert das Löschen inkrementeller Snapshots

Wenn Sie regelmäßig Snapshots von einem Volume erstellen, sind die Snapshots inkrementell. In dem neuen Snapshot werden nur die Blöcke auf dem Gerät gespeichert, die sich seit dem letzten Snapshot geändert haben. Obwohl Snapshots inkrementell gespeichert werden, ist der Löschungsprozess von Snapshots derart beschaffen, dass Sie nur den aktuellen Snapshot benötigen, um Volumes zu erstellen.

Falls Daten, die in einem Volume in einem ehemaligen Snapshot oder in einer Reihe ehemaliger Snapshots verfügbar waren, und die Daten anschließend zu einem späteren Zeitpunkt im betreffenden Volume gelöscht wurden, werden die Daten weiterhin als eindeutige Daten der ehemaligen Snapshots angesehen. Eindeutige Daten werden nur aus der Sequenz der Snapshots gelöscht, nachdem alle Snapshots, die auf diese eindeutigen Daten verweisen, gelöscht wurden.

Wenn Sie einen Snapshot löschen, werden nur die exklusiv von diesem Snapshot referenzierten Daten entfernt. Eindeutige Daten werden nur gelöscht, wenn alle Snapshots, die darauf verweisen, gelöscht werden. Das Löschen von vorherigen Snapshots eines Volumes hat keinen Einfluss auf die Erstellung von Volumes aus späteren Snapshots des Volumes.

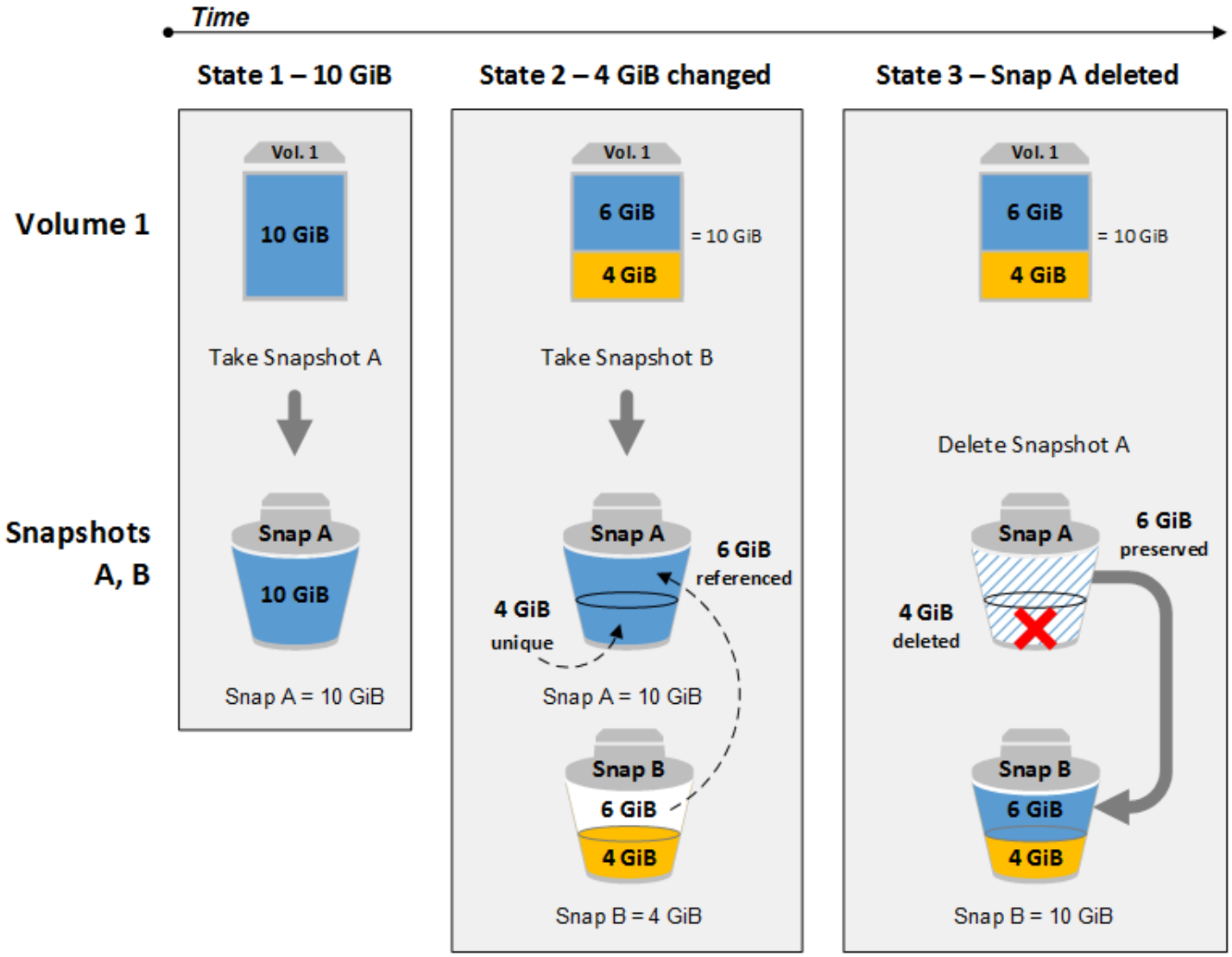
Das Löschen eines Snapshots führt möglicherweise nicht zu einer Reduzierung der Datenspeicherkosten Ihrer Organisation. Andere Snapshots verweisen ggf. auf die Daten dieses Snapshots und referenzierte Daten bleiben immer erhalten. Wenn Sie einen Snapshot löschen, der Daten enthält, die von einem späteren Snapshot verwendet werden, werden die mit den referenzierten Daten verknüpften Kosten dem späteren Snapshot zugeordnet. Weitere Informationen zur Datenspeicherung von Snapshots erhalten Sie unter So funktionieren Amazon EBS-Snapshots sowie im nachfolgenden Beispiel.

Im folgenden Diagramm wird Volume 1 an drei verschiedenen Zeitpunkten dargestellt. Ein Snapshot hat die ersten beiden Status erfasst. Im dritten Fall wurde ein Snapshot gelöscht.

- Im Status 1 enthält das Volume 10 GiB an Daten. Da Snap A der erste Snapshot für dieses Volume ist, müssen die gesamten 10 GiB an Daten kopiert werden. In diesem Zustand wird Ihnen das Speichern von 10 GiB an Snapshot-Daten in Rechnung gestellt.
- Im Status 2 enthält das Volume immer noch 10 GiB an Daten, aber 4 GiB haben sich geändert. Snap B speichert nur die 4 GiB, die sich nach der Aufnahme von Snap A geändert haben, und verweist auf die 6 GiB unveränderter Daten, die bereits in Snap A gespeichert sind. In diesem Zustand wird Ihnen das Speichern von 14 GiB an Snapshot-Daten in Rechnung gestellt (10 GB von Snap A + 4 GiB von Snap B).

- In Status 3 ist das Volume unverändert, Snap A wird jedoch gelöscht. Da Snap B immer noch auf die 6 GiB unveränderter Daten in Snap A verweist, werden diese Daten beibehalten und Snap B zugeordnet. Die 4 GiB an eindeutigen Daten in Snap A werden gelöscht, da sie nicht mehr von anderen Snapshots referenziert werden. In diesem Zustand wird Ihnen das Speichern von 10 GiB an Snapshot-Daten in Rechnung gestellt (6 GiB an Daten, die in Snap A gespeichert wurden, plus 4 GiB an Daten in Snap B).

Löschen eines Snapshots, bei dem ein Teil seiner Daten von einem anderen Snapshot referenziert wird



Löschen eines Snapshots

Console

So löschen Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus.
4. Wählen Sie Aktionen, Snapshot löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

AWS CLI

So löschen Sie einen Snapshot

Verwenden Sie den Befehl delete-snapshot .

```
aws ec2 delete-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

So löschen Sie einen Snapshot

Verwenden Sie das cmdlet Remove-EC2Snapshot.

```
Remove-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

> **Tipp zur Problembehebung**
>
> Wenn Sie eine `Failed to delete snapshot` Fehlermeldung erhalten, die darauf hinweist, dass der Snapshot derzeit von einem AMI verwendet wird, müssen Sie das zugehörige AMI deregistrieren, bevor Sie den Snapshot löschen können. Sie können keine Snapshots löschen, die mit einem AMI verbunden sind.

Wenn Sie die Konsole verwenden und das zugehörige AMI deaktiviert ist, müssen Sie auf dem AMI-Bildschirm den Filter Deaktivierte Bilder auswählen, um deaktivierte AMIs anzuzeigen.

Löschen Sie Snapshots mit mehreren Volumes

Zum Löschen von Multi-Volume-Snapshots rufen Sie mithilfe des Tags, das Sie beim Erstellen der Snapshots auf die Multi-Volume angewendet haben, alle Snapshots für Ihre Multi-Volume-Reihe ab. Löschen Sie anschließend die Snapshots einzeln.

Es ist möglich, einzelne Snapshots in der Multi-Volume-Snapshot-Reihe zu löschen. Wenn Sie einen Snapshot löschen, während er sich im `pending state` befindet, wird nur dieser Snapshot gelöscht. Die anderen Snapshots im Multi-Volumes-Snapshot-Set werden weiterhin erfolgreich abgeschlossen.

Schnelle Amazon EBS-Snapshot-Wiederherstellung

Mit der schnellen Amazon EBS-Snapshot-Wiederherstellung können Sie ein Volume aus einem Snapshot erstellen, das bei der Erstellung vollständig initialisiert wird. Dadurch entfällt die Latenz von I/O Vorgängen auf einem Block, wenn er zum ersten Mal aufgerufen wird. Volumes, die mit schneller Snapshot-Wiederherstellung erstellt wurden, stellen umgehend ihre gesamte bereitgestellt Leistung zur Verfügung.

Zum Einstieg aktivieren Sie die schnelle Snapshot-Wiederherstellung für bestimmte Snapshots in bestimmten Availability Zones. Jedes Snapshot- und Availability Zone-Paar bezieht sich auf eine schnelle Snapshot-Wiederherstellung. Wenn Sie ein Volume aus einem dieser Snapshots in einer der aktivierten Availability Zones erstellen, wird das Volume mithilfe der schnellen Snapshot-Wiederherstellung wiederhergestellt.

Sie müssen die schnelle Snapshot-Wiederherstellung für jeden Snapshot explizit aktivieren. Wenn Sie beispielsweise einen neuen Snapshot von einem Volume erstellen, das aus einem Snapshot mit Aktivierung der schnellen Snapshot-Wiederherstellung wiederhergestellt wurde, wird der neue Snapshot nicht automatisch für die schnelle Snapshot-Wiederherstellung aktiviert. Wenn Sie einen Snapshot kopieren, der für die schnelle Snapshot-Wiederherstellung aktiviert ist, wird die Snapshot-Kopie nicht automatisch für die schnelle Snapshot-Wiederherstellung aktiviert.

Die Anzahl der Volumes, die Sie mit den vollständigen Leistungsvorteilen der schnellen Snapshot-Wiederholung wiederherstellen können, wird durch die Guthaben zur Volume-Erstellung für den

Snapshot bestimmt. Weitere Informationen finden Sie unter Amazon EBS, Guthaben für die schnelle Snapshot-Wiederherstellung, Erstellung von Volumes.

Sie können die schnelle Snapshot-Wiederherstellung für Snapshots aktivieren, die Sie besitzen, sowie für öffentliche und private Snapshots, die für Sie freigegeben werden.

Inhalt

- Überlegungen
- Preise und Fakturierung
- Amazon EBS, Guthaben für die schnelle Snapshot-Wiederherstellung, Erstellung von Volumes
- Konfigurieren Sie die schnelle Snapshot-Wiederherstellung für einen Amazon EBS-Snapshot
- Überprüfen Sie den Status der schnellen Snapshot-Wiederherstellung für einen Amazon EBS-Snapshot
- Zeigen Sie Amazon EBS-Volumes an, die mithilfe der schnellen Snapshot-Wiederherstellung wiederhergestellt wurden

Überlegungen

- Die schnelle Snapshot-Wiederherstellung wird mit AWS Outposts Local Zones und Wavelength Zones nicht unterstützt.
- Die schnelle Snapshot-Wiederherstellung kann für Snapshots mit einer Größe von 16 TiB oder weniger aktiviert werden.
- Volumes, die mit einer Leistung von bis zu 64.000 IOPS und einem MiB/s Durchsatz von 1.000 IOPS ausgestattet sind, profitieren von den vollen Leistungsvorteilen einer schnellen Snapshot-Wiederherstellung. Für Volumes, die mit einer Leistung von mehr als 64.000 IOPS oder einem MiB/s Durchsatz von 1.000 IOPS bereitgestellt werden, empfehlen wir, das Volume zu initialisieren, um die volle Leistung zu erhalten.
- Pro Region können Sie bis zu 5 Snapshots für eine schnelle Snapshot-Wiederherstellung aktivieren. Das Kontingent gilt für Snapshots, die Sie besitzen, und Snapshots, die für Sie freigegeben werden. Wenn Sie die schnelle Snapshot-Wiederherstellung für einen für Sie freigegebenen Snapshot aktivieren, werden auf Ihr Kontingent für schnelle Snapshot-Wiederherstellung angerechnet. Sie werden nicht auf das Kontingent für schnelle Snapshot-Wiederherstellung des Besitzers des Snapshot angerechnet.

- Amazon EBS gibt CloudWatch Amazon-Ereignisse aus, wenn sich der Status der schnellen Snapshot-Wiederherstellung für einen Snapshot ändert. Weitere Informationen finden Sie unter EBS – schnelle Snapshot-Wiederherstellungsereignisse.

Preise und Fakturierung

Es wird Ihnen jede Minute in Rechnung gestellt, in der die schnelle Snapshot-Wiederherstellung für einen Snapshot in einer bestimmten Availability Zone aktiviert ist. Die Gebühren werden mit mindestens einer Stunde anteilig bewertet.

Wenn Sie beispielsweise die schnelle Snapshot-Wiederherstellung für einen Snapshot in `US-East-1a` für einen Monat (30 Tage) aktivieren, werden Ihnen 540 USD (1 Snapshot x 1 AZ x `720` Stunden x `$0.75` pro Stunde) in Rechnung gestellt. Wenn Sie die schnelle Snapshot-Wiederherstellung für zwei Snapshots in `us-east-1a`, `us-east-1b`, und `us-east-1c` für denselben Zeitraum aktivieren, werden Ihnen 3 240 USD (2 Snapshots x `3` AZs x `720` Stunden x `$0.75` pro Stunde) in Rechnung gestellt.

Wenn Sie die schnelle Snapshot-Wiederherstellung für einen öffentlichen oder privaten Snapshot aktivieren, der für Sie freigegeben wird, wird dies Ihrem Konto in Rechnung gestellt. Dem Besitzer des Snapshot wird nichts in Rechnung gestellt. Wenn ein Snapshot, der für Sie freigegeben wird, vom Snapshot-Besitzer gelöscht oder freigegeben wird, wird die schnelle Snapshot-Wiederherstellung für den Snapshot in Ihrem Konto deaktiviert, und die Abrechnung wird beendet.

Weitere Informationen finden Sie unter Amazon EBS – Preise.

Amazon EBS, Guthaben für die schnelle Snapshot-Wiederherstellung, Erstellung von Volumes

Die Anzahl der Volumes, die die vollständigen Leistungsvorteile der schnellen Snapshot-Wiederholung erhalten, wird von der Menge der Guthaben zum Erstellen eines Volumes für den Snapshot bestimmt. Es gibt pro Snapshot und Availability Zone einen Guthaben-Bucket. Jedes Volume, das Sie von einem Snapshot mit aktivierter schneller Snapshot-Wiederherstellung erstellen, verbraucht ein Guthabenpunkt vom Guthaben-Bucket. Sie müssen über mindestens ein Guthaben im Bucket verfügen, um aus dem Snapshot ein initialisiertes Volume erstellen zu können. Wenn Sie ein Volume erstellen, aber weniger als ein Guthaben im Bucket enthalten ist, wird das Volumen ohne den Vorteil einer schnellen Snapshot-Wiederherstellung erstellt.

Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktivieren, der für Sie freigegeben wird, erhalten Sie einen separaten Kredit-Bucket für den freigegebenen Snapshot in Ihrem Konto. Wenn Sie Volumes aus dem freigegebenen Snapshot erstellen, werden die Guthaben aus Ihrem Kredit-Bucket verbraucht; sie werden nicht aus dem Kredit-Bucket des Snapshot-Besitzers verbraucht.

Die Größe des Kredit-Buckets und die Refill-Rate basieren auf der Größe des Snapshots (die auch der Größe des Quell-Volumes entspricht), nicht auf der Größe der Snapshot-Daten. Wenn Sie beispielsweise einen Snapshot von einem 200-GiB-Volume mit 150 GiB an Daten erstellen und ihn für die schnelle Snapshot-Wiederherstellung aktivieren, basieren die Kreditgröße und die Refill-Rate auf 200 GiB.

Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktivieren, hat der Guthaben-Bucket zu Beginn kein Guthaben und er wird mit einer festgelegten Rate gefüllt, bis er seine maximale Guthabenkapazität erreicht hat. Wenn Sie Guthaben verbrauchen, wird der Guthaben-Bucket im Laufe der Zeit ebenfalls wieder gefüllt, bis er seine maximale Guthabenkapazität erreicht.

Die Füllrate für einen Guthaben-Bucket wird wie folgt berechnet:

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

Die Größe des Guthaben-Buckets wird wie folgt berechnet:

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

Beispiel: Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot mit einer Größe von `128 GiB` aktivieren, werden `0.1333` Guthaben pro Minute aufgefüllt.

```
MIN (10, (1024 ÷ 128))
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

Die maximale Größe des Guthaben-Buckets liegt in diesem Fall bei 8 Guthaben.

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
 = MAX (1, 8)
 = 8 credits
```

Wenn Sie in diesem Beispiel die schnelle Snapshot-Wiederherstellung aktivieren, enthält der Guthaben-Bucket zu Beginn kein Guthaben. Nach 8 Minuten ist genügend Guthaben im Bucket, um ein initialisiertes Volume (`0.1333 credits × 8 minutes = 1.066 credits`) zu erstellen. Wenn der Guthaben-Bucket voll ist, können Sie 8 initialisierte Volumes gleichzeitig erstellen (8 Guthaben). Solange die maximale Kapazität des Buckets noch nicht erreicht ist, wird er mit `0.1333` Guthaben pro Minute aufgefüllt.

Mithilfe von CloudWatch Kennzahlen können Sie die Größe Ihrer Kredit-Buckets und die Anzahl der in jedem Bucket verfügbaren Credits überwachen. Weitere Informationen finden Sie unter Metriken für die schnelle Snapshot-Wiederherstellung.

Nachdem Sie ein Volume aus einem Snapshot mit aktivierter schneller Snapshot-Wiederherstellung erstellt haben, können Sie das Volume mit describe-volumes beschreiben und im Feld `fastRestored` in der Ausgabe prüfen, ob das Volume als initialisiertes Volume mit schneller Snapshot-Wiederherstellung erstellt wurde.

Konfigurieren Sie die schnelle Snapshot-Wiederherstellung für einen Amazon EBS-Snapshot

Die schnelle Snapshot-Wiederherstellung ist für einen Snapshot standardmäßig deaktiviert. Sie können die schnelle Snapshot-Wiederherstellung für Snapshots, die Sie besitzen, und für Snapshots, die für Sie freigegeben werden, aktivieren oder deaktivieren. Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktivieren oder deaktivieren, gelten die Änderungen nur für Ihr Konto.

> **Note**
>
> Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktivieren, wird Ihrem Konto jede Minute in Rechnung gestellt, in der die schnelle Snapshot-Wiederherstellung in einer bestimmten Availability Zone aktiviert ist. Die Gebühren werden mit mindestens einer Stunde anteilig bewertet.

Wenn Sie einen Snapshot löschen, den Sie besitzen, wird die schnelle Snapshot-Wiederherstellung für diesen Snapshot in Ihrem Konto automatisch deaktiviert. Wenn Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktiviert haben, der für Sie freigegeben ist, und der Snapshot-Besitzer diesen löscht oder die Freigabe aufhebt, wird die schnelle Snapshot-Wiederherstellung für den freigegebenen Snapshot in Ihrem Konto automatisch deaktiviert.

Wenn Sie die schnelle Snapshot-Wiederherstellung für einen für Sie freigegebenen Snapshot aktiviert haben und dieser mit einem benutzerdefinierten CMK verschlüsselt ist, wird die schnelle Snapshot-Wiederherstellung nicht automatisch für den Snapshot deaktiviert, wenn der Snapshot-Besitzer Ihren Zugriff auf das benutzerdefinierte CMK aufhebt. Sie müssen die schnelle Snapshot-Wiederherstellung für diesen Snapshot manuell deaktivieren.

Nachdem Sie die schnelle Snapshot-Wiederherstellung für einen Snapshot aktiviert haben, tritt er in den `optimizing`-Status ein. Snapshots, die sich im `optimizing`-Status befinden, bieten einige Leistungsvorteile, wenn sie zur Wiederherstellung von Volumes verwendet werden. Sie bieten erst nach dem Eintritt in den `enabled`-Status die volle Leistungsvorteile der schnellen Snapshot-Wiederherstellung.

Console

Um die schnelle Snapshot-Wiederherstellung zu konfigurieren

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus und wählen Sie Aktionen, Verwalten der schnellen Snapshot-Wiederherstellung.
4. Im Bereich Einstellungen für die schnelle Snapshot-Wiederherstellung werden alle Availability Zones, lokalen Zonen und Wavelength-Zonen aufgelistet, in denen Sie die schnelle Snapshot-Wiederherstellung für den ausgewählten Snapshot aktivieren können. Das Volume Aktueller Status gibt an, ob die schnelle Snapshot-Wiederherstellung aktuell für die einzelnen Zonen aktiviert oder deaktiviert ist.

   Um die schnelle Snapshot-Wiederherstellung in einer Zone zu aktivieren, in der sie derzeit deaktiviert ist, wählen Sie die Zone aus, wählen Sie Aktivieren und wählen Sie dann zum Bestätigen Aktivieren aus.

   Um die schnelle Snapshot-Wiederherstellung in einer Zone zu deaktivieren, in der sie derzeit aktiviert ist, wählen Sie die Zone aus und wählen Sie dann Deaktivieren aus.
5. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, wählen Sie Schließen.

AWS CLI

So aktivieren Sie die schnelle Snapshot-Wiederherstellung

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/enable-fast-snapshot-restores.html enable-fast-snapshot-restore.

```
aws ec2 enable-fast-snapshot-restores \
    --availability-zones us-east-1a us-east-1b \
    --source-snapshot-ids snap-0abcdef1234567890
```

So deaktivieren Sie schnelle Snapshot-Wiederherstellung

Verwenden Sie den https://docs.aws.amazon.com/cli/latest/reference/ec2/disable-fast-snapshot-restores.html Befehl disable-fast-snapshot-restore.

```
aws ec2 disable-fast-snapshot-restores \
    --availability-zones us-east-1a \
    --source-snapshot-ids snap-0abcdef1234567890
```

Im folgenden Beispiel wird der Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-fast-snapshot-restores.html describe-fast-snapshot-restore verwendet, um Ihre deaktivierten schnellen Snapshot-Wiederherstellungen zu beschreiben.

```
aws ec2 describe-fast-snapshot-restores \
    --filters Name=state,Values=disabled
```

PowerShell

So aktivieren Sie die schnelle Snapshot-Wiederherstellung

Verwenden Sie das cmdlet Enable-EC2FastSnapshotRestore.

```
Enable-EC2FastSnapshotRestore `
    -AvailabilityZone us-east-1a us-east-1b `
    -SourceSnapshotId snap-0abcdef1234567890
```

So deaktivieren Sie schnelle Snapshot-Wiederherstellung

Verwenden Sie das cmdlet Disable-EC2FastSnapshotRestore.

```
Disable-EC2FastSnapshotRestore `
    -AvailabilityZone us-east-1a `
```

```
    -SourceSnapshotId snap-0abcdef1234567890
```

Im folgenden Beispiel wird das Get-EC2FastSnapshotRestore Cmdlet verwendet, um Ihre deaktivierten schnellen Snapshot-Wiederherstellungen zu beschreiben.

```
Get-EC2FastSnapshotRestore `
    -Filter @{Name="state"; Values="disabled"}
```

Überprüfen Sie den Status der schnellen Snapshot-Wiederherstellung für einen Amazon EBS-Snapshot

Die schnelle Snapshot-Wiederherstellung für einen Snapshot kann einen der folgenden Statuswerte haben.

- `enabling`: Es wurde eine Anfrage zur Aktivierung einer schnellen Snapshot-Wiederherstellung gestellt.
- `optimizing`: Schnelle Snapshot-Wiederherstellung wird aktiviert. Es dauert pro TiB 60 Minuten, um einen Snapshot zu optimieren. Snapshots in diesem Zustand bieten einen gewissen Leistungsvorteil bei der Wiederherstellung von Volumes.
- `enabled`: Schnelle Snapshot-Wiederherstellung ist aktiviert. Snapshots in diesem Zustand und mit ausreichenden Volumes Creation Credits bieten den vollen Leistungsvorteil bei der Wiederherstellung von Volumes.
- `disabling`: Es wurde eine Anfrage zur Deaktivierung der schnellen Snapshot-Wiederherstellung gestellt oder die Anfrage zur Aktivierung der schnellen Snapshot-Wiederherstellung ist fehlgeschlagen.
- `disabled`: Schnelle Snapshot-Wiederherstellung ist deaktiviert. Sie können die schnelle Snapshot-Wiederherstellung bei Bedarf erneut aktivieren.

Sie können den Status der schnellen Snapshot-Wiederherstellung für einen Snapshot, den Sie besitzen, oder für einen Snapshot, der mit Ihnen geteilt wird, anzeigen.

Console

Um den Status der schnellen Snapshot-Wiederherstellung anzuzeigen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus.
4. Auf der Registerkarte Details zeigt Schnelle Snapshot-Wiederherstellung den aktuellen Status der schnellen Snapshot-Wiederherstellung an.

AWS CLI

Um Snapshots mit aktivierter schneller Snapshot-Wiederherstellung anzuzeigen

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-fast-snapshot-restores.html describe-fast-snapshot-restore.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

Es folgt eine Beispielausgabe.

```
{
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        }
    ]
```

```
}
```

PowerShell

Um Snapshots mit aktivierter schneller Snapshot-Wiederherstellung anzuzeigen

Verwenden Sie das cmdlet Get-EC2FastSnapshotRestore.

```
Get-EC2FastSnapshotRestore `
    -Filter @{Name="state"; Values="enabled"}
```

Zeigen Sie Amazon EBS-Volumes an, die mithilfe der schnellen Snapshot-Wiederherstellung wiederhergestellt wurden

Wenn Sie ein Volume aus einem Snapshot erstellen, der für die schnelle Snapshot-Wiederherstellung in der Availability Zone für das Volume aktiviert ist, wird es mithilfe der schnellen Snapshot-Wiederherstellung wiederhergestellt.

AWS CLI

Um Volumes anzuzeigen, die aus einem Snapshot erstellt wurden, der für die schnelle Snapshot-Wiederherstellung aktiviert ist

Verwenden Sie den Befehl describe-volumes.

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

Es folgt eine Beispielausgabe.

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
```

```
            "SnapshotId": "snap-0abcdef1234567890",
            "State": "available",
            "VolumeId": "vol-01234567890abcdef",
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

PowerShell

Um Volumes anzuzeigen, die aus einem Snapshot erstellt wurden, der für die schnelle Snapshot-Wiederherstellung aktiviert ist

Verwenden Sie das cmdlet Get-EC2Volume.

```
Get-EC2Volume -Filter @{Name="fast-restored"; Values="true"}
```

Amazon-EBS-Snapshot-Sperre

Sie können Ihre Amazon-EBS-Snapshots sperren, um sie vor versehentlichem oder böswilligem Löschen zu schützen oder um sie für eine bestimmte Dauer im WORM-Format (write-once-read-many) zu speichern. Solange ein Snapshot gesperrt ist, kann er von keinem Benutzer gelöscht werden, unabhängig von dessen IAM-Berechtigungen. Sie können einen gesperrten Snapshot weiterhin genauso verwenden wie jeden anderen Snapshot.

> **Note**
>
> Die Snapshot-Sperre wurde von Cohasset Associates in Bezug auf die Verwendung in Umgebungen bewertet, die den Bestimmungen von SEC 17a-4, CFTC und FINRA unterliegen. Weitere Informationen zur Snapshot-Sperre im Zusammenhang mit diesen Bestimmungen finden Sie unter Compliance-Bewertung durch Cohasset Associates.

Sie können Snapshots in einem von zwei Modi sperren: im Compliance-Modus oder im Governance-Modus. Außerdem können Snapshots für eine bestimmte Dauer oder bis zu einem bestimmten Datum gesperrt werden. Weitere Informationen erhalten Sie unter Sperrmodus und Sperrdauer.

Preisgestaltung

Sie können Snapshots ohne zusätzliche Kosten sperren und entsperren. Sie zahlen die standardmäßigen Amazon-EBS-Snapshot-Speicherkosten für gesperrte Snapshots.

Themen

- Konzepte zum Sperren von Amazon EBS-Snapshots
- Überlegungen zur Amazon EBS-Snapshotsperre
- Kontrollieren Sie den Zugriff auf Amazon EBS Snapshot Lock
- Sperren Sie einen Amazon EBS-Snapshot
- Entsperren Sie einen Amazon EBS-Snapshot
- Aktualisieren Sie die Amazon EBS-Snapshot-Sperreinstellungen
- Überwachen Sie die Amazon EBS-Snapshotsperre

Konzepte zum Sperren von Amazon EBS-Snapshots

Im Folgenden finden Sie wichtige Konzepte, die Sie verstehen sollten, wenn Sie mit der Verwendung der Snapshot-Sperre beginnen.

Inhalt

- Sperrmodus
- Sperrdauer
- Cooling-off Zeitraum
- Sperrzustand

Sperrmodus

Sie können einen Snapshot in einem von zwei Modi sperren:

Governance-Modus

Nachdem ein Snapshot gesperrt wurde, können Benutzer mit entsprechenden IAM-Berechtigungen den Snapshot entsperren und den Sperrmodus sowie die Dauer oder das Ablaufdatum der Sperre jederzeit ändern. Wenn Sie einen Snapshot im Governance-Modus sperren, wird der Snapshot sofort

gesperrt. Es gibt keine Sperrfrist. Um einen Snapshot zu löschen, nachdem er im Governance-Modus gesperrt wurde, müssen Sie zuerst den Snapshot entsperren oder warten, bis die Sperre abläuft.

Sie können den Governance-Modus verwenden, um die Datenverwaltungsanforderungen Ihres Unternehmens zu erfüllen, indem Sie sicherstellen, dass nur bestimmte Benutzer dazu berechtigt sind, Snapshots zu entsperren und Snapshot-Sperrkonfigurationen zu ändern. Sie können den Governance-Modus außerdem verwenden, um Ihre Sperrkonfiguration zu testen, bevor Sie einen Snapshot im Compliance-Modus sperren.

Compliance-Modus

Wenn Sie einen Snapshot im Compliance-Modus sperren, können Sie optional eine Sperrfrist angeben, die unmittelbar nach dem Sperren des Snapshots beginnt. Während der Sperrfrist können Benutzer mit den entsprechenden Berechtigungen den Snapshot entsperren, den Sperrmodus ändern, die Sperrfrist verlängern oder verkürzen und die Sperrdauer oder das Ablaufdatum verlängern bzw. verkürzen. Nach Ablauf der Sperrfrist ist es nicht mehr möglich, den Snapshot zu entsperren, den Sperrmodus zu ändern oder die Sperrdauer oder das Ablaufdatum zu verringern. Sie können nur die Sperrdauer oder das Ablaufdatum erhöhen. Um einen Snapshot zu löschen, nachdem er im Compliance-Modus gesperrt wurde und die Sperrfrist abgelaufen ist, müssen Sie warten, bis die Sperre abgelaufen ist.

> **Note**
>
> Sie können einen Snapshot im Compliance-Modus ohne Sperrfrist sperren, indem Sie die Sperrfrist bei der Anfrage weglassen. In diesem Fall tritt die Sperre sofort in Kraft und es ist nicht mehr möglich, den Snapshot zu entsperren, den Sperrmodus zu ändern oder die Sperrdauer oder das Ablaufdatum zu verringern. Sie können nur die Sperrdauer oder das Ablaufdatum erhöhen.

Sie können den Compliance-Modus verwenden, um Snapshots zu schützen, die aus Compliance-Gründen für einen bestimmten Zeitraum nicht gelöscht werden dürfen. Der Compliance-Modus bietet die folgenden Vorteile:

- Er ermöglicht die WORM-Konfiguration (Write-Once, Read-Many) für Ihre Snapshots.
- Er bietet eine zusätzliche Schutzebene, die Snapshots vor versehentlichem oder böswilligem Löschen schützt.

- Er setzt Aufbewahrungsfristen durch, die vorzeitige Löschungen durch berechtigte Benutzer verhindern und die Datenschutzrichtlinien und -verfahren Ihrer Organisation einhalten.

> **Note**
>
> Die einzige Möglichkeit, einen Snapshot zu löschen, der im Kompatibilitätsmodus gesperrt ist, bevor seine Sperre abläuft, besteht darin, das zugehörige AWS Konto zu schließen.

Sperrdauer

Die Sperrdauer ist der Zeitraum, für den der Snapshot gesperrt bleiben soll. Sie können die Sperrdauer in einem der folgenden Formate angeben, aber nicht in beiden gleichzeitig:

Anzahl der Tage

Die Sperrdauer wird als Anzahl der Tage angegeben, für die der Snapshot gesperrt bleiben soll. Nach Ablauf der angegebenen Anzahl von Tagen wird der Snapshot automatisch entsperrt. Die Dauer kann zwischen 1 Tag und 36 500 Tagen (100 Jahren) liegen.

Ablaufdatum der Sperre

Die Dauer der Sperre wird durch ein Ablaufdatum in der Zukunft bestimmt. Der Snapshot bleibt gesperrt, bis das Ablaufdatum der Sperre erreicht wurde. Wenn das Ablaufdatum der Sperre erreicht wurde, wird der Snapshot automatisch entsperrt.

Cooling-off Zeitraum

Die Sperrfrist ist ein optionaler Zeitraum, den Sie angeben können, wenn Sie einen Snapshot im Compliance-Modus sperren. Während der Sperrfrist können Benutzer mit den entsprechenden Berechtigungen den Snapshot entsperren, den Sperrmodus ändern, die Sperrfrist verlängern oder verkürzen und die Sperrdauer verlängern bzw. verkürzen. Nach Ablauf der Sperrfrist ist es Benutzern nicht möglich, den Snapshot zu entsperren, den Sperrmodus zu ändern, die Sperrzeit wieder zu aktivieren oder die Sperrdauer zu verkürzen, unabhängig von ihren Berechtigungen.

Während der Sperrfrist kann ein Snapshot nicht gelöscht werden.

Falls angegeben, beginnt die Sperrfrist unmittelbar nach dem Sperren des Snapshots. Wenn dieser Wert nicht angegeben wird, wird der Snapshot sofort ohne Sperrfrist im Compliance-Modus gesperrt.

Die Sperrfrist kann zwischen 1 und 72 Stunden liegen. Um einen Snapshot im Compliance-Modus ohne Sperrfrist sofort zu sperren, müssen Sie die Sperrfrist bei der Anfrage weglassen.

Sperrzustand

Eine Snapshot-Sperre kann sich in einem der folgenden Zustände befinden:

- `compliance-cooloff` – Der Snapshot wurde im Compliance-Modus gesperrt, befindet sich aber noch in der Sperrfrist. Das Löschen des Snapshots ist nicht möglich, doch er lässt sich entsperren und die Sperreinstellungen können von Benutzern mit entsprechenden Berechtigungen geändert werden.
- `governance` – Der Snapshot ist im Governance-Modus gesperrt. Das Löschen des Snapshots ist nicht möglich, doch er lässt sich entsperren und die Sperreinstellungen können von Benutzern mit entsprechenden Berechtigungen geändert werden.
- `compliance` – Der Snapshot ist im Compliance-Modus ohne Sperrfrist gesperrt oder die Sperrfrist ist abgelaufen. Der Snapshot kann nicht entsperrt oder gelöscht werden. Die Sperrdauer kann nur von Benutzern mit entsprechenden Berechtigungen verlängert werden.
- `expired` – Der Snapshot wurde im Compliance- oder Governance-Modus gesperrt, aber die Sperre ist abgelaufen. Der Snapshot ist nicht gesperrt und kann gelöscht werden.

Überlegungen zur Amazon EBS-Snapshotsperre

Beachten Sie beim Sperren von Amazon EBS-Snapshots Folgendes.

- Sie können einen Snapshot nur sperren, wenn er sich im Status `pending` oder `completed` befindet.
  - Wenn Sie einen Snapshot sperren, während er sich im Status `pending` befindet, und Sie ihn für eine bestimmte Dauer sperren, beginnt die Sperrdauer erst, wenn der Snapshot den Status `completed` erreicht hat. Der Snapshot kann nicht gelöscht werden, solange er sich im Status `pending` befindet.
  - Wenn Sie einen Snapshot sperren, während er sich im Status `pending` befindet und die Snapshot-Erstellung aus irgendeinem Grund fehlschlägt, wird die Sperre aufgehoben.
- Wenn Sie die Sperrdauer für einen Snapshot verlängern, der nach Ablauf der Sperrfrist im Compliance-Modus gesperrt ist, können Sie keine weitere Sperrfrist angeben. Wenn Sie eine Sperrfrist angeben, schlägt die Anforderung fehl.
- Sie können archivierte Snapshots sperren. Sie können gesperrte Snapshots außerdem archivieren.

- Sie können Snapshots sperren, die einem AMI zugeordnet sind.
- Sie können ein AMI abmelden, dem gesperrte Snapshots zugeordnet sind.
- Sie können den KMS-Schlüssel löschen, der zum Verschlüsseln eines gesperrten Snapshots verwendet wurde.
- Wir empfehlen, Snapshots, die von erstellt wurden, nicht zu sperren. AWS Backup AWS Backup stellt bereits sicher, dass die Snapshots nicht gelöscht werden, bevor ihre Aufbewahrungsfrist abläuft. Um eine zusätzliche Sicherheitsebene für Snapshots hinzuzufügen, die von verwaltet werden AWS Backup, empfehlen wir die Verwendung von AWS Backup Vault Lock. Weitere Informationen finden Sie unter AWS Backup Vault Lock.
- Sie können Snapshots während der Erstellung und während der AMI-Registrierung nicht sperren.
- Sie können lokale Amazon-EBS-Snapshots auf AWS Outposts nicht sperren.
- Die einzige Möglichkeit, einen Snapshot zu löschen, der im Compliance-Modus gesperrt ist, bevor seine Sperre abläuft, besteht darin, das zugehörige AWS Konto zu schließen.

  Wenn Sie Ihr AWS Konto schließen, während Sie Snapshots gesperrt haben, wird Ihr Konto für 90 Tage AWS gesperrt, wobei Ihre Snapshots intakt sind. Wenn du dein Konto nicht innerhalb der 90 Tage wieder eröffnest, werden deine Schnappschüsse AWS gelöscht, auch wenn sie gesperrt sind.

Kontrollieren Sie den Zugriff auf Amazon EBS Snapshot Lock

Standardmäßig sind Benutzer nicht dazu berechtigt, mit Snapshot-Sperren zu arbeiten. Um die Verwendung von Snapshot-Sperren für Benutzer zuzulassen, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Verwendung bestimmter Ressourcen und API-Aktionen gewähren. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Themen

- Erforderliche Berechtigungen
- Beschränken des Zugriffs mit Bedingungsschlüsseln

Erforderliche Berechtigungen

Für das Arbeiten mit Snapshot-Sperren benötigen Benutzer die folgenden Berechtigungen.

- `ec2:LockSnapshot` – Zum Sperren von Snapshots.
- `ec2:UnlockSnapshot` – Zum Entsperren von Snapshots.

- `ec2:DescribeLockedSnapshots` – Zum Anzeigen der Einstellungen für die Snapshot-Sperre.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die Benutzern die Berechtigung zum Sperren und Entsperren von Snapshots sowie zum Anzeigen der Einstellungen der Snapshot-Sperre gewährt. Es umfasst die `ec2:DescribeSnapshots`-Berechtigung für Konsolenbenutzer. Werden einige Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSnapshotLockOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:LockSnapshot",
        "ec2:UnlockSnapshot",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeSnapshots"
      ],
      "Resource": [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:111122223333:volume/*"
      ]
    }
  ]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Beschränken des Zugriffs mit Bedingungsschlüsseln

Mit Bedingungsschlüsseln können Sie einschränken, wie Benutzer Snapshots sperren dürfen.

Themen

- ec2: SnapshotLockDuration
- ec2: CoolOffPeriod

ec2: SnapshotLockDuration

Sie können den Bedingungsschlüssel `ec2:SnapshotLockDuration` verwenden, um Benutzer beim Sperren von Snapshots auf eine bestimmte Sperrdauer zu beschränken.

Die folgende Beispielrichtlinie schränkt die Angabe einer Sperrdauer durch Benutzer auf eine Dauer zwischen `10` und `50` Tagen ein.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSnapshotLockWithDurationCondition",
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
```

```
        "NumericGreaterThan": {
          "ec2:SnapshotLockDuration": 10
        },
        "NumericLessThan": {
          "ec2:SnapshotLockDuration": 50
        }
      }
    }
  ]
}
```

ec2: CoolOffPeriod

Sie können den Bedingungsschlüssel `ec2:CoolOffPeriod` verwenden, um zu verhindern, dass Benutzer Snapshots im Compliance-Modus ohne Sperrfrist sperren.

Die folgende Beispielrichtlinie verhindert, dass Benutzer beim Sperren von Snapshots im Compliance-Modus eine Sperrfrist von mehr als 48 Stunden angeben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSnapshotLockWithCondition",
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "NumericGreaterThan": {
          "ec2:SnapshotTime": 48
        }
      }
    }
  ]
}
```

Sperren Sie einen Amazon EBS-Snapshot

Sie können einen Snapshot sperren, der sich im Status `pending` oder `completed` befindet. Weitere Informationen finden Sie unter Überlegungen zur Amazon EBS-Snapshotsperre.

Console

So sperren Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den zu sperrenden Snapshot aus und wählen Sie Aktionen, Snapshot-Einstellungen, Snapshot-Sperre verwalten.
4. Wählen Sie Snapshot sperren.
5. Wählen Sie unter Sperrmodus entweder den Governance-Modus oder den Compliance-Modus. Weitere Informationen finden Sie unter Sperrmodus.
6. Führen Sie für die Sperrdauer einen der folgenden Schritte aus:

   - Um den Snapshot für einen bestimmten Zeitraum zu sperren, wählen Sie Snapshot sperren für und geben Sie dann den Zeitraum in Tagen oder Jahren ein.
   - Um den Snapshot bis zu einem bestimmten Datum und einer bestimmten Uhrzeit zu sperren, wählen Sie Snapshot sperren bis aus und geben Sie dann das Ablaufdatum und die Uhrzeit an.

   Weitere Informationen finden Sie unter Sperrdauer.
7. (Nur Compliance-Modus) Geben Sie für den Cooling-off Zeitraum eine Wartezeit an, während der Sie den Snapshot entsperren und die Sperrkonfiguration ändern können. Weitere Informationen finden Sie unter Cooling-off Zeitraum.
8. (Nur Compliance-Modus) Bestätigen Sie, dass Sie den Snapshot im Compliance-Modus sperren möchten und ihn erst wieder entsperren können, wenn die Sperrfrist abgelaufen ist, indem Sie Bestätigen auswählen.
9. Wählen Sie Sperreinstellungen speichern.

AWS CLI

So sperren Sie einen Snapshot im Governance-Modus

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/lock-snapshot.html lock-snapshot. Legen Sie für `--lock-mode` die Option `governance` fest. Um den Snapshot für einen bestimmten Zeitraum zu sperren`--lock-duration`, geben Sie z. B. den Zeitraum in Tagen an.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --lock-duration 30
```

Um den Snapshot bis zu einem bestimmten Datum zu sperren`--expiration-date`, geben Sie beispielsweise in der UTC-Zeitzone das Datum und die Uhrzeit an, zu denen die Sperre ablaufen muss.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Um einen Snapshot im Compliance-Modus zu sperren

Verwenden Sie den Befehl lock-snapshot. Legen Sie für `--lock-mode` die Option `compliance` fest. Für`--cool-off-period`, geben Sie optional eine Bedenkzeit in Stunden an. Um den Snapshot für einen bestimmten Zeitraum zu sperren, geben Sie z. B. die Anzahl der Tage an`--lock-duration`, an denen der Snapshot gesperrt werden soll.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode compliance \
    --cool-off-period 24 \
    --lock-duration 30
```

Um den Snapshot bis zu einem bestimmten Datum zu sperren`--expiration-date`, geben Sie beispielsweise in der UTC-Zeitzone das Datum und die Uhrzeit an, zu denen die Sperre ablaufen muss.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode compliance \
```

```
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

So sperren Sie einen Snapshot im Governance-Modus

Verwenden Sie das cmdlet Lock-EC2Snapshot. Sie können optional die Dauer der Snapshot-Sperre in Tagen angeben.

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -LockDuration 30
```

Alternativ können Sie den Snapshot bis zu einem bestimmten Datum in der UTC-Zeitzone sperren.

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Um einen Snapshot im Compliance-Modus zu sperren

Verwenden Sie das cmdlet Lock-EC2Snapshot. Sie können optional eine Bedenkzeit in Stunden angeben. Sie können optional auch die Dauer der Snapshot-Sperre in Tagen angeben.

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "compliance" `
    -CoolOffPeriod 24 `
    -LockDuration 30
```

Alternativ können Sie den Snapshot bis zu einem bestimmten Datum in der UTC-Zeitzone sperren.

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "compliance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Entsperren Sie einen Amazon EBS-Snapshot

Sie können einen Snapshot nur entsperren, wenn er im Governance-Modus gesperrt ist oder wenn er im Compliance-Modus gesperrt ist und sich noch in der Sperrfrist befindet.

Console

So entsperren Sie einen Snapshot

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den zu entsperrenden Snapshot aus und wählen Sie Aktionen, Snapshot-Einstellungen, Snapshot-Sperre verwalten.
4. Wählen Sie „Snapshot entsperren“ und wählen Sie dann zur Bestätigung erneut „Snapshot entsperren“.

AWS CLI

So entsperren Sie einen Snapshot

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/unlock-snapshot.html unlock-snapshot.

```
aws ec2 unlock-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

So entsperren Sie einen Snapshot

Verwenden Sie das cmdlet Unlock-EC2Snapshot.

```
Unlock-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

Aktualisieren Sie die Amazon EBS-Snapshot-Sperreinstellungen

Die zulässigen Updates hängen vom Sperrstatus ab:

- `governance` – Sie können den Sperrmodus ändern und die Sperrdauer oder das Ablaufdatum verlängern oder verringern.

- `compliance-cooloff` – Sie können den Sperrmodus ändern, die Sperrfrist verlängern oder verkürzen und die Sperrdauer oder das Ablaufdatum verlängern oder verringern.
- `compliance` –Sie können nur die Sperrdauer oder das Ablaufdatum verlängern.

Console

So aktualisieren Sie die Einstellungen der Snapshot-Sperre

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus, für den Sie die Sperreinstellungen bearbeiten möchten, und wählen Sie Aktionen, Snapshot-Einstellungen, Snapshot-Sperre verwalten.
4. Aktualisieren Sie die Einstellungen nach Bedarf und wählen Sie dann Sperreinstellungen speichern.

AWS CLI

So aktualisieren Sie die Einstellungen der Snapshot-Sperre

Verwenden Sie den Befehl lock-snapshot. Geben Sie die ID des Snapshots und die zu ändernden Optionen an. Im folgenden Beispiel wird das Ablaufdatum geändert.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

So aktualisieren Sie die Einstellungen der Snapshot-Sperre

Verwenden Sie das cmdlet Lock-EC2Snapshot. Geben Sie die ID des Snapshots und die zu ändernden Optionen an. Im folgenden Beispiel wird das Ablaufdatum geändert.

```
Lock-EC2Snapshot `
    -SnapshoId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Überwachen Sie die Amazon EBS-Snapshotsperre

Sie können Aktionen im Zusammenhang mit der Amazon EBS-Snapshot-Sperre mithilfe der folgenden Tools überwachen:

Themen

- Überwachen Sie Amazon EBS-Snapshot-Sperren mit AWS CloudTrail
- Überwachen Sie Amazon EBS-Snapshot-Sperren mithilfe von Amazon EventBridge

Überwachen Sie Amazon EBS-Snapshot-Sperren mit AWS CloudTrail

Sie können API-Aufrufe für Snapshot-Sperren als Ereignisse überwachen, einschließlich Aufrufen von der Konsole und von Codeaufrufen an die APIs. Anhand der gesammelten Informationen von können Sie die Anfrage CloudTrail, die gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen finden Sie unter API-Aufrufe protokollieren mithilfe von AWS CloudTrail.

Überwachen Sie Amazon EBS-Snapshot-Sperren mithilfe von Amazon EventBridge

Amazon EBS sendet Ereignisse im Zusammenhang mit Snapshot-Sperraktionen aus. Sie können Amazon verwenden AWS Lambda EventBridge , um Ereignisbenachrichtigungen programmgesteuert zu verarbeiten. Ereignisse werden auf bestmögliche Weise ausgegeben. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Die folgenden Ereignisse werden ausgegeben:

- Der Snapshot wurde erfolgreich im Governance- oder Compliance-Modus gesperrt.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
```

```
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Fehlgeschlagenes Sperrereignis, wenn ein Snapshot gesperrt ist, während er sich im Status `pending` befindet und den Status `completed` nicht erreicht.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Sperre abgelaufen

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}
```

- Cooling-off Der Zeitraum ist abgelaufen, nachdem er im Compliance-Modus gesperrt wurde.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Sperren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots

Um zu verhindern, dass Ihre Snapshots öffentlich freigegeben werden, können Sie das Blockieren des öffentlichen Zugriffs auf Snapshots aktivieren. Nachdem Sie das Blockieren des öffentlichen Zugriffs auf Snapshots in einer Region aktiviert haben, wird jeder Versuch, Snapshots in dieser Region öffentlich freizugeben, automatisch blockiert. Dies hilft Ihnen dabei, die Sicherheit Ihrer Snapshots zu verbessern und Ihre Snapshot-Daten vor unbefugtem oder unbeabsichtigtem Zugriff zu schützen.

Das Blockieren des öffentlichen Zugriffs auf Snapshots kann in zwei Modi erfolgen:

- Blockieren der gesamten Freigabe – hierdurch wird die gesamte öffentliche Freigabe Ihrer Snapshots blockiert. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
- Blockieren der neuen Freigabe – hierdurch wird nur die neue öffentliche Freigabe Ihrer Snapshots blockiert. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

Überlegungen

Beachten Sie Folgendes, wenn Sie mit dem Blockieren des öffentlichen Zugriffs für Snapshots arbeiten.

- Durch das Blockieren des öffentlichen Zugriffs auf Snapshots wird die gemeinsame Nutzung privater Snapshots nicht verhindert.
- Wenn Sie den öffentlichen Zugriff für Schnappschüsse im Modus „Alle Freigaben blockieren“ aktivieren, werden die Berechtigungen für Schnappschüsse, die bereits öffentlich geteilt wurden, nicht geändert. Stattdessen wird verhindert, dass diese Snapshots öffentlich sichtbar und öffentlich

zugänglich sind. Daher verweisen die Attribute für diese Snapshots immer noch auf die öffentliche Freigabe, obwohl sie nicht öffentlich verfügbar sind.

Wenn Sie später die Option „Öffentlichen Zugriff blockieren“ deaktivieren oder den Modus so ändern, dass neue Freigaben blockiert werden, sind diese Snapshots wieder öffentlich verfügbar.

- Beim Blockieren des öffentlichen Zugriffs auf Snapshots handelt es sich um eine regionale Einstellung. Sie gilt für alle Snapshots in der Region, in der sie aktiviert ist. Sie müssen das Blockieren des öffentlichen Zugriffs auf Snapshots in jeder Region aktivieren, in der Sie die öffentliche Freigabe Ihrer Snapshots verhindern möchten.
- Den öffentlichen Zugriff blockieren ist eine Einstellung auf Kontoebene. Sie gilt für alle Benutzer des Kontos, einschließlich Administratorbenutzer. Sie können das Blockieren des öffentlichen Zugriffs auf Snapshots nicht auf Organisationsebene aktivieren.
- Die Einstellung „Öffentlichen Zugriff blockieren“ wird entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie konfiguriert. Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.
- Das Sperren des öffentlichen Zugriffs für Snapshots verhindert nicht das öffentliche Teilen von AMIs EBS-backed . Wenn Sie die Sperrung des öffentlichen Zugriffs für Snapshots aktivieren, können Benutzer AMIs weiterhin öffentlich teilen EBS-backed . Wenn ein EBS-backed AMI öffentlich geteilt wird, können Benutzer mit Zugriff auf dieses AMI Volumes aus den zugehörigen Snapshots erstellen. Um zu verhindern, dass Ihre AMIs öffentlich geteilt werden, aktivieren Sie die Option „Öffentlichen Zugriff für AMIs https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-intro.html#block-public-access-to-amis blockieren“.
- Das Blockieren des öffentlichen Zugriffs für Snapshots wird nicht unterstützt, wenn lokale Snapshots aktiviert sind. AWS Outposts

Preisgestaltung

Das Blockieren des öffentlichen Zugriffs auf Snapshots lässt sich ohne Zusatzkosten aktivieren.

Inhalt

- IAM-Berechtigungen zum Blockieren des öffentlichen Zugriffs auf Amazon EBS-Snapshots
- Konfigurieren Sie den blockierten öffentlichen Zugriff für Amazon EBS-Snapshots

- Sehen Sie sich die Einstellung „Öffentlichen Zugriff blockieren“ für Amazon EBS-Snapshots an
- Deaktivieren Sie die Blockierung des öffentlichen Zugriffs für Amazon EBS-Snapshots
- Überwachen, blockieren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots mit EventBridge

IAM-Berechtigungen zum Blockieren des öffentlichen Zugriffs auf Amazon EBS-Snapshots

Standardmäßig sind Benutzer nicht dazu berechtigt, mit dem blockierten öffentlichen Zugriff auf Snapshots zu arbeiten. Damit Benutzer mit dem blockierten öffentlichen Zugriff auf Snapshots arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Verwendung bestimmter API-Aktionen gewähren. Sobald die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Um mit dem blockierten öffentlichen Zugriff auf Snapshots arbeiten zu können, benötigen Benutzer die folgenden Berechtigungen.

- `ec2:EnableSnapshotBlockPublicAccess` – aktivieren Sie das Blockieren des öffentlichen Zugriffs auf Snapshots und ändern Sie den Modus.
- `ec2:DisableSnapshotBlockPublicAccess` – Deaktivieren Sie das Blockieren des öffentlichen Zugriffs auf Snapshots.
- `ec2:GetSnapshotBlockPublicAccessState` – Zeigen Sie die Einstellung für das Blockieren des öffentlichen Zugriffs auf Snapshots für eine Region an.

Es folgt eine IAM-Beispielrichtlinie. Werden einige Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:EnableSnapshotBlockPublicAccess",
            "ec2:DisableSnapshotBlockPublicAccess",
            "ec2:GetSnapshotBlockPublicAccessState"
```

```
        ],
        "Resource": "*"
    }]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in: AWS IAM Identity Center

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Konfigurieren Sie den blockierten öffentlichen Zugriff für Amazon EBS-Snapshots

Sie können das Blockieren des öffentlichen Zugriffs auf Snapshots aktivieren, um zu verhindern, dass Ihre Snapshots in der Region öffentlich freigegeben werden. Nach der Aktivierung dieses Features werden Anfragen zur öffentlichen Freigabe von Snapshots in der Region blockiert.

> **Important**
>
> Wenn Sie den öffentlichen Zugriff für Schnappschüsse im Modus „Alle Freigaben blockieren“ aktivieren, werden die Berechtigungen für Schnappschüsse, die bereits öffentlich geteilt wurden, nicht geändert. Stattdessen wird verhindert, dass diese Snapshots öffentlich sichtbar und öffentlich zugänglich sind. Daher verweisen die Attribute für diese Snapshots immer noch auf die öffentliche Freigabe, obwohl sie nicht öffentlich verfügbar sind.

Wenn Sie später die Option „Öffentlichen Zugriff blockieren“ deaktivieren oder den Modus so ändern, dass neue Freigaben blockiert werden, sind diese Snapshots wieder öffentlich verfügbar.

> **Note**
>
> Diese Einstellung wird auf Kontoebene konfiguriert, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Es muss an jedem AWS-Region Ort konfiguriert werden, an dem Sie das öffentliche Teilen von Schnappschüssen verhindern möchten. Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Console

So konfigurieren Sie das Blockieren des öffentlichen Zugriffs auf Snapshots

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard aus und wählen Sie dann unter Kontoattribute (auf der rechten Seite) Datenschutz und Sicherheit.
3. Wählen Sie im Abschnitt Blockieren des öffentlichen Zugriffs auf EBS-Snapshots die Option Verwalten.
4. Wählen Sie Öffentlichen Zugriff blockieren und anschließend eine der folgenden Optionen:

   - Blockieren des gesamten öffentlichen Zugriffs – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
   - Blockieren der neuen öffentlichen Freigabe – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

5. Wählen Sie Aktualisieren aus.

AWS CLI

So aktivieren oder bearbeiten Sie das Blockieren des öffentlichen Zugriffs auf Snapshots

Verwenden Sie den Befehl enable-snapshot-block-public-access. Geben Sie für `--state` einen der folgenden Werte an:

- `block-all-sharing` – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
- `block-new-sharing` – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

Um den öffentlichen Zugriff für Schnappschüsse für eine bestimmte Region zu aktivieren oder zu ändern, blockieren Sie den öffentlichen Zugriff

```
aws ec2 enable-snapshot-block-public-access \
    --state block-new-sharing \
    --region us-east-1
```

Es folgt eine Beispielausgabe.

```
{
    "State": "block-new-sharing"
}
```

Um den öffentlichen Zugriff auf Schnappschüsse für alle Regionen zu aktivieren oder zu ändern

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
```

```
        --output text
    );
    do (output=$(
        aws ec2 enable-snapshot-block-public-access \
            --region $region \
            --state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

So aktivieren oder bearbeiten Sie das Blockieren des öffentlichen Zugriffs auf Snapshots

Verwenden Sie den Befehl Enable-EC2SnapshotBlockPublicAccess. Geben Sie für `-State` einen der folgenden Werte an:

- `block-all-sharing` – zum Blockieren der gesamten öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht mehr öffentlich verfügbar.
- `block-new-sharing` – nur zum Blockieren der neuen öffentlichen Freigabe Ihrer Snapshots. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.

Um den öffentlichen Zugriff für Schnappschüsse für eine bestimmte Region zu aktivieren oder zu ändern

```
Enable-EC2SnapshotBlockPublicAccess `
    -Region us-east-1 `
```

```
    -State block-new-sharing
```

Es folgt eine Beispielausgabe.

```
Value
-----
block-new-sharing
```

Um den öffentlichen Zugriff auf Schnappschüsse für alle Regionen zu aktivieren oder zu ändern

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
            Enable-EC2SnapshotBlockPublicAccess `
                -Region $_ `
                -State block-new-sharing)
    }
} | Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Sehen Sie sich die Einstellung „Öffentlichen Zugriff blockieren“ für Amazon EBS-Snapshots an

Das Blockieren des öffentlichen Zugriffs kann für jede Region Ihres Kontos in einem der folgenden Status festgelegt werden.

- Blockieren der gesamten Freigabe – die gesamte öffentliche Freigabe Ihrer Snapshots wird blockiert. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Darüber

hinaus sind Snapshots, die bereits öffentlich freigegeben wurden, privat und nicht öffentlich verfügbar.

- Blockieren der neuen Freigabe – nur die neue öffentliche Freigabe Ihrer Snapshots wird blockiert. Benutzer dieses Kontos können keine neue öffentliche Freigabe beantragen. Snapshots, die bereits öffentlich freigegeben wurden, bleiben jedoch weiterhin öffentlich verfügbar.
- Blockierung aufgehoben – die öffentliche Freigabe wird nicht blockiert. Benutzer können Snapshots öffentlich freigeben.

Console

So zeigen Sie die Einstellung für das Blockieren des öffentlichen Zugriffs auf Snapshots an

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard aus und wählen Sie dann unter Kontoattribute (auf der rechten Seite) Datenschutz und Sicherheit.
3. Im Abschnitt Blockieren des öffentlichen Zugriffs auf EBS-Snapshots wird die aktuelle Einstellung angezeigt.

AWS CLI

So zeigen Sie die Einstellung für das Blockieren des öffentlichen Zugriffs auf Snapshots an

Verwenden Sie den Befehl get-snapshot-block-public-access-state.

- Für eine bestimmte Region

```
aws ec2 get-snapshot-block-public-access-state
```

In dieser Beispielausgabe gibt das `ManagedBy` Feld die Entität an, die die Einstellung konfiguriert hat, und `account` gibt an, dass die Einstellung direkt im Konto konfiguriert wurde. Ein Wert von `declarative-policy` würde bedeuten, dass die Einstellung durch eine deklarative Richtlinie konfiguriert wurde. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

```
{
    "State": "unblocked",
    "ManagedBy": "account"
```

```
}
```

- Für alle Regionen

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-snapshot-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

PowerShell

So zeigen Sie die Einstellung für das Blockieren des öffentlichen Zugriffs auf Snapshots an

Verwenden Sie das Get-EC2SnapshotBlockPublicAccessState Cmdlet.

- Für eine bestimmte Region

```
Get-EC2SnapshotBlockPublicAccessState -Region us-east-1
```

Es folgt eine Beispielausgabe.

```
Value
```

```
-----
block-new-sharing
```

- Für alle Regionen

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Get-EC2SnapshotBlockPublicAccessState -Region $_)
    }
} | Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

Deaktivieren Sie die Blockierung des öffentlichen Zugriffs für Amazon EBS-Snapshots

Sie können das Blockieren des öffentlichen Zugriffs auf Snapshots deaktivieren, um zuzulassen, dass Ihre Snapshots in der Region öffentlich freigegeben werden. Nachdem dieses Feature deaktiviert wurde, können Benutzer Snapshots in der Region öffentlich freigeben.

> **Important**
>
> Wenn Sie den öffentlichen Zugriff für Snapshots blockieren im Modus „Alle Freigaben blockieren“ aktivieren, werden die Berechtigungen für Snapshots, die bereits öffentlich geteilt wurden, nicht geändert. Stattdessen wird verhindert, dass diese Snapshots öffentlich sichtbar und öffentlich zugänglich sind. Daher verweisen die Attribute für diese Snapshots immer noch auf die öffentliche Freigabe, obwohl sie nicht öffentlich verfügbar sind.
> Wenn Sie die Option „Öffentlichen Zugriff blockieren“ deaktivieren, werden diese Schnappschüsse wieder öffentlich verfügbar.

> **Note**
>
> Diese Einstellung wird auf Kontoebene konfiguriert, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Es muss in jedem Bereich konfiguriert werden, in AWS-Region dem Sie das öffentliche Teilen von Schnappschüssen zulassen möchten. Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Console

So deaktivieren Sie das Blockieren des öffentlichen Zugriffs für Snapshots

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard aus und wählen Sie dann unter Kontoattribute (auf der rechten Seite) Datenschutz und Sicherheit.
3. Wählen Sie im Abschnitt Blockieren des öffentlichen Zugriffs auf EBS-Snapshots die Option Verwalten.
4. Deaktivieren Sie die Option Blockieren des öffentlichen Zugriffs und wählen Sie Aktualisieren.

AWS CLI

So deaktivieren Sie das Blockieren des öffentlichen Zugriffs auf Snapshots

Verwenden Sie den Befehl disable-snapshot-block-public-access.

- Für eine bestimmte Region

```
aws ec2 disable-snapshot-block-public-access --region us-east-1
```

Es folgt eine Beispielausgabe.

```
{
    "State": "unblocked"
```

```
}
```

- Für alle Regionen

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-snapshot-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

PowerShell

So deaktivieren Sie das Blockieren des öffentlichen Zugriffs für Snapshots

Verwenden Sie das Disable-EC2SnapshotBlockPublicAccess Cmdlet.

- Für eine bestimmte Region

```
Disable-EC2SnapshotBlockPublicAccess -Region us-east-1
```

Es folgt eine Beispielausgabe.

```
Value
```

```
-----
unblocked
```

- Für alle Regionen

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2SnapshotBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

Überwachen, blockieren Sie den öffentlichen Zugriff für Amazon EBS-Snapshots mit EventBridge

Amazon EBS gibt Ereignisse im Zusammenhang mit dem Blockieren des öffentlichen Zugriffs auf Snapshots aus. Sie können Amazon verwenden AWS Lambda , um Ereignisbenachrichtigungen EventBridge programmgesteuert zu verarbeiten. Ereignisse werden auf bestmögliche Weise ausgegeben. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Die folgenden Ereignisse werden ausgegeben:

- Aktivieren des Blockierens des öffentlichen Zugriffs auf Snapshots im Modus „Blockieren der gesamten Freigabe“

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
```

```
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing'
 mode"
  }
}
```

- Aktivieren des Blockierens des öffentlichen Zugriffs auf Snapshots im Modus „Blockieren der neuen Freigabe“

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing'
 mode"
  }
}
```

- Blockierens des öffentlichen Zugriffs auf Snapshots deaktivieren

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
```

```
}
```

Lokale Amazon-EBS-Snapshots auf Outposts

Amazon EBS Snapshots sind zeitpunktbezogene Kopien Ihrer EBS-Volumes.

Standardmäßig werden Snapshots von EBS-Volumes auf einem AWS Outpost in Amazon S3 in der Region von gespeichert. Outpost Sie können auch lokale Amazon EBS-Snapshots auf Outposts verwenden, um Snapshots von Volumes Outpost lokal in Amazon S3 auf dem System selbst zu speichern. Outpost Dadurch wird sichergestellt, dass sich die Snapshot-Daten auf und bei Ihnen vor Ort Outpost befinden. Darüber hinaus können Sie mithilfe von AWS Identity and Access Management (IAM) -Richtlinien und -Berechtigungen Richtlinien zur Durchsetzung der Datenspeicherorte einrichten, um sicherzustellen, dass Snapshot-Daten das System nicht verlassen. Outpost Dies ist besonders nützlich, wenn Sie in einem Land oder einer Region wohnen, das bzw. die noch nicht von einer Region bedient wird und für das ein AWS Datenspeicherort erforderlich ist.

Unter diesem Thema finden Sie Informationen zur Arbeit mit Lokaler Amazon EBS-Snapshots bei Outposts. Weitere Informationen zu Amazon EBS-Snapshots und zur Arbeit mit Snapshots in einer Region finden Sie unter. AWS Amazon EBS-Snapshots

Weitere Informationen finden Sie unter AWS Outposts Familie und in der AWS Outposts Familiendokumentation.

Themen

- Häufig gestellte Fragen
- Voraussetzungen
- Überlegungen
- Zugriffssteuerung mit IAM
- Arbeiten mit lokale Snapshots

Häufig gestellte Fragen

1. Was sind lokale Snapshots?

   Standardmäßig werden Amazon EBS-Snapshots von Volumes auf einem Outpost in Amazon S3 in der Region von gespeichert. Outpost Wenn S3 auf Outposts bereitgestellt Outpost wird,

können Sie wählen, ob die Snapshots lokal auf dem System selbst gespeichert werden sollen. Outpost Lokale Snapshots sind inkrementell, d. h, es werden nur die Blöcke des Volumes gespeichert, die sich seit Ihrem letzten Snapshot geändert haben. Sie können diese Snapshots jederzeit verwenden, um ein Volume wiederherzustellen, das sich auf demselben Outpost wie der Snapshot befindet. Weitere Informationen zu Amazon EBS-Snapshots finden Sie unter Amazon EBS-Snapshots.

2. Weshalb sollte ich lokale Snapshots verwenden?

   Snapshots sind eine bequeme Möglichkeit, Ihre Daten zu sichern. Bei lokalen Snapshots werden alle Ihre Snapshot-Daten lokal auf dem gespeichert. Outpost Dies bedeutet, dass sie Ihre Räumlichkeiten nicht verlassen. Dies ist besonders nützlich, wenn Sie in einem Land oder einer Region wohnen, das noch nicht von einer AWS Region bedient wird und für das Wohnsitzerfordernisse gelten.

   Darüber hinaus kann die Verwendung lokaler Snapshots dazu beitragen, die Bandbreite zu reduzieren, die für die Kommunikation zwischen der Region und Umgebungen mit eingeschränkter Bandbreite verwendet wird. Outpost

3. Wie erzwinge ich die Speicherung von Snapshot-Daten auf einem? Outpost

   Mithilfe von AWS Identity and Access Management (IAM-) Richtlinien können Sie die Berechtigungen kontrollieren, die Principals (AWS Konten, IAM-Benutzer und IAM-Rollen) bei der Arbeit mit lokalen Snapshots haben, und um die Datenresidenz durchzusetzen. Sie können eine Richtlinie erstellen, die verhindert, dass Principals Snapshots von Outpost Volumes und Instances erstellen und die Snapshots in einer Region speichern. AWS Derzeit wird das Kopieren von Schnappschüssen und Bildern von einer Outpost in eine Region nicht unterstützt. Weitere Informationen finden Sie unter Zugriffssteuerung mit IAM.

4. Werden mehrvolumige, absturzkonsistente lokale Snapshots unterstützt?

   Ja, Sie können absturzkonsistente lokale Snapshots mit mehreren Volumes von Instanzen auf einem erstellen. Outpost

5. Wie erstelle ich lokale Snapshots?

   Sie können Snapshots manuell mithilfe der AWS Command Line Interface (AWS CLI) - oder der Amazon EC2-Konsole erstellen. Weitere Informationen finden Sie unter Arbeiten mit lokale Snapshots. Sie können auch den Lebenszyklus von lokale Snapshots mit Amazon Data Lifecycle Manager automatisieren. Weitere Informationen finden Sie unter Automatisieren Sie Schnappschüsse auf einem Outpost.

6. Kann ich lokale Snapshots erstellen, verwenden oder löschen, wenn mein System die Verbindung zu seiner Region Outpost verliert?

Nein. Die Region Outpost muss mit ihrer Region verbunden sein, da die Region die Zugriffs-, Autorisierungs-, Protokollierungs- und Überwachungsdienste bereitstellt, die für den Zustand Ihrer Snapshots von entscheidender Bedeutung sind. Wenn keine Konnektivität besteht, können Sie keine neuen lokale Snapshots erstellen, Volumes erstellen oder Instances aus vorhandenen lokale Snapshots starten oder lokale Snapshots löschen.

7. Wie schnell wird Amazon S3 Speicherkapazität nach dem Löschen von lokale Snapshots bereitgestellt?

Amazon S3-Speicherkapazität wird innerhalb von 72 Stunden nach dem Löschen von lokale Snapshots und den Volumes, auf die sie verweisen, verfügbar.

8. Wie kann ich sicherstellen, dass mir die Amazon S3-Kapazität auf meinem Gerät nicht ausgeht? Outpost

Wir empfehlen Ihnen, CloudWatch Amazon-Alarme zu verwenden, um Ihre Amazon S3-Speicherkapazität zu überwachen und Snapshots und Volumes zu löschen, die Sie nicht mehr benötigen, um zu verhindern, dass Ihnen die Speicherkapazität ausgeht. Wenn Sie Amazon Data Lifecycle Manager verwenden, um den Lebenszyklus lokaler Snapshots zu automatisieren, stellen Sie sicher, dass Ihre Snapshot-Aufbewahrungsrichtlinien Snapshots nicht länger als nötig aufbewahren.

9. Was passiert, wenn mir die lokale Amazon S3-Kapazität auf einem ausgeht? Outpost

Wenn Ihnen die lokale Amazon S3-Kapazität auf einem Outpost ausgeht, kann Amazon Data Lifecycle Manager keine erfolgreichen lokalen Snapshots auf dem Outpost erstellen. Amazon Data Lifecycle Manager versucht, die lokalen Snapshots auf dem zu erstellenOutpost, aber die Snapshots gehen sofort in den `error` Status über und werden schließlich von Amazon Data Lifecycle Manager gelöscht. Wir empfehlen, dass Sie die `SnapshotsCreateFailed` CloudWatch Amazon-Metrik verwenden, um Ihre Snapshot-Lebenszyklusrichtlinien auf Fehler bei der Snapshot-Erstellung zu überwachen. Weitere Informationen finden Sie unter Überwachen Sie die Data Lifecycle Manager-Richtlinien mit CloudWatch.

10. Kann ich lokale Snapshots und AMIs verwenden, die von lokale Snapshots mit Spot-Instances und Spot-Flotte unterstützt werden?

Nein, Sie können keine AMIs oder lokale Snapshots verwenden, die von lokale Snapshots unterstützt werden, um Spot-Instances oder eine Spot-Flotte zu starten.

11. Kann ich lokale Snapshots und AMIs verwenden, die von lokale Snapshots mit Amazon EC2 Auto Scaling unterstützt werden?

Ja, Sie können lokale Snapshots und AMIs verwenden, die durch lokale Snapshots unterstützt werden, um Auto Scaling-Gruppen in einem Subnetz zu starten, das sich auf demselben Subnetz Outpost wie die Snapshots befindet. Die Gruppen-Serviceverknüpfte Rolle Amazon EC2 Auto Scaling muss die Berechtigung haben, den Verschlüsselung zu verwenden, mit dem die Snapshots verschlüsselt werden.

Sie können keine lokalen Snapshots oder AMIs verwenden, die durch lokale Snapshots unterstützt werden, um Auto Scaling-Gruppen in einer Region zu starten. AWS

Voraussetzungen

Um Snapshots auf einem zu speichernOutpost, benötigen Sie einenOutpost, der mit S3 on Outposts ausgestattet ist. Weitere Informationen zu S3 on Outposts finden Sie unter S3 on Outposts im Amazon S3 on Outposts User Guide.

Überlegungen

Bedenken Sie bei der Arbeit mit lokale Snapshots Folgendes.

- Sie Outpost müssen über Konnektivität zu ihrer AWS Region verfügen, um lokale Snapshots verwenden zu können.
- Snapshot-Metadaten werden in der AWS Region gespeichert, die dem Outpost zugeordnet ist. Dies umfasst keine Snapshot-Daten.
- Snapshots, die auf einem gespeichert Outpost sind, sind standardmäßig verschlüsselt. Unverschlüsselte Snapshots werden nicht unterstützt. Wenn Sie ein Volume auf einem Outpost lokalen Snapshot erstellen, wird das Volume mit demselben KMS-Schlüssel wie der Quell-Snapshot verschlüsselt. Sie können den Verschlüsselungsschlüssel jedoch ändern, wenn Sie einen lokalen Snapshot kopieren.
- Nachdem Sie lokale Snapshots aus einem gelöscht habenOutpost, ist die Amazon S3-Speicherkapazität, die von den gelöschten Snapshots verwendet wird, innerhalb von 72 Stunden verfügbar. Weitere Informationen finden Sie unter Löschen Sie lokale Snapshots.
- Sie können keine lokalen Snapshots von einem exportieren. Outpost
- Sie können die schnelle Snapshot-Wiederherstellung nicht für lokale Snapshots aktivieren.
- EBS-Direct-APIs wird von lokale Snapshots nicht unterstützt.

- Sie können keine lokalen Snapshots oder AMIs von einer in eine Outpost AWS Region, von einer in eine Outpost andere oder innerhalb einer kopieren. Outpost Sie können jedoch Snapshots von einer AWS Region in eine kopieren. Outpost Weitere Informationen finden Sie unter Kopieren Sie Schnappschüsse aus einem AWS Region in eine Outpost.
- Beim Kopieren eines Snapshots von einer AWS Region in eine Outpost werden die Daten über den Service-Link übertragen. Das gleichzeitige Kopieren mehrerer Snapshots könnte sich auf andere Dienste auswirken, die Outpost auf dem ausgeführt werden.
- Sie können lokale Snapshots nicht teilen.
- Sie müssen IAM-Richtlinien verwenden, um sicherzustellen, dass Ihre Anforderungen an die Datenresidenz erfüllt werden. Weitere Informationen finden Sie unter Zugriffssteuerung mit IAM.
- Lokale Snapshot sind inkrementelle Backups. Nur die Blöcke des Volumes werden gespeichert, die sich seit dem letzten Snapshot geändert haben. Jeder lokaler Snapshot enthält alle erforderlichen Informationen für die Wiederherstellung Ihrer Daten (ab dem Erstellungszeitpunkt des Snapshots) auf einem neuen EBS-Volume. Weitere Informationen finden Sie unter So funktionieren Amazon EBS-Snapshots.
- Sie können IAM-Richtlinien nicht verwenden, um die Datenspeicherung von Daten und Aktionen durchzusetzen. CopySnapshot CopyImage

Zugriffssteuerung mit IAM

Mithilfe von AWS Identity and Access Management (IAM-) Richtlinien können Sie steuern, welche Berechtigungen Principals (AWS Konten, IAM-Benutzer und IAM-Rollen) bei der Arbeit mit lokalen Snapshots haben. Im Folgenden finden Sie Beispielrichtlinien, mit denen Sie die Berechtigung zum Ausführen mit lokale Snapshots bestimmter Aktionen erteilen oder verweigern können.

> **Important**
>
> Das Kopieren von Schnappschüssen und Bildern von einer in eine Region wird Outpost derzeit nicht unterstützt. Daher können Sie derzeit keine IAM-Richtlinien verwenden, um Datenspeicherort und Aktionen durchzusetzen. CopySnapshot CopyImage

Themen

- Durchsetzen der Datenspeicherorte für Snapshots
- Verhindern, dass Prinzipalen lokale Snapshots löschen

Durchsetzen der Datenspeicherorte für Snapshots

Die folgende Beispielrichtlinie verhindert, dass alle Principals Snapshots von Volumes und Instances in einer Region erstellen und die Snapshot-Daten in einer Region speichern. Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` AWS Prinzipalen können immer noch lokale Snapshots erstellen. Diese Richtlinie stellt sicher, dass alle Snapshots auf dem verbleiben. Outpost

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Verhindern, dass Prinzipalen lokale Snapshots löschen

Die folgende Beispielrichtlinie verhindert, dass alle Prinzipale lokale Snapshots löschen, die auf gespeichert sind. Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Arbeiten mit lokale Snapshots

In den folgenden Abschnitten wird die Verwendung von lokale Snapshots erläutert.

Themen

- Regeln zum Speichern von Snapshots

- Erstellen Sie lokale Snapshots von Volumes auf einem Outpost
- Erstellen Sie AMIs von lokale Snapshots
- Kopieren Sie Schnappschüsse aus einem AWS Region in eine Outpost
- Kopieren Sie AMIs aus einem AWS Region in eine Outpost
- Erstellen von Volumes aus lokale Snapshots
- Starten Sie Instances von AMIs, unterstützt von lokale Snapshots
- Löschen Sie lokale Snapshots
- Automatisieren Sie Schnappschüsse auf einem Outpost

Regeln zum Speichern von Snapshots

Die folgenden Regeln gelten für Snapshot-Speicher:

- Wenn der neueste Snapshot eines Volumes auf einem gespeichert istOutpost, müssen alle nachfolgenden Snapshots auf demselben gespeichert werden. Outpost
- Wenn der neueste Snapshot eines Volumes in einer AWS Region gespeichert ist, müssen alle nachfolgenden Snapshots in derselben Region gespeichert werden. Um lokale Snapshots von diesem Volume zu erstellen, führen Sie die folgenden Schritte aus:

  1. Erstellen Sie einen Snapshot des Volumes in der AWS Region.
  2. Kopieren Sie den Snapshot Outpost aus der AWS Region in den.
  3. Erstellen Sie ein neues Volume aus dem lokaler Snapshot.
  4. Hängen Sie das Volume an eine Instanz auf dem anOutpost.

  Für das neue Volume auf dem Outpost kann der nächste Snapshot in der Outpost oder in der AWS Region gespeichert werden. Alle aufeinanderfolgenden Snapshots müssen dann am selben Ort gespeichert werden.
- Lokale Snapshots, einschließlich Snapshots, die in einer Region erstellt wurden, Outpost und Snapshots, die in eine oder Outpost aus einer AWS Region kopiert wurden, können nur verwendet werden, um Volumes in derselben Region zu erstellen. Outpost
- Wenn Sie ein Volume auf einem Outpost Snapshot in einer Region erstellen, müssen sich alle nachfolgenden Snapshots dieses neuen Volumes in derselben Region befinden.
- Wenn Sie ein Volume auf oder Outpost aus einem lokalen Snapshot erstellen, müssen sich alle nachfolgenden Snapshots dieses neuen Volumes auf demselben befinden. Outpost

Erstellen Sie lokale Snapshots von Volumes auf einem Outpost

Sie können lokale Snapshots von Volumes auf Ihrem erstellen. Outpost Sie können wählen, ob Sie die Snapshots auf demselben Laufwerk Outpost wie das Quell-Volume oder in der Region für das speichern möchten. Outpost

Lokale Snapshots können nur verwendet werden, um Volumes auf demselben Outpost zu erstellen.

Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots.

Erstellen Sie AMIs von lokale Snapshots

Sie können Amazon Machine Images (AMIs) mithilfe einer Kombination aus lokalen Snapshots und Snapshots erstellen, die in der Region von gespeichert sind. Outpost Wenn Sie beispielsweise über einen Eingang verfügen`us-east-1`, können Sie ein Outpost AMI mit Datenvolumes erstellen, die durch lokale Snapshots unterstützt werdenOutpost, und einem Root-Volume, das durch einen Snapshot in der Region gesichert wird. `us-east-1`

Sie können ein AMI auch direkt von einer Instance aus erstellenOutpost, die lokale Snapshots unterstützt. Die für das AMI erstellten Backing-Snapshots können auf derselben Outpost Instance oder in ihrer übergeordneten Region gespeichert werden.

> **Note**
>
> - Sie können keine AMIs erstellen, die Backing-Snapshots enthalten, die auf mehreren gespeichert sind. Outposts
> - AMIs, die von lokalen Snapshots unterstützt werden, können nur zum Starten von Instances auf denselben Outpost verwendet werden.

Um ein AMI auf einem zu erstellen Outpost aus Schnappschüssen in einer Region

1. Kopieren Sie die Schnappschüsse aus der Region in die. Outpost Weitere Informationen finden Sie unter Kopieren Sie Schnappschüsse aus einem AWS Region in eine Outpost.
2. Verwenden Sie die Amazon EC2-Konsole oder den Befehl register-image, um das AMI mithilfe der Snapshot-Kopien auf dem zu erstellen. Outpost Weitere Informationen finden Sie unter Erstellen einer AMI aus einem Snapshot.

Um ein AMI direkt aus einer Instance auf einem zu erstellen Outpost

Verwenden Sie den Befehl create-image mit dem `--snapshot-location` Parameter, um zu steuern, wo die Backing-Snapshots gespeichert werden:

- Um Snapshots lokal auf derselben Instanz Outpost wie die Instanz zu speichern, geben Sie Folgendes an. `local`
- Um Snapshots in der übergeordneten Region von zu speichernOutpost, geben Sie an. `regional`

Wenn sich die Quellinstanz auf einer befindetOutpost, die lokale Snapshots unterstützt, ist der `--snapshot-location` Parameter erforderlich. Wenn Sie ihn weglassen, schlägt die Anfrage mit einem `InvalidParameterValue` Fehler fehl.

Im folgenden Beispiel wird ein AMI erstellt und die Backing-Snapshots auf derselben Ebene Outpost wie die Instance gespeichert.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "My Outpost image" \
    --snapshot-location local
```

Um ein AMI in einer Region aus einer Instance auf einer zu erstellen Outpost

Verwenden Sie den Befehl create-image und geben Sie den `regional` `--snapshot-location` Parameter an.

Im folgenden Beispiel wird ein AMI erstellt und die Backing-Snapshots in der übergeordneten Region von gespeichert. Outpost

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "My Regional image" \
    --snapshot-location regional
```

Kopieren Sie Schnappschüsse aus einem AWS Region in eine Outpost

Sie können Schnappschüsse von einer AWS Region in eine kopieren. Outpost Sie können dies nur tun, wenn sich die Schnappschüsse in der Region für die befinden. Outpost Wenn sich die Snapshots in einer anderen Region befinden, müssen Sie den Snapshot zuerst in die Region für kopieren und ihn dann von dieser Region in die kopieren. Outpost Outpost

> **Note**
>
> Sie können lokale Snapshots nicht von einer in eine Outpost Region, von einer Region in eine Outpost andere oder innerhalb derselben kopieren. Outpost

Weitere Informationen finden Sie unter Kopieren Sie einen Amazon EBS-Snapshot.

Kopieren Sie AMIs aus einem AWS Region in eine Outpost

Sie können AMIs von einer AWS Region in eine kopierenOutpost. Wenn Sie ein AMI von einer Region in eine kopierenOutpost, werden alle mit dem AMI verknüpften Snapshots von der Region in die Outpost kopiert.

Sie können ein AMI Outpost nur dann von einer Region in eine kopieren, wenn sich die mit dem AMI verknüpften Snapshots in der Region für die befinden. Outpost Wenn sich die Snapshots in einer anderen Region befinden, müssen Sie das AMI zuerst in die Region für kopieren und dann von dieser Region in dieOutpost. Outpost

> **Note**
>
> Sie können ein AMI nicht von einer in eine Outpost Region, von einer Outpost in eine andere oder innerhalb einer Outpost kopieren.

Sie können AMIs nur Outpost mit dem AWS CLI Befehl copy-image von einer Region in eine kopieren.

Erstellen von Volumes aus lokale Snapshots

Sie können Volumes auf und Outpost aus lokalen Snapshots erstellen. Volumes müssen auf derselben Grundlage Outpost wie die Quell-Snapshots erstellt werden. Sie können keine lokalen Snapshots verwenden, um Volumes in der Region für die zu erstellen. Outpost

Wenn Sie ein Volume aus einem lokaler Snapshot erstellen, können Sie das Volume nicht mit einem anderen Verschlüsselung neu verschlüsseln. Volumes, die aus lokale Snapshots erstellt wurden, müssen mit demselben Verschlüsselung wie der Quell-Snapshot verschlüsselt werden.

Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.

Starten Sie Instances von AMIs, unterstützt von lokale Snapshots

Sie können Instances von AMIs starten, die von lokale Snapshots unterstützt werden. Sie müssen Instances auf demselben Gerät Outpost wie das Quell-AMI starten. Weitere Informationen finden Sie Outpost im AWS Outposts Benutzerhandbuch unter Starten einer Instance auf Ihrem.

Löschen Sie lokale Snapshots

Sie können lokale Snapshots aus einem Outpost löschen. Nachdem Sie einen Snapshot aus einem gelöscht habenOutpost, ist die vom gelöschten Snapshot verwendete Amazon S3-Speicherkapazität innerhalb von 72 Stunden nach dem Löschen des Snapshots und der Volumes, die auf diesen Snapshot verweisen, verfügbar.

Da die Amazon S3-Speicherkapazität nicht sofort verfügbar wird, empfehlen wir Ihnen, CloudWatch Amazon-Alarme zu verwenden, um Ihre Amazon S3-Speicherkapazität zu überwachen. Löschen Sie Snapshots und Volumes, die Sie nicht mehr benötigen, um zu vermeiden, dass die Speicherkapazität knapp wird.

Weitere Informationen zum Löschen von Snapshots erhalten Sie unter Löschen eines Snapshots.

Automatisieren Sie Schnappschüsse auf einem Outpost

Sie können Amazon Data Lifecycle Manager-Snapshot-Lebenszyklusrichtlinien erstellen, die automatisch Snapshots Ihrer Volumes und Instances auf einem erstellen, kopieren, speichern und löschen. Outpost Sie können wählen, ob Sie die Snapshots in einer Region oder lokal in einer speichern möchten. Outpost Darüber hinaus können Sie Schnappschüsse, die in einer AWS Region erstellt und gespeichert werden, automatisch in eine kopieren. Outpost

Die folgende Tabelle bietet einen Überblick über die unterstützten Features.

Standort der Ressource	Snapshot-Ziel	Cross-region in Region kopieren	Cross-region kopieren nach Outpost	Schnelle Snapshot-Wiederherstellung	Cross-account teilen
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Überlegungen

- Derzeit werden nur Amazon EBS-Snapshot-Lifecycle-Richtlinien unterstützt. EBS-backed AMI-Richtlinien und Richtlinien für Cross-account gemeinsame Ereignisse werden nicht unterstützt.
- Wenn eine Richtlinie Snapshots für Volumes oder Instances in einer Region verwaltet, werden Snapshots in derselben Region wie die Quellressource erstellt.
- Wenn eine Richtlinie Snapshots für Volumes oder Instances auf einem verwaltetOutpost, können Snapshots auf der Quelle Outpost oder in der entsprechenden Region erstellt werden. Outpost
- Eine einzelne Richtlinie kann nicht sowohl Snapshots in einer Region als auch Snapshots in einer verwalten. Outpost Wenn Sie Snapshots in einer Region und in einer automatisieren müssenOutpost, müssen Sie separate Richtlinien erstellen.
- Die schnelle Wiederherstellung von Snapshots wird nicht für Snapshots unterstützt, die auf einem erstellt wurdenOutpost, oder für Snapshots, die auf ein kopiert wurden. Outpost
- Cross-account Das Teilen wird für Snapshots, die auf einem erstellt wurden, nicht unterstützt. Outpost
- Pre-scripts und Post-Skripts werden für Snapshots, die auf einem erstellt wurden, nicht unterstützt. Outpost

Weitere Informationen zum Erstellen eines Snapshot-Lebenszyklus, der lokale Snapshots verwaltet, finden Sie unter Automatisieren von Snapshot-Lebenszyklen.

Lokale Schnappschüsse in lokalen Zonen

Amazon EBS Snapshots sind zeitpunktbezogene Kopien Ihrer EBS-Volumes.

Snapshots von EBS-Volumes in einer AWS lokalen Zone können in Amazon S3 in derselben lokalen Zone oder in der übergeordneten Region dieser lokalen Zone gespeichert werden. Das Speichern von Snapshots in einer lokalen Zone kann Ihnen helfen, die Anforderungen an den Speicherort von Daten zu erfüllen, indem sichergestellt wird, dass Snapshot-Daten in einem bestimmten Land, Bundesstaat oder einer bestimmten Gemeinde verarbeitet und gespeichert werden. Mithilfe von IAM können Sie auch Richtlinien zur Durchsetzung der Datenresidenz einrichten, um sicherzustellen, dass Snapshot-Daten die Local Zone nicht verlassen.

Local Zones eignen sich ideal für Anwendungen, die eine Latenz im einstelligen Millisekundenbereich oder eine lokale Datenverarbeitung erfordern, da sie die AWS Infrastruktur näher an Ihre Endbenutzer und Geschäftszentren heranführen. Darüber hinaus können Sie die

Datenspeicheranforderungen für regulatorische und konformitätsrelevante Workloads erfüllen. Weitere Informationen finden Sie unter Was sind lokale Zonen. AWS

Lokale Snapshots werden derzeit in lokalen Zonen unterstützt, die Amazon S3 unterstützen. Weitere Informationen finden Sie unter Funktionen für AWS lokale Zonen. .

Themen

- Häufig gestellte Fragen
- Überlegungen
- Zugriffssteuerung mit IAM

Häufig gestellte Fragen

1. Was sind lokale Schnappschüsse in lokalen Zonen?

   Lokale Snapshots in lokalen Zonen sind Schnappschüsse, die in Amazon S3 in einer lokalen Zone gespeichert werden. Standardmäßig werden Snapshots von Amazon EBS-Volumes in einer lokalen Zone in Amazon S3 in der übergeordneten Region gespeichert. Wenn die lokale Zone Amazon S3 unterstützt, können Sie die Snapshots stattdessen lokal in der lokalen Zone speichern. Wie Snapshots in AWS Regionen sind auch lokale Snapshots in lokalen Zonen inkrementell, was bedeutet, dass nur die Blöcke des Volumes gespeichert werden, die sich nach Ihrem letzten Snapshot geändert haben. Sie können diese Snapshots verwenden, um ein Amazon EBS-Volume in derselben lokalen Zone jederzeit wiederherzustellen.
2. Warum sollte ich lokale Snapshots verwenden?

   Verwenden Sie lokale Snapshots in lokalen Zonen, um die Anforderungen an den Speicherort von Daten oder die Datenisolierung zu erfüllen, indem Sie sicherstellen, dass sich Ihre Snapshot-Daten an einem bestimmten geografischen Standort befinden, z. B. in einem Land, Bundesstaat oder einer Gemeinde.
3. Wie erzwinge ich den Speicherort von Snapshot-Daten in lokalen Zonen?

   Mithilfe von AWS Identity and Access Management (IAM-) Richtlinien können Sie die Berechtigungen kontrollieren, die Principals (AWS Konten, IAM-Benutzer und IAM-Rollen) bei der Arbeit mit lokalen Snapshots in lokalen Zonen haben, und um die Datenresidenz durchzusetzen. Sie können beispielsweise eine Richtlinie erstellen, die verhindert, dass Benutzer Snapshots von Volumes in lokalen Zonen erstellen und diese Snapshots in einer Region speichern. AWS Weitere Informationen finden Sie unter Zugriffssteuerung mit IAM.

4. Werden absturzkonsistente lokale Snapshots mit mehreren Volumes unterstützt?

   Ja, Sie können absturzkonsistente lokale Snapshots mit mehreren Volumes in lokalen Zonen von Instances in einer lokalen Zone erstellen.

5. Wie erstelle ich lokale Snapshots in Local Zones?

   Sie können lokale Snapshots in lokalen Zonen manuell mithilfe der AWS CLI oder der Amazon EC2-Konsole erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Snapshot eines EBS-Volumes. Sie können den Lebenszyklus lokaler Snapshots in lokalen Zonen auch mithilfe von Amazon Data Lifecycle Manager automatisieren. Weitere Informationen finden Sie unter Erstellen Sie eine benutzerdefinierte Amazon Data Lifecycle Manager-Richtlinie für EBS-Snapshots.

6. Kann ich lokale Snapshots in Local Zones kopieren?

   Ja, Sie können Schnappschüsse von einer Region in eine lokale Zone in derselben Region, von einer lokalen Zone in ihre Region und von einer lokalen Zone in eine andere lokale Zone in derselben lokalen Zonengruppe kopieren.

7. Wie kann ich Daten aus lokalen Snapshots in lokalen Zonen wiederherstellen?

   Sie können lokale Snapshots in lokalen Zonen verwenden, um Amazon EBS-Volumes nur in derselben lokalen Zone zu erstellen.

8. Wie werden lokale Snapshots in lokalen Zonen verschlüsselt?

   Informationen Amazon EBS-Verschlüsselung in lokalen Zonen, Außenposten und Wellenlängenzonen zum Verhalten der lokalen Zone-specific Verschlüsselung finden Sie unter. In lokalen Zonen, in denen Amazon EBS-Ressourcen standardmäßig verschlüsselt sind, werden aus lokalen Snapshots erstellte Volumes immer mit demselben AWS KMS Schlüssel wie der Snapshot verschlüsselt. Sie können den Verschlüsselungsschlüssel jedoch ändern, wenn Sie einen lokalen Snapshot kopieren.

9. Kann ich EBS-backed AMIs mithilfe von lokalen Snapshots in lokalen Zonen erstellen?

   Ja, Sie können lokale Snapshots in lokalen Zonen verwenden, wenn Sie EBS-backed AMIs erstellen, indem Sie das Snapshot-Ziel als Local Zones angeben. Weitere Informationen finden Sie unter Erstellen eines EBS-backed Amazon-AMI.

10. Kann ich lokale Snapshots in Local Zones teilen?

    Ja, Sie können lokale Schnappschüsse in lokalen Zonen mit anderen AWS Konten teilen, die die lokale Zone für die Verwendung in ihrem Konto aktiviert haben.

11. Kann ich einen lokalen Snapshot eines Volumes erstellen und dann zur Erstellung von Snapshots in der übergeordneten Region wechseln?

Nein, nachdem Sie einen lokalen Snapshot eines Volumes erstellt haben, können Sie keine aufeinanderfolgenden Snapshots dieses Volumes in der übergeordneten Region erstellen. Da alle Snapshots inkrementell sind, müssen alle nachfolgenden Snapshots dieses Volumes lokale Snapshots sein, wenn der letzte Snapshot eines Volumes ein lokaler Snapshot ist.

Überlegungen

Beachten Sie Folgendes, wenn Sie mit lokalen Snapshots in lokalen Zonen arbeiten.

- Lokale Snapshots werden derzeit in lokalen Zonen unterstützt, die Amazon S3 unterstützen.
- Die folgenden Funktionen können nicht mit lokalen Snapshots in lokalen Zonen verwendet werden:
  - VM-Aktionen Import/Export
  - Schnelle Snapshot-Wiederherstellung
  - Direkte EBS-APIs
  - Papierkorb
  - Snapshot-Archiv
- Sie müssen IAM-Richtlinien verwenden, um Ihre Anforderungen an den Speicherort Ihrer Daten durchzusetzen. Weitere Informationen finden Sie unter Zugriffssteuerung mit IAM.
- Wenn der letzte Snapshot eines Volumes ein lokaler Snapshot ist, müssen alle nachfolgenden Snapshots lokale Snapshots sein. Ebenso müssen, wenn der neueste Snapshot eines Volumes in einer AWS Region gespeichert ist, alle nachfolgenden Snapshots in derselben Region gespeichert werden.

Zugriffssteuerung mit IAM

Mithilfe von AWS Identity and Access Management (IAM-) Richtlinien können Sie steuern, welche Berechtigungen Principals (AWS Konten, IAM-Benutzer und IAM-Rollen) bei der Arbeit mit lokalen Snapshots in lokalen Zonen haben. Im Folgenden finden Sie Beispielrichtlinien, mit denen Sie die Berechtigung zum Ausführen bestimmter Aktionen mit lokalen Snapshots in lokalen Zonen gewähren oder verweigern können.

Themen

- Erzwingen Sie die Datenresidenz für lokale Snapshots in lokalen Zonen
- Verhindern Sie das Teilen lokaler Snapshots in lokalen Zonen
- Verhindern Sie, dass Hauptbenutzer lokale Snapshots in lokalen Zonen löschen

Erzwingen Sie die Datenresidenz für lokale Snapshots in lokalen Zonen

Die folgende Beispielrichtlinie beschränkt Benutzer darauf, nur lokale Snapshots in lokalen Zonen von Volumes und Instances in einer lokalen Zone zu erstellen. Sie verhindert, dass Benutzer in einer Region Snapshots von Volumes und Instances in einer lokalen Zone erstellen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Effect": "Deny",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*",
            "Condition":
            {
                "StringEquals":
                {
                    "ec2:Location": "regional",
                    "ec2:SourceAvailabilityZone": "local_zone"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*",
```

```
            "Condition":
            {
                "StringEquals":
                {
                    "ec2:SourceAvailabilityZone": "local_zone"
                },
                "Null":
                {
                    "ec2:Location": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Verhindern Sie das Teilen lokaler Snapshots in lokalen Zonen

Die folgende Beispielrichtlinie verhindert, dass alle Benutzer lokale Snapshots in lokalen Zonen teilen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenySnapshotModifyInLocalZone",
      "Effect": "Deny",
      "Action": [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
```

```
        "StringEquals": {
        "ec2:AvailabilityZone": "use1-atl2-az1"
        }
      }
    },
    {
      "Sid": "AllowSnapshotModifyElsewhere",
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    }
  ]
}
```

Verhindern Sie, dass Hauptbenutzer lokale Snapshots in lokalen Zonen löschen

Die folgende Beispielrichtlinie verhindert, dass alle Benutzer lokale Snapshots in lokalen Zonen löschen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenySnapshotDeleteInLocalZone",
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "StringEquals": {
        "ec2:AvailabilityZone": "use1-atl2-az1"
        }
      }
    },
```

```
    {
      "Sid": "AllowSnapshotDeleteElsewhere",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    }
  ]
}
```

Amazon EBS-Verschlüsselung

Verwenden Sie die Amazon EBS-Verschlüsselung als unkomplizierte Verschlüsselungslösung für Ihre Amazon EBS-Ressourcen, die mit Ihren Amazon EC2-Instances verknüpft sind. Mit der Amazon EBS-Verschlüsselung müssen Sie keine eigene Schlüsselverwaltungsinfrastruktur aufbauen, pflegen und sichern. Amazon EBS-Verschlüsselung nutzt AWS KMS keys beim Erstellen verschlüsselter Volumes und Snapshots.

Die Verschlüsselung wird auf den Servern ausgeführt, auf denen die Amazon EC2-Instances gehostet werden, um die Sicherheit sowohl ruhender Daten als auch übertragener Daten zwischen einer Instance und dem verbundenen EBS-Speicher zu gewährleisten.

Sie können diesen Instances sowohl verschlüsselte als auch unverschlüsselte Volumes gleichzeitig zuordnen. Alle Amazon EC2-Instance-Typen unterstützen die Amazon EBS-Verschlüsselung.

Inhalt

- So funktioniert die Amazon EBS-Verschlüsselung
- Amazon EBS-Verschlüsselung in lokalen Zonen, Außenposten und Wellenlängenzonen
- Anforderungen für die Amazon EBS-Verschlüsselung
- Aktivieren Sie standardmäßig die Amazon EBS-Verschlüsselung
- Verschlüsseln von EBS-Ressourcen
- Drehen AWS KMS Schlüssel, die für die Amazon EBS-Verschlüsselung verwendet werden
- Beispiele für Amazon EBS-Verschlüsselung

So funktioniert die Amazon EBS-Verschlüsselung

Sie können sowohl Boot- als auch Daten-Volumes einer EC2-Instance verschlüsseln.

Wenn Sie ein verschlüsseltes EBS-Volume erstellen und einem unterstützten Instance-Typ zuordnen, werden die folgenden Datentypen verschlüsselt:

- Die auf dem Volume gespeicherten Daten
- Alle Daten, die zwischen dem Volume und der Instance verschoben werden
- Alle Snapshots, die von dem Volume erstellt werden
- Alle Volumes, die von diesen Snapshots erstellt werden

Amazon EBS verschlüsselt Ihr Volume mit einem Datenschlüssel und verwendet dabei branchenübliche AES-256 Datenverschlüsselung. Der Datenschlüssel wird von einem Schlüssel generiert AWS KMS und dann AWS KMS mit einem AWS KMS Schlüssel verschlüsselt, bevor er zusammen mit Ihren Volume-Informationen gespeichert wird. Amazon EBS erstellt automatisch eine eindeutige Datei Von AWS verwalteter Schlüssel in jeder Region, in der Sie Amazon EBS-Ressourcen erstellen. Der Alias für den KMS-Schlüssel lautet. `aws/ebs` Amazon EBS verwendet standardmäßig diesen Verschlüsselung für die Verschlüsselung. Alternativ können Sie einen symmetrischen, vom Kunden verwalteten Verschlüsselungsschlüssel verwenden, den Sie erstellen. Die Verwendung eines eigenen Verschlüsselung gibt Ihnen mehr Flexibilität, einschließlich der Fähigkeit, KMS-Schlüssel zu erstellen, zu rotieren und zu deaktivieren.

Amazon EC2 arbeitet mit AWS KMS , um Ihre EBS-Volumes auf leicht unterschiedliche Weise zu verschlüsseln und zu entschlüsseln, je nachdem, ob der Snapshot, aus dem Sie ein verschlüsseltes Volume erstellen, verschlüsselt oder unverschlüsselt ist.

So funktioniert die EBS-Verschlüsselung bei verschlüsseltem Snapshot

Wenn Sie ein verschlüsseltes Volume aus einem verschlüsselten Snapshot erstellen, den Sie besitzen, verwendet Amazon EC2, um Ihre EBS-Volumes wie folgt AWS KMS zu verschlüsseln und zu entschlüsseln:

1. Amazon EC2 sendet eine GenerateDataKeyWithoutPlaintext Anfrage an, in der der KMS-Schlüssel angegeben AWS KMS wird, den Sie für die Volumenverschlüsselung ausgewählt haben.
2. Wenn das Volume mit demselben KMS-Schlüssel wie der Snapshot verschlüsselt ist, AWS KMS verwendet es denselben Datenschlüssel wie der Snapshot und verschlüsselt ihn unter demselben KMS-Schlüssel. Wenn das Volume mit einem anderen KMS-Schlüssel verschlüsselt ist, AWS KMS generiert einen neuen Datenschlüssel und verschlüsselt ihn unter dem von Ihnen angegebenen KMS-Schlüssel. Der verschlüsselte Datenschlüssel wird an Amazon EBS gesendet, damit er mit den Volume-Metadaten gespeichert wird.
3. Wenn Sie das verschlüsselte Volume an eine Instance anhängen, sendet Amazon EC2 eine CreateGrant Anfrage an, AWS KMS damit der Datenschlüssel entschlüsselt werden kann.
4. AWS KMS entschlüsselt den verschlüsselten Datenschlüssel und sendet den entschlüsselten Datenschlüssel an Amazon EC2.
5. Amazon EC2 verwendet den Klartext-Datenschlüssel in der Nitro-Hardware, um die Festplatte auf dem Volume zu verschlüsseln. I/O Der Klartext-Datenschlüssel bleibt solange im Speicher, wie das Volume an die Instance angefügt ist.

So funktioniert die EBS-Verschlüsselung bei unverschlüsseltem Snapshot

Wenn Sie ein verschlüsseltes Volume aus einem unverschlüsselten Snapshot erstellen, arbeitet Amazon EC2 wie folgt mit AWS KMS zusammen, um Ihre EBS-Volumes zu ver- und entschlüsseln:

1. Amazon EC2 sendet eine CreateGrant Anfrage an AWS KMS, damit das Volume, das aus dem Snapshot erstellt wird, verschlüsselt werden kann.
2. Amazon EC2 sendet eine GenerateDataKeyWithoutPlaintext Anfrage an AWS KMS, in der der KMS-Schlüssel angegeben wird, den Sie für die Volumenverschlüsselung ausgewählt haben.
3. AWS KMS generiert einen neuen Datenschlüssel, verschlüsselt ihn unter dem KMS-Schlüssel, den Sie für die Volumenverschlüsselung ausgewählt haben, und sendet den verschlüsselten Datenschlüssel an Amazon EBS, um ihn zusammen mit den Volume-Metadaten zu speichern.
4. Amazon EC2 sendet eine https://docs.aws.amazon.com/kms/latest/APIReference/API_Decrypt.html Entschlüsselungsanforderung an, AWS KMS um den verschlüsselten Datenschlüssel zu entschlüsseln, den es dann zum Verschlüsseln der Volume-Daten verwendet.
5. Wenn Sie das verschlüsselte Volume an eine Instance anhängen, sendet Amazon EC2 eine CreateGrant Anfrage an AWS KMS, damit der Datenschlüssel entschlüsselt werden kann.
6. Wenn Sie das verschlüsselte Volume an eine Instance anhängen, sendet Amazon EC2 eine https://docs.aws.amazon.com/kms/latest/APIReference/API_Decrypt.html Entschlüsselungsanforderung an AWS KMS, in der der verschlüsselte Datenschlüssel angegeben wird.
7. AWS KMS entschlüsselt den verschlüsselten Datenschlüssel und sendet den entschlüsselten Datenschlüssel an Amazon EC2.
8. Amazon EC2 verwendet den Klartext-Datenschlüssel in der Nitro-Hardware, um die Festplatte auf dem Volume zu verschlüsseln. I/O Der Klartext-Datenschlüssel bleibt solange im Speicher, wie das Volume an die Instance angefügt ist.

Weitere Informationen finden Sie unter So verwendet Amazon Elastic Block Store (Amazon EBS) AWS KMS und Amazon EC2 – Beispiel zwei im AWS Key Management Service - Entwicklerhandbuch.

Auswirkung von unbrauchbaren KMS-Schlüsseln auf Datenschlüssel

Wenn ein KMS-Schlüssel unbrauchbar wird, wirkt sich das fast sofort aus (vorbehaltlich einer letztendlichen Konsistenz). Der Schlüsselstatus des KMS-Schlüssels ändert sich, um seinen

neuen Zustand widerzuspiegeln, und alle Anforderungen der Verwendung des KMS-Schlüssels in kryptografischen Vorgängen schlagen fehl.

Wenn Sie eine Aktion ausführen, die den KMS-Schlüssel unbrauchbar macht, hat dies keine unmittelbaren Auswirkungen auf die EC2-Instance oder die angehängten EBS-Volumes. Amazon EC2 verwendet den Datenschlüssel, nicht den KMS-Schlüssel, um die gesamte Festplatte zu verschlüsseln, I/O während das Volume an die Instance angeschlossen ist.

Wenn jedoch das verschlüsselte EBS-Volume von der EC2-Instance getrennt wird, entfernt Amazon EBS den Datenschlüssel von der Nitro-Hardware. Wird das verschlüsselte EBS-Volume dann wieder an eine EC2-Instance angefügt, schlägt dies fehl, weil Amazon EBS nicht den KMS-Schlüssel verwenden kann, um den verschlüsselten Datenschlüssel des Volumes zu entschlüsseln. Um das EBS-Volume wieder zu verwenden, müssen Sie den KMS-Schlüssel wieder brauchbar machen.

> **Tip**
>
> Wenn Sie nicht mehr auf Daten zugreifen möchten, die auf einem EBS-Volume gespeichert sind, das mit einem aus einem KMS-Schlüssel generierten Datenschlüssel verschlüsselt ist, den Sie unbrauchbar machen möchten, empfehlen wir, das EBS-Volume von der EC2-Instance zu trennen, bevor Sie den KMS-Schlüssel unbrauchbar machen.

Weitere Informationen finden Sie unter Wie sich unbrauchbare KMS-Schlüssel auf Datenschlüssel auswirken im AWS Key Management Service -Entwicklerhandbuch.

Amazon EBS-Verschlüsselung in lokalen Zonen, Außenposten und Wellenlängenzonen

Das Verhalten der Amazon EBS-Verschlüsselung variiert je nach Art des Standorts, an dem Sie Ihre Ressourcen erstellen.

Local Zones

In den folgenden lokalen Zonen sind alle Amazon EBS-Ressourcen standardmäßig verschlüsselt. Sie können keine unverschlüsselten Volumes oder Snapshots erstellen. Wenn Sie keinen KMS-Schlüssel angeben, verschlüsselt Amazon EBS Ihre Ressourcen mit dem Standardverschlüsselungsschlüssel Ihres Kontos. In der Standardeinstellung ist dies Von AWS verwalteter Schlüssel ()`aws/ebs`.

Informationen zum Ändern des Standardverschlüsselungsschlüssels für Ihr Konto finden Sie unterStandard-Verschlüsselungsschlüssel.

- Nordamerika:us-east-1-atl-1a,, us-east-1-bos-1aus-east-1-chi-1a,us-east-1-dfw-1a,us-east-1-iah-1a,us-east-1-mci-1a,us-east-1-mia-1a,us-east-1-msp-1a,us-east-1-nyc-1a,us-east-1-phl-1a,us-east-1-qro-1a,us-east-2-mci-1a, us-east-2-mci-1bus-west-2-den-1a,us-west-2-hnl-1a,us-west-2-las-1a,us-west-2-las-1b,us-west-2-pdx-1a,us-west-2-phx-1a, us-west-2-sea-1a
- Asien-Pazifik: ap-northeast-1-tpe-1a ap-south-1-ccu-1aap-south-1-ccu-2a,ap-south-1-del-1a,ap-south-1-del-2a,ap-southeast-1-bkk-1a,ap-southeast-1-han-1a,ap-southeast-1-mnl-1a,ap-southeast-2-akl-1a, ap-southeast-2-per-1a
- Europa:eu-central-1-ath-1a,eu-central-1-ham-1a,eu-central-1-ist-1a,eu-central-1-waw-1a,eu-north-1-cph-1a, eu-north-1-hel-1a
- Südamerika:us-east-1-bue-1a,us-east-1-lim-1a, us-east-1-scl-1a
- Naher Osten: me-south-1-mct-1a
- Afrika: af-south-1-los-1a

In allen anderen lokalen Zonen folgt die Amazon EBS-Verschlüsselung dem gleichen Verhalten wie in der übergeordneten Region.

Außenposten und Wellenlängenzonen

Alle Amazon EBS-Ressourcen auf AWS Outposts und in Wavelength Zones sind standardmäßig verschlüsselt. Sie können keine unverschlüsselten Volumes oder Snapshots erstellen. Wenn Sie keinen KMS-Schlüssel angeben, verschlüsselt Amazon EBS Ihre Ressourcen mit dem Standardverschlüsselungsschlüssel Ihres Kontos. In der Standardeinstellung ist dies Von AWS verwalteter Schlüssel ()aws/ebs. Informationen zum Ändern des Standardverschlüsselungsschlüssels für Ihr Konto finden Sie unterStandard-Verschlüsselungsschlüssel.

Wenn Sie in diesen Zonen ein Volume aus einem lokalen Snapshot erstellen, wird das Volume mit demselben KMS-Schlüssel wie der Quell-Snapshot verschlüsselt. Sie können den Verschlüsselungsschlüssel jedoch ändern, wenn Sie einen lokalen Snapshot kopieren.

Anforderungen für die Amazon EBS-Verschlüsselung

Prüfen Sie, ob die folgenden Anforderungen erfüllt sind, bevor Sie beginnen:

Voraussetzungen

- Unterstützte Volume-Typen
- Unterstützte Instance-Typen
- Berechtigungen für --Benutzer
- Berechtigungen für Instances

Unterstützte Volume-Typen

Die Verschlüsselung wird von allen Arten von EBS-Volumes unterstützt. Sie können bei verschlüsselten Volumes dieselbe IOPS-Leistung voraussetzen wie bei unverschlüsselten Volumes, mit minimalen Auswirkungen auf die Latenz. Der Zugriff auf verschlüsselte Volumes erfolgt genau wie der Zugriff auf andere Volumes. Ver- und Entschlüsselung werden transparent behandelt und erfordern von Ihnen oder Ihren Anwendungen keine weiteren Aktionen.

Unterstützte Instance-Typen

Die Amazon EBS-Verschlüsselung ist für alle Instance-Typen der aktuellen und vorherigen Generation verfügbar.

Berechtigungen für --Benutzer

Wenn Sie einen KMS-Schlüssel für die EBS-Verschlüsselung verwenden, ermöglicht die KMS-Schlüsselrichtlinie jedem Benutzer mit Zugriff auf die erforderlichen AWS KMS Aktionen, diesen KMS-Schlüssel zum Verschlüsseln oder Entschlüsseln von EBS-Ressourcen zu verwenden. Sie müssen Benutzern die Berechtigung zum Aufrufen der folgenden Aktionen gewähren, um die EBS-Verschlüsselung zu verwenden:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn der Zuschuss im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter Erlaubt den Zugriff auf das AWS Konto und aktiviert IAM-Richtlinien im Abschnitt Standardschlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch.

Berechtigungen für Instances

Wenn eine Instance versucht, mit einem verschlüsselten AMI, Volume oder Snapshot zu interagieren, wird der reine Identitätsrolle der Instance ein KMS-Schlüssel gewährt. Die reine Identitätsrolle ist

eine IAM-Rolle, die von der Instance verwendet wird, um mit verschlüsselten AMIs, Volumes oder Snapshots in Ihrem Namen zu interagieren.

Identity-only Rollen müssen nicht manuell erstellt oder gelöscht werden, und ihnen sind keine Richtlinien zugeordnet. Außerdem haben Sie keinen Zugriff auf die Anmeldeinformationen, die nur für Identitätsrollen gelten.

> **Note**
>
> Identity-only Rollen werden von Anwendungen auf Ihrer Instance nicht für den Zugriff auf andere AWS KMS verschlüsselte Ressourcen wie Amazon S3-Objekte oder Dynamo-DB-Tabellen verwendet. Diese Operationen werden mithilfe der Anmeldeinformationen einer Amazon EC2-Instance-Rolle oder anderer AWS Anmeldeinformationen ausgeführt, die Sie auf Ihrer Instance konfiguriert haben.

Identity-only Rollen unterliegen Service Control Policies (SCPs) und KMS-Schlüsselrichtlinien. Wenn ein SCP- oder KMS-Schlüssel der reinen Identitätsrolle den Zugriff auf einen KMS-Schlüssel verweigert, kann es sein, dass Sie EC2-Instances nicht mit verschlüsselten Volumes oder mit verschlüsselten AMIs oder Snapshots starten können.

Wenn Sie eine SCP- oder Schlüsselrichtlinie erstellen, die den Zugriff anhand des Netzwerkstandorts mithilfe der `aws:SourceVpce` AWS globalen Bedingungsschlüssel `aws:SourceIpaws:VpcSourceIp`,`aws:SourceVpc`,, oder verweigert, müssen Sie sicherstellen, dass diese Richtlinienanweisungen nicht für reine Instanzrollen gelten. Beispiele für Richtlinien finden Sie unter Beispiele für Datenperimeter-Richtlinien.

Identity-only Rollen-ARNs verwenden das folgende Format:

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

Wenn einer Instance ein Schlüssel gewährt wird, wird der Schlüssel an die für diese spezielle Instance geltende Sitzung mit der angenommenen Rolle gewährt. Der Prinzipal-ARN des Bewilligungsempfängers verwendet das folgende Format:

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

Aktivieren Sie standardmäßig die Amazon EBS-Verschlüsselung

Sie können Ihr AWS Konto so konfigurieren, dass die Verschlüsselung der neuen EBS-Volumes und Snapshot-Kopien, die Sie erstellen, erzwungen wird. Beispielsweise verschlüsselt Amazon EBS die beim Starten einer Instance erstellten EBS-Volumes und die Snapshots, die Sie aus einem nicht verschlüsselten Snapshot oder Volume erstellen. Beispiele für den Wechsel von unverschlüsselten zu verschlüsselten EBS-Ressourcen finden Sie unter Verschlüsseln unverschlüsselter Ressourcen.

Die standardmäßige Verschlüsselung wirkt sich nicht auf vorhandene EBS-Volumes oder Snapshots aus.

Überlegungen

- Die Verschlüsselung ist standardmäßig eine Region-specific Einstellung. Wenn Sie sie für eine Region aktivieren, kann sie nicht für einzelne Volumes oder Snapshots in dieser Region deaktiviert werden.
- Die Amazon EBS-Verschlüsselung wird standardmäßig auf allen Instance-Typen der aktuellen und vorherigen Generation unterstützt.
- Wenn Sie einen Snapshot kopieren und mit einem neuen KMS-Schlüssel verschlüsseln, wird eine vollständige (nicht inkrementelle) Kopie erstellt. Dies führt zu zusätzlichen Lagerkosten.

Console

So aktivieren Sie die standardmäßige Verschlüsselung für eine Region

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste die Region aus.
3. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Datenschutz und Sicherheit aus.
4. Wählen Sie im Abschnitt EBS-Verschlüsselung die Option Verwalten aus.
5. Wählen Sie Enable (Aktivieren). Sie behalten den Von AWS verwalteter Schlüssel mit dem in Ihrem Namen `aws/ebs` erstellten Alias als Standardverschlüsselungsschlüssel bei oder wählen einen symmetrischen, vom Kunden verwalteten Verschlüsselungsschlüssel.
6. Wählen Sie Update EBS encryption (EBS-Verschlüsselung aktualisieren).

AWS CLI

Um die Standardeinstellung der Verschlüsselung anzuzeigen

Verwenden Sie den Befehl get-ebs-encryption-by-default.

- Für eine bestimmte Region

```
aws ec2 get-ebs-encryption-by-default --region region
```

- Für alle Regionen in Ihrem Konto

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 get-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

So aktivieren Sie die Verschlüsselung standardmäßig

Verwenden Sie den https://docs.aws.amazon.com/cli/latest/reference/ec2/enable-ebs-encryption-by-default.html Befehl enable-ebs-encryption-by-default.

- Für eine bestimmte Region

```
aws ec2 enable-ebs-encryption-by-default --region region
```

- Für alle Regionen in Ihrem Konto

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 enable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
```

```
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

So deaktivieren Sie die Verschlüsselung standardmäßig

Verwenden Sie den https://docs.aws.amazon.com/cli/latest/reference/ec2/disable-ebs-encryption-by-default.html Befehl disable-ebs-encryption-by-default.

- Für eine bestimmte Region

```
aws ec2 disable-ebs-encryption-by-default --region region
```

- Für alle Regionen in Ihrem Konto

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 disable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

PowerShell

Um die Standardeinstellung der Verschlüsselung anzuzeigen

Verwenden Sie das cmdlet Get-EC2EbsEncryptionByDefault.

- Für eine bestimmte Region

```
Get-EC2EbsEncryptionByDefault -Region region
```

- Für alle Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName |
```

```
    ForEach-Object {
    [PSCustomObject]@{
        Region                      = $_
        EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |
    Format-Table -AutoSize
```

So aktivieren Sie die Verschlüsselung standardmäßig

Verwenden Sie das cmdlet Enable-EC2EbsEncryptionByDefault.

- Für eine bestimmte Region

```
Enable-EC2EbsEncryptionByDefault -Region region
```

- Für alle Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName |
    ForEach-Object {
    [PSCustomObject]@{
        Region                      = $_
        EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |
    Format-Table -AutoSize
```

So deaktivieren Sie die Verschlüsselung standardmäßig

Verwenden Sie das cmdlet Disable-EC2EbsEncryptionByDefault.

- Für eine bestimmte Region

```
Disable-EC2EbsEncryptionByDefault -Region region
```

- Für alle Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName |
    ForEach-Object {
    [PSCustomObject]@{
        Region                      = $_
```

```
        EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |
    Format-Table -AutoSize
```

Sie können den KMS-Schlüssel, der einem vorhandenen Snapshot oder verschlüsselten Volume zugeordnet ist, nicht ändern. Sie können jedoch beim Kopieren eines Snapshots einen anderen Verschlüsselung zuweisen, sodass der kopierte Snapshot anschließend mit dem neuen Verschlüsselung verschlüsselt wird.

Standard-Verschlüsselungsschlüssel

Amazon EBS erstellt automatisch einen eindeutigen Wert Von AWS verwalteter Schlüssel in jeder Region, in der Sie Amazon EBS-Ressourcen erstellen. Der Alias für diesen KMS-Schlüssel lautet. `aws/ebs` Dies ist Ihr Standard-Verschlüsselungsschlüssel. Sie können den Standardverschlüsselungsschlüssel in einen vom Kunden verwalteten Schlüssel ändern.

Verwenden Sie eine der folgenden Methoden, um den Standardverschlüsselungsschlüssel für eine Region zu ändern.

Console

Um den Standardverschlüsselungsschlüssel für eine Region zu ändern

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste die Region aus.
3. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Datenschutz und Sicherheit aus.
4. Wählen Sie im Abschnitt EBS-Verschlüsselung die Option Verwalten aus.
5. Wählen Sie für den Standardverschlüsselungsschlüssel die KMS-Schlüssel-ID aus, die Sie verwenden möchten.
6. Wählen Sie Update EBS encryption (EBS-Verschlüsselung aktualisieren).

AWS CLI

Verwenden Sie den Befehl modify-ebs-default-kms-key-id.

```
aws ec2 modify-ebs-default-kms-key-id --kms-key-id key-id --region region
```

PowerShell

Verwenden Sie das cmdlet Edit-EC2EbsDefaultKmsKeyId.

```
Edit-EC2EbsDefaultKmsKeyId -KmsKeyId key-id -Region region
```

Verschlüsseln von EBS-Ressourcen

Sie verschlüsseln EBS-Volumes, indem Sie die Verschlüsselung aktivieren. Hierzu verwenden Sie entweder die standardmäßige Verschlüsselung oder aktivieren die Verschlüsselung beim Erstellen eines Volumes, das Sie verschlüsseln möchten.

Wenn Sie ein Volume verschlüsseln, können Sie den symmetrischen KMS-Schlüssel zur Verschlüsselung angeben, der für die Verschlüsselung des Volumes verwendet wird. Wenn Sie keinen Verschlüsselung angeben, ist der für die Verschlüsselung verwendete Verschlüsselung vom Verschlüsselungszustand des Quell-Snapshots und von dessen Besitzer abhängig. Weitere Informationen finden Sie in der Tabelle der Verschlüsselungsergebnisse.

> **Note**
>
> Wenn Sie die API verwenden oder einen KMS-Schlüssel angeben möchten, beachten Sie, AWS CLI dass der KMS-Schlüssel asynchron authentifiziert wird. AWS Wenn Sie eine Verschlüsselung-ID, einen Aliasnamen oder ARN angeben, die nicht gültig sind, kann es so wirken, als würde die Aktion abgeschlossen, aber schlussendlich schlägt sie fehl.

Sie können den Verschlüsselung, der mit einem vorhandenen Snapshot oder Volume verknüpft ist, nicht ändern. Sie können jedoch beim Kopieren eines Snapshots einen anderen Verschlüsselung zuweisen, sodass der kopierte Snapshot anschließend mit dem neuen Verschlüsselung verschlüsselt wird.

Verschlüsseln eines leeren Volumes bei der Erstellung

Wenn Sie ein neues, leeres EBS-Volume erstellen, können Sie es durch die Aktivierung der Verschlüsselung für den spezifischen Volume-Erstellungsvorgang verschlüsseln. Wenn Sie standardmäßig die EBS-Verschlüsselung aktiviert haben, wird das Volume automatisch mit Ihrem

Standard-Verschlüsselung für die EBS-Verschlüsselung verschlüsselt. Alternativ können Sie einen anderen symmetrischen KMS-Schlüssel zur Verschlüsselung für den spezifischen Volume-Erstellungsvorgang angeben. Das Volume ist zum Zeitpunkt der Verfügbarkeit verschlüsselt, sodass Ihre Daten stets sicher sind. Die detaillierten Schritte finden Sie unter Erstellen Sie ein Amazon EBS-Volume.

Standardmäßig verschlüsselt der beim Erstellen des Volumes ausgewählte Verschlüsselung die Snapshots, die Sie für das Volume erstellen, und die Volumes, die Sie aus diesen verschlüsselten Snapshots wiederherstellen. Sie können die Verschlüsselung eines verschlüsselten Volumes oder Snapshots nicht entfernen. Das bedeutet, dass ein Volume, das aus einem verschlüsselten Snapshot oder einer Kopie eines verschlüsselten Snapshots wiederhergestellt wurde, stets verschlüsselt ist.

Öffentliche Snapshots verschlüsselter Volumes werden nicht unterstützt, aber Sie können einen verschlüsselten Snapshot für bestimmte Konten freigeben. Detaillierte Anweisungen finden Sie unter Teilen Sie einen Amazon EBS-Snapshot mit anderen AWS Konten.

Verschlüsseln unverschlüsselter Ressourcen

Sie können vorhandene unverschlüsselte Volumes oder Snapshots nicht direkt verschlüsseln.

Um ein unverschlüsseltes Volume zu verschlüsseln, erstellen Sie einen Snapshot dieses Volumes und verwenden Sie dann den Snapshot, um ein neues verschlüsseltes Volume zu erstellen. Weitere Informationen erhalten Sie unter Erstellen von -Snapshots und Ein Volume erstellen.

Um einen unverschlüsselten Snapshot zu verschlüsseln, erstellen Sie eine verschlüsselte Kopie dieses Snapshots. Weitere Informationen finden Sie unter Kopieren eines -Snapshots.

Wenn Sie Ihr Konto standardmäßig für die Verschlüsselung aktivieren, werden Volumes und Snapshot-Kopien, die aus unverschlüsselten Snapshots erstellt wurden, immer verschlüsselt. Andernfalls müssen Sie die Verschlüsselungsparameter in der Anfrage angeben. Weitere Informationen finden Sie unter Aktivieren Sie standardmäßig die Verschlüsselung.

Drehen AWS KMS Schlüssel, die für die Amazon EBS-Verschlüsselung verwendet werden

Die bewährten Methoden für die Kryptografie raten von einer extensiven Weiterverwendung von Verschlüsselungsschlüsseln ab.

Um neues kryptografisches Material für die Verwendung mit der Amazon EBS-Verschlüsselung zu erstellen, können Sie entweder einen neuen, vom Kunden verwalteten Schlüssel erstellen und dann

Ihre Anwendungen so ändern, dass sie diesen neuen KMS-Schlüssel verwenden. Oder Sie können die automatische Schlüsselrotation für einen vorhandenen, vom Kunden verwalteten Schlüssel aktivieren.

Wenn Sie die automatische Schlüsselrotation für einen vom Kunden verwalteten Schlüssel aktivieren, AWS KMS generiert jedes Jahr neues kryptografisches Material für den KMS-Schlüssel. AWS KMS speichert alle früheren Versionen des kryptografischen Materials, sodass Sie Volumes und Snapshots, die zuvor mit diesem KMS-Schlüsselmaterial verschlüsselt wurden, weiterhin entschlüsseln und verwenden können. AWS KMS löscht kein rotiertes Schlüsselmaterial, bis Sie den KMS-Schlüssel löschen.

Wenn Sie einen rotierten, vom Kunden verwalteten Schlüssel verwenden, um ein neues Volume oder einen neuen Snapshot zu verschlüsseln, AWS KMS wird das aktuelle (neue) Schlüsselmaterial verwendet. Wenn Sie einen rotierten, vom Kunden verwalteten Schlüssel zum Entschlüsseln eines Volumes oder Snapshots verwenden, AWS KMS wird die Version des kryptografischen Materials verwendet, mit der es verschlüsselt wurde. Wenn ein Volume oder Snapshot mit einer früheren Version des kryptografischen Materials verschlüsselt ist, verwendet AWS KMS weiterhin diese vorherige Version, um es zu entschlüsseln. AWS KMS verschlüsselt zuvor verschlüsselte Volumes oder Snapshots nicht erneut, um das neue kryptografische Material nach einer Schlüsselrotation zu verwenden. Sie bleiben mit dem kryptografischen Material verschlüsselt, mit dem sie ursprünglich verschlüsselt wurden. Sie können einen rotierten, vom Kunden verwalteten Schlüssel problemlos in Anwendungen und AWS Diensten verwenden, ohne dass der Code geändert werden muss.

> **Note**
>
> - Die automatische Schlüsselrotation wird nur für symmetrische, vom Kunden verwaltete Schlüssel unterstützt, bei denen Schlüsselmaterial AWS KMS entsteht.
> - AWS KMS rotiert automatisch Von AWS verwaltete Schlüssel jedes Jahr. Sie können die Schlüsselrotation von Von AWS verwaltete Schlüssel nicht aktivieren oder deaktivieren.

Weitere Informationen finden Sie unter Rotieren von KMS-Schlüsseln im Entwicklerhandbuch von AWS Key Management Service .

Beispiele für Amazon EBS-Verschlüsselung

Wenn Sie eine verschlüsselte EBS-Ressource erstellen, wird sie mit dem Standard-VerschlüsselungIhres Kontos für die EBS-Verschlüsselung verschlüsselt, wenn Sie in den

Parametern für die Volume-Erstellung oder in der Blockgerät-Zuweisung für den AMI oder die Instance keinen anderen Kundenverwalteter Schlüssel angegeben haben.

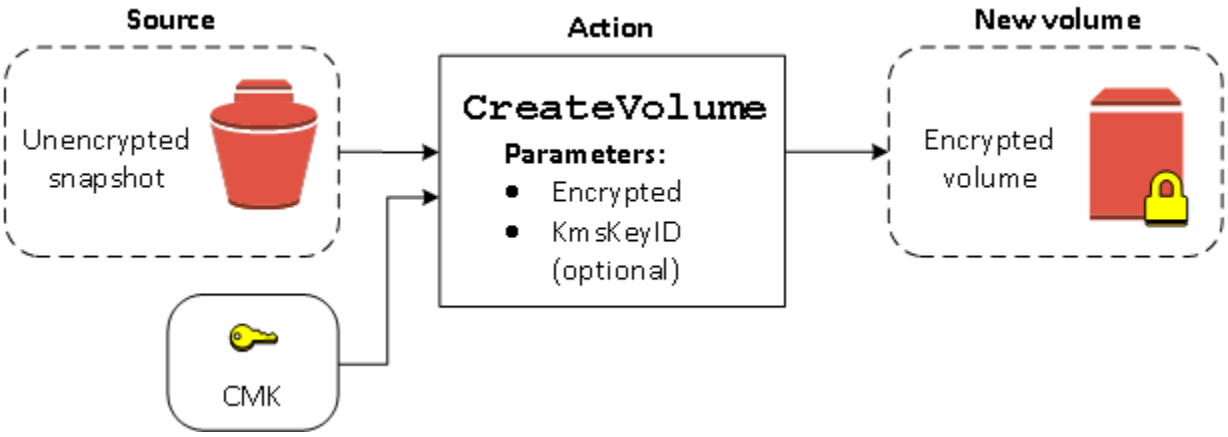
Das folgende Beispiel zeigt die Verwaltung des Verschlüsselungszustands Ihrer Volumes und Snapshots. Die vollständige Liste der Verschlüsselungsszenarien finden Sie in der Tabelle der Verschlüsselungsergebnisse.

Beispiele

- Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung nicht aktiviert)
- Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung aktiviert)
- Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung nicht aktiviert)
- Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung aktiviert)
- Re-encrypt ein verschlüsseltes Volume
- Re-encrypt ein verschlüsselter Snapshot
- Migrieren von Daten zwischen verschlüsselten und unverschlüsselten Volumes
- Verschlüsselungsergebnisse

Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung nicht aktiviert)

Ohne die aktivierte standardmäßige Verschlüsselung ist ein Volume, das aus einem unverschlüsselten Snapshot wiederhergestellt wurde, standardmäßig unverschlüsselt. Sie können jedoch das resultierende Volume verschlüsseln, indem Sie den `Encrypted`-Parameter und optional den `KmsKeyId`-Parameter festlegen. Das folgende Diagramm zeigt den Prozess.

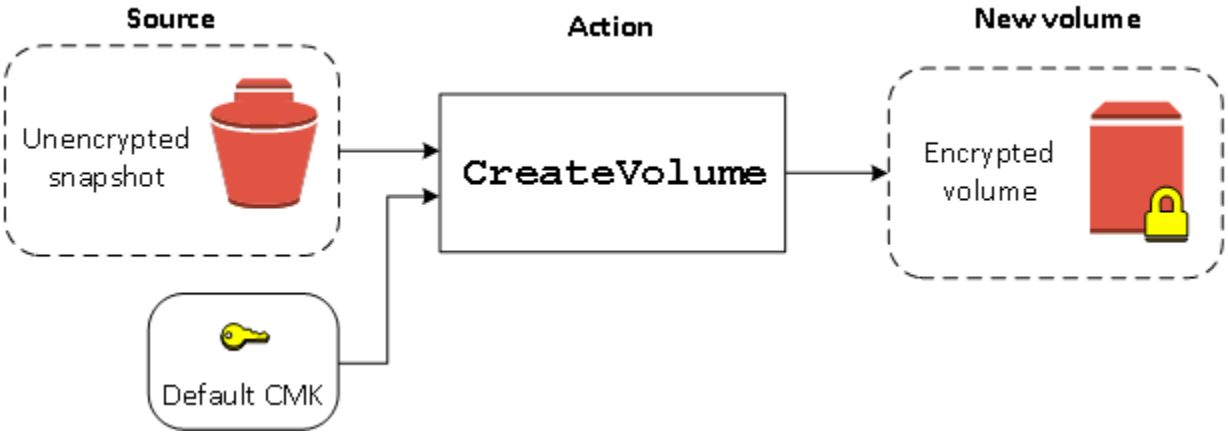


Wenn Sie den Parameter `KmsKeyId` auslassen, wird das resultierende Volume mit Ihrem Standard-Verschlüsselung für die EBS-Verschlüsselung verschlüsselt. Sie müssen eine Verschlüsselung-ID angeben, um das Volume mit einem anderen Verschlüsselung zu verschlüsseln.

Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.

Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung aktiviert)

Wenn Sie die standardmäßige Verschlüsselung aktiviert haben, ist die Verschlüsselung für Volumes, die aus unverschlüsselten Snapshots wiederhergestellt wurden, zwingend erforderlich und es sind keine Verschlüsselungsparameter für Ihren Standard-Verschlüsselung erforderlich. Im folgenden Diagramm wird dieser einfache Standardfall veranschaulicht:

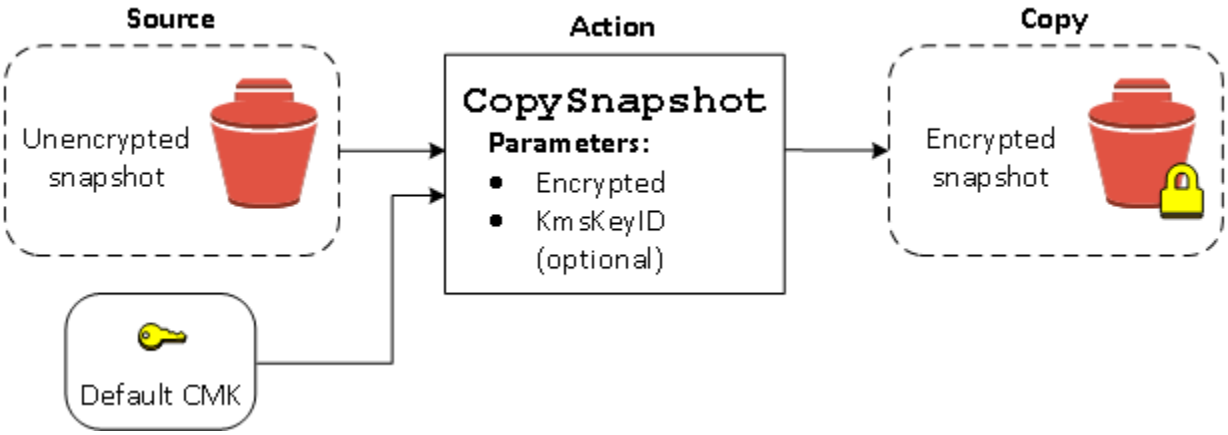


Wenn Sie das wiederhergestellte Volume mit einem symmetrischen vom Kunden verwalteten Verschlüsselungsschlüssel verschlüsseln möchten, müssen Sie sowohl die `Encrypted`- als auch die `KmsKeyId`-Parameter, wie in Wiederherstellen eines unverschlüsselten Volumes (standardmäßige Verschlüsselung nicht aktiviert) gezeigt, angeben.

Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung nicht aktiviert)

Ohne aktivierte standardmäßige Verschlüsselung ist eine unverschlüsselte Snapshot-Kopie standardmäßig unverschlüsselt. Sie können jedoch den resultierenden Snapshot verschlüsseln, indem Sie den `Encrypted`-Parameter und optional den `KmsKeyId`-Parameter festlegen. Wenn Sie `KmsKeyId` weglassen, wird der resultierende Snapshot mit Ihrem Standard-Verschlüsselung verschlüsselt. Sie müssen eine Verschlüsselungs-ID angeben, um das Volume mit einem anderen symmetrischen KMS-Schlüssel zur Verschlüsselung zu verschlüsseln.

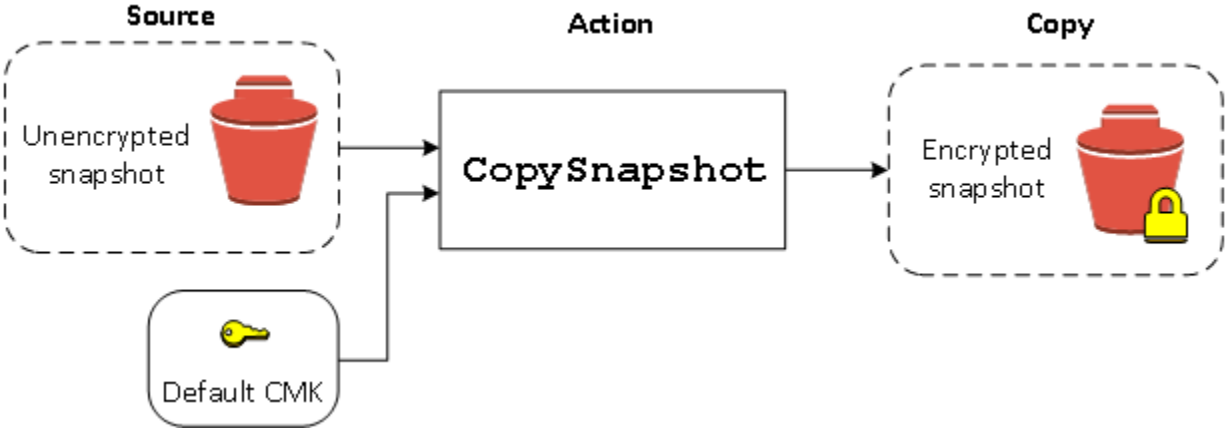
Das folgende Diagramm zeigt den Prozess.



Sie können ein EBS-Volume verschlüsseln, indem Sie einen unverschlüsselten Snapshot in einen verschlüsselten Snapshot kopieren und dann ein Volume aus dem verschlüsselten Snapshot erstellen. Weitere Informationen finden Sie unter Kopieren Sie einen Amazon EBS-Snapshot.

Kopieren eines unverschlüsselten Snapshots (standardmäßige Verschlüsselung aktiviert)

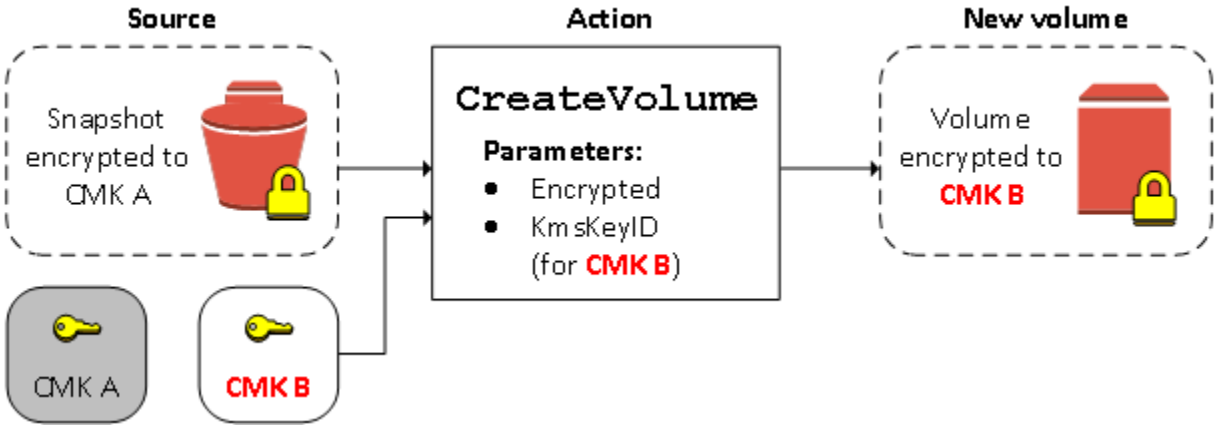
Wenn Sie die standardmäßige Verschlüsselung aktiviert haben, ist die Verschlüsselung für unverschlüsselte Snapshot-Kopien zwingend erforderlich und es sind keine Verschlüsselungsparameter erforderlich, wenn der Standard-Verschlüsselung verwendet wird. Das folgende Diagramm veranschaulicht diesen Standardfall.



Re-encrypt ein verschlüsseltes Volume

Wenn die `CreateVolume`-Aktion für einen verschlüsselten Snapshot ausgeführt wird, haben Sie die Möglichkeit, ihn mit einem anderen Verschlüsselung erneut zu verschlüsseln. Das folgende

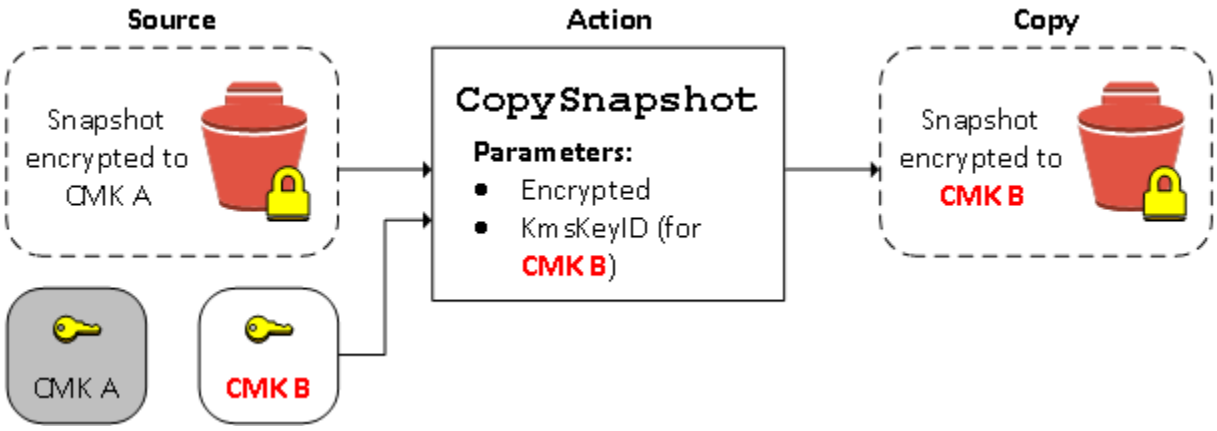
Diagramm zeigt den Prozess. In diesem Beispiel besitzen Sie zwei KMS-Schlüssel, Verschlüsselung A und Verschlüsselung B. Der Quell-Snapshot wird mit Verschlüsselung A verschlüsselt. Während der Volume-Erstellung wird die Verschlüsselung-ID von Verschlüsselung B als Parameter angegeben. Die Quelldaten werden automatisch entschlüsselt und dann mit Verschlüsselung B erneut verschlüsselt.



Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.

Re-encrypt ein verschlüsselter Snapshot

Durch die Möglichkeit, einen Snapshot beim Kopieren zu verschlüsseln, können Sie einen neuen symmetrischen KMS-Schlüssel zur Verschlüsselung auf einen bereits verschlüsselten Snapshot anwenden, den Sie besitzen. Auf Volumes, die aus dieser verschlüsselten Kopie wiederhergestellt wurden, kann nur mit dem neuen Verschlüsselung zugegriffen werden. Das folgende Diagramm zeigt den Prozess. In diesem Beispiel besitzen Sie zwei KMS-Schlüssel, Verschlüsselung A und Verschlüsselung B. Der Quell-Snapshot wird mit Verschlüsselung A verschlüsselt. Während des Kopierens wird die Verschlüsselung-ID von Verschlüsselung B als Parameter angegeben. Die Quelldaten werden automatisch mit Verschlüsselung B erneut verschlüsselt.



Ein ähnliches Szenario liegt vor, wenn Sie neue Verschlüsselungsparameter auf eine Kopie eines Snapshot anwenden möchten, der für Sie freigegeben wurde. Die Kopie ist standardmäßig mit einem Verschlüsselung verschlüsselt, den der Eigentümer des Snapshots freigegeben hat. Wir empfehlen jedoch, dass Sie eine Kopie des geteilten Snapshot mit einem anderen Verschlüsselung, den Sie kontrollieren, erstellen. Dies schützt Ihren Zugriff auf das Volume, wenn der Original-Verschlüsselung kompromittiert wurde oder der Eigentümer den Verschlüsselung aus einem beliebigen Grund widerruft. Weitere Informationen finden Sie unter Verschlüsselung und Kopieren von Snapshots.

Migrieren von Daten zwischen verschlüsselten und unverschlüsselten Volumes

Wenn Sie Zugriff auf ein verschlüsseltes und ein unverschlüsseltes Volume haben, können Sie jederzeit Daten vom einen zum anderen übertragen. EC2 führt die Verschlüsselungs- und Entschlüsselungsvorgänge auf transparente Weise aus.

Linux-Instances

Verwenden Sie zum Beispiel den Befehl rsync zum Kopieren der Daten. Im folgenden Befehl befinden sich die Quelldaten in `/mnt/source` und das Ziel-Volume ist unter `/mnt/destination` gemountet.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

Windows-Instances

Verwenden Sie zum Beispiel den Befehl robocopy zum Kopieren der Daten. Im folgenden Befehl befinden sich die Quelldaten in `D:\` und das Ziel-Volume ist unter `E:\` gemountet.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

Wir empfehlen die Verwendung von Ordnern, anstatt das gesamte Volume zu kopieren, da so potenzielle Probleme mit verborgenen Ordnern vermieden werden.

Verschlüsselungsergebnisse

Die folgende Tabelle zeigt das Verschlüsselungsergebnis für jede mögliche Kombination von Einstellungen.

Ist Verschlüsselung aktiviert?	Ist Verschlüsselung standardmäßig aktiviert?	Quelle des Volumes	Standard (kein vom Kunden verwalteter Schlüssel angegeben)	Benutzerdefiniert (vom Kunden verwalteter Schlüssel angegeben)
Nein	Nein	Neues (leeres) Volume	Unverschlüsselt	N/A
Nein	Nein	Unverschlüsselter eigener Snapshot	Unverschlüsselt	
Nein	Nein	Verschlüsselter eigener Snapshot	Verschlüsselt mit demselben Schlüssel	
Nein	Nein	Unverschlüsselter Snapshot, der mit Ihnen geteilt wird	Unverschlüsselt	
Nein	Nein	Verschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel*	
Ja	Nein	Neues Volume	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	Verschlüsselt durch angegebenen vom Kunden verwalteten Schlüssel**
Ja	Nein	Unverschlüsselter eigener Snapshot	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	

Ist Verschlüsselung aktiviert?	Ist Verschlüsselung standardmäßig aktiviert?	Quelle des Volumes	Standard (kein vom Kunden verwalteter Schlüssel angegeben)	Benutzerdefiniert (vom Kunden verwalteter Schlüssel angegeben)
Ja	Nein	Verschlüsselter eigener Snapshot	Verschlüsselt mit demselben Schlüssel	
Ja	Nein	Unverschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Ja	Nein	Verschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Nein	Ja	Neues (leeres) Volume	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	N/A
Nein	Ja	Unverschlüsselter eigener Snapshot	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Nein	Ja	Verschlüsselter eigener Snapshot	Verschlüsselt mit demselben Schlüssel	

Ist Verschlüsselung aktiviert?	Ist Verschlüsselung standardmäßig aktiviert?	Quelle des Volumes	Standard (kein vom Kunden verwalteter Schlüssel angegeben)	Benutzerdefiniert (vom Kunden verwalteter Schlüssel angegeben)
Nein	Ja	Unverschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Nein	Ja	Verschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Ja	Ja	Neues Volume	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	Verschlüsselt durch angegebenen vom Kunden verwalteten Schlüssel
Ja	Ja	Unverschlüsselter eigener Snapshot	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Ja	Ja	Verschlüsselter eigener Snapshot	Verschlüsselt mit demselben Schlüssel	

Ist Verschlüsselung aktiviert?	Ist Verschlüsselung standardmäßig aktiviert?	Quelle des Volumes	Standard (kein vom Kunden verwalteter Schlüssel angegeben)	Benutzerdefiniert (vom Kunden verwalteter Schlüssel angegeben)
Ja	Ja	Unverschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	
Ja	Ja	Verschlüsselter Snapshot, der mit Ihnen geteilt wird	Verschlüsselt durch standardmäßigen vom Kunden verwalteten Schlüssel	

* Dies ist der vom Kunden verwaltete Standardschlüssel, der für die EBS-Verschlüsselung für das AWS Konto und die Region verwendet wird. Standardmäßig ist dies ein eindeutiger Von AWS verwalteter Schlüssel EBS-Schlüssel, oder Sie können einen vom Kunden verwalteten Schlüssel angeben.

** Dies ist ein vom Kunden verwalteter Schlüssel, der beim Start für das Volume angegeben wurde. Dieser vom Kunden verwaltete Schlüssel wird anstelle des standardmäßigen kundenverwalteten Schlüssels für das AWS Konto und die Region verwendet.

Leistung des Amazon EBS-Volumes

Verschiedene Faktoren, einschließlich der I/O Eigenschaften und der Konfiguration Ihrer Instances und Volumes, können die Leistung von Amazon EBS beeinflussen. Wenn Sie die Anweisungen auf unseren Amazon EBS- und Amazon EC2-Produktdetailseiten befolgen, erzielen Sie in der Regel eine gute Leistung. Es gibt jedoch einige Fälle, in denen Sie möglicherweise einige Optimierungen vornehmen müssen, um eine Spitzenleistung zu erzielen. Wir empfehlen Ihnen, die Leistung anhand von Informationen aus Ihrer tatsächlichen Workload zu optimieren und mithilfe von Benchmark-Tests die optimale Konfiguration zu finden. Nachdem Sie sich mit den Grundlagen der Arbeit mit EBS-Volumes vertraut gemacht haben, sollten Sie sich ansehen, welche I/O Leistung Sie benötigen und welche Optionen Sie haben, um die Amazon EBS-Leistung zu erhöhen, um diese Anforderungen zu erfüllen.

AWS Aktualisierungen der Leistung von EBS-Volumetypen werden möglicherweise nicht sofort auf Ihre vorhandenen Volumes wirksam. Zum Anzeigen der vollen Leistung eines älteren Volumes müssen Sie zunächst eine `ModifyVolume`-Aktion darauf ausführen. Weitere Informationen finden Sie unter Ändern Sie ein Amazon EBS-Volume mithilfe von Elastic Volumes-Vorgängen.

Inhalt

- Tipps zur Amazon EBS-Leistung
- Amazon-EBS-Optimierung
- Initialisieren von Volumes Amazon EBS
- Konfigurierbare Gewichtung der Instanz-Bandbreite
- I/O Eigenschaften und Überwachung von Amazon EBS
- Amazon EBS- und RAID-Konfiguration
- Benchmarken Sie Amazon EBS-Volumes

Tipps zur Amazon EBS-Leistung

Diese Tipps stellen die bewährten Methoden dar, um in einer Vielzahl von Benutzerszenarien die optimale Leistung für EBS-Volumes zu erzielen.

Verwenden Sie Instanzen EBS-optimized

Bei Instances ohne EBS-optimized Durchsatzunterstützung kann der Netzwerkverkehr mit dem Verkehr zwischen Ihrer Instance und Ihren EBS-Volumes überlastet werden. Bei EBS-optimized Instances werden die beiden Arten von Datenverkehr getrennt. Für einige EBS-optimized Instance-Konfigurationen fallen zusätzliche Kosten an (wie C3, R3 und M3), während für andere immer EBS-optimized keine zusätzlichen Kosten anfallen (wie M4, C4, C5 und D2). Weitere Informationen finden Sie unter Amazon-EBS-Optimierung.

Konfigurieren Sie die Instanzbandbreite

Für unterstützte Instance-Typen können Sie die Gewichtung der Instance-Bandbreite so konfigurieren, dass die Amazon EBS-Bandbreite mithilfe der Bandbreitengewichtung um 25 Prozent erhöht wird. `ebs-1` Mit dieser Funktion können Sie die Netzwerkressourcenzuweisung Ihrer Instance zwischen EBS- und VPC-Netzwerken optimieren und so möglicherweise die EBS-Leistung für Workloads verbessern. I/O-intensive Weitere Informationen finden Sie unter Konfigurierbare Gewichtung der Instanz-Bandbreite.

Informationen zum Berechnen der Leistung

Wenn Sie die Leistung Ihrer EBS-Volumes messen, sollten Sie die verwendeten Maßeinheiten kennen und wissen, wie die Leistung berechnet wird. Weitere Informationen finden Sie unter I/O Eigenschaften und Überwachung von Amazon EBS.

Informationen zum Workload

Es besteht ein Zusammenhang zwischen der maximalen Leistung Ihrer EBS-Volumes, der Größe und Anzahl der I/O Operationen und der Zeit, die für die Ausführung der einzelnen Aktionen benötigt wird. Jeder dieser Faktoren (Leistung und Latenz) wirkt sich auf die anderen aus, und verschiedene Anwendungen reagieren empfindlicher auf den einen oder anderen Faktor. I/O Weitere Informationen finden Sie unter Benchmarken Sie Amazon EBS-Volumes.

Berücksichtigen der Leistungseinbußen, die beim Initialisieren von Volumes aus Snapshots auftreten

Die Latenz steigt erheblich an, wenn Sie zuerst auf jeden Datenblock in einem neuen EBS-Volume zugreifen, das aus einem Snapshot erstellt wurde. Sie können diesen Leistungseinbruch mit einer der folgenden Optionen vermeiden:

- Greifen Sie auf jeden Block zu, bevor Sie das Volumen in die Produktion bringen. Dieser Prozess heißt Initialisierung (früher als "Vorwärmung" bezeichnet). Weitere Informationen finden Sie unter Initialisieren Sie die Volumes nach der Erstellung manuell.
- Ermöglichen Sie die schnelle Snapshot-Wiederherstellung auf einem Snapshot, um sicherzustellen, dass die daraus erstellten EBS-Volumes bei der Erstellung vollständig initialisiert werden und sofort die gesamte bereitgestellte Leistung bereitstellen. Weitere Informationen finden Sie unter Schnelle Amazon EBS-Snapshot-Wiederherstellung.

Faktoren, die die HDD-Leistung beeinträchtigen können

Wenn Sie einen Snapshot eines durchsatzoptimierten HDD-Volumes (`st1`) oder Cold-HDD-Volumes (`sc1`) erstellen, kann die Leistung bis auf den Basiswert des Volumes absinken, während der Snapshot generiert wird. Dieses Verhalten ist für diese Volume-Typen spezifisch. Zu den weiteren Faktoren, die die Leistung einschränken können, gehören ein höherer Durchsatz, als die Instance unterstützen kann, Leistungseinbußen bei der Initialisierung von Volumes, die aus einem Snapshot erstellt wurden, und zu viele kleine, zufällige Mengen auf dem Volume. I/O Weitere Informationen zum Berechnen des Durchsatzes für HDD-Volumes finden Sie unter Amazon EBS-Volume-Typen.

Ihre Leistung kann auch beeinträchtigt werden, wenn Ihre Anwendung nicht genügend I/O Anfragen sendet. Dies kann anhand der Warteschlangenlänge und I/O -größe Ihres Volumes überwacht werden. Die Warteschlangenlänge ist die Anzahl der ausstehenden I/O Anfragen von Ihrer Anwendung auf Ihr Volume. Um eine maximale Konsistenz zu gewährleisten, müssen HDD-backed Volumes eine Warteschlangenlänge (auf die nächste ganze Zahl gerundet) von 4 oder mehr einhalten, wenn eine I/O sequentielle Ausführung von 1 MiB erfolgt. Weitere Informationen zur Leistungsoptimierung Ihrer Volumes finden Sie unter I/O Eigenschaften und Überwachung von Amazon EBS.

Erhöhen Sie den Read-Ahead-Wert für Workloads mit hohem Durchsatz und leseintensiven Workloads auf st1 und sc1 (Nur Linux-Instanzen)

Einige Workloads sind leseintensiv und greifen über den Betriebssystem-Seiten-Cache auf das Blockgerät zu (z. B. aus einem Dateisystem). Um den maximalen Durchsatz zu erzielen, empfehlen wir in diesem Fall, eine Read-Ahead-Einstellung von 1 MiB zu konfigurieren. Dies ist eine Blockgerät-spezifische Einstellung, die nur auf Ihre HDD-Volumes angewendet werden sollte.

Verwenden Sie den folgenden Befehl, um den aktuellen Wert des Read-Aheads für Ihre Blockgeräte zu überprüfen:

```
$ sudo blockdev --report /dev/<device>
```

Die Blockgerätinformationen werden im folgenden Format zurückgegeben:

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

Das angezeigte Gerät meldet einen Read-Ahead-Wert (RA) von 256 (Standardwert). Multiplizieren Sie diese Zahl mit der Sektorgröße (512 Bytes), um die Größe des Read-Ahead-Puffers zu ermitteln, der in diesem Fall 128 KiB groß ist. Verwenden Sie den folgenden Befehl, um den Pufferwert auf 1 MiB festzulegen:

```
$ sudo blockdev --setra 2048 /dev/<device>
```

Stellen Sie sicher, dass für die Read-Ahead-Einstellung nun 2 048 angezeigt wird, indem Sie den ersten Befehl erneut ausführen.

Verwenden Sie diese Einstellung nur, wenn Ihre Arbeitslast aus großen, sequentiellen I/Os Workloads besteht. Wenn es sich hauptsächlich um kleine, zufällige Werte handelt I/Os, beeinträchtigt diese Einstellung tatsächlich Ihre Leistung. Wenn Ihre Arbeitslast hauptsächlich aus kleinen oder zufälligen Aufgaben besteht, sollten Sie im Allgemeinen erwägen I/Os, ein Allzweck-SSD-Volume (gp2undgp3) anstelle eines `st1` `sc1` OR-Volumes zu verwenden.

Verwenden Sie einen modernen Linux-Kernel (Nur Linux-Instanzen)

Verwenden Sie einen modernen Linux-Kernel, der indirekte Beschreibungen akzeptiert. Diese Unterstützung ist in Linux-Kernel 3.8 und höher sowie in jeder EC2-Instance der aktuellen Generation verfügbar. Wenn Ihre durchschnittliche I/O Größe bei oder in der Nähe von 44 KiB liegt, verwenden Sie möglicherweise eine Instanz oder einen Kernel ohne Unterstützung für indirekte Deskriptoren. Informationen zum Ableiten der I/O Durchschnittsgröße anhand von CloudWatch Amazon-Metriken finden Sie unter. I/O Eigenschaften und Überwachung von Amazon EBS

Um den maximalen Durchsatz auf `st1`- oder `sc1`-Volumes zu erzielen, empfehlen wir, für den Parameter `xen_blkfront.max` (für Linux-Kernel-Versionen unter 4.6) oder für den Parameter `xen_blkfront.max_indirect_segments` (für Linux-Kernel-Version 4.6 und höher) den Wert 256 festzulegen. Sie können den richtigen Parameter in der BS-Start-Befehlszeile festlegen.

In einem Amazon Linux-AMI mit einem älteren Kernel können Sie ihn am Ende der Kernelzeile in der GRUB-Konfiguration unter hinzufüge `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

Bei einem neueren Kernel würde der Befehl ähnlich wie folgt aussehen:

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

Starten Sie Ihre Instance neu, damit diese Einstellung wirksam wird.

Weitere Informationen finden Sie unter GRUB für paravirtuelle AMIs konfigurieren. Für andere Linux-Distributionen, insbesondere die, die keinen GRUB-Bootloader verwenden, ist möglicherweise ein anderer Ansatz notwendig, um die Kernel-Parameter anzupassen.

Weitere Informationen zu den I/O EBS-Eigenschaften finden Sie in der re:Invent-Präsentation zu Amazon EBS: Designing for Performance zu diesem Thema.

Verwenden von RAID 0 zur maximalen Nutzung der Instance-Ressourcen

Einige Instance-Typen können einen höheren I/O Durchsatz erzielen, als Sie für ein einzelnes EBS-Volume bereitstellen können. Sie können mehrere Volumes in einer RAID 0-Konfiguration miteinander verbinden, um die verfügbare Bandbreite für diese Instances zu verwenden. Weitere Informationen finden Sie unter Amazon EBS- und RAID-Konfiguration.

Überwachen Sie die Leistung des Amazon EBS-Volumes

Sie können die Leistung Ihrer Amazon EBS-Volumes mithilfe von Amazon CloudWatch, Statusüberprüfungen und detaillierten EBS-Leistungsstatistiken überwachen und analysieren. Weitere Informationen erhalten Sie unter CloudWatch Amazon-Metriken für Amazon EBS und Detaillierte Leistungsstatistiken von Amazon EBS.

Amazon-EBS-Optimierung

Eine für Amazon EBS optimierte Instance verwendet einen optimierten Konfigurationsstapel und bietet zusätzliche, dedizierte Kapazität für Amazon EBS. I/O Diese Optimierung bietet die beste Leistung für Ihre EBS-Volumes, indem Konflikte zwischen Amazon EBS und anderem Datenverkehr von Ihrer Instance minimiert werden. I/O

EBS-optimierte Instances bieten eine dedizierte Bandbreite für Amazon EBS. Bei Anschluss an eine EBS-optimierte Instance:

- `io2`Block Express-Volumes sind so konzipiert, dass sie bei 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten. I/O `io2` Block Express-Volumes bieten im Vergleich zu Allzweck-Volumes auch eine bessere Ausreißerlatenz, wodurch die Häufigkeit von I/Os Überschreitungen von 800 Mikrosekunden um mehr als das Zehnfache reduziert wird. `io1`und `io2` Volumes sind so konzipiert, dass sie mindestens 90% ihrer bereitgestellten IOPS-Leistung in 99,9% der Fälle in einem bestimmten Jahr bereitstellen.
- `gp2`und `gp3` Volumes sind so konzipiert, dass sie in einem bestimmten Jahr in 99% der Fälle mindestens 90% der bereitgestellten IOPS-Leistung bereitstellen.
- `st1`und `sc1` Volumes liefern in einem bestimmten Jahr in 99% der Fälle mindestens 90% ihrer erwarteten Durchsatzleistung.

Non-compliant Die Zeiträume sind ungefähr gleichmäßig verteilt, sodass 99% des erwarteten Gesamtdurchsatzes pro Stunde angestrebt werden. Weitere Informationen finden Sie unter Amazon EBS-Volume-Typen.

Die I/O Größe Ihrer Arbeitslast wirkt sich auf die beobachtete durchschnittliche Latenz aus, da die Latenz mit zunehmender I/O Größe zunimmt. `io2`Block Express-Volumes sind beispielsweise so konzipiert, dass sie bei 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten. I/O

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

Initialisieren von Volumes Amazon EBS

Wenn Sie ein Amazon EBS-Volume entweder aus einem EBS-Snapshot oder aus einem anderen EBS-Volume (Volumenkopie) erstellen, müssen die Datenblöcke auf das Volume geschrieben werden, bevor Sie darauf zugreifen können. Bei Volumes, die aus Snapshots erstellt wurden, müssen die Datenblöcke von Amazon S3 auf das neue Volume heruntergeladen werden. Für Volumenkopien müssen die Datenblöcke vom Quell-Volume auf die Volume-Kopie kopiert werden. Dieser Vorgang wird als Volume-Initialisierung bezeichnet. Während dieser Zeit kann es bei dem zu initialisierenden Volume zu einer erhöhten I/O Latenz und einer verringerten Leistung kommen. Die volle Leistung des Datenträgers wird erst erreicht, wenn alle Speicherblöcke heruntergeladen und auf das Volume geschrieben wurden.

> **Note**
>
> Leere Volumes bieten ihre maximale Leistung sofort nach der Erstellung und müssen nicht initialisiert werden.

Die Standard-Volume-Initialisierungsrate schwankt während des Initialisierungsprozesses, wodurch die Abschlusszeiten unvorhersehbar werden können. Um die mit der Volume-Initialisierung verbundenen Leistungseinbußen zu minimieren, könnten Sie die folgenden Optionen verwenden:

Themen

- Verwenden Sie eine von Amazon EBS bereitgestellte Rate für die Volumeninitialisierung
- Verwenden Sie einen Snapshot, der für die schnelle Snapshot-Wiederherstellung aktiviert ist
- Initialisieren Sie die Volumes nach der Erstellung manuell
- Überwachen Sie den Status der Amazon EBS-Volume-Initialisierung

> **Note**
>
> Amazon EBS Provisioned Rate for Volume Initialization und Fast Snapshot Restore werden für Volume-Kopien nicht unterstützt. Weitere Informationen finden Sie unter Initialisierung von Volumenkopien.

Verwenden Sie eine von Amazon EBS bereitgestellte Rate für die Volumeninitialisierung

Wenn Sie ein Amazon EBS-Volume aus einem Snapshot erstellen, können Sie optional eine Amazon EBS-Bereitstellungsrate für die Volumeninitialisierung (Volume-Initialisierungsrate) angeben, die zwischen 100 und 300 liegt. MiB/s Wenn Sie eine Volume-Initialisierungsrate angeben, werden die Snapshot-Blöcke von Amazon S3 heruntergeladen und nach der Erstellung mit der angegebenen Rate auf das Volume geschrieben. Auf diese Weise können Sie Volumes erstellen, die in einer vorhersehbaren Zeit vollständig initialisiert und voll leistungsfähig sind.

Die Verwendung einer Volume-Initialisierungsrate ist besonders nützlich, wenn Sie mehrere Volumes gleichzeitig erstellen und alle in einem vorhersehbaren Zeitraum initialisiert werden müssen.

> **Note**
>
> Amazon EBS Provisioned Rate for Volume Initialization wird für alle Amazon EBS-Volume-Typen und alle Amazon EC2-Instance-Typen, einschließlich Amazon EC2 Mac-Instances, unterstützt.

Sie können eine Volume-Initialisierungsrate angeben:

- Für individuelle Anfragen zur Volumenerstellung
- Für EBS-Volume-Block-Gerätezuordnungen in Instance-Startanfragen
- Für EBS-Volume-Block-Gerätezuordnungen in Startvorlagen
- Für EBS-Volumes, die durch Aufgaben zum Ersetzen des Root-Volumes erstellt wurden
- Für EBS-Volumes auf Amazon EKS-Clustern (erstellt mit EBS CSI Driver) und Amazon ECS-Clustern

Themen

- Funktionsweise
- Überlegungen
- Kontingente
- Fakturierung
- Geben Sie eine Rate für die Volumeninitialisierung an

Funktionsweise

Wenn Sie ein Volume mit einer Volume-Initialisierungsrate erstellen, werden die Snapshot-Blöcke mit der von Ihnen angegebenen Rate von Amazon S3 auf das Volume heruntergeladen.

Die Zeit, die für die Initialisierung des Volumes benötigt wird, hängt von folgenden Faktoren ab:

- Die Größe der Snapshot-Daten, nicht die Größe des zu erstellenden Volumes.

> **Tip**
>
> Um die Datengröße eines Snapshots zu ermitteln, überprüfen Sie das `FullSnapshotSizeInBytes` Feld in der Befehlsausgabe von describe-snapshots oder das Feld Vollständige Snapshot-Größe in der Konsole.

- Die von Ihnen angegebene Initialisierungsrate des Volumes

Wenn Sie beispielsweise ein 20-GiB-Volume mithilfe eines Snapshots mit 10 GiB an Daten erstellen und eine Volume-Initialisierungsrate von 300 angeben MiB/s, wird das Volume in ungefähr 34,1 Sekunden vollständig initialisiert (10 GiB/300 MiB/s = 34,1 Sekunden). Wenn Sie ebenfalls 10 Volumes mit demselben Snapshot und derselben Volume-Initialisierungsrate gleichzeitig erstellen, werden alle 10 Volumes in 34,1 Sekunden vollständig initialisiert.

Überlegungen

- Sie können eine Volume-Initialisierungsrate zwischen 100 und 300 angeben. MiB/s
- Wenn Sie eine Volume-Initialisierungsrate angeben, basieren die Gebühren und die Abschlusszeit auf der Größe der Snapshot-Daten (nicht der Größe des Volumes) und der von Ihnen angegebenen Rate. Weitere Informationen finden Sie unter Fakturierung.
- Amazon EBS liefert eine Durchschnittsrate, die in 99 Prozent der Fälle innerhalb von 10 Prozent der von Ihnen angegebenen Volume-Initialisierungsrate liegt.
- Wenn Sie eine Volume-Initialisierungsrate angeben und einen Snapshot verwenden, der für die schnelle Snapshot-Wiederherstellung aktiviert ist, verwendet Amazon EBS die angegebene Rate anstelle der schnellen Snapshot-Wiederherstellung. Wenn Sie stattdessen die schnelle Snapshot-Wiederherstellung verwenden möchten, geben Sie keine Volume-Initialisierungsrate an.
- Wenn Amazon EBS das Volume aufgrund von Kapazitätsbeschränkungen oder weil Sie Ihr Kontingent überschritten haben, nicht mit der angegebenen Volume-Initialisierungsrate initialisieren kann, schlägt die Anfrage fehl.
- Sie können keine Volume-Initialisierungsrate für Volumes angeben AWS Outposts, die auf oder in Local Zones oder Wavelength Zones erstellt wurden.

Kontingente

Die kumulative Volume-Initialisierungsrate, die Sie MiB/s bei gleichzeitigen Anfragen zur Volume-Erstellung anfordern können, ist auf 5.000 begrenzt. Sie können beispielsweise 50 gleichzeitige Anfragen zur Volumenerstellung mit einer Rate von 100 MiB/s (50 gleichzeitige Anfragen * MiB/s Rate 100) oder 25 gleichzeitige Anfragen mit einer Rate von 200 MiB/s (25 gleichzeitige Anfragen * Rate 200) stellen. MiB/s Dieses Limit gilt pro Region. Wenn eine Anfrage dieses Limit überschreitet, schlägt sie fehl. Warten Sie entweder, bis einige der laufenden Anfragen abgeschlossen sind, oder fordern Sie eine Kontingenterhöhung an. Weitere Informationen finden Sie unter Kontingente für Amazon EBS.

Fakturierung

Wenn Sie ein Volume mit einer Volume-Initialisierungsrate erstellen, wird Ihnen eine Rate pro GiB berechnet, die auf der ausgewählten Initialisierungsstufe basiert. Die Rate variiert je nach Region. Um den Tarif für Ihre gewählte Initialisierungsstufe zu ermitteln, öffnen Sie die Amazon EBS-Preisgestaltung, wählen Sie Ihre Region aus und suchen Sie den Abschnitt Bereitgestellte Rate für die Volumeninitialisierung.

Ihnen wird die gesamte Snapshot-Datengröße berechnet, nicht die Größe des Volumes. Wenn Sie beispielsweise einen Snapshot eines 100-GiB-Volumes erstellen, das 50 GiB an geschriebenen Daten enthält, beträgt die gesamte Snapshot-Datengröße 50 GiB. Wenn Sie diesen Snapshot verwenden, um ein Volume zu erstellen und eine Volume-Initialisierungsrate anzugeben, basieren Ihre Gebühren auf 50 GiB.

> **Tip**
>
> Um die vollständige Snapshot-Datengröße zu ermitteln, überprüfen Sie das `FullSnapshotSizeInBytes` Feld in der Befehlsausgabe von describe-snapshots oder das Feld Vollständige Snapshot-Größe in der Konsole.

Die Formel lautet wie folgt:

```
Rate for the selected initialization tier in the Region × full snapshot data size
```

Ihnen wird der volle Betrag in Rechnung gestellt, sobald das Volumen den `active` Status erreicht hat. Fehlgeschlagene Anfragen werden nicht in Rechnung gestellt.

Wenn Sie ein Volume löschen, bevor die Initialisierung abgeschlossen ist, wird Ihnen trotzdem die angeforderte Rate für die Volume-Initialisierung in Rechnung gestellt.

Geben Sie eine Rate für die Volumeninitialisierung an

Verwenden Sie eine der folgenden Methoden, um ein Volume aus einem Snapshot mit einer Volume-Initialisierungsrate zu erstellen.

Console

So erstellen Sie ein Volume

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes und anschließend Create volume aus.
3. Wählen Sie für Volume-Typ den Typ des zu erstellenden Volumes aus.
4. Geben Sie für Größe eine Größe ein, die der Volumegröße des Quell-Snapshots entspricht oder diese übersteigt.
5. Wählen Sie unter Availability Zone die Availability Zone aus, in der das Volume erstellt werden soll.
6. Wählen Sie für Snapshot-ID den Snapshot aus, den Sie verwenden möchten.
7. Geben Sie für die Volumeninitialisierungsrate eine Rate von `100` — `300` MiB/s ein. Bei Angabe einer Rate fallen zusätzliche Gebühren an. Wenn Sie die Standardinitialisierungsrate oder die schnelle Snapshot-Wiederherstellung verwenden möchten, lassen Sie dieses Feld leer, falls sie für den ausgewählten Snapshot aktiviert ist.

   > **Note**
   >
   > Hinweise dazu, wie sich die Rate und die vollständige Snapshot-Datengröße auf die Initialisierungszeit auswirken, finden Sie unter. Funktionsweise Informationen zu den Preisen finden Sie unter Fakturierung.

8. Konfigurieren Sie alle anderen erforderlichen Volumeneinstellungen und fügen Sie bei Bedarf Tags hinzu.
9. Wählen Sie Create Volume (Volume erstellen) aus.
10. Sehen Sie sich im Raster „Volumes“ den Initialisierungsstatus und den Fortschritt des Volumes an.

AWS CLI

So erstellen Sie ein Volume

Verwenden Sie den Befehl create-volume. Im folgenden Beispiel wird ein gp3 Volume aus einem Snapshot in der angegebenen Availability Zone mit einer Volume-Initialisierungsrate von erstellt. 300 MiB/s Ersetzen Sie die Beispielregion, Availability Zone und Snapshot-ID durch die Werte für Ihre Ressourcen:

```
aws ec2 create-volume \
    --region us-east-1 \
    --availability-zone us-east-1a \
    --volume-type gp3 \
    --snapshot-id snap-0abcdef1234567890 \
    --volume-initialization-rate 300
```

Wenn Sie nichts angeben--size, verwendet das Volume die Volume-Größe des Quell-Snapshots. Wenn Sie dies angeben--size, muss der Wert gleich oder größer als die Volumegröße des Quell-Snapshots sein.

PowerShell

So erstellen Sie ein Volume

Verwenden Sie das cmdlet New-EC2Volume. Im folgenden Beispiel wird ein gp3 Volume aus einem Snapshot in der angegebenen Availability Zone mit einer Volume-Initialisierungsrate von 300 MiB/s erstellt. Der Befehl speichert das zurückgegebene Volume-Objekt in$volume. Ersetzen Sie die Beispielregion, Availability Zone und Snapshot-ID durch die Werte für Ihre Ressourcen:

```
$volume = New-EC2Volume `
    -Region us-east-1 `
    -AvailabilityZone us-east-1a `
    -VolumeType gp3 `
    -SnapshotId snap-0abcdef1234567890 `
    -VolumeInitializationRate 300
```

Überwachen Sie die Initialisierung

Es kann bis zu 5 Minuten dauern, bis die Informationen zur Volume-Initialisierung aktualisiert werden. Anweisungen zur Überwachung der Initialisierung finden Sie unter. Überwachen Sie den Status der Amazon EBS-Volume-Initialisierung

Verwenden Sie einen Snapshot, der für die schnelle Snapshot-Wiederherstellung aktiviert ist

Wenn Sie ein Volume aus einem Snapshot erstellen, der für die schnelle Snapshot-Wiederherstellung aktiviert ist, wird das Volume bei der Erstellung vollständig initialisiert und bietet sofort seine volle Leistung. Weitere Hinweise zur Verwendung der schnellen Snapshot-Wiederherstellung finden Sie unterSchnelle Amazon EBS-Snapshot-Wiederherstellung.

Initialisieren Sie die Volumes nach der Erstellung manuell

Sie können ein Amazon EBS-Volume nach der Erstellung manuell initialisieren, um die Leistungseinbußen der Volume-Initialisierung zu minimieren.

Sie können die folgenden Verfahren verwenden, um ein Amazon EBS-Volume nach der Erstellung manuell zu initialisieren.

> **Important**
>
> Bei der Initialisierung bereitgestellter IOPS-SSD-Volumes, die anhand von Snapshots erstellt wurden, kann die Leistung des Volumes unter 50 Prozent des erwarteten Niveaus fallen, was dazu führt, dass das Volume in der Leistungsstatusüberprüfung einen `warning` Status anzeigt. I/O Dies ist normal. Sie können den Status `warning` bei Bereitgestellte IOPS-SSD-Volumes bei der Initialisierung ignorieren. Weitere Informationen finden Sie unter Statusüberprüfungen des Amazon EBS-Volumes.

Linux-Instances

So initialisieren Sie ein Volume, das aus einem Snapshot unter Linux wiederhergestellt wurde

1. Fügen Sie das soeben wiederhergestellte Volume an Ihre Linux-Instance an.
2. Verwenden Sie den Befehl lsblk, um die Blockgeräte auf Ihrer Instance aufzulisten.

```
$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

Hier können Sie sehen, dass das neue Volume `/dev/xvdf` angefügt, aber noch nicht aufgespielt ist (da der Pfad nicht in der Spalte `MOUNTPOINT` aufgeführt ist).

3. Verwenden Sie den Befehl dd oder fio, um alle Blöcke auf einem Gerät zu lesen. Der Befehl dd ist in Linux-Systemen standardmäßig installiert, aber fio ist beträchtlich schneller, da er Multithread-Leseoperationen zulässt.

> **Note**
>
> Dieser Schritt kann zwischen einigen Minuten und mehreren Stunden dauern. Das hängt von der Bandbreite der EC2-Instance, der für das Volume bereitgestellten IOPS und der Größe des Volumes ab.

[dd]Der Parameter `if` (Eingabedatei) sollte auf das Laufwerk festgelegt werden, das Sie initialisieren möchten. Der Parameter `of` (Ausgabedatei) sollte auf die virtuelle Gerätedatei (Nulldevice) `/dev/null` festgelegt werden. Mit dem Parameter `bs` wird die Blockgröße der Leseoperation angegeben. Um eine optimale Leistung zu erzielen, sollte dieser Parameter auf 1 MB festgelegt werden.

> **Important**
>
> Die falsche Verwendung des Befehls dd kann die Daten eines Volumes ohne Weiteres zerstören. Achten Sie darauf, den Beispielbefehl unten genau zu befolgen. Nur der Parameter `if=/dev/`*`xvdf`* unterscheidet sich abhängig vom gelesenen Gerätenamen.

```
$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] Wenn der Befehl fio in Ihrem System installiert ist, verwenden Sie den folgenden Befehl, um Ihr Volume zu initialisieren. Der Parameter `--filename` (Eingabedatei) sollte auf das Laufwerk festgelegt werden, das Sie initialisieren möchten.

```
$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --ioengine=libaio --
direct=1 --name=volume-initialize
```

Mit dem folgenden Befehl können Sie fio auf Amazon Linux installieren.

```
sudo yum install -y fio
```

Verwenden Sie den folgenden Befehl, um fio unter Ubuntu zu installieren:

```
sudo apt-get install -y fio
```

Wenn die Operation abgeschlossen ist, sehen Sie einen Bericht zur Leseoperation. Das Volume ist nun einsatzbereit. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

Windows-Instances

Sammeln Sie wie folgt Informationen zu den Datenträgern in Ihrem System, bevor Sie das Tool verwenden:

Sammeln von Informationen über die Systemdisketten

1. Verwenden Sie den Befehl wmic, um die verfügbaren Datenträger in Ihrem System aufzulisten:

   ```
   wmic diskdrive get size,deviceid
   ```

   Ausgabebeispiel:

   ```
   DeviceID            Size
   \\.\PHYSICALDRIVE2  80517265920
   \\.\PHYSICALDRIVE1  80517265920
   \\.\PHYSICALDRIVE0  128849011200
   \\.\PHYSICALDRIVE3  107372805120
   ```

2. Mit dem Befehl dd oder fio können Sie den zu initialisierenden Datenträger angeben. Das Laufwerk `C:` befindet sich auch `\\.\PHYSICALDRIVE0`. Sie können den Befehl `diskmgmt.msc` verwenden, um die Laufwerkbuchstaben mit den Laufwerkzahlen zu vergleichen, wenn Sie nicht genau wissen, welche Laufwerknummer Sie verwenden sollen.

Use the dd utility

Führen Sie die folgenden Schritte aus, um dd zu installieren und damit ein Volume zu initialisieren.

Wichtige Überlegungen

- Die Initialisierung eines Volumes kann zwischen einigen Minuten und mehreren Stunden dauern. Das hängt von der Bandbreite der EC2-Instance, der für das Volume bereitgestellten IOPS und der Größe des Volumes ab.
- Die falsche Verwendung des Befehls dd kann die Daten eines Volumes ohne Weiteres zerstören. Befolgen Sie dieses Verfahren unbedingt genau.

Installieren von dd für Windows

Der Befehl dd für Windows funktioniert ähnlich wie der Befehl dd, der allgemein für Linux- und Unix-Systeme verfügbar ist. Sie können damit Amazon EBS-Volumes initialisieren, die aus Snapshots erstellt wurden. Die neuesten Beta-Versionen unterstützen das virtuelle Gerät `/dev/null`. Wenn Sie eine frühere Version installieren, können Sie stattdessen das virtuelle Gerät `nul` verwenden. Die vollständige Dokumentation finden Sie unter. http://www.chrysocome.net/dd

1. Laden Sie die neueste Binärversion von dd für Windows von herunter http://www.chrysocome.net/dd.
2. (Optional) Erstellen Sie einen Ordner für Befehlszeilenprogramme, der sich leicht finden und einprägen lässt, etwa `C:\bin`. Wenn Sie bereits einen Ordner für Befehlszeilenprogramme haben, können Sie stattdessen diesen Ordner im nachfolgenden Schritt verwenden.
3. Extrahieren Sie das Binärpaket und kopieren Sie die Datei `dd.exe` in Ihren Ordner für Befehlszeilenprogramme (z. B. `C:\bin`).
4. Fügen Sie den Ordner für Befehlszeilenprogramme der Umgebungsvariable "Path" hinzu, damit Sie die Programme in diesem Ordner von überall aus ausführen können.
   a. Wählen Sie die Option Start aus, öffnen Sie das Kontextmenü (rechte Maustaste) für Computer und wählen Sie dann Eigenschaften aus.
   b. Wählen Sie Erweiterte Systemeinstellungen, Umgebungsvariablen aus.
   c. Wählen Sie unter Systemvariablen die Variable Path und dann Bearbeiten aus.
   d. Fügen Sie unter Wert der Variablen ein Semikolon und den Pfad des Befehlszeilenprogramm-Ordners (**`;C:\bin\`**) an das Ende des vorhandenen Werts an.
   e. Klicken Sie auf OK, um das Fenster Systemvariable bearbeiten zu schließen.

5. Öffnen Sie ein neues Befehlszeilenfenster. Mit dem vorherigen Schritt werden die Umgebungsvariablen in Ihren aktuellen Befehlszeilenfenstern nicht aktualisiert. Die Befehlszeilenfenster, die Sie jetzt öffnen, nachdem Sie den vorherigen Schritt abgeschlossen haben, werden aktualisiert.

Initialisieren eines Volumes mit dd für Windows

Führen Sie den folgenden Befehl aus, um alle Blöcke auf dem angegebenen Gerät zu lesen (und die Ausgabe an das virtuelle Gerät `/dev/null` zu senden). Mit diesem Befehl können Sie Ihre vorhandenen Daten sicher initialisieren.

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Möglicherweise tritt ein Fehler auf, wenn dd versucht, über das Ende des Volumes hinaus zu lesen. Sie können diesen Fehler ignorieren.

Wenn Sie eine frühere Version des dd-Befehls verwendet haben, wird das `/dev/null`-Gerät nicht unterstützt. Stattdessen können Sie das `nul`-Gerät wie folgt verwenden.

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

Führen Sie die folgenden Schritte aus, um fio zu installieren und damit ein Volume zu initialisieren.

Um zu installieren fio für Windows

Der Befehl fio für Windows funktioniert ähnlich wie der Befehl fio, der allgemein für Linux- und Unix-Systeme verfügbar ist. Sie können damit Amazon EBS-Volumes initialisieren, die aus Snapshots erstellt wurden. Weitere Informationen finden Sie unter https://github.com/axboe/fio.

1. Laden Sie das fio MSI-Installationsprogramm herunter, indem Sie Assets für die neueste Version erweitern und das MSI-Installationsprogramm auswählen.
2. Installieren fio.

Um ein Volume zu initialisieren mit fio für Windows

1. Führen Sie einen ähnlichen Befehl wie den folgenden aus, um ein Volume zu initialisieren:

```
fio --filename=\\.\PHYSICALDRIVEn  --rw=read --bs=1M --iodepth=32 --direct=1 --
name=volume-initialize
```

2. Wenn die Operation abgeschlossen ist, ist das neue Volume einsatzbereit. Weitere Informationen finden Sie unter Stellen Sie ein Amazon EBS-Volume zur Verwendung zur Verfügung.

Überwachen Sie den Status der Amazon EBS-Volume-Initialisierung

Wenn Sie ein Volume entweder aus einem Snapshot oder aus einem anderen Volume (Volumenkopie) erstellen, können Sie den Status der Volume-Initialisierung überwachen, um festzustellen, ob der Initialisierungsvorgang abgeschlossen ist. Sie können die Volume-Initialisierung mithilfe der folgenden Optionen überwachen:

Themen

- AWS CLI, AWS Werkzeuge für PowerShellund Amazon EC2-Konsole
- Amazon EventBridge

AWS CLI, AWS Werkzeuge für PowerShellund Amazon EC2-Konsole

Sie können die AWS CLI, AWS Tools for und die Amazon EC2-Konsole verwendenPowerShell, um den Status der Volume-Initialisierung jederzeit nach der Erstellung des Volumes zu überprüfen. Die folgenden Informationen werden bereitgestellt:

- Initialisierungstyp (AWS CLI und PowerShell nur AWS Tools für) — Gibt den Typ der verwendeten Volumeninitialisierung an. `default`für schnelle Snapshot-Wiederherstellung und Standard-Volume-Initialisierung, `provisioned-rate` für Amazon EBS Provisioned Rate für die Volume-Initialisierung und für die Volume-Copy-Initialisierung. `volume-copy`
- Geschätzte Zeit bis zur Fertigstellung (AWS CLI und nur AWS Tools für) — PowerShell Nur für Volumes, die mit einer Amazon EBS Provisioned Rate für die Volume-Initialisierung erstellt wurden. Die geschätzte verbleibende Zeit in Sekunden, bis die Volume-Initialisierung abgeschlossen ist.
- Fortschritt — Der Fortschritt der Volumeninitialisierung in Prozent (0—100). Bei Volumes, die mit der schnellen Snapshot-Wiederherstellung initialisiert wurden, steigt der Fortschritt unmittelbar nach der Erstellung auf 100 Prozent.

- Initialisierungsstatus — Der Gesamtstatus der Volume-Initialisierung (`initializing`oder). `completed` Bei Volumes, die mit einer schnellen Snapshot-Wiederherstellung initialisiert wurden, wechselt der Status in den Zustand `completed` unmittelbar nach der Erstellung.

> **Note**
>
> Es kann bis zu 5 Minuten dauern, bis die Informationen zur Volume-Initialisierung aktualisiert sind.

Verwenden Sie die folgenden Registerkarten, um den Status der Volume-Initialisierung für Ihr Volume zu überprüfen.

Console

Um den Status der Volume-Initialisierung zu überwachen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus, für das Sie den Initialisierungsstatus des Volumes überprüfen möchten.
4. Das Feld Initialisierungsstatus im Raster und auf der Registerkarte Details enthält Fortschrittsinformationen im folgenden Format: Initialisierungsstatus (Fortschrittsprozentsatz). Zum Beispiel Initialisierung (75%).

   Zu den möglichen Initialisierungszuständen gehören: Initialisieren und Abgeschlossen.

AWS CLI

Um den Status der Volume-Initialisierung zu überwachen

Verwenden Sie den AWS CLI Befehl describe-volume-status, um den Initialisierungsstatus anzuzeigen. Die Ausgabe bezieht sich `EstimatedTimeToCompleteInSeconds` nur auf Volumes, die mit einer von Amazon EBS bereitgestellten Rate für die Volumeninitialisierung erstellt wurden.

Beispielsweise überprüft der folgende Befehl den Initialisierungsstatus für ein Volume`vol-1111111111111111`, das mit einer Amazon EBS Provisioned Rate for Volume Initialization erstellt wurde.

```
aws ec2 describe-volume-status --volume-ids vol-1111111111111111
```

Es folgt eine Beispielausgabe.

```
{
    "VolumeStatuses": [
        {
            "Actions": [],
            "AvailabilityZone": "us-east-1a",
            "Events": [],
            "VolumeId": "vol-1111111111111111",
            "VolumeStatus": {
                "Details": [
                    {
                        "Name": "io-enabled",
                        "Status": "passed"
                    },
                    {
                        "Name": "io-performance",
                        "Status": "not-applicable"
                    },
                    {
                        "Name": "initialization-state",
                        "Status": "completed"
                    }
                ],
                "Status": "ok"
            },
            "InitializationStatusDetails": {
                "InitializationType": "provisioned-rate",
                "Progress": 75,
                "EstimatedTimeToCompleteInSeconds": 850
            }
        }
    ]
}
```

PowerShell

Um den Status der Volume-Initialisierung zu überwachen

Verwenden Sie das Get-EC2VolumeStatus Cmdlet, um den Initialisierungsstatus anzuzeigen. Die Ausgabe bezieht sich `EstimatedTimeToCompleteInSeconds` nur auf Volumes, die mit einer Amazon EBS-Bereitstellungsrate für die Volumeninitialisierung erstellt wurden.

Beispielsweise überprüft der folgende Befehl den Initialisierungsstatus für ein Volume`vol-1111111111111111`, das mit einer Amazon EBS Provisioned Rate for Volume Initialization erstellt wurde.

```
(Get-EC2VolumeStatus `
    -Region us-east-1 `
    -VolumeId vol-1111111111111111).InitializationStatusDetails |
    Select-Object `
        InitializationType,
        Progress,
        EstimatedTimeToCompleteInSeconds
```

Amazon EventBridge

Ein EventBridge Amazon-Event wird innerhalb von fünf Minuten nach Abschluss der Volumeninitialisierung an Ihr Konto gesendet. Sie können Regeln erstellen, die als Reaktion auf diese Ereignisse programmatische Aktionen auslösen.

> **Note**
>
> - Ereignisse werden auf bestmögliche Weise ausgegeben.
> - Wenn Sie das Volume vor Abschluss der Initialisierung oder innerhalb von 5 Minuten nach Abschluss der Initialisierung löschen, erhalten Sie das Ereignis möglicherweise nicht.

Weitere Informationen zu dem Ereignis finden Sie unter. Ereignis zur Initialisierung des EBS-Volumes

Um den Status der Volume-Initialisierung zu überwachen, verwenden Sie EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter. https://console.aws.amazon.com/events/

2. Wählen Sie Regeln, Regel erstellen.
3. Gehen Sie für Schritt 1 wie folgt vor:
   a. Geben Sie einen Namen und eine Beschreibung für die Regel an.
   b. Wählen Sie für Event-Bus den Bus aus, der die Ereignisse empfangen soll. Wenn Sie keinen benutzerdefinierten Event-Bus erstellt haben, behalten Sie die Standardeinstellung bei. Weitere Informationen finden Sie unter Event-Bus erstellen.
   c. Behalten Sie als Regeltyp die Option Regel mit einem Ereignismuster bei.
   d. Wählen Sie Weiter aus.
4. Gehen Sie für Schritt 2 wie folgt vor:
   a. Behalten Sie als Eventquelle AWS Ereignisse oder EventBridge Partnerereignisse bei.
   b. Wählen Sie als Creation method (Erstellungsmethode) die Option Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.
   c. Fügen Sie für Event-Muster Folgendes hinzu:

```
{
    "detail-type": ["EBS Volume Notification"],
    "source": ["aws.ec2"],
    "detail": {
        "event": ["initializeVolume"],
        "result": ["succeeded"]
    }
}
```

      Ein Beispiel für ein Ereignis finden Sie unter Ereignis zur Initialisierung des EBS-Volumes.
   d. Wählen Sie Weiter aus.
5. Gehen Sie für Schritt 3 wie folgt vor:
   a. Bei Zieltypen wählen Sie AWS -Service aus.
   b. Wählen Sie unter Ziel auswählen die Option SNS-Thema aus, und wählen Sie für Thema das gewünschte Thema aus. Wenn Sie keine Themen erstellt haben, finden Sie weitere Informationen unter Ein Thema https://docs.aws.amazon.com/sns/latest/dg/sns-create-topic.html erstellen.
   c. Halten Sie für Berechtigungen die Option Ausführungsrolle verwenden (empfohlen) aktiviert.

   d. Halten Sie für die Ausführungsrolle die Option Neue Rolle für diese spezifische Ressource erstellen und den Standardrollennamen ausgewählt.
   e. Wählen Sie Weiter aus.
6. Geben Sie für Schritt 4 bei Bedarf Tags für die Regel an, und wählen Sie dann Weiter aus.
7. Überprüfen Sie in Schritt 5 die Regel und wählen Sie dann Regel erstellen aus.

Konfigurierbare Gewichtung der Instanz-Bandbreite

Die Instance-Bandbreitenkonfiguration (IBC) ist eine Funktion, mit der Sie die Zuweisung der Netzwerkbandbreite zwischen Amazon EBS und VPC-Netzwerken für eine Amazon EC2-Instance anpassen können. Diese Funktion kann Ihnen helfen, die Leistung für Workloads mit bestimmten Bandbreitenanforderungen zu optimieren. Die Konfiguration der Instanzbandbreite wird nur auf einigen Instances unterstützt. Weitere Informationen finden Sie unter Konfiguration der Gewichtung der Instanzbandbreite.

Für die EBS-Leistung erhöht die Verwendung der `ebs-1` Bandbreitengewichtung die EBS-Grundbandbreite um 25 Prozent, während die VPC-Netzwerkbandbreite um den gleichen absoluten Betrag reduziert wird. Dies kann für I/O-intensive Workloads von Vorteil sein, die einen höheren EBS-Durchsatz erfordern.

Berücksichtigen Sie bei der Planung Ihrer Arbeitslast sorgfältig Ihre I/O Größe und Muster. Kleinere I/O Größen sind im Allgemeinen weniger von Bandbreitenbeschränkungen betroffen, während bei größeren I/O Größen oder sequentiellen Workloads stärkere Auswirkungen von Bandbreitenänderungen auftreten können. Es ist wichtig, dass Sie Ihren spezifischen Workload gründlich testen, um eine optimale Leistung mit der von Ihnen gewählten Bandbreitengewichtung sicherzustellen.

Überlegungen

- Die konfigurierbare Instanzbandbreite wird für ausgewählte Instance-Typen unterstützt. Weitere Informationen finden Sie unter Unterstützte Instanztypen.
- Durch die Verwendung der `ebs-1` Bandbreitengewichtung wird die EBS-Bandbreite um bis zu 25 Prozent erhöht, was die Leistung von I/O-intensive Anwendungen verbessern kann. Beachten Sie jedoch, dass die VPC-Netzwerkbandbreite um den gleichen absoluten Betrag reduziert wird (die kombinierte Bandbreitenspezifikation zwischen EBS und Netzwerk ändert sich nicht).
- Änderungen der Bandbreitengewichtung können die Leistung erheblich beeinträchtigen. I/O Durch die `vpc-1` Bandbreitengewichtung wird die Netzwerkbandbreite erhöht, allerdings kann

es bei EBS-Volumes zu niedrigeren IOPS kommen als erwartet. Dies liegt daran, dass Sie das EBS-Bandbreitenlimit möglicherweise vor dem IOPS-Limit erreichen, insbesondere bei größeren Größen. I/O Beispielsweise kann ein Instance-Typ, der in der Regel 240.000 IOPS mit einer I/O Größe von 16 KiB unterstützt, aufgrund der verringerten EBS-Bandbreite weniger IOPS erzielen, wenn das `vpc-1` Bandbreitengewicht verwendet wird.

- Testen Sie immer Ihre spezifische Arbeitslast, um sicherzustellen, dass die gewählte Bandbreitengewichtung Ihren Leistungsanforderungen entspricht.
- Sie können die Bandbreitengewichtung beim Start der Instance konfigurieren oder sie für gestoppte Instances ändern. Weitere Informationen finden Sie unter Konfigurieren der Bandbreitengewichtung für Ihre Instance.
- Sie können die Gewichtung der Instance-Bandbreite ohne zusätzliche Kosten konfigurieren.

I/O Eigenschaften und Überwachung von Amazon EBS

Bei einer bestimmten Volume-Konfiguration bestimmen bestimmte I/O Merkmale das Leistungsverhalten Ihrer EBS-Volumes.

- SSD-backed Volumes, General Purpose SSD (`gp2`und`gp3`) und Provisioned IOPS SSD (`io1`und`io2`), bieten eine konsistente Leistung, unabhängig davon, ob ein I/O Vorgang zufällig oder sequentiell erfolgt.
- HDD-backed Volumes, Throughput Optimized HDD (`st1`) und Cold HDD (`sc1`), bieten nur bei umfangreichen und sequentiellen I/O Vorgängen eine optimale Leistung.

Um zu verstehen, wie SSD- und HDD-Volumes in Ihrer Anwendung funktionieren, ist es wichtig, den Zusammenhang zwischen der Auslastung des Volumes, der Menge der verfügbaren IOPS, der Zeit, die bis zum Abschluss eines I/O Vorgangs benötigt wird, und den Durchsatzgrenzen des Volumes zu kennen.

Themen

- E/A\Sek
- Länge und Latenz der Volume-Warteschlange
- I/O Grenzwerte für Größe und Volumen beim Durchsatz
- Überwachen Sie die Eigenschaften I/O mit CloudWatch
- Überwachen Sie Leistungsstatistiken in Echtzeit I/O

- Zugehörige Ressourcen

E/A\Sek

IOPS sind eine Maßeinheit, die input/output Operationen pro Sekunde darstellt. Die Operationen werden in KiB gemessen, und die zugrundeliegende Antriebstechnologie bestimmt die maximale Datenmenge, die ein Datenträgertyp als Einheit zählt. I/O I/O Die Größe ist auf 256 KiB für SSD-Volumes und 1.024 KiB für HDD-Volumes begrenzt, da SSD-Volumes kleine oder zufällige Volumes I/O viel effizienter verarbeiten als HDD-Volumes.

Wenn kleine I/O Operationen physisch sequentiell ablaufen, versucht Amazon EBS, sie bis zur maximalen Größe zu einem einzigen I/O Vorgang zusammenzuführen. I/O Ähnlich versucht Amazon EBS, I/O Operationen, die die maximale I/O Größe überschreiten, in kleinere Operationen aufzuteilen. I/O Die folgende Tabelle zeigt einige Beispiele.

Volume-Typ	Maximale Größe I/O	I/O Operationen aus Ihrer Anwendung	Anzahl IOPS	Hinweise
SSD	256 KiB	1 x 1024 I/O KiB-Vorgang	4 (1 024÷256=4)	Amazon EBS teilt den I/O 1.024-KiB-Vorgang in vier kleinere 256-KiB-Operationen auf.
		8 x sequentielle 32-KiB-Operationen I/O	1 (8x32=256)	Amazon EBS führt die acht sequentiellen I/O 32-KiB-Operationen zu einer einzigen 256-KiB-Operation zusammen.
		8 zufällige 32-KiB-Operationen I/O	8	Amazon EBS zählt zufällige I/O Operationen separat.

Volume-Typ	Maximale Größe I/O	I/O Operationen aus Ihrer Anwendung	Anzahl IOPS	Hinweise
HDD	1 024 KiB	Betrieb mit 1 x 1024 KiB I/O	1	Die I/O Operation entspricht bereits der maximalen I/O Größe. Er wird nicht zusammengeführt oder geteilt.
		8 x sequentielle 128 KiB-Operationen I/O	1 (8x128=1 024)	Amazon EBS führt die acht sequentiellen I/O 128-KiB-Operationen zu einer einzigen 1.024-KiB-Operation zusammen. I/O
		8 zufällige 32-KiB-Operationen I/O	8	Amazon EBS zählt zufällige I/O Operationen separat.

Wenn Sie also ein SSD-backed Volume erstellen, das 3.000 IOPS unterstützt (entweder indem Sie ein `io1` `io2` OR-Volume mit 3.000 IOPS bereitstellen, indem Sie ein `gp2` Volume auf 1.000 GiB dimensionieren oder ein `gp3` Volume verwenden), und Sie es an eine EBS-optimized Instance anhängen, die ausreichend Bandbreite bereitstellen kann, können Sie bis zu 3.000 Daten pro Sekunde übertragen, wobei der Durchsatz I/Os von der Größe abhängt. I/O

Länge und Latenz der Volume-Warteschlange

Die Länge der Volume-Warteschlange ist die Anzahl der ausstehenden I/O Anfragen für ein Gerät. Die Latenz ist die tatsächliche Client-Zeit eines I/O Vorgangs, mit anderen Worten, die Zeit, die zwischen dem Senden einer Nachricht an EBS und dem Empfangen einer I/O Bestätigung von EBS verstrichen ist, dass der I/O Lese- oder Schreibvorgang abgeschlossen ist. Die Warteschlangenlänge

muss korrekt auf I/O Größe und Latenz abgestimmt werden, um Engpässe entweder auf dem Gastbetriebssystem oder auf der Netzwerkverbindung zu EBS zu vermeiden.

Die optimale Warteschlangenlänge für jeden Workload variiert und hängt davon ab, wie empfindlich Ihre jeweilige Anwendung auf IOPS und Latenz reagiert. Wenn Ihr Workload nicht genügend I/O Anfragen übermittelt, um die für Ihr EBS-Volume verfügbare Leistung voll auszuschöpfen, liefert Ihr Volume möglicherweise nicht die IOPS oder den Durchsatz, den Sie bereitgestellt haben.

Transaction-intensive Anwendungen reagieren empfindlich auf erhöhte I/O Latenz und eignen sich gut für Volumes. SSD-backed Um eine hohe IOPS-Rate bei geringer Latenz sicherzustellen, können Sie eine kurze Warteschlange verwenden und dafür sorgen, dass auf dem Volume eine große Anzahl von IOPS verfügbar ist. Wenn ein Volume ständig mehr IOPS als zur Verfügung steht, kann dies zu einer erhöhten I/O Latenz führen. Für maximale Konsistenz muss ein Volume eine durchschnittliche Warteschlangentiefe (auf die nächste ganze Zahl gerundet) von einer pro 1.000 bereitgestellten IOPS pro Minute beibehalten. Bei einem Volume, das mit 3.000 IOPS bereitgestellt wird, muss die durchschnittliche Warteschlangentiefe beispielsweise 3 betragen.

Throughput-intensive Anwendungen reagieren weniger empfindlich auf erhöhte I/O Latenz und eignen sich daher gut für Volumes. HDD-backed Sie können einen hohen Durchsatz für HDD-backed Volumes aufrechterhalten, indem Sie eine hohe Warteschlangenlänge beibehalten, wenn große, I/O sequentielle Aufgaben ausgeführt werden.

I/O Grenzwerte für Größe und Volumen beim Durchsatz

Bei SSD-backed Volumes kann es bei sehr großen Datenträgern zu I/O einer geringeren Anzahl von IOPS kommen, als Sie bereitgestellt haben, da Sie das Durchsatzlimit des Volumes erreichen. Beispielsweise hat ein gp2 Volume unter 1.000 GiB, für das Burst-Guthaben verfügbar ist, ein IOPS-Limit von 3.000 und ein Volumendurchsatzlimit von 250. MiB/s Wenn Sie eine I/O Größe von 256 KiB verwenden, erreicht Ihr Volume sein Durchsatzlimit bei 1000 IOPS (1000 x 256 KiB = 250 MiB). Bei kleineren I/O Größen (z. B. 16 KiB) kann dasselbe Volume 3.000 IOPS unterstützen, da der Durchsatz deutlich unter 250 liegt. MiB/s (Bei diesen Beispielen I/O wird davon ausgegangen, dass Ihr Volume die Durchsatzgrenzen der Instance nicht erreicht.) Weitere Informationen zu den Durchsatzlimits für jeden EBS-Volume-Typ finden Sie unter Amazon EBS-Volume-Typen.

Bei kleineren I/O Vorgängen wird möglicherweise ein IOPS-Wert angezeigt, der höher ist als der bereitgestellte IOPS-Wert, der von Ihrer Instance aus gemessen wird. Dies passiert, wenn das Instance-Betriebssystem kleine I/O Operationen zu einem größeren Vorgang zusammenführt, bevor sie an Amazon EBS übergeben werden.

Wenn Ihr Workload sequenzielles I/Os Einschalten HDD-backed `st1` und `sc1` Volumes verwendet, kann es sein, dass die Anzahl von IOPS, gemessen innerhalb Ihrer Instance, höher als erwartet ist. Das passiert, wenn das Instance-Betriebssystem sequentiell zusammenführt I/Os und sie in 1.024 Einheiten zählt. KiB-sized Wenn Ihre Arbeitslast klein oder zufällig verwendet wird I/Os, ist der Durchsatz möglicherweise niedriger als erwartet. Das liegt daran, dass alle zufälligen, nicht sequentiellen I/O IOPS-Werte zur Gesamtzahl der IOPS gezählt werden, was dazu führen kann, dass Sie das IOPS-Limit des Volumes früher als erwartet erreichen.

Unabhängig von Ihrem EBS-Volume-Typ sollten Sie sicherstellen, dass die Bandbreite Ihrer EC2-Instance nicht der limitierende Faktor ist, wenn Sie nicht die IOPS oder den Durchsatz erzielen, den Sie in Ihrer Konfiguration erwarten. Für eine optimale Leistung sollten Sie immer eine EBS-optimized Instance der aktuellen Generation (oder eine, die 10 Gb/s Netzwerkkonnektivität umfasst) verwenden. Eine weitere mögliche Ursache dafür, dass die erwarteten IOPS nicht erreicht werden, ist, dass Sie nicht genug I/O zu den EBS-Volumes fahren.

Überwachen Sie die Eigenschaften I/O mit CloudWatch

Sie können diese I/O Merkmale mit den Volumenmetriken jedes CloudWatch Volumes überwachen.

Überwachen Sie, ob es blockiert ist I/O

`VolumeStalledIOCheck` überwacht den Status Ihrer EBS-Volumes, um festzustellen, wenn Ihre Volumes beeinträchtigt sind. Die Metrik ist ein Binärwert, der je nachdem, ob das EBS-Volume Operationen abschließen I/O kann, den Status `0` `1` (bestanden) oder (nicht bestanden) zurückgibt.

Wenn die `VolumeStalledIOCheck` Metrik ausfällt, können Sie entweder warten, AWS bis das Problem behoben ist, oder Sie können Maßnahmen ergreifen, z. B. das betroffene Volume austauschen oder die Instance, an die das Volume angeschlossen ist, anhalten und neu starten. In den meisten Fällen, wenn diese Metrik fehlschlägt, diagnostiziert EBS Ihr Volume automatisch und stellt es innerhalb weniger Minuten wieder her. Sie können die I/O Pause-Aktion verwenden AWS Fault Injection Service , um kontrollierte Experimente durchzuführen, um Ihre Architektur und Überwachung auf der Grundlage dieser Metrik zu testen, um Ihre Widerstandsfähigkeit gegenüber Speicherfehlern zu verbessern.

Überwachen Sie die I/O Latenz für ein Volume

Sie können die durchschnittliche Latenz für Lese- und Schreibvorgänge für ein Amazon EBS-Volume mithilfe der jeweiligen `VolumeAvgWriteLatency` Metriken `VolumeAvgReadLatency` und überwachen. Sie können die Aktion Latency Injection verwenden AWS Fault Injection Service , um

kontrollierte Experimente durchzuführen, um Ihre Architektur und Überwachung auf der Grundlage dieser Metrik zu testen, um Ihre Widerstandsfähigkeit gegenüber einer Verschlechterung der Speicherleistung zu verbessern.

Wenn Ihre I/O Latenz höher ist als Sie benötigen, stellen Sie sicher, dass Ihre Anwendung nicht versucht, mehr IOPS oder Durchsatz zu erzielen, als Sie für Ihr Volume bereitgestellt haben. Sie können die `VolumeAvgThroughput` Metriken `VolumeAvgIOPS` und verwenden, um die durchschnittlichen IOPS und den Durchsatz Ihres Volumes innerhalb einer Minute zu überwachen und diese dann mit den bereitgestellten IOPS und dem Durchsatz des Volumes zu vergleichen. Wenn das Volume während einer Minute keine Operationen durchführt, melden die Metriken den Wert Null (). `0` Wenn Bursts mit hohen IOPS oder Durchsatz für einen kürzeren Zeitraum als das Minutenintervall auftreten, kommt es auf dem Volume zu Mikro-Bursts. Die durchschnittlichen IOPS- und Durchsatzmetriken geben jedoch möglicherweise an, dass Sie eine niedrigere Leistung erzielen, als die für Ihr Volume bereitgestellten IOPS- oder Durchsatzgrenzwerte. Mithilfe der Messwerte und können Sie ermitteln, ob es bei Ihrem Volume innerhalb einer bestimmten Minute zu Leistungsspitzen kommt. `VolumeIOPSExceededCheck` `VolumeThroughputExceededCheck` Sie können diese Metriken überwachen, um festzustellen, ob Ihre Arbeitslast in einer bestimmten Minute kontinuierlich versucht hat, IOPS oder einen Durchsatz zu erzielen, der die von Ihrem Volume bereitgestellte Leistung übersteigt. Wenn die berechneten IOPS-Werte für eine Sekunde innerhalb einer Minute konstant die von Ihrem Volume bereitgestellte IOPS-Leistung überschreiten, wird die Metrik zurückgegeben. `VolumeIOPSExceededCheck` `1` Wenn der getriebene Durchsatz für eine Sekunde innerhalb einer Minute die von Ihrem Volume bereitgestellte Durchsatzleistung konstant übersteigt, wird die Metrik zurückgegeben. `VolumeThroughputExceededCheck` `1` Wenn der getriebene IOPS und der Durchsatz innerhalb der von Ihrem Volume bereitgestellten Leistung liegen, kehren die Metriken zurück. `0`

Wenn Ihre Anwendung eine größere Anzahl von IOPS benötigt, als Ihr Volume bereitstellen kann, sollten Sie eine der folgenden Optionen erwägen:

- Ein `gp3`-, `io2`- oder `io1`-Volume, das mit genügend IOPS bereitgestellt wird, um die erforderliche Latenz zu erreichen
- Ein größeres `gp2`-Volume, das eine ausreichende IOPS-Grundleistung bietet

HDD-backed `st1`und `sc1` Volumes sind so konzipiert, dass sie bei Workloads, die die maximale Größe von 1.024 KiB nutzen, am besten funktionieren. I/O Um die durchschnittliche I/O Größe Ihres Volumes zu ermitteln, teilen Sie es durch`VolumeWriteBytes`. `VolumeWriteOps` Dieselbe Berechnung gilt für Leseoperationen. Wenn die durchschnittliche I/O Größe unter 64 KiB liegt,

sollte eine Erhöhung der Größe der an ein `st1` oder `sc1` -Volume gesendeten I/O Operationen die Leistung verbessern.

Überwachen Sie das Burst-Bucket-Gleichgewicht für **`GP2-`**, **`ST1- und SC1-Volumes`**

`BurstBalance` zeigt die Burst Bucket-Menge für die Volumes `gp2`, `st1` und `sc1` als Prozentsatz der Restmenge an. Wenn Ihr Burst-Bucket erschöpft ist, wird das Volumen I/O (für `gp2` Volumes) oder der Volumendurchsatz (für Volumes `st1` und `sc1` Volumes) auf den Ausgangswert gedrosselt. Prüfen Sie den `BurstBalance`-Wert, um festzustellen, ob Ihr Volume aus diesem Grund gedrosselt wird. Eine vollständige Liste der verfügbaren Amazon EBS-Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS und Amazon EBS-Metriken für Instances. Nitro-based

Überwachen Sie Leistungsstatistiken in Echtzeit I/O

Sie können in Echtzeit auf detaillierte Leistungsstatistiken für Amazon EBS-Volumes zugreifen, die an Nitro-based Amazon EC2-Instances angehängt sind.

Sie können diese Statistiken kombinieren, um die durchschnittliche Latenz und IOPS abzuleiten oder um zu überprüfen, ob die I/O Operationen abgeschlossen werden. Sie können auch die Gesamtzeit einsehen, in der Ihre Anwendung die bereitgestellten IOPS- oder Durchsatzgrenzwerte Ihres EBS-Volumes oder der angehängten Instance überschritten hat. Indem Sie den Anstieg dieser Statistiken im Laufe der Zeit verfolgen, können Sie feststellen, ob Sie Ihre bereitgestellten IOPS- oder Durchsatzgrenzwerte erhöhen müssen, um die Leistung Ihrer Anwendung zu optimieren. Die detaillierten Leistungsstatistiken enthalten auch Histogramme für Lese- und I/O Schreibvorgänge, die eine Verteilung Ihrer I/O Latenz angeben, indem sie die Gesamtzahl der innerhalb eines Latenzbandes abgeschlossenen I/O Operationen verfolgen.

Weitere Informationen finden Sie unter Detaillierte Leistungsstatistiken von Amazon EBS.

Zugehörige Ressourcen

Weitere Informationen zu den I/O Merkmalen von Amazon EBS finden Sie in der folgenden re:Invent-Präsentation: Amazon EBS: Designing for Performance.

Amazon EBS- und RAID-Konfiguration

Mit Amazon EBS können Sie jede der Standard-RAID-Konfigurationen verwenden, die Sie auch für einen traditionellen blanken Metallserver verwenden können; Voraussetzung ist lediglich, dass die jeweilige RAID-Konfigurationen von dem Betriebssystem Ihrer Instance unterstützt wird. Dies liegt daran, dass RAID immer auf Softwareebene realisiert wird.

Amazon EBS-Volume-Daten werden über mehrere Server in einer Availability Zone repliziert, um den Verlust von Daten durch den Ausfall einer einzigen Komponente zu verhindern. Durch diese Replikation sind Amazon EBS-Volumes zehn mal so zuverlässig wie normale, handelsübliche Laufwerke. Weitere Informationen finden Sie unter Amazon EBS-Funktionen.

Inhalt

- RAID-Konfigurationsoptionen
- Erstellen Sie ein RAID 0-Array
- Erstellen von Snapshots von Volumes in einem RAID-Array

RAID-Konfigurationsoptionen

Wenn Sie ein RAID 0-Array erstellen, können Sie eine höhere Leistungsstufe für ein Dateisystem erreichen als mit einem einzigen Amazon EBS-Volume. Verwenden Sie RAID 0, wenn I/O Leistung von größter Bedeutung ist. Bei RAID 0 I/O wird es in einem Stripe über die Volumes verteilt. Wenn Sie ein Volume hinzufügen, erhalten Sie einen beträchtlichen Zuwachs an Durchsatz und IOPS. Beachten Sie jedoch, dass die Leistung des Stripe auf das am schlechtesten leistungsfähige Volume im Set beschränkt ist und dass der Verlust eines einzelnen Volumes im Set zu einem vollständigen Datenverlust für das Array führt.

Die sich daraus ergebende Größe für einen RAID 0-Array entspricht der Summe der Größen der darin enthaltenen Volumes, und die Bandbreite ist die Summe der für die einzelnen Volumes jeweils verfügbaren Bandbreiten. Beispielsweise bilden zwei `io1` 500-GiB-Volumes mit jeweils 4.000 bereitgestellten IOPS ein 1.000-GiB-RAID-0-Array mit einer verfügbaren Bandbreite von 8.000 IOPS und einem Durchsatz von 1.000. MiB/s

Important

RAID 5 und RAID 6 werden für Amazon EBS nicht empfohlen, da die Schreibvorgänge für Paritätsinformationen bei diesen RAID-Modi einen Teil der für Ihre Volumes verfügbaren IOPS verbrauchen. Abhängig von der Konfiguration Ihres RAID-Arrays bieten diese RAID-Modi 20-30 % weniger nutzbare IOPS als eine RAID 0-Konfiguration. Die höheren Kosten spielen bei diesen RAID-Modi auch eine Rolle; bei identischen Größen und Geschwindigkeiten kann ein RAID 0-Array mit 2 Volumes ein RAID 6-Array mit 4 Volumes, das doppelt soviel kostet, an Leistung übertreffen.
RAID 1 wird auch nicht für die Verwendung mit Amazon EBS empfohlen. RAID 1 erfordert mehr Bandbreite von Amazon EC2 zu Amazon EBS als Nicht-RAID-Konfigurationen, da die

Daten gleichzeitig auf mehrere Volumes geschrieben werden. Darüber hinaus bietet RAID 1 keine Verbesserung der Schreibleistung.

Erstellen Sie ein RAID 0-Array

Führen Sie die folgenden Schritte durch, um das RAID-0-Array zu erstellen.

Überlegungen

- Bevor Sie dieses Verfahren ausführen, müssen Sie entscheiden, wie groß Ihr RAID 0-Array sein soll und wie viele IOPS bereitgestellt werden sollen.
- Erstellen Sie Volumes mit jeweils identischen Werten für die Größe und IOPS-Leistung für Ihr Array. Stellen Sie sicher, dass Sie kein Array erstellen, das die verfügbare Bandbreite Ihrer EC2-Instance überschreitet.
- Sie sollten es vermeiden, von einem RAID-Volume zu booten. Wenn eines der Geräte ausfällt, können Sie das Betriebssystem möglicherweise nicht starten.

Linux-Instances

So erstellen Sie ein RAID-0-Array unter Linux

1. Erstellen Sie die Amazon EBS-Volumes für Ihr Array. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.
2. Weisen Sie die Amazon EBS-Volumes der Instance zu, in der das Array gehostet werden soll. Weitere Informationen finden Sie unter Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.
3. Verwenden Sie den Befehl mdadm, um ein logisches RAID-Gerät aus den gerade zugewiesenen Amazon EBS-Volumes zu erstellen. Ersetzen Sie die Anzahl der Volumes in Ihrem Array durch *`number_of_volumes`* und die Gerätenamen für jedes Volume im Array (z. B. `/dev/xvdf`) durch*`device_name`*. Sie können das Array auch *`MY_RAID`* durch Ihren eigenen eindeutigen Namen ersetzen.

   > **Note**
   >
   > Sie können die Geräte in Ihrer Instance mit dem Befehl lsblk auflisten, um die Gerätenamen anzuzeigen.

Sie erstellen ein RAID 0-Array, indem Sie den folgenden Befehl ausführen (achten Sie auf die Option `--level=0` für das Striping des Arrays):

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

> **Tip**
>
> Wenn Sie den Fehler `mdadm: command not found` erhalten, verwenden Sie den folgenden Befehl, um mdadm zu installieren: `sudo yum install mdadm`.

4. Warten Sie, bis das RAID-Array initialisiert und synchronisiert wird. Sie können den Fortschritt dieser Vorgänge mit dem folgenden Befehl verfolgen:

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

Ausgabebeispiel:

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

Allgemein können Sie detaillierte Informationen zu Ihrem RAID-Array mit dem folgenden Befehl anzeigen:

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

Ausgabebeispiel:

```
/dev/md0:
           Version : 1.2
     Creation Time : Wed May 19 11:12:56 2021
        Raid Level : raid0
        Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
```

```
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Wed May 19 11:12:56 2021
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

        Chunk Size : 512K

Consistency Policy : none

              Name : MY_RAID
              UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
            Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. Erstellen Sie ein Dateisystem in Ihrem RAID-Array und geben Sie diesem Dateisystem eine Bezeichnung; Sie verwenden diese Bezeichnung, wenn Sie es später mounten. Um beispielsweise ein ext4-Dateisystem mit der Bezeichnung zu erstellen*MY_RAID*, führen Sie den folgenden Befehl aus:

   ```
   [ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
   ```

   Abhängig von den Anforderungen an Ihre Anwendung oder den Einschränkungen für Ihr Betriebssystem können Sie einen anderes Dateisystem wie Ext3 oder XFS verwenden (weitere Informationen finden Sie in der Dokumentation zum entsprechenden Befehl für die Erstellung des Dateisystems).

6. Um sicherzustellen, dass das RAID-Array beim Booten automatisch wieder zusammengesetzt wird, erstellen Sie eine Konfigurationsdatei, die die RAID-Informationen enthält:

   ```
   [ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
   ```

> **Note**
>
> Wenn Sie eine andere Linux-Distribution als Amazon Linux verwenden, müssen Sie diesen Befehl möglicherweise ändern. Sie könnten beispielsweise die Datei an einem anderen Ort ablegen oder Sie müssen möglicherweise die `--examine`-Parameter hinzufügen. Um weitere Informationen zu erhalten, führen Sie man mdadm.conf auf Ihrer Linux-Instance aus.

7. Erstellen Sie ein neues Ramdisk-Image, um die Blockgerät-Module für Ihre neue RAID-Konfiguration korrekt vorzuladen:

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Erstellen Sie einen Einhängepunkt für Ihr RAID-Array.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Als letzten Schritt mounten Sie das RAID-Gerät an dem Einhängepunkt, den Sie erstellt haben:

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

   Das RAID-Gerät ist nun einsatzbereit.

10. (Optional) Sie mounten dieses Amazon EBS-Volume bei jedem Neustart des Systems, indem Sie in der Datei `/etc/fstab` einen Eintrag für das Gerät hinzufügen.

    a. Erstellen Sie eine Backup-Kopie der Datei `/etc/fstab` für den Fall, dass Sie diese Datei beim Bearbeiten versehentlich beschädigen oder löschen.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

    b. Öffnen Sie die Datei `/etc/fstab` mit einem Texteditor Ihrer Wahl (z. B. nano oder vim).

    c. Kommentieren Sie alle Zeilen aus, die mit "UUID=" beginnen, und fügen Sie am Ende der Datei eine neue Zeile für Ihr RAID-Volume hinzu; verwenden Sie dabei das folgende Format:

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

Die letzten drei Felder in dieser Zeile sind die Mounting-Optionen, die Sicherungshäufigkeit und die Reihenfolge der Überprüfungen beim Starten des Dateisystems. Wenn Sie nicht wissen, welche Werte Sie hier angeben sollten, dann verwenden Sie die Werte im Beispiel unten (`defaults,nofail 0 2`). Weitere Informationen zu `/etc/fstab`-Einträgen finden Sie in der fstab-Handbuchseite (durch Eingabe von man fstab in der Befehlszeile). Sie mounten z. B. das Ext4-Dateisystem auf dem Gerät mit der Bezeichnung MY_RAID an dem Einhängepunkt `/mnt/raid`, indem Sie den folgenden Eintrag in `/etc/fstab` hinzufügen.

> **Note**
>
> Wenn Sie jemals vorhaben, Ihre Instance zu booten, ohne dass dieses Volume angefügt ist (z. B. wenn dieses Volume zwischen verschiedenen Instances hin und her bewegt wird), sollten Sie die Mount-Option `nofail` hinzufügen; auf diese Weise ist ein Booten der Instance möglich, auch wenn beim Mounten des Volumes Probleme auftreten. Unter Debian-Derivaten wie Ubuntu muss außerdem die Mount-Option `nobootwait` hinzugefügt werden.

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. Wenn Sie den neuen Eintrag in `/etc/fstab` hinzugefügt haben, müssen Sie prüfen, ob Ihr Eintrag funktioniert. Führen Sie den Befehl sudo mount -a zum Mounten aller Dateisysteme in `/etc/fstab` aus.

```
[ec2-user ~]$ sudo mount -a
```

Wenn der letzte Befehl keinen Fehler produziert, dann ist die `/etc/fstab`-Datei in Ordnung und das Dateisystem wird beim nächste Bootvorgang automatisch gemountet. Wenn der Befehl Fehler zurückgibt, prüfen Sie diese und versuchen Sie, den Eintrag in entsprechend zu korrigiere `/etc/fstab`.

> **Warning**
>
> Fehler in der Datei `/etc/fstab` können dazu führen, dass ein System nicht mehr gestartet werden kann. Fahren Sie das System nicht herunter, wenn Fehler in der Datei `/etc/fstab` auftreten.

e. (Optional) Wenn Sie nicht sicher sind, wie Sie die Fehler in `/etc/fstab` korrigieren können, können Sie immer noch Ihre Backup-Kopie der Datei `/etc/fstab` wiederherstellen, indem Sie den folgenden Befehl ausführen.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

Windows-Instances

So erstellen Sie ein RAID-0-Array unter Windows

1. Erstellen Sie die Amazon EBS-Volumes für Ihr Array. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-Volume.
2. Weisen Sie die Amazon EBS-Volumes der Instance zu, in der das Array gehostet werden soll. Weitere Informationen finden Sie unter Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.
3. Herstellen einer Verbindung mit Ihrer Windows-Instance. Weitere Informationen finden Sie unter Verbinden mit Ihrer Windows-Instance.
4. Öffnen Sie eine Eingabeaufforderung und geben Sie den Befehl diskpart ein.

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. Listen Sie an der `DISKPART`-Eingabeaufforderung mit dem folgenden Befehl die verfügbaren Datenträger auf.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B
  Disk 2    Online            8 GB      0 B
```

Bestimmen Sie die Datenträger, die Sie in Ihrem Array verwenden möchten, und notieren Sie sich die entsprechenden Nummern.

6. Jeder Datenträger, den Sie in Ihrem Array verwenden möchten, muss ein dynamischer Online-Datenträger sein, auf dem keine Volumes vorhanden sind. Führen Sie die folgenden Schritte aus, um Basis-Datenträger in dynamische Datenträger zu konvertieren und alle vorhandenen Volumes zu löschen.

   a. Wählen Sie mit dem folgenden Befehl ein Laufwerk aus, das Sie in Ihrem Array verwenden möchten, und ersetzen Sie es durch Ihre Festplattennummer*n*.

   ```
   DISKPART> select disk n

   Disk n is now the selected disk.
   ```

   b. Wenn der ausgewählte Datenträger als `Offline` angezeigt wird, schalten Sie ihn online, indem Sie den Befehl online disk ausführen.

   c. Wenn für den ausgewählten Datenträger in der Spalte `Dyn` in der letzten list disk-Befehlsausgabe kein Sternchen angezeigt wird, müssen Sie ihn in einen dynamische Datenträger konvertieren.

   ```
   DISKPART> convert dynamic
   ```

   > **Note**
   >
   > Wenn eine Fehlermeldung ausgegeben wird, dass der Datenträger schreibgeschützt ist, können Sie das Schreibgeschützt-Flag mit dem Befehl ATTRIBUTE DISK CLEAR READONLY löschen und anschließend erneut versuchen, die Konvertierung in einen dynamische Datenträger durchzuführen.

   d. Mit dem Befehl detail disk können Sie prüfen, ob auf dem ausgewählten Datenträger Volumes vorhanden sind.

   ```
   DISKPART> detail disk

   XENSRC PVDISK SCSI Disk Device
   Disk ID: 2D8BF659
   Type   : SCSI
   Status : Online
   Path   : 0
   Target : 1
   LUN ID : 0
   ```

```
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 2     D   NEW VOLUME   FAT32  Simple      8189 MB  Healthy
```

Notieren Sie sich die Nummern für alle Volumes auf dem Datenträger. In diesem Beispiel lautet die Nummer für das Volume 2. Wenn keine Volumes vorhanden sind, können Sie den nächsten Schritt überspringen.

e. (Nur wenn im letzten Schritt Volumes ermittelt wurden) Wählen Sie alle im letzten Schritt ermittelten Volumes auf dem Datenträger aus und löschen Sie sie.

> ⚠ Warning
>
> Dadurch werden alle vorhandenen Daten auf dem Volume gelöscht.

i. Wählen Sie das Volume aus und ersetzen Sie es durch Ihre *n* Datenträgernummer.

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. Löschen Sie das Volume.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

iii. Wiederholen Sie diese Teilschritte für jedes Volume, das Sie auf dem ausgewählten Datenträger löschen müssen.

f. Wiederholen Sie Step 6 für jeden Datenträger, den Sie in Ihrem Array verwenden möchten.

7. Stellen Sie sicher, dass alle Datenträger, die Sie verwenden möchten, dynamische Datenträger sind. In diesem Fall werden in diesem Beispiel die Festplatten 1 und 2 für das RAID-Volume verwendet.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B   *
  Disk 2    Online            8 GB      0 B   *
```

8. Erstellen Sie Ihr RAID-Array. Unter Windows wird ein RAID 0-Volume als Stripe-Volume bezeichnet.

   Um ein Stripe-Volume-Array auf den Datenträgern 1 und 2 zu erstellen, verwenden Sie den folgenden Befehl (beachten Sie die `stripe`-Option zum Stripe des Arrays):

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

9. Überprüfen Sie das neue Volume.

```
DISKPART> list volume

  DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     C                NTFS   Partition     29 GB  Healthy    System
  Volume 1                      RAW    Stripe        15 GB  Healthy
```

   Beachten Sie, dass die Spalte `Type` jetzt anzeigt, dass Volume 1 ein `stripe`-Volume ist.

10. Wählen Sie Ihr Volume aus und formatieren Sie es; anschließend können Sie es verwenden.

    a. Wählen Sie das Volume aus, das Sie formatieren möchten, und ersetzen *n* Sie es durch Ihre Datenträgernummer.

```
DISKPART> select volume n
```

```
Volume n is the selected volume.
```

b. Formatieren Sie das Volume.

> **Note**
>
> Sie führen eine vollständige Formatierung durch, indem Sie die Option `quick` auslassen.

```
DISKPART> format quick recommended label="My new volume"

  100 percent completed

DiskPart successfully formatted the volume.
```

c. Weisen Sie Ihrem Volume einen verfügbaren Laufwerkbuchstaben zu.

```
DISKPART> assign letter f

DiskPart successfully assigned the drive letter or mount point.
```

Ihr neues Volume ist jetzt einsatzbereit.

Erstellen von Snapshots von Volumes in einem RAID-Array

Wenn Sie die Daten auf den EBS-Volumes in einem RAID-Array mithilfe von Snapshots sichern möchten, müssen Sie sicherstellen, dass die Snapshots konsistent sind. Dies liegt daran, dass die Snapshots dieser Volumes unabhängig voneinander erstellt werden. Die Wiederherstellung von EBS-Volumes in einem RAID-Array aus nicht synchronisierten Snapshots würde die Integrität des Arrays beeinträchtigen.

Verwenden Sie EBS-Schnappschüsse für mehrere Volumes, um einen konsistenten Satz von Snapshots für Ihr RAID-Array zu erstellen. Multi-volume Mit Snapshots können Sie zeitpunktgenaue, datenkoordinierte und absturzkonsistente Snapshots auf mehreren EBS-Volumes erstellen, die mit einer EC2-Instance verbunden sind. Sie müssen Ihre Instance nicht anhalten, um die Koordination zwischen den Volumes sicherzustellen, um die Konsistenz sicherzustellen, da Snapshots automatisch über mehrere EBS-Volumes hinweg erstellt werden. Weitere Informationen

finden Sie in den Schritten zum Erstellen von Snapshots mit mehreren Volumes unter Amazon EBS-Snapshots erstellen.

Benchmarken Sie Amazon EBS-Volumes

Sie können die Leistung von Amazon EBS-Volumes testen, indem Sie Workloads simulieren I/O . Der Prozess läuft folgendermaßen ab:

1. Starten Sie eine Instance. EBS-optimized
2. Erstellen Sie neue EBS-Volumes.
3. Hängen Sie die Volumes an Ihre EBS-optimized Instance an.
4. Konfigurieren Sie das Blockgerät und spielen Sie es auf.
5. Installieren Sie ein Tool zum I/O Leistungsvergleich.
6. Vergleichen Sie die I/O Leistung Ihrer Volumes.
7. Löschen Sie Ihre Volumes und beenden Sie Ihre Instance, damit keine weiteren Kosten anfallen.

> **Important**
>
> Einige der in diesem Thema beschriebenen Verfahren führen dazu, dass auf den EBS-Volumes, für die Sie Benchmark-Tests durchführen, vorhandene Daten gelöscht werden. Die Benchmark-Verfahren sind für die Verwendung auf Volumes vorgesehen, die speziell zu Testzwecken erstellt wurden, und nicht für Produktions-Volumes.

Einrichten Ihrer Instance

Um die optimale Leistung von EBS-Volumes zu erzielen, empfehlen wir Ihnen, eine EBS-optimized Instance zu verwenden. EBS-optimized Instances bieten eine dedizierte Bandbreite zwischen Amazon EC2 und Amazon EBS, wobei die Spezifikationen vom Instance-Typ abhängen.

Um eine EBS-optimized Instance zu erstellen, wählen Sie Launch as an EBS-optimized Instance, wenn Sie die Instance über die Amazon EC2-Konsole starten, oder geben Sie an, --ebs-optimized wenn Sie die Befehlszeile verwenden. Stellen Sie sicher, dass Sie einen Instance-Typ auswählen, der diese Option unterstützt.

Einrichten von Bereitgestellte IOPS-SSD- oder Allzweck-SSD-Volumes

Um Bereitgestellte IOPS-SSD- (`io1` und `io2`) oder Allzweck-SSD-Volumes (`gp2` und `gp3`) mithilfe der Amazon EC2-Konsole zu erstellen, wählen Sie als Volume-Typ Bereitgestellte IOPS-SSD (io1), Bereitgestellte IOPS-SSD (io2), Allzweck-SSD (gp2) oder Allzweck-SSD (gp3) aus. Geben Sie in der Befehlszeile `io1`, `io2`, `gp2` oder `gp3` für den --volume-type-Parameter an. Geben Sie für `io1io2`, und `gp3` Volumes die Anzahl der I/O Operationen pro Sekunde (IOPS) für den --iops Parameter an. Weitere Informationen erhalten Sie unter Amazon EBS-Volume-Typen und Erstellen Sie ein Amazon EBS-Volume.

(Nur Linux-Instanzen) Für die Beispieltests empfehlen wir, ein RAID 0-Array mit 6 Volumes zu erstellen, das ein hohes Leistungsniveau bietet. Wie hoch Ihre Kosten sind, hängt von den bereitgestellten Gigabytes (und der Anzahl der bereitgestellten IOPS für io1-, io2-, und gp3-Volumes) und nicht von der Anzahl der Volumes ab. Daher entstehen Ihnen keine zusätzlichen Kosten, wenn Sie mehrere, kleinere Volumes erstellen und zum Erstellen eines Stripesets verwenden. Wenn Sie Oracle Orion verwenden, um Benchmark-Tests auf Volumes durchzuführen, kann damit das Striping auf dieselbe Weise simuliert werden wie mit Oracle ASM. Wir empfehlen Ihnen daher, Orion das Striping zu überlassen. Wenn Sie ein anderes Benchmarking-Tool verwenden, müssen Sie die Volumes selbst mithilfe von Stripes verbinden.

Weitere Informationen zum Erstellen eines RAID 0-Arrays finden Sie unterErstellen Sie ein RAID 0-Array.

Richten Sie die Volumes Throughput Optimized HDD (**`st1`**) oder Cold HDD (**`sc1`**) ein

Wählen Sie beim Erstellen eines `st1`-Volumes mit der Amazon EC2-Konsole durchsatzoptimierte HDD aus oder geben Sie --type **`st1`** an, wenn Sie die Befehlszeile verwenden. Wählen Sie beim Erstellen eines `sc1`-Volumes mit der Amazon-EC2-Konsole „Cold-HDD“ aus oder geben Sie --type **`sc1`** an, wenn Sie die Befehlszeile verwenden. Informationen zum Erstellen von EBS-Volumes finden Sie unter Erstellen Sie ein Amazon EBS-Volume. Informationen zum Anfügen dieser Volumes zu Ihrer Instance finden Sie unter Hängen Sie ein Amazon EBS-Volume an eine Amazon EC2-Instance an.

(nur für Linux-Instances) AWS stellt eine JSON-Vorlage zur Verfügung CloudFormation , mit der dieser Einrichtungsvorgang vereinfacht wird. Greifen Sie auf die Vorlage zu und speichern Sie sie als JSON-Datei. CloudFormation ermöglicht Ihnen die Konfiguration Ihrer eigenen SSH-Schlüssel und bietet eine einfachere Möglichkeit, eine Leistungstestumgebung zur Bewertung von `st1` Volumes einzurichten. Die Vorlage erstellt eine Instance der aktuellen Generation und ein 2 TiB `st1`-Volume und fügt das Volume an die Instance unter `/dev/xvdf` an.

(Nur Linux-Instanzen) Um ein HDD-Volume mithilfe der Vorlage zu erstellen

1. Öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie Create Stack aus.
3. Klicken Sie auf Upload a Template to Amazon S3 und wählen Sie die JSON-Vorlage aus, die Sie zuvor erhalten haben.
4. Geben Sie Ihrem Stack einen Namen, etwa "ebs-perf-testing", und wählen Sie einen Instance-Typ (der Standardwert ist "r3.8xlarge") und SSH-Schlüssel aus.
5. Wählen Sie zweimal Next und anschließend Create Stack aus.
6. Nachdem sich der Status für Ihren neuen Stack von CREATE_IN_PROGRESS zu COMPLETE geändert hat, wählen Sie Outputs (Ausgaben) aus, um den öffentlichen DNS-Eintrag für Ihre neue Instance abzurufen, an die ein 2 TiB-`st1`-Volume angefügt wird.
7. Stellen Sie mithilfe von SSH eine Verbindung zum neuen Stack als Benutzer **`ec2-user`** her. Verwenden Sie hierbei den Hostnamen aus dem DNS-Eintrag, den Sie im vorherigen Schritt abgerufen haben.
8. Fahren Sie mit Installieren von Benchmark-Tools fort.

Installieren von Benchmark-Tools

In der folgenden Tabelle sind einige der möglichen Tools aufgeführt, mit denen Sie die Leistung von EBS-Volumes vergleichen können.

Linux-Instances

Tool	Beschreibung
fio	Zum Benchmarking I/O der Leistung. (Beachten Sie, dass für fio eine Abhängigkeit von `libaio-devel` besteht.) Führen Sie zum Installieren des fio auf Amazon Linux den folgenden Befehl aus: `$ sudo yum install -y fio` Verwenden Sie den folgenden Befehl, um fio unter Ubuntu zu installieren:

Tool	Beschreibung
	`sudo apt-get install -y fio`
Oracle Orion Calibration Tool	Zur Kalibrierung der I/O Leistung von Speichersystemen, die mit Oracle-Da tenbanken verwendet werden sollen.

Windows-Instances

Tool	Description
DiskSpd	DiskSpd ist ein Tool zur Speicherleistung, das von den Entwicklungsteams für Windows, Windows Server und Cloud Server Infrastructure von Microsoft entwickelt wurde. Es steht unter zum Download bereit https://github.com/Microsoft/diskspd/releases. Nachdem Sie die ausführbare Datei `diskspd.exe` heruntergeladen haben, öffnen Sie eine Eingabeaufforderung mit Administratorrechten (indem Sie „Als Administrator ausführen“ auswählen) und navigieren Sie dann zu dem Verzeichnis, in das Sie die Datei `diskspd.exe` kopiert haben. Kopieren Sie die gewünschte ausführbare Datei `diskspd.exe` aus dem entsprechenden ausführbaren Ordner (`amd64fre`, `armfre` oder `x86fre`)) in einen kurzen, einfachen Pfad wie `C:\DiskSpd` . In den meisten Fällen benötigen Sie die 64-Bit-Version von DiskSpd aus dem `amd64fre` Ordner. Der Quellcode für DiskSpd wird GitHub unter gehostet: https://github.com/Microsoft/diskspd.
CrystalDiskMark	CrystalDiskMark ist eine einfache Festplatten-Benchmark-Software. Sie steht unter zum Download bereit https://crystalmark.info/en/software/crystaldiskmark/.

Diese Benchmarking-Tools unterstützen zahlreiche Testparameter. Sie sollten nur Befehle verwenden, die die von Ihren Volumes unterstützten Workloads durch Annäherung bestimmen. Diese Befehle sind unten aufgeführt und dienen als Beispiele, um Ihnen den Einstieg zu erleichtern.

Auswählen der Volume-Warteschlangenlänge

Wählen Sie die beste Länge der Volume-Warteschlange basierend auf Ihrem Workload und Volume-Typ aus.

Länge der Warteschlange auf SSD-backed Volumes

Um die optimale Warteschlangenlänge für Ihre Arbeitslast auf SSD-backed Volumes zu ermitteln, empfehlen wir, eine Warteschlangenlänge von 1 pro 1000 verfügbaren IOPS anzustreben (Basiswert für SSD-Volumes für allgemeine Zwecke und bereitgestellte Menge für bereitgestellte IOPS-SSD-Volumes). Sie können dann die Leistung Ihrer Anwendung beobachten und diesen Wert basierend auf den Anwendungsanforderungen optimieren.

Das Verlängern der Warteschlange ist nützlich, bis Sie die bereitgestellten IOPS, den bereitgestellten Durchsatz oder den optimalen Wert für die Systemwarteschlangenlänge erreicht haben, der derzeit auf 32 festgelegt ist. Für ein Volume mit 3 000 bereitgestellten IOPS empfiehlt sich beispielsweise eine Warteschlangenlänge von 3. Sie sollten mit diesen Werten experimentieren und sie nach oben oder unten anpassen, um den für Ihre Anwendung optimalen Wert zu finden.

Warteschlangenlänge auf Volumes HDD-backed

Um die optimale Warteschlangenlänge für Ihre Arbeitslast auf HDD-backed Volumes zu ermitteln, empfehlen wir Ihnen, eine Warteschlangenlänge von mindestens 4 anzustreben und gleichzeitig eine sequentielle Ausführung von 1 MiB durchzuführen. I/Os Sie können dann die Leistung Ihrer Anwendung beobachten und diesen Wert basierend auf den Anwendungsanforderungen optimieren. Beispielsweise sollte ein `st1` 2-TiB-Volume mit einem Burst-Durchsatz von 500 MiB/s und IOPS von 500 eine Warteschlangenlänge von 4, 8 oder 16 bei sequentieller Leistung von 1.024 KiB, 512 KiB oder 256 KiB anstreben. I/Os Sie sollten mit diesen Werten experimentieren und sie nach oben oder unten anpassen, um den für Ihre Anwendung optimalen Wert zu finden.

Deaktivieren C-states

Bevor Sie das Benchmarking ausführen, sollten Sie den Prozessor C-states deaktivieren. C-state Um Strom zu sparen, können Kerne in einer unterstützten CPU vorübergehend inaktiv sein. Wenn der Kern aufgerufen wird, vergeht eine gewisse Zeit, bis der Kern wieder voll funktionsfähig ist. Diese Latenzzeit kann die Prozessor-Benchmarking-Routinen stören. Weitere Informationen dazu C-states und welche EC2-Instance-Typen sie unterstützen, finden Sie unter Prozessorstatussteuerung für Ihre EC2-Instance.

Linux-Instances

Sie können das Gerät C-states auf Amazon Linux, RHEL und CentOS wie folgt deaktivieren:

1. Ermitteln Sie die Anzahl von. C-states

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. Deaktiviere den C-states Wert von c1 bis cN. Im Idealfall sollten sich die Kerne im Zustand c0 befinden.

```
$ for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

Windows-Instances

Sie können es C-states unter Windows wie folgt deaktivieren:

1. Rufen Sie PowerShell unter das aktuelle aktive Energieschema ab.

```
$current_scheme = powercfg /getactivescheme
```

2. Holen Sie sich die GUID für das Energiesparschema.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter
 "ElementName='High performance'").InstanceID
```

3. Holen Sie sich die GUID für die Energieeinstellungen.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter
 "ElementName='Processor idle disable'").InstanceID
```

4. Holen Sie sich die GUID für die Energieeinstellungen-Untergruppe.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -
Filter "ElementName='Processor power management'").InstanceID
```

5. Deaktivieren Sie, C-states indem Sie den Wert des Indexes auf 1 setzen. Ein Wert von 0 gibt an, dass C-states sie deaktiviert sind.

```
powercfg /
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>
 1
```

6. Stellen Sie das aktive Schema ein, um sicherzustellen, dass die Einstellungen gespeichert werden.

```
powercfg /setactive <power_scheme_guid>
```

Durchführen von Benchmark-Tests

In den folgenden Verfahren werden die Benchmarking-Befehle für verschiedene EBS-Volume-Typen beschrieben.

Führen Sie die folgenden Befehle auf einer EBS-optimized Instance mit angehängten EBS-Volumes aus. Wenn die EBS-Volumes aus Snapshots erstellt wurden, sollten Sie sie vor dem Benchmark-Test initialisieren. Weitere Informationen finden Sie unter Initialisieren Sie die Volumes nach der Erstellung manuell.

> **Tip**
>
> Sie können die I/O Latenzhistogramme verwenden, die in den detaillierten Leistungsstatistiken von EBS bereitgestellt werden, um die Leistungsverteilung in Ihren Benchmark-Tests I/O zu vergleichen. Weitere Informationen finden Sie unter Detaillierte Leistungsstatistiken von Amazon EBS.

Wenn Sie mit dem Testen Ihrer Volumes fertig sind, finden Sie in den folgenden Themen Hilfe beim Aufräumen: Löschen eines Amazon EBS-Volumes und Beenden Sie Ihre Instance.

Durchführen von Benchmark-Tests der Bereitgestellte IOPS-SSD- und Allzweck-SSD-Volumes

Linux-Instances

Führen Sie fio das RAID 0-Array aus, das Sie erstellt haben.

Mit dem folgenden Befehl werden zufällige 16 KB-Schreiboperationen ausgeführt.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --name fio_test_file --
direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --
group_reporting --norandommap
```

Mit dem folgenden Befehl werden zufällige 16 KB-Leseoperationen ausgeführt.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1 --rw=randread
 --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --
norandommap
```

Weitere Informationen zum Interpretieren der Ergebnisse finden Sie in diesem Tutorial: Inspecting disk IO performance with fio (Untersuchen der Festplatten-I/O-Leistung mit "fio").

Windows-Instances

Führen Sie DiskSpd für das Volume aus, das Sie erstellt haben.

Mit dem folgenden Befehl wird ein I/O 30-Sekunden-Zufallstest unter Verwendung einer 20-GB-Testdatei auf dem `C:` Laufwerk mit einer Schreibrate von 25% und einer Leserate von 75% sowie einer Blockgröße von 8 K ausgeführt. Er verwendet acht Worker-Threads mit jeweils vier ausstehenden I/Os Threads und einem Startwert für die Schreibentropie von 1 GB. Die Ergebnisse des Tests werden in einer Textdatei mit dem Namen `DiskSpeedResults.txt` gespeichert. Diese Parameter simulieren eine SQL Server-OLTP-Workload.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Weitere Informationen zum Interpretieren der Ergebnisse finden Sie in diesem Tutorial: Inspecting disk IO performance with DiskSPd.

Benchmark-Volumes `st1` und `sc1` (Linux-Instanzen)

Führen Sie fio auf Ihrem `st1` oder `sc1` Volume aus.

> **Note**
>
> Bevor Sie diese Tests ausführen, stellen Sie den Puffermodus I/O auf Ihrer Instance ein, wie unter beschrieben. Erhöhen Sie den Read-Ahead-Wert für Workloads mit hohem Durchsatz und leseintensiven Workloads auf st1 und sc1 (Nur Linux-Instanzen)

Mit dem folgenden Befehl werden sequenzielle 1 MiB-Leseoperationen auf einem angeschlossenen `st1`-Blockgerät durchgeführt (z. B. `/dev/xvdf`):

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

Mit dem folgenden Befehl werden sequenzielle 1 MiB-Schreiboperationen auf einem angeschlossenen `st1`-Blockgerät durchgeführt:

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

Bei einigen Workloads wird eine Mischung aus sequenziellen Lese- und Schreiboperationen auf verschiedenen Teilen des Blockgeräts ausgeführt. Um für einen solchen Workload einen Benchmark-Test durchzuführen, wird empfohlen, separate, gleichzeitige fio-Jobs für Lese- und Schreiboperationen zu verwenden. Zudem sollten Sie die Option fio `offset_increment` verwenden, um für jeden Job andere Blockgerät-Speicherorte zu nutzen.

Das Ausführen dieses Workloads ist etwas komplizierter als bei einem Workload mit sequenziellen Schreib- oder sequentiellen Leseoperationen. Verwenden Sie einen Texteditor, um eine fio-Jobdatei (in diesem Beispiel `fio_rw_mix.cfg`) zu erstellen, die Folgendes enthält:

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
```

```
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

Führen Sie anschließend den folgenden Befehl aus:

```
$ sudo fio fio_rw_mix.cfg
```

Weitere Informationen zur Interpretation der Ergebnisse finden Sie in diesem Tutorial: Überprüfen der I/O Festplattenleistung mit fio.

Mehrere direkte fio Aufträge können I/O, obwohl sequentielle Lese- oder Schreibvorgänge verwendet werden, zu einem niedrigeren Durchsatz als erwartet für `st1` und Volumes führen. `sc1` Es wird empfohlen, einen direkten I/O Auftrag zu verwenden und den `iodepth` Parameter zu verwenden, um die Anzahl der gleichzeitigen I/O Operationen zu steuern.

Automatisieren Sie Backups mit Amazon Data Lifecycle Manager

Sie können Amazon Data Lifecycle Manager verwenden, um die Erstellung, Aufbewahrung und Löschung von EBS-Snapshots und AMIs zu automatisieren. EBS-backed Wenn Sie die Snapshot- und AMI-Verwaltung automatisieren, können Sie Folgendes tun:

- Wertvolle Daten zu schützen, indem ein regelmäßiger Backup-Plan eingehalten wird.
- Erstellen Sie standardisierte AMIs, die in regelmäßigen Abständen aktualisiert werden können.
- Backups aufzubewahren, die für Prüfer oder interne Compliance-Vorschriften benötigt werden.
- Speicherkosten zu reduzieren, indem veraltete Backups gelöscht werden.
- Erstellen Sie Backup-Richtlinien für die Notfallwiederherstellung, die Daten in isolierten Regionen oder Konten sichern.

In Kombination mit Amazon EventBridge und AWS CloudTrail Monitoring bietet Amazon Data Lifecycle Manager eine komplette Backup-Lösung für Amazon EC2-Instances und EBS-Volumes ohne zusätzliche Kosten.

> **Important**
>
> - Amazon Data Lifecycle Manager kann keine Snapshots oder AMIs verwalten, die auf andere Weise erstellt wurden.
> - Amazon Data Lifecycle Manager kann die Erstellung, Aufbewahrung und Löschung von Instance-Speicher-gestützten AMIs nicht automatisieren.

Amazon Data Lifecycle Manager wird als Servicefähigkeit von Amazon Elastic Block Store (Amazon EBS) bewertet. Alle AWS Services im Rahmen des Compliance-Programms (FedRAMP, HIPAA BAA, SOC usw.), in denen Amazon EBS aufgeführt ist, gelten auch für Amazon Data Lifecycle Manager.

Kontingente

Für Ihr AWS Konto gelten die folgenden Kontingente im Zusammenhang mit Amazon Data Lifecycle Manager:

Description	Kontingent
Benutzerdefinierte Lebenszyklusrichtlinien nach Region	100
Standardrichtlinien für EBS-Snapshots nach Region	1
Standardrichtlinien für EBS-backed AMIs pro Region	1
Tags pro Ressource	45

Funktionsweise von Amazon Data Lifecycle Manager

Im Folgenden werden die Schlüsselelemente von Amazon Data Lifecycle Manager beschrieben.

Elemente

- Richtlinien
- Zeitpläne für Richtlinien (Nur benutzerdefinierte Richtlinien)
- Zielressourcen-Tags (Nur benutzerdefinierte Richtlinien)
- -Snapshots
- EBS-backed AMIs
- Amazon-Data-Lifecycle-Manager-Tags

Richtlinien

Mit Amazon Data Lifecycle Manager erstellen Sie Richtlinien, um Ihre Anforderungen an die Erstellung und Aufbewahrung von Backups zu definieren. In diesen Richtlinien sind in der Regel folgende Angaben enthalten:

- Richtlinientyp — Definiert die Art der Backup-Ressourcen, die von der Richtlinie verwaltet werden (Snapshots oder EBS-backed AMIs).
- Zielressourcen – definiert den Typ der Ressourcen, für die die Richtlinien gelten (Instances oder EBS-Volumes).
- Erstellungshäufigkeit – definiert, wie oft die Richtlinie ausgeführt wird, und erstellt Snapshots oder AMIs.
- Aufbewahrungsschwellenwert – definiert, wie lange die Richtlinie Snapshots oder AMIs nach der Erstellung aufbewahrt.
- Zusätzliche Aktionen – definiert zusätzliche Aktionen, die die Richtlinie ausführen soll, wie z. B. regionsübergreifendes Kopieren, Archivieren oder Ressourcen-Tagging.

Amazon Data Lifecycle Manager bietet Standardrichtlinien und benutzerdefinierte Richtlinien.

Standardrichtlinien

Standardrichtlinien sichern alle Volumes und Instances in einer Region, für die es keine aktuellen Backups gibt. Sie können Volumes und Instances optional ausschließen, indem Sie Ausschlussparameter angeben.

Amazon Data Lifecycle Manager unterstützt die folgenden Standardrichtlinien:

- Standardrichtlinie für EBS-Snapshots – zielt auf Volumes ab und automatisiert die Erstellung, Aufbewahrung und Löschung von Snapshots.
- Standardrichtlinie für EBS-backed AMIs — Zielt auf Instances ab und automatisiert die Erstellung, Aufbewahrung und Deregistrierung von AMIs. EBS-backed

Sie können in jedem Konto und in jeder AWS -Region nur eine Standardrichtlinie pro Ressourcentyp festlegen.

Benutzerdefinierte Richtlinien

Benutzerdefinierte Richtlinien zielen auf der Grundlage der zugewiesenen Tags auf bestimmte Ressourcen ab und unterstützen erweiterte Features wie die schnelle Snapshot-Wiederherstellung, die Snapshot-Archivierung, kontoübergreifendes Kopieren und Vor- und Nach-Skripte. Eine benutzerdefinierte Richtlinie kann bis zu 4 Zeitpläne enthalten, wobei jeder Zeitplan eine eigene Erstellungshäufigkeit, einen eigenen Aufbewahrungsschwellenwert und eine erweiterte Featurekonfiguration aufweisen kann.

Amazon Data Lifecycle Manager unterstützt die folgenden benutzerdefinierten Richtlinien:

- Richtlinie für EBS-Snapshots – zielt auf Volumes oder Instances ab und automatisiert die Erstellung, Aufbewahrung und Löschung von EBS-Snapshots.
- EBS-backed AMI-Richtlinie — Zielt auf Instances ab und automatisiert die Erstellung, Aufbewahrung und Deregistrierung von AMIs. EBS-backed
- Cross-account Event-Richtlinie kopieren — Automatisiert regionsübergreifende Kopieraktionen für Snapshots, die mit Ihnen geteilt werden.

Weitere Informationen finden Sie unter Standardrichtlinien von Amazon Data Lifecycle Manager im Vergleich zu benutzerdefinierten Richtlinien.

Zeitpläne für Richtlinien (Nur benutzerdefinierte Richtlinien)

Zeitpläne von Richtlinien definieren, wann Snapshots oder AMIs von der Richtlinie erstellt werden. Richtlinien können bis zu vier Zeitpläne umfassen—einen obligatorischen Zeitplan und bis zu drei optionale Zeitpläne.

Durch das Hinzufügen mehrerer Zeitpläne zu einer einzelnen Richtlinie können Sie Snapshots oder AMIs mit unterschiedlicher Häufigkeit mit derselben Richtlinie erstellen. Sie können beispielsweise eine einzelne Richtlinie erstellen, die tägliche, wöchentliche, monatliche und jährliche Snapshots erstellt. Dadurch entfällt die Notwendigkeit, mehrere Richtlinien zu verwalten.

Für jeden Zeitplan können Sie die Häufigkeit, Einstellungen für die schnelle Snapshot-Wiederherstellung (nur Snapshot-Lebenszyklusrichtlinien), regionsübergreifende Kopierregeln und Tags (Markierungen) definieren. Die einem Zeitplan zugewiesenen Tags (Markierungen) werden automatisch den Snapshots oder AMIs zugewiesen, die beim Auslösen des Zeitplans erstellt werden. Darüber hinaus weist Amazon Data Lifecycle Manager jedem Snapshot oder AMI basierend auf der Häufigkeit des Zeitplans automatisch einen vom System generierten Tag (Markierung) zu.

Jeder Zeitplan wird individuell basierend auf seiner Häufigkeit ausgelöst. Wenn mehrere Zeitpläne gleichzeitig ausgelöst werden, erstellt Amazon Data Lifecycle Manager nur einen Snapshot oder AMI und verwendet die Aufbewahrungseinstellungen des Zeitplans, der den höchsten Aufbewahrungszeitraum aufweist. Die Tags (Markierungen) aller ausgelösten Zeitpläne werden auf den Snapshot oder AMI angewendet.

- (Nur Snapshot-Lebenszyklusrichtlinien) Wenn für mehr als einen der ausgelösten Zeitpläne eine schnelle Snapshot-Wiederherstellung aktiviert ist, wird für den Snapshot die schnelle

Snapshot-Wiederherstellung in allen Availability Zones aktiviert, die in allen ausgelösten Zeitplänen angegeben sind. Die höchsten Aufbewahrungseinstellungen der ausgelösten Zeitpläne werden für jede Availability Zone verwendet.

- Wenn für mehr als einen der ausgelösten Zeitpläne eine bereichsübergreifenden Kopie aktiviert ist, wird der Snapshot oder AMI in alle Regionen kopiert, die allen ausgelösten Zeitplänen angegeben sind. Die höchste Aufbewahrungsdauer der ausgelösten Zeitpläne wird angewendet.

Zielressourcen-Tags (Nur benutzerdefinierte Richtlinien)

Benutzerdefinierte Richtlinien von Amazon Data Lifecycle Manager verwenden Ressourcen-Tags für die Identifizierung der zu sichernden Ressourcen. Wenn Sie einen Snapshot oder eine EBS-backed AMI-Richtlinie erstellen, können Sie mehrere Zielressourcen-Tags angeben. Alle Ressourcen des festgelegten Typs (Instance oder Volume), die mindestens eines der angegebenen Zielressourcen-Tags haben, werden von der Richtlinie erfasst. Wenn Sie beispielsweise eine Snapshot-Richtlinie erstellen, die auf Volumes abzielt, und Sie `purpose=prod`, `costcenter=prod` und `environment=live` als Zielressourcen-Tags angeben, dann zielt die Richtlinie auf alle Volumes ab, die eines dieser Tag-Schlüsselwert-Paare haben.

Wenn Sie mehrere Richtlinien für eine Ressource anwenden möchten, können Sie der Zielressource mehrere Tags zuweisen und dann separate Richtlinien erstellen, die jeweils auf ein bestimmtes Ressourcen-Tag abzielen.

Die Zeichen \ und = können Sie in einem Tag-Schlüssel nicht verwenden. Bei Zielressourcen-Tags muss die Groß-/Kleinschreibung beachtet werden. Weitere Informationen finden Sie unter Taggen Sie Ihre Ressourcen.

-Snapshots

Snapshots sind die primäre Methode, Daten von Ihren EBS-Volumes zu sichern. Um Speicherkosten zu sparen, sind aufeinanderfolgende Snapshots inkrementell und enthalten nur die Volume-Daten, die sich seit dem vorherigen Snapshot geändert haben. Wenn Sie einen Snapshot in einer Reihe von Snapshots für ein Volume löschen, werden nur die Daten entfernt, die nur in diesem Snapshot vorhanden sind. Der Rest des erfassten Volume-Verlaufs wird beibehalten. Weitere Informationen finden Sie unter Amazon EBS-Snapshots.

EBS-backed AMIs

Ein Amazon Machine Image (AMI) stellt die Informationen zur Verfügung, die zum Starten einer Instance erforderlich sind. Sie können mehrere Instances aus einem einzigen AMI starten, wenn Sie mehrere Instances mit derselben Konfiguration benötigen. Amazon Data Lifecycle Manager unterstützt nur EBS-backed AMIs. EBS-backed AMIs enthalten einen Snapshot für jedes EBS-Volume, das an die Quell-Instance angehängt ist. Weitere Informationen finden Sie unter Amazon Machine Images (AMI).

Amazon-Data-Lifecycle-Manager-Tags

Amazon Data Lifecycle Manager wendet die folgenden System-Tags auf alle Snapshots und AMIs an, die durch eine Richtlinie erstellt werden, um sie von Snapshots und AMIs zu unterscheiden, die auf andere Weise erstellt werden:

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` – Für Snapshots, die nach einem altersbasierten Zeitplan erstellt wurden. Gibt an, wann der Snapshot aus der Standardstufe gelöscht werden muss.
- `dlm:managed`
- `aws:dlm:archived` – Für Snapshots, die nach einem Zeitplan archiviert wurden.
- `aws:dlm:pre-script` – für Snapshots, die mit Vor-Skripten erstellt wurden.
- `aws:dlm:post-script` – für Snapshots, die mit Nach-Skripten erstellt wurden.

Sie können auch benutzerdefinierte Tags (Markierungen) angeben, die bei der Erstellung auf Snapshots und AMIs angewendet werden. Die Zeichen \ und = können Sie in einem Tag-Schlüssel nicht verwenden.

Die Ziel-Tags (Markierungen), die Amazon Data Lifecycle Manager zum Zuordnen der Volumes zu einer Snapshot-Richtlinie verwendet, können optional auf Snapshots angewendet werden, die von der Richtlinie erstellt wurden. In ähnlicher Weise können die Ziel-Tags (Markierungen), die verwendet werden, um Instances mit einer AMI-Richtlinie zu verknüpfen, optional auf AMIs angewendet werden, die von der Richtlinie erstellt wurden.

Standardrichtlinien von Amazon Data Lifecycle Manager im Vergleich zu benutzerdefinierten Richtlinien

In diesem Abschnitt werden Standardrichtlinien und benutzerdefinierte Richtlinien verglichen und ihre Gemeinsamkeiten und Unterschiede hervorgehoben.

Themen

- Vergleich der EBS-Snapshot-Richtlinien
- EBS-backed Vergleich der AMI-Richtlinien

Vergleich der EBS-Snapshot-Richtlinien

In der folgenden Tabelle werden die Unterschiede zwischen der Standardrichtlinie für EBS-Snapshots und benutzerdefinierten EBS-Snapshot-Richtlinien hervorgehoben.

Feature	Standardrichtlinie für EBS-Snapshots	Benutzerdefinierte Richtlinie für EBS-Snapshot
Verwaltete Backup-Ressource	EBS Snapshot	EBS Snapshot
Typen von Zielressourcen	Datenträger	Volumes oder Instances
Ausrichtung auf Ressourcen	Zielt auf alle Volumes in der Region ab, für die keine aktuellen Snapshots vorhanden sind. Sie können Ausschlussparameter angeben, um bestimmte Volumes auszuschließen.	Zielt nur auf Volumes oder Instances ab, die über bestimmte Tags verfügen.
Ausschlussparameter	Ja, kann Startvolumes, bestimmte Volume-Typen und Volumes mit bestimmten Tags ausschließen.	Ja, kann bei der Ausrichtung auf Instances Startvolumes und Volumes mit bestimmten Tags ausschließen.
Support AWS Outposts	Nein	Ja

Feature	Standardrichtlinie für EBS-Snapshots	Benutzerdefinierte Richtlinie für EBS-Snapshot
Unterstützung mehrerer Zeitpläne	Nein	Ja, bis zu 4 Zeitpläne pro Richtlinie
Unterstützte Aufbewahrungsarten	Age-based Nur Aufbewahrung	Age-based und zahlenbasierte Aufbewahrung
Häufigkeit der Erstellung von Snapshots	Alle 1 bis 7 Tage.	Tägliche, wöchentliche, monatliche, jährliche oder benutzerdefinierte Häufigkeit unter Verwendung eines Cron-Ausdrucks.
Snapshot-Aufbewahrung	2 bis 14 Tage.	Bis zu 1 000 Snapshots (anzahlbasiert) oder bis zu 100 Jahre (altersbasiert).
Unterstützung für anwendungskonsistente Snapshots	Nein	Ja, bei Vor- und Nach-Skripten
Unterstützung der Snapshot-Archivierung	Nein	Ja
Unterstützung der schnellen Snapshot-Wiederherstellung	Nein	Ja

Feature	Standardrichtlinie für EBS-Snapshots	Benutzerdefinierte Richtlinie für EBS-Snapshot
Unterstützung für regionsübergreifendes Kopieren	Ja, mit den Standardeinstellungen [1]	Ja, mit benutzerdefinierten Einstellungen
Unterstützung der kontoübergreifenden Freigabe	Nein	Ja
Unterstützung für erweitertes Löschen [2]	Ja	Nein

[1] Für Standardrichtlinien:

- Sie können keine Tags in regionsübergreifende Kopien kopieren.
- Für Kopien gilt der gleiche Aufbewahrungszeitraum wie für den Quell-Snapshot.
- Kopien erhalten den gleichen Verschlüsselungsstatus wie der Quell-Snapshot. Wenn die Zielregion standardmäßig für die Verschlüsselung aktiviert ist, werden Kopien immer verschlüsselt, auch wenn die Quell-Snapshots unverschlüsselt sind. Kopien werden immer mit dem standardmäßigen KMS-Schlüssel für die Zielregion verschlüsselt.

[2] Für Standard- und benutzerdefinierte Richtlinien:

- Wenn eine Ziel-Instance oder ein Zielvolume gelöscht wird, löscht Amazon Data Lifecycle Manager auf Grundlage des Aufbewahrungszeitraums weiterhin Snapshots bis zum letzten Snapshot, jedoch nicht einschließlich dieses Snapshots. Bei Standardrichtlinien können Sie den Löschvorgang auf den letzten Snapshot ausweiten.
- Wenn eine Richtlinie gelöscht oder in den Status „Fehler“ oder „Deaktiviert“ versetzt wird, beendet Amazon Data Lifecycle Manager das Löschen von Snapshots. Bei Standardrichtlinien können Sie den Löschvorgang ausweiten und weiterhin Snapshots löschen, einschließlich des letzten.

EBS-backed Vergleich der AMI-Richtlinien

In der folgenden Tabelle werden die Unterschiede zwischen der Standardrichtlinie für EBS-backed AMIs und den benutzerdefinierten EBS-backed AMI-Richtlinien hervorgehoben.

Feature	Standardrichtlinie für EBS-backed AMIs	Benutzerdefinierte EBS-backed AMI-Richtlinie
Verwaltete Backup-Ressource	EBS-backed AMIs	EBS-backed AMIs
Typen von Zielressourcen	Instances	Instances
Ausrichtung auf Ressourcen	Zielt auf alle Instances in der Region ab, die über keine aktuellen AMIs verfügen. Sie können Ausschlussparameter angeben, um bestimmte Instances auszuschließen.	Zielt nur auf Instances ab, die über bestimmte Tags verfügen.
Instances vor der AMI-Erstellung neu starten	Nein	Ja
Ausschlussparameter	Ja, kann Instances mit bestimmten Tags ausschließen.	Nein
Unterstützung mehrerer Zeitpläne	Nein	Ja, bis zu 4 Zeitpläne pro Richtlinie.
Häufigkeit der AMI-Erstellung	Alle 1 bis 7 Tage.	Tägliche, wöchentliche, monatliche, jährliche oder benutzerdefinierte Häufigkeit unter Verwendung eines Cron-Ausdrucks.

Feature	Standardrichtlinie für EBS-backed AMIs	Benutzerdefinierte EBS-backed AMI-Richtlinie
Unterstützte Aufbewahrungsarten	Age-based Nur Aufbewahrung.	Age-based und auf Anzahl basierende Aufbewahrung.
Aufbewahrung von AMIs	2 bis 14 Tage.	Bis zu 1 000 AMIs (anzahlbasiert) oder bis zu 100 Jahre (altersbasiert).
Unterstützung für AMI-Veralterung	Nein	Ja
Unterstützung für regionsübergreifendes Kopieren	Ja, mit den Standardeinstellungen [1]	Ja, mit benutzerdefinierten Einstellungen
Unterstützung für erweitertes Löschen [2]	Ja	Nein

[1] Für Standardrichtlinien:

- Sie können keine Tags in regionsübergreifende Kopien kopieren.
- Für Kopien gilt der gleiche Aufbewahrungszeitraum wie für das Quell-AMI.
- Kopien erhalten den gleichen Verschlüsselungsstatus wie das Quell-AMI. Wenn die Zielregion standardmäßig für die Verschlüsselung aktiviert ist, werden Kopien immer verschlüsselt, auch wenn die Quell-AMIs unverschlüsselt sind. Kopien werden immer mit dem standardmäßigen KMS-Schlüssel für die Zielregion verschlüsselt.

[2] Für Standard- und benutzerdefinierte Richtlinien:

- Wenn eine Ziel-Instance beendet wird, meldet Amazon Data Lifecycle Manager auf Grundlage des Aufbewahrungszeitraums weiterhin AMIs bis zum letzten AMI ab, jedoch nicht einschließlich dieses AMIs. Bei Standardrichtlinien können Sie die Abmeldung auf das letzte AMI ausweiten.

- Wenn eine Richtlinie gelöscht oder in den Status „Fehler“ oder „Deaktiviert“ versetzt wird, beendet Amazon Data Lifecycle Manager das Abmelden von AMIs. Bei Standardrichtlinien können Sie den Abmeldevorgang ausweiten und weiterhin AMIs löschen, einschließlich des letzten.

Erstellen Sie Amazon Data Lifecycle Manager-Standardrichtlinien

Verwenden Sie die Standardrichtlinie für EBS-backed AMIs, um regelmäßig EBS-backed AMIs aus Instances zu erstellen. Verwenden Sie die Standardrichtlinie für EBS-Snapshots, um unabhängig von ihrem Anhangsstatus Snapshots aller Volumes zu erstellen oder bestimmte Volumes auszuschließen.

In diesem Abschnitt wird beschrieben, wie Standardrichtlinien erstellt werden.

Themen

- Überlegungen zu Standardrichtlinien
- Erstellen Sie eine Standardrichtlinie für Amazon EBS-Snapshots
- Erstellen Sie eine Standardrichtlinie für AMIs EBS-backed
- Aktivieren Sie die Data Lifecycle Manager-Standardrichtlinien für alle Konten und Regionen

Überlegungen zu Standardrichtlinien

Bedenken Sie bei der Arbeit mit Standardrichtlinien Folgendes:

- Mit Standardrichtlinien werden keine Zielressourcen (Instances oder Volumes) gesichert, für die aktuelle Sicherungen (Snapshots oder AMIs) vorhanden sind. Die Häufigkeit der Erstellung bestimmt, welche Ressourcen gesichert werden. Ein Volume oder eine Instance wird nur gesichert, wenn der letzte Snapshot oder das letzte AMI älter als die Erstellungshäufigkeit der Richtlinie ist. Wenn Sie beispielsweise eine Erstellungshäufigkeit von 3 Tagen angeben, erstellt die Standardrichtlinie für EBS-Snapshots nur dann einen Snapshot eines Volumes, wenn der letzte Snapshot älter als 3 Tage ist.
- Standardmäßig zielen Standardrichtlinien auf alle Instances oder Volumes in der Region ab, sofern keine Ausschlussparameter angegeben sind.
- Durch Standardrichtlinien wird ein Mindestsatz an eindeutigen Snapshots erstellt. Wenn Sie beispielsweise die EBS-backed AMI-Richtlinie und die EBS-Snapshot-Richtlinie aktivieren, dupliziert die Snapshot-Richtlinie keine Snapshots von Volumes, die bereits durch die EBS-backed AMI-Richtlinie gesichert wurden.
- Standardrichtlinien zielen zunächst nur auf Ressourcen ab, die mindestens 24 Stunden alt sind.

- Wenn Sie ein Volume löschen oder eine Instance beenden, für das bzw. die eine Standardrichtlinie gilt, löscht Amazon Data Lifecycle Manager weiterhin die zuvor erstellten Sicherungen (Snapshots oder AMIs) entsprechend der Aufbewahrungsdauer bis zur letzten Sicherung, aber nicht einschließlich dieser. Sie müssen diese Sicherung manuell löschen, wenn sie nicht benötigt wird.

  Wenn Sie möchten, dass Amazon Data Lifecycle Manager die letzte Sicherung löscht, können Sie Löschen verlängern aktivieren.
- Wenn eine Standardrichtlinie gelöscht oder in den Status „Fehler“ oder „Deaktiviert“ versetzt wird, beendet Amazon Data Lifecycle Manager das Löschen zuvor erstellter Sicherungen (Snapshots oder AMIs). Wenn Sie möchten, dass Amazon Data Lifecycle Manager weiterhin Sicherungen löscht, einschließlich der letzten, müssen Sie Löschen verlängern aktivieren, bevor Sie die Richtlinie löschen oder bevor der Status der Richtlinie zu „Deaktiviert“ oder „Gelöscht“ wechselt.
- Wenn Sie eine Standardrichtlinie erstellen und aktivieren, weist Amazon Data Lifecycle Manager einem Zeitfenster von vier Stunden nach dem Zufallsprinzip zielgerichtete Ressourcen zu. Zielgerichtete Ressourcen werden während des ihnen zugewiesenen Zeitfensters mit der angegebenen Erstellungshäufigkeit gesichert. Wenn eine Richtlinie beispielsweise eine Erstellungshäufigkeit von 3 Tagen umfasst und eine Zielressource dem Fenster von 12:00 bis 16:00 Uhr zugewiesen ist, wird diese Ressource alle 3 Tage zwischen 12:00 und 16:00 Uhr gesichert.

Erstellen Sie eine Standardrichtlinie für Amazon EBS-Snapshots

Das folgende Verfahren zeigt, wie Sie eine Standardrichtlinie für EBS-Snapshots erstellen.

Console

So erstellen Sie eine Standardrichtlinie für EBS-Snapshots

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Lifecycle Manager und dann Lebenszyklusrichtlinie erstellen aus.
3. Wählen Sie als Richtlinientyp die Option Standardrichtlinie und dann EBS-Snapshot-Richtlinie aus.
4. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Richtlinie ein.
5. Wählen Sie für die IAM-Rolle die IAM-Rolle aus, die über Berechtigungen zum Verwalten von Snapshots verfügt.

Wir empfehlen die Auswahl von Standardrolle, um die von Amazon Data Lifecycle Manager bereitgestellte Standard-IAM-Rolle zu verwenden. Sie können jedoch auch eine benutzerdefinierte IAM-Rolle verwenden, die Sie zuvor erstellt haben.

6. Geben Sie unter Erstellungshäufigkeit an, wie oft die Richtlinie ausgeführt werden und Snapshots Ihrer Volumes erstellen soll.

   Die von Ihnen angegebene Häufigkeit bestimmt auch, welche Volumes gesichert werden. Über die Richtlinie werden nur Volumes gesichert, die nicht innerhalb der angegebenen Häufigkeit auf andere Weise gesichert wurden. Wenn Sie beispielsweise eine Erstellungshäufigkeit von 3 Tagen angeben, erstellt die Richtlinie nur Snapshots von Volumes, die in den letzten 3 Tagen nicht gesichert wurden.

7. Geben Sie unter Aufbewahrungsfrist an, wie lange die Richtlinie die von ihr erstellten Snapshots aufbewahren soll. Wenn ein Snapshot den Aufbewahrungs-Schwellenwert erreicht, wird er automatisch gelöscht. Die Aufbewahrungsfrist muss mindestens so groß wie die Erstellungshäufigkeit sein.

8. (Optional) Konfigurieren Sie die Ausschlussparameter, um bestimmte Volumes von den geplanten Sicherungen auszuschließen. Ausgeschlossene Volumes werden nicht gesichert, wenn die Richtlinie ausgeführt wird.

   a. Um Startvolumes auszuschließen, wählen Sie Startvolumes ausschließen. Wenn Sie Startvolumes ausschließen, werden nur Datenvolumes (keine Startvolumes) durch die Richtlinie gesichert. Mit anderen Worten: Es werden keine Snapshots von Volumes erstellt, die als Startvolume an Instances angehängt sind.

   b. Um bestimmte Volume-Typen auszuschließen, wählen Sie Bestimmte Volume-Typen ausschließen und anschließend die auszuschließenden Volume-Typen aus. Nur Volumes der verbleibenden Typen werden durch die Richtlinie gesichert.

   c. Um Volumes mit bestimmten Tags auszuschließen, wählen Sie Tag hinzufügen aus und geben Sie dann die Tag-Schlüssel und -Werte an. Die Richtlinie erstellt keine Snapshots von Volumes, die über eines der angegebenen Tags verfügen.

9. (Optional) Geben Sie in den erweiterten Einstellungen zusätzliche Aktionen an, die die Richtlinie ausführen soll.

   a. Um zugewiesene Tags automatisch vom Quell-Volume auf die Snapshots zu kopieren, wählen Sie Kopieren von Tags aus den Volumes.

   b. Wenn Löschen verlängern deaktiviert ist:

- Wenn eine Quell-Instance gelöscht wird, löscht Amazon Data Lifecycle Manager auf Grundlage des Aufbewahrungszeitraums weiterhin zuvor erstellte Snapshots bis zum letzten Snapshot, jedoch nicht einschließlich dieses Snapshots. Wenn Amazon Data Lifecycle Manager alle Snapshots, einschließlich des letzten, löschen soll, wählen Sie Löschen verlängern.
- Wenn eine Richtlinie gelöscht oder in den Status „`error`“ oder „`disabled`“ versetzt wird, beendet Amazon Data Lifecycle Manager das Löschen von Snapshots. Wenn Amazon Data Lifecycle Manager weiterhin alle Snapshots, einschließlich des letzten, löschen soll, wählen Sie Löschen verlängern aus.

> **Note**
>
> Wenn Sie „Löschen verlängern“ aktivieren, überschreiben Sie beide oben beschriebenen Verhaltensweisen gleichzeitig.

c. Um mit der Richtlinie erstellte Snapshots in andere Regionen zu kopieren, wählen Sie Regionsübergreifende Kopien erstellen und anschließend bis zu 3 Zielregionen aus.

- Wenn der Quell-Snapshot verschlüsselt ist oder die Verschlüsselung standardmäßig für die Zielregion aktiviert ist, werden die Snapshots-Kopien mit dem standardmäßigen KMS-Schlüssel für die EBS-Verschlüsselung in der Zielregion verschlüsselt.
- Wenn der Quell-Snapshot unverschlüsselt ist und die Verschlüsselung standardmäßig für die Zielregion deaktiviert ist, werden die Snapshots-Kopien nicht verschlüsselt.

10. (Optional) Sie können der Richtlinie ein neues Tag hinzufügen, indem Sie Tag hinzufügen auswählen und dann den Tag-Schlüssel und das Wert-Paar angeben.
11. Wählen Sie Standardrichtlinie erstellen.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRole already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

AWS CLI

So erstellen Sie eine Standardrichtlinie für EBS-Snapshots

Verwenden Sie den Befehl create-lifecycle-policy. Sie können die Anfrageparameter je nach Anwendungsfall oder Einstellungen mit einer von zwei Methoden angeben:

- Methode 1

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
 ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
 gp3 | io1 | io2 | st1 | sc1"
```

Um beispielsweise eine Standardrichtlinie für EBS-Snapshots zu erstellen, die auf alle Volumes in der Region abzielt, die Standard-IAM-Rolle verwendet, täglich ausgeführt wird (Standard) und Snapshots 7 Tage lang aufbewahrt (Standard), müssen Sie die folgenden Parameter angeben:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- Methode 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

Wenn `policyDetails.json` Folgendes umfasst:

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceType": "VOLUME",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
  "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Erstellen Sie eine Standardrichtlinie für AMIs EBS-backed

Das folgende Verfahren zeigt Ihnen, wie Sie eine Standardrichtlinie für EBS-backed AMIs erstellen.

Console

So erstellen Sie eine Standardrichtlinie für EBS-backed AMIs

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Lifecycle Manager und dann Lebenszyklusrichtlinie erstellen aus.
3. Wählen Sie als Richtlinientyp die Option Standardrichtlinie und dann EBS-backed AMI-Richtlinie aus.
4. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Richtlinie ein.
5. Wählen Sie für die IAM-Rolle die IAM-Rolle aus, die über Berechtigungen zum Verwalten von AMIs verfügt.

Wir empfehlen die Auswahl von Standardrolle, um die von Amazon Data Lifecycle Manager bereitgestellte Standard-IAM-Rolle zu verwenden. Sie können jedoch auch eine benutzerdefinierte IAM-Rolle verwenden, die Sie zuvor erstellt haben.

6. Geben Sie unter Erstellungshäufigkeit an, wie oft die Richtlinie ausgeführt werden und AMIs aus Ihren Instances erstellen soll.

   Die von Ihnen angegebene Häufigkeit bestimmt auch, welche Instances gesichert werden. Über die Richtlinie werden nur Instances gesichert, die nicht innerhalb der angegebenen Häufigkeit auf andere Weise gesichert wurden. Wenn Sie beispielsweise eine Erstellungshäufigkeit von 3 Tagen angeben, erstellt die Richtlinie nur AMIs von Instances, die in den letzten 3 Tagen nicht gesichert wurden.

7. Geben Sie unter Aufbewahrungsfrist an, wie lange die Richtlinie die von ihr erstellten AMIs beibehalten soll. Wenn ein AMI den Aufbewahrungsschwellenwert erreicht, wird es automatisch abgemeldet und die zugeordneten Snapshots werden gelöscht. Die Aufbewahrungsfrist muss mindestens so groß wie die Erstellungshäufigkeit sein.

8. (Optional) Konfigurieren Sie die Ausschlussparameter, um bestimmte Instances von den geplanten Sicherungen auszuschließen. Ausgeschlossene Instances werden nicht gesichert, wenn die Richtlinie ausgeführt wird.

   - Um Instances mit bestimmten Tags auszuschließen, wählen Sie Tag hinzufügen aus und geben Sie dann die Tag-Schlüssel und -Werte an. Die Richtlinie erstellt keine AMIs aus Instances, die über eines der angegebenen Tags verfügen.

9. (Optional) Geben Sie in den erweiterten Einstellungen zusätzliche Aktionen an, die die Richtlinie ausführen soll.

   a. Um zugewiesene Tags von den Quell-Instances in ihre AMIs zu kopieren, wählen Sie Tags aus Instances kopieren aus.

   b. Wenn Löschen verlängern deaktiviert ist:

      - Wenn eine Quell-Instance beendet wird, meldet Amazon Data Lifecycle Manager auf Grundlage des Aufbewahrungszeitraums weiterhin zuvor erstellte AMIs bis zum letzten AMI ab, jedoch nicht einschließlich dieses AMIs. Wenn Amazon Data Lifecycle Manager alle AMIs, einschließlich des letzten, löschen soll, wählen Sie Löschen verlängern aus.
      - Wenn eine Richtlinie gelöscht oder in den Status „`error`“ oder „`disabled`“ versetzt wird, beendet Amazon Data Lifecycle Manager das Abmelden von AMIs. Wenn

Amazon Data Lifecycle Manager weiterhin alle AMIs, einschließlich des letzten, abmelden soll, wählen Sie Löschen verlängern aus.

> **Note**
>
> Wenn Sie das verlängerte Löschen aktivieren, überschreiben Sie beide oben beschriebenen Verhaltensweisen gleichzeitig.

c. Um mit der Richtlinie erstellte AMIs in andere Regionen zu kopieren, wählen Sie Regionsübergreifende Kopien erstellen und anschließend bis zu 3 Zielregionen aus.

- Wenn das Quell-AMI verschlüsselt ist oder die Verschlüsselung standardmäßig für die Zielregion aktiviert ist, werden die AMI-Kopien mit dem standardmäßigen KMS-Schlüssel für die EBS-Verschlüsselung in der Zielregion verschlüsselt.
- Wenn der Quell-AMI unverschlüsselt ist und die Verschlüsselung standardmäßig für die Zielregion deaktiviert ist, werden die AMI-Kopien nicht verschlüsselt.

10. (Optional) Sie können der Richtlinie ein neues Tag hinzufügen, indem Sie Tag hinzufügen auswählen und dann den Tag-Schlüssel und das Wert-Paar angeben.
11. Wählen Sie Standardrichtlinie erstellen.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

AWS CLI

Um eine Standardrichtlinie für EBS-backed AMIs zu erstellen

Verwenden Sie den Befehl create-lifecycle-policy. Sie können die Anfrageparameter je nach Anwendungsfall oder Einstellungen mit einer von zwei Methoden angeben:

- Methode 1

```
$ aws dlm create-lifecycle-policy \
```

```
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

Um beispielsweise eine Standardrichtlinie für EBS-backed AMIs zu erstellen, die auf alle Instances in der Region abzielt, die Standard-IAM-Rolle verwendet, täglich ausgeführt wird (Standard) und AMIs 7 Tage lang aufbewahrt (Standard), müssen Sie die folgenden Parameter angeben:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- Methode 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

Wenn `policyDetails.json` Folgendes umfasst:

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceType": "INSTANCE",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
```

```
 "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Aktivieren Sie die Data Lifecycle Manager-Standardrichtlinien für alle Konten und Regionen

Mithilfe von CloudFormation StackSets Amazon Data Lifecycle Manager können Sie die Standardrichtlinien von Amazon Data Lifecycle Manager mit einem einzigen Vorgang für mehrere Konten und AWS Regionen aktivieren.

Sie können Stack-Sets verwenden, um Standardrichtlinien auf eine der folgenden Arten zu aktivieren:

- Unternehmensweit — Stellt sicher, dass Standardrichtlinien in der gesamten AWS Organisation oder in bestimmten Organisationseinheiten einer Organisation einheitlich aktiviert und konfiguriert werden. AWS Dies erfolgt mithilfe von vom Dienst verwalteten Berechtigungen. CloudFormation StackSets erstellt die erforderlichen IAM-Rollen in Ihrem Namen.
- AWS Kontenübergreifend — Stellt sicher, dass Standardrichtlinien für bestimmte Zielkonten aktiviert und einheitlich konfiguriert werden. Dies erfordert selbstverwaltete Berechtigungen. Sie erstellen die IAM-Rollen, die erforderlich sind, um die Vertrauensstellung zwischen dem Stack-Set-Administratorkonto und den Zielkonten herzustellen.

Weitere Informationen finden Sie im AWS CloudFormation Benutzerhandbuch unter Berechtigungsmodelle für Stack-Sets.

Verwenden Sie die folgenden Verfahren, um die Standardrichtlinien von Amazon Data Lifecycle Manager für eine gesamte AWS Organisation, für bestimmte Organisationseinheiten oder für bestimmte Zielkonten zu aktivieren.

Voraussetzungen

Führen Sie je nachdem, wie Sie die Standardrichtlinien aktivieren, eine der folgenden Aktionen aus:

- (AWS Organisationsübergreifend) Sie müssen alle Funktionen in Ihrer Organisation aktivieren und den vertrauenswürdigen Zugriff mit aktivieren AWS Organizations. Sie müssen auch das Verwaltungskonto der Organisation oder ein delegiertes Administratorkonto verwenden.
- (Für bestimmte Zielkonten) Sie müssen selbstverwaltete Berechtigungen gewähren, indem Sie die Rollen erstellen, die erforderlich sind, um eine vertrauenswürdige Beziehung zwischen dem Stack-Set-Administratorkonto und den Zielkonten herzustellen.

Console

Um Standardrichtlinien für eine zu aktivieren AWS Organisation oder für bestimmte Zielkonten

1. Öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie im Navigationsbereich StackSets und dann Erstellen aus StackSet.
3. Führen Sie für Berechtigungen einen der folgenden Schritte aus, je nachdem, wie Sie die Standardrichtlinien aktivieren:
   - (In der gesamten AWS Organisation) Wählen Sie Service-managed Berechtigungen aus.
   - (Für bestimmte Zielkonten) Wählen Sie Self-service Berechtigungen aus. Wählen Sie dann für ARN der IAM-Administratorrolle die IAM-Servicerolle aus, die Sie für das Administratorkonto erstellt haben, und geben Sie für den Namen der IAM-Ausführungsrolle den Namen der IAM-Dienstrolle ein, die Sie in den Zielkonten erstellt haben.
4. Wählen Sie für Vorlage vorbereiten die Option Eine Beispielvorlage verwenden aus.
5. Führen Sie für Beispielvorlagen einen der folgenden Schritte aus:
   - (Standardrichtlinie für EBS-Snapshots) Wählen Sie Amazon Data Lifecycle Manager-Standardrichtlinien für EBS-Snapshots erstellen aus.
   - (Standardrichtlinie für EBS-backed AMIs) Wählen Sie Amazon Data Lifecycle Manager-Standardrichtlinien für EBS-backed AMIs erstellen aus.
6. Wählen Sie Weiter aus.
7. Geben Sie für StackSet Name und StackSet Beschreibung einen beschreibenden Namen und eine kurze Beschreibung ein.
8. Konfigurieren Sie im Abschnitt Parameter die standardmäßigen Richtlinieneinstellungen nach Bedarf.

> **Note**
>
> Für kritische Workloads empfehlen wir CreateInterval = 1 Tag und RetainInterval = 7 Tage.

9. Wählen Sie Weiter aus.
10. (Optional) Geben Sie für Tags Tags an, anhand derer Sie die Ressourcen leichter identifizieren StackSet und stapeln können.
11. Wählen Sie für Verwaltete Ausführung die Option Aktiv aus.
12. Wählen Sie Weiter aus.
13. Wählen Sie für Add stacks to stack set (Stacks zum Stack-Set hinzufügen) Deploy new stacks (Neue Stacks bereitstellen).
14. Führen Sie einen der folgenden Schritte aus, je nachdem, wie Sie die Standardrichtlinien aktivieren:

    - (AWS Unternehmensübergreifend) Wählen Sie für Bereitstellungsziele eine der folgenden Optionen aus:
      - Um die Bereitstellung in einer gesamten AWS Organisation durchzuführen, wählen Sie In der Organisation bereitstellen aus.
      - Um die Bereitstellung für bestimmte Organisationseinheiten (OU) durchzuführen, wählen Sie Auf Organisationseinheiten bereitstellen aus, und geben Sie dann für OU-ID die OU-ID ein. Um weitere Organisationseinheiten hinzuzufügen, wählen Sie Weitere Organisationseinheit hinzufügen aus.
    - (Für bestimmte Zielkonten) Führen Sie für Konten einen der folgenden Schritte aus:
      - Um die Bereitstellung für bestimmte Zielkonten durchzuführen, wählen Sie Stapel in Konten bereitstellen aus, und geben Sie dann für Kontonummern die IDs der Zielkonten ein.
      - Um die Bereitstellung für alle Konten in einer bestimmten Organisationseinheit durchzuführen, wählen Sie Stapel für alle Konten in einer Organisationseinheit bereitstellen aus, und geben Sie dann für Organisationsnummern die ID der Ziel-OU ein.
15. Wählen Sie für Automatische Bereitstellung die Option Aktiviert aus.
16. Wählen Sie für das Verhalten beim Entfernen von Konten die Option „Stapel speichern“ aus.

17. Wählen Sie unter Regionen angeben bestimmte Regionen aus, in denen Standardrichtlinien aktiviert werden sollen, oder wählen Sie Alle Regionen hinzufügen, um die Standardrichtlinien in allen Regionen zu aktivieren.
18. Wählen Sie Weiter aus.
19. Überprüfen Sie die Stack-Set-Einstellungen, wählen Sie Ich bestätige, dass CloudFormation möglicherweise IAM-Ressourcen erstellt werden, und klicken Sie dann auf Senden.

AWS CLI

Um Standardrichtlinien für eine zu aktivieren AWS Organisation

1. Erstellen Sie das Stack-Set. Verwenden Sie den Befehl create-stack-set.

   Legen Sie für `--permission-model` die Option `SERVICE_MANAGED` fest.

   Geben Sie für eine `--template-url` der folgenden Vorlagen-URLs an:

   - (Standardrichtlinien für EBS-backed AMIs) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Standardrichtlinien für EBS-Snapshots) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Geben Sie für `--parameters` die Einstellungen für die Standardrichtlinien an. Für unterstützte Parameter, Parameterbeschreibungen und gültige Werte laden Sie die Vorlage mithilfe der URL herunter und sehen Sie sich die Vorlage dann mit einem Texteditor an.

   Legen Sie für `--auto-deployment` die Option `Enabled=true, RetainStacksOnAccountRemoval=true` fest.

   ```
   $ aws cloudformation create-stack-set \
   --stack-set-name stackset_name \
   --permission-model SERVICE_MANAGED \
   --template-url template_url \
   --parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
    "ParameterKey=param_name_2,ParameterValue=param_value_2" \
   --auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
   ```

2. Stellen Sie das Stack-Set bereit. Verwenden Sie den Befehl create-stack-instances.

   Geben Sie für den Namen des Stack-Sets an`--stack-set-name`, das Sie im vorherigen Schritt erstellt haben.

   Geben Sie `--deployment-targets OrganizationalUnitIds` beispielsweise die ID der Stamm-Organisationseinheit an, die für eine gesamte Organisation bereitgestellt werden soll, oder die OU-IDs, die für bestimmte Organisationseinheiten in der Organisation bereitgestellt werden sollen.

   Geben Sie für `--regions` die AWS Regionen an, in denen die Standardrichtlinien aktiviert werden sollen.

   ```
   $ aws cloudformation create-stack-instances \
   --stack-set-name stackset_name \
   --deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",
    "ou_id_2]' \
   --regions '["region_1", "region_2"]'
   ```

Um Standardrichtlinien für bestimmte Zielkonten zu aktivieren

1. Erstellen Sie das Stack-Set. Verwenden Sie den Befehl create-stack-set.

   Geben Sie für eine `--template-url` der folgenden Vorlagen-URLs an:

   - (Standardrichtlinien für EBS-backed AMIs) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Standardrichtlinien für EBS-Snapshots) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Geben Sie für `--administration-role-arn` den ARN der IAM-Servicerolle an, die Sie zuvor für den Stack-Set-Administrator erstellt haben.

   Geben Sie für `--execution-role-name` den Namen der IAM-Servicerolle an, die Sie in den Zielkonten erstellt haben.

Geben Sie für `--parameters` die Einstellungen für die Standardrichtlinien an. Für unterstützte Parameter, Parameterbeschreibungen und gültige Werte laden Sie die Vorlage mithilfe der URL herunter und sehen Sie sich die Vorlage dann mit einem Texteditor an.

Legen Sie für `--auto-deployment` die Option `Enabled=true, RetainStacksOnAccountRemoval=true` fest.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Stellen Sie das Stack-Set bereit. Verwenden Sie den Befehl create-stack-instances.

   Geben Sie für den Namen des Stack-Sets an`--stack-set-name`, das Sie im vorherigen Schritt erstellt haben.

   Geben Sie für `--accounts` die IDs der AWS Zielkonten an.

   Geben Sie für `--regions` die AWS Regionen an, in denen die Standardrichtlinien aktiviert werden sollen.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

Erstellen Sie eine benutzerdefinierte Amazon Data Lifecycle Manager-Richtlinie für EBS-Snapshots

Das folgende Verfahren zeigt, wie Sie Amazon Data Lifecycle Manager verwenden, um Amazon-EBS-Snapshot-Lebenszyklen zu automatisieren.

Themen

- Erstellen einer Snapshot-Lebenszyklusrichtlinie
- Überlegungen zu Snapshot-Lebenszyklusrichtlinien
- Weitere Ressourcen
- Automatisieren Sie anwendungskonsistente Snapshots mit Data Lifecycle Manager
- Andere Anwendungsfälle für Data Lifecycle Manager: Pre- und Post-Skripts
- So funktionieren Pre- und Post-Skripts von Amazon Data Lifecycle Manager
- Identifizieren Sie Snapshots, die mit den Pre- und Post-Skripten von Data Lifecycle Manager erstellt wurden
- Überwachen Sie Amazon Data Lifecycle Manager vor und nach den Skripten

Erstellen einer Snapshot-Lebenszyklusrichtlinie

Verwenden Sie eines der folgenden Verfahren, um eine Snapshot-Lebenszyklusrichtlinie zu erstellen.

Console

So erstellen Sie eine Snapshot-Richtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store und Lifecycle Manager aus. Wählen Sie dann Create lifecycle policy (Lebenszyklusrichtlinie erstellen) aus.
3. Wählen Sie auf dem Bildschirm Richtlinientyp auswählen die Option EBS-Snapshot-Richtlinie und dann Weiter aus.
4. Gehen Sie im Abschnitt Zielressourcen wie folgt vor:

   a. Wählen Sie für Zielressourcentypen den Typ der zu sichernden Ressource aus. Wählen Sie `Volume`, um Snapshots einzelner Volumes zu erstellen oder `Instance`, um Snapshots mit mehreren Volumes aus den Volumes zu erstellen, die an eine Instance angefügt sind.

   b. (Outpostund nur für Local Zone-Kunden) Geben Sie an, wo sich die Zielressourcen befinden.

      Geben Sie unter Zielressourcenspeicherort an, wo sich die Zielressourcen befinden.

      - Um Ressourcen in einer Region anzuvisieren, wählen Sie AWS Region. Amazon Data Lifecycle Manager sichert nur in der aktuellen Region alle Ressourcen des

angegebenen Typs, die über übereinstimmende Ziel-Tags verfügen. Snapshots werden in derselben Region erstellt.

- Um auf Ressourcen in lokalen Zonen abzuzielen, wählen Sie AWS Lokale Zonen aus. Amazon Data Lifecycle Manager sichert alle Ressourcen des angegebenen Typs, die über übereinstimmende Ziel-Tags für alle lokalen Zonen in der aktuellen Region verfügen. Snapshots können in derselben lokalen Zone wie die Quellressource oder in der übergeordneten Region erstellt werden.
- Um Ressourcen als Ziel zu verwendenOutpost, wählen Sie AWS Outpost. Amazon Data Lifecycle Manager erstellt eine Sicherungskopie aller Ressourcen des angegebenen Typs, für die alle Ressourcen Outposts in Ihrem Konto dieselben Ziel-Tags aufweisen. Snapshots können auf derselben Ressource Outpost wie die Quellressource oder in der übergeordneten Region erstellt werden.

c. Wählen Sie für Zielressourcen-Tags die Ressourcen-Tags aus, die die zu sichernden Volumes oder Instances identifizieren. Nur Ressourcen, die die angegebenen Tag (Markierung)-Schlüssel- und Wertepaare haben, werden von der Richtlinie gesichert.

5. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Richtlinie ein.
6. Wählen Sie für IAM-Rolle die IAM-Rolle aus, die über Berechtigungen zum Verwalten von Snapshots und zum Beschreiben von Volumes und Instances verfügt. Um die von Amazon Data Lifecycle Manager bereitgestellte Standardrolle zu verwenden, wählen Sie Standardrolle. Um alternativ eine benutzerdefinierte IAM-Rolle zu verwenden, die Sie zuvor erstellt haben, wählen Sie Andere Rolle auswählen und dann die zu verwendende Rolle aus.
7. Fügen Sie für Richtlinien-Tags die Tags hinzu, die auf die Lebenszyklusrichtlinie angewendet werden sollen. Sie können diese Tags (Markierungen) verwenden, um Ihre Richtlinien zu identifizieren und zu kategorisieren.
8. Wählen Sie für Policy status (Richtlinienstatus) die Option Enable (Aktivieren) aus, um die Ausführung der Richtlinie zum nächsten geplanten Zeitpunkt zu starten oder Disable policy (Richtlinie deaktivieren), um die Ausführung der Richtlinie zu verhindern. Wenn Sie die Richtlinie jetzt nicht aktivieren, beginnt sie erst mit der Erstellung von Snapshots, wenn Sie sie nach der Erstellung manuell aktivieren.
9. (Richtlinien, die nur auf Instances abzielen) Schließen Sie Volumes aus Snapshot-Sets mit mehreren Volumes aus.

   Standardmäßig erstellt Amazon Data Lifecycle Manager Snapshots aller Volumes, die an die Ziel-Instances angefügt sind. Sie können jedoch Snapshots einer Teilmenge der

angehängten Volumes erstellen. Gehen Sie im Abschnitt Parameters (Parameter) wie folgt vor:

- Wenn Sie keine Snapshots der Root-Volumes erstellen möchten, die den Ziel-Instances angefügt sind, wählen Sie Exclude root volume (Root-Volume ausschließen). Wenn Sie diese Option wählen, werden nur die Datenvolumes (Nicht-Root), die an die Ziel-Instances angefügt sind, in die Multi-Volume-Snapshot-Sets aufgenommen.
- Wenn Sie Snapshots von einer Teilmenge der Daten-Volumes (Nicht-Root) erstellen möchten, die an die anvisierten Instances angefügt sind, wählen Sie Exclude specific data volumes (Bestimmte Daten-Volumes ausschließen) und geben Sie dann die Tags an, die verwendet werden sollen, um die Daten-Volumes zu identifizieren, die nicht in den Snapshot aufgenommen werden sollen. Amazon Data Lifecycle Manager erstellt keine Snapshots von Daten-Volumes, die über eines der angegebenen Tags verfügen. Amazon Data Lifecycle Manager erstellt nur Snapshots von Daten-Volumes, die keines der angegebenen Tags haben.

10. Wählen Sie Weiter aus.
11. Konfigurieren Sie auf dem Bildschirm Zeitplan konfigurieren die Richtlinienzeitpläne. Eine Richtlinie kann bis zu 4 Zeitpläne aufweisen. Zeitplan 1 ist obligatorisch. Die Zeitpläne 2, 3 und 4 sind optional. Gehen Sie für jeden Richtlinienzeitplan, den Sie hinzufügen, wie folgt vor:

    a. Gehen Sie im Abschnitt Zeitplandetails wie folgt vor:

        i. Geben Sie für Zeitplanname einen beschreibenden Namen für den Zeitplan an.

        ii. Konfigurieren Sie für Häufigkeit und die zugehörigen Felder das Intervall zwischen Richtlinienausführungen.

        Sie können Richtlinienausführungen nach einem täglichen, wöchentlichen, monatlichen oder jährlichen Zeitplan konfigurieren. Alternativ können Sie Custom cron expression (Benutzerdefinierter Cron-Ausdruck) wählen, um ein Intervall von bis zu 1 Jahr anzugeben. Weitere Informationen finden Sie unter Cron- und Rate-Ausdrücke im EventBridge Amazon-Benutzerhandbuch.

        > **Note**
        >
        > Wenn Sie die Snapshot-Archivierung für den Zeitplan aktivieren müssen, müssen Sie als Häufigkeit monthly (monatlich) oder yearly (jährlich)

auswählen oder einen Cron-Ausdruck mit einer Erstellungshäufigkeit von mindestens 28 Tagen angeben.
Wenn Sie eine monatliche Häufigkeit angeben, mit der Snapshots an einem bestimmten Tag in einer bestimmten Woche erstellt werden (z. B. am zweiten Donnerstag des Monats), muss für einen anzahlbasierten Zeitplan die Aufbewahrungsanzahl für die Archivstufe mindestens 4 betragen.

iii. Geben Sie für Starten um die Uhrzeit an, zu der die Richtlinienausführungen für den Start geplant sind. Die erste Richtlinienausführung beginnt innerhalb einer Stunde nach der geplanten Zeit. Die Uhrzeit muss im `hh:mm` UTC-Format eingegeben werden.

iv. Geben Sie für Aufbewahrungstyp die Aufbewahrungsrichtlinie für Schnappschüsse an, die vom Zeitplan erstellt wurden.

Sie können Snapshots basierend auf ihrer Gesamtzahl oder ihrem Alter aufbewahren.

- Count-based Aufbewahrung
  - Wenn die Snapshot-Archivierung deaktiviert ist, reicht der Bereich von 1 bis `1000`. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot dauerhaft gelöscht.
  - Bei aktivierter Snapshot-Archivierung reicht der Bereich von `0` (Archivierung sofort nach Erstellung) bis `1000`. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot in einen vollständigen Snapshot umgewandelt und in die Archivebene verschoben.
- Age-based Beibehaltung
  - Wenn die Snapshot-Archivierung deaktiviert ist, reicht der Bereich von 1 Tagen bis `100` Jahren. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot dauerhaft gelöscht.
  - Bei aktivierter Snapshot-Archivierung reicht der Bereich von `0` Tagen (Archivierung sofort nach Erstellung) bis `100` Jahren. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot in einen vollständigen Snapshot umgewandelt und in die Archivebene verschoben.

> **Note**
>
> - Alle Zeitpläne müssen denselben Aufbewahrungstyp aufweisen (alters- oder anzahlbasiert). Sie können den Aufbewahrungstyp nur für Zeitplan 1 angeben. Die Zeitpläne 2, 3 und 4 erben den Aufbewahrungstyp aus Plan 1. Jeder Zeitplan kann über eine eigene Aufbewahrungsanzahl oder einen eigenen Zeitraum verfügen.
> - Wenn Sie die schnelle Snapshot-Wiederherstellung, das regionsübergreifende Kopieren oder die Snapshot-Freigabe aktivieren, müssen Sie eine Aufbewahrungsanzahl von mindestens 1 oder einen Aufbewahrungszeitraum von mindestens 1 Tag angeben.

v. (AWS Outposts und nur für Local Zone-Kunden) Geben Sie das Snapshot-Ziel an.

Geben Sie unter Snapshot-Ziel das Ziel für Snapshots an, die von der Richtlinie erstellt wurden.

- Wenn die Richtlinie auf Ressourcen in einer Region abzielt, müssen Snapshots in derselben Region erstellt werden. AWS Die Region ist für Sie ausgewählt.
- Wenn die Richtlinie auf Ressourcen in einer lokalen Zone abzielt, können Sie Snapshots in derselben lokalen Zone wie die Quellressource oder in der übergeordneten Region erstellen.
- Wenn die Richtlinie auf Ressourcen in einer abzieltOutpost, können Sie Snapshots auf derselben Ressource Outpost wie die Quellressource oder in der übergeordneten Region erstellen.

b. Konfigurieren Sie das Markieren von Snapshots.

Gehen Sie im Abschnitt Tag (Markierung) wie folgt vor:

i. Um alle benutzerdefinierten Tags vom Quell-Volume in die vom Zeitplan erstellten Schnappschüsse zu kopieren, wählen Sie Tags aus Quelle kopieren.

ii. Um zusätzliche Tags (Markierungen) anzugeben, die Snapshots zugewiesen werden sollen, die von diesem Zeitplan erstellt wurden, wählen Sie Tags (Markierungen) hinzufügen.

c. Konfigurieren Sie Vor- und Nach-Skripte für anwendungskonsistente Snapshots.

Weitere Informationen finden Sie unter Automatisieren Sie anwendungskonsistente Snapshots mit Data Lifecycle Manager.

d. (Richtlinien, die nur auf Volumes abzielen) Konfigurieren Sie die Snapshot-Archivierung.

Gehen Sie im Abschnitt Snapshot-Archivierung wie folgt vor:

> **Note**
>
> Die Snapshot-Archivierung lässt sich nur für einen Zeitplan in einer Richtlinie aktivieren.

i. Zum Aktivieren der Snapshot-Archivierung für den Zeitplan wählen Sie Archive snapshots created by this schedule (Mit diesem Zeitplan erstellte Snapshots archivieren) aus.

> **Note**
>
> Die Snapshot-Archivierung lässt sich nur aktivieren, wenn Snapshots monatlich oder jährlich erstellt werden oder wenn Sie einen Cron-Ausdruck mit einer Erstellungshäufigkeit von mindestens 28 Tagen angeben.

ii. Geben Sie die Aufbewahrungsregel für Snapshots auf der Archivstufe an.

- Geben Sie für anzahlbasierte Zeitpläne die Anzahl der Snapshots an, die auf der Archivstufe aufbewahrt werden sollen. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot dauerhaft aus der Archivstufe gelöscht. Wenn Sie beispielsweise drei angeben, behält der Zeitplan maximal drei Snapshots auf der Archivstufe bei. Bei Archivierung des vierten Snapshots wird der älteste der drei vorhandenen Snapshots auf der Archivstufe gelöscht.
- Geben Sie für altersbasierte Zeitpläne den Zeitraum an, für den Snapshots auf der Archivstufe aufbewahrt werden sollen. Wenn der Aufbewahrungsschwellenwert erreicht ist, wird der älteste Snapshot dauerhaft aus der Archivstufe gelöscht. Wenn Sie beispielsweise 120 Tage angeben, werden Snapshots automatisch aus der Archivstufe gelöscht, wenn sie dieses Alter erreicht haben.

> **Important**
>
> Der Mindestaufbewahrungszeitraum für archivierte Snapshots beträgt 90 Tage. Sie müssen eine Aufbewahrungsregel angeben, die den Snapshot mindestens 90 Tage lang aufbewahrt.

e. Aktivieren Sie die schnelle Snapshot-Wiederherstellung.

Um die schnelle Snapshot-Wiederherstellung für vom Zeitplan erstellte Snapshots zu aktivieren, wählen Sie im Abschnitt Schnelle Snapshot-Wiederherstellung die Option Schnelle Snapshot-Wiederherstellung aktivieren aus. Wenn Sie die schnelle Snapshot-Wiederherstellung aktivieren, müssen Sie die Availability Zones auswählen, in denen sie aktiviert werden soll. Wenn der Zeitplan einen altersbasierten Aufbewahrungszeitplan verwendet, müssen Sie den Zeitraum angeben, für den die schnelle Snapshot-Wiederherstellung für jeden Snapshot aktiviert werden soll. Wenn der Zeitplan eine zahlbasierte Aufbewahrung verwendet, müssen Sie die maximale Anzahl von Snapshots angeben, um die schnelle Snapshot-Wiederherstellung zu aktivieren.

Wenn der Zeitplan Snapshots auf einer erstelltOutpost, können Sie die schnelle Snapshot-Wiederherstellung nicht aktivieren. Die schnelle Snapshot-Wiederherstellung wird bei lokalen Snapshots, die auf einem gespeichert sind, nicht unterstützt. Outpost

> **Note**
>
> Es wird Ihnen jede Minute in Rechnung gestellt, in der die schnelle Snapshot-Wiederherstellung für einen Snapshot in einer bestimmten Availability Zone aktiviert ist. Die Gebühren werden mit mindestens einer Stunde anteilig bewertet.

f. Konfigurieren Sie das regionsübergreifende Kopieren.

Um im Zeitplan erstellte Snapshots in eine Outpost oder eine andere Region zu kopieren, wählen Sie im Abschnitt Cross-Region Kopieren die Option Regionsübergreifendes Kopieren aktivieren aus.

Wenn der Zeitplan Snapshots in einer Region erstellt, können Sie die Snapshots in bis zu drei weitere Regionen oder Outposts in Ihr Konto kopieren. Sie müssen für jede Zielregion oder eine separate regionsübergreifende Kopierregel angeben. Outpost

Für jede Region oder Outpost können Sie unterschiedliche Aufbewahrungsrichtlinien auswählen und wählen, ob alle Tags oder keine Tags kopiert werden sollen. Wenn der Quell-Snapshot verschlüsselt ist oder wenn die Verschlüsselung standardmäßig aktiviert ist, werden die Snapshots-Kopien verschlüsselt. Wenn der Quell-Snapshot unverschlüsselt ist, können Sie die Verschlüsselung aktivieren. Wenn Sie keinen Verschlüsselung angeben, werden die Snapshots mit der Standard-Verschlüsselung für die EBS-Verschlüsselung in jeder Zielregion verschlüsselt. Wenn Sie einen Verschlüsselung für die Zielregion angeben, muss die ausgewählte IAM-Rolle Zugriff auf das Verschlüsselung haben.

> **Note**
>
> Sie müssen sicherstellen, dass Sie die Anzahl der gleichzeitigen Snapshot-Kopien pro Region nicht überschreiten.

Wenn die Richtlinie Snapshots auf einer erstelltOutpost, können Sie die Snapshots nicht in eine oder andere Region kopieren Outpost und die Einstellungen für regionsübergreifendes Kopieren sind nicht verfügbar.

g. Konfigurieren Sie die kontoübergreifende gemeinsame Nutzung.

   Konfigurieren Sie beim Cross-account Teilen die Richtlinie so, dass die im Zeitplan erstellten Snapshots automatisch für andere Konten freigegeben werden. AWS Gehen Sie wie folgt vor:

   i. Um das Teilen mit anderen AWS Konten zu aktivieren, wählen Sie Kontoübergreifendes Teilen aktivieren aus.

   ii. Um die Konten hinzuzufügen, mit denen die Schnappschüsse geteilt werden sollen, wählen Sie Konto hinzufügen, geben Sie die 12-stellige AWS -Konto-ID ein und wählen Sie Hinzufügen.

   iii. Um die Freigabe freigegebener Snapshots nach einem bestimmten Zeitraum automatisch aufzuheben, wählen Sie Unshare automatically (Freigabe automatisch aufheben). Wenn Sie sich dafür entschieden haben, die Freigabe freigegebener Snapshots automatisch aufzuheben, kann der Zeitraum, nach dem die Snapshots automatisch aufgegeben werden, nicht länger sein als der Zeitraum, in dem die Richtlinie ihre Snapshots aufbewahrt. Wenn die Aufbewahrungskonfiguration der

Richtlinie beispielsweise Snapshots für einen Zeitraum von 5 Tagen aufbewahrt, können Sie die Richtlinie nur so konfigurieren, dass freigegebene Snapshots automatisch nach Zeiträumen von bis zu 4 Tagen freigegeben werden. Dies gilt für Richtlinien mit alters- und anzahlbasierten Snapshot-Aufbewahrungskonfigurationen.

Wenn Sie die automatische Freigabe nicht aktivieren, wird der Snapshot freigegeben, bis er gelöscht wird.

> **Note**
>
> Sie können nur Snapshots freigeben, die unverschlüsselt oder mit einem Kundenverwalteter Schlüssel verschlüsselt sind. Sie können keine Snapshots freigeben, die mit dem standardmäßigen EBS-Verschlüsselungs-Verschlüsselung verschlüsselt sind. Wenn Sie verschlüsselte Snapshots teilen, müssen Sie auch den Verschlüsselung, der zum Verschlüsseln des Quell-Volumes verwendet wurde, mit den Zielkonten teilen. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch.

h. Um weitere Zeitpläne hinzuzufügen, wählen Sie die Option Weiteren Zeitplan hinzufügen, die sich oben auf dem Bildschirm befindet. Füllen Sie für jeden zusätzlichen Zeitplan die Felder wie oben in diesem Thema beschrieben aus.

i. Nachdem Sie die erforderlichen Zeitpläne hinzugefügt haben, wählen Sie Richtlinie überprüfen aus.

12. Überprüfen Sie die Richtlinienzusammenfassung und wählen Sie dann Richtlinie erstellen aus.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRole already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

Command line

Verwenden Sie den Befehl create-lifecycle-policy, um eine Snapshot-Lebenszyklus-Richtlinie zu erstellen. Legen Sie für `PolicyType` die Option `EBS_SNAPSHOT_MANAGEMENT` fest.

> **Note**
>
> Zur Vereinfachung der Syntax wird in den folgenden Beispielen eine JSON-Datei `policyDetails.json` verwendet, die die Richtliniendetails enthält.

Beispiel 1 – Snapshot-Lebenszyklusrichtlinie mit zwei Zeitplänen

In diesem Beispiel wird eine Snapshot-Lebenszyklusrichtlinie erstellt, die Snapshots aller Volumes erstellt, die einen Tag (Markierung)-Schlüssel `costcenter` mit dem Wert von 115 haben. Die Richtlinie enthält zwei Zeitpläne. Der erste Zeitplan erstellt jeden Tag um 03:00 Uhr UTC einen Snapshot. Der zweite Zeitplan erstellt jeden Freitag um 17:00 Uhr UTC einen wöchentlichen Snapshot.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
```

```
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Wenn die Anforderung erfolgreich ist, gibt der Befehl die ID der neu erstellten Richtlinie zurück. Es folgt eine Beispielausgabe.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Beispiel 2 – Snapshot-Lebenszyklusrichtlinie, die auf Instances abzielt und Snapshots einer Untergruppe von Datenvolumes (Nicht-Root) erstellt

In diesem Beispiel wird eine Snapshot-Lebenszyklusrichtlinie erstellt, die Multi-Volume-Snapshot-Sets aus Instaces erstellt, die mit `code=production` gekennzeichnet sind. Die Richtlinie

enthält nur einen Zeitplan. Der Zeitplan erstellt keine Snapshots von den Daten-Volumes, die mit `code=temp` gekennzeichnet sind.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
```

```
        "CopyTags": false
    }
]}
```

Wenn die Anforderung erfolgreich ist, gibt der Befehl die ID der neu erstellten Richtlinie zurück. Es folgt eine Beispielausgabe.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Beispiel 3 — Snapshot-Lebenszyklusrichtlinie, die lokale Snapshots von automatisiert Outpost Ressourcen

In diesem Beispiel wird eine Snapshot-Lebenszyklusrichtlinie erstellt, die Snapshots von Volumes erstellt, die mit `team=dev` all Ihren markiert sind. Outposts Die Richtlinie erstellt die Snapshots auf denselben Volumes Outposts wie die Quell-Volumes. Die Richtlinie erstellt alle 12 Stunden Snapshots bei `00:00` UTC.

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CreateRule": {
            "Interval": 12,
```

```
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
        },
        "CopyTags": false
    }
]}
```

Beispiel 4 — Snapshot-Lebenszyklusrichtlinie, die Snapshots in einer Region erstellt und sie in eine kopiert Outpost

Die folgende Beispielrichtlinie erstellt Snapshots von Volumes, die mit `team=dev` markiert sind. Die Snapshots werden in der gleichen Region erstellt wie das Quell-Volume. Snapshots werden alle 12 Stunden bei `00:00` UTC erstellt und bewahren ein Maximum an Snapshots von 1. Die Richtlinie kopiert auch die Snapshots Outpost`arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`, verschlüsselt die kopierten Snapshots mit dem KMS-Standardschlüssel für die Verschlüsselung und bewahrt die Kopien einen Monat lang auf. 1

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
```

```
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

Beispiel 5 – Snapshot-Lebenszyklusrichtlinie mit einem archivfähigen, altersbasierten Zeitplan

In diesem Beispiel wird eine Snapshot-Lebenszyklusrichtlinie erstellt, die für mit `Name=Prod` markierte Volumes gilt. Die Richtlinie hat einen altersbasierten Zeitplan, der Snapshots am ersten Tag eines jeden Monats um 09.00 Uhr erstellt. Der Zeitplan bewahrt alle Snapshots auf der Standardstufe einen Tag lang auf. Danach werden sie in die Archivstufe verschoben. Snapshots werden 90 Tage lang auf der Archivstufe gespeichert, bevor sie gelöscht werden.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
```

```
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

Beispiel 6 – Snapshot-Lebenszyklusrichtlinie mit einem archivfähigen, anzahlbasierten Zeitplan

In diesem Beispiel wird eine Snapshot-Lebenszyklusrichtlinie erstellt, die für mit `Purpose=Test` markierte Volumes gilt. Die Richtlinie hat einen anzahlbasierten Zeitplan, der Snapshots

am ersten Tag eines jeden Monats um 09.00 Uhr erstellt. Der Zeitplan archiviert Snapshots unmittelbar nach der Erstellung und bewahrt maximal drei Snapshots auf der Archivstufe auf.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
```

```
}
```

Überlegungen zu Snapshot-Lebenszyklusrichtlinien

Die folgenden allgemeinen Überlegungen gelten für Snapshot-Lebenszyklusrichtlinien:

- Snapshot-Lebenszyklusrichtlinien zielen nur auf Instances oder Volumes ab, die sich in derselben Region wie die Richtlinie befinden.
- Der erste Snapshot-Erstellungsvorgang beginnt innerhalb einer Stunde nach der angegebenen Startzeit. Nachfolgende Snapshot-Erstellungsvorgänge beginnen innerhalb einer Stunde nach ihrer geplanten Zeit.
- Sie können mehrere Richtlinien zum Sichern eines Volumes oder einer Instance erstellen. Wenn ein Volume zwei Tags hat, wobei Tag A das Ziel für Richtlinie A ist, alle 12 Stunden einen Snapshot zu erstellen, und Tag B das Ziel für Richtlinie B, alle 24 Stunden einen Snapshot zu erstellen, erstellt Amazon Data Lifecycle Manager Snapshots gemäß den Zeitplänen für beide Richtlinien. Alternativ können Sie dasselbe Ergebnis erzielen, indem Sie eine einzelne Richtlinie mit mehreren Zeitplänen erstellen. Sie können beispielsweise eine einzelne Richtlinie erstellen, die nur auf Tag (Markierung) Aabzielt, und zwei Zeitpläne angeben – einen für alle 12 Stunden und einen für alle 24 Stunden.
- Bei Zielressourcen-Tags muss die Groß-/Kleinschreibung beachtet werden.
- Wenn Sie die Ziel-Tags von einer Ressource entfernen, auf die eine Richtlinie abzielt, verwaltet Amazon Data Lifecycle Manager die vorhandenen Snapshots im Standard-Tier und Archiv-Tier nicht mehr; Sie müssen sie manuell löschen, wenn sie nicht mehr benötigt werden.
- Wenn Sie eine Richtlinie erstellen, die auf Instances abzielt, und neue Volumes an die Ziel-Instance angefügt werden, nachdem die Richtlinie erstellt wurde, werden die neu hinzugefügten Volumes bei der nächsten Richtlinienausführung in das Backup einbezogen. Alle Volumes, die zum Zeitpunkt der Richtlinienausführung mit der Instance verbunden sind, sind enthalten.
- Wenn Sie eine Richtlinie mit einem benutzerdefinierten Cron-basierten Zeitplan so erstellen und konfigurieren, dass nur ein Snapshot erstellt wird, wird die Richtlinie diesen Snapshot nicht automatisch löschen, wenn der Aufbewahrungsschwellenwert erreicht ist. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr länger benötigt wird.
- Wenn Sie eine altersbasierte Richtlinie erstellen, bei der der Aufbewahrungszeitraum kürzer ist als die Erstellungshäufigkeit, behält Amazon Data Lifecycle Manager immer den letzten Snapshot bei, bis der nächste erstellt wird. Wenn zum Beispiel eine altersbasierte Richtlinie jeden Monat einen Snapshot mit einer Aufbewahrungsfrist von sieben Tagen erstellt, behält Amazon Data

Lifecycle Manager jeden Snapshot einen Monat lang bei, obwohl die Aufbewahrungsfrist sieben Tage beträgt.

Die folgenden Überlegungen beziehen sich auf die Snapshot-Archivierung:

- Die Snapshot-Archivierung lässt sich nur für Snapshot-Richtlinien aktivieren, die für Volumes gelten.
- Pro Richtlinie können Sie nur eine Archivierungsregel für einen Zeitplan angeben.
- Bei Verwendung der Konsole lässt sich die Snapshot-Archivierung nur aktivieren, wenn der Zeitplan eine monatliche oder jährliche Erstellungshäufigkeit oder einen Cron-Ausdruck mit einer Erstellungshäufigkeit von mindestens 28 Tagen aufweist.

  Wenn Sie die AWS API oder das AWS SDK verwenden AWS CLI, können Sie die Snapshot-Archivierung nur aktivieren, wenn der Zeitplan einen Cron-Ausdruck mit einer Erstellungshäufigkeit von mindestens 28 Tagen enthält.
- Der Mindestaufbewahrungszeitraum auf der Archivstufe beträgt 90 Tage.
- Wenn ein Snapshot archiviert wird, wird er beim Verschieben in die Archivstufe in einen vollständigen Snapshot konvertiert. Dies kann zu höheren Kosten für die Snapshot-Speicherung führen. Weitere Informationen finden Sie unter Preise und Abrechnung für die Archivierung von Amazon EBS-Snapshots.
- Die schnelle Snapshot-Wiederherstellung und die Snapshot-Freigabe werden für Snapshots deaktiviert, wenn sie archiviert werden.
- Wenn Ihre Aufbewahrungsregel in einem Schaltjahr zu einem Archivierungszeitraum von weniger als 90 Tagen führt, stellt Amazon Data Lifecycle Manager sicher, dass Snapshots mindestens 90 Tage lang aufbewahrt werden.
- Wenn Sie einen von Amazon Data Lifecycle Manager erstellten Snapshot manuell archivieren und der Snapshot bei Erreichen des Aufbewahrungsschwellenwerts des Zeitplans immer noch archiviert ist, wird dieser Snapshot nicht mehr von Amazon Data Lifecycle Manager verwaltet. Wenn Sie den Snapshot jedoch vor Erreichen des Aufbewahrungsschwellenwerts des Zeitplans wieder in die Standardstufe verschieben, wird er vom Zeitplan weiterhin gemäß den Aufbewahrungsregeln verwaltet.
- Wenn Sie einen von Amazon Data Lifecycle Manager archivierten Snapshot dauerhaft oder temporär wieder in die Standardstufe verschieben und der Snapshot sich bei Erreichen des Aufbewahrungsschwellenwerts des Zeitplans immer noch auf der Standardstufe befindet, wird dieser Snapshot nicht mehr von Amazon Data Lifecycle Manager verwaltet. Wenn Sie

den Snapshot jedoch vor Erreichen des Aufbewahrungsschwellenwerts des Zeitplans erneut archivieren, wird er vom Zeitplan gelöscht, sobald der Aufbewahrungsschwellenwert erreicht ist.

- Von Amazon Data Lifecycle Manager archivierte Snapshots werden auf Ihre `Archived snapshots per volume-` und `In-progress snapshot archives per account-` Kontingente angerechnet.
- Wenn ein Zeitplan einen Snapshot nicht archivieren kann, nachdem dies 24 Stunden lang immer wieder versucht wurde, verbleibt der Snapshot auf der Standardstufe. Seine Löschung wird dann zu dem Zeitpunkt geplant, zu dem er aus der Archivstufe gelöscht worden wäre. Wenn der Zeitplan Snapshots beispielsweise 120 Tage lang archiviert, bleibt der Snapshot nach der fehlgeschlagenen Archivierung 120 Tage lang auf der Standardstufe, bevor er endgültig gelöscht wird. Bei anzahlbasierten Zeitplänen wird der Snapshot nicht auf die Aufbewahrungsanzahl des Zeitplans angerechnet.
- Snapshots müssen in derselben Region archiviert werden, in der sie erstellt wurden. Wenn Sie das regionsübergreifende Kopieren und die Snapshot-Archivierung aktiviert haben, wird die Snapshot-Kopie von Amazon Data Lifecycle Manager nicht archiviert.
- Von Amazon Data Lifecycle Manager archivierte Snapshots werden mit dem System-Tag `aws:dlm:archived=true` markiert. Darüber hinaus werden Snapshots, die nach einem für die Archivierung aktivierten, altersbasierten Zeitplan erstellt wurden, mit dem System-Tag `aws:dlm:expirationTime` markiert, das das Datum und die Uhrzeit für die geplante Archivierung des Snapshots angibt.

Die folgenden Überlegungen gelten für das Ausschließen von Root-Volumes und Daten-Volumes (Nicht-Root):

- Wenn Sie Startvolumes ausschließen und Tags angeben, die folglich alle zusätzlichen Datenvolumes ausschließen, die an eine Instance angehängt sind, erstellt Amazon Data Lifecycle Manager keine Snapshots für die betroffene Instance und gibt eine `SnapshotsCreateFailed` CloudWatch Metrik aus. Weitere Informationen finden Sie unter Überwachen Sie Richtlinien mithilfe von CloudWatch.

Die folgenden Überlegungen gelten für das Löschen von Volumes oder das Beenden von Instances, die von Snapshot-Lebenszyklus-Richtlinien betroffen sind:

- Wenn Sie ein Volume löschen oder eine Instance beenden, für das oder die eine Richtlinie mit einem anzahlbasierten Aufbewahrungszeitplan gilt, werden die Snapshots auf der Standard- und Archivstufe, die von dem gelöschten Volume oder der beendeten Instance erstellt wurden,

nicht mehr von Amazon Data Lifecycle Manager verwaltet. Sie müssen diese früheren Snapshots manuell löschen, wenn sie nicht mehr benötigt werden.

- Wenn Sie ein Volume löschen oder eine Instance beenden, für das oder die eine Richtlinie mit einem altersbasierten Aufbewahrungszeitplan gilt, werden die Snapshots, die von dem gelöschten Volume oder der beendeten Instance erstellt wurden, von der Richtlinie weiterhin nach dem definierten Zeitplan gelöscht, und zwar bis zum letzten Snapshot, aber nicht einschließlich. Sie müssen den letzten Snapshot manuell löschen, wenn er nicht mehr benötigt wird.

Die folgenden Überlegungen gelten für Snapshot-Lebenszyklusrichtlinien und fast snapshot restore (schnelle Snapshot-Wiederherstellung):

- Amazon Data Lifecycle Manager kann die schnelle Snapshot-Wiederherstellung nur für Snapshots mit einer Größe von 16 TiB oder weniger ermöglichen. Weitere Informationen finden Sie unter Schnelle Amazon EBS-Snapshot-Wiederherstellung.
- Ein Snapshot, der für die schnelle Snapshot-Wiederherstellung aktiviert ist, bleibt auch dann aktiviert, wenn Sie die Richtlinie löschen oder deaktivieren, die schnelle Snapshot-Wiederherstellung für die Richtlinie deaktivieren oder die schnelle Snapshot-Wiederherstellung für die Availability Zone deaktivieren. Sie müssen die schnelle Snapshot-Wiederherstellung für diese Snapshots manuell deaktivieren.
- Wenn Sie die schnelle Snapshot-Wiederherstellung für eine Richtlinie aktivieren und die maximale Anzahl von Snapshots überschreiten, die für die schnelle Snapshot-Wiederherstellung aktiviert werden können, erstellt Amazon Data Lifecycle Manager Snapshots wie geplant, aktiviert sie aber nicht für die schnelle Snapshot-Wiederherstellung. Nachdem ein Snapshot, der zur einer schnellen Snapshot-Wiederherstellung fähig ist, gelöscht wurde, wird der nächste von Amazon Data Lifecycle Manager erstellte Snapshot für die schnelle Snapshot-Wiederherstellung aktiviert.
- Wenn die schnelle Snapshot-Wiederherstellung für einen Snapshot aktiviert wird, dauert es 60 Minuten pro TiB, bis der Snapshot optimiert ist. Wir empfehlen Ihnen die Konfiguration Ihrer Zeitpläne, sodass jeder Snapshot vollständig optimiert ist, bevor Amazon Data Lifecycle Manager den nächsten Snapshot erstellt.
- Wenn Sie die schnelle Snapshot-Wiederherstellung für eine Richtlinie aktivieren, die auf Instances abzielt, aktiviert Amazon Data Lifecycle Manager die schnelle Snapshot-Wiederherstellung individuell für jeden Snapshot im Satz von Multi-Volume-Snapshots. Wenn Amazon Data Lifecycle Manager die schnelle Snapshot-Wiederherstellung für einen der Snapshots im Satz von Multi-Volume-Snapshots nicht aktiviert, wird er weiterhin versuchen, die schnelle Snapshot-Wiederherstellung für die verbleibenden Snapshots im Snapshot-Satz zu aktivieren.

- Es wird Ihnen jede Minute in Rechnung gestellt, in der die schnelle Snapshot-Wiederherstellung für einen Snapshot in einer bestimmten Availability Zone aktiviert ist. Die Gebühren werden mit mindestens einer Stunde anteilig bewertet. Weitere Informationen finden Sie unter Preise und Fakturierung.

> **Note**
>
> Abhängig von der Konfiguration Ihrer Lebenszyklusrichtlinien können mehrere Snapshots aktiviert werden, um gleichzeitig eine schnelle Snapshot-Wiederherstellung in mehreren Availability Zones zu ermöglichen.

Die folgenden Überlegungen gelten für Snapshot-Lebenszyklusrichtlinien und Multi-Attach aktivierte Volumes:

- Bei der Erstellung einer Lifecycle-Richtlinie, die auf Instances abzielt, die dasselbe Multi-Attach aktivierte Volume haben, initiiert Amazon Data Lifecycle Manager für jede angehängte Instance einen Snapshot des Volumes. Verwenden Sie das timestamp-Tag, um die Menge zeitkonsistenter Snapshots zu bestimmen, die von den angefügten Instances erstellt wurden.

Die folgenden Überlegungen gelten für die kontoübergreifende Freigabe von Snapshots:

- Sie können nur Snapshots freigeben, die unverschlüsselt oder mit einem Kundenverwalteter Schlüssel verschlüsselt sind.
- Sie können keine Snapshots freigeben, die mit dem standardmäßigen EBS-Verschlüsselungs-Verschlüsselung verschlüsselt sind.
- Wenn Sie verschlüsselte Snapshots freigeben, müssen Sie auch den KMS-Schlüssel, der zum Verschlüsseln des Quell-Volumes verwendet wurde, für die Zielkonten freigeben. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch.

Die folgenden Überlegungen gelten für Snapshot-Richtlinien und die Snapshot–Archivierung:

- Wenn Sie einen Snapshot, der von einer Richtlinie erstellt wurde, manuell archivieren und sich dieser Snapshot auf der Archivstufe befindet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot nicht. Amazon Data Lifecycle Manager verwaltet keine Snapshots, während sie auf der Archivstufe gespeichert sind. Wenn

Sie auf der Archivstufe gespeicherte Snapshots nicht mehr benötigen, müssen Sie sie manuell löschen.

Die folgenden Überlegungen gelten für Snapshot-Richtlinien und den Papierkorb:

- Wenn Amazon Data Lifecycle Manager einen Snapshot löscht und ihn an den Papierkorb sendet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, und Sie den Snapshot manuell aus dem Papierkorb wiederherstellen, müssen Sie diesen Snapshot manuell löschen, wenn er nicht mehr benötigt wird. Amazon Data Lifecycle Manager verwaltet den Snapshot nicht mehr.
- Wenn Sie einen Snapshot, der von einer Richtlinie erstellt wurde, manuell löschen und sich dieser Snapshot im Papierkorb befindet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot nicht. Amazon Data Lifecycle Manager verwaltet die Snapshots nicht, während sie im Papierkorb gespeichert sind.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, bevor der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot, sobald der Aufbewahrungsschwellenwert der Richtlinie erreicht wird.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, nachdem der Aufbewahrungsschwellenwert der Richtlinie erreicht wurde, löscht Amazon Data Lifecycle Manager den Snapshot nicht mehr. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr benötigt wird.

Die folgenden Überlegungen gelten für Snapshot-Lebenszyklusrichtlinien, die sich im error-Status befinden:

- Bei Richtlinien mit altersbasierten Aufbewahrungszeitplänen werden Snapshots, deren Aufbewahrungszeiträume ablaufen, während sich die Richtlinie im `error`-Status befindet, auf unbestimmte Zeit aufbewahrt. Die Snapshots müssen Sie manuell löschen. Wenn Sie die Richtlinie erneut aktivieren, setzt Amazon Data Lifecycle Manager das Löschen von Snapshots fort, wenn ihre Aufbewahrungszeiträume ablaufen.
- Bei Richtlinien mit anzahlbasierten Aufbewahrungszeitplänen stoppt die Richtlinie das Erstellen und Löschen von Snapshots, während sie sich im `error`-Status befindet. Wenn Sie die Richtlinie erneut aktivieren, setzt Amazon Data Lifecycle Manager das Erstellen von Snapshots sowie das Löschen von Snapshots bei Erreichen des Aufbewahrungsschwellenwerts fort.

Die folgenden Überlegungen gelten für Snapshot-Richtlinien und das Sperren von Snapshots:

- Wenn Sie einen von Amazon Data Lifecycle Manager erstellten Snapshot manuell sperren und dieser Snapshot bei Erreichen des Aufbewahrungsschwellenwerts des Zeitplans immer noch gesperrt ist, wird dieser Snapshot nicht mehr von Amazon Data Lifecycle Manager verwaltet. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr länger benötigt wird.
- Wenn Sie einen von Amazon Data Lifecycle Manager erstellten und für die schnelle Snapshot-Wiederherstellung aktivierten Snapshot manuell sperren und der Snapshot bei Erreichen des Aufbewahrungsschwellenwerts immer noch gesperrt ist, wird Amazon Data Lifecycle Manager die schnelle Snapshot-Wiederherstellung nicht deaktivieren oder den Snapshot löschen. Sie müssen die schnelle Snapshot-Wiederherstellung manuell deaktivieren und den Snapshot löschen, wenn er nicht mehr länger benötigt wird.
- Wenn Sie einen Snapshot, der von Amazon Data Lifecycle Manager mit einem AMI erstellt wurde, manuell anmelden, diesen Snapshot dann sperren und er immer noch gesperrt und dem AMI zugeordnet ist, wenn der Aufbewahrungsschwellenwert erreicht wird, versucht Amazon Data Lifecycle Manager weiterhin, diesen Snapshot zu löschen. Wenn das AMI abgemeldet ist und der Snapshot entsperrt wurde, löscht Amazon Data Lifecycle Manager den Snapshot automatisch.

Weitere Ressourcen

Weitere Informationen finden Sie im Blog Automating Amazon EBS Snapshot and AMI Management using Amazon Data Lifecycle Manager AWS Storage.

Automatisieren Sie anwendungskonsistente Snapshots mit Data Lifecycle Manager

Sie können anwendungskonsistente Snapshots mit Amazon Data Lifecycle Manager automatisieren, indem Sie in Ihren Snapshot-Lebenszyklusrichtlinien Vor- und Nach-Skripts aktivieren, die auf Instances abzielen.

Amazon Data Lifecycle Manager lässt sich in AWS Systems Manager (Systems Manager) integrieren, um anwendungskonsistente Snapshots zu unterstützen. Amazon Data Lifecycle Manager verwendet Systems-Manager-Befehlsdokumente (SSM-Befehlsdokumente), die Vor- und Nach-Skripte enthalten, um die Aktionen zu automatisieren, die für die Erstellung anwendungskonsistenter Snapshots erforderlich sind. Bevor Amazon Data Lifecycle Manager die Snapshot-Erstellung initiiert, führt er die Befehle im Pre-Skript aus, um ihn einzufrieren und zu leeren. I/O Nachdem Amazon Data

Lifecycle Manager die Snapshot-Erstellung initiiert hat, führt er die Befehle im Post-Skript aus, um ihn aufzutauen. I/O

Amazon Data Lifecycle Manager ermöglicht die Automatisierung anwendungskonsistenter Snapshots der folgenden Elemente:

- Windows-Anwendungen unter Verwendung von Volume Shadow Copy Service (VSS)
- SAP HANA verwendet ein AWS verwaltetes SSDM-Dokument. Weitere Informationen finden Sie unter Amazon-EBS-Snapshots für SAP HANA.
- Self-managed Datenbanken wie MySQL, PostgreSQL oder InterSystems IRIS, die SSM-Dokumentvorlagen verwenden

Themen

- Anforderungen an die Verwendung von Vor- und Nach-Skripten
- Erste Schritte mit anwendungskonsistenten Snapshots
- Überlegungen zu VSS-Backups mit Amazon Data Lifecycle Manager
- Geteilte Verantwortlichkeit für anwendungskonsistente Snapshots

Anforderungen an die Verwendung von Vor- und Nach-Skripten

In der folgenden Tabelle werden die Anforderungen an die Verwendung von Vor- und Nach-Skripten mit Amazon Data Lifecycle Manager beschrieben.

	Application-consistent Schnappschüsse		
Anforderung	VSS-Backup	Benutzerdefiniertes SSM-Dokument	Andere Anwendungsfälle
SSM Agent ist installiert und wird auf Zielinstanzen ausgeführt	✓	✓	✓
Die VSS-Systemanforderungen	✓		

	Application-consistent Schnappschüsse		
wurden auf den Zielinstanzen erfüllt			
VSS-fähiges Instanzprofil, das Zielinstanzen zugeordnet ist	✓		
Auf Zielinstanzen installierte VSS-Komponenten	✓		
Bereiten Sie das SSM-Dokument mit Befehlen vor und nach dem Skript vor		✓	✓
Bereiten Sie die Amazon Data Lifecycle Manager-IAM-Rolle vor und führen Sie Pre- und Post-Skripts aus	✓	✓	✓
Erstellen Sie eine Snapshot-Richtlinie, die auf Instances abzielt und für Pre- und Post-Skripts konfiguriert ist	✓	✓	✓

Erste Schritte mit anwendungskonsistenten Snapshots

In diesem Abschnitt werden die Schritte erläutert, die Sie ausführen müssen, um anwendungskonsistente Snapshots mit Amazon Data Lifecycle Manager zu automatisieren.

Schritt 1: Vorbereiten der Ziel-Instances

Sie müssen die Ziel-Instances für anwendungskonsistente Snapshots mit Amazon Data Lifecycle Manager vorbereiten. Führen Sie je nach Anwendungsfall einen der folgenden Schritte durch.

Prepare for VSS Backups

Zur Vorbereitung Ihrer Ziel-Instances für VSS-Backups

1. Installieren Sie den SSM-Agent auf Ihren Ziel-Instances, falls noch nicht geschehen. Wenn der SSM-Agent bereits auf Ihren Ziel-Instances installiert ist, überspringen Sie diesen Schritt.

   Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agenten auf EC2-Instances für Windows Server.
2. Stellen Sie sicher, dass der SSM Agent läuft. Weitere Informationen finden Sie unter Prüfen des Status des SSM-Agents und Starten des Agenten.
3. Richten Sie Systems Manager für Amazon-EC2-Instances ein. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon-EC2-Instances im AWS Systems Manager -Benutzerhandbuch.
4. Stellen Sie sicher, dass die Systemanforderungen für VSS-Backups erfüllt sind.
5. Hängen Sie ein VSS-enabled Instanzprofil an die Zielinstanzen an.
6. Installieren Sie die VSS-Komponenten.

Prepare for SAP HANA backups

Zur Vorbereitung Ihrer Ziel-Instances für SAP–HANA-Backups

1. Bereiten Sie die SAP-HANA-Umgebung auf Ihre Ziel-Instances vor.

   a. Richten Sie Ihre Instance mit SAP HANA ein. Wenn Sie noch nicht über eine bestehende SAP-HANA-Umgebung verfügen, finden Sie unter Einrichtung einer SAP-HANA-Umgebung auf AWS weitere Informationen.

   b. Melden Sie sich als geeigneter Administratorbenutzer bei der SystemDB an.

   c. Erstellen Sie einen Datenbank-Backup-Benutzer, der mit Amazon Data Lifecycle Manager verwendet werden soll.

   ```
   CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

Mit dem folgenden Befehl wird beispielsweise ein Benutzer mit dem Namen `dlm_user` und dem Passwort `password` erstellt.

```
CREATE USER dlm_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

d. Weisen Sie die `BACKUP OPERATOR`-Rolle dem Datenbank-Backup-Benutzer zu, den Sie im vorherigen Schritt erstellt haben.

```
GRANT BACKUP OPERATOR TO username
```

Mit dem folgenden Befehl wird die Rolle beispielsweise einem Benutzer mit dem Namen `dlm_user` zugewiesen.

```
GRANT BACKUP OPERATOR TO dlm_user
```

e. Melden Sie sich als Administrator beim Betriebssystem an, beispielsweise *sid*`adm`.

f. Erstellen Sie einen `hdbuserstore`-Eintrag zum Speichern von Verbindungsinformationen, sodass das SAP-HANA-SSM-Dokument eine Verbindung zu SAP HANA herstellen kann, ohne dass Benutzer die Informationen eingeben müssen.

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER
 localhost:3hana_instance_number13 username password
```

Beispiel:

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. Testen Sie die Verbindung.

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. Installieren Sie den SSM-Agent auf Ihren Ziel-Instances, falls noch nicht geschehen. Wenn der SSM-Agent bereits auf Ihren Ziel-Instances installiert ist, überspringen Sie diesen Schritt.

   Weitere Informationen finden Sie unter Manuelles Installieren des SSM Agents auf EC2-Instances für Linux.

3. Stellen Sie sicher, dass der SSM Agent läuft. Weitere Informationen finden Sie unter Prüfen des Status des SSM-Agents und Starten des Agenten.

4. Richten Sie Systems Manager für Amazon-EC2-Instances ein. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon-EC2-Instances im AWS Systems Manager -Benutzerhandbuch.

Prepare for custom SSM documents

Vorbereitung benutzerdefinierter SSM-Dokumente für Ihre Ziel-Instances

1. Installieren Sie den SSM-Agent auf Ihren Ziel-Instances, falls noch nicht geschehen. Wenn der SSM-Agent bereits auf Ihren Ziel-Instances installiert ist, überspringen Sie diesen Schritt.
   - (Linux-Instanzen) Manuelles Installieren des SSM Agents auf EC2-Instances für Linux
   - (Windows-Instanzen) Arbeiten mit dem SSM Agent auf EC2-Instances für Windows Server
2. Stellen Sie sicher, dass der SSM Agent läuft. Weitere Informationen finden Sie unter Prüfen des Status des SSM-Agents und Starten des Agenten.
3. Richten Sie Systems Manager für Amazon-EC2-Instances ein. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon-EC2-Instances im AWS Systems Manager -Benutzerhandbuch.

Schritt 2: Vorbereiten des SSM-Dokuments

> **Note**
>
> Dieser Schritt ist nur für benutzerdefinierte SSM-Dokumente erforderlich. Für VSS-Backup oder SAP HANA ist er nicht erforderlich. Für VSS-Backups und SAP HANA verwendet Amazon Data Lifecycle Manager das AWS verwaltete SSM-Dokument.

Wenn Sie anwendungskonsistente Snapshots für eine selbstverwaltete Datenbank wie MySQL, PostgreSQL oder InterSystems IRIS automatisieren, müssen Sie ein SSM-Befehlsdokument erstellen, das ein Pre-Skript zum Einfrieren und Leeren I/O vor der Snapshot-Erstellung sowie ein Post-Skript zum Auftauen nach der Snapshot-Erstellung enthält. I/O

Wenn Ihre MySQL-, PostgreSQL- oder InterSystems IRIS-Datenbank Standardkonfigurationen verwendet, können Sie ein SSM-Befehlsdokument erstellen, indem Sie den unten stehenden SSM-Beispieldokumentinhalt verwenden. Wenn Ihre MySQL-, PostgreSQL- oder InterSystems IRIS-Datenbank eine nicht standardmäßige Konfiguration verwendet, können Sie den folgenden

Beispielinhalt als Ausgangspunkt für Ihr SSM-Befehlsdokument verwenden und es dann an Ihre Anforderungen anpassen. Wenn Sie ein SSM-Dokument von Grund auf neu erstellen möchten, können Sie alternativ die leere SSM-Dokumentvorlage unten verwenden und Ihre Vor- und Nach-Befehle in den entsprechenden Dokumentabschnitten hinzufügen.

⚠ Beachten Sie Folgendes:

- Es liegt in Ihrer Verantwortung, sicherzustellen, dass das SSM-Dokument die richtigen und erforderlichen Aktionen für Ihre Datenbankkonfiguration ausführt.
- Snapshots sind nur dann garantiert anwendungskonsistent, wenn die Pre- und Post-Skripts in Ihrem SSM-Dokument erfolgreich eingefroren, geleert und wieder aufgetaut werden können. I/O
- Das SSM-Dokument muss die erforderlichen Felder für `allowedValues` enthalten, einschließlich `pre-script`, `post-script` und `dry-run`. Amazon Data Lifecycle Manager führt Befehle auf Ihrer Instance basierend auf den Inhalten dieser Abschnitte aus. Wenn Ihr SSM-Dokument diese Abschnitte nicht enthält, behandelt Amazon Data Lifecycle Manager dies als fehlgeschlagene Ausführung.

MySQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

```
###=====================================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###=====================================================================================###
      ### Error Codes
```

```
###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206

     ###====================================================================###
     ### Global variables
     ###====================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}
     FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
     FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
     FS_BUSY_ERROR='mount point is busy'

     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
         # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
         check_fs_freeze
         # Execute the DB commands to flush the DB in preparation for snapshot
         snap_db
         # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
         freeze_fs
```

```
        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
        unfreeze_fs
        thaw_db
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
```

```
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
```

```
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    sudo mysql -e 'UNLOCK TABLES;'
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                thaw_db
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
```

```
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Flush and Lock command."
            sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
            # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
        fi
    }

    thaw_db() {
        # Run the unlock command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Unlock"
            sudo mysql -e 'UNLOCK TABLES;'
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Unlock command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs
    export -f thaw_db

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"
```

```
      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
          pre-script)
              execute_pre_script
              ;;
          post-script)
              execute_post_script
              execute_disable_auto_thaw
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

PostgreSQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
```

```
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash
```

```
###============================================================================###
     ### Error Codes

###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
     ### Global variables

###============================================================================###
     START=$(date +%s)
     OPERATION={{ command }}
     FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
     FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
     FS_BUSY_ERROR='mount point is busy'

     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
         # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
         check_fs_freeze
         # Execute the DB commands to flush the DB in preparation for snapshot
```

```
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
        unfreeze_fs
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }
```

```
    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
```

```
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
```

```
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when PostgreSQL DB service is up and running
        sudo systemctl is-active --quiet postgresql
        if [ $? -eq 0 ]; then
            echo "INFO: Execute Postgres CHECKPOINT"
            # PostgreSQL command to flush the transactions in memory to disk
            sudo -u postgres psql -c 'CHECKPOINT;'
            # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: Postgres CHECKPOINT command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            execute_disable_auto_thaw
            ;;
        dry-run)
```

```
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

InterSystems IRIS sample document content

```
###############################################################################
# MIT License
#
# Copyright (c) 2024 InterSystems
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature for InterSystems IRIS.
parameters:
```

```
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
 execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
 You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
 trigger pre and post script actions.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

 ###============================================================================###
      ### Global variables

 ###============================================================================###
      DOCKER_NAME=iris
      LOGDIR=./
      EXIT_CODE=0
      OPERATION={{ command }}
      START=$(date +%s)
```

```
     # Check if Docker is installed
     # By default if Docker is present, script assumes that InterSystems IRIS is
 running in Docker
     # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
 non-containerised (and Docker is present).
     # Script assumes irissys user has OS auth enabled, change the OS user or
 supply login/password depending on your configuration.
     if command -v docker &> /dev/null
     then
       DOCKER_EXEC="docker exec $DOCKER_NAME"
     else
       DOCKER_EXEC="sudo -i -u irissys"
     fi


     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
       echo "INFO: Start execution of pre-script"

       # find all iris running instances
       iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
       echo "`date`: Running iris instances $iris_instances"

       # Only for running instances
       for INST in $iris_instances; do

         echo "`date`: Attempting to freeze $INST"

         # Detailed instances specific log
         LOGFILE=$LOGDIR/$INST-pre_post.log

         #check Freeze status before starting
         $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
         freeze_status=$?
         if [ $freeze_status -eq 5 ]; then
           echo "`date`:   ERROR: $INST IS already FROZEN"
           EXIT_CODE=204
         else
           echo "`date`:   $INST is not frozen"
           # Freeze
           # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
```

```
            $DOCKER_EXEC irissession $INST -U '%SYS'
"##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS FROZEN"
                ;;
              3) echo "`date`:   $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
            esac
            echo "`date`:   Completed freeze of $INST"
          fi
        done
        echo "`date`: Pre freeze script finished"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
        echo "INFO: Start execution of post-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5-  | awk '{print $1}')
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to thaw $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status befor starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
"##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:  $INST is in frozen state"
            # Thaw
```

```
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS THAWED"
                  $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
              3) echo "`date`:   $INST THAW FAILED"
                  EXIT_CODE=202
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                  EXIT_CODE=202
                ;;
            esac
            echo "`date`:   Completed thaw of $INST"
          else
            echo "`date`:   ERROR: $INST IS already THAWED"
            EXIT_CODE=205
          fi
        done
        echo "`date`: Post thaw script finished"
      }

      # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
        pre-script)
          execute_pre_script
          ;;
        post-script)
          execute_post_script
            ;;
        dry-run)
          echo "INFO: dry-run option invoked - taking no action"
          ;;
        *)
```

```
          echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
          # return failure
          EXIT_CODE=1
          ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
      exit $EXIT_CODE
```

Weitere Informationen finden Sie im Repository. GitHub

Empty document template

```
###====================================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###====================================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
```

```
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
```

```
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206


###############################################################################
    ### Global variables

###############################################################################
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
    }

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
```

```
                echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
                exit 1 # return failure
                ;;
        esac

        END=$(date +%s)
        # Debug Log for profiling the script time
        echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Sobald Sie über den Inhalt Ihres SSM-Dokuments verfügen, verwenden Sie eines der folgenden Verfahren, um das benutzerdefinierte SSM-Dokument zu erstellen.

Console

Erstellen eines SSM-Befehlsdokuments

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com//systems-manager/.
2. Wählen Sie im Navigationsbereich Dokumente und dann Dokument erstellen, Befehl oder Sitzung aus.
3. Geben Sie unter Name einen aussagekräftigen Namen für das Dokument ein.
4. Wählen Sie als Zieltyp /AWS::EC2::Instance.
5. Wählen Sie als Dokumenttyp Befehl.
6. Wählen Sie im Feld Inhalt die Option YAML aus und fügen Sie dann den Inhalt des Dokuments ein.
7. Fügen Sie im Abschnitt Dokument-Tags ein Tag mit einem Tag-Schlüssel von `DLMScriptsAccess` und einem Tag-Wert von `true` hinzu.

> **Important**
>
> Das `DLMScriptsAccess:true` Tag ist für die AWSDataLifecycleManagerSSMFullAccess AWS verwaltete Richtlinie erforderlich, die in Schritt 3: Vorbereiten der Amazon Data Lifecycle Manager-IAM-Rolle verwendet wurde. Die Richtlinie verwendet den `aws:ResourceTag-`

Bedingungsschlüssel, um den Zugriff auf SSM-Dokumente mit diesem Tag einzuschränken.

8. Wählen Sie Create document (Dokument erstellen) aus.

AWS CLI

Erstellen eines SSM-Befehlsdokuments

Verwenden Sie den Befehl create-document. Geben Sie für `--name` einen beschreibenden Namen für das Dokument ein. Legen Sie für `--document-type` die Option `Command` fest. Geben Sie für `--content` den Pfad zur .yaml-Datei mit dem SSM-Dokumentinhalt an. Legen Sie für `--tags` die Option `"Key=DLMScriptsAccess,Value=true"` fest.

```
$ aws ssm create-document \
--content file://path/to/file/documentContent.yaml \
--name "document_name" \
--document-type "Command" \
--document-format YAML \
--tags "Key=DLMScriptsAccess,Value=true"
```

Schritt 3: Vorbereiten der IAM-Rolle für Amazon Data Lifecycle Manager

Note

Dieser Schritt ist erforderlich, wenn:

- Sie erstellen oder aktualisieren eine pre/post skriptfähige Snapshot-Richtlinie, die eine benutzerdefinierte IAM-Rolle verwendet.
- Sie verwenden die Befehlszeile, um eine pre/post skriptfähige Snapshot-Richtlinie zu erstellen oder zu aktualisieren, die die Standardrichtlinie verwendet.

Wenn Sie die Konsole verwenden, um eine pre/post skriptfähige Snapshot-Richtlinie zu erstellen oder zu aktualisieren, die die Standardrolle für die Verwaltung von Snapshots (AWSDataLifecycleManagerDefaultRole) verwendet, überspringen Sie diesen Schritt. In diesem Fall wird die AWSDataLifecycleManagerSSMFullAccess Richtlinie automatisch an diese Rolle angehängt.

Sie müssen sicherstellen, dass die IAM-Rolle, die Sie für die Richtlinie verwenden, Amazon Data Lifecycle Manager die Erlaubnis erteilt, die SSM-Aktionen auszuführen, die für die Ausführung von Pre- und Post-Skripts auf Instances erforderlich sind, auf die die Richtlinie abzielt.

Amazon Data Lifecycle Manager stellt eine verwaltete Richtlinie (AWSDataLifecycleManagerSSMFullAccess) bereit, die die erforderlichen Berechtigungen enthält. Sie können diese Richtlinie an Ihre IAM-Rolle für die Verwaltung von Snapshots anhängen, um sicherzustellen, dass sie die Berechtigungen enthält.

> **Important**
>
> Die AWSDataLifecycleManagerSSMFullAccess verwaltete Richtlinie verwendet den `aws:ResourceTag` Bedingungsschlüssel, um den Zugriff auf bestimmte SSM-Dokumente einzuschränken, wenn Pre- und Post-Skripts verwendet werden. Damit Amazon Data Lifecycle Manager auf die SSM-Dokumente zugreifen kann, müssen Sie sicherstellen, dass Ihre SSM-Dokumente mit folgenden Tags versehen sind. `DLMScriptsAccess:true`

Alternativ können Sie manuell eine benutzerdefinierte Richtlinie erstellen oder die erforderlichen Berechtigungen direkt der von Ihnen verwendeten IAM-Rolle zuweisen. Sie können dieselben Berechtigungen verwenden, die in der AWSDataLifecycleManagerSSMFullAccess verwalteten Richtlinie definiert sind, der `aws:ResourceTag` Bedingungsschlüssel ist jedoch optional. Wenn Sie sich dafür entscheiden, diesen Bedingungsschlüssel nicht zu verwenden, müssen Sie Ihre SSM-Dokumente nicht mit `DLMScriptsAccess:true` markieren.

Verwenden Sie eine der folgenden Methoden, um die AWSDataLifecycleManagerSSMFullAccess Richtlinie zu Ihrer IAM-Rolle hinzuzufügen.

Console

So hängen Sie die verwaltete Richtlinie an Ihre benutzerdefinierte Rolle an

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationspanel Rollen aus.
3. Suchen Sie nach Ihrer benutzerdefinierten Rolle zur Verwaltung von Snapshots und wählen Sie sie aus.
4. Wählen Sie auf der Registerkarte Berechtigungen Berechtigungen hinzufügen und dann Richtlinien anfügen aus.

5. Suchen Sie nach der AWSDataLifecycleManagerSSMFullAccess verwalteten Richtlinie, wählen Sie sie aus und wählen Sie dann Berechtigungen hinzufügen aus.

AWS CLI

So hängen Sie die verwaltete Richtlinie an Ihre benutzerdefinierte Rolle an

Verwenden Sie den Befehl attach-role-policy. Geben Sie für `---role-name` den Namen Ihrer benutzerdefinierten Rolle an. Legen Sie für `--policy-arn` die Option `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess` fest.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Schritt 4: Erstellen der Snapshot-Lebenszyklusrichtlinie

Um anwendungskonsistente Snapshots zu automatisieren, müssen Sie eine Snapshot-Lebenszyklusrichtlinie für Instances erstellen und Vor- und Nach-Skripte für diese Richtlinie konfigurieren.

Console

So erstellen Sie die Snapshot-Lebenszyklusrichtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store und Lifecycle Manager aus. Wählen Sie dann Create lifecycle policy (Lebenszyklusrichtlinie erstellen) aus.
3. Wählen Sie auf dem Bildschirm Richtlinientyp auswählen die Option EBS-Snapshot-Richtlinie und dann Weiter aus.
4. Gehen Sie im Abschnitt Zielressourcen wie folgt vor:
   a. Wählen Sie für Ziel-Ressourcentypen die Option `Instance`.
   b. Geben Sie für Zielressourcen-Tags die Ressourcen-Tags an, die die zu sichernden Instances identifizieren. Nur Ressourcen mit den angegebenen Tags werden gesichert.
5. Wählen Sie für die IAM-Rolle entweder AWSDataLifecycleManagerDefaultRole (die Standardrolle für die Verwaltung von Snapshots) oder eine benutzerdefinierte Rolle, die Sie für Pre- und Post-Skripts erstellt und vorbereitet haben.

6. Konfigurieren Sie die Zeitpläne und zusätzlichen Optionen nach Bedarf. Wir empfehlen Ihnen, die Snapshot-Erstellung für Zeiträume einzuplanen, die Ihrem Workload entsprechen, z. B. während Wartungsfenstern.

   Für SAP HANA empfehlen wir, die schnelle Snapshot-Wiederherstellung zu aktivieren.

   > **Note**
   >
   > Wenn Sie einen Zeitplan für VSS-Backups aktivieren, können Sie die Optionen Ausschließen bestimmter Daten-Volumes oder Tags aus der Quelle kopieren nicht aktivieren.

7. Wählen Sie im Abschnitt Vor- und Nach-Skripte die Option Vor- und Nach-Skripte aktivieren aus und gehen Sie dann je nach Workload wie folgt vor:

   - Um anwendungskonsistente Snapshots Ihrer Windows-Anwendungen zu erstellen, wählen Sie VSS-Backup.
   - Um anwendungskonsistente Snapshots Ihrer SAP-HANA-Workloads zu erstellen, wählen Sie SAP HANA.
   - Um anwendungskonsistente Snapshots aller anderen Datenbanken und Workloads, einschließlich Ihrer selbstverwalteten MySQL-, PostgreSQL- oder InterSystems IRIS-Datenbanken, mithilfe eines benutzerdefinierten SSM-Dokuments zu erstellen, wählen Sie Benutzerdefiniertes SSM-Dokument aus.

     1. Wählen Sie für Option automatisieren Vor- und Nach-Skripte aus.
     2. Wählen Sie unter SSM-Dokument das SSM-Dokument aus, das Sie vorbereitet haben.

8. Konfigurieren Sie je nach der ausgewählten Option die folgenden zusätzlichen Optionen:

   - Timeout für das Skript – (nur benutzerdefiniertes SSM-Dokument) Der Timeout-Zeitraum, nach dem Amazon Data Lifecycle Manager die versuchte Skriptausführung als fehlgeschlagen behandelt, wenn sie nicht abgeschlossen wurde. Wenn ein Skript nicht innerhalb des Timeout-Zeitraums abgeschlossen wird, schlägt der Versuch von Amazon Data Lifecycle Manager fehl. Der Timeout-Zeitraum gilt für die Vor- und Nach-Skripte einzeln. Der Minimal- und Standardwert für den Timeout beträgt 10 Sekunden. Die maximale Timeout-Zeit beträgt 120 Sekunden.
   - Fehlgeschlagene Skripte erneut versuchen – Wählen Sie diese Option, um Skripte zu wiederholen, die nicht innerhalb ihres Timeouts abgeschlossen werden. Wenn das Vor-Skript fehlschlägt, wiederholt Amazon Data Lifecycle Manager den gesamten Snapshot-

Erstellungsprozess, einschließlich der Ausführung der Vor- und Nach-Skripte. Wenn das Nach-Skript fehlschlägt, wiederholt Amazon Data Lifecycle Manager nur das Nach-Skript. In diesem Fall ist das Vor-Skript abgeschlossen und der Snapshot wurde möglicherweise erstellt.

- Standardmäßig absturzkonsistente Snapshots – Wählen Sie diese Option, um standardmäßig absturzkonsistente Snapshots zu verwenden, falls das Vor-Skript nicht ausgeführt werden kann. Dies ist das Standardverhalten bei der Snapshot-Erstellung für Amazon Data Lifecycle Manager, wenn Vor- und Nach-Skripte nicht aktiviert sind. Wenn Sie Wiederholungen aktiviert haben, verwendet Amazon Data Lifecycle Manager standardmäßig nur dann absturzkonsistente Snapshots, wenn alle Wiederholungsversuche ausgeschöpft sind. Wenn das Vor-Skript fehlschlägt und Sie nicht standardmäßig absturzkonsistente Snapshots verwenden, erstellt Amazon Data Lifecycle Manager während dieser geplanten Ausführung keine Snapshots für die Instance.

> **Note**
>
> Wenn Sie Snapshots für SAP HANA erstellen, möchten Sie diese Option möglicherweise deaktivieren. Crash-consistent Snapshots von SAP HANA-Workloads können nicht auf dieselbe Weise wiederhergestellt werden.

9. Wählen Sie Standardrichtlinie erstellen.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRole already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

AWS CLI

So erstellen Sie die Snapshot-Lebenszyklusrichtlinie

Verwenden Sie den Befehl create-lifecycle-policy und schließen Sie die `Scripts`-Parameter in `CreateRule` ein. Weitere Informationen finden Sie in der API-Referenz für Amazon Data Lifecycle Manager.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Wenn `policyDetails.json` einen der folgenden Aspekte beinhaltet, gehen Sie je nach Anwendungsfall wie folgt vor:

- VSS-Backup

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "ExecutionHandler":"AWS_VSS_BACKUP",
                "ExecuteOperationOnScriptFailure":true|false,
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- SAP-HANA-Backups

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
```

```
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Benutzerdefiniertes SSM-Dokument

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
```

```
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Überlegungen zu VSS-Backups mit Amazon Data Lifecycle Manager

Mit Amazon Data Lifecycle Manager können Sie VSS-fähige Windows-Anwendungen (Volume Shadow Copy Service), die auf Amazon-EC2-Instances ausgeführt werden, sichern und wiederherstellen. Wenn für die Anwendung ein VSS-Schreiber bei Windows VSS registriert ist, erstellt Amazon Data Lifecycle Manager einen Snapshot, der für diese Anwendung anwendungskonsistent ist.

> **Note**
>
> Amazon Data Lifecycle Manager unterstützt derzeit nur anwendungskonsistente Snapshots von Ressourcen, die auf Amazon EC2 ausgeführt werden, insbesondere für Sicherungsszenarien, in denen Anwendungsdaten wiederhergestellt werden können, indem eine bestehende Instance durch eine neue, aus der Sicherung erstellte Instance ersetzt wird. Nicht alle Instance-Typen oder Anwendungen werden für VSS-Backups unterstützt. Weitere Informationen finden Sie unter Application-consistent Windows VSS-Snapshots im Amazon EC2-Benutzerhandbuch.

Nicht unterstützte Instance-Typen

Die folgenden Instance-Typen von Amazon EC2 werden für VSS-Backups nicht unterstützt. Wenn Ihre Richtlinie auf einen dieser Instance-Typen abzielt, erstellt Amazon Data Lifecycle Manager möglicherweise trotzdem VSS-Backups, aber die Snapshots sind unter Umständen nicht mit den erforderlichen System-Tags gekennzeichnet. Ohne diese Tags werden die Snapshots nach der Erstellung nicht von Amazon Data Lifecycle Manager verwaltet. Sie müssen diese Snapshots möglicherweise manuell löschen.

- T3: `t3.nano` | `t3.micro`
- T3a: `t3a.nano` | `t3a.micro`
- T2: `t2.nano` | `t2.micro`

Geteilte Verantwortlichkeit für anwendungskonsistente Snapshots

Sie müssen sicherstellen, dass:

- Der SSM-Agent ist installiert, aktuell und läuft auf Ihren Ziel-Instances.
- Systems Manager verfügt über Berechtigungen zum Ausführen der erforderlichen Aktionen auf den Ziel-Instances.
- Amazon Data Lifecycle Manager ist berechtigt, die Systems-Manager-Aktionen auszuführen, die für die Ausführung von Vor- und Nach-Skripten auf den Ziel-Instances erforderlich sind.
- Für benutzerdefinierte Workloads, wie z. B. selbstverwaltete MySQL-, PostgreSQL- oder InterSystems IRIS-Datenbanken, enthält das von Ihnen verwendete SSM-Dokument die richtigen und erforderlichen Aktionen zum Einfrieren, Leeren und Auftauen Ihrer Datenbankkonfiguration. I/O
- Die Zeiten für die Snapshot-Erstellung richten sich nach Ihrem Workload-Zeitplan. Versuchen Sie beispielsweise, die Snapshot-Erstellung für geplante Wartungsfenster einzuplanen.

Amazon Data Lifecycle Manager stellt sicher, dass:

- Die Snapshot-Erstellung wird innerhalb von 60 Minuten nach der geplanten Snapshot-Erstellung initiiert.
- Vor-Skripte werden ausgeführt, bevor die Snapshot-Erstellung initiiert wird.
- Nach-Skripte werden ausgeführt, nachdem das Vor-Skript erfolgreich war und die Snapshot-Erstellung initiiert wurde. Amazon Data Lifecycle Manager führt das Nach-Skript nur aus, wenn das Vor-Skript erfolgreich war. Wenn das Vor-Skript fehlschlägt, führt Amazon Data Lifecycle Manager das Nach-Skript nicht aus.
- Snapshots werden bei der Erstellung mit den passenden Tags versehen.
- CloudWatch Metriken und Ereignisse werden ausgegeben, wenn Skripts initiiert werden und wenn sie fehlschlagen oder erfolgreich sind.

Andere Anwendungsfälle für Data Lifecycle Manager: Pre- und Post-Skripts

Neben der Verwendung von Vor- und Nach-Skripten zur Automatisierung anwendungskonsistenter Snapshots können Sie Vor- und Nach-Skripte zusammen oder einzeln verwenden, um andere Verwaltungsaufgaben vor oder nach der Snapshot-Erstellung zu automatisieren. Beispiel:

- Verwenden Sie ein Vor-Skript, um Patches vor dem Erstellen von Snapshots anzuwenden. Dies ist hilfreich bei der Snapshot-Erstellung, nachdem Sie Ihre regulären wöchentlichen oder monatlichen Softwareupdates installiert haben.

  > **Note**
  >
  > Wenn Sie nur ein Vor-Skript ausführen möchten, ist die Option Standardmäßig absturzkonsistente Snapshots standardmäßig aktiviert.

- Verwenden eines Nach-Skripts zum Anwenden von Patches nach der Snapshot-Erstellung Dies ist bei der Snapshot-Erstellung hilfreich, bevor Sie Ihre regulären wöchentlichen oder monatlichen Softwareupdates installieren.

Erste Schritte für andere Anwendungsfälle

In diesem Abschnitt werden die Schritte erläutert, die Sie ausführen müssen, wenn Sie and/or Pre-Post-Skripts für andere Anwendungsfälle als anwendungskonsistente Snapshots verwenden.

Schritt 1: Vorbereiten der Ziel-Instances

So bereiten Sie Ihre Ziel-Instances auf Pre-Post-Skripts vor and/or

1. Installieren Sie den SSM-Agent auf Ihren Ziel-Instances, falls noch nicht geschehen. Wenn der SSM-Agent bereits auf Ihren Ziel-Instances installiert ist, überspringen Sie diesen Schritt.
   - (Linux-Instances) Manuelles Installieren des SSM Agents auf EC2-Instances für Linux
   - (Windows-Instanzen) Arbeiten mit dem SSM Agent auf EC2-Instances für Windows Server
2. Stellen Sie sicher, dass der SSM Agent läuft. Weitere Informationen finden Sie unter Prüfen des Status des SSM-Agents und Starten des Agenten.
3. Richten Sie Systems Manager für Amazon-EC2-Instances ein. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon-EC2-Instances im AWS Systems Manager - Benutzerhandbuch.

Schritt 2: Vorbereiten des SSM-Dokuments

Sie müssen ein SSM-Befehlsdokument erstellen, das die and/or Pre-Post-Skripts mit den Befehlen enthält, die Sie ausführen möchten.

Sie können mithilfe der unten stehenden leeren SSM-Dokumentvorlage ein SSM-Dokument erstellen und Ihre Vor- und Nach-Skriptbefehle in den entsprechenden Dokumentabschnitten hinzufügen.

⚠ Beachten Sie Folgendes:

- Es liegt in Ihrer Verantwortung, sicherzustellen, dass das SSM-Dokument die richtigen und erforderlichen Aktionen für Ihre Arbeitslast ausführt.
- Das SSM-Dokument muss die erforderlichen Felder für `allowedValues` enthalten, einschließlich `pre-script`, `post-script` und `dry-run`. Amazon Data Lifecycle Manager führt Befehle auf Ihrer Instance basierend auf den Inhalten dieser Abschnitte aus. Wenn Ihr SSM-Dokument diese Abschnitte nicht enthält, behandelt Amazon Data Lifecycle Manager dies als fehlgeschlagene Ausführung.

```
###======================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###======================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
```

```
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions during
 policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager to
 successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should be
 executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###========================================================================###
      ### Error Codes

 ###========================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
```

```
    # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
    ### Global variables

###============================================================================###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
    }

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
```

```
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Schritt 3: Vorbereiten der IAM-Rolle für Amazon Data Lifecycle Manager

> **Note**
>
> Dieser Schritt ist erforderlich, wenn:
>
> - Sie erstellen oder aktualisieren eine pre/post skriptfähige Snapshot-Richtlinie, die eine benutzerdefinierte IAM-Rolle verwendet.
> - Sie verwenden die Befehlszeile, um eine pre/post skriptfähige Snapshot-Richtlinie zu erstellen oder zu aktualisieren, die die Standardrichtlinie verwendet.
>
> Wenn Sie die Konsole verwenden, um eine pre/post skriptfähige Snapshot-Richtlinie zu erstellen oder zu aktualisieren, die die Standardrolle für die Verwaltung von Snapshots (AWSDataLifecycleManagerDefaultRole) verwendet, überspringen Sie diesen Schritt. In diesem Fall wird die AWSDataLifecycleManagerSSMFullAccess Richtlinie automatisch an diese Rolle angehängt.

Sie müssen sicherstellen, dass die IAM-Rolle, die Sie für die Richtlinie verwenden, Amazon Data Lifecycle Manager die Erlaubnis erteilt, die SSM-Aktionen auszuführen, die für die Ausführung von Pre- und Post-Skripts auf Instances erforderlich sind, auf die die Richtlinie abzielt.

Amazon Data Lifecycle Manager stellt eine verwaltete Richtlinie (AWSDataLifecycleManagerSSMFullAccess) bereit, die die erforderlichen Berechtigungen enthält. Sie können diese Richtlinie an Ihre IAM-Rolle für die Verwaltung von Snapshots anhängen, um sicherzustellen, dass sie die Berechtigungen enthält.

> **Important**
>
> Die AWSDataLifecycleManagerSSMFullAccess verwaltete Richtlinie verwendet den `aws:ResourceTag` Bedingungsschlüssel, um den Zugriff auf bestimmte SSM-Dokumente einzuschränken, wenn Pre- und Post-Skripts verwendet werden. Damit Amazon Data Lifecycle Manager auf die SSM-Dokumente zugreifen kann, müssen Sie sicherstellen, dass Ihre SSM-Dokumente mit folgenden Tags versehen sind. `DLMScriptsAccess:true`

Alternativ können Sie manuell eine benutzerdefinierte Richtlinie erstellen oder die erforderlichen Berechtigungen direkt der von Ihnen verwendeten IAM-Rolle zuweisen. Sie können dieselben Berechtigungen verwenden, die in der AWSDataLifecycleManagerSSMFullAccess verwalteten Richtlinie definiert sind, der `aws:ResourceTag` Bedingungsschlüssel ist jedoch optional. Wenn Sie sich dafür entscheiden, diesen Bedingungsschlüssel nicht zu verwenden, müssen Sie Ihre SSM-Dokumente nicht mit `DLMScriptsAccess:true` markieren.

Verwenden Sie eine der folgenden Methoden, um die AWSDataLifecycleManagerSSMFullAccess Richtlinie zu Ihrer IAM-Rolle hinzuzufügen.

Console

So hängen Sie die verwaltete Richtlinie an Ihre benutzerdefinierte Rolle an

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationspanel Rollen aus.
3. Suchen Sie nach Ihrer benutzerdefinierten Rolle zur Verwaltung von Snapshots und wählen Sie sie aus.
4. Wählen Sie auf der Registerkarte Berechtigungen Berechtigungen hinzufügen und dann Richtlinien anfügen aus.
5. Suchen Sie nach der AWSDataLifecycleManagerSSMFullAccess verwalteten Richtlinie, wählen Sie sie aus und wählen Sie dann Berechtigungen hinzufügen aus.

AWS CLI

So hängen Sie die verwaltete Richtlinie an Ihre benutzerdefinierte Rolle an

Verwenden Sie den Befehl attach-role-policy. Geben Sie für `---role-name` den Namen Ihrer benutzerdefinierten Rolle an. Legen Sie für `--policy-arn` die Option `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess` fest.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Snapshot-Lebenszyklusrichtlinie erstellen

Console

So erstellen Sie die Snapshot-Lebenszyklusrichtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store und Lifecycle Manager aus. Wählen Sie dann Create lifecycle policy (Lebenszyklusrichtlinie erstellen) aus.
3. Wählen Sie auf dem Bildschirm Richtlinientyp auswählen die Option EBS-Snapshot-Richtlinie und dann Weiter aus.
4. Gehen Sie im Abschnitt Zielressourcen wie folgt vor:
   a. Wählen Sie für Ziel-Ressourcentypen die Option `Instance`.
   b. Geben Sie für Zielressourcen-Tags die Ressourcen-Tags an, die die zu sichernden Instances identifizieren. Nur Ressourcen mit den angegebenen Tags werden gesichert.
5. Wählen Sie für die IAM-Rolle entweder AWSDataLifecycleManagerDefaultRole (die Standardrolle für die Verwaltung von Snapshots) oder eine benutzerdefinierte Rolle, die Sie für Pre- und Post-Skripts erstellt und vorbereitet haben.
6. Konfigurieren Sie die Zeitpläne und zusätzlichen Optionen nach Bedarf. Wir empfehlen Ihnen, die Snapshot-Erstellung für Zeiträume einzuplanen, die Ihrem Workload entsprechen, z. B. während Wartungsfenstern.
7. Wählen Sie im Abschnitt Vor- und Nach-Skripte die Option Vor- und Nach-Skripte aktivieren und gehen Sie dann wie folgt vor:
   a. Wählen Sie Benutzerdefiniertes SSM-Dokument.
   b. Wählen Sie unter Option automatisieren die Option aus, die den auszuführenden Skripten entspricht.

c. Wählen Sie unter SSM-Dokument das SSM-Dokument aus, das Sie vorbereitet haben.

8. Konfigurieren Sie bei Bedarf die folgenden zusätzlichen Optionen:

   - Timeout für das Skript – Der Timeout-Zeitraum, nach dem Amazon Data Lifecycle Manager die versuchte Skriptausführung als fehlgeschlagen behandelt, wenn sie nicht abgeschlossen wurde. Wenn ein Skript nicht innerhalb des Timeout-Zeitraums abgeschlossen wird, schlägt der Versuch von Amazon Data Lifecycle Manager fehl. Der Timeout-Zeitraum gilt für die Vor- und Nach-Skripte einzeln. Der Minimal- und Standardwert für den Timeout beträgt 10 Sekunden. Die maximale Timeout-Zeit beträgt 120 Sekunden.
   - Fehlgeschlagene Skripte erneut versuchen – Wählen Sie diese Option, um Skripte zu wiederholen, die nicht innerhalb ihres Timeouts abgeschlossen werden. Wenn das Vor-Skript fehlschlägt, wiederholt Amazon Data Lifecycle Manager den gesamten Snapshot-Erstellungsprozess, einschließlich der Ausführung der Vor- und Nach-Skripte. Wenn das Nach-Skript fehlschlägt, wiederholt Amazon Data Lifecycle Manager nur das Nach-Skript. In diesem Fall ist das Vor-Skript abgeschlossen und der Snapshot wurde möglicherweise erstellt.
   - Standardmäßig absturzkonsistente Snapshots – Wählen Sie diese Option, um standardmäßig absturzkonsistente Snapshots zu verwenden, falls das Vor-Skript nicht ausgeführt werden kann. Dies ist das Standardverhalten bei der Snapshot-Erstellung für Amazon Data Lifecycle Manager, wenn Vor- und Nach-Skripte nicht aktiviert sind. Wenn Sie Wiederholungen aktiviert haben, verwendet Amazon Data Lifecycle Manager standardmäßig nur dann absturzkonsistente Snapshots, wenn alle Wiederholungsversuche ausgeschöpft sind. Wenn das Vor-Skript fehlschlägt und Sie nicht standardmäßig absturzkonsistente Snapshots verwenden, erstellt Amazon Data Lifecycle Manager während dieser geplanten Ausführung keine Snapshots für die Instance.

9. Wählen Sie Standardrichtlinie erstellen.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRole already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

AWS CLI

So erstellen Sie die Snapshot-Lebenszyklusrichtlinie

Verwenden Sie den Befehl create-lifecycle-policy und schließen Sie die `Scripts`-Parameter in `CreateRule` ein. Weitere Informationen finden Sie in der API-Referenz für Amazon Data Lifecycle Manager.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

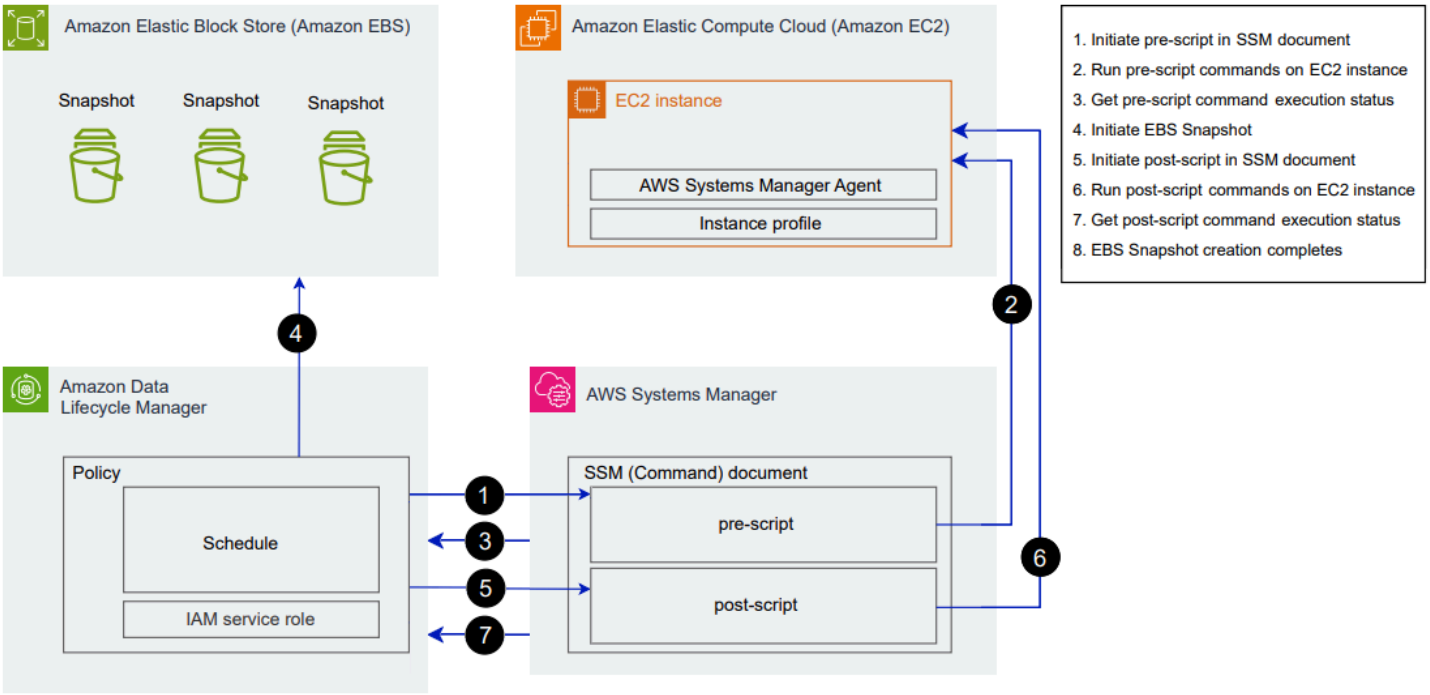
Wenn `policyDetails.json` Folgendes umfasst.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE" | "POST" | "PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
```

```
}
```

So funktionieren Pre- und Post-Skripts von Amazon Data Lifecycle Manager

Die folgende Abbildung zeigt den Prozessablauf für Vor- und Nach-Skripte bei der Verwendung benutzerdefinierter SSM-Dokumente. Dies gilt nicht für VSS-Backups.



Zum geplanten Zeitpunkt der Snapshot-Erstellung finden die folgenden Aktionen und dienstübergreifenden Interaktionen statt.

1. Amazon Data Lifecycle Manager initiiert die Vor-Skript-Aktion durch Aufrufen des SSM-Dokuments und Übergeben des Parameters `pre-script`.

   > **Note**
   >
   > Die Schritte 1 bis 3 finden nur statt, wenn Sie Vor-Skripte ausführen. Wenn Sie nur Nach-Skripte ausführen, werden die Schritte 1 bis 3 übersprungen.

2. Systems Manager sendet Vor-Skript-Befehle an den SSM-Agent, der auf den Ziel-Instances ausgeführt wird. Der SSM-Agent führt die Befehle auf der Instance aus und sendet Statusinformationen zurück an Systems Manager.

Wenn das SSM-Dokument beispielsweise zur Erstellung anwendungskonsistenter Snapshots verwendet wird, friert das Pre-Skript möglicherweise ein und wird geleert, I/O um sicherzustellen, dass alle gepufferten Daten auf das Volume geschrieben werden, bevor der Snapshot erstellt wird.

3. Systems Manager sendet Statusaktualisierungen zu dem Vor-Skript-Befehl an Amazon Data Lifecycle Manager. Wenn das Vor-Skript fehlschlägt, führt Amazon Data Lifecycle Manager je nachdem, wie Sie die Optionen vor und nach dem Skript konfigurieren, eine der folgenden Aktionen aus:

Erneute Versuche	Standardmäßig absturzkonsistente Snapshots	Action
Aktiviert mit verbleibenden Wiederhol versuchen	Aktiviert	Führen Sie das Skript erneut aus, bis es erfolgreich ist oder die Wiederholversuche erschöpft sind
Ohne erfolgrei chen Abschluss erschöpft	Aktiviert	Erstellen Sie absturzkonsistente Snapshots und führen Sie kein Nach-Skript aus.
Aktiviert mit verbleibenden Wiederhol versuchen	Disabled	Führen Sie das Skript erneut aus, bis es erfolgreich ist oder die Wiederholversuche erschöpft sind
Ohne erfolgrei chen Abschluss erschöpft	Disabled	Überspringen Sie die Snapshot-Erstellung für die Ziel-Instance und führen Sie kein Nach-Skript aus.
Disabled	Aktiviert	Erstellen Sie absturzkonsistente Snapshots und führen Sie kein Nach-Skript aus.
Disabled	Disabled	Überspringen Sie die Snapshot-Erstellung für die Ziel-Instance und führen Sie kein Nach-Skript aus.

4. Amazon Data Lifecycle Manager initiiert die Snapshot-Erstellung.
5. Amazon Data Lifecycle Manager initiiert die Nach-Skript-Aktion durch Aufrufen des SSM-Dokuments und Übergeben des Parameters `post-script`.

> **Note**
>
> Die Schritte 5 bis 7 finden nur statt, wenn Sie Vor-Skripte ausführen. Wenn Sie nur Nach-Skripte ausführen, werden die Schritte 1 bis 3 übersprungen.

6. Systems Manager sendet Nach-Skript-Befehle an den SSM-Agent, der auf den Ziel-Instances ausgeführt wird. Der SSM-Agent führt die Befehle auf der Instance aus und sendet Statusinformationen zurück an Systems Manager.

   Wenn das SSM-Dokument beispielsweise anwendungskonsistente Snapshots ermöglicht, taut dieses Postscript möglicherweise auf, I/O um sicherzustellen, dass Ihre Datenbanken nach der Erstellung des Snapshots den normalen Betrieb wieder aufnehmen. I/O
7. Wenn Sie ein Nach-Skript ausführen und Systems Manager anzeigt, dass es erfolgreich abgeschlossen wurde, ist der Vorgang abgeschlossen.

   Wenn das Nach-Skript fehlschlägt, führt Amazon Data Lifecycle Manager je nachdem, wie Sie die Optionen vor und nach dem Skript konfigurieren, eine der folgenden Aktionen aus:

Erneute Versuche	Action
Aktiviert mit verbleibenden Wiederholversuchen	Führen Sie das Nach-Skript erneut aus, bis es erfolgreich ist oder die Wiederholversuche erschöpft sind
Erschöpft ohne Erfolg	Nach-Skript überspringen
Disabled	Nach-Skript überspringen

Hinweis: Wenn das Nach-Skript fehlschlägt, wurde das Vor-Skript (falls aktiviert) erfolgreich abgeschlossen und die Snapshots wurden möglicherweise erstellt. Möglicherweise müssen Sie weitere Maßnahmen an der Instance ergreifen, um sicherzustellen, dass sie erwartungsgemäß funktioniert. Wenn beispielsweise das Pre-Skript angehalten und geleert wurde, das Post-Skript jedoch nicht aufgetaut werden konnte I/O, müssen Sie möglicherweise Ihre Datenbank

so konfigurieren I/O, dass es automatisch auftaut, I/O oder Sie müssen das Auftauen manuell durchführen. I/O

8. Der Snapshot-Erstellungsprozess wird möglicherweise abgeschlossen, nachdem das Nach-Skript abgeschlossen ist. Wie viel Zeit das Abschließen des Snapshots in Anspruch nimmt, hängt von der Snapshot-Größe ab.

Identifizieren Sie Snapshots, die mit den Pre- und Post-Skripten von Data Lifecycle Manager erstellt wurden

Amazon Data Lifecycle Manager weist Snapshots, die mit Vor- und Nach-Skripten erstellt wurden, automatisch die folgenden System-Tags zu.

- Schlüssel: `aws:dlm:pre-script`; Wert: `SUCCESS|FAILED`

  Der Tag-Wert von `SUCCESS` gibt an, dass das Vor-Skript erfolgreich ausgeführt wurde. Der Tag-Wert von `FAILED` gibt an, dass das Vor-Skript nicht erfolgreich ausgeführt wurde.

- Schlüssel: `aws:dlm:post-script`; Wert: `SUCCESS|FAILED`

  Der Tag-Wert von `SUCCESS` gibt an, dass das Nach-Skript erfolgreich ausgeführt wurde. Der Tag-Wert von `FAILED` gibt an, dass das Nach-Skript nicht erfolgreich ausgeführt wurde.

Bei benutzerdefinierten SSM-Dokumenten und SAP HANA-Sicherungen können Sie auf eine erfolgreiche anwendungskonsistente Snapshot-Erstellung schließen, wenn der Snapshot sowohl mit `aws:dlm:pre-script:SUCCESS` als auch `aws:dlm:post-script:SUCCESS` getaggt ist.

Darüber hinaus werden anwendungskonsistente Snapshots, die mit VSS-Backup erstellt wurden, automatisch mit folgenden Tags versehen:

- Schlüssel: `AppConsistent tag`; Wert: `true|false`

  Ein Tag-Wert von `true` gibt an, dass das VSS-Backup erfolgreich war und die Snapshots anwendungskonsistent sind. Ein Tag-Wert von `false` gibt an, dass das VSS-Backup nicht erfolgreich war und die Snapshots nicht anwendungskonsistent sind.

Überwachen Sie Amazon Data Lifecycle Manager vor und nach den Skripten

CloudWatch Amazon-Metriken

Amazon Data Lifecycle Manager veröffentlicht die folgenden CloudWatch Metriken, wenn Pre- und Post-Skripts fehlschlagen und erfolgreich sind und wenn VSS-Backups fehlschlagen und erfolgreich sind.

- `PreScriptStarted`
- `PreScriptCompleted`
- `PreScriptFailed`
- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`
- `VSSBackupCompleted`
- `VSSBackupFailed`

Weitere Informationen finden Sie unter Überwachen Sie die Data Lifecycle Manager-Richtlinien mit CloudWatch.

Amazon EventBridge

Amazon Data Lifecycle Manager gibt das folgende EventBridge Amazon-Ereignis aus, wenn ein Pre- oder Post-Skript initiiert wird, erfolgreich ist oder fehlschlägt

- `DLM Pre Post Script Notification`

Weitere Informationen finden Sie unter Überwachen Sie die Data Lifecycle Manager-Richtlinien mit EventBridge.

Erstellen Sie eine benutzerdefinierte Amazon Data Lifecycle Manager-Richtlinie für EBS-backed AMIs

Das folgende Verfahren zeigt Ihnen, wie Sie Amazon Data Lifecycle Manager verwenden, um EBS-backed AMI-Lebenszyklen zu automatisieren.

Themen

- Erstellen einer AMI-Lebenszyklusrichtlinie
- Überlegungen zu AMI-Lebenszyklusrichtlinien
- Weitere Ressourcen

Erstellen einer AMI-Lebenszyklusrichtlinie

Verwenden Sie eines der folgenden Verfahren, um eine AMI-Lebenszyklusrichtlinie zu erstellen.

Console

So erstellen Sie eine AMI-Richtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store und Lifecycle Manager aus. Wählen Sie dann Create lifecycle policy (Lebenszyklusrichtlinie erstellen) aus.
3. Wählen Sie auf dem Bildschirm „Richtlinientyp auswählen“ die Option EBS-backed AMI-Richtlinie und dann Weiter aus.
4. Wählen Sie im Abschnitt Zielressourcen für Zielressourcen-Tags die Ressourcen-Tags aus, die die zu sichernden Volumes oder Instances identifizieren. Die Richtlinie sichert nur die Ressourcen mit den angegebenen Tag (Markierung)-Schlüssel-Wert-Paaren.
5. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Richtlinie ein.
6. Wählen Sie für IAM-Rolle die IAM-Rolle aus, die über Berechtigungen zum Verwalten von AMIs und Snapshots sowie zum Beschreiben von Instances verfügt. Um die von Amazon Data Lifecycle Manager bereitgestellte Standardrolle zu verwenden, wählen Sie Standardrolle. Um alternativ eine benutzerdefinierte IAM-Rolle zu verwenden, die Sie zuvor erstellt haben, wählen Sie Andere Rolle auswählen und dann die zu verwendende Rolle aus.

7. Fügen Sie für Richtlinien-Tags die Tags hinzu, die auf die Lebenszyklusrichtlinie angewendet werden sollen. Sie können diese Tags (Markierungen) verwenden, um Ihre Richtlinien zu identifizieren und zu kategorisieren.
8. Wählen Sie für Richtlinienstatus nach der Erstellung die Option Richtlinie aktivieren, um die Ausführungen der Richtlinie zum nächsten eingeplanten Zeitpunkt zu starten oder Richtlinie deaktivieren, um zu verhindern, dass die Richtlinie ausgeführt wird. Wenn Sie die Richtlinie jetzt nicht aktivieren, beginnt sie erst mit der Erstellung von AMIs, wenn Sie sie nach der Erstellung manuell aktivieren.
9. Geben Sie im Abschnitt Instance-Neustart an, ob Instances vor der AMI-Erstellung neu gestartet werden sollen. Um zu verhindern, dass die Zielinstances neu gestartet werden, wählen Sie Nein. Die Auswahl von Nein kann zu Problemen mit der Datenkonsistenz führen. Um Instances vor der AMI-Erstellung neu zu starten, wählen Sie Ja. Die Wahl dieser Option gewährleistet die Datenkonsistenz, könnte jedoch dazu führen, dass mehrere abgezielte Instances gleichzeitig neu gestartet werden.
10. Wählen Sie Weiter aus.
11. Konfigurieren Sie auf dem Bildschirm Zeitplan konfigurieren die Richtlinienzeitpläne. Eine Richtlinie kann bis zu vier Zeitpläne aufweisen. Zeitplan 1 ist obligatorisch. Die Zeitpläne 2, 3 und 4 sind optional. Gehen Sie für jeden Richtlinienzeitplan, den Sie hinzufügen, wie folgt vor:

    a. Gehen Sie im Abschnitt Zeitplandetails wie folgt vor:

        i. Geben Sie für Zeitplanname einen beschreibenden Namen für den Zeitplan an.

        ii. Konfigurieren Sie für Häufigkeit und die zugehörigen Felder das Intervall zwischen Richtlinienausführungen.

            Sie können Richtlinienausführungen nach einem täglichen, wöchentlichen, monatlichen oder jährlichen Zeitplan konfigurieren. Alternativ können Sie Custom cron expression (Benutzerdefinierter Cron-Ausdruck) wählen, um ein Intervall von bis zu 1 Jahr anzugeben. Weitere Informationen finden Sie unter Cron- und Rate-Ausdrücke im EventBridge Amazon-Benutzerhandbuch.

        iii. Geben Sie für Starten um die Zeit an, zu der die Richtlinienausführungen gestartet werden sollen. Die erste Richtlinienausführung beginnt innerhalb einer Stunde nach der geplanten Zeit. Die Uhrzeit muss im `hh:mm` UTC-Format eingegeben werden.

        iv. Geben Sie für Aufbewahrungstyp die Aufbewahrungsrichtlinie für AMIs an, die vom Zeitplan erstellt wurden.

Sie können AMIs basierend auf ihrer Gesamtzahl oder ihrem Alter aufbewahren.

Für die anzahlbasierte Aufbewahrung liegt der Bereich zwischen 1 und `1000`. Nach Erreichen der maximalen Anzahl wird die Registrierung des ältesten Snapshotes oder des ältesten AMIs aufgehoben, wenn ein neuer oder ein neues erstellt wird.

Für die auf dem Alter basierende Aufbewahrung reicht die Spanne von 1 Tag bis `100` Jahre. Nach Ablauf des Aufbewahrungszeitraums des Snapshots oder AMI wird die Registrierung aufgehoben.

> **Note**
>
> Alle Zeitpläne müssen denselben Aufbewahrungstyp haben. Sie können den Aufbewahrungstyp nur für Zeitplan 1 angeben. Die Zeitpläne 2, 3 und 4 erben den Aufbewahrungstyp aus Plan 1. Jeder Zeitplan kann über eine eigene Aufbewahrungsanzahl oder einen eigenen Zeitraum verfügen.

b. Konfigurieren Sie die Markierung für AMIs.

Gehen Sie im Abschnitt Tag (Markierung) wie folgt vor:

i. Um alle benutzerdefinierten Tags aus der Quell-Instance in die vom Zeitplan erstellten AMIs zu kopieren, wählen Sie Tags aus Quelle kopieren aus.

ii. Standardmäßig werden AMIs, die durch den Zeitplan erstellt wurden, automatisch mit der ID der Quell-Instance gekennzeichnet. Um dieses automatische Markieren zu verhindern, entfernen Sie bei Variablen-Tags (Markierungen) die `instance-id:$(instance-id)`-Kachel.

iii. Um zusätzliche Tags anzugeben, die den von diesem Zeitplan erstellten AMIs zugewiesen werden sollen, wählen Sie Tags hinzufügen.

c. Konfigurieren Sie die AMI-Veralterung.

Um AMIs zu verwerfen, wenn sie nicht mehr verwendet werden sollten, wählen Sie im Abschnitt AMI-Veraltung den AMI-Veraltung für diesen Zeitplan und geben Sie dann die AMI-Veraltungsregel an. Die AMI-Veraltungsregel gibt an, wann AMIs veraltet werden sollen.

Wenn der Zeitplan eine zahlbasierte AMI-Aufbewahrung verwendet, müssen Sie die Anzahl der ältesten AMIs angeben, die veraltet werden soll. Die Anzahl der

Veraltungszeiten muss kleiner oder gleich der AMI-Aufbewahrungsanzahl des Zeitplans sein und darf nicht größer als 1000 sein. Wenn der Zeitplan beispielsweise so konfiguriert ist, dass maximal 5 AMIs beibehalten werden, können Sie die geplanten bis zu alten 5 ältesten AMIs konfigurieren.

Wenn der Zeitplan eine altersbasierte AMI-Aufbewahrung verwendet, müssen Sie den Zeitraum angeben, nach dem AMIs veraltet werden sollen. Die Anzahl der Veraltungszeiten muss kleiner oder gleich dem AMI-Aufbewahrungszeitraum des Zeitplans sein und darf nicht größer als 10 Jahre sein (120 Monate, 520 Wochen oder 3650 Tage). Wenn der Zeitplan beispielsweise so konfiguriert ist, dass AMIs 10 Tage lang beibehalten werden, können Sie die geplanten AMIs so konfigurieren, dass sie nach Zeiträumen bis zu 10 Tage nach der Erstellung veraltet sind.

d. Konfigurieren Sie das regionsübergreifende Kopieren.

Um die vom Zeitplan erstellten AMIs in verschiedene Regionen zu kopieren, wählen Sie im Abschnitt Cross-Region Kopieren die Option Regionsübergreifendes Kopieren aktivieren aus. Sie können AMIs in bis zu drei zusätzliche Regionen in Ihrem Konto kopieren. Sie müssen für jede Zielregion eine separate regionsübergreifende Kopierregel angeben.

Sie können für jede Zielregion Folgendes angeben:

- Eine Aufbewahrungsregel für die AMI-Kopie. Wenn der Aufbewahrungszeitraum abgläuft, wird die Kopie in der Zielregion automatisch aufgehoben.
- Verschlüsselungsstatus für die AMI Kopie. Wenn das Quell-AMI verschlüsselt ist oder die standardmäßige Verschlüsselung aktiviert ist, werden die kopierten AMIs stets verschlüsselt. Wenn der Quell-AMI unverschlüsselt ist und die Verschlüsselung standardmäßig deaktiviert ist, können Sie optional die Verschlüsselung aktivieren. Wenn Sie keinen Verschlüsselung angeben, werden die AMIs mit dem Standard-Verschlüsselung für die EBS-Verschlüsselung in jeder Zielregion verschlüsselt. Wenn Sie einen Verschlüsselung für die Zielregion angeben, muss die ausgewählte IAM-Rolle Zugriff auf das Verschlüsselung haben.
- Eine Veraltungsregel für die AMI Kopie. Wenn die Veraltungsperiode abgelaufen ist, wird die AMI-Kopie automatisch veraltet. Die Veraltungsfrist muss kleiner oder gleich dem Kopieraufbewahrungszeitraum sein und darf nicht länger als 10 Jahre sein.
- Ob alle Tags oder keine Tags aus dem Quell-AMI kopiert werden sollen.

> **Note**
>
> Überschreiten Sie nicht die Anzahl gleichzeitiger AMI-Kopien pro Region.

e. Um weitere Zeitpläne hinzuzufügen, wählen Sie die Option Weiteren Zeitplan hinzufügen, die sich oben auf dem Bildschirm befindet. Füllen Sie für jeden zusätzlichen Zeitplan die Felder wie oben in diesem Thema beschrieben aus.

f. Nachdem Sie die erforderlichen Zeitpläne hinzugefügt haben, wählen Sie Richtlinie überprüfen aus.

12. Überprüfen Sie die Richtlinienzusammenfassung und wählen Sie dann Richtlinie erstellen aus.

> **Note**
>
> Falls Sie den Fehler `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` erhalten, finden Sie weitere Informationen unter Beheben Sie Probleme mit Amazon Data Lifecycle Manager.

Command line

Verwenden Sie den Befehl create-lifecycle-policy, um eine AMI-Lebenszyklus-Richtlinie zu erstellen. Legen Sie für `PolicyType` die Option `IMAGE_MANAGEMENT` fest.

> **Note**
>
> Zur Vereinfachung der Syntax wird in den folgenden Beispielen eine JSON-Datei `policyDetails.json` verwendet, die die Richtliniendetails enthält.

Beispiel 1: Age-based Aufbewahrung und AMI-Abwertung

In diesem Beispiel wird eine AMI-Lebenszyklusrichtlinie erstellt, die AMIs aller Instances erstellt, die einen Tag (Markierung)-Schlüssel `purpose` mit einem Wert von `production` haben, ohne die Ziel-Instances neu zu starten. Die Richtlinie enthält einen Zeitplan, der jeden Tag um `01:00`

Uhr UTC ein AMI erstellt. Die Richtlinie behält AMIs für 2 Tage und veraltet sie nach 1 Tagen. Sie kopiert die Tags (Markierungen) auch von der Quell-Instance in die AMIs, die sie erstellt.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
```

```
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
}
```

Wenn die Anforderung erfolgreich ist, gibt der Befehl die ID der neu erstellten Richtlinie zurück. Es folgt eine Beispielausgabe.

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

Beispiel 2: Count-based Aufbewahrung und AMI-Abwertung mit regionsübergreifendem Kopieren

In diesem Beispiel wird eine AMI-Lebenszyklusrichtlinie erstellt, die AMIs aller Instances erstellt, die einen Tag (Markierung)-Schlüssel `purpose` mit einem Wert von `production` haben und startet die Ziel-Instances neu. Die Richtlinie enthält einen Zeitplan, der täglich alle 6 Stunden, beginnend um `17:30` Uhr UTC, ein AMI erstellt. Die Richtlinie behält 3-AMIs und veraltet automatisch die 2 ältesten AMIs. Es verfügt auch über eine regionsübergreifende Kopierregel, die AMIs nach `us-east-1` kopiert, 2-AMI-Kopien behält und automatisch das älteste AMI veraltet.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Das folgende Beispiel zeigt eine `policyDetails.json`-Datei.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
```

```
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
                "IntervalUnit": "DAYS",
                "Interval": 1
            },
            "CopyTags": true
        }]
    }]
}
```

Überlegungen zu AMI-Lebenszyklusrichtlinien

Die folgenden allgemeinen Überlegungen gelten für die Erstellung von AMI-Lebenzyklusrichtlinien:

- AMI-Lebenszyklusrichtlinien zielen nur auf Instances ab, die sich in derselben Region wie die Richtlinie befinden.

- Der erste AMI-Erstellungsvorgang beginnt innerhalb einer Stunde nach der angegebenen Startzeit. Nachfolgende AMI-Erstellungsvorgänge beginnen innerhalb einer Stunde nach ihrer geplanten Zeit.
- Wenn Amazon Data Lifecycle Manager ein AMI abmeldet, löscht er es automatisch mit Snapshots zum Backup.
- Bei Zielressourcen-Tags muss die Groß-/Kleinschreibung beachtet werden.
- Wenn Sie die Ziel-Tags von einer Instance entfernen, auf die eine Richtlinie abzielt, verwaltet Amazon Data Lifecycle Manager die vorhandenen AMIs im Standard-Tier nicht mehr; Sie müssen sie manuell löschen, wenn sie nicht mehr benötigt werden.
- Sie können mehrere Richtlinien zum Sichern einer Instance erstellen. Wenn eine Instance zwei Tags hat, wobei Tag A das Ziel für Richtlinie A ist, alle 12 Stunden ein AMI zu erstellen, und Tag B das Ziel für Richtlinie B, alle 24 Stunden ein AMI zu erstellen, erstellt Amazon Data Lifecycle Manager AMIs gemäß den Zeitplänen für beide Richtlinien. Alternativ können Sie dasselbe Ergebnis erzielen, indem Sie eine einzelne Richtlinie mit mehreren Zeitplänen erstellen. Sie können beispielsweise eine einzelne Richtlinie erstellen, die nur auf Tag (Markierung) Aabzielt, und zwei Zeitpläne angeben – einen für alle 12 Stunden und einen für alle 24 Stunden.
- Neue Volumes, die an eine Ziel-Instance angehängt werden, nachdem die Richtlinie erstellt wurde, werden bei der nächsten Richtlinienausführung automatisch in das Backup einbezogen. Alle Volumes, die zum Zeitpunkt der Richtlinienausführung mit der Instance verbunden sind, sind enthalten.
- Wenn Sie eine Richtlinie mit einem benutzerdefinierten Cron-basierten Zeitplan so erstellen und konfigurieren, dass nur ein AMI erstellt wird, wird die Richtlinie dieses AMI nicht automatisch abmelden, wenn der Aufbewahrungsschwellenwert erreicht ist. Sie müssen das AMI manuell abmelden, wenn es nicht mehr benötigt wird.
- Wenn Sie eine altersbasierte Richtlinie erstellen, bei der der Aufbewahrungszeitraum kürzer ist als die Erstellungshäufigkeit, behält Amazon Data Lifecycle Manager immer den letzten AMI bei, bis der nächste erstellt wird. Wenn zum Beispiel eine altersbasierte Richtlinie jeden Monat einen AMI mit einer Aufbewahrungsfrist von sieben Tagen erstellt, behält Amazon Data Lifecycle Manager jeden AMI einen Monat lang bei, obwohl die Aufbewahrungsfrist sieben Tage beträgt.
- Bei auf der Anzahl basierenden Richtlinien erstellt Amazon Data Lifecycle Manager immer AMIs entsprechend der Erstellungshäufigkeit, bevor er versucht, das älteste AMI gemäß der Aufbewahrungsrichtlinie zu deregistrieren.
- Es kann mehrere Stunden dauern, bis ein AMI erfolgreich aus der Registrierung abgemeldet wird und die zugehörigen Backup-Snapshots gelöscht sind. Wenn Amazon Data Lifecycle Manager das

nächste AMI erstellt, bevor das zuvor erstellte AMI erfolgreich aus der Registrierung abgemeldet wurde, können Sie vorübergehend eine Anzahl von AMIs beibehalten, die größer ist als Ihre Aufbewahrungsanzahl.

Die folgenden Überlegungen gelten für das Beenden von Instances, die Ziel einer Richtlinie sind:

- Wenn Sie eine Instance beenden, die Ziel einer Richtlinie mit einem anzahlbasierten Aufbewahrungsplan war, verwaltet die Richtlinie die AMIs nicht mehr, die zuvor von der beendeten Instance erstellt wurden. Sie müssen diese früheren AMIs manuell abmelden, wenn sie nicht mehr benötigt werden.
- Wenn Sie eine Instance beenden, die Ziel einer Richtlinie mit einem altersbasierten Aufbewahrungszeitplan war, meldet die Richtlinie zuvor von der beendeten Instance erstellte AMIs weiterhin nach dem definierten Zeitplan bis zum letzten AMI aber nicht einschließlich des letzten AMI ab. Sie müssen das letzte AMI manuell abmelden, wenn es nicht mehr benötigt wird.

Die folgenden Überlegungen gelten für AMI-Richtlinien und AMI-Veralterung:

- Wenn Sie die AMI-Veraltungsanzahl für einen Zeitplan mit zählbasierter Aufbewahrung erhöhen, wird die Änderung auf alle AMIs (vorhandene und neue) angewendet, die durch den Zeitplan erstellt wurden.
- Wenn Sie den AMI-Veraltungszeitraum für einen Zeitplan mit altersbasierter Aufbewahrung erhöhen, wird die Änderung nur auf neue AMIs angewendet. Vorhandene AMIs sind nicht betroffen.
- Wenn Sie die AMI-Abwärtsregel aus einem Zeitplan entfernen, wird Amazon Data Lifecycle Manager die Veraltungsregel für AMIs, die zuvor durch diesen Zeitplan veraltet waren, nicht abbrechen.
- Wenn Sie die AMI-Veraltungsanzahl oder -periode für einen Zeitplan verringern, wird Amazon Data Lifecycle Manager die Verwarnung für AMIs, die zuvor durch diesen Zeitplan veraltet waren, nicht abbrechen.
- Wenn Sie ein AMI, das mit einer AMI-Richtlinie erstellt wurde, manuell verwerfen, überschreibt Amazon Data Lifecycle Manager die Veraltungsphase nicht.
- Wenn Sie die Veraltung für ein AMI manuell abbrechen, das zuvor durch eine AMI-Richtlinie veraltet wurde, überschreibt Amazon Data Lifecycle Manager die Stornierung nicht.
- Wenn ein AMI durch mehrere in Konflikt stehende Zeitpläne erstellt wird und für einen oder mehrere dieser Zeitpläne keine AMI-Veraltungsregel vorhanden ist, wird Amazon Data Lifecycle Manager dieses AMI nicht veraltet.

- Wenn ein AMI durch mehrere in Konflikt stehende Zeitpläne erstellt wird und alle diese Zeitpläne über eine AMI-Ablehnungsregel verfügen, verwendet Amazon Data Lifecycle Manager die Veralterungsregel, die zum letzten Veralterungsdatum führt.

Die folgenden Überlegungen gelten für AMI-Richtlinien und den Papierkorb:

- Wenn Amazon Data Lifecycle Manager ein AMI abmeldet und es an den Papierkorb sendet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht ist, und Sie dieses AMI manuell aus dem Papierkorb wiederherstellen, müssen Sie das AMI manuell abmelden, wenn es nicht mehr benötigt wird. Amazon Data Lifecycle Manager verwaltet die AMI nicht mehr.
- Wenn Sie eine AMI, die durch eine Richtlinie erstellt wurde, manuell abmelden und diese AMI sich im Papierkorb befindet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht ist, wird Amazon Data Lifecycle Manager die AMI nicht abmelden. Amazon Data Lifecycle Manager verwaltet die AMIs nicht, während sie im Papierkorb sind.

  Wenn die AMI aus dem Papierkorb wiederhergestellt wird, bevor der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, meldet Amazon Data Lifecycle Manager die AMI ab, sobald der Aufbewahrungsschwellenwert der Richtlinie erreicht wird.

  Wenn die AMI aus dem Papierkorb wiederhergestellt wird, nachdem der Aufbewahrungsschwellenwert der Richtlinie erreicht wurde, meldet Amazon Data Lifecycle Manager die AMI nicht mehr ab. Sie müssen ihn manuell löschen, wenn er nicht mehr benötigt wird.

Die folgenden Überlegungen gelten für AMI-Richtlinien, die sich im error-Status befinden:

- Bei Richtlinien mit altersbasierten Aufbewahrungszeitplänen werden AMIs, deren Aufbewahrungszeiträume ablaufen, während sich die Richtlinie im `error`-Status befindet, auf unbestimmte Zeit aufbewahrt. Die AMIs müssen Sie manuell abmelden. Wenn Sie die Richtlinie erneut aktivieren, setzt Amazon Data Lifecycle Manager das Abmelden von AMIs fort, wenn ihre Aufbewahrungszeiträume ablaufen.
- Bei Richtlinien mit anzahlbasierten Aufbewahrungszeitplänen stoppt die Richtlinie das Erstellen und Abmelden von AMIs, während sie sich im `error`-Status befindet. Wenn Sie die Richtlinie erneut aktivieren, setzt Amazon Data Lifecycle Manager das Erstellen von AMIs sowie das Abmelden von AMIs bei Erreichen des Aufbewahrungsschwellenwerts fort.

Die folgenden Überlegungen gelten für AMI-Richtlinien und das Deaktivieren von AMIs:

- Wenn Sie ein AMI, das von Amazon Data Lifecycle Manager erstellt wurde, deaktivieren und dieses AMI bei Erreichen des Aufbewahrungsschwellenwerts deaktiviert wird, meldet Amazon Data Lifecycle Manager das AMI ab und löscht die zugehörigen Snapshots.
- Wenn Sie ein von Amazon Data Lifecycle Manager erstelltes AMI deaktivieren und die zugehörigen Snapshots manuell archivieren und diese Snapshots archiviert werden, wenn ihr Aufbewahrungsschwellenwert erreicht ist, löscht Amazon Data Lifecycle Manager diese Snapshots nicht und verwaltet sie nicht mehr.

Die folgenden Überlegungen gelten für AMI-Richtlinien und den AMI-Deregistrierungsschutz:

- Wenn Sie den Abmeldeschutz für ein AMI, das von Amazon Data Lifecycle Manager erstellt wurde, manuell aktivieren und er immer noch aktiviert ist, wenn der AMI-Aufbewahrungsschwellenwert erreicht ist, verwaltet Amazon Data Lifecycle Manager dieses AMI nicht mehr. Sie müssen das AMI manuell abmelden und die zugrunde liegenden Snapshots löschen, wenn es nicht mehr benötigt wird.

Weitere Ressourcen

Weitere Informationen finden Sie im Blog Automating Amazon EBS Snapshot and AMI Management using Amazon Data Lifecycle Manager Storage. AWS

Automatisieren Sie kontoübergreifende Snapshot-Kopien mit Data Lifecycle Manager

Die Automatisierung kontoübergreifender Snapshot-Kopien ermöglicht es Ihnen, Ihre Amazon-EBS-Snapshots in bestimmte Regionen in einem isolierten Konto zu kopieren und diese Snapshots mit einem Verschlüsselungsschlüssel zu verschlüsseln. Auf diese Weise können Sie sich vor Datenverlust schützen, falls Ihr Konto kompromittiert wird.

Die Automatisierung von kontenübergreifenden Snapshots umfasst zwei Konten:

- Source account (Quellkonto)—Das Quellkonto ist das Konto, das die Snapshots erstellt und mit dem Zielkonto teilt. In diesem Konto müssen Sie eine EBS-Snapshot-Richtlinie erstellen, die in festgelegten Intervallen Snapshots erstellt und diese dann mit anderen Konten teilt. AWS

- Target account (Zielkonto)—Das Zielkonto ist das Konto mit dem Zielkonto, für das die Snapshots freigegeben werden, und es ist das Konto, das Kopien der freigegebenen Snapshots erstellt. In diesem Konto müssen Sie eine Richtlinie für kontoübergreifende Kopierereignisse erstellen, die automatisch Snapshots kopiert, die von einem oder mehreren angegebenen Quellkonten mit ihm geteilt werden.

> **Note**
>
> Sowohl die EBS-Snapshot-Richtlinie für das Quellkonto als auch die Event-Richtlinie für kontoübergreifendes Kopieren des Zielkontos müssen in derselben Region erstellt werden. AWS Das Zielkonto kann dann bei Bedarf Snapshots in verschiedene Zielregionen kopieren.

Themen

- Kontoübergreifende Richtlinien für Snapshot-Kopierrichtlinien
- Festlegen von Snapshot-Beschreibungsfiltern
- Überlegungen zu Richtlinien für das kontoübergreifende Kopieren von Snapshots
- Weitere Ressourcen

Kontoübergreifende Richtlinien für Snapshot-Kopierrichtlinien

Um die Quell- und Zielkonten für das kontoübergreifende Snapshot-Kopieren vorzubereiten, müssen Sie die folgenden Schritte ausführen:

Schritt 1: Erstellen Sie die EBS-Snapshot-Richtlinie (Quellkonto)

Erstellen Sie im Quellkonto eine EBS-Snapshot-Richtlinie, die die Snapshots erstellt und mit den erforderlichen Zielkonten teilt.

Stellen Sie beim Erstellen der Richtlinie sicher, dass Sie die kontoübergreifende gemeinsame Nutzung aktivieren und die AWS Zielkonten angeben, mit denen die Snapshots geteilt werden sollen. Dies sind die Konten, mit denen die Snapshots geteilt werden sollen. Wenn Sie verschlüsselte Snapshots freigeben, müssen Sie den ausgewählten Zielkonten die Berechtigung erteilen, das zum Verschlüsseln des Quell-Volume verwendeten Verschlüsselung zu verwenden. Weitere Informationen finden Sie unter Schritt 2: Teilen Sie den vom Kunden verwalteten Schlüssel (Quellkonto).

> **Note**
>
> - Erstellen Sie diese Richtlinie in derselben AWS Region, in der Sie in Schritt 3 die kontoübergreifende Kopierereignisrichtlinie für das Zielkonto erstellen werden. Beide Richtlinien müssen sich in derselben Region befinden, damit das kontoübergreifende Teilen von Snapshots ordnungsgemäß funktioniert.
> - Sie können nur Snapshots freigeben, die unverschlüsselt oder mit einem Kundenverwalteter Schlüssel verschlüsselt sind. Sie können keine Snapshots freigeben, die mit dem standardmäßigen EBS-Verschlüsselungs-Verschlüsselung verschlüsselt sind. Wenn Sie verschlüsselte Snapshots teilen, müssen Sie auch den Verschlüsselung, der zum Verschlüsseln des Quell-Volumes verwendet wurde, mit den Zielkonten teilen. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch.

Weitere Informationen zum Erstellen einer EBS-Snapshot-Richtlinie finden Sie unter Erstellen Sie eine benutzerdefinierte Amazon Data Lifecycle Manager-Richtlinie für EBS-Snapshots.

Verwenden Sie eine der folgenden Methoden, um die EBS-Snapshot-Richtlinie zu erstellen.

Schritt 2: Teilen Sie den vom Kunden verwalteten Schlüssel (Quellkonto)

Wenn Sie verschlüsselte Snapshots freigeben, müssen Sie der IAM-Rolle und den Ziel- AWS -Konten (die Sie im vorherigen Schritt ausgewählt haben) Berechtigungen erteilen, um den vom Kunden verwalteten Schlüssel zu verwenden, der zum Verschlüsseln des Quell-Volumes verwendet wurde.

> **Note**
>
> Führen Sie diesen Schritt nur aus, wenn Sie verschlüsselte Snapshots freigeben. Wenn Sie unverschlüsselte Snapshots freigeben, überspringen Sie diesen Schritt.

Console

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

3. Wählen Sie im Navigationsbereich Customer managed key (Vom Kunden verwalteter Schlüssel) und dann den KMS-Schlüssel aus, den Sie für die Zielkonten freigeben müssen.

   Notieren Sie sich den ARN des Verschlüsselung, den Sie später benötigen.

4. Scrollen Sie auf der Registerkarte Key policy (Schlüsselrichtlinie) nach unten zum Abschnitt Key users (Schlüsselbenutzer). Wählen Sie Hinzufügen, geben Sie den Namen der IAM-Rolle ein, die Sie im vorherigen Schritt ausgewählt haben, und wählen Sie dann Hinzufügen aus.
5. Scrollen Sie auf der Registerkarte Schlüsselrichtlinie nach unten zum Abschnitt Andere AWS -Konten. Wählen Sie Weitere AWS Konten hinzufügen und fügen Sie dann alle AWS Zielkonten hinzu, mit denen Sie die Snapshots im vorherigen Schritt geteilt haben.
6. Wählen Sie Save Changes.

Command line

Verwenden Sie den Befehl get-key-policy, um die Schlüsselrichtlinie, die derzeit an das Verschlüsselung angehängt ist, zu abzurufen.

Der folgende Befehl ruft beispielsweise die Schlüsselrichtlinie für ein Verschlüsselung mit einer ID von `9d5e2b3d-e410-4a27-a958-19e220d83a1e` ab und schreibt sie in eine Datei namens `snapshotKey.json`.

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

Öffnen Sie die Schlüsselrichtlinie mit Ihrem bevorzugten Texteditor. Fügen Sie den ARN der IAM-Rolle hinzu, die Sie beim Erstellen der Snapshot-Richtlinie angegeben haben, und die ARNs der Zielkonten, mit denen der Verschlüsselung geteilt werden soll.

In der folgenden Richtlinie wird beispielsweise der ARN der Standard-IAM-Rolle zusammen mit dem ARN des Stammkontos für das Zielkonto angegeben `222222222222`.

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu.

Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn der Zuschuss im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
    }
}
```

Speichern Sie die Datei und schließen Sie sie. Verwenden Sie dann den Befehl put-key-policy, um die aktualisierte Schlüsselrichtlinie an das Verschlüsselung anzuhängen.

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

Schritt 3: Event-Richtlinie für kontoübergreifendes Kopieren erstellen (Zielkonto)

Im Zielkonto müssen Sie eine Richtlinie für kontoübergreifende Kopierereignisse erstellen, die automatisch Snapshots kopiert, die von den erforderlichen Quellkonten freigegeben werden.

Diese Richtlinie wird nur auf dem Zielkonto ausgeführt, wenn eines der angegebenen Quellkonten Snapshots mit dem Konto teilt.

> **Note**
>
> Erstellen Sie diese Richtlinie in derselben AWS Region wie die in Schritt 1 erstellte EBS-Snapshot-Richtlinie des Quellkontos. Beide Richtlinien müssen sich in derselben Region befinden, damit das kontoübergreifende Teilen von Snapshots ordnungsgemäß funktioniert. Sie können diese Richtlinie dann so konfigurieren, dass Snapshots nach Bedarf in verschiedene Zielregionen kopiert werden.

Verwenden Sie eine der folgenden Methoden, um die Richtlinie für kontoübergreifende Kopierereignisse zu erstellen.

Console

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store und Lifecycle Manager aus. Wählen Sie dann Create lifecycle policy (Lebenszyklusrichtlinie erstellen) aus.

3. Wählen Sie im Bildschirm „Richtlinientyp auswählen“ die Option „Ereignisrichtlinie Cross-account kopieren“ und dann „Weiter“.
4. Geben Sie unter Richtlinienbeschreibung eine kurze Beschreibung der Richtlinie ein.
5. Fügen Sie für Richtlinien-Tags die Tags hinzu, die auf die Lebenszyklusrichtlinie angewendet werden sollen. Sie können diese Tags (Markierungen) verwenden, um Ihre Richtlinien zu identifizieren und zu kategorisieren.
6. Definieren Sie im Abschnitt Ereigniseinstellungen das Snapshot-Freigabeereignis, das die Ausführung der Richtlinie bewirkt. Gehen Sie wie folgt vor:

   a. Geben Sie für Sharing-Konten die AWS Quellkonten an, von denen Sie die geteilten Snapshots kopieren möchten. Wählen Sie Konto hinzufügen, geben Sie die 12-stellige AWS Konto-ID ein und wählen Sie dann Hinzufügen.

   b. Geben Sie für Snapshot-Beschreibungsfilter die erforderliche Snapshot-Beschreibung mit einem regulären Ausdruck ein. Nur Snapshots, die von den angegebenen Quellkonten gemeinsam genutzt werden und Beschreibungen haben, die mit dem angegebenen Filter übereinstimmen, werden von der Richtlinie kopiert. Weitere Informationen finden Sie unter Festlegen von Snapshot-Beschreibungsfiltern.
7. Wählen Sie für die IAM-Rolle die IAM-Rolle aus, die über Berechtigungen zum Durchführen der Aktion zum Kopieren von Snapshots verfügt. Um die von Amazon Data Lifecycle Manager bereitgestellte Standardrolle zu verwenden, wählen Sie Standardrolle. Um alternativ eine benutzerdefinierte IAM-Rolle zu verwenden, die Sie zuvor erstellt haben, wählen Sie Andere Rolle auswählen und dann die zu verwendende Rolle aus.

   Wenn Sie verschlüsselte Snapshots kopieren, müssen Sie der ausgewählten IAM-Rolle Berechtigungen zur Verwendung des zur Verschlüsselung des Quell-Volumes verwendeten Verschlüsselungs-Verschlüsselung erteilen. Wenn Sie den Snapshot in der Zielregion mit einem anderen Verschlüsselung verschlüsseln, müssen Sie der IAM-Rolle die Berechtigung zur Verwendung des Ziel-Verschlüsselung erteilen. Weitere Informationen finden Sie unter Schritt 4: Erlauben Sie der IAM-Rolle, die erforderlichen KMS-Schlüssel zu verwenden (Zielkonto).
8. Definieren Sie im Abschnitt Kopieraktion die Snapshot-Kopieraktionen, die die Richtlinie ausführen soll, wenn sie aktiviert wird. Die Richtlinie kann Snapshots in bis zu drei Regionen kopieren. Sie müssen für jede Zielregion eine separate Kopierregel angeben. Gehen Sie für jede hinzugefügte Regel wie folgt vor:

   a. Geben Sie unter Name einen aussagekräftigen Namen für die Kopieraktion ein.

b. Wählen Sie für Target Region (Zielregion) die Region aus, in die Sie die Snapshots kopieren möchten.

c. Geben Sie unter Ablauf an, wie lange die Snapshot-Kopien nach der Erstellung in der Zielregion aufbewahrt werden sollen.

d. Um die Snapshot-Kopie zu verschlüsseln, wählen Sie für Verschlüsselung die Option Verschlüsselung aktivieren aus. Wenn der Quell-Snapshot verschlüsselt ist oder wenn die Verschlüsselung standardmäßig für Ihr Konto aktiviert ist, wird die Snapshot-Kopie immer verschlüsselt, selbst wenn Sie hier keine Verschlüsselung aktivieren. Wenn der Quell-Snapshot unverschlüsselt ist und die Verschlüsselung für Ihr Konto standardmäßig nicht aktiviert ist, können Sie die Verschlüsselung aktivieren oder deaktivieren. Wenn Sie die Verschlüsselung aktivieren, aber keinVerschlüsselung angeben, werden die Snapshots in jeder Zielregion mit dem Standardverschlüsselungs-Verschlüsselung verschlüsselt. Wenn Sie einenVerschlüsselung für die Zielregion angeben, müssen Sie Zugriff auf den Verschlüsselung haben.

9. Um zusätzliche Snapshot-Kopieraktionen hinzuzufügen, wählen Sie Neue Regionen hinzufügen.
10. Wählen Sie für Richtlinienstatus nach der Erstellung die Option Richtlinie aktivieren, um die Ausführungen der Richtlinie zum nächsten eingeplanten Zeitpunkt zu starten oder Richtlinie deaktivieren, um zu verhindern, dass die Richtlinie ausgeführt wird. Wenn Sie die Richtlinie jetzt nicht aktivieren, beginnt sie erst mit dem Kopieren von Snapshots, wenn Sie sie nach der Erstellung manuell aktivieren.
11. Wählen Sie Richtlinie erstellen aus.

Command line

Verwenden Sie den Befehl create-lifecycle-policy, um eine Richtlinie zu erstellen. Um eine Richtlinie für kontoübergreifende Kopierereignisse `PolicyType` zu erstellen, geben Sie `EVENT_BASED_POLICY` an.

Mit dem folgenden Befehl wird beispielsweise eine Richtlinie für kontoübergreifende Kopierereignisse im Zielkonto `222222222222` erstellt. Die Richtlinie kopiert Snapshots, die vom Quellkonto `111111111111` freigegeben werden. Die Richtlinie kopiert Snapshots nach `sa-east-1` und `eu-west-2`. Snapshots, die in `sa-east-1` kopiert wurden, sind unverschlüsselt und werden 3 Tage lang aufbewahrt. Snapshots, die in `eu-west-2` kopiert werden, werden mit Verschlüsselung `8af79514-350d-4c52-bac8-8985e84171c7` verschlüsselt und 1 Monat lang aufbewahrt. Die Richtlinie verwendet die Standard-IAM-Rolle.

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Im Folgenden werden die Inhalte der `policyDetails.json`-Datei angezeigt.

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-
west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
```

```
}
```

Wenn die Anforderung erfolgreich ist, gibt der Befehl die ID der neu erstellten Richtlinie zurück. Es folgt eine Beispielausgabe.

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

Schritt 4: Erlauben Sie der IAM-Rolle, die erforderlichen KMS-Schlüssel zu verwenden (Zielkonto)

Wenn Sie verschlüsselte Snapshots kopieren, müssen Sie der IAM-Rolle (die Sie im vorherigen Schritt ausgewählt haben) Berechtigungen erteilen, den Kundenverwalteter Schlüssel zu verwenden, der zur Verschlüsselung des Quell-Volumes verwendet wurde.

> **Note**
>
> Führen Sie diesen Schritt nur aus, wenn Sie verschlüsselte Snapshots kopieren. Wenn Sie unverschlüsselte Snapshots kopieren, überspringen Sie diesen Schritt.

Verwenden Sie eine der folgenden Methoden, um die erforderlichen Richtlinien zur IAM-Rolle hinzuzufügen.

Console

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich die Option Roles (Rollen) aus. Suchen Sie nach der IAM-Rolle, die Sie beim Erstellen der Richtlinie für kontoübergreifende Kopierereignisse im vorherigen Schritt ausgewählt haben, und wählen Sie sie aus. Wenn Sie sich für die Verwendung der Standardrolle entschieden haben, wird die Rolle benannt AWSDataLifecycleManagerDefaultRole.
3. Wählen Sie Add inline policy (Inline-Richtlinie hinzufügen) und anschließend die Registerkarte JSON.
4. Ersetzen Sie die vorhandene Richtlinie durch die folgende und geben Sie den ARN des KMS-Schlüssels an, mit dem die Quell-Volumes verschlüsselt wurden und der vom Quellkonto in Schritt 2 für Sie freigegeben wurde.

> **Note**
>
> Wenn Sie von mehreren Quellkonten kopieren, müssen Sie den entsprechenden KMS-Schlüssel-ARN jedes Quellkontos angeben.

Im folgenden Beispiel gewährt die Richtlinie der IAM-Rolle die Berechtigung, Verschlüsselung `1234abcd-12ab-34cd-56ef-1234567890ab` zu verwenden, das vom Quellkonto `111111111111` freigegeben wurde, und Verschlüsselung `4567dcba-23ab-34cd-56ef-0987654321yz`, das im Zielkonto `222222222222` vorhanden ist.

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn die Gewährung im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

5. Wählen Sie Review policy (Richtlinie überprüfen) aus.
6. Geben Sie unter Name einen beschreibenden Namen für die Richtlinie ein, und wählen Sie dann Create policy (Richtlinie erstellen).

Command line

Erstellen Sie mit Ihrem bevorzugten Texteditor eine neue JSON-Datei mit dem Namen `policyDetails.json`. Fügen Sie die folgende Richtlinie hinzu und geben Sie den ARN des KMS-Schlüssels an, mit dem die Quell-Volumes verschlüsselt wurden und der vom Quellkonto in Schritt 2 für Sie freigegeben wurde.

> **Note**
>
> Wenn Sie von mehreren Quellkonten kopieren, müssen Sie den entsprechenden KMS-Schlüssel-ARN jedes Quellkontos angeben.

Im folgenden Beispiel gewährt die Richtlinie der IAM-Rolle die Berechtigung, Verschlüsselung `1234abcd-12ab-34cd-56ef-1234567890ab` zu verwenden, das vom Quellkonto `111111111111` freigegeben wurde, und Verschlüsselung `4567dcba-23ab-34cd-56ef-0987654321yz`, das im Zielkonto `222222222222` vorhanden ist.

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel gewähren kann, wenn der Zuschuss im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
```

```
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

Speichern und schließen Sie die Datei. Verwenden Sie dann den Befehl put-role-policy, um die Richtlinie der IAM-Rolle hinzuzufügen.

Beispiel

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

Festlegen von Snapshot-Beschreibungsfiltern

Wenn Sie die Richtlinie für Snapshot-Kopien im Zielkonto erstellen, müssen Sie einen Snapshot-Beschreibungsfilter angeben. Mit dem Snapshot-Beschreibungsfilter können Sie eine zusätzliche Filterstufe angeben, mit der Sie steuern können, welche Snapshots von der Richtlinie kopiert

werden. Dies bedeutet, dass ein Snapshot nur von der Richtlinie kopiert wird, wenn er von einem der angegebenen Quellkonten gemeinsam genutzt wird, und eine Snapshot-Beschreibung hat, die dem angegebenen Filter entspricht. Mit anderen Worten, wenn ein Snapshot von einem der angegebenen Kurskonten geteilt wird, aber keine Beschreibung hat, die dem angegebenen Filter entspricht, wird er nicht von der Richtlinie kopiert.

Die Beschreibung des Snapshot-Filters muss mit einem regulären Ausdruck angegeben werden. Dies ist ein Pflichtfeld beim Erstellen von Richtlinien für kontoübergreifende Kopierereignisse mit der Konsole und der Befehlszeile. Im Folgenden finden Sie reguläre Beispielausdrücke, die verwendet werden können:

- `.*`—Dieser Filter entspricht allen Snapshot-Beschreibungen. Wenn Sie diesen Ausdruck verwenden, kopiert die Richtlinie alle Snapshots, die von einem der angegebenen Quellkonten gemeinsam genutzt werden.
- `Created for policy: policy-0123456789abcdef0.*`—Dieser Filter stimmt nur mit Snapshots überein, die von einer Richtlinie mit der ID `policy-0123456789abcdef0` erstellt wurden. Wenn Sie einen Ausdruck wie diesen verwenden, werden nur Snapshots, die von einem der angegebenen Quellkonten mit Ihrem Konto geteilt werden und die von einer Richtlinie mit der angegebenen ID erstellt wurden, von der Richtlinie kopiert.
- `.*production.*`—Dieser Filter entspricht jedem Snapshot, der das Wort `production` irgendwo in seiner Beschreibung enthält. Wenn Sie diesen Ausdruck verwenden, kopiert die Richtlinie alle Snapshots, die von einem der angegebenen Quellkonten gemeinsam genutzt werden und die den angegebenen Text in ihrer Beschreibung enthalten.

Überlegungen zu Richtlinien für das kontoübergreifende Kopieren von Snapshots

Die folgenden Überlegungen gelten für Richtlinien für kontoübergreifende Kopierereignisse:

- Die EBS-Snapshot-Richtlinie für das Quellkonto und die Event-Richtlinie für das kontoübergreifende Kopieren des Zielkontos müssen in derselben AWS Region erstellt werden. Nachdem der Snapshot gemeinsam genutzt wurde, kann die Zielkonto-Richtlinie den Snapshot in verschiedene Zielregionen kopieren, wie in den Kopieraktionen angegeben.
- Sie können nur Snapshots kopieren, die unverschlüsselt oder mit einem Kundenverwalteter Schlüssel verschlüsselt sind.

- Sie können eine Richtlinie für kontoübergreifende Kopierereignisse erstellen, um Snapshots zu kopieren, die außerhalb von Amazon Data Lifecycle Manager freigegeben werden.
- Wenn Sie Snapshots im Zielkonto verschlüsseln möchten, muss die IAM-Rolle, die für die Richtlinie für kontoübergreifende Kopierereignisse ausgewählt wurde, über die Berechtigung verfügen, den erforderlichen Verschlüsselung zu verwenden.

Weitere Ressourcen

Weitere Informationen finden Sie im Blog Automatisieren des Kopierens verschlüsselter Amazon EBS-Snapshots zwischen AWS Konten AWS und Speicher.

Ändern Sie die Amazon Data Lifecycle Manager-Richtlinien

Beachten Sie bei der Änderung der Amazon Data Lifecycle Manager-Richtlinien Folgendes:

- Wenn Sie eine AMI- oder Snapshot-Richtlinie ändern, indem Sie ihre Ziel-Tags (Markierungen) entfernen, werden die Volumes oder Instances mit diesen Tags (Markierungen) nicht mehr von der Richtlinie verwaltet.
- Wenn Sie einen Zeitplannamen ändern, werden die unter dem alten Zeitplannamen erstellten Snapshots oder AMIs nicht mehr von der Richtlinie verwaltet.
- Wenn Sie einen altersbasierten Aufbewahrungszeitplan ändern, um ein neues Zeitintervall zu verwenden, wird das neue Intervall nur für neue Snapshots oder AMIs verwendet, die nach der Änderung erstellt wurden. Der neue Zeitplan hat keinen Einfluss auf den Aufbewahrungszeitplan von Snapshots oder AMIs, die vor der Änderung erstellt wurden.
- Sie können den Aufbewahrungszeitplan einer Richtlinie nach der Erstellung nicht von anzahlbasiert auf altersbasiert ändern. Um diese Änderung vorzunehmen, müssen Sie eine neue Richtlinie anlegen.
- Wenn Sie eine Richtlinie mit einem altersbasierten Aufbewahrungszeitplan deaktivieren, werden die Snapshots oder AMIs, deren Aufbewahrungszeiträume ablaufen, während die Richtlinie deaktiviert ist, auf unbestimmte Zeit aufbewahrt. Sie müssen die Snapshots löschen oder die AMIs manuell abmelden. Wenn Sie die Richtlinie erneut aktivieren, setzt Amazon Data Lifecycle Manager das Löschen von Snapshots oder die Deregistrierung von AMIs fort, wenn ihre Aufbewahrungszeiträume ablaufen.
- Wenn Sie eine Richtlinie mit einem auf der Anzahl basierenden Aufbewahrungszeitplan deaktivieren, wird das Erstellen und Löschen von Snapshots oder AMIs durch die Richtlinie

beendet. Wenn Sie die Richtlinie erneut aktivieren, erstellt Amazon Data Lifecycle Manager weiterhin Snapshots und AMIs und löscht weiterhin Snapshots oder AMIs, wenn der Aufbewahrungsschwellenwert erreicht ist.

- Wenn Sie eine Richtlinie deaktivieren, für die eine Snapshot-Archivierung aktiviert ist, werden Snapshots, die sich zum Zeitpunkt der Deaktivierung der Richtlinie auf der Archivstufe befinden, nicht mehr von Amazon Data Lifecycle Manager verwaltet. Sie müssen die Snapshots manuell löschen, wenn sie nicht mehr benötigt werden.
- Wenn Sie die Snapshot-Archivierung nach einem anzahlbasierten Zeitplan aktivieren, gilt die Archivierungsregel für alle neuen Snapshots, die nach dem Zeitplan erstellt und archiviert werden. Sie gilt auch für vorhandene Snapshots, die zuvor nach dem Zeitplan erstellt und archiviert wurden.
- Wenn Sie die Snapshot-Archivierung nach einem altersbasierten Zeitplan aktivieren, gilt die Archivierungsregel nur für neue Snapshots, die nach Aktivierung der Snapshot-Archivierung erstellt werden. Vorhandene Snapshots, die vor der Aktivierung der Snapshot-Archivierung erstellt wurden, werden weiterhin gemäß dem Zeitplan, der bei der ursprünglichen Erstellung und Archivierung dieser Snapshots galt, aus den entsprechenden Speicherstufen gelöscht.
- Wenn Sie die Snapshot-Archivierung für einen anzahlbasierten Zeitplan deaktivieren, wird die Archivierung von Snapshots umgehend gestoppt. Snapshots, die zuvor nach dem Zeitplan archiviert wurden, verbleiben auf der Archivstufe und werden von Amazon Data Lifecycle Manager nicht gelöscht.
- Wenn Sie die Snapshot-Archivierung für einen altersbasierten Zeitplan deaktivieren, werden die durch die Richtlinie erstellten Snapshots, deren Archivierung geplant ist, zum geplanten Archivierungsdatum und zur geplanten Archivierungszeit dauerhaft gelöscht, wie vom System-Tag `aws:dlm:expirationTime` angegeben.
- Wenn Sie die Snapshot-Archivierung für einen Zeitplan deaktivieren, wird die Archivierung von Snapshots umgehend gestoppt. Snapshots, die zuvor nach dem Zeitplan archiviert wurden, verbleiben auf der Archivstufe und werden von Amazon Data Lifecycle Manager nicht gelöscht.
- Wenn Sie die Archivaufbewahrungsanzahl für einen anzahlbasierten Zeitplan ändern, umfasst die neue Aufbewahrungsanzahl vorhandene Snapshots, die zuvor nach dem Zeitplan archiviert wurden.
- Wenn Sie den Archivaufbewahrungszeitraum für einen altersbasierten Zeitplan ändern, gilt der neue Aufbewahrungszeitraum nur für Snapshots, die nach dem Ändern der Aufbewahrungsregel archiviert werden.

Verwenden Sie eines der folgenden Verfahren, um eine Lebenszyklusrichtlinie zu ändern.

Console

Ändern einer Lebenszyklus-Richtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store, Lifecycle Manager aus.
3. Wählen Sie eine Lebenszyklus-Richtlinie aus der Liste aus.
4. Wählen Sie Aktionen, Lebenszyklusrichtlinie ändern.
5. Ändern Sie die Richtlinieneinstellungen nach Bedarf. Sie können beispielsweise den Zeitplan ändern, Tags (Markierungen) hinzufügen oder entfernen oder die Richtlinie aktivieren oder deaktivieren.
6. Wählen Sie Richtlinie ändern aus.

Command line

Verwenden Sie den Befehl update-lifecycle-policy, um Informationen über eine Lebenszyklus-Richtlinie zu ändern. Um die Syntax zu vereinfachen, wird in diesem Beispiel eine JSON-Datei, `policyDetailsUpdated.json`, referenziert, die die Richtliniendetails enthält.

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
    --policy-details file://policyDetailsUpdated.json
```

Das folgende Beispiel zeigt eine `policyDetailsUpdated.json`-Datei.

```
{
   "ResourceTypes":[
      "VOLUME"
   ],
   "TargetTags":[
      {
         "Key": "costcenter",
         "Value": "120"
      }
   ],
   "Schedules":[
```

```
        {
            "Name": "DailySnapshots",
            "TagsToAdd": [
                {
                    "Key": "type",
                    "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 12,
                "IntervalUnit": "HOURS",
                "Times": [
                    "15:00"
                ]
            },
            "RetainRule": {
                "Count" :5
            },
            "CopyTags": false
        }
    ]
}
```

Verwenden Sie den Befehl `get-lifecycle-policy`, um die aktualisierte Richtlinie anzuzeigen. Sie sehen, dass der Status, der Wert des Tags (Markierung), das Snapshot-Intervall und die Snapshot-Startzeit geändert wurden.

Löschen Sie die Amazon Data Lifecycle Manager-Richtlinien

Beachten Sie beim Löschen der Amazon Data Lifecycle Manager-Richtlinien Folgendes:

- Wenn Sie eine Richtlinie löschen, werden die durch diese Richtlinie erstellten Snapshots oder AMIs nicht automatisch gelöscht. Wenn Sie die Snapshots oder AMIs nicht mehr benötigen, müssen Sie sie manuell löschen.
- Wenn Sie eine Richtlinie löschen, für die eine Snapshot-Archivierung aktiviert ist, werden Snapshots, die sich zum Zeitpunkt des Löschens der Richtlinie auf der Archivstufe befinden, nicht mehr von Amazon Data Lifecycle Manager verwaltet. Sie müssen die Snapshots manuell löschen, wenn sie nicht mehr benötigt werden.
- Wenn Sie eine Richtlinie mit einem für die Archivierung aktivierten, altersbasierten Zeitplan löschen, werden die durch die Richtlinie erstellten Snapshots, deren Archivierung geplant ist, zum

geplanten Archivierungsdatum und zur geplanten Archivierungszeit dauerhaft gelöscht, wie vom System-Tag `aws:dlm:expirationtime` angegeben.

Verwenden Sie eines der folgenden Verfahren, um eine Lebenszyklusrichtlinie zu löschen.

Console

So löschen Sie eine Lebenszyklus-Richtlinie

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic Block Store, Lifecycle Manager aus.
3. Wählen Sie eine Lebenszyklus-Richtlinie aus der Liste aus.
4. Wählen Sie Aktionen, Lebenszyklusrichtlinie löschen.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Richtlinie löschen.

Command line

Verwenden Sie den Befehl delete-lifecycle-policy, um eine Lebenszyklus-Richtlinie zu löschen und die in der Richtlinie verwendeten Ziel-Tags freizugeben, sodass sie erneut verwendet werden können.

> **Note**
>
> Sie können Snapshots löschen, die nur von Amazon Data Lifecycle Manager erstellt wurden.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Die Amazon Data Lifecycle Manager-API-Referenz enthält Beschreibungen und die Syntax für die einzelnen Aktionen und Datentypen der Amazon Data Lifecycle Manager-Abfrage-API.

Alternativ können Sie eines der AWS SDKs verwenden, um auf eine Weise auf die API zuzugreifen, die auf die von Ihnen verwendete Programmiersprache oder Plattform zugeschnitten ist. Weitere Informationen finden Sie unter AWS -SDKs.

Steuern Sie den Zugriff auf Amazon Data Lifecycle Manager mithilfe von IAM

Für den Zugriff auf Amazon Data Lifecycle Manager sind Anmeldeinformationen erforderlich. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS -Ressourcen wie Instances, Volumes, Snapshots und AMIs verfügen.

Die folgenden IAM-Berechtigungen sind für die Verwendung von Amazon Data Lifecycle Manager erforderlich.

> **Note**
>
> - Die Berechtigungen `ec2:DescribeAvailabilityZones`, `ec2:DescribeRegions`, `kms:ListAliases` und `kms:DescribeKey` sind nur für Konsolenbenutzer erforderlich. Wenn kein Konsolenzugriff erforderlich ist, können Sie die Berechtigungen entfernen.
> - Das ARN-Format der AWSDataLifecycleManagerDefaultRole Rolle unterscheidet sich je nachdem, ob sie mit der Konsole oder der AWS CLI erstellt wurde. Wenn die Rolle mit der Konsole erstellt wurde, lautet das ARN-Format `arn:aws:iam::`*`account_id`*`:role/service-role/AWSDataLifecycleManagerDefaultRole`. Wenn die Rolle mit dem erstellt wurde AWS CLI, lautet das ARN-Format`arn:aws:iam::`*`account_id`*`:role/AWSDataLifecycleManagerDefaultRole`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
```

```
                "arn:aws:iam::111122223333:role/
AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::111122223333:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement",
                "arn:aws:iam::111122223333:role/service-role/
AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::111122223333:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Berechtigungen für die Verschlüsselung

Berücksichtigen Sie Folgendes, wenn Sie mit Amazon Data Lifecycle Manager und verschlüsselten Ressourcen arbeiten.

- Wenn das Quell-Volume verschlüsselt ist, stellen Sie sicher, dass die Amazon Data Lifecycle Manager-Standardrollen (AWSDataLifecycleManagerDefaultRoleund AWSDataLifecycleManagerDefaultRoleForAMIManagement) berechtigt sind, die zum Verschlüsseln des Volumes verwendeten KMS-Schlüssel zu verwenden.
- Wenn Sie regionsübergreifendes Kopieren für unverschlüsselte Snapshots oder AMIs, die von unverschlüsselten Snapshots unterstützt werden, aktivieren und sich dafür entscheiden, die Verschlüsselung in der Zielregion zu aktivieren, stellen Sie sicher, dass die Standardrollen

berechtigt sind, den KMS-Schlüssel zu verwenden, der für die Verschlüsselung in der Zielregion erforderlich ist.

- Wenn Sie regionsübergreifendes Kopieren für verschlüsselte Snapshots oder AMIs aktivieren, die durch verschlüsselte Snapshots unterstützt werden, stellen Sie sicher, dass die Standardrollen berechtigt sind, sowohl den Quell- als auch den Ziel-KMS-Schlüssel zu verwenden.
- Wenn Sie die Snapshot-Archivierung für verschlüsselte Snapshots aktivieren, stellen Sie sicher, dass die Amazon Data Lifecycle Manager-Standardrolle () berechtigt AWSDataLifecycleManagerDefaultRole ist, den KMS-Schlüssel zu verwenden, der zum Verschlüsseln des Snapshots verwendet wird.

Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch.

Weitere Informationen finden Sie unter Ändern von Berechtigungen für einen Benutzer im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Amazon Data Lifecycle Manager

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen. AWS Mit verwalteten Richtlinien können Sie Benutzern, Gruppen und Rollen die entsprechenden Berechtigungen effizienter zuweisen, als wenn Sie die Richtlinien selbst schreiben müssten.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen jedoch nicht ändern. AWS aktualisiert gelegentlich die in einer AWS verwalteten Richtlinie definierten Berechtigungen. Diese Aktualisierung wirkt sich auf alle Prinzipal-Entitäten (Benutzer, Gruppen und Rollen) aus, an die die Richtlinie angefügt ist.

Amazon Data Lifecycle Manager bietet AWS verwaltete Richtlinien für allgemeine Anwendungsfälle. Diese Richtlinien erleichtern die Definition der geeigneten Berechtigungen und die Steuerung des Zugriffs auf Ihre Ressourcen. Die von Amazon Data Lifecycle Manager bereitgestellten AWS verwalteten Richtlinien sind so konzipiert, dass sie Rollen zugeordnet werden können, die Sie an Amazon Data Lifecycle Manager übergeben.

Themen

- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement

- AWSDataLifecycleManagerSSMFullAccess
- AWS verwaltete Richtlinienaktualisierungen

AWSDataLifecycleManagerServiceRole

Die AWSDataLifecycleManagerServiceRole Richtlinie gewährt Amazon Data Lifecycle Manager die entsprechenden Berechtigungen zur Erstellung und Verwaltung von Amazon EBS-Snapshot-Richtlinien und Kontenübergreifendem Kopieren von Ereignissen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

Die AWSDataLifecycleManagerServiceRoleForAMIManagement Richtlinie gewährt Amazon Data Lifecycle Manager die entsprechenden Berechtigungen zur Erstellung und Verwaltung von Amazon EBS-backed AMI-Richtlinien.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

AWSDataLifecycleManagerSSMFullAccess

Berechtigt Amazon Data Lifecycle Manager dazu, die Systems-Manager-Aktionen auszuführen, die für die Ausführung von Vor- und Nach-Skripten auf allen Amazon-EC2-Instances erforderlich sind.

> **Important**
>
> Die Richtlinie verwendet den Bedingungsschlüssel `aws:ResourceTag`, um den Zugriff auf bestimmte SSM-Dokumente einzuschränken, wenn Vor- und Nach-Skripte verwendet werden. Damit Amazon Data Lifecycle Manager auf die SSM-Dokumente zugreifen kann, müssen Sie sicherstellen, dass Ihre SSM-Dokumente mit gekennzeichnet sind. `DLMScriptsAccess:true`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTaggedSSMDocumentsOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
```

```
        {
            "Sid": "AllowSpecificAWSOwnedSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
                "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA"
            ]
        },
        {
            "Sid": "AllowAllEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinienaktualisierungen

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Dienste aktualisieren eine AWS verwaltete Richtlinie am ehesten, wenn eine neue Funktion gestartet wird oder wenn neue Funktionen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

Die folgende Tabelle enthält Einzelheiten zu den Aktualisierungen der AWS verwalteten Richtlinien für Amazon Data Lifecycle Manager, seit dieser Service mit der Erfassung dieser Änderungen

begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed auf Dokumentenverlauf für das Amazon EBS-Benutzerhandbuch.

Änderungen	Beschreibung	Date
AWSDataLifecycleManagerServiceRole— Die Richtlinienberechtigungen wurden aktualisiert.	Amazon Data Lifecycle Manager hat die `ec2:DescribeAvailabilityZones` Aktion hinzugefügt, mit der Snapshot-Richtlinien die Erlaubnis erteilt werden, Informationen über lokale Zonen abzurufen.	16. Dezember 2024
AWSDataLifecycleManagerSSMFullAccess— Die Richtlinienberechtigungen wurden aktualisiert.	Die Richtlinie wurde aktualisiert, um anwendungskonsistente Snapshots für SAP HANA unter Verwendung des SSM-Dokuments `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPH`	17. November 2023

Änderungen	Beschreibung	Date
	ANA zu unterstützen.	
AWSDataLifecycleManagerSSMFullAccess— Eine neue AWS verwaltete Richtlinie wurde hinzugefügt.	Amazon Data Lifecycle Manager hat die AWSDataLifecycleManagerSSMFullAccess AWS verwaltete Richtlinie hinzugefügt.	7. November 2023

Änderungen	Beschreibung	Date
AWSDataLifecycleManagerServiceRole— Es wurden Berechtigungen zur Unterstützung der Snapshot-Archivierung hinzugefügt.	In Amazon Data Lifecycle Manager wurden die Aktionen `ec2:ModifySnapshotTier` und `ec2:DescribeSnapshotTierStatus` der Berechtigung zum Erteilen von Snapshot-Richtlinien hinzugefügt, um Snapshots zu archivieren und den Archivierungsstatus für Snapshots zu überprüfen.	30. September 2022

Änderungen	Beschreibung	Date
AWSDataLifecycleManagerServiceRoleForAMIManagement— Es wurden Berechtigungen hinzugefügt, um die AMI-Abwertung zu unterstützen.	Amazon Data Lifecycle Manager hat die `ec2:DisableImageDeprecation` Aktionen `ec2:EnableImageDeprecation` und hinzugefügt, um AMI-Richtlinien die Erlaubnis zu erteilen, die EBS-backed AMI-Abwertung zu aktivieren und zu deaktivieren.	23. August 2021
Amazon Data Lifecycle Manager hat mit der Verfolgung von Änderungen begonnen	Amazon Data Lifecycle Manager hat damit begonnen, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	23. August 2021

IAM-Servicerollen für Amazon Data Lifecycle Manager

Eine AWS Identity and Access Management (IAM-) Rolle ähnelt einer Benutzerrolle insofern, als es sich um eine AWS Identität mit Berechtigungsrichtlinien handelt, die festlegen, was die Identität tun kann 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 annimmt, um Aktionen in Ihrem Namen auszuführen. Als Service, der für Sie Backup-Operationen durchführt, erfordert der Amazon Data Lifecycle Manager die Übergabe einer Rolle, die es annehmen soll, wenn es für Sie Rechtslinien-Geschäfte durchführt. Weitere Informationen zu IAM-Rollen finden Sie unter IAM-Rollen im IAM-Benutzerhandbuch.

Die Rolle, die Sie an Amazon Data Lifecycle Manager übergeben, muss über eine IAM-Richtlinie mit den Berechtigungen verfügen, mit denen Amazon Data Lifecycle Manager Aktionen ausführen kann, die mit Richtlinienvorgängen verknüpft sind, z. B. das Erstellen von Snapshots und AMIs, das Kopieren von Snapshots und AMIs, das Löschen von Snapshots und das Abmelden von AMIs. Für jeden der Amazon Data Lifecycle Manager-Richtlinientypen sind unterschiedliche Berechtigungen erforderlich. Die Rolle muss außerdem Amazon Data Lifecycle Manager als vertrauenswürdige Entität aufgelistet haben. Dadurch kann Amazon Data Lifecycle Manager die Rolle übernehmen.

Themen

- Standard-Servicerollen für Amazon Data Lifecycle Manager
- Benutzerdefinierte Service-Rollen für Amazon Data Lifecycle Manager

Standard-Servicerollen für Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager verwendet die folgenden Standard-Service-Rollen:

- AWSDataLifecycleManagerDefaultRole— Standardrolle für die Verwaltung von Snapshots. Es vertraut nur dem `dlm.amazonaws.com`-Dienst, um die Rolle zu übernehmen, und Amazon Data Lifecycle Manager kann die Aktionen ausführen, die für Snapshot- und kontoübergreifende Snapshot-Kopierrichtlinien in Ihrem Namen erforderlich sind. Diese Rolle verwendet die `AWSDataLifecycleManagerServiceRole` AWS verwaltete Richtlinie.

> **Note**
>
> Das ARN-Format der Rolle unterscheidet sich je nachdem, ob sie mit der Konsole oder der AWS CLI erstellt wurde. Wenn die Rolle mit der Konsole erstellt wurde, lautet das ARN-Format `arn:aws:iam::`*`account_id`*`:role/service-role/AWSDataLifecycleManagerDefaultRole`. Wenn die Rolle mit dem erstellt wurde AWS CLI, lautet das ARN-Format`arn:aws:iam::`*`account_id`*`:role/AWSDataLifecycleManagerDefaultRole`.

- AWSDataLifecycleManagerDefaultRoleForAMIManagement— Standardrolle für die Verwaltung von AMIs. Es vertraut darauf, dass nur der `dlm.amazonaws.com` Service die Rolle übernimmt, und Amazon Data Lifecycle Manager kann die gemäß den EBS-backed AMI-Richtlinien erforderlichen Aktionen in Ihrem Namen ausführen. Diese Rolle verwendet die `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS verwaltete Richtlinie.

Wenn Sie die Amazon Data Lifecycle Manager-Konsole verwenden, erstellt Amazon Data Lifecycle Manager automatisch die AWSDataLifecycleManagerDefaultRole Servicerolle, wenn Sie zum ersten Mal eine Snapshot- oder kontoübergreifende Snapshot-Kopierrichtlinie erstellen. Die AWSDataLifecycleManagerDefaultRoleForAMIManagement Servicerolle wird automatisch erstellt, wenn Sie zum ersten Mal eine EBS-backed AMI-Richtlinie erstellen.

Wenn Sie die Konsole nicht verwenden, können Sie die Dienstrollen mit dem Befehl create-default-role manuell erstellen. Für`--resource-type`, geben Sie `snapshot` an AWSDataLifecycleManagerDefaultRole, ob Sie erstellen oder erstellen `image` AWSDataLifecycleManagerDefaultRoleForAMIManagement möchten.

```
$ aws dlm create-default-role --resource-type snapshot|image
```

Wenn Sie diese standardmäßigen Servicerollen löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die sie in Ihrem Konto neu anzulegen.

Benutzerdefinierte Service-Rollen für Amazon Data Lifecycle Manager

Alternativ zur Verwendung der Standarddienstrollen können Sie benutzerdefinierte IAM-Rollen mit den erforderlichen Berechtigungen erstellen und sie dann beim Erstellen einer Lebenszyklus-Richtlinie auswählen.

Erstellen einer benutzerdefinierten IAM-Rolle

1. Erstellen Sie Rollen mit den folgenden Berechtigungen.

   - Notwendige Berechtigungen zum Verwalten von Snapshot-Lebenszyklusrichtlinien

     JSON

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AwsDataLifecycleRule.managed-cwe.*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringNotLike": {
```

```
                    "aws:ResourceTag/DLMScriptsAccess": "false"
                }
            }
        }
    ]
}
```

- Notwendige Berechtigungen zum Verwalten von AMI-Lebenszyklusrichtlinien

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
```

```
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

Weitere Informationen finden Sie unter Erstellen einer Rolle im IAM-Benutzerhandbuch.

2. Fügen Sie eine Vertrauensstellung für die Rollen hinzu.

   a. Wählen Sie in der IAM-Konsole Roles (Rollen) aus.

   b. Wählen Sie die erstellte Rolle aus und wählen Sie Trust relationships (Vertrauensstellungen).

   c. Wählen Sie Edit Trust Relationship (Vertrauensstellung bearbeiten), fügen Sie die folgende Richtlinie hinzu und wählen Sie Update Trust Policy (Vertrauensstellung aktualisieren).

      JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": "dlm.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
 }]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zu verwenden, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Beispielsweise können Sie der vorherigen Vertrauensrichtlinie den folgenden Bedingungsblock hinzufügen. Das `aws:SourceAccount` ist der Besitzer der Lebenszyklusrichtlinie und das `aws:SourceArn` ist der ARN der Lebenszyklusrichtlinie. Wenn Sie die Lebenszyklusrichtlinie IF nicht kennen, können Sie diesen Teil des ARN durch einen Platzhalter (*) ersetzen und dann die Vertrauensrichtlinie aktualisieren, nachdem Sie die Lebenszyklusrichtlinie erstellt haben.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

Überwachen Sie die Amazon Data Lifecycle Manager-Richtlinien

Sie können die folgenden Features zum Überwachen des Lebenszyklus Ihrer Snapshots und AMIs verwenden.

Features

- Konsole und AWS CLI
- Überwachen Sie die Data Lifecycle Manager-Richtlinien mit EventBridge
- Überwachen Sie die Data Lifecycle Manager-Richtlinien mit CloudWatch
- Protokollieren Amazon-Data-Lifecycle-Manager-API-Aufrufen mithilfe von AWS CloudTrail

Konsole und AWS CLI

Sie können Ihre Lebenszyklus-Richtlinien mit der Amazon-EC2-Konsole oder der AWS CLI anzeigen. Jeder von einer Richtlinie erstellte Snapshot und AMI verfügt über einen Zeitstempel und richtlinienbezogene Tags (Markierungen). Sie können Snapshots und AMIs mithilfe von

diesen Markierungen filtern, um sicherzustellen, dass Ihre Backups so erstellt werden, wie Sie es beabsichtigen.

Überwachen Sie die Data Lifecycle Manager-Richtlinien mit EventBridge

Amazon EBS und Amazon Data Lifecycle Manager geben Ereignisse im Hinblick auf Aktionen von Lebenszyklus-Richtlinien aus. Sie können Amazon CloudWatch Events verwenden AWS Lambda , um Ereignisbenachrichtigungen programmgesteuert zu verarbeiten. Ereignisse werden auf bestmögliche Weise ausgegeben. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Die folgenden Ereignisse sind verfügbar:

> **Note**
>
> Es werden keine Ereignisse für Aktionen der AMI-Lebenszyklusrichtlinie ausgegeben.

- `createSnapshot` – Ein Amazon-EBS-Ereignis, das ausgegeben wird, wenn eine `CreateSnapshot`-Aktion erfolgreich ist oder fehlschlägt. Weitere Informationen finden Sie unter EventBridge Amazon-Ereignisse für Amazon EBS.
- `DLM Policy State Change` – Ein Amazon Data Lifecycle Manager-Ereignis, das ausgegeben wird, wenn eine Lebenszyklus-Richtlinie einen Fehlerstatus annimmt. Das Ereignis enthält eine Beschreibung der Fehlerursache.

  Das folgende Beispiel zeigt ein Ereignis, bei dem die von der IAM-Rolle gewährten Berechtigungen nicht ausreichen.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
```

```
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

Das folgende Beispiel zeigt ein Ereignis, das ausgegeben wird, wenn ein Limit überschritten wird.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

- `DLM Pre Post Script Notification` – Ein Ereignis, das ausgegeben wird, wenn ein Vor- oder Nach-Skript initiiert wird, erfolgreich ist oder fehlschlägt.

  Beispielsweise wird folgendes Ereignis ausgegeben, wenn ein VSS-Backup erfolgreich durchgeführt wird.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "DLM Pre Post Script Notification",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
        "script_stage": "",
        "result": "success",
        "cause": "",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
        "execution_handler": "AWS_VSS_BACKUP",
        "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
        "resource_type": "EBS_SNAPSHOT",
        "resources": [{
            "status": "pending",
            "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
            "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
        }],
        "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
        "start_time": "2023-10-27T22:03:29.370Z",
        "end_time": "2023-10-27T22:04:51.370Z",
        "timeout_time": ""
    }
}
```


Überwachen Sie die Data Lifecycle Manager-Richtlinien mit CloudWatch

Sie können Ihre Amazon Data Lifecycle Manager-Lebenszyklusrichtlinien mithilfe von CloudWatch Amazon Data Lifecycle Manager überwachen. Dieses Tool sammelt Rohdaten und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit ablaufen. Anhand dieser Metriken können Sie genau sehen, wie viele Amazon EBS-Snapshots und EBS-backed AMIs im Laufe der Zeit durch Ihre Richtlinien erstellt, gelöscht und kopiert werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden.

Die Metriken werden über einen Zeitraum von 15 Monaten aufbewahrt, sodass Sie auf historische Informationen zugreifen und ein besseres Verständnis darüber erhalten, wie Ihre Lebenszyklus-Richtlinien über einen längeren Zeitraum funktionieren.

Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Themen

- Unterstützte Metriken
- Sehen Sie sich CloudWatch Kennzahlen für Ihre Richtlinien an
- Diagrammen von Metriken für Ihre Richtlinien
- Erstellen Sie einen CloudWatch Alarm für eine Richtlinie
- Beispielanwendungsfälle
- Verwalten von Richtlinien, die fehlerhafte Aktionen melden

Unterstützte Metriken

Die folgenden Amazon Data Lifecycle Manager-Metriken sind im `AWS/EBS` Namespace enthalten. Die Metriken unterscheiden sich je nach Richtlinientyp.

Alle Metriken können auf der `DLMPolicyId`-Dimension gemessen werden. Die nützlichsten Statistiken sind `sum` und `average`, und die Maßeinheit ist `count`.

Wählen Sie eine Registerkarte, um die von diesem Richtlinientyp unterstützten Metriken anzuzeigen.

EBS snapshot policies

Metrik	Description
`ResourcesTargeted`	Die Anzahl der Ressourcen, auf die die in einem Snapshot oder einer EBS-backed AMI-Richtlinie angegebenen Tags abzielen.
`SnapshotsCreateStarted`	Die Anzahl der Snapshot-Aktionen, die von einer Snapshot-Richtlinie initiiert wurden. Jede Aktion wird nur einmal aufgezeichnet, auch wenn mehrere nachfolgende Wiederholungen vorliegen. Wenn eine Snapshot-Erstellung fehlschlägt, sendet Amazon Data Lifecycle Manager eine `SnapshotsCreateFailed` -Metrik.
`SnapshotsCreateCompleted`	Die Anzahl der Snapshots, die von einer Snapshot-Richtlinie erstellt wurden. Dies schließt erfolgreiche Wiederholungen innerhalb von 60 Minuten nach der geplanten Zeit ein.

Metrik	Description
`SnapshotsCreateFailed`	Die Anzahl der Snapshots, die von einer Snapshot-Richtlinie nicht erstellt werden konnten. Dies schließt erfolglose Wiederholungen innerhalb von 60 Minuten nach der geplanten Zeit ein.
`SnapshotsSharedCompleted`	Die Anzahl der Snapshots, die von einer Snapshot-Richtlinie für Konten freigegeben werden.
`SnapshotsDeleteCompleted`	Die Anzahl der Snapshots, die durch eine Snapshot- oder EBS-backed AMI-Richtlinie gelöscht wurden. Diese Metrik gilt nur für Snapshots, die von der Richtlinie erstellt wurden. Sie gilt nicht für regionsübergreifende Snapshot-Kopien, die von der Richtlinie erstellt wurden. Diese Metrik umfasst Snapshots, die gelöscht werden, wenn eine EBS-backed AMI-Richtlinie die Registrierung von AMIs aufhebt.
`SnapshotsDeleteFailed`	Die Anzahl der Snapshots, die durch einen Snapshot oder eine AMI-Richtlinie nicht gelöscht werden konnten. EBS-backed Diese Metrik gilt nur für Snapshots, die von der Richtlinie erstellt wurden. Sie gilt nicht für regionsübergreifende Snapshot-Kopien, die von der Richtlinie erstellt wurden. Diese Metrik umfasst Snapshots, die gelöscht werden, wenn eine EBS-backed AMI-Richtlinie die Registrierung von AMIs aufhebt.
`SnapshotsCopiedRegionStarted`	Die Anzahl der regionsübergreifenden Snapshot-Kopieraktionen, die von einer Snapshot-Richtlinie gestartet wurden.
`SnapshotsCopiedRegionCompleted`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die von einer Snapshot-Richtlinie erstellt. Dies schließt erfolgreiche Wiederholungen innerhalb von 24 Stunden nach der geplanten Zeit ein.
`SnapshotsCopiedRegionFailed`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die von einer Snapshot-Richtlinie nicht erstellt werden konnten. Dies schließt erfolglose Wiederholungen innerhalb von 24 Stunden nach der geplanten Zeit ein.

Metrik	Description
`SnapshotsCopiedRegionDeleteCompleted`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine Snapshot-Richtlinie gelöscht wurden.
`SnapshotsCopiedRegionDeleteFailed`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine Snapshot-Richtlinie nicht gelöscht werden konnten.
`snapshotsArchiveDeletionFailed`	Die Anzahl der archivierten Snapshots, die von einer Snapshot Richtlinie aus der Archivstufe nicht gelöscht werden konnten.
`snapshotsArchiveScheduled`	Die Anzahl der Snapshots, die von einer Snapshot Richtlinie für die Archivierung vorgesehen waren.
`snapshotsArchiveCompleted`	Die Anzahl der Snapshots, die von einer Snapshot Richtlinie erfolgreich archiviert wurden.
`snapshotsArchiveFailed`	Die Anzahl der Snapshots, die von einer Snapshot-Richtlinie nicht archiviert werden konnten.
`snapshotsArchiveDeletionCompleted`	Die Anzahl der archivierten Snapshots, die von einer Snapshot Richtlinie aus der Archivstufe erfolgreich gelöscht werden konnten.
`PreScriptStarted`	Die Anzahl der Instances, für die ein Vor-Skript erfolgreich initiiert wurde. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.

Metrik	Description
`PreScriptCompleted`	Die Anzahl der Instances, für die ein Vor-Skript erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das Vor-Skript außerhalb des angegebenen Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
`PreScriptFailed`	Die Anzahl der Instances, für die ein Vor-Skript nicht erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das Vor-Skript außerhalb des angegebenen Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
`PostScriptStarted`	Die Anzahl der Instances, für die ein Nach-Skript erfolgreich initiiert wurde. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
PostScriptCompleted	Die Anzahl der Instances, für die ein Nach-Skript erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das Nach-Skript außerhalb des angegebenen Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
PostScriptFailed	Die Anzahl der Instances, für die ein Nach-Skript nicht erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das Nach-Skript außerhalb des angegebenen Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.

Metrik	Description
`VSSBackupStarted`	Die Anzahl der Instances, für die ein VSS-Backup erfolgreich initiiert wurde. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
`VSSBackupCompleted`	Die Anzahl der Instances, für die ein VSS-Backup erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das VSS-Backup außerhalb des Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.
`VSSBackupFailed`	Die Anzahl der Instances, für die ein VSS-Backup nicht erfolgreich abgeschlossen wurde. Die Metrik wird auch dann ausgegeben, wenn das VSS-Backup außerhalb des Timeout-Zeitraums abgeschlossen wird. Wenn Skriptwiederholungen aktiviert sind, kann diese Metrik pro Richtlinienausführung mehrmals ausgegeben werden.

EBS-backed AMI policies

Die folgenden Metriken können mit EBS-backed AMI-Richtlinien verwendet werden:

Metrik	Description
`ResourcesTargeted`	Die Anzahl der Ressourcen, auf die die in einem Snapshot oder einer EBS-backed AMI-Richtlinie angegebenen Tags abzielen.
`SnapshotsDeleteCompleted`	Die Anzahl der Snapshots, die durch eine Snapshot- oder EBS-backed AMI-Richtlinie gelöscht wurden. Diese Metrik gilt nur für Snapshots, die von der Richtlinie erstellt wurden. Sie gilt nicht für regionsübergreifende Snapshot-Kopien, die von der Richtlinie erstellt wurden.

Metrik	Description
	Diese Metrik umfasst Snapshots, die gelöscht werden, wenn eine EBS-backed AMI-Richtlinie die Registrierung von AMIs aufhebt.
`SnapshotsDeleteFailed`	Die Anzahl der Snapshots, die durch einen Snapshot oder eine AMI-Richtlinie nicht gelöscht werden konnten. EBS-backed Diese Metrik gilt nur für Snapshots, die von der Richtlinie erstellt wurden. Sie gilt nicht für regionsübergreifende Snapshot-Kopien, die von der Richtlinie erstellt wurden. Diese Metrik umfasst Snapshots, die gelöscht werden, wenn eine EBS-backed AMI-Richtlinie die Registrierung von AMIs aufhebt.
`SnapshotsCopiedRegionDeleteCompleted`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine Snapshot-Richtlinie gelöscht wurden.
`SnapshotsCopiedRegionDeleteFailed`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine Snapshot-Richtlinie nicht gelöscht werden konnten.
`ImagesCreateStarted`	Die Anzahl der durch eine AMI-Richtlinie initiierten CreateImage EBS-backed Aktionen.
`ImagesCreateCompleted`	Die Anzahl der AMIs, die durch eine EBS-backed AMI-Richtlinie erstellt wurden.
`ImagesCreateFailed`	Die Anzahl der AMIs, die nicht durch eine EBS-backed AMI-Richtlinie erstellt werden konnten.

Metrik	Description
`ImagesDeregisterCompleted`	Die Anzahl der AMIs, die aufgrund einer EBS-backed AMI-Richtlinie abgemeldet wurden.
`ImagesDeregisterFailed`	Die Anzahl der AMIs, die aufgrund einer AMI-Richtlinie nicht deregistriert werden konnten. EBS-backed
`ImagesCopiedRegionStarted`	Die Anzahl der regionsübergreifenden Kopieraktionen, die durch eine EBS-backed AMI-Richtlinie initiiert wurden.
`ImagesCopiedRegionCompleted`	Die Anzahl der regionsübergreifenden AMI-Kopien, die durch eine EBS-backed AMI-Richtlinie erstellt wurden.
`ImagesCopiedRegionFailed`	Die Anzahl der regionsübergreifenden AMI-Kopien, die nicht durch eine EBS-backed AMI-Richtlinie erstellt werden konnten.
`ImagesCopiedRegionDeregisterCompleted`	Die Anzahl der regionsübergreifenden AMI-Kopien, deren Registrierung gemäß der Aufbewahrungsregel aufgrund einer AMI-Richtlinie aufgehoben wurde. EBS-backed
`ImagesCopiedRegionDeregisteredFailed`	Die Anzahl der regionsübergreifenden AMI-Kopien, die gemäß der Aufbewahrungsregel aufgrund einer AMI-Richtlinie nicht deregistriert werden konnten. EBS-backed

Metrik	Description
`EnableImageDeprecationCompleted`	Die Anzahl der AMIs, die durch eine AMI-Richtlinie als veraltet markiert wurden. EBS-backed
`EnableImageDeprecationFailed`	Die Anzahl der AMIs, die nicht durch eine AMI-Richtlinie als veraltet markiert werden konnten. EBS-backed
`EnableCopiedImageDeprecationCompleted`	Die Anzahl der regionsübergreifenden AMI-Kopien, die durch eine AMI-Richtlinie als veraltet markiert wurden. EBS-backed
`EnableCopiedImageDeprecationFailed`	Die Anzahl der regionsübergreifenden AMI-Kopien, die nicht durch eine AMI-Richtlinie als veraltet markiert werden konnten. EBS-backed

Cross-account copy event policies

Die folgenden Metriken können mit kontoübergreifenden Kopierereignissen verwendet werden:

Metrik	Description
`SnapshotsCopiedAccountStarted`	Die Anzahl der kontoübergreifende Snapshot-Kopieraktionen, die von einer Richtlinie für kontoübergreifende Kopierereignisse.
`SnapshotsCopiedAccountCompleted`	Die Anzahl der Snapshots, die von einer Richtlinie für kontoüber greifende Kopierereignisse kopiert werden. Dies schließt erfolgreiche

Metrik	Description
	Wiederholungen innerhalb von 24 Stunden nach der geplanten Zeit ein.
`SnapshotsCopiedAccountFailed`	Die Anzahl der Snapshots, die von einer Richtlinie für kontoüber greifende Kopierereignisse nicht von einem anderen Konto kopiert werden konnten. Dies schließt erfolglose Wiederholungen innerhalb von 24 Stunden nach der geplanten Zeit ein.
`SnapshotsCopiedAccountDeleteCompleted`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine kontoübergreifende Kopierere ignisrichtlinie gelöscht wurden.
`SnapshotsCopiedAccountDeleteFailed`	Die Anzahl der regionsübergreifenden Snapshot-Kopien, die gemäß der Aufbewahrungsregel durch eine kontoübergreifende Kopierere ignisrichtlinie nicht gelöscht werden konnten.

Sehen Sie sich CloudWatch Kennzahlen für Ihre Richtlinien an

Sie können die AWS-Managementkonsole oder die Befehlszeilentools verwenden, um die Metriken aufzulisten, die Amazon Data Lifecycle Manager an Amazon sendet CloudWatch.

Amazon EC2 console

Zeigen Sie Metriken mithilfe der Amazon EC2-Konsole wie folgt an:

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Lifecycle Manager aus.
3. Wählen Sie eine Richtlinie im Raster aus, und wählen Sie dann die Registerkarte Überwachung.

CloudWatch console

Um Metriken mithilfe der CloudWatch Amazon-Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie das EBS-Namespace und dann Data Lifecycle Manager-Metriken aus.

AWS CLI

So listen Sie alle verfügbaren Metriken für Amazon Data Lifecycle Manager auf

Verwenden Sie den list-metrics-Befehl:

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

So listen Sie alle Metriken für eine bestimmte Richtlinie auf

Verwenden Sie den Befehl list-metrics und geben Sie die `DLMPolicyId`-Dimension an.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

So listen Sie eine einzelne Metrik für alle Richtlinien auf

Verwenden Sie den Befehl list-metrics und geben Sie die `--metric-name`-Option an.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

Diagrammen von Metriken für Ihre Richtlinien

Nachdem Sie die Richtlinie erstellt haben, können Sie die Amazon EC2-Konsole öffnen und auf der Registerkarte Monitoring (Überwachung) die Überwachungsdiagramme für die Richtlinie anzeigen. Jedes Diagramm basiert auf einer der verfügbaren Amazon EC2-Metriken.

Folgende Diagramm-Metriken sind verfügbar:

- Zielgerichtete Ressourcen (basierend auf `ResourcesTargeted`)
- Snapshot-Erstellung gestartet (basierend auf `SnapshotsCreateStarted`)
- Snapshot-Erstellung abgeschlossen (basierend auf `SnapshotsCreateCompleted`)
- Snapshot-Erstellung fehlgeschlagen (basierend auf `SnapshotsCreateFailed`)
- Snapshot-Freigabe abgeschlossen (basierend auf `SnapshotsSharedCompleted`)
- Snapshot-Löschen abgeschlossen (basierend auf `SnapshotsDeleteCompleted`)
- Snapshot-Löschen fehlgeschlagen (basierend auf `SnapshotsDeleteFailed`)
- Snapshot regionenübergreifende Kopie wurde gestartet (basierend auf `SnapshotsCopiedRegionStarted`)
- Erstellen eines Snapshots regionenübergreifenden Kopie (basierend auf `SnapshotsCopiedRegionCompleted`)
- Fehler bei regionenübergreifender Kopie des Snapshots (basierend auf `SnapshotsCopiedRegionFailed`)
- Snapshot regionsübergreifendes Kopieren wurde abgeschlossen (basierend auf `SnapshotsCopiedRegionDeleteCompleted`)
- Fehler beim Löschen regionsübergreifender Snapshot-Kopieren (basierend auf `SnapshotsCopiedRegionDeleteFailed`)
- Kontoübergreifende Snapshot-Kopie gestartet (basierend auf `SnapshotsCopiedAccountStarted`)
- Kontoübergreifende Kopie des Snapshots abgeschlossen (basierend auf `SnapshotsCopiedAccountCompleted`)
- Kontoübergreifende Snapshot-Kopie fehlgeschlagen (basierend auf `SnapshotsCopiedAccountFailed`)
- Kontoübergreifende Snapshot-Löschung abgeschlossen (basierend auf `SnapshotsCopiedAccountDeleteCompleted`)
- Kontoübergreifende Snapshot-Kopieren fehlgeschlagen (basierend auf `SnapshotsCopiedAccountDeleteFailed`)
- AMI-Erstellung gestartet (basierend auf `ImagesCreateStarted`)
- AMI-Erstellung abgeschlossen (basierend auf `ImagesCreateCompleted`)
- AMI-Erstellung fehlgeschlagen (basierend auf `ImagesCreateFailed`)

- AMI-Abmeldung abgeschlossen (basierend auf `ImagesDeregisterCompleted`)
- AMI-Abmeldung fehlgeschlagen (basierend auf `ImagesDeregisterFailed`)
- Erstellen einer AMI regionenübergreifenden Kopie (basierend auf `ImagesCopiedRegionStarted`)
- AMI regionenübergreifende Kopie abgeschlossen (basierend auf `ImagesCopiedRegionCompleted`)
- Fehler bei AMI regionenübergreifenden Kopieren (basierend auf `ImagesCopiedRegionFailed`)
- AMI regionsübergreifende Kopie Abmeldung abgeschlossen (basierend auf `ImagesCopiedRegionDeregisterCompleted`)
- AMI regionsübergreifende Kopie Abmeldung fehlgeschlagen (basierend auf `ImagesCopiedRegionDeregisteredFailed`)
- AMI Veraltungs-Aktivierung abgeschlossen (basierend auf `EnableImageDeprecationCompleted`)
- AMI Veraltungs-Aktivierung fehlgeschlagen (basierend auf `EnableImageDeprecationFailed`)
- AMI regionsübergreifende Kopie Veraltungs-Aktivierung abgeschlossen (basierend auf `EnableCopiedImageDeprecationCompleted`)
- AMI regionsübergreifende Kopie Veraltungs-Aktivierung fehlgeschlagen (basierend auf `EnableCopiedImageDeprecationFailed`)

Erstellen Sie einen CloudWatch Alarm für eine Richtlinie

Sie können einen CloudWatch Alarm erstellen, der die CloudWatch Kennzahlen für Ihre Richtlinien überwacht. CloudWatch sendet Ihnen automatisch eine Benachrichtigung, wenn die Metrik einen von Ihnen angegebenen Schwellenwert erreicht. Sie können mithilfe der CloudWatch Konsole einen CloudWatch Alarm erstellen.

Weitere Informationen zum Erstellen von Alarmen mithilfe der CloudWatch Konsole finden Sie im folgenden Thema im CloudWatch Amazon-Benutzerhandbuch.

- Erstellen Sie einen CloudWatch Alarm auf der Grundlage eines statischen Schwellenwerts
- Erstellen Sie einen CloudWatch Alarm auf der Grundlage einer Anomalieerkennung

Beispielanwendungsfälle

Im Folgenden finden Sie Beispiele für Anwendungsfälle:

Themen

- Beispiel 1: Metrik ResourcesTargeted
- Beispiel 2: Metrik SnapshotDeleteFailed
- Beispiel 3: Metrik SnapshotsCopiedRegionFailed

Beispiel 1: Metrik ResourcesTargeted

Sie können die `ResourcesTargeted`-Metrik nutzen, um die Gesamtzahl der Ressourcen zu überwachen, die von einer bestimmten Richtlinie bei jeder Ausführung ausgerichtet sind. Auf diese Weise können Sie einen Alarm auslösen, wenn die Anzahl der Zielressourcen unter oder über einem erwarteten Schwellenwert liegt.

Wenn Sie beispielsweise erwarten, dass Ihre tägliche Richtlinie Backups von nicht mehr als `50`-Volumes können Sie einen Alarm erstellen, der eine E-Mail-Benachrichtigung sendet, wenn die `sum` für `ResourcesTargeted` größer als `50` über einen 1-Stunden-Zeitraum ist. Auf diese Weise können Sie sicherstellen, dass keine unerwarteten Snapshots von Volumes erstellt wurden, die falsch markiert wurden.

Sie können den folgenden Befehl verwenden, um diesen Alarm zu erstellen:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Beispiel 2: Metrik SnapshotDeleteFailed

Sie können die `SnapshotDeleteFailed`-Metrik nutzen, um auf Fehler beim Löschen von Snapshots gemäß der Snapshot-Aufbewahrungsregel der Richtlinie zu überwachen.

Wenn Sie beispielsweise eine Richtlinie erstellt haben, die Snapshots automatisch alle zwölf Stunden löschen soll, können Sie einen Alarm erstellen, der Ihr Engineering-Team benachrichtigt, wenn `sum`

von `SnapshotDeletionFailed` größer als `0` über einen 1-Stunden-Zeitraum ist. Dies könnte helfen, eine unsachgemäße Aufbewahrung von Snapshots zu untersuchen und sicherzustellen, dass Ihre Speicherkosten nicht durch unnötige Snapshots erhöht werden.

Sie können den folgenden Befehl verwenden, um diesen Alarm zu erstellen:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Beispiel 3: Metrik SnapshotsCopiedRegionFailed

Verwenden der `SnapshotsCopiedRegionFailed`-Metrik, um zu ermitteln, wann Ihre Richtlinien Snapshots nicht in andere Regionen kopieren können.

Wenn Ihre Richtlinie beispielsweise Snapshots täglich über Regionen hinweg kopiert, können Sie einen Alarm erstellen, der eine SMS an Ihr Engineering-Team sendet, wenn `sum` von `SnapshotCrossRegionCopyFailed` größer als `0` über einen 1-Stunden-Zeitraum ist. Dies kann hilfreich sein, um zu überprüfen, ob nachfolgende Snapshots in der Herkunft von der Richtlinie erfolgreich kopiert wurden.

Sie können den folgenden Befehl verwenden, um diesen Alarm zu erstellen:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
```

```
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Verwalten von Richtlinien, die fehlerhafte Aktionen melden

Weitere Informationen darüber, was zu tun ist, wenn eine Ihrer Richtlinien einen unerwarteten Wert ungleich Null für eine Metrik für fehlgeschlagene Aktionen meldet, finden Sie im Artikel Was sollte ich tun, wenn Amazon Data Lifecycle Manager fehlgeschlagene Aktionen in CloudWatch Metriken meldet?

Protokollieren Amazon-Data-Lifecycle-Manager-API-Aufrufen mithilfe von AWS CloudTrail

Mit können Sie Benutzeraktivitäten und API-Nutzung verfolgen AWS CloudTrail, um die Einhaltung interner Richtlinien und behördlicher Standards nachzuweisen. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst in Amazon Data Lifecycle Manager ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon Data Lifecycle Manager als Ereignisse, einschließlich Aufrufe von der Amazon Data Lifecycle Manager-Konsole und von Codeaufrufen an die Amazon Data Lifecycle Manager-APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Data Lifecycle Manager. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der gesammelten Informationen von können Sie ermitteln CloudTrail, welche Anfrage an Amazon Data Lifecycle Manager gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Amazon Data Lifecycle Manager finden Sie unter CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in Amazon Data Lifecycle Manager eine CloudTrail Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im Eventverlauf in einem Ereignis aufgezeichnet. Sie können die letzten

Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Amazon Data Lifecycle Manager, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Amazon Data Lifecycle Manager-Aktionen werden von protokolliert CloudTrail. Beispielsweise generieren Aufrufe von `CreateLifecyclePolicy` und `DeleteLifecyclePolicy` Aktionen Einträge in den CloudTrail Protokolldateien. Die vollständige Liste der Aktionen finden Sie unter Aktionen.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Welcher Benutzer hat die Anfrage gestellt.
- 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.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes zu Amazon Data Lifecycle Manager-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon 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 Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie nicht in einer bestimmten Reihenfolge.

Example Beispiel: CreateLifecyclePolicy

Im Folgenden finden Sie ein Beispiel für einen CloudTrail Protokolleintrag für die `CreateLifecyclePolicy` Aktion.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAJA2ELRVCPEXAMPLE",
        "userName": "user",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-07-24T18:01:05Z"
            }
        }
    },
    "eventTime": "2018-07-24T18:20:28Z",
    "eventSource": "dlm.amazonaws.com",
    "eventName": "CreateLifecyclePolicy",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.179",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "ExecutionRoleArn": "arn:aws:iam::123456789012:role/service-role/
AWSDataLifecycleManagerServiceRole",
        "PolicyDetails": {
            "ResourceTypes": [
                "VOLUME"
            ],
            "Schedules": [
                {
                    "CreateRule": {
                        "Interval": 12,
```

```
                        "IntervalUnit": "HOURS",
                        "Times": [
                            "09:00"
                        ]
                    },
                    "Name": "Default Schedule",
                    "RetainRule": {
                        "Count": 3
                    },
                    "TagsToAdd": [
                        {
                            "Key": "Name",
                            "Value": "backup-my-volume"
                        }
                    ]
                }
            ],
            "TargetTags": [
                {
                    "Key": "Name",
                    "Value": "my-volume"
                }
            ]
        },
        "Description": "test-cloudtrail",
        "State": "DISABLED"
    },
    "responseElements": {
        "PolicyId": "policy-04ff8755fce0599eb"
    },
    "requestID": "3d714ca6-8f6e-11e8-92a4-35fd765427f0",
    "eventID": "28ab3121-6040-4a40-80c7-ae59b3adf405",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


Example Beispiel: DeleteLifecyclePolicy

Im Folgenden finden Sie ein Beispiel für einen CloudTrail Protokolleintrag für die `DeleteLifecyclePolicy` Aktion.


```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAJA2ELRVCPEXAMPLE",
        "userName": "user",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-07-24T18:01:05Z"
            }
        }
    },
    "eventTime": "2018-07-24T19:33:33Z",
    "eventSource": "dlm.amazonaws.com",
    "eventName": "DeleteLifecyclePolicy",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.241",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "policyId": "policy-04ff8755fce0599eb"
    },
    "responseElements": null,
    "requestID": "73260971-8f78-11e8-a156-598016e53fb2",
    "eventID": "3740f2fb-0d6a-4712-a7ad-eb9f17103fb2",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


Service-Endpunkte für Amazon Data Lifecycle Manager

Ein Endpunkt ist eine URL, die als Einstiegspunkt für einen AWS Webservice dient. Amazon Data Lifecycle Manager unterstützt die folgenden Endpunkttypen:

- IPv4-Endpunkte
- Dual-stack Endpunkte, die sowohl IPv4 als auch IPv6 unterstützen
- FIPS-Endpunkte

Wenn Sie eine Anfrage stellen, können Sie den Endpunkt und die Region angeben, die verwendet werden sollen. Wenn Sie keinen Endpunkt festlegen, wird standardmäßig der IPv4-Endpunkt verwendet. Um einen anderen Endpunkttyp zu verwenden, müssen Sie ihn in Ihrer Anforderung angeben. Beispiele für diese Vorgehensweise finden Sie unter Angeben von Endpunkten.

Informationen zum Amazon Data Lifecycle Manager finden Sie unter Amazon Data Lifecycle Manager-Endpunkte im. Allgemeine Amazon Web Services-Referenz

Themen

- IPv4-Endpunkte
- Dual-stack (IPv4 und IPv6) -Endpunkte
- FIPS-Endpunkte
- Angeben von Endpunkten

IPv4-Endpunkte

IPv4 Endpunkte unterstützen nur IPv4-Datenverkehr. IPv4-Endpunkte sind für alle Regionen verfügbar.

Sie müssen die Region als Teil des Endpunktnamens angeben. Die Endpunktnamen verwenden die folgende Namenskonvention:

- dlm. *region*.amazonaws.com

Der IPv4-Endpunkt für die Region USA Ost (Nord-Virginia) lautet beispielsweise. `dlm.us-east-1.amazonaws.com`

Dual-stack (IPv4 und IPv6) -Endpunkte

Dual-stack Endpunkte unterstützen sowohl IPv4- als auch IPv6-Verkehr. Dual-stack Endpunkte sind für alle Regionen verfügbar.

Um IPv6 verwenden zu können, müssen Sie einen Dual-Stack-Endpunkt verwenden. Wenn Sie eine Anfrage an einen Dual-Stack-Endpunkt stellen, löst die Endpunkt-URL eine IPv6- oder eine IPv4-Adresse auf, je nachdem, welches Protokoll Ihr Netzwerk und Ihr Client verwendet.

Sie müssen die Region als Teil des Endpunktnamens angeben. Dual-stack Bei Endpunktnamen wird die folgende Namenskonvention verwendet:

- `dlm.region.api.aws`

Der Dual-Stack-Endpunkt für die Region USA Ost (Nord-Virginia) lautet `dlm.us-east-1.api.aws` beispielsweise.

FIPS-Endpunkte

Amazon Data Lifecycle Manager bietet FIPS-validated Dual-Stack-Endpunkte (IPv4 und IPv6) für die folgenden Regionen:

- `us-east-1` – USA Ost (Nord-Virginia)
- `us-east-2` – USA Ost (Ohio)
- `us-west-1` – USA West (Nordkalifornien)
- `us-west-2` – USA West (Oregon)
- `ca-central-1` – Kanada (Zentral)
- `ca-west-1`— Kanada West (Calgary)

FIPS-Dual-Stack-Endpunkte verwenden die folgende Namenskonvention:. `dlm-fips.region.api.aws` Der FIPS-Dual-Stack-Endpunkt für die Region USA Ost (Nord-Virginia) lautet beispielsweise. `dlm-fips.us-east-1.api.aws`

Angeben von Endpunkten

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS CLI einen Endpunkt für die `US East (N. Virginia)`-Region angeben.

- Dual-stack

```
aws dlm create-default-role \
--resource-type snapshot \
--endpoint-url https://dlm.us-east-2.api.aws
```

- IPv4

```
aws dlm create-default-role \
--resource-type snapshot \
--endpoint-url https://dlm.us-east-2.amazonaws.com
```

Erstellen Sie eine private Verbindung zwischen einer VPC und Amazon EBS

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon EBS herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen, unterstützt von. AWS PrivateLink Sie können auf Amazon EBS zugreifen, als ob es in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung zu verwenden. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon EBS zu kommunizieren.

Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren.

Weitere Informationen finden Sie AWS PrivateLink im Handbuch unter Access AWS-Services through. AWS PrivateLink

> **Note**
>
> Amazon Data Lifecycle Manager unterstützt VPC-Endpunkte mit IPv4-Schnittstelle für alle kommerziellen und regionalen Bereiche sowie IPv6-Schnittstellen-VPC-Endpunkte nur für kommerzielle AWS GovCloud (US) Regionen.

Überlegungen zu Amazon EBS-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon EBS einrichten, lesen Sie die Überlegungen im Handbuch. AWS PrivateLink

Standardmäßig ist der vollständige Zugriff auf Amazon EBS über den Endpunkt zulässig. Sie können den Zugriff auf den Schnittstellenendpunkt mithilfe von VPC-Endpunktrichtlinien steuern. Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Amazon EBS steuert. Die Richtlinie gibt die folgenden Informationen an:

- Der Prinzipal, der Aktionen ausführen kann.
- Die Aktionen, die ausgeführt werden können.
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Amazon EBS. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Benutzern die Erlaubnis, zusammenfassende Informationen zu den Amazon Data Lifecycle Manager-Richtlinien abzurufen.

```
{
  "Statement": [{
    "Action": "dlm:GetLifecyclePolicies",
    "Effect": "Allow",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

Erstellen Sie einen Schnittstellen-VPC-Endpunkt für Amazon EBS

Sie können einen VPC-Endpunkt für Amazon EBS entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen VPC-Endpunkt für Amazon EBS mit dem folgenden Servicenamen:

- `com.amazonaws.region.dlm`

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Amazon EBS unter Verwendung des Standard-DNS-Namens für die Region stellen, z. B. `dlm.us-east-1.amazonaws.com`

Beheben Sie Probleme mit Amazon Data Lifecycle Manager

Die folgende Dokumentation kann zum Beheben möglicher Probleme nützlich sein.

Themen

- Fehler: Die Rolle mit dem Namen ist bereits vorhanden

Fehler: Die **`Rolle mit dem Namen ist bereits vorhanden`**

Description

Sie erhalten den Fehler `Role with name AWSDataLifecycleManagerDefaultRole already exists` oder `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, wenn Sie versuchen, eine Richtlinie unter Verwendung der Konsole zu erstellen.

Ursache

Das ARN-Format der Standardrolle unterscheidet sich je nachdem, ob sie mit der Konsole oder der AWS CLI erstellt wurde. Die ARNs sind zwar unterschiedlich, doch für die Rollen wird der gleiche Rollenname verwendet, was zu einem Rollenbenennungskonflikt zwischen der Konsole und der AWS CLI führt.

Lösung

Führen Sie folgende Schritte aus, um dieses Problem zu lösen:

1. (Nur für Snapshot-Richtlinien, die für Pre- und Post-Skripts aktiviert sind) Hängen Sie die AWSDataLifecycleManagerSSMFullAccess AWS verwaltete Richtlinie manuell an die AWSDataLifecycleManagerDefaultRole IAM-Rolle an. Weitere Informationen finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen.
2. Wenn Sie Ihre Amazon Data Lifecycle Manager-Richtlinie erstellen, wählen Sie für die IAM-Rolle die Option Andere Rolle auswählen und wählen Sie dann entweder AWSDataLifecycleManagerDefaultRole (für eine Snapshot-Richtlinie) oder AWSDataLifecycleManagerDefaultRoleForAMIManagement (für eine AMI-Richtlinie).
3. Fahren Sie mit der Erstellung der Richtlinie wie gewohnt fort.

AWS Backup für Amazon Elastic Block Store

AWS Backup ist ein vollständig verwalteter Service, der den Datenschutz in Ihrer gesamten Umgebung zentralisiert und automatisiert. AWS Anstatt Snapshot-Zeitpläne und Aufbewahrung pro Ressource zu verwalten, definieren Sie eine einzige Backup-Richtlinie und wenden sie für alle Konten und Regionen an. Taggen Sie Ihre Ressourcen und AWS Backup schützen sie automatisch, ohne dass eine Konfiguration pro Team erforderlich ist. Der Service unterstützt viele AWS Dienste, darunter Amazon EBS, Amazon EC2, Amazon S3, Amazon EFS, Amazon RDS und Aurora. Daher kann eine einzige Richtlinie Volumes, Datenbanken, Dateisysteme und Objektspeicher zusammen schützen, ohne dass separate Backup-Tools pro Workload erforderlich sind.

Stellt für Amazon EBS absturzkonsistente Snapshots mehrerer Volumes AWS Backup bereit, die Point-in-Time-Backups auf allen Volumes koordinieren, die mit einer Amazon EC2-Instance verbunden sind. Dies ist wichtig für Datenbanken und geclusterte Anwendungen, die sich über mehrere Volumes erstrecken. AWS Backup Die Suche geht noch einen Schritt weiter und ermöglicht die Wiederherstellung auf Objektebene. Sie können einzelne Dateien oder Verzeichnisse aus Amazon EBS-Snapshots finden und wiederherstellen, ohne das gesamte Volume wiederherstellen zu müssen.

AWS Backup verleiht Ihren Snapshots außerdem Sicherheit und Compliance auf Unternehmensebene. Logischerweise isolieren Air-Gap-Vaults die Recovery-Punkte von Ihrer Produktionsumgebung. Vault Lock erzwingt Unveränderlichkeit. Die GuardDuty Amazon-Integration scannt Backups auf Malware. Backup Audit Manager bewertet kontinuierlich Ihren Backup-Status und generiert revisionssichere Compliance-Berichte.

Sehen Sie sich die folgenden Ressourcen an, um loszulegen:

- AWS Backup Entwicklerhandbuch
- Erstellen Sie absturzsichere Backups mit mehreren Volumes
- Stellen Sie Amazon EBS-Volumes wieder her
- Suchen und stellen Sie einzelne Dateien aus Amazon EBS-Snapshots wieder her

Verwenden von EBS-Direct-APIs für den Zugriff auf den Inhalt eines EBS-Snapshots

Sie können die direkten Amazon Elastic Block Store(Amazon EBS)-APIs verwenden, um EBS-Snapshots zu erstellen, Daten direkt in Ihre Snapshots zu schreiben, Daten auf Ihren Snapshots zu lesen und die Unterschiede oder Änderungen zwischen zwei Snapshots zu identifizieren. Wenn Sie ein unabhängiger Softwareanbieter (ISV) sind, der Backup-Services für Amazon EBS anbietet, machen EBS-Direct-APIs es effizienter und kostengünstiger, inkrementelle Änderungen an Ihren EBS-Volumes durch Snapshots zu verfolgen. Dies kann getan werden, ohne neue Volumes aus Snapshots erstellen und dann Amazon Elastic Compute Cloud(Amazon EC2)-Instances zum Vergleichen der Unterschiede verwenden zu müssen.

Sie können inkrementelle Snapshots direkt aus On-Premises-Daten in EBS-Volumes und in der Cloud erstellen, um sie für eine schnelle Notfallwiederherstellung zu verwenden. Mit der Möglichkeit, Snapshots zu schreiben und zu lesen, können Sie Ihre On-Premises-Daten während eines Notfalls in einen EBS-Snapshot schreiben. Nach der Wiederherstellung können Sie sie dann auf dem Snapshot AWS oder lokal aus dem Snapshot wiederherstellen. Sie müssen keine komplexen Mechanismen mehr erstellen und verwalten, um Daten nach und aus Amazon EBS zu kopieren.

Dieses Benutzerhandbuch bietet eine Übersicht der Elemente, aus denen sich die EBS-Direct-APIs zusammensetzt, und Beispiele dafür, wie sie effektiv eingesetzt werden können. Weitere Informationen zu den Aktionen, Datentypen, Parametern und Fehlern der APIs finden Sie in der EBS-Direct-APIs-Referenz. Weitere Informationen zu den unterstützten AWS Regionen, Endpunkten und Servicekontingenten für die direkten EBS-APIs finden Sie unter Amazon EBS-Endpunkte und -Kontingente im. Allgemeine AWS-Referenz

Themen

- Preise für EBS-Direct-APIs
- Konzepte für direkte EBS-APIs
- Steuern Sie den Zugriff auf direkte EBS-APIs mithilfe von IAM
- Lesen Sie Amazon EBS-Snapshots mit direkten EBS-APIs
- Schreiben Sie Amazon EBS-Snapshots mit direkten EBS-APIs
- Verschlüsselungsergebnisse für direkte EBS-APIs
- Verwenden Sie die Prüfsummen der direkten EBS-APIs, um Snapshot-Daten zu validieren
- Stellen StartSnapshot Sie die Idempotenz bei API-Anfragen sicher

- Fehlerhafte Wiederholungsversuche für direkte EBS-APIs
- Optimieren Sie die Leistung für direkte EBS-APIs
- Service-Endpunkte für direkte EBS-APIs
- AWS SDK-Codebeispiele für direkte EBS-APIs
- Erstellen Sie eine private Verbindung zwischen einer VPC und den direkten EBS-APIs
- Protokollieren Sie direkte EBS-API-Aufrufe mit AWS CloudTrail
- Häufig gestellte Fragen zu direkten EBS-APIs

Preise für EBS-Direct-APIs

Preise für APIs

Der Preis, den Sie zahlen, um die EBS-Direct-APIs zu verwenden, hängt von den Anfragen ab, die Sie machen. Weitere Informationen finden Sie unter Amazon EBS – Preise.

- ListChangedBlocksund ListSnapshotBlocks APIs werden pro Anfrage berechnet. Wenn Sie beispielsweise 100.000 ListSnapshotBlocks API-Anfragen in einer Region stellen, für die 0,0006 USD pro 1.000 Anfragen berechnet werden, werden Ihnen 0,06 USD (0,0006 USD pro 1.000 Anfragen x 100) berechnet.
- GetSnapshotBlockwird pro zurückgegebenem Block berechnet. Wenn Sie beispielsweise 100.000 GetSnapshotBlock API-Anfragen in einer Region stellen, für die 0,003 USD pro 1.000 zurückgegebenen Blöcke berechnet werden, werden Ihnen 0,30 USD berechnet (0,003 USD pro 1.000 zurückgegebenen Blöcken x 100).
- PutSnapshotBlockwird pro geschriebenem Block berechnet. Wenn Sie beispielsweise 100.000 PutSnapshotBlock API-Anfragen in einer Region stellen, für die 0,006 USD pro 1.000 geschriebenen Blöcke berechnet werden, werden Ihnen 0,60 USD berechnet (0,006 USD pro 1.000 geschriebenen Blöcken x 100).

Netzwerkkosten

Datenübertragungskosten

Daten, die direkt zwischen direkten EBS-APIs und Amazon EC2-Instances in derselben AWS Region übertragen werden, sind kostenlos, wenn Sie Nicht-FIPS-Endpunkte verwenden. https://docs.aws.amazon.com/general/latest/gr/ebs-service.html#ebs_direct_apis Weitere Informationen

finden Sie unter AWS -Service-Endpunkte. Wenn andere AWS Dienste Ihre Datenübertragung behindern, werden Ihnen die entsprechenden Datenverarbeitungskosten in Rechnung gestellt. Zu diesen Diensten gehören unter anderem PrivateLink Endpunkte, NAT Gateway und Transit Gateway.

VPC-Schnittstellenendpunkte

Wenn Sie direkte EBS-APIs von Amazon EC2-Instances oder AWS Lambda Funktionen in privaten Subnetzen verwenden, können Sie VPC-Schnittstellenendpunkte anstelle von NAT-Gateways verwenden, um die Kosten für die Netzwerkdatenübertragung zu senken. Weitere Informationen finden Sie unter Erstellen Sie eine private Verbindung zwischen einer VPC und den direkten EBS-APIs.

Konzepte für direkte EBS-APIs

Im Folgenden sind die wichtigsten Konzepte aufgeführt, die Sie verstehen sollten, bevor Sie mit den direkten EBS-APIs beginnen.

-Snapshots

Snapshots sind die primäre Methode, Daten von Ihren EBS-Volumes zu sichern. Mit den EBS-Direct-APIs können Sie auch Daten von Ihren On-Premises-Datenträgern auf Snapshots sichern. Um Speicherkosten zu sparen, sind aufeinanderfolgende Snapshots inkrementell und enthalten nur die Volume-Daten, die sich seit dem vorherigen Snapshot geändert haben. Weitere Informationen finden Sie unter Amazon EBS-Snapshots.

> **Note**
>
> EBS Direct APIs unterstützen keine öffentlichen Snapshots und lokale Snapshots auf. AWS Outposts

Blöcke

Ein Block ist ein Fragment von Daten innerhalb eines Snapshots. Jeder Snapshot kann Tausende von Blöcken enthalten. Alle Blöcke in einem Snapshot haben eine feste Größe.

Blockindizes

Ein Blockindex ist ein logischer Index in Einheiten von 512-KiB-Blöcken. Um den Blockindex zu identifizieren, teilen Sie den logischen Offset der Daten im logischen Volume durch die Blockgröße (logischer Offset der Daten/524288). Der logische Offset der Daten muss an 512 KiB ausgerichtet rein.

Block-Tokens

Ein Block-Token ist der identifizierende Hash eines Blocks innerhalb eines Snapshots und wird verwendet, um die Blockdaten zu finden. Von EBS-Direct-APIs zurückgegebene Block-Token sind temporär. Sie ändern sich an dem für sie angegebenen Ablaufzeitstempel oder wenn Sie einen anderen ausführen ListSnapshotBlocks oder denselben Snapshot ListChangedBlocks anfordern.

Prüfsumme

Eine Prüfsumme ist ein kleiner Bezug, der aus einem Datenblock abgeleitet wird, um Fehler zu erkennen, die während der Übertragung oder Speicherung eingeführt wurden. Die EBS-Direct-APIs verwenden Prüfsummen zur Validierung der Datenintegrität. Wenn Sie Daten aus einem EBS-Snapshot lesen, stellt der Dienst Base64-encoded SHA256-Prüfsummen für jeden übertragenen Datenblock bereit, die Sie zur Validierung verwenden können. Wenn Sie Daten in einen EBS-Snapshot schreiben, müssen Sie für jeden übertragenen Datenblock eine Base64-codierte SHA256-Prüfsumme angeben. Der Dienst validiert die empfangenen Daten mit der angegebenen Prüfsumme. Weitere Informationen finden Sie Verwenden Sie die Prüfsummen der direkten EBS-APIs, um Snapshot-Daten zu validieren weiter unten in diesem Handbuch.

Verschlüsselung

Verschlüsselung schützt Ihre Daten, indem sie sie in unlesbaren Code konvertiert, der nur von Personen entschlüsselt werden kann, die Zugriff auf den Verschlüsselung haben, mit dem sie verschlüsselt wurden. Sie können die EBS-Direct-APIs verwenden um verschlüsselte Snapshots zu lesen und zu schreiben, aber es gibt einige Einschränkungen. Weitere Informationen finden Sie Verschlüsselungsergebnisse für direkte EBS-APIs weiter unten in diesem Handbuch.

API-Aktionen

Die EBS-Direct-APIs bestehen aus sechs Aktionen. Es gibt drei Leseaktionen und drei Schreibaktionen. Diese Leseaktionen sind:

- ListSnapshotBlocks— gibt die Blockindizes und Block-Token der Blöcke im angegebenen Snapshot zurück
- ListChangedBlocks— gibt die Blockindizes und Block-Token von Blöcken zurück, die sich zwischen zwei angegebenen Snapshots desselben Volumes und derselben Snapshot-Herkunft unterscheiden.
- GetSnapshotBlock— gibt die Daten in einem Block für die angegebene Snapshot-ID, den Blockindex und das Block-Token zurück.

Die Schreibaktionen sind:

- StartSnapshot— startet einen Snapshot, entweder als inkrementellen Snapshot eines vorhandenen Snapshots oder als neuen Snapshot. Der gestartete Snapshot verbleibt im Status „Ausstehend“, bis er mithilfe der CompleteSnapshot Aktion abgeschlossen wird.
- PutSnapshotBlock— fügt einem gestarteten Snapshot Daten in Form einzelner Blöcke hinzu. Sie müssen eine Base64-encoded SHA256-Prüfsumme für den übertragenen Datenblock angeben. Der Dienst validiert die Prüfsumme, nachdem die Übertragung abgeschlossen ist. Die Anforderung schlägt fehl, wenn die vom Dienst berechnete Prüfsumme nicht mit der von Ihnen angegebenen übereinstimmt.
- CompleteSnapshot— vervollständigt einen gestarteten Snapshot, der sich im Status Ausstehend befindet. Der Snapshot wird dann in den Status „Abgeschlossen“ geändert.

Signatur, Version 4, Signierung

Signaturversion 4 ist das Verfahren zum Hinzufügen von Authentifizierungsinformationen zu AWS Anfragen, die über HTTP gesendet werden. Aus Sicherheitsgründen AWS müssen die meisten Anfragen mit einem Zugriffsschlüssel signiert werden, der aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel besteht. Diese beiden Schlüssel werden in der Regel als Sicherheitsanmeldeinformationen bezeichnet. Informationen dazu, wie Sie Anmeldeinformationen für Ihr Konto erhalten, finden Sie unter AWS -Sicherheitsanmeldeinformationen.

Wenn Sie HTTP-Anforderungen manuell erstellen möchten, müssen Sie lernen, wie Sie diese signieren. Wenn Sie das AWS Command Line Interface (AWS CLI) oder eines der AWS SDKs verwenden, um Anfragen an diese zu stellen AWS, signieren diese Tools die Anfragen automatisch für Sie mit dem Zugriffsschlüssel, den Sie bei der Konfiguration der Tools angeben. Wenn Sie diese Tools verwenden, müssen Sie nicht lernen, wie Sie Anfragen signieren.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Signieren von AWS API-Anfragen.

Steuern Sie den Zugriff auf direkte EBS-APIs mithilfe von IAM

Ein Benutzer muss über die folgenden Richtlinien verfügen, um die direkten EBS-APIs verwenden zu können. Weitere Informationen finden Sie unter Ändern von Berechtigungen für einen Benutzer.

Weitere Informationen zu EBS-Direct-API-Ressourcen, -Aktionen und -Bedingungskontextschlüsseln für die Verwendung in IAM-Berechtigungsrichtlinien finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Block Store in der Service-Authorization-Referenz.

> **Important**
>
> Seien Sie vorsichtig, wenn Sie den -Benutzern die folgenden Richtlinien zuweisen. Indem Sie diese Richtlinien zuweisen, können Sie einem Benutzer Zugriff gewähren, dem der Zugriff auf dieselbe Ressource über die Amazon EC2-APIs verweigert wird, z. B. die CopySnapshot Aktionen oder. CreateVolume

Berechtigungen zum Lesen von Snapshots

Die folgende Richtlinie ermöglicht die Verwendung der direkten EBS-Read-APIs für alle Snapshots in einer bestimmten Region. AWS Ersetzen Sie in der Richtlinie *<Region>* durch die Region des Snapshots.

Mit der folgenden Richtlinie kann der Lese-EBS-Direct-APIs für Snapshots mit einem bestimmten Schlüssel-Wert-Tag (Markierung) verwendet werden. Ersetzen Sie in der Richtlinie *<Key>* durch den Schlüsselwert des Tags und *<Value>* durch den Wert des Tags.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
```

```
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

Mit der folgenden Richtlinie können alle Lesevorgänge in EBS-Direct-APIs für alle Snapshots im Konto nur innerhalb eines bestimmten Zeitraums verwendet werden. Diese Richtlinie autorisiert die Verwendung des EBS-Direct-APIs auf der Basis des globalen Bedingungsschlüssels `aws:CurrentTime`. Stellen Sie sicher, dass Sie in der Richtlinie den angezeigten Datums- und Zeitbereich durch den Datums- und Zeitbereich für Ihre Richtlinie ersetzen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
```

```
}
```

Weitere Informationen finden Sie unter Ändern von Berechtigungen für einen Benutzer im IAM-Benutzerhandbuch.

Berechtigungen zum Schreiben von Snapshots

Die folgende Richtlinie ermöglicht die Verwendung der Write-EBS Direct-APIs für alle Snapshots in einer bestimmten AWS Region. Ersetzen Sie in der Richtlinie *<Region>* durch die Region des Snapshots.

Mit der folgenden Richtlinie kann der Schreib-EBS-Direct-APIs für Snapshots mit einem bestimmten Schlüssel-Werte-Tag (Markierung) verwendet werden. Ersetzen Sie in der Richtlinie *<Key>* durch den Schlüsselwert des Tags und *<Value>* durch den Wert des Tags.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

Mit der folgenden Richtlinie kann der gesamte EBS-Direct-APIs verwendet werden. Sie lässt darüber hinaus die Aktion `StartSnapshot` nur zu, wenn eine übergeordnete Snapshot-ID

angegeben ist. Daher blockiert diese Richtlinie das Starten neuer Snapshots ohne Verwendung eines übergeordneten Snapshots.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

Mit der folgenden Richtlinie kann der gesamte EBS-Direct-APIs verwendet werden. Sie lässt außerdem für einen neuen Snapshot ausschließlich die Erstellung des Tag (Markierung)-Schlüssels `user` zu. Diese Richtlinie stellt darüber hinaus sicher, dass der Benutzer Tags (Markierungen) erstellen kann. Die Aktion `StartSnapshot` ist die einzige Aktion, die Tags angeben kann.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Mit der folgenden Richtlinie kann der gesamte Schreib-EBS-Direct-APIs für alle Snapshots im Konto nur innerhalb eines bestimmten Zeitraums verwendet werden. Diese Richtlinie autorisiert die Verwendung des EBS-Direct-APIs auf der Basis des globalen Bedingungsschlüssels `aws:CurrentTime`. Stellen Sie sicher, dass Sie in der Richtlinie den angezeigten Datums- und Zeitbereich durch den Datums- und Zeitbereich für Ihre Richtlinie ersetzen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter Ändern von Berechtigungen für einen Benutzer im IAM-Benutzerhandbuch.

Nutzungsberechtigungen AWS KMS keys

Die folgende Richtlinie gewährt die Berechtigung zum Entschlüsseln eines verschlüsselten Snapshots mithilfe einer spezifischen Verschlüsselung. Sie erteilt auch die Berechtigung, neue Snapshots mit dem standardmäßigen KMS-Schlüssel für die EBS-Verschlüsselung zu verschlüsseln. *<Region>*Ersetzen Sie in der Richtlinie durch die Region des KMS-Schlüssels, *<AccountId>* durch die ID des AWS Kontos des KMS-Schlüssels und *<KeyId>* durch die ID des KMS-Schlüssels.

> **Note**
>
> Standardmäßig haben alle Principals im Konto Zugriff auf den standardmäßigen AWS verwalteten KMS-Schlüssel für die Amazon EBS-Verschlüsselung und können ihn für EBS-Verschlüsselungs- und Entschlüsselungsvorgänge verwenden. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie eine neue Schlüsselrichtlinie erstellen oder die vorhandene Schlüsselrichtlinie für den vom Kunden verwalteten Schlüssel ändern, um dem Prinzipal Zugriff auf den vom Kunden verwalteten Schlüssel zu gewähren. Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

> **Tip**
>
> Um den Grundsatz der Erteilung der geringsten erforderlichen Berechtigungen zu befolgen, lassen Sie den vollständigen Zugriff auf `kms:CreateGrant` nicht zu. Verwenden Sie stattdessen den `kms:GrantIsForAWSResource` Bedingungsschlüssel, damit der Benutzer nur dann Zuschüsse für den KMS-Schlüssel erstellen kann, wenn der Zuschuss im Namen des Benutzers von einem AWS Dienst erstellt wird, wie im folgenden Beispiel gezeigt.

Weitere Informationen finden Sie unter Ändern von Berechtigungen für einen Benutzer im IAM-Benutzerhandbuch.

Lesen Sie Amazon EBS-Snapshots mit direkten EBS-APIs

In den folgenden Schritten wird beschrieben, wie Sie Snapshots mit EBS-Direct-APIs lesen können:

1. Verwenden Sie die ListSnapshotBlocks Aktion, um alle Blockindizes und Block-Token von Blöcken in einem Snapshot anzuzeigen. Oder verwenden Sie die ListChangedBlocks Aktion, um nur die Blockindizes und Block-Token von Blöcken anzuzeigen, die sich zwischen zwei Snapshots desselben Volumes und derselben Snapshot-Herkunft unterscheiden. Diese Aktionen helfen Ihnen, die Block-Token und Blockindizes von Blöcken zu identifizieren, für die Sie möglicherweise Daten abrufen möchten.
2. Verwenden Sie die GetSnapshotBlock Aktion und geben Sie den Blockindex und das Block-Token des Blocks an, für den Sie Daten abrufen möchten.

> **Note**
>
> Sie können keine direkten EBS-APIs mit archivierten Snapshots verwenden.

In den folgenden Beispielen wird gezeigt, wie Sie mit den EBS-Direct-APIs Snapshots lesen.

Themen

- Liste der Blöcke in einem Snapshot
- Liste der Blöcke, die sich zwischen zwei Snapshots unterscheiden
- Abrufen von Blockdaten aus einem Snapshot

Liste der Blöcke in einem Snapshot

AWS CLI

Der folgende Beispielbefehl list-snapshot-blocks gibt die Block-Indizes und Block-Token von Blöcken im Snapshot `snap-0987654321` zurück. Der Parameter `--starting-block-index` schränkt die Ergebnisse auf Block-Indizes ein, die größer als `1000` sind. Der Parameter `--max-results` schränkt die Ergebnisse auf die ersten `100` Blöcke ein.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-
index 1000 --max-results 100
```

Die folgende Beispielantwort für den vorherigen Befehl listet die Block-Indizes und Block-Token im Snapshot auf. Mithilfe des Befehls `get-snapshot-block` können Sie den Block-Index und das

Block-Token des Blocks angeben, für den Sie Daten abrufen möchten. Die Block-Token sind bis zur angegebenen Ablaufzeit gültig.


```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
              "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
          },
          {
              "BlockIndex": 1002,
              "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
          },
          {
              "BlockIndex": 1007,
              "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
          },
          {
              "BlockIndex": 1012,
              "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
          },
          {
              "BlockIndex": 1030,
              "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
          },
          {
              "BlockIndex": 1031,
              "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
          },
          ...
      ],
      "ExpiryTime": 1576287332.806,
      "VolumeSize": 32212254720,
      "BlockSize": 524288
  }
```

AWS API

Die folgende ListSnapshotBlocks Beispielanforderung gibt die Blockindizes und Block-Token von Blöcken zurück, die sich im Snapshot befinden. `snap-0acEXAMPLEcf41648` Der Parameter `startingBlockIndex` schränkt die Ergebnisse auf Block-Indizes ein, die größer als `1000` sind. Der Parameter `maxResults` schränkt die Ergebnisse auf die ersten `100` Blöcke ein.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

Die folgende Beispielantwort für die vorherige Anforderung listet die Block-Indizes und Block-Token im Snapshot auf. Verwenden Sie die GetSnapshotBlock Aktion und geben Sie den Blockindex und das Blocktoken des Blocks an, für den Sie Daten abrufen möchten. Die Block-Token sind bis zur angegebenen Ablaufzeit gültig.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
```

```
            "BlockToken":
"AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
        },
        {
            "BlockIndex": 3073,
            "BlockToken":
"AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
        },
        ...
    ],
    "ExpiryTime": 1.59298379649E9,
    "VolumeSize": 3
}
```

Liste der Blöcke, die sich zwischen zwei Snapshots unterscheiden

Beachten Sie Folgendes, wenn Sie paginierte Anforderungen stellen, um die geänderten Blöcke zwischen zwei Snapshots aufzulisten:

- Die Antwort kann eine oder mehrere leere `ChangedBlocks`-Arrays enthalten. Zum Beispiel:
  - Snapshot 1 – vollständiger Snapshot mit 1 000 Blöcken mit Blockindizes `0` – 999.
  - Snapshot 2 – inkrementeller Snapshot mit nur einem geänderten Block mit Blockindex 999.

  Das Auflisten der geänderten Blöcke für diese Snapshots mit `StartingBlockIndex = 0` und `MaxResults = 100` ergibt ein leeres Array von `ChangedBlocks`. Sie müssen die übrigen Ergebnisse mit `nextToken` anfordern, bis der geänderte Block in der zehnten Ergebnismenge zurückgegeben wird, die Blöcke mit Blockindizes `900` – 999 umfasst.
- Die Antwort kann ungeschriebene Blöcke in den Snapshots überspringen. Zum Beispiel:
  - Snapshot 1 – vollständiger Snapshot mit 1 000 Blöcken mit Blockindizes `2000` – 2999.
  - Snapshot 2 – inkrementeller Snapshot mit nur einem geänderten Block mit Blockindex `2000`.

  Auflisten der geänderten Blöcke für diese Snapshots mit `StartingBlockIndex = 0` und `MaxResults = 100`, überspringt die Blockindizes `0` – 1999 und beinhaltet Blockindex `2000`. Die Antwort wird keine leeren `ChangedBlocks`-Arrays enthalten.

AWS CLI

Der folgende Beispielbefehl list-changed-blocks gibt die Block-Indizes und Block-Token von Blöcken zurück, die sich zwischen den Snapshots `snap-1234567890` und `snap-0987654321` unterscheiden. Der Parameter `--starting-block-index` schränkt die Ergebnisse auf Block-Indizes ein, die größer als `0` sind. Der Parameter `--max-results` schränkt die Ergebnisse auf die ersten `500` Blöcke ein.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

Die folgende Beispielantwort für den vorherigen Befehl zeigt, dass sich die Block-Indizes 0, 6000, 6001, 6002 und 6003 zwischen den beiden Snapshots unterscheiden. Darüber hinaus sind die Block-Indizes 6001, 6002 und 6003 nur in der ersten angegebenen Snapshot-ID und nicht in der zweiten Snapshot-ID vorhanden, da in der Antwort kein zweites Block-Token aufgeführt ist.

Mithilfe des Befehls `get-snapshot-block` können Sie den Block-Index und das Block-Token des Blocks angeben, für den Sie Daten abrufen möchten. Die Block-Token sind bis zur angegebenen Ablaufzeit gültig.

```
{
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
              "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
          },
          {
              "BlockIndex": 6000,
              "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
              "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
          },
          {
              "BlockIndex": 6001,
              "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
          },
          {
```

```
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1576308931.973,
    "VolumeSize": 32212254720,
    "BlockSize": 524288,
    "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//
O6Mdi/BbJarBnp8h"
  }
```

AWS API

Die folgende ListChangedBlocks Beispielanforderung gibt die Blockindizes und Blocktoken von Blöcken zurück, die sich zwischen Snapshots `snap-0acEXAMPLEcf41648` und unterscheiden. `snap-0c9EXAMPLE1b30e2f` Der Parameter `startingBlockIndex` schränkt die Ergebnisse auf Block-Indizes ein, die größer als `0` sind. Der Parameter `maxResults` schränkt die Ergebnisse auf die ersten `500` Blöcke ein.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
  Authorization: <Authentication parameter>
```

Die folgende Beispielantwort für die vorherige Anforderung zeigt, dass sich die Block-Indizes `0`, `3072`, `6002` und `6003` zwischen den beiden Snapshots unterscheiden. Darüber hinaus sind die Block-Indizes `6002` und `6003` nur in der ersten angegebenen Snapshot-ID und nicht in der zweiten Snapshot-ID vorhanden, da in der Antwort kein zweites Block-Token aufgeführt ist.

Mithilfe der Aktion `GetSnapshotBlock` können Sie den Block-Index und das Block-Token des Blocks angeben, für den Sie Daten abrufen möchten. Die Block-Token sind bis zur angegebenen Ablaufzeit gültig.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
              "FirstBlockToken":
 "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/Yb24MaS",
              "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
          },
          {
              "BlockIndex": 6003,
              "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
          },
          ...
      ],
      "ExpiryTime": 1.592976647009E9,
      "VolumeSize": 3
  }
```

Abrufen von Blockdaten aus einem Snapshot

AWS CLI

Der folgende Beispielbefehl get-snapshot-block gibt die Daten im Block-Index `6001` mit dem Block-Token `AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR` zurück, im Snapshot `snap-1234567890`. Die Binärdaten werden auf einem Windows-Computer in die Datei `data` im Verzeichnis `C:\Temp` ausgegeben. Wenn Sie den Befehl auf einem Linux- oder Unix-Computer ausführen, ersetzen Sie den Ausgabepfad durch `/tmp/data`, um die Daten in die Datei `data` im Verzeichnis `/tmp` auszugeben.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

Die folgende Beispielantwort für den vorherigen Befehl zeigt die Größe der zurückgegebenen Daten, die Prüfsumme zur Validierung der Daten und den Algorithmus der Prüfsumme. Die Binärdaten werden automatisch in dem Verzeichnis und in der Datei gespeichert, die Sie im Anforderungsbefehl angegeben haben.

```
{
      "DataLength": "524288",
      "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
      "ChecksumAlgorithm": "SHA256"
  }
```

AWS API

Die folgende GetSnapshotBlock Beispielanforderung gibt die Daten im Blockindex `3072` mit Block-Token `AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid` als Snapshot zurück. `snap-0c9EXAMPLE1b30e2f`

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

Die folgende Beispielantwort für die vorherige Anforderung zeigt die Größe der zurückgegebenen Daten, die Prüfsumme zur Validierung der Daten und den Algorithmus, der zum Generieren der Prüfsumme verwendet wird. Die Binärdaten werden im Hauptteil der Antwort übertragen und wie *BlockData* im folgenden Beispiel dargestellt.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
  Date: Wed, 17 Jun 2020 23:28:38 GMT
  Connection: keep-alive

  BlockData
```

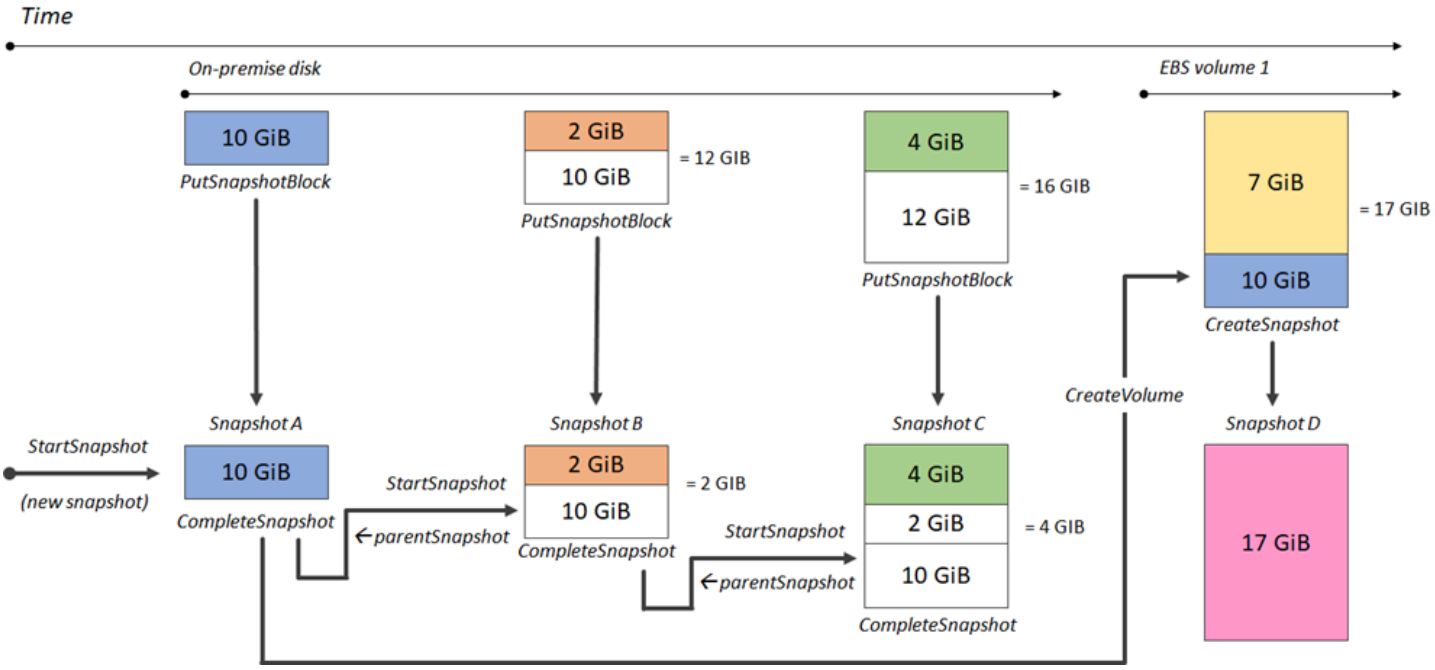
Schreiben Sie Amazon EBS-Snapshots mit direkten EBS-APIs

In den folgenden Schritten wird beschrieben, wie Sie inkrementelle Snapshots mit EBS-Direct-APIs schreiben:

1. Verwenden Sie die StartSnapshot Aktion und geben Sie eine übergeordnete Snapshot-ID an, um einen Snapshot als inkrementellen Snapshot eines vorhandenen Snapshots zu starten, oder lassen Sie die übergeordnete Snapshot-ID weg, um einen neuen Snapshot zu starten. Diese Aktion gibt die neue Snapshot-ID zurück, die sich im Status „Ausstehend“ befindet.
2. Verwenden Sie die PutSnapshotBlock Aktion und geben Sie die ID des ausstehenden Snapshots an, um ihm Daten in Form einzelner Blöcke hinzuzufügen. Sie müssen eine Base64-encoded SHA256-Prüfsumme für den übertragenen Datenblock angeben. Der Dienst berechnet die Prüfsumme der empfangenen Daten und validiert sie mit der angegebenen Prüfsumme. Die Aktion schlägt fehl, wenn die Prüfsummen nicht übereinstimmen.
3. Wenn Sie mit dem Hinzufügen von Daten zum ausstehenden Snapshot fertig sind, verwenden Sie die CompleteSnapshot Aktion, um einen asynchronen Workflow zu starten, der den Snapshot versiegelt und in den Status „Abgeschlossen“ versetzt.

Wiederholen Sie diese Schritte, um einen neuen inkrementellen Snapshot mit dem zuvor erstellten Snapshot als übergeordneter Snapshot zu erstellen.

Im folgenden Diagramm ist Snapshot A beispielsweise der erste neue Snapshot, der gestartet wurde. Snapshot A wird als übergeordneter Snapshot zum Starten von Snapshot B verwendet. Snapshot B wird als übergeordneter Snapshot zum Starten und Erstellen von Snapshots C verwendet. Snapshots A, B und C sind inkrementelle Snapshots. Snapshot A wird verwendet, um EBS-Volume 1 zu erstellen. Snapshot D wird aus EBS-Volume 1 erstellt. Snapshot D ist ein inkrementeller Snapshot von A; es handelt sich nicht um einen inkrementellen Snapshot von B oder C.



In den folgenden Beispielen wird gezeigt, wie Sie mit den EBS-Direct-APIs Snapshots schreiben.

Themen

- Starten eines Snapshots
- Einfügen von Daten in einen Snapshot
- Abschluss eines Snapshots

Starten eines Snapshots

AWS CLI

Der folgende Beispielbefehl start-Snapshot startet einen 8-GiB-Snapshot, wobei der Snapshot `snap-123EXAMPLE1234567` als übergeordneter Snapshot verwendet wird. Der neue Snapshot ist ein inkrementeller Snapshot des übergeordneten Snapshots. Der Snapshot wird in einen Fehlerzustand verschoben, wenn innerhalb des angegebenen Timeout-Zeitraums von `60` Minuten

keine Einfüge- oder Abschlussanforderungen für den Snapshot gesendet werden. Das Client-Token `550e8400-e29b-41d4-a716-446655440000` stellt Idempotenz für die Anforderung sicher. Wenn das Client-Token weggelassen wird, generiert das AWS SDK automatisch eines für Sie. Weitere Informationen zur Idempotenz finden Sie unter Stellen StartSnapshot Sie die Idempotenz bei API-Anfragen sicher.

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

Die folgende Beispielantwort für den vorherigen Befehl zeigt die Snapshot-ID, die AWS -Konto-ID, den Status, die Volume-Größe in GiB und die Größe der Blöcke im Snapshot. Der Snapshot wird im Zustand `pending` gestartet. Geben Sie die Snapshot-ID in nachfolgenden `put-snapshot-block`-Befehlen an, um Daten in den Snapshot zu schreiben. Verwenden Sie anschließend den Befehl `complete-snapshot`, um den Snapshot abzuschließen und den Status in `completed` zu ändern.

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

AWS API

Die folgende StartSnapshot Beispielanforderung startet einen 8 GiB-Snapshot, wobei der Snapshot `snap-123EXAMPLE1234567` als übergeordneter Snapshot verwendet wird. Der neue Snapshot ist ein inkrementeller Snapshot des übergeordneten Snapshots. Der Snapshot wird in einen Fehlerzustand verschoben, wenn innerhalb des angegebenen Timeout-Zeitraums von `60` Minuten keine Einfüge- oder Abschlussanforderungen für den Snapshot gesendet werden. Das Client-Token `550e8400-e29b-41d4-a716-446655440000` stellt Idempotenz für die Anforderung sicher. Wenn das Client-Token weggelassen wird, generiert das AWS SDK automatisch eines für Sie. Weitere Informationen zur Idempotenz finden Sie unter Stellen StartSnapshot Sie die Idempotenz bei API-Anfragen sicher.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
```

```
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Die folgende Beispielantwort für die vorherige Anforderung zeigt die Snapshot-ID, die AWS -Konto-ID, den Status, die Volume-Größe in GiB und die Größe der Blöcke im Snapshot. Der Snapshot wird im Status „Ausstehend“ gestartet. Geben Sie die Snapshot-ID in einer nachfolgenden `PutSnapshotBlocks`-Anforderung an, um Daten in den Snapshot zu schreiben.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

Einfügen von Daten in einen Snapshot

AWS CLI

Der folgende https://docs.aws.amazon.com/cli/latest/reference/ebs/put-snapshot-block.html Put-snapshot-block-Beispielbefehl schreibt `524288` Datenbytes in den

Blockindex im Snapshot. `1000` `snap-0aaEXAMPLEe306d62` Die Base64-codierte `QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=`-Prüfsumme wurde mit dem SHA256-Algorithmus generiert. Die übertragenen Daten befinden sich in der Datei `/tmp/data`.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

Die folgende Beispielantwort für den vorherigen Befehl bestätigt die Datenlänge, die Prüfsumme und den Prüfsummenalgorithmus für die vom Service empfangenen Daten.

```
{
    "DataLength": "524288",
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

AWS API

Die folgende PutSnapshot Beispielanforderung schreibt `524288` Datenbytes in den Blockindex im Snapshot. `1000` `snap-052EXAMPLEc85d8dd` Die Base64-codierte `QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=`-Prüfsumme wurde mit dem SHA256-Algorithmus generiert. Die Daten werden im Hauptteil der Anfrage übertragen und wie *`BlockData`* im folgenden Beispiel dargestellt.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

          BlockData
```

Die folgende Beispielantwort für die vorherige Anforderung bestätigt Datenlänge, Prüfsumme und Prüfsummenalgorithmus für die vom Service empfangenen Daten.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Abschluss eines Snapshots

AWS CLI

Mit dem folgenden Beispielbefehl complete-snapshot wird der Snapshot `snap-0aaEXAMPLEe306d62` abgeschlossen. Der Befehl gibt an, dass 5 Blöcke in den Snapshot geschrieben wurden. Die Prüfsumme `6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=` stellt die Prüfsumme für den gesamten Datensatz dar, der in den Snapshot geschrieben wurde. Weitere Informationen zu Prüfsummen finden Sie unter Verwenden Sie die Prüfsummen der direkten EBS-APIs, um Snapshot-Daten zu validieren weiter oben in dieser Anleitung.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-
count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-
algorithm SHA256 --checksum-aggregation-method LINEAR
```

Im Folgenden finden Sie eine Beispielantwort für den vorherigen Befehl.

```
{
    "Status": "pending"
}
```

AWS API

Die folgende CompleteSnapshot Beispielanforderung vervollständigt den Snapshot`snap-052EXAMPLEc85d8dd`. Der Befehl gibt an, dass 5 Blöcke in den Snapshot geschrieben wurden. Die Prüfsumme `6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=` stellt die Prüfsumme für den gesamten Datensatz dar, der in den Snapshot geschrieben wurde.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

Im Folgenden finden Sie eine Beispielantwort für die vorherige Anforderung.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

Verschlüsselungsergebnisse für direkte EBS-APIs

Wenn Sie einen neuen Snapshot mit starten StartSnapshot, hängt der Verschlüsselungsstatus von den Werten ab, die Sie für Encrypted und KmsKeyArn, angeben ParentSnapshotId, und davon, ob Ihr AWS Konto standardmäßig für die Verschlüsselung aktiviert ist.

> **Note**
>
> - Möglicherweise benötigen Sie zusätzliche IAM-Berechtigungen, um den EBS-Direct-APIs mit Verschlüsselung verwenden zu können. Weitere Informationen finden Sie unter Nutzungsberechtigungen AWS KMS keys.
> - Wenn die Amazon EBS-Verschlüsselung in Ihrem AWS Konto standardmäßig aktiviert ist, können Sie keine unverschlüsselten Snapshots erstellen.
> - Wenn die Amazon EBS-Verschlüsselung in Ihrem AWS Konto standardmäßig aktiviert ist, können Sie keinen neuen Snapshot mit einem unverschlüsselten übergeordneten Snapshot starten. Sie müssen zuerst den übergeordneten Snapshot verschlüsseln, indem

Sie ihn kopieren. Weitere Informationen finden Sie unter Kopieren Sie einen Amazon EBS-Snapshot.

Themen

- Verschlüsselungsergebnisse: unverschlüsselter übergeordneter Snapshot
- Verschlüsselungsergebnisse: verschlüsselter übergeordneter Snapshot
- Verschlüsselungsergebnisse: kein übergeordneter Snapshot

Verschlüsselungsergebnisse: unverschlüsselter übergeordneter Snapshot

Die folgende Tabelle zeigt das Verschlüsselungsergebnis für jede mögliche Kombination von Einstellungen beim Festlegen eines unverschlüsselten übergeordneten Snapshots.

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
Unverschlüsselt	Ausgelassen	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	Der Snapshot ist unverschlüsselt.
		Angegeben	Enabled	
			Disabled	
Unverschlüsselt	Wahr	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
		Angegeben	Enabled	
			Disabled	

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
Unverschlüsselt	Falsch	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
		Angegeben	Enabled	
			Disabled	

Verschlüsselungsergebnisse: verschlüsselter übergeordneter Snapshot

Die folgende Tabelle zeigt das Verschlüsselungsergebnis für jede mögliche Kombination von Einstellungen beim Festlegen eines verschlüsselten übergeordneten Snapshots.

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
Verschlüsselt	Ausgelassen	Ausgelassen	Aktiviert	Der Snapshot wird mit demselben KMS-Schlüssel wie der übergeordnete Snapshot verschlüsselt.
			Disabled	
		Angegeben	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
Verschlüsselt	Wahr	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
		Angegeben	Enabled	

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
			Disabled	
Verschlüsselt	Falsch	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
		Angegeben	Enabled	
			Disabled	

Verschlüsselungsergebnisse: kein übergeordneter Snapshot

Die folgenden Tabellen zeigen das Verschlüsselungsergebnis für jede mögliche Kombination von Einstellungen, wenn kein übergeordneter Snapshot verwendet wird.

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
Ausgelassen	Wahr	Ausgelassen	Aktiviert	Der Snapshot wird mit dem Standard-KMS-Schlüssel für Ihr Konto verschlüsselt. *
			Disabled	
		Angegeben	Aktiviert	Der Snapshot wird mit dem für angegebenen KMS-Schlüssel verschlüsselt KmsKeyArn.
			Disabled	
Ausgelassen	Falsch	Ausgelassen	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.

ParentSnapshotId	Verschlüsselt	KmsKeyArn	Standardmäßige Verschlüsselung	Ergebnis
			Disabled	Der Snapshot ist unverschlüsselt.
		Angegeben	Aktiviert	Die Anforderung schlägt mit `ValidationException` fehl.
			Disabled	
Ausgelassen	Ausgelassen	Ausgelassen	Aktiviert	Der Snapshot wird mit dem Standard-KMS-Schlüssel für Ihr Konto verschlüsselt. *
			Disabled	Der Snapshot ist unverschlüsselt.
		Angegeben	Aktiviert	Der Snapshot wird mit dem für angegebenen KMS-Schlüssel verschlüsselt KmsKeyArn.
			Disabled	

* Bei diesem Standard-KMS-Schlüssel kann es sich um einen vom Kunden verwalteten Schlüssel oder um den standardmäßigen AWS verwalteten KMS-Schlüssel für die Amazon EBS-Verschlüsselung handeln.

Verwenden Sie die Prüfsummen der direkten EBS-APIs, um Snapshot-Daten zu validieren

Die GetSnapshotBlock Aktion gibt Daten zurück, die sich in einem Block eines Snapshots befinden, und die PutSnapshotBlock Aktion fügt Daten zu einem Block in einem Snapshot hinzu. Die übertragenen Blockdaten werden nicht im Rahmen des Signature Version 4-Signaturvorgangs signiert. Daher werden Prüfsummen verwendet, um die Integrität der Daten wie folgt zu überprüfen:

- Wenn Sie die GetSnapshotBlock Aktion verwenden, liefert die Antwort eine Base64-encoded SHA256-Prüfsumme für die Blockdaten mithilfe des X-AMZ-Prüfsum-Headers und des

Prüfsummenalgorithmus mithilfe des x-amz-Headers. Checksum-Algorithm Mithilfe der zurückgegebenen Prüfsumme können Sie die Integrität der Daten überprüfen. Wenn die von Ihnen generierte Prüfsumme nicht mit der von Amazon EBS bereitgestellten Prüfsumme übereinstimmt, sollten Sie die Daten als ungültig betrachten und die Anforderung erneut senden.

- Wenn Sie die PutSnapshotBlock Aktion verwenden, muss Ihre Anfrage eine Base64-encoded SHA256-Prüfsumme für die Blockdaten mithilfe des X-AMZ-Prüfsum-Headers und des Prüfsummenalgorithmus mithilfe des x-amz-Headers bereitstellen. Checksum-Algorithm Die von Ihnen bereitgestellte Prüfsumme wird anhand einer von Amazon EBS generierten Prüfsumme validiert, um die Integrität der Daten zu überprüfen. Wenn die Prüfsummen nicht übereinstimmen, schlägt die Anforderung fehl.
- Wenn Sie die CompleteSnapshot Aktion verwenden, kann Ihre Anfrage optional eine aggregierte Base64-encoded SHA256-Prüfsumme für den vollständigen Datensatz bereitstellen, der dem Snapshot hinzugefügt wurde. Geben Sie die Prüfsumme mithilfe des X-AMZ-Prüfsum-Headers, den Prüfsummenalgorithmus mithilfe des x-amz-Headers und die Prüfsummen-Aggregationsmethode mithilfe des Checksum-Algorithm x-amz-Headers an. Checksum-Aggregation-Method Um die aggregierte Prüfsumme mithilfe der linearen Aggregationsmethode zu generieren, ordnen Sie die Prüfsummen für die einzelnen geschriebenen Blöcke in aufsteigender Reihenfolge des Blockindexes an, verketten sie zu einer einzelnen Zeichenfolge und generieren dann die Prüfsumme für die gesamte Zeichenfolge mit dem SHA256-Algorithmus.

Die Prüfsummen in diesen Aktionen sind Teil des Signature Version 4-Signaturvorgangs.

Stellen StartSnapshot Sie die Idempotenz bei API-Anfragen sicher

Idempotenz stellt sicher, dass eine API-Anforderung nur einmal durchgeführt wird. Wenn bei einer Idempotenz-Anfrage die ursprüngliche Anfrage erfolgreich abgeschlossen wird, geben die nachfolgenden Wiederholungen das Ergebnis der ursprünglichen erfolgreichen Anfrage zurück und haben keine zusätzliche Wirkung.

Die StartSnapshot API unterstützt Idempotenz mithilfe eines Client-Tokens. Ein Client-Token ist eine eindeutige Zeichenfolge, die Sie beim Senden einer API-Anforderung angeben. Wenn Sie eine API-Anforderung mit demselben Client-Token und denselben Anforderungsparametern wiederholen, nachdem sie erfolgreich abgeschlossen wurde, wird das Ergebnis der ursprünglichen Anforderung zurückgegeben. Wenn Sie eine Anforderung mit demselben Client-Token wiederholen, einen oder mehrere der Anforderungsparameter jedoch ändern, wird der Fehler `ConflictException` zurückgegeben.

Wenn Sie kein eigenes Client-Token angeben, generieren die AWS SDKs automatisch ein Client-Token für die Anfrage, um sicherzustellen, dass sie idempotent ist.

Ein Client-Token kann eine beliebige Zeichenfolge sein, die bis zu 64 ASCII-Zeichen enthält. Sie sollten dieselben Client-Token nicht für verschiedene Anforderungen wiederverwenden.

Um mithilfe der API eine idempotente StartSnapshot Anfrage mit Ihrem eigenen Client-Token zu stellen

Geben Sie den Anforderungsparameter `ClientToken` an.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Um eine idempotente StartSnapshot Anfrage mit Ihrem eigenen Client-Token zu stellen, verwenden Sie das AWS CLI

Geben Sie den Anforderungsparameter `client-token` an.

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

Fehlerhafte Wiederholungsversuche für direkte EBS-APIs

Die AWS -SDKs implementieren die automatische Wiederholungslogik für Anfragen, die Fehlerantworten zurückgeben. Sie können die Wiederholungs-Einstellungen für AWS -SDKs konfigurieren. Weitere Informationen finden Sie in der Dokumentation Ihres SDK.

Sie können die AWS CLI so konfigurieren, dass einige fehlgeschlagene Anforderungen automatisch wiederholt werden. Weitere Informationen zur Konfiguration von Wiederholungsversuchen für den AWS CLI finden Sie unter AWS CLI Wiederholungen im Benutzerhandbuch. AWS Command Line Interface

Die AWS -Abfrage-API unterstützt keine Wiederholungslogik für fehlgeschlagene Anfragen. Wenn Sie HTTP- oder HTTPS-Anforderungen verwenden, müssen Sie eine Wiederholungslogik in Ihre Client-Anwendung implementieren.

Die folgende Tabelle zeigt die möglichen API-Fehlerreaktionen. Einige API-Fehler sind wiederholbar. Ihre Clientanwendung sollte fehlgeschlagene Anforderungen, die einen wiederholbaren Fehler erhalten, immer wiederholen.

Fehler	Antwortcode	Description	Ausgeworfen von	Wiederholbar?
`InternalServerException`	500	Die Anfrage ist aufgrund eines Netzwerk- oder AWS Serverprobleme fehlgeschlagen.	Alle APIs	Ja
`ThrottlingException`	400	Die Anzahl der API-Anfragen hat das maximal zulässige Drosselungslimit für API-Anfragen für das Konto überschritten.	Alle APIs	Ja
`RequestThrottleException`	400	Die Anzahl der API-Anfragen hat den maximal nzulässige Grenzwert für die Drosselung von	GetSnapshotBlock | PutSnapshotBlock	Ja

Fehler	Antwortcode	Description	Ausgeworfen von	Wiederholbar?
		API-Anfragen für den Snapshot überschritten.		
`ValidationException` mit Nachricht „`Failed to read block data`“	400	Der bereitgestellte Datenblock konnte nicht gelesen werden.	PutSnapshotBlock	Ja
`ValidationException` mit jeder anderen Nachricht	400	Die Anforderungssyntax ist falsch formatiert oder die Eingabe erfüllt nicht die vom AWS-Service festgelegten Einschränkungen.	Alle APIs	Nein
`ResourceNotFoundException`	404	Die angegebene Snapshot-ID ist nicht vorhanden.	Alle APIs	Nein

Fehler	Antwortcode	Description	Ausgeworfen von	Wiederholbar?
`ConflictException`	409	Das angegebene Client-Token wurde zuvor in einer ähnlichen Anfrage mit anderen Anfragepa rametern verwendet. Weitere Informationen finden Sie unter Stellen StartSnapshot Sie die Idempotenz bei API-Anfragen sicher.	StartSnapshot	Nein
`AccessDeniedException`	403	Sie sind nicht berechtigt, die angefragte Operation durchzuführen.	Alle APIs	Nein
`ServiceQuotaExceededException`	402	Die Anfrage schlug fehl, weil die Erfüllung der Anfrage ein oder mehrere abhängige Service Quotas für Ihr Konto überschreiten würde.	Alle APIs	Nein

Fehler	Antwortcode	Description	Ausgeworfen von	Wiederholbar?
`InvalidSignatureException`	403	Die Autorisierungssignatur der Anfrage ist abgelaufen. Sie können die Anfrage erst wiederholen, nachdem Sie die Autorisierungssignatur aktualisiert haben.	Alle APIs	Nein

Optimieren Sie die Leistung für direkte EBS-APIs

Sie können API-Anforderungen gleichzeitig ausführen. Unter der Annahme, dass die PutSnapshotBlock Latenz 100 ms beträgt, kann ein Thread 10 Anfragen in einer Sekunde verarbeiten. Wenn Ihre Client-Anwendung dazu mehrere Threads und Verbindungen erstellt (z. B. 100 Verbindungen), kann sie insgesamt 1000 (10 * 100) Anforderungen pro Sekunde senden. Dies entspricht einem Durchsatz von rund 500 MB pro Sekunde.

Die folgende Liste enthält einige Punkte, auf die Sie für Ihre Anwendung achten müssen:

- Verwendet jeder Thread eine separate Verbindung? Wenn die Verbindungen für die Anwendung eingeschränkt sind, warten mehrere Threads, bis eine Verbindung verfügbar ist, und Sie werden einen geringeren Durchsatz feststellen.
- Gibt es eine Wartezeit in der Anwendung zwischen zwei Put-Anforderungen? Dies reduziert den effektiven Durchsatz eines Threads.
- Das Bandbreitenlimit für die Instanz — Wenn die Bandbreite auf der Instanz von anderen Anwendungen gemeinsam genutzt wird, kann dies den verfügbaren Durchsatz für PutSnapshotBlock Anfragen einschränken.

Berücksichtigen Sie die übrigen Workloads, die im Konto möglicherweise ausgeführt werden, um Engpässe zu vermeiden. Sie sollten auch Wiederholungsmechanismen in Ihre EBS-Direct-APIs-Workflows einbauen, um Ablehnungen, Timeouts und die Nichtverfügbarkeit von Services zu behandeln.

Überprüfen Sie die EBS-Direct-APIs-Service Quotas, um die maximale Zahl der API-Anforderungen zu ermitteln, die Sie pro Sekunde ausführen können. Weitere Informationen finden Sie unter Amazon Elastic Block Store-Endpunkte und -Kontingente in der Allgemeinen Referenz zu AWS .

Service-Endpunkte für direkte EBS-APIs

Ein Endpunkt ist eine URL, die als Einstiegspunkt für einen AWS Webdienst dient. EBS-Direct-APIs unterstützen die folgenden Endpunkttypen:

- IPv4-Endpunkte
- Dual-stack Endpunkte, die sowohl IPv4 als auch IPv6 unterstützen
- FIPS-Endpunkte

Wenn Sie eine Anfrage stellen, können Sie den Endpunkt und die Region angeben, die verwendet werden sollen. Wenn Sie keinen Endpunkt festlegen, wird standardmäßig der IPv4-Endpunkt verwendet. Um einen anderen Endpunkttyp zu verwenden, müssen Sie ihn in Ihrer Anforderung angeben. Beispiele für diese Vorgehensweise finden Sie unter Angeben von Endpunkten.

Weitere Informationen zu Regionen finden Sie unter Regionen und Availability Zones im Amazon EC2-Benutzerhandbuch. Eine Liste der Endpunkte für EBS-Direct-APIs finden Sie unter Endpunkte für EBS-Direct-APIs in der Allgemeine Amazon Web Services-Referenz.

Themen

- IPv4-Endpunkte
- Dual-stack Endpunkte (IPv4 und IPv6)
- FIPS-Endpunkte
- Angeben von Endpunkten

IPv4-Endpunkte

IPv4 Endpunkte unterstützen nur IPv4-Datenverkehr. IPv4-Endpunkte sind für alle Regionen verfügbar.

EBS Direct APIs unterstützen nur regionale IPv4-Endpunkte, die Sie für Ihre Anfragen verwenden können. Sie müssen die Region als Teil des Endpunktnamens angeben. Die Endpunktnamen verwenden die folgende Namenskonvention:

- `ebs.region.amazonaws.com`

Um Ihre Anfragen beispielsweise an den `us-east-2` IPv4-Endpunkt weiterzuleiten, müssen Sie ihn `ebs.us-east-2.amazonaws.com` als Endpunkt angeben. Eine Liste der Endpunkte für EBS-Direct-APIs finden Sie unter Endpunkte für EBS-Direct-APIs in der Allgemeine Amazon Web Services-Referenz.

Preisgestaltung

Für Daten, die direkt zwischen EBS-direct-APIs und Amazon-EC2-Instances unter Verwendung eines IPv4-Endpunkts in derselben Region übertragen werden, fallen keine Gebühren an. Wenn es jedoch Zwischendienste wie AWS PrivateLink Endpunkte, NAT Gateway oder Amazon VPC Transit Gateways gibt, werden Ihnen die damit verbundenen Kosten in Rechnung gestellt.

Dual-stack Endpunkte (IPv4 und IPv6)

Dual-stack Endpunkte unterstützen sowohl IPv4- als auch IPv6-Verkehr. Dual-stack Endpunkte sind für alle Regionen verfügbar.

Um IPv6 verwenden zu können, müssen Sie einen Dual-Stack-Endpunkt verwenden. Wenn Sie eine Anfrage an einen Dual-Stack-Endpunkt stellen, löst die Endpunkt-URL eine IPv6- oder eine IPv4-Adresse auf, je nachdem, welches Protokoll Ihr Netzwerk und Ihr Client verwendet.

EBS Direct-APIs unterstützen nur regionale Dual-Stack-Endpunkte, was bedeutet, dass Sie die Region als Teil des Endpunktnamens angeben müssen. Dual-stack Endpunktnamen verwenden die folgende Namenskonvention:

- `ebs.region.api.aws`

Beispielsweise ist der Dual-Stack-Endpunktname für die Region `eu-west-1` `ebs.eu-west-1.api.aws`. Eine Liste der Endpunkte für EBS-Direct-APIs finden Sie unter Endpunkte für EBS-Direct-APIs in der Allgemeine Amazon Web Services-Referenz.

Preisgestaltung

Für Daten, die direkt zwischen EBS direct APIs und Amazon-EC2-Instances unter Verwendung einem Dual-Stack-Endpunkt in derselben Region übertragen werden, fallen keine Gebühren an. Wenn es jedoch Zwischendienste wie AWS PrivateLink Endpoints, NAT Gateway oder Amazon VPC Transit Gateways gibt, werden Ihnen die damit verbundenen Kosten in Rechnung gestellt.

FIPS-Endpunkte

Die direkten EBS-APIs bieten FIPS-validated IPv4- und Dual-Stack-Endpunkte (IPv4 und IPv6) für die folgenden Regionen:

- `us-east-1` – USA Ost (Nord-Virginia)
- `us-east-2` – USA Ost (Ohio)
- `us-west-1` – USA West (Nordkalifornien)
- `us-west-2` – USA West (Oregon)
- `ca-central-1` – Kanada (Zentral)
- `ca-west-1`— Kanada West (Calgary)

FIPS-IPv4-Endpunkte verwenden die folgende Namenskonvention: `ebs-fips.`*`region`*`.amazonaws.com`. Beispielsweise ist der FIPS-IPv4-Endpunkt für `us-east-1` `ebs-fips.us-east-1.amazonaws.com`.

FIPS-Dual-Stack-Endpunkte verwenden die folgende Namenskonvention: `ebs-fips.`*`region`*`.api.aws`. Beispielsweise ist der FIPS-Dual-Stack-Endpunkt für `us-east-1` `ebs-fips.us-east-1.api.aws`.

Weitere Informationen über FIPS-Endpunkte finden Sie unter FIPS-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Angeben von Endpunkten

Dieser Abschnitt enthält einige Beispiele dafür, wie Sie einen Endpunkt angeben, wenn Sie eine Anforderung stellen.

AWS CLI

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS CLI einen Endpunkt für die `us-east-2`-Region angeben.

- Dual-stack

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

AWS SDK for Java 2.x

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS SDK for Java 2.x einen Endpunkt für die `us-east-2`-Region angeben.

- Dual-stack

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-
east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com",
 "us-east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

AWS SDK for Go

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS SDK für Go einen Endpunkt für die `us-east-2`-Region angeben.

- Dual-stack

```
sess := session.Must(session.NewSession())
```

```
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

AWS SDK-Codebeispiele für direkte EBS-APIs

Die folgenden Codebeispiele zeigen, wie direkte EBS-APIs mit einem AWS Software Development Kit (SDK) verwendet werden.

Aktionen

- Verwenden Sie StartSnapshot mit einem AWS SDK oder CLI
- Verwenden Sie PutSnapshotBlock mit einem AWS SDK oder CLI
- Verwenden Sie CompleteSnapshot mit einem AWS SDK oder CLI

Verwenden Sie **`StartSnapshot`** mit einem AWS SDK oder CLI

Das folgende Codebeispiel zeigt die Verwendung`StartSnapshot`.

Rust

SDK für Rust

> **Note**
>
> Es läuft noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn start(client: &Client, description: &str) -> Result<String, Error> {
```

```
    let snapshot = client
        .start_snapshot()
        .description(description)
        .encrypted(false)
        .volume_size(1)
        .send()
        .await?;

    Ok(snapshot.snapshot_id.unwrap())
}
```

- API-Details finden Sie StartSnapshot in der AWS SDK for Rust API-Referenz.

Verwenden Sie **PutSnapshotBlock** mit einem AWS SDK oder CLI

Das folgende Codebeispiel zeigt die VerwendungPutSnapshotBlock.

Rust

SDK für Rust

> **Note**
>
> Es läuft noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn add_block(
    client: &Client,
    id: &str,
    idx: usize,
    block: Vec<u8>,
    checksum: &str,
) -> Result<(), Error> {
    client
        .put_snapshot_block()
        .snapshot_id(id)
        .block_index(idx as i32)
        .block_data(ByteStream::from(block))
        .checksum(checksum)
```

```
        .checksum_algorithm(ChecksumAlgorithm::ChecksumAlgorithmSha256)
        .data_length(EBS_BLOCK_SIZE as i32)
        .send()
        .await?;

    Ok(())
}
```

- API-Details finden Sie PutSnapshotBlock in der AWS SDK for Rust API-Referenz.

Verwenden Sie **CompleteSnapshot** mit einem AWS SDK oder CLI

Das folgende Codebeispiel zeigt die VerwendungCompleteSnapshot.

Rust

SDK für Rust

> **Note**
>
> Es läuft noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn finish(client: &Client, id: &str) -> Result<(), Error> {
    client
        .complete_snapshot()
        .changed_blocks_count(2)
        .snapshot_id(id)
        .send()
        .await?;

    println!("Snapshot ID {}", id);
    println!("The state is 'completed' when all of the modified blocks have been
 transferred to Amazon S3.");
    println!("Use the get-snapshot-state code example to get the state of the
 snapshot.");

    Ok(())
}
```

- API-Details finden Sie CompleteSnapshot in der AWS SDK for Rust API-Referenz.

Erstellen Sie eine private Verbindung zwischen einer VPC und den direkten EBS-APIs

Sie können eine private Verbindung zwischen Ihrer VPC und EBS-Direct-APIs herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt durch AWS PrivateLink erstellen. Sie können auf EBS wie in Ihrer VPC zugreifen, ohne dass dafür ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect -Verbindung notwendig ist. Die Instances in Ihrer VPC benötigen für die Kommunikation mit EBS-Direct-APIs keine öffentlichen IP-Adressen.

Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren.

Weitere Informationen finden Sie AWS PrivateLink im Handbuch unter Access AWS-Services through. AWS PrivateLink

Überlegungen zu VPC-Endpunkten für EBS-Direct-APIs

Bevor Sie einen Schnittstellen-VPC-Endpunkt für EBS-Direct-APIs einrichten, lesen Sie Überlegungen im AWS PrivateLink -Leitfaden.

Standardmäßig wird über den Endpunkt vollständiger Zugriff auf EBS-Direct-APIs erlaubt. Sie können den Zugriff auf den Schnittstellenendpunkt mithilfe von VPC-Endpunktrichtlinien steuern. Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf direkte EBS-APIs steuert. Die Richtlinie gibt die folgenden Informationen an:

- Der Prinzipal, der Aktionen ausführen kann.
- Die Aktionen, die ausgeführt werden können.
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

Das Folgende ist ein Beispiel für eine Endpunktrichtlinie für direkte EBS-APIs. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie Zugriff auf alle direkten EBS-API-Aktionen auf

allen Ressourcen, mit Ausnahme von Snapshots, die mit Schlüssel `Environment` und Wert gekennzeichnet sind. `Test`

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Erstellen eines Schnittstellen-VPC-Endpunkts für EBS-Direct-APIs

Sie können einen VPC-Endpunkt für EBS-Direct-APIs-Service entweder über die Amazon VPC-Konsole oder die AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen VPC-Endpunkt für direkte EBS-APIs mit einem der folgenden Dienstnamen:

- `com.amazonaws.`*`region`*`.ebs`
- `com.amazonaws.`*`region`*`.ebs-fips`— Um einen VPC-Schnittstellen-Endpunkt zu erstellen, der dem US-amerikanischen Regierungsstandard Federal Information Processing Standard (FIPS) Publication 140-2 entspricht.

> **Note**
>
> FIPS-compliant Schnittstellen-VPC-Endpunkte können für die folgenden Regionen erstellt werden: `us-east-1` | | | |. `us-east-2` `us-west-1` `us-west-2` `ca-central-1` `ca-west-1` FIPS-compliant Schnittstellen-VPC-Endpunkte unterstützen sowohl IPv4- als auch IPv6-Verkehr.

Wenn Sie einen privaten DNS für den Endpunkt aktivieren, können Sie mit seinem standardmäßigen DNS-Namen für die Region, beispielsweise `ebs.us-east-1.amazonaws.com`, API-Anforderungen an EBS-Direct-APIs senden.

Protokollieren Sie direkte EBS-API-Aufrufe mit AWS CloudTrail

Die direkten EBS-APIs sind in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst Aufrufe der direkten EBS-APIs als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von AWS-Managementkonsole und Codeaufrufen an die direkten EBS-APIs. Anhand der gesammelten Informationen können Sie ermitteln CloudTrail, welche Anfrage an die direkten EBS-APIs gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details.

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 Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Eventverlauf 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 CloudTrail Lake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Alle Trails, die mit dem erstellt wurden, AWS-Managementkonsole sind multiregional. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Wanderweg mit mehreren Regionen zu erstellen, da du alle Aktivitäten AWS-Regionen in deinem Konto aufzeichnest. 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-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Lake Event Data Stores

CloudTrail Mit Lake können Sie SQL-based Abfragen zu Ihren Ereignissen 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 Das Speichern und Abfragen von Lake Event-Daten ist mit Kosten verbunden. 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.

EBS Direct APIs, Daten, Ereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die an oder in einer Ressource ausgeführt werden. Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Standardmäßig werden CloudTrail keine Datenereignisse protokolliert. Der CloudTrail Event-Verlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

Sie können Datenereignisse für die Ressourcentypen der direkten EBS-APIs protokollieren AWS CLI, indem Sie die CloudTrail Konsole oder CloudTrail API-Operationen verwenden. Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit dem AWS-Managementkonsole und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

Sie können die folgenden direkten EBS-API-Operationen als Datenereignisse protokollieren.

- ListSnapshotBlocks
- ListChangedBlocks
- GetSnapshotBlock
- PutSnapshotBlock

> **Note**
>
> Wenn Sie eine Aktion an einem Snapshot ausführen, der für Sie freigegeben ist, werden Datenereignisse nicht an das AWS Konto gesendet, dem der Snapshot gehört.

Verwaltungsereignisse für direkte EBS-APIs in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die für Ressourcen in Ihrem AWS-Konto Unternehmen ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

Der Dienst EBS Direct APIs protokolliert die folgenden Operationen auf Steuerungsebene CloudTrail als Verwaltungsereignisse.

- StartSnapshot
- CompleteSnapshot

Beispiele für Ereignisse mit EBS Direct APIs

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Im Folgenden finden Sie CloudTrail Beispielereignisse für die direkten EBS-APIs.

StartSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
```

```
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

ListSnapshotBlocks


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
```

```
}
```

ListChangedBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
```

```
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrail Datensatzinhalte.

Häufig gestellte Fragen zu direkten EBS-APIs

Kann auf einen Snapshot über EBS-Direct-APIs zugegriffen werden, wenn er den Status „Ausstehend“ hat?

Nein. Auf einen Snapshot kann nur zugegriffen werden, wenn er den Status „Abgeschlossen“ hat.

Werden die Block-Indizes in numerischer Reihenfolge von EBS-Direct-APIs zurückgegeben?

Ja. Die Block-Indizes sind eindeutig und werden in numerischer Reihenfolge zurückgegeben.

Kann ich eine Anfrage mit einem MaxResults Parameterwert unter 100 einreichen?

Nein. Der kleinste MaxResult Parameterwert, den Sie verwenden können, ist 100. Wenn Sie eine Anfrage mit einem MaxResult Parameterwert unter 100 einreichen und der Snapshot mehr als 100 Blöcke enthält, gibt die API mindestens 100 Ergebnisse zurück.

Kann ich API-Anfragen gleichzeitig ausführen?

Sie können API-Anforderungen gleichzeitig ausführen. Berücksichtigen Sie die übrigen Workloads, die im Konto möglicherweise ausgeführt werden, um Engpässe zu vermeiden.

Sie sollten auch Wiederholungsmechanismen in Ihre EBS-Direct-APIs-Workflows einbauen, um Ablehnungen, Timeouts und die Nichtverfügbarkeit von Services zu behandeln. Weitere Informationen finden Sie unter Optimieren Sie die Leistung für direkte EBS-APIs.

Überprüfen Sie die EBS-Direct-APIs-Service Quotas, um die Zahl der API-Anforderungen zu ermitteln, die Sie pro Sekunde ausführen können. Weitere Informationen finden Sie unter Amazon Elastic Block Store-Endpunkte und -Kontingente in der Allgemeinen Referenz zu AWS .

Ist es möglich, beim Ausführen der ListChangedBlocks Aktion eine leere Antwort zu erhalten, obwohl der Snapshot Blöcke enthält?

Ja. Wenn die geänderten Blöcke im Snapshot knapp sind, ist die Antwort möglicherweise leer, während die API den Token-Wert „Nächste Seite“ zurückgibt. Mithilfe des Token-Werts „Nächste Seite“ können Sie zur nächsten Ergebnisseite fortfahren. Sie haben die letzte Ergebnisseite erreicht, wenn die API null als Wert des Tokens „Nächste Seite“ zurückgibt.

Wenn der NextToken Parameter zusammen mit einem StartingBlockIndex Parameter angegeben wird, welcher der beiden Parameter wird verwendet?

Der NextToken wird verwendet und der StartingBlockIndex wird ignoriert.

Wie lange sind Block-Token und Next-Token gültig?

Block-Token sind sieben Tage gültig. Next-Token sind 60 Minuten gültig.

Werden verschlüsselte Snapshots unterstützt?

Ja. Auf verschlüsselte Snapshots kann über EBS-Direct-APIs zugegriffen werden.

Um auf einen verschlüsselten Snapshot zuzugreifen, benötigen Sie Zugriff auf den KMS-Schlüssel, der zum Verschlüsseln des Snapshots verwendet wurde, und auf die AWS KMS Entschlüsselungsaktion. Die AWS KMS Richtlinie, die einem Benutzer zugewiesen werden soll, finden Sie im Steuern Sie den Zugriff auf direkte EBS-APIs mithilfe von IAM Abschnitt weiter oben in diesem Handbuch.

Werden öffentliche Snapshots unterstützt?

Öffentliche Snapshots werden nicht unterstützt.

Werden lokale Amazon EBS-Snapshots unterstützt? AWS Outposts

Lokale Amazon EBS-Snapshots werden nicht unterstützt. AWS Outposts

Gibt „List snapshot block (Snapshot-Block auflisten)“ alle Block-Indizes und Block-Token in einem Snapshot zurück oder nur solche, die Daten enthalten?

Es werden ausschließlich Block-Indizes und Block-Token zurückgegeben, die Daten enthalten.

Kann ich für Sicherheitsanalysen und zu Fehlerbehebungszwecken einen Verlauf der API-Aufrufe abrufen, die von EBS-Direct-APIs in meinem Konto gesendet wurden?

Ja. Um einen Verlauf der API-Aufrufe mit EBS-Direct-APIs in Ihrem Konto zu erhalten, aktivieren Sie AWS CloudTrail in der AWS-Managementkonsole. Weitere Informationen finden Sie unter Protokollieren Sie direkte EBS-API-Aufrufe mit AWS CloudTrail.

Stellen Sie gelöschte EBS-Volumes, EBS-Snapshots und EBS-backed AMIs mit dem Papierkorb wieder her

Der Papierkorb ist eine Datenwiederherstellungsfunktion, mit der Sie versehentlich gelöschte EBS-Volumes, EBS-Snapshots und AMIs wiederherstellen können. EBS-backed Wenn Sie den Papierkorb verwenden, werden Ressourcen nach dem Löschen für einen von Ihnen angegebenen Zeitraum im Papierkorb aufbewahrt, bevor sie endgültig gelöscht werden.

Sie können eine Ressource vor Ablauf des Aufbewahrungszeitraums jederzeit aus dem Papierkorb wiederherstellen. Nachdem Sie eine Ressource aus dem Papierkorb wiederhergestellt haben, wird die Ressource aus dem Papierkorb entfernt und Sie können sie genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wird, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und kann nicht mehr wiederhergestellt werden.

Durch die Verwendung des Papierkorbs wird die Geschäftskontinuität gewährleistet, indem Ihre geschäftskritischen Daten vor versehentlichem Löschen geschützt werden.

Der Papierkorb wird als Servicefähigkeit von Amazon Elastic Block Store (Amazon EBS) bewertet. Alle AWS Services im Rahmen des Scope by Compliance-Programms (FedRAMP, HIPAA BAA, SOC usw.), in dem Amazon EBS aufgeführt ist, gelten auch für den Papierkorb.

Themen

- Unterstützte Ressourcen
- Wie funktioniert der Papierkorb?
- Überlegungen zum Thema Papierkorb
- Kontingente
- Zugehörige Services
- Preisgestaltung
- Steuern Sie den Zugriff auf den Papierkorb mit IAM
- Erstellen Sie eine Aufbewahrungsregel für den Papierkorb
- Aktualisieren Sie eine bestehende Aufbewahrungsregel für den Papierkorb
- Sperren Sie eine Aufbewahrungsregel für den Papierkorb, um zu verhindern, dass sie aktualisiert oder gelöscht wird

- Entsperren Sie eine Aufbewahrungsregel für den Papierkorb, damit sie aktualisiert oder gelöscht werden kann
- Kennzeichnen Sie eine Aufbewahrungsregel für den Papierkorb
- Löschen Sie eine Aufbewahrungsregel für den Papierkorb, um zu verhindern, dass Ressourcen aufbewahrt werden
- Stellen Sie gelöschte Schnappschüsse aus dem Papierkorb wieder her
- Stellen Sie gelöschte Volumes aus dem Papierkorb wieder her
- Stellen Sie gelöschte AMIs aus dem Papierkorb wieder her
- Überwachen Sie den Papierkorb mithilfe von Amazon EventBridge
- Überwachen Sie den Papierkorb mit AWS CloudTrail
- Dienstendpunkte für den Papierkorb
- Erstellen Sie eine private Verbindung zwischen einer VPC und dem Papierkorb

Unterstützte Ressourcen

Der Papierkorb unterstützt das Erstellen der folgenden Ressourcentypen:

- Amazon-EBS-Volumes
- Amazon EBS snapshots

> **Important**
>
> Die Aufbewahrungsregeln für den Papierkorb gelten auch für archivierte Snapshots auf der Archivspeicherebene. Wenn Sie einen archivierten Snapshot löschen, der einer Aufbewahrungsregel entspricht, wird dieser archivierte Snapshot für den in der Aufbewahrungsregel festgelegten Archivierungszeitraum im Papierkorb beibehalten. Archivierte Snapshots werden mit dem Satz für archivierte Snapshots abgerechnet, während sie sich im Papierkorb befinden.

- Amazon Amazon Machine Images (AMIs) EBS-backed

> **Note**
>
> Aufbewahrungsregeln gelten auch für deaktivierte AMIs.

Wie funktioniert der Papierkorb?

Um den Papierkorb zu aktivieren und zu verwenden, müssen Sie Aufbewahrungsregeln in den AWS Regionen erstellen, in denen Sie Ihre Ressourcen schützen möchten. Die Aufbewahrungsregeln umfassen Folgendes:

- Der Ressourcentyp, den Sie schützen möchten (Volumes, Snapshots oder AMIs).
- Der Typ der Aufbewahrungsregel:
  - Tag-level Aufbewahrungsregeln — Diese Aufbewahrungsregeln verwenden Ressourcen-Tags, um die zu schützenden Ressourcen zu identifizieren. Für jede Aufbewahrungsregel geben Sie einen oder mehrere Tag-Schlüssel/Wert-Paare an. Ressourcen (des angegebenen Typs), die über mindestens eines dieser Tag-Schlüssel-Wert-Paare verfügen, werden beim Löschen automatisch im Papierkorb aufbewahrt. Verwenden Sie diese Art von Aufbewahrungsregel, um bestimmte Ressourcen in Ihrem Konto anhand ihrer Stichwörter zu schützen.
  - Region-level Aufbewahrungsregeln — Diese Aufbewahrungsregeln gelten standardmäßig für alle Ressourcen (des angegebenen Typs) in der Region, auch wenn die Ressourcen nicht markiert sind. Sie können jedoch Ausschluss-Tags angeben, um Ressourcen mit bestimmten Tags auszuschließen. Verwenden Sie diese Art von Aufbewahrungsregel, um alle Ressourcen eines bestimmten Typs in einer Region zu schützen.
- Der Aufbewahrungszeitraum, um Ressourcen nach dem Löschen aufzubewahren. Nach Ablauf dieses Zeitraums werden die Ressourcen dauerhaft aus dem Papierkorb gelöscht. Die unterstützten Aufbewahrungsfristen sind:
  - EBS-Volumes: 1 — 7 Tage
  - EBS-Snapshots und EBS-backed AMIs: 1 — 365 Tage

Während sich eine Ressource im Papierkorb befindet, können Sie sie jederzeit zur Verwendung wiederherstellen. Die Ressource verbleibt im Papierkorb, bis eines der folgenden Ereignisse eintritt:

- Sie stellen den Snapshot manuell wieder her, um ihn zu verwenden. Wenn Sie eine Ressource aus dem Papierkorb wiederherstellen, wird sie aus dem Papierkorb entfernt und kann sofort verwendet werden. Sie können wiederhergestellte Ressourcen genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden.
- Der Aufbewahrungszeitraum läuft ab. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wurde, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und sie kann nicht mehr angezeigt oder wiederhergestellt werden.

Überlegungen zum Thema Papierkorb

Bei der Arbeit mit Papierkorb und Aufbewahrungsregeln gelten die folgenden Überlegungen.

Allgemeine Überlegungen

- Gelöschte Ressourcen werden nur dann in den Papierkorb verschoben, wenn sie einer vorhandenen Aufbewahrungsregel entsprechen. Wenn Sie eine Ressource löschen, die keiner Aufbewahrungsregel entspricht, oder wenn Sie zu diesem Zeitpunkt keine Aufbewahrungsregeln haben, wird diese Ressource dauerhaft gelöscht; sie wird nicht in den Papierkorb verschoben.
- **Important**

  Aufbewahrungsregeln folgen einem Konsistenzmodell für die erste Aufbewahrungsregel, die pro Ressourcentyp und pro Region in Ihrem Konto erstellt wird. Wenn Sie Ihre erste Aufbewahrungsregel für einen Ressourcentyp in einer Region erstellen, wird diese Regel möglicherweise nicht aktiv und Sie beginnen sofort mit der Aufbewahrung von Ressourcen. Alle nachfolgenden Aufbewahrungsregeln, die Sie für denselben Ressourcentyp in derselben Region erstellen, werden jedoch aktiv und beginnen fast sofort mit der Aufbewahrung von Ressourcen.
- Wenn eine Ressource mehreren Aufbewahrungsregeln entspricht, wenn er gelöscht wird, hat die Aufbewahrungsregel mit dem längsten Aufbewahrungszeitraum Vorrang.
- Sie können eine Ressource nicht manuell aus dem Papierkorb löschen. Die Ressource wird automatisch gelöscht, wenn sein Aufbewahrungszeitraum abläuft.
- Während sich eine Ressource im Papierkorb befindet, können Sie sie nur anzeigen, wiederherstellen oder ihre Tags ändern. Bevor Sie die Ressource auf andere Weise verwenden können, müssen Sie ihn zuerst wiederherstellen.
- Wenn eine Ressource AWS-Service, wie AWS Backup oder Amazon Data Lifecycle Manager, eine Ressource löscht, die einer Aufbewahrungsregel entspricht, wird diese Ressource automatisch im Papierkorb aufbewahrt. Bei Bedarf können Sie verhindern, dass diese Ressourcen beim Löschen in den Papierkorb gelangen, indem Sie diese Ressourcen kennzeichnen und diese Tags dann als Ausschluss-Tags zu Ihren Aufbewahrungsregeln hinzufügen.
- Wenn eine Ressource in den Papierkorb gesendet wird, wird der Ressource das folgende vom System generierte Tag zugewiesen:
  - Tag-Schlüssel – `aws:recycle-bin:resource-in-bin`
  - Tag-Wert – `true`

Sie können dieses Tag nicht manuell bearbeiten oder löschen. Wenn die Ressource aus dem Papierkorb wiederhergestellt wird, wird das Tag automatisch entfernt.

Überlegungen zu -Volumes

- Volumes, die aufgrund einer Instanzbeendigung oder eines Austauschs des Root-Volumes gelöscht wurden, sind durch den Papierkorb geschützt.
- Volumes, die nicht erstellt werden können, werden beim Löschen nicht durch den Papierkorb geschützt.
- Volumes mit fehlgeschlagenen Instanzstarts werden beim Löschen nicht durch den Papierkorb geschützt.
- Volumes verwalteter Instanzen werden beim Löschen nicht durch den Papierkorb geschützt.
- Die laufende Erstellung oder Änderung eines Volumes wird nicht unterbrochen, wenn das Volume in den Papierkorb verschoben wird. Das bedeutet, dass Ihnen auch dann eine entsprechende Rechnung gestellt wird, wenn das Volume mit einem von Amazon EBS bereitgestellten Tarif für die Volumeninitialisierung erstellt wurde.
- Volumes im Papierkorb werden auf die gleiche Weise auf Ihre Kontingente angerechnet wie reguläre Volumes.
- Volumes im Papierkorb werden nach Ablauf der Zeit, in der sie den Papierkorb verlassen haben, nicht in Rechnung gestellt. Sie können diese Volumes nicht wiederherstellen, aber Sie können sie finden, falls sie noch nicht gelöscht wurden.
- Das `deleteVolume` Ereignis wird erst gesendet, nachdem das Volume aus dem Papierkorb gelöscht wurde. Dieses Ereignis wird nicht ausgelöst, wenn das Volume in den Papierkorb verschoben wird.

Überlegungen zu Snapshots

- **Important**

  Wenn Sie über Aufbewahrungsregeln für AMIs und die zugehörigen Snapshots verfügen, sollten Sie den Aufbewahrungszeitraum für die Snapshots gleich oder länger als den Aufbewahrungszeitraum für die AMIs festlegen. Dadurch löscht der Papierkorb die mit einem AMI verknüpften Snapshots nicht, bevor das AMI selbst gelöscht wird, da das AMI ansonsten nicht wiederhergestellt werden könnte.

- Wenn ein Snapshot für die schnelle Snapshot-Wiederherstellung aktiviert ist, wenn er gelöscht wird, wird die schnelle Snapshot-Wiederherstellung kurz nach dem Verschieben des Snapshots in den Papierkorb automatisch deaktiviert.
  - Wenn Sie den Snapshot wiederherstellen, bevor die schnelle Snapshot-Wiederherstellung für den Snapshot deaktiviert wird, bleibt er aktiviert.
  - Wenn Sie den Snapshot wiederherstellen, nachdem die schnelle Snapshot-Wiederherstellung deaktiviert wurde, bleibt er deaktiviert. Bei Bedarf müssen Sie die schnelle Snapshot-Wiederherstellung manuell wieder aktivieren.
- Wenn ein Snapshot freigegeben ist, wenn er gelöscht wird, wird die Freigabe automatisch aufgehoben, wenn er in den Papierkorb verschoben wird. Wenn Sie den Snapshot wiederherstellen, werden alle vorherigen Freigabeberechtigungen automatisch wiederhergestellt.
- Wenn ein Snapshot, der von einem anderen AWS Dienst erstellt wurde, z. B. in den Papierkorb verschoben AWS Backup wird und Sie diesen Snapshot später aus dem Papierkorb wiederherstellen, wird er nicht mehr von dem AWS Dienst verwaltet, der ihn erstellt hat. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr länger benötigt wird.

Überlegungen für AMIs

- Nur EBS-backed Amazon-AMIs werden unterstützt.
- **Important**

  Wenn Sie über Aufbewahrungsregeln für AMIs und die zugehörigen Snapshots verfügen, sollten Sie den Aufbewahrungszeitraum für die Snapshots gleich oder länger als den Aufbewahrungszeitraum für die AMIs festlegen. Dadurch löscht der Papierkorb die mit einem AMI verknüpften Snapshots nicht, bevor das AMI selbst gelöscht wird, da das AMI ansonsten nicht wiederhergestellt werden könnte.
- Wenn ein AMI freigegeben ist, wenn es gelöscht wird, wird die Freigabe automatisch aufgehoben, wenn es in den Papierkorb verschoben wird. Wenn Sie das AMI wiederherstellen, werden alle vorherigen Freigabeberechtigungen automatisch wiederhergestellt.
- Bevor Sie ein AMI aus dem Papierkorb wiederherstellen können, müssen Sie zunächst alle zugehörigen Snapshots aus dem Papierkorb wiederherstellen und sicherstellen, dass sie sich im Status befinden. `available`

- Wenn die Snapshots, die mit dem AMI verknüpft sind, aus dem Papierkorb gelöscht werden, kann das AMI nicht mehr wiederhergestellt werden. Das AMI wird nach Ablauf der Aufbewahrungsfrist gelöscht.
- Wenn ein AMI, das von einem anderen AWS Dienst wie AWS Backup erstellt wurde, in den Papierkorb gesendet wird und Sie dieses AMI später aus dem Papierkorb wiederherstellen, wird es nicht mehr von dem Dienst verwaltet, der AWS es erstellt hat. Sie müssen das letzte AMI manuell löschen, wenn es nicht mehr benötigt wird.

Überlegungen zu den Snapshot-Richtlinien von Amazon Data Lifecycle Manager

- Wenn der Amazon Data Lifecycle Manager einen Snapshot löscht, der einer Aufbewahrungsregel entspricht, wird dieser Snapshot automatisch im Papierkorb beibehalten.
- Wenn Amazon Data Lifecycle Manager einen Snapshot löscht und ihn an den Papierkorb sendet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, und Sie den Snapshot manuell aus dem Papierkorb wiederherstellen, müssen Sie diesen Snapshot manuell löschen, wenn er nicht mehr benötigt wird. Amazon Data Lifecycle Manager verwaltet den Snapshot nicht mehr.
- Wenn Sie einen Snapshot, der von einer Richtlinie erstellt wurde, manuell löschen und sich dieser Snapshot im Papierkorb befindet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot nicht. Amazon Data Lifecycle Manager verwaltet die Snapshots nicht, während sie im Papierkorb gespeichert sind.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, bevor der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot, sobald der Aufbewahrungsschwellenwert der Richtlinie erreicht wird.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, nachdem der Aufbewahrungsschwellenwert der Richtlinie erreicht wurde, löscht Amazon Data Lifecycle Manager den Snapshot nicht mehr. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr benötigt wird.

Überlegungen für AWS Backup

- Wenn AWS Backup einen Snapshot löscht, der einer Aufbewahrungsregel entspricht, wird dieser Snapshot automatisch im Papierkorb aufbewahrt.

Überlegungen zu archivierten Snapshots

- Die Aufbewahrungsregeln für den Papierkorb gelten auch für archivierte Snapshots auf der Archivspeicherebene. Wenn Sie einen archivierten Snapshot löschen, der einer Aufbewahrungsregel entspricht, wird dieser archivierte Snapshot für den in der Aufbewahrungsregel festgelegten Archivierungszeitraum im Papierkorb beibehalten.

  Archivierte Snapshots werden mit dem Satz für archivierte Snapshots abgerechnet, während sie sich im Papierkorb befinden.

  Wenn eine Aufbewahrungsregel einen archivierten Snapshot vor Ablauf der Mindestarchivierungsdauer von 90 Tagen aus dem Papierkorb löscht, werden Ihnen die verbleibenden Tage in Rechnung gestellt. Weitere Informationen finden Sie unter Preise und Abrechnung archivierter Snapshots.

  Um einen archivierten Snapshot zu verwenden, der sich im Papierkorb befindet, müssen Sie den Snapshot zunächst aus dem Papierkorb wiederherstellen und ihn dann von der Archivstufe auf die Standardstufe zurückbringen.

Kontingente

Die folgenden Kontingente gelten für den Papierkorb.

Kontingent	Standardkontingent			
Aufbewahrungsregeln pro Region	250			
Tag-Schlüssel/Wert-Paare pro Aufbewahrungsregel	50			

Zugehörige Services

Der Papierkorb funktioniert in Verbindung mit den folgenden Services:

- AWS CloudTrail – Ermöglicht es Ihnen, Ereignisse aufzuzeichnen, die im Papierkorb erfolgen. Weitere Informationen finden Sie unter Überwachen Sie den Papierkorb mit AWS CloudTrail.

Preisgestaltung

Für die Verwendung des Papierkorbs und von Aufbewahrungsregeln fallen keine zusätzlichen Gebühren an. Weitere Informationen finden Sie unter Amazon EBS – Preise.

- Amazon EBS-Volumes — Volumes im Papierkorb werden zum gleichen Preis abgerechnet wie reguläre Volumes in Ihrem Konto.
- Amazon EBS-Snapshots — Snapshots im Papierkorb werden zum gleichen Preis abgerechnet wie reguläre Snapshots in Ihrem Konto.
- EBS-backed AMIs — Für AMIs im Papierkorb fallen keine zusätzlichen Gebühren an.

> **Note**
>
> Einige Ressourcen werden möglicherweise noch für kurze Zeit in der Papierkorb-Konsole oder in der AWS CLI API-Ausgabe angezeigt, nachdem ihre Aufbewahrungsfristen abgelaufen sind und sie dauerhaft gelöscht wurden. Diese Ressourcen werden Ihnen nicht in Rechnung gestellt. Die Abrechnung endet, sobald der Aufbewahrungszeitraum abgelaufen ist.

Bei der Verwendung können Sie die folgenden AWS generierten Kostenzuordnungs-Tags zur Kostenverfolgung und -zuweisung verwenden AWS Fakturierung und Kostenmanagement.

- Schlüssel: `aws:recycle-bin:resource-in-bin`
- Wert: `true`

Weitere Informationen finden Sie unter Von AWS generierte Kostenzuordnungs-Tags im AWS Fakturierung und Kostenmanagement -Benutzerhandbuch.

Steuern Sie den Zugriff auf den Papierkorb mit IAM

Standardmäßig verfügen Benutzer nicht über die Berechtigung, mit dem Papierkorb, mit Aufbewahrungsregeln oder mit Ressourcen, die sich im Papierkorb befinden, zu arbeiten. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Themen

- Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln
- Berechtigungen zum Arbeiten mit Ressourcen im Papierkorb
- Bedingungsschlüssel für den Papierkorb

Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln

Um mit Papierkorb- und Aufbewahrungsregeln arbeiten zu können, benötigen Benutzer die folgenden Berechtigungen.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `tag:GetResources`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie, die die `tag:GetResources`-Berechtigung für Konsolenbenutzer enthält. Werden einige Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rbin:CreateRule",
                "rbin:UpdateRule",
                "rbin:GetRule",
                "rbin:ListRules",
                "rbin:DeleteRule",
                "rbin:TagResource",
                "rbin:UntagResource",
                "rbin:ListTagsForResource",
                "rbin:LockRule",
                "rbin:UnlockRule",
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Berechtigungen zum Arbeiten mit Ressourcen im Papierkorb

Weitere Informationen zu den IAM-Berechtigungen, die für die Arbeit mit Ressourcen im Papierkorb erforderlich sind, finden Sie im folgenden Abschnitt:

- Berechtigungen für die Arbeit mit Volumes im Papierkorb
- Berechtigungen zum Arbeiten mit Snapshots im Papierkorb
- Berechtigungen zum Arbeiten mit AMIs im Papierkorb

Bedingungsschlüssel für den Papierkorb

Der Papierkorb definiert die folgenden Bedingungsschlüssel, die Sie im `Condition`-Element einer IAM-Richtlinie zur Kontrolle der Bedingungen, unter denen die Richtlinienanweisung angewendet wird, verwenden können. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Themen

- Robin: Request/ResourceType Bedingungsschlüssel
- Robin: Bedingungsschlüssel Attribute/ResourceType

`Robin: Request/ResourceType` Bedingungsschlüssel

Der `rbin:Request/ResourceType` Bedingungsschlüssel kann verwendet werden, um ListRules Zugriffe CreateRule und Anfragen auf der Grundlage des für den `ResourceType` Anforderungsparameter angegebenen Werts zu filtern.

Beispiel 1 — CreateRule

Die folgende Beispiel-IAM-Richtlinie erlaubt IAM-Prinzipalen nur dann, CreateRule Anfragen zu stellen, wenn der für den `ResourceType` Anforderungsparameter angegebene Wert oder ist.

`EBS_SNAPSHOT` `EC2_IMAGE` Dies ermöglicht es dem Prinzipal, neue Aufbewahrungsregeln nur für Snapshots und AMIs zu erstellen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Beispiel 2 — ListRules

Die folgende Beispiel-IAM-Richtlinie ermöglicht es IAM-Prinzipalen, nur dann ListRules Anfragen zu stellen, wenn der für den `ResourceType` Anforderungsparameter angegebene Wert lautet. `EBS_SNAPSHOT` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots aufzulisten, und verhindert, dass er Aufbewahrungsregeln für jeden anderen Ressourcentyp auflisten kann.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
```

```
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Robin: Bedingungsschlüssel Attribute/ResourceType

Der `rbin:Attribute/ResourceType` Bedingungsschlüssel kann verwendet werden, um den Zugriff auf DeleteRule, GetRule, UpdateRule, LockRule, UnlockRule TagResource UntagResource, und ListTagsForResource Anfragen basierend auf dem Wert des `ResourceType` Attributs der Aufbewahrungsregel zu filtern.

Beispiel 1 — UpdateRule

Mit der folgenden Beispiel-IAM-Richtlinie können IAM-Prinzipale nur dann UpdateRule Anfragen stellen, wenn das `ResourceType` Attribut der angeforderten Aufbewahrungsregel oder lautet. `EBS_SNAPSHOT` `EC2_IMAGE` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots und AMIs zu aktualisieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
```

```
            }
        }
    ]
}
```

Beispiel 2 — DeleteRule

Mit der folgenden Beispiel-IAM-Richtlinie können IAM-Prinzipale nur dann DeleteRule Anfragen stellen, wenn das `ResourceType` Attribut der angeforderten Aufbewahrungsregel lautet. `EBS_SNAPSHOT` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots zu löschen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Erstellen Sie eine Aufbewahrungsregel für den Papierkorb

Beim Erstellen einer Aufbewahrungsregel müssen Sie die folgenden erforderlichen Parameter angeben:

- Der zu schützende Ressourcentyp (Volumes, Snapshots oder AMIs).

- Der Typ der Aufbewahrungsregel (auf Tag-Ebene oder). Region-level Tag-level Regeln schützen nur Ressourcen, die über bestimmte Tags verfügen. Region-level Regeln schützen alle Ressourcen in der Region, können jedoch Ressourcen mit bestimmten Stichwörtern ausschließen.
- Der Aufbewahrungszeitraum, für den Ressourcen nach dem Löschen aufbewahrt werden. Nach Ablauf dieses Zeitraums werden die Ressourcen dauerhaft aus dem Papierkorb gelöscht. Die unterstützten Aufbewahrungsfristen sind:
  - EBS-Volumes: 1 — 7 Tage
  - EBS-Snapshots und EBS-backed AMIs: 1 — 365 Tage

Sie können optional auch einen Regelnamen und eine Beschreibung mit jeweils bis zu 255 Zeichen sowie Tags angeben, die Ihnen bei der Identifizierung und Organisation Ihrer Regeln helfen. Wir empfehlen, dass der Name, die Beschreibung oder die Tags keine personenbezogenen, vertraulichen oder sensiblen Informationen enthalten.

Optional können Sie die Region-level Aufbewahrungsregeln auch bei der Erstellung sperren. Wenn Sie eine Aufbewahrungsregel bei der Erstellung sperren, müssen Sie auch den Zeitraum für die Verzögerung beim Entsperren angeben, der 7 bis 30 Tage betragen kann. Aufbewahrungsregeln bleiben standardmäßig entsperrt, sofern Sie sie nicht ausdrücklich sperren.

> **Note**
>
> Aufbewahrungsregeln funktionieren nur in den Regionen, in denen sie erstellt wurden. Wenn Sie den Papierkorb in anderen Regionen verwenden möchten, müssen Sie in diesen Regionen zusätzliche Aufbewahrungsregeln erstellen.

Sie können mit einer der folgenden Methoden eine Aufbewahrungsregel für den Papierkorb erstellen.

Recycle Bin console

So erstellen Sie eine Aufbewahrungsregel auf Tag-Ebene

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) und dann Create retention rule (Aufbewahrungsregel erstellen) aus.
3. (Optional) Geben Sie im Feld Retention rule name (Name der Aufbewahrungsregel) einen aussagekräftigen Namen für die Aufbewahrungsregel ein.

4. (Optional) Geben Sie im Feld Retention rule description (Beschreibung der Aufbewahrungsregel) eine kurze Beschreibung für die Aufbewahrungsregel ein.
5. Wählen Sie unter Ressourcentyp den Ressourcentyp aus, den die Aufbewahrungsregel schützen soll. Die Aufbewahrungsregel behält nur Ressourcen dieses Typs im Papierkorb bei.
6. Wählen Sie für Wählen Sie die Ressourcen aus, die aufbewahrt werden sollen die Option Ressourcen beibehalten, die bestimmte Tags haben.
7. Geben Sie für Ressourcen-Tags die Tag-Schlüssel- und Wertepaare ein, anhand derer die Ressourcen identifiziert werden sollen, die im Papierkorb aufbewahrt werden sollen. Nur Ressourcen des angegebenen Typs, die mindestens eines der angegebenen Tags enthalten, werden gemäß der Aufbewahrungsregel aufbewahrt.
8. Geben Sie für den Aufbewahrungszeitraum die Anzahl der Tage ein, nach der gelöschte Ressourcen im Papierkorb aufbewahrt werden sollen.
9. Klicken Sie auf Create retention rule (Aufbewahrungsregel erstellen).

So erstellen Sie eine Region-level Aufbewahrungsregel

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) und dann Create retention rule (Aufbewahrungsregel erstellen) aus.
3. (Optional) Geben Sie im Feld Retention rule name (Name der Aufbewahrungsregel) einen aussagekräftigen Namen für die Aufbewahrungsregel ein.
4. (Optional) Geben Sie im Feld Retention rule description (Beschreibung der Aufbewahrungsregel) eine kurze Beschreibung für die Aufbewahrungsregel ein.
5. Wählen Sie unter Ressourcentyp den Ressourcentyp aus, den die Aufbewahrungsregel schützen soll. Die Aufbewahrungsregel behält nur Ressourcen dieses Typs im Papierkorb bei.
6. Wählen Sie für Wählen Sie die Ressourcen aus, die aufbewahrt werden sollen die Option Alle Ressourcen beibehalten aus.
7. (Optional) Um Ressourcen mit bestimmten Stichwörtern auszuschließen, geben Sie für Ausschluss-Tags bis zu fünf Tag-Schlüssel-Wert-Paare ein, anhand derer die auszuschließenden Ressourcen identifiziert werden. Ressourcen, die über eines dieser Tags verfügen, werden von der Aufbewahrungsregel ignoriert.

8. Geben Sie für den Aufbewahrungszeitraum die Anzahl der Tage ein, nach der gelöschte Ressourcen im Papierkorb aufbewahrt werden sollen.
9. (Optional) Um die Aufbewahrungsregel zu sperren, wählen Sie unter Rule lock settings (Regelsperreinstellungen) die Option Lock (Sperren) aus und geben Sie dann für Unlock delay period (Verzögerungszeitraum entsperren) den Zeitraum für die Entsperrung in Tagen an. Eine gesperrte Aufbewahrungsregel kann nicht geändert oder gelöscht werden. Um die Regel zu ändern oder zu löschen, müssen Sie sie zuerst entsperren und dann warten, bis der Zeitraum für die Verzögerung beim Entsperren abgelaufen ist. Weitere Informationen finden Sie unter Sperren Sie eine Aufbewahrungsregel für den Papierkorb, um zu verhindern, dass sie aktualisiert oder gelöscht wird.

   Um die Aufbewahrungsregel entsperrt zu lassen, behalten Sie für die Rule lock settings (Regelsperreinstellungen) die Option Unlock (Entsperren) bei. Eine entsperrte Aufbewahrungsregel kann jederzeit geändert oder gelöscht werden.

   > **Note**
   >
   > Region-level Aufbewahrungsregeln mit Ausschluss-Tags können nicht gesperrt werden.

10. Klicken Sie auf Create retention rule (Aufbewahrungsregel erstellen).

AWS CLI

So erstellen Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl create-rule. Geben Sie für `--retention-period` die Anzahl der Tage an, die gelöschte Snapshots im Papierkorb aufbewahrt werden sollen. Für`--resource-type`, geben Sie `EBS_VOLUME` für Volumes, `EBS_SNAPSHOT` für Snapshots oder `EC2_IMAGE` für AMIs an. Um eine Aufbewahrungsregel auf Tag-Ebene zu erstellen, geben Sie für die Tags an`--resource-tags`, die zur Identifizierung der Ressourcen verwendet werden sollen, die aufbewahrt werden sollen. Um eine Region-level Aufbewahrungsregel zu erstellen, lassen Sie Ressourcen mit bestimmten `--resource-tags` Tags aus und geben Sie optional an`--exclude-resource-tags`, ob diese ausgeschlossen werden sollen. Um eine Region-level Aufbewahrungsregel zu sperren, geben Sie den `--lock-configuration` Zeitraum für die Entsperrung in Tagen an und geben Sie ihn an.

```
aws rbin create-rule \
```

```
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_VOLUME|EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value \
--exclude-resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Beispiel 1

Mit dem folgenden Beispielbefehl wird eine Regel für die entsperrte Region-level Aufbewahrung erstellt, die alle gelöschten Snapshots für einen Zeitraum von 7 Tagen aufbewahrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Beispiel 2

Der folgende Beispielbefehl erstellt eine Regel auf Tag-Ebene, die gelöschte Snapshots, die mit `purpose=production` gekennzeichnet sind, für einen Zeitraum von 7 Tagen aufbewahrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Beispiel 3

Mit dem folgenden Beispielbefehl wird eine Regel Region-level zur gesperrten Aufbewahrung erstellt, die alle gelöschten Snapshots für einen Zeitraum von 7 Tagen aufbewahrt. Die Aufbewahrungsregel ist mit einer Freigabeverzögerung von 7 Tagen gesperrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Beispiel 4

Mit dem folgenden Beispielbefehl wird eine Regel Region-level zur Aufbewahrung entsperrter Dateien erstellt, die alle gelöschten Snapshots, mit Ausnahme der Schnappschüsse, die mit gekennzeichnet sind`purpose:testing`, für einen Zeitraum von 7 Tagen aufbewahrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match only production snapshots" \
--exclude-resource-tags ResourceTagKey=purpose,ResourceTagValue=testing
```

Aktualisieren Sie eine bestehende Aufbewahrungsregel für den Papierkorb

Sie können Beschreibung, Ressourcen-Tags und den Aufbewahrungszeitraum einer entsperrten Aufbewahrungsregel jederzeit aktualisieren, nachdem sie erstellt wurde. Sie können den Ressourcentyp oder den Entsperrzeitraum einer Aufbewahrungsregel nicht aktualisieren, selbst wenn die Aufbewahrungsregel entsperrt ist.

Sie können eine gesperrte Aufbewahrungsregel in keiner Weise aktualisieren. Wenn Sie eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie sie zunächst entsperren und warten, bis der Zeitraum für die Verzögerung beim Entsperren abgelaufen ist.

Wenn Sie den Zeitraum für die Entsperrverzögerung für eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie die Aufbewahrungsregel entsperren und warten, bis der aktuelle Entsperrverzögerungszeitraum abläuft. Wenn der Zeitraum für die Entsperrung abgelaufen ist, müssen Sie die Aufbewahrungsregel erneut sperren und den neuen Zeitraum für die Entsperrverzögerung angeben.

> **Note**
>
> Wir empfehlen, dass Sie keine personenbezogenen, vertraulichen oder sensiblen Informationen in die Beschreibung der Aufbewahrungsregel aufnehmen.

Nachdem Sie eine Aufbewahrungsregel aktualisiert haben, gelten die Änderungen nur für neue Ressourcen, die damit beibehalten werden. Die Änderungen wirken sich nicht auf Ressourcen aus, die zuvor an den Papierkorb gesendet wurden. Wenn Sie beispielsweise den Aufbewahrungszeitraum einer Aufbewahrungsregel aktualisieren, werden nur Snapshots, die nach

der Aktualisierung gelöscht werden, für den neuen Aufbewahrungszeitraum beibehalten. Snapshots, die vor dem Update an den Papierkorb gesendet wurden, werden weiterhin für die Dauer des vorherigen (alten) Aufbewahrungszeitraums beibehalten.

Sie können eine Aufbewahrungsregel mit einer der folgenden Methoden aktualisieren.

Recycle Bin console

So aktualisieren Sie eine Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie im Raster die zu aktualisierende Aufbewahrungsregel aus und wählen Sie dann Aktionen, Edit retention rule (Aufbewahrungsregel bearbeiten).
4. Aktualisieren Sie im Abschnitt Regeldetails den Namen der Aufbewahrungsregel und die Beschreibung der Aufbewahrungsregel nach Bedarf.
5. Aktualisieren Sie im Abschnitt Rule settings (Regeleinstellungen) die Angaben für Resource type (Ressourcentyp), Resource tags to match (Zuzuordnende Ressourcen-Tags) und Retention period (Aufbewahrungszeitraum) nach Bedarf.
6. Fügen Sie im Abschnitt Tags nach Bedarf Tags für Aufbewahrungsregeln hinzu oder entfernen Sie sie.
7. Klicken Sie auf Save retention rule (Aufbewahrungsregel speichern).

AWS CLI

So aktualisieren Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl update-rule. Geben Sie die ID der Aufbewahrungsregel an`--identifier`, für die aktualisiert werden soll`--resource-types`, und geben Sie `EBS_VOLUME` für Volumes, `EBS_SNAPSHOT` für Snapshots oder `EC2_IMAGE` für AMIs an.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_VOLUME|EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Beispiel

Der folgende Beispielbefehl aktualisiert die Aufbewahrungsregel `6lsJ2Fa9nh9`, um alle Snapshots für 7 Tage aufzubewahren, und aktualisiert ihre Beschreibung.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Sperren Sie eine Aufbewahrungsregel für den Papierkorb, um zu verhindern, dass sie aktualisiert oder gelöscht wird

Mit dem Papierkorb können Sie die Region-level Aufbewahrungsregeln jederzeit sperren.

Eine gesperrte Aufbewahrungsregel kann nicht geändert oder gelöscht werden, auch nicht von Benutzern, die über die erforderlichen IAM-Berechtigungen verfügen. Aufbewahrungsregeln können gesperrt werden, um sie vor versehentlichen oder böswilligen Änderungen und Löschungen zu schützen.

Beim Sperren einer Aufbewahrungsregel müssen Sie einen Entsperrverzögerungszeitraum angeben. Dies ist der Zeitraum, den Sie nach dem Entsperren der Aufbewahrungsregel warten müssen, bevor Sie sie ändern oder löschen können. Sie können die Aufbewahrungsregel während des Zeitraums der Entsperrverzögerung nicht ändern oder löschen. Sie können die Aufbewahrungsregel erst ändern oder löschen, wenn die Verzögerungszeit für die Entsperrung abgelaufen ist.

Sie können den Zeitrahmen für die Entsperrung nach dem Sperren der Aufbewahrungsregel nicht mehr ändern. Wenn Ihre Kontoberechtigungen beeinträchtigt wurden, haben Sie durch die Verzögerung der Entsperrung zusätzliche Zeit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Die Dauer dieses Zeitraums sollte länger sein als die Zeit, die Sie benötigen, um Sicherheitsverstöße zu erkennen und darauf zu reagieren. Um die richtige Dauer festzulegen, können Sie frühere Sicherheitsvorfälle sowie die Zeit überprüfen, die zur Identifizierung und Behebung einer Kontoverletzung benötigt wurde.

Wir empfehlen Ihnen, die EventBridge Amazon-Regeln zu verwenden, um Sie über Änderungen des Sperrstatus der Aufbewahrungsregeln zu informieren. Weitere Informationen finden Sie unter Überwachen Sie den Papierkorb mithilfe von Amazon EventBridge.

Überlegungen

- Sie können keine Aufbewahrungsregeln auf Tag-Ebene oder Region-level Aufbewahrungsregeln mit Ausschluss-Tags sperren.
- Sie können eine entsperrte Aufbewahrungsregel jederzeit sperren.
- Die Verzögerung beim Entsperren muss 7 bis 30 Tage betragen.
- Sie können eine Aufbewahrungsregel während der Dauer der Entsperrverzögerung erneut sperren. Durch das erneute Sperren der Aufbewahrungsregel wird der Zeitraum für die Entsperrverzögerung zurückgesetzt.

Sie können eine Region-level Aufbewahrungsregel mit einer der folgenden Methoden sperren.

Recycle Bin console

So sperren Sie eine Aufbewahrungsregel

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Aufbewahrungsregeln aus.
3. Wählen Sie im Raster die zu sperrende Aufbewahrungsregel aus und wählen Sie dann Actions (Aktionen), Edit retention rule (Aufbewahrungsregel bearbeiten) aus.
4. Wählen Sie im Bildschirm „Sperrung der Aufbewahrungsregel bearbeiten“ die Option Lock (Sperren) und geben Sie dann unter Unlock delay period (Verzögerungszeit für die Entsperrung) die Verzögerungszeit für die Entsperrung in Tagen an.
5. Aktivieren Sie das Kontrollkästchen I acknowledge that locking the retention rule will prevent it from being modified or deleted (Ich bin mir bewusst, dass das Sperren der Aufbewahrungsregel verhindert, dass sie geändert oder gelöscht wird) und wählen Sie dann Save (Speichern).

AWS CLI

So sperren Sie eine entsperrte Aufbewahrungsregel

Verwenden Sie den AWS CLI -Befehl lock-rule. Geben Sie für `--identifier` die ID der zu sperrenden Aufbewahrungsregel an. Geben Sie für `--lock-configuration` den Zeitraum der Entsperrverzögerung in Tagen an.

```
aws rbin lock-rule \
--identifier rule_ID \
```

```
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Beispiel

Der folgende Beispielbefehl sperrt die Aufbewahrungsregel `6lsJ2Fa9nh9` und legt den Zeitraum für die Verzögerung beim Entsperren auf 15 Tage fest.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Entsperren Sie eine Aufbewahrungsregel für den Papierkorb, damit sie aktualisiert oder gelöscht werden kann

Sie können eine gesperrte Aufbewahrungsregel nicht löschen oder ändern. Wenn Sie eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie sie zunächst entsperren. Nachdem Sie die Aufbewahrungsregel entsperrt haben, müssen Sie warten, bis die Frist zum Entsperren abgelaufen ist, bevor Sie sie ändern oder löschen können. Sie können eine Aufbewahrungsregel während des Zeitraums der Entsperrverzögerung nicht ändern oder löschen.

Eine entsperrte Aufbewahrungsregel kann jederzeit von einem Benutzer geändert und gelöscht werden, der über die erforderlichen IAM-Berechtigungen verfügt. Wenn Sie Ihre Aufbewahrungsregeln nicht sperren, können sie versehentlich oder böswillig geändert oder gelöscht werden.

Überlegungen

- Sie können eine Aufbewahrungsregel während der Dauer der Entsperrverzögerung erneut sperren.
- Sie können eine Aufbewahrungsregel erneut sperren, nachdem die Frist für die Entsperrung abgelaufen ist.
- Sie können die Entsperrverzögerung nicht umgehen.
- Sie können die Zeitdauer der Entsperrung nach der ersten Sperre nicht mehr ändern.

Wir empfehlen, dass Sie die EventBridge Amazon-Regeln verwenden, um Sie über Änderungen des Sperrstatus der Aufbewahrungsregeln zu informieren. Weitere Informationen finden Sie unter Überwachen Sie den Papierkorb mithilfe von Amazon EventBridge.

Sie können eine gesperrte Region-level Aufbewahrungsregel mit einer der folgenden Methoden entsperren.

Recycle Bin console

So entsperren Sie eine Aufbewahrungsregel

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Aufbewahrungsregeln aus.
3. Wählen Sie im Raster die zu gesperrte Aufbewahrungsregel aus und wählen Sie dann zum entsperren Actions (Aktionen), Edit retention rule (Aufbewahrungsregel bearbeiten).
4. Wählen Sie im Bildschirm „Sperrung der Aufbewahrungsregel bearbeiten“ die Option Unlock (Entsperren) und dann Save (Speichern).

AWS CLI

So entsperren Sie eine gesperrte Aufbewahrungsregel

Verwenden Sie den AWS CLI -Befehl unlock-rule. Geben Sie für `--identifier` die ID der zu entsperrenden Aufbewahrungsregel an.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Beispiel

Der folgende Beispielbefehl entsperrt die Aufbewahrungsregel `6lsJ2Fa9nh9`

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Kennzeichnen Sie eine Aufbewahrungsregel für den Papierkorb

Sie können Ihren Aufbewahrungsregeln benutzerdefinierte Tags zuweisen, um sie auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Auf diese Weise können Sie basierend auf den von Ihnen zugewiesenen benutzerdefinierten Tags effizient eine bestimmte Aufbewahrungsregel finden.

Gehen Sie wie folgt vor, um einer Aufbewahrungsregel ein Tag zuzuweisen.

Recycle Bin console

So weisen Sie einer Aufbewahrungsregel ein Tag zu:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, der Sie das Tag zuweisen möchten, und wählen Sie dann die Registerkarte Tags und dann Tags verwalten aus.
4. Wählen Sie Add tag. Geben Sie für Key (Schlüssel) den Tag-Schlüssel ein. Geben Sie für Value (Wert) den Tag-Wert ein.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So weisen Sie einer Aufbewahrungsregel ein Tag zu:

Verwenden Sie den Befehl tag-resource AWS CLI . Geben Sie für `--resource-arn` den Amazon-Ressourcennamen (ARN) der Aufbewahrungsregel an, die mit Tags versehen werden soll, und für `--tags` das Tag-Schlüssel/Wert-Paar.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Beispiel

Der folgende Beispielbefehl weist der Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` das Tag `purpose=production` zu.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tags key=purpose,value=production
```

Anzeigen von Tags für Aufbewahrungsregeln

Gehen Sie wie folgt vor, um die Tags anzuzeigen, die einer Aufbewahrungsregel zugewiesen sind.

Recycle Bin console

So zeigen Sie die Tags einer Aufbewahrungsregel an:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, für die Tags angezeigt werden sollen, und wählen Sie die Registerkarte Tags aus.

AWS CLI

So zeigen Sie die Tags an, die einer Aufbewahrungsregel zugewiesen sind:

Verwenden Sie den AWS CLI -Befehl list-tags-for-resource. Geben Sie für `--resource-arn` den ARN der Aufbewahrungsregel an.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Beispiel

Der folgende Beispielbefehl listet die Tags für die Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` auf.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

Entfernen von Tags von Aufbewahrungsregeln

Sie können Tags mithilfe einer der folgenden Methoden aus einer Aufbewahrungsregel entfernen.

Recycle Bin console

So entfernen Sie ein Tag aus einer Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, aus der das Tag entfernt werden soll, wählen Sie die Registerkarte Tags und dann Tags verwalten aus.

4. Wählen Sie neben dem zu entfernenden Tag Entfernen aus.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So entfernen Sie ein Tag aus einer Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl untag-resource. Geben Sie für `--resource-arn` den ARN der Aufbewahrungsregel an. Geben Sie für `--tagkeys` die Tag-Schlüssel der zu entfernenden Tags an.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Beispiel

Der folgende Beispielbefehl entfernt Tags mit dem Tag-Schlüssel `purpose` aus der Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Löschen Sie eine Aufbewahrungsregel für den Papierkorb, um zu verhindern, dass Ressourcen aufbewahrt werden

Sie können eine Aufbewahrungsregel jederzeit löschen. Wenn Sie eine Aufbewahrungsregel löschen, werden im Papierkorb keine neuen Ressourcen mehr aufbewahrt, nachdem sie gelöscht wurden. Ressourcen, die vor dem Löschen der Aufbewahrungsregel an den Papierkorb gesendet wurden, werden gemäß dem Aufbewahrungszeitraum, der in der Aufbewahrungsregel festgelegt ist, weiterhin im Papierkorb aufbewahrt. Wenn der Zeitraum abläuft, wird die Ressource dauerhaft aus dem Papierkorb gelöscht.

Sie können eine Aufbewahrungsregel mit einer der folgenden Methoden löschen.

Recycle Bin console

So löschen Sie eine Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie im Raster die zu löschende Aufbewahrungsregel aus und wählen Sie Actions (Aktionen), Delete retention rule (Aufbewahrungsregel löschen) aus.
4. Geben Sie die Bestätigungsnachricht ein, wenn Sie dazu aufgefordert werden, und wählen Sie Delete retention rule (Aufbewahrungsregel löschen).

AWS CLI

So löschen Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl delete-rule. Geben Sie für `--identifier` die ID der zu löschenden Aufbewahrungsregel an.

```
aws rbin delete-rule --identifier rule_ID
```

Beispiel

Der folgende Beispielbefehl löscht die Aufbewahrungsregel `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Stellen Sie gelöschte Schnappschüsse aus dem Papierkorb wieder her

In diesem Thema wird erklärt, wie Amazon EBS-Snapshots aus dem Papierkorb wiederhergestellt werden.

Themen

- Berechtigungen zum Arbeiten mit Snapshots im Papierkorb
- Anzeigen von Snapshots im Papierkorb
- Wiederherstellen von Snapshots aus dem Papierkorb

Berechtigungen zum Arbeiten mit Snapshots im Papierkorb

Standardmäßig verfügen Benutzer nicht über die Berechtigung zum Arbeiten mit Snapshots, die sich im Papierkorb befinden. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Um Snapshots im Papierkorb anzuzeigen und wiederherzustellen, müssen Benutzer über die folgenden Berechtigungen verfügen:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Zum Verwalten von Tags für Schnappschüsse im Papierkorb benötigen Benutzer die folgenden zusätzlichen Berechtigungen.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `ec2:DescribeTags`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie. Sie umfasst die `ec2:DescribeTags`-Berechtigung für Konsolenbenutzer und enthält die `ec2:CreateTags`- und `ec2:DeleteTags`-Berechtigungen zum Verwalten von Tags. Werden die Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zu den Berechtigungen, die zur Verwendung des Papierkorbs erforderlich sind, finden Sie unter Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln.

Anzeigen von Snapshots im Papierkorb

Während sich ein Snapshot im Papierkorb befindet, können Sie beschränkte Informationen darüber anzeigen. Hier einige Beispiele:

- Die ID des Snapshots.
- Die Beschreibung des Snapshots.
- Die ID des Volumes, aus dem der Snapshot erstellt wurde.
- Das Datum und die Uhrzeit, zu der der Snapshot gelöscht und in den Papierkorb verschoben wurde.
- Das Datum und die Uhrzeit, zu der der Aufbewahrungszeitraum abläuft. Der Snapshot wird nun dauerhaft aus dem Papierkorb entfernt.

Sie haben mehrere Möglichkeiten, um die Snapshots im Papierkorb anzuzeigen.

Recycle Bin console

So zeigen Sie Snapshots im Papierkorb mit der Konsole an:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Snapshots aufgelistet, die sich derzeit im Papierkorb befinden. Um die Details für einen bestimmten Snapshot anzuzeigen, wählen Sie ihn im Raster aus und wählen Sie Aktionen, Details anzeigen.

AWS CLI

Um Schnappschüsse im Papierkorb anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/list-snapshots-in-recycle-bin.html AWS CLI list-snapshots-in-recycle-bin. Schließen Sie die Option `--snapshot-id` ein, um einen bestimmten Snapshot anzuzeigen. Oder lassen Sie die `--snapshot-id`-Option weg, um alle Snapshots im Papierkorb anzuzeigen.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Der folgende Befehl bietet beispielsweise Informationen zum Snapshot `snap-01234567890abcdef` im Papierkorb.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Beispielausgabe:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Wiederherstellen von Snapshots aus dem Papierkorb

Solange sich ein Snapshot im Papierkorb befindet, können Sie ihn auf keine Weise verwenden. Um den Snapshot verwenden zu können, müssen Sie ihn zuerst wiederherstellen. Wenn Sie einen Snapshot aus dem Papierkorb wiederherstellen, kann er sofort verwendet werden und wird aus dem Papierkorb entfernt. Sie können einen wiederhergestellten Snapshot genauso verwenden wie jeden anderen Snapshot in Ihrem Konto.

Sie haben mehrere Möglichkeiten, um einen Snapshot aus dem Papierkorb wiederherzustellen.

Recycle Bin console

So stellen Sie einen Snapshot mit der Konsole aus dem Papierkorb wieder her:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Snapshots aufgelistet, die sich derzeit im Papierkorb befinden. Wählen Sie den wiederherzustellenden Snapshot aus und wählen Sie Wiederherstellen.
4. Wählen Sie Wiederherstellen, wenn Sie dazu aufgefordert werden.

AWS CLI

Um einen gelöschten Snapshot aus dem Papierkorb wiederherzustellen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-from-recycle-bin.html AWS CLI restore-snapshot-from-recycle-bin. Geben Sie für `--snapshot-id` die ID des wiederherzustellenden Snapshots an.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Mit dem folgenden Befehl wird beispielsweise der Snapshot `snap-01234567890abcdef` aus dem Papierkorb wiederhergestellt.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Beispielausgabe:

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Stellen Sie gelöschte Volumes aus dem Papierkorb wieder her

In diesem Thema wird erklärt, wie Amazon EBS-Volumes aus dem Papierkorb wiederhergestellt werden.

Themen

- Berechtigungen für die Arbeit mit Volumes im Papierkorb
- Volumes im Papierkorb anzeigen
- Stellen Sie Volumes aus dem Papierkorb wieder her

Berechtigungen für die Arbeit mit Volumes im Papierkorb

Standardmäßig sind Benutzer nicht berechtigt, mit Volumes zu arbeiten, die sich im Papierkorb befinden. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Zum Anzeigen und Wiederherstellen von Volumes, die sich im Papierkorb befinden, benötigen Benutzer die folgenden Berechtigungen:

- `ec2:ListVolumesInRecycleBin`
- `ec2:RestoreVolumeFromRecycleBin`

Um die Tags für Volumes im Papierkorb zu verwalten, benötigen Benutzer die folgenden zusätzlichen Berechtigungen.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `ec2:DescribeTags`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie. Sie umfasst die `ec2:DescribeTags`-Berechtigung für Konsolenbenutzer und enthält die `ec2:CreateTags`- und `ec2:DeleteTags`-Berechtigungen zum

Verwalten von Tags. Werden die Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRecycleBinVolumeOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:ListVolumesInRecycleBin",
        "ec2:RestoreVolumeFromRecycleBin"
      ],
      "Resource": "arn:aws:ec2:*:123456789012:volume/*"
    },
    {
      "Sid": "AllowVolumeTagOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags"
      ],
      "Resource": "arn:aws:ec2:*:123456789012:volume/*"
    }
  ]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.

- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zu den Berechtigungen, die zur Verwendung des Papierkorbs erforderlich sind, finden Sie unter Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln.

Volumes im Papierkorb anzeigen

Solange sich ein Volume im Papierkorb befindet, können Sie nur begrenzte Informationen dazu einsehen, darunter:

- Die ID des Volumes.
- Die Größe des Volumes.
- Der Volume-Typ.
- Datum und Uhrzeit, an dem das Volume gelöscht und in den Papierkorb verschoben wurde.
- Das Datum und die Uhrzeit, zu der der Aufbewahrungszeitraum abläuft. Das Volume wird zu diesem Zeitpunkt dauerhaft aus dem Papierkorb gelöscht.

Sie können die Volumes im Papierkorb mit einer der folgenden Methoden anzeigen.

Recycle Bin console

So zeigen Sie die Volumes im Papierkorb mithilfe der Konsole an

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Das Raster listet alle Volumes auf, die sich derzeit im Papierkorb befinden. Um die Details für ein bestimmtes Volume anzuzeigen, wählen Sie es im Raster aus und wählen Sie „Aktionen“, „Details anzeigen“.

AWS CLI

Um Bände im Papierkorb anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/list-volumes-in-recycle-bin.html AWS CLI list-volumes-in-recycle-bin. Fügen Sie die Option zum Anzeigen eines

bestimmten Volumes hinzu. `--volume-id` Oder lassen Sie die `--volume-id` Option aus, alle Volumes im Papierkorb anzuzeigen.

```
aws ec2 list-volumes-in-recycle-bin --volume-id volume_id
```

Der folgende Befehl liefert beispielsweise Informationen über das Volumen `vol-01234567890abcdef` im Papierkorb.

```
aws ec2 list-volumes-in-recycle-bin --volume-id vol-01234567890abcdef
```

Beispielausgabe:

```
{
    "VolumeRecycleBinInfo": [
        {
            "VolumeId": "vol-01234567890abcdef",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-08T13:00:00.000Z"
        }
    ]
}
```

Stellen Sie Volumes aus dem Papierkorb wieder her

Sie können ein Volume in keiner Weise verwenden, solange es sich im Papierkorb befindet. Um das Volume verwenden zu können, müssen Sie es zuerst wiederherstellen. Wenn Sie ein Volume aus dem Papierkorb wiederherstellen, ist das Volume sofort einsatzbereit und wird aus dem Papierkorb entfernt. Sie können ein wiederhergestelltes Volume auf die gleiche Weise verwenden wie jedes andere Volume in Ihrem Konto.

Sie können ein Volume mithilfe einer der folgenden Methoden aus dem Papierkorb wiederherstellen.

Recycle Bin console

So stellen Sie mithilfe der Konsole ein Volume aus dem Papierkorb wieder her

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.

3. Das Raster listet alle Volumes auf, die sich derzeit im Papierkorb befinden. Wählen Sie das wiederherzustellende Volume aus und klicken Sie auf Wiederherstellen.
4. Wählen Sie Wiederherstellen, wenn Sie dazu aufgefordert werden.

AWS CLI

Um ein gelöschtes Volume aus dem Papierkorb wiederherzustellen, verwenden Sie das AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-volume-from-recycle-bin.html AWS CLI restore-volume-from-recycle-bin. Geben Sie für die ID des wiederherzustellenden Volumes an`--volume-id`.

```
aws ec2 restore-volume-from-recycle-bin --volume-id volume_id
```

Der folgende Befehl stellt beispielsweise das Volumen `vol-01234567890abcdef` aus dem Papierkorb wieder her.

```
aws ec2 restore-volume-from-recycle-bin --volume-id vol-01234567890abcdef
```

Beispielausgabe:

```
{
    "VolumeId": "vol-01234567890abcdef",
    "State": "available",
    "Size": 100,
    "VolumeType": "gp3",
    "AvailabilityZone": "us-east-1a",
    "CreateTime": "2021-12-01T13:00:00.000000+00:00",
    "Encrypted": false
}
```

Stellen Sie gelöschte AMIs aus dem Papierkorb wieder her

In diesem Thema wird erklärt, wie EBS-backed Amazon-AMIs aus dem Papierkorb wiederhergestellt werden.

Themen

- Berechtigungen zum Arbeiten mit AMIs im Papierkorb

- Anzeigen von AMIs im Papierkorb
- Wiederherstellen von AMIs aus dem Papierkorb

Berechtigungen zum Arbeiten mit AMIs im Papierkorb

Standardmäßig verfügen Benutzer nicht über die Berechtigung zum Arbeiten mit AMIs, die sich im Papierkorb befinden. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Um AMIs, die sich im Papierkorb befinden, anzeigen und wiederherstellen zu können, müssen Benutzer über die folgenden Berechtigungen verfügen:

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Zur Verwaltung von Tags für AMIs im Papierkorb, müssen Benutzer über die folgenden zusätzlichen Berechtigungen verfügen.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `ec2:DescribeTags`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie. Sie umfasst die `ec2:DescribeTags`-Berechtigung für Konsolenbenutzer und enthält die `ec2:CreateTags`- und `ec2:DeleteTags`-Berechtigungen zum Verwalten von Tags. Werden die Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zu den Berechtigungen, die zur Verwendung des Papierkorbs erforderlich sind, finden Sie unter Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln.

Anzeigen von AMIs im Papierkorb

Wenn sich ein AMI im Papierkorb befindet, können Sie eingeschränkte Informationen dazu anzeigen, unter anderem:

- Name, Beschreibung und eindeutige ID des AMI
- Datum und Uhrzeit, zu der das AMI gelöscht und in den Papierkorb verschoben wurde
- Das Datum und die Uhrzeit, zu der der Aufbewahrungszeitraum abläuft. Das AMI wird zu diesem Zeitpunkt dauerhaft gelöscht.

Sie haben mehrere Möglichkeiten, um die AMIs im Papierkorb anzuzeigen.

Recycle Bin console

Gelöschte AMIs im Papierkorb über die Konsole anzeigen

1. Öffnen Sie die Papierkorb-Konsole unter console.aws.amazon. com/rbin/home/.
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Ressourcen aufgelistet, die sich derzeit im Papierkorb befinden. Um Details zu einem bestimmten AMI anzuzeigen, wählen Sie es im Raster aus und wählen dann Actions (Aktionen), View details (Details anzeigen) aus.

AWS CLI

Um gelöschte AMIs im Papierkorb anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/list-images-in-recycle-bin.html AWS CLI list-images-in-recycle-bin. Um bestimmte AMIs anzuzeigen, schließen Sie die `--image-id`-Option ein und geben Sie die IDs der anzuzeigenden AMIs an. Sie können bis zu 20 IDs in einer einzigen Anforderung angeben.

Um alle AMIs im Papierkorb anzuzeigen, lassen Sie die `--image-id`-Option weg. Wenn Sie keinen Wert für `--max-items` angeben, gibt der Befehl standardmäßig 1 000 Elemente pro Seite zurück. Weitere Informationen finden Sie unter Paginierung in der Amazon-EC2-API-Referenz.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Der folgende Befehl bietet beispielsweise Informationen über das AMI `ami-01234567890abcdef` im Papierkorb.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Beispielausgabe:

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

> **Important**
>
> Wenn Sie die folgende Fehlermeldung erhalten, müssen Sie möglicherweise Ihre Version aktualisieren. AWS CLI Weitere Informationen finden Sie unter Befehl nicht gefunden-Fehlermeldungen.

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Wiederherstellen von AMIs aus dem Papierkorb

Solange sich ein AMI im Papierkorb befindet, können Sie es in keiner Weise verwenden. Um das AMI verwenden zu können, müssen Sie es zuerst wiederherstellen. Wenn Sie ein AMI aus dem Papierkorb wiederherstellen, kann es sofort verwendet werden und wird aus dem Papierkorb entfernt. Sie können ein wiederhergestelltes AMI genauso verwenden wie jedes andere AMI in Ihrem Konto.

Sie haben mehrere Möglichkeiten, ein AMI aus dem Papierkorb wiederherzustellen.

Recycle Bin console

AMI aus dem Papierkorb über die Konsole wiederherstellen

1. Öffnen Sie die Papierkorb-Konsole unter console.aws.amazon. com/rbin/home/.
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Ressourcen aufgelistet, die sich derzeit im Papierkorb befinden. Wählen Sie das wiederherzustellende AMI aus und wählen Sie dann Recover (Wiederherstellen).
4. Wählen Sie Wiederherstellen, wenn Sie dazu aufgefordert werden.

AWS CLI

Um ein gelöschtes AMI aus dem Papierkorb wiederherzustellen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-image-from-recycle-bin.html AWS CLI restore-image-from-recycle-bin. Geben Sie für `--image-id` die ID des wiederherzustellenden AMI an.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Mit dem folgenden Befehl wird beispielsweise das AMI `ami-01234567890abcdef` aus dem Papierkorb wiederhergestellt.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

Wenn der Befehl erfolgreich ausgeführt wird, wird keine Ausgabe zurückgegeben.

> **Important**
>
> Wenn Sie die folgende Fehlermeldung erhalten, müssen Sie möglicherweise Ihre Version aktualisieren. AWS CLI Weitere Informationen finden Sie unter Befehl nicht gefunden-Fehlermeldungen.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Überwachen Sie den Papierkorb mithilfe von Amazon EventBridge

Der Papierkorb sendet Ereignisse an Amazon EventBridge für Aktionen, die im Rahmen der Aufbewahrungsregeln ausgeführt werden. Mit können Sie Regeln einrichten EventBridge, die als Reaktion auf diese Ereignisse programmatische Aktionen einleiten. Sie können beispielsweise eine EventBridge Regel erstellen, die eine Benachrichtigung an Ihre E-Mail sendet, wenn eine Aufbewahrungsregel entsperrt wird und der Zeitraum für die Entsperrung eintritt. Weitere Informationen finden Sie unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren.

Ereignisse in EventBridge werden als JSON-Objekte dargestellt. Die Felder, die für das Ereignis einzigartig sind, sind im Abschnitt `detail` des JSON-Objekt enthalten. Im Feld `event` ist der Name des Ereignisses enthalten. Das Feld `result` enthält den vollständigen Status der Aktion, die zur Auslösung des Ereignisses führte. Weitere Informationen finden Sie unter EventBridge Amazon-Ereignismuster im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen zu Amazon EventBridge finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch.

Ereignisse

- RuleLocked
- RuleChangeAttempted
- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb generiert, wenn eine Aufbewahrungsregel erfolgreich gesperrt wurde. Dieses Ereignis kann durch CreateRule und durch LockRule Anfragen generiert werden. Die API, die das Ereignis generiert hat, ist im `api-name`-Feld vermerkt.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Locked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "CreateRule"
 }
 }
```

RuleChangeAttempted

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb für erfolglose Versuche, eine gesperrte Regel zu ändern oder zu löschen, generiert. Dieses Ereignis kann durch DeleteRule und durch UpdateRule Anfragen generiert werden. Die API, die das Ereignis generiert hat, ist im `api-name`-Feld vermerkt.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Change Attempted",
 "source": "aws.rbin",
 "account": "123456789012",
```

```
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "DeleteRule"
 }
 }
```

RuleUnlockScheduled

Im Folgenden sehen Sie ein Beispiel für ein Ereignis, das der Papierkorb erzeugt, wenn eine Aufbewahrungsregel entsperrt wird und die Verzögerungszeit für die Entsperrung beginnt.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlock Scheduled",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z",
 }
 }
```

RuleUnlockingNotice

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb täglich generiert, während sich eine Aufbewahrungsregel in ihrer Entsperrungsverzögerung befindet, bis zum Tag vor dem Ablauf der Entsperrungsverzögerung.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocking Notice",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z"
 }
 }
```

RuleUnlocked

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb generiert, wenn die Frist für die Entsperrung einer Aufbewahrungsregel abläuft und die Aufbewahrungsregel geändert oder gelöscht werden kann.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
```

```
"region": "us-west-2",
"resources": [
"arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail":
{
"detail-version": " 1.0.0",
"rule-id": "a12345abcde",
"rule-description": "locked account level rule",
"unlock-delay-period": "30 days",
"scheduled-unlock-time": "2022-09-10T16:37:50Z"
}
}
```

Überwachen Sie den Papierkorb mit AWS CloudTrail

Der Papierkorb-Service ist integriert in. AWS CloudTrail CloudTrail ist ein Dienst, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe, die im Papierkorb ausgeführt werden, als Ereignisse. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Verwaltungsereignisse trotzdem in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der gesammelten Informationen können Sie ermitteln, welche Anfrage CloudTrail an den Papierkorb gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Details.

Weitere Informationen dazu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum Papierkorb finden Sie unter CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine unterstützte Ereignisaktivität im Papierkorb stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Eventverlauf als Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Eventverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für den Papierkorb, erstellen Sie einen Pfad. Ein Trail ermöglicht die Bereitstellung CloudTrail von

Protokolldateien an einen S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter Übersicht zum Erstellen eines Trails im AWS CloudTrail -Benutzerhandbuch.

Unterstützte API-Aktionen

Für den Papierkorb können Sie CloudTrail die folgenden API-Aktionen als Verwaltungsereignisse protokollieren.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Weitere Informationen zur Protokollierung von Verwaltungsereignissen finden Sie unter Protokollieren von Verwaltungsereignissen für Pfade im CloudTrail Benutzerhandbuch.

Informationen zur Identität

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- 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.

Weitere Informationen erhalten Sie beim CloudTrail Benutzer IdentityElement.

Auswerten der Papierkorb-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen 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 Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie in keiner bestimmten Reihenfolge.

Im Folgenden finden CloudTrail Sie Beispiele für Protokolleinträge.

CreateRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:45:22Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "CreateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
```

```
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"description": "Match all snapshots",
"resourceType": "EBS_SNAPSHOT"
},
"responseElements": {
"identifier": "jkrnexample"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


GetRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
```

```
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:45:33Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "GetRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

ListRules

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
```

```
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:44:37Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "ListRules",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"resourceTags": [
  {
    "resourceTagKey": "test",
    "resourceTagValue": "test"
  }
]
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
```

```
 }
```

UpdateRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:03Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "UpdateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample",
 "retentionPeriod": {
   "retentionPeriodValue": 365,
   "retentionPeriodUnit": "DAYS"
 },
 "description": "Match all snapshots",
 "resourceType": "EBS_SNAPSHOT"
 },
```

```
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

DeleteRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:25Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "DeleteRule",
```

```
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample"
 },
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

TagResource

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
```

```
    "creationDate": "2021-10-22T21:38:34Z"
  }
 }
 },
 "eventTime": "2021-10-22T21:43:15Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "TagResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
 "tags": [
  {
    "key": "purpose",
    "value": "production"
  }
 ]
 },
 "responseElements": null,
 "requestID": "examplee-7962-49ec-8633-795efexample",
 "eventID": "example4-6826-4c0a-bdec-0bab1example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```


UntagResource


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
```

```
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-10-22T21:38:34Z"
  }
}
},
"eventTime": "2021-10-22T21:44:16Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UntagResource",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
"requestParameters": {
"resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
"tagKeys": [
  "purpose"
]
},
"responseElements": null,
"requestID": "example7-6c1e-4f09-9e46-bb957example",
"eventID": "example6-75ff-4c94-a1cd-4d5f5example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
```

```
 }
```

ListTagsForResource

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-10-22T21:38:34Z"
   }
 }
 },
 "eventTime": "2021-10-22T21:42:31Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "ListTagsForResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
 },
 "responseElements": null,
 "requestID": "example8-10c7-43d4-b147-3d9d9example",
 "eventID": "example2-24fc-4da7-a479-c9748example",
 "readOnly": true,
 "eventType": "AwsApiCall",
 "managementEvent": true,
```

```
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

LockRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "creationDate": "2022-10-25T00:45:11Z",
     "mfaAuthenticated": "false"
   }
 }
 },
 "eventTime": "2022-10-25T00:45:19Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "LockRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "python-requests/2.25.1",
 "requestParameters": {
 "identifier": "jkrnexample",
 "lockConfiguration": {
```

```
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
 }
 },
 "responseElements": {
 "identifier": "jkrnexample",
 "description": "",
 "resourceType": "EBS_SNAPSHOT",
 "retentionPeriod": {
   "retentionPeriodValue": 7,
   "retentionPeriodUnit": "DAYS"
 },
 "resourceTags": [],
 "status": "available",
 "lockConfiguration": {
   "unlockDelay": {
     "unlockDelayValue": 7,
     "unlockDelayUnit": "DAYS"
   }
 },
 "lockState": "locked"
 },
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "recipientAccountId": "123456789012",
 "eventCategory": "Management",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

UnlockRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
```

```
"type": "AssumedRole",
"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2022-10-25T00:45:11Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2022-10-25T00:46:17Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UnlockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": {
"identifier": "jkrnexample",
"description": "",
"resourceType": "EC2_IMAGE",
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
```

```
},
"lockState": "pending_unlock",
"lockEndTime": "Nov 1, 2022, 12:46:17 AM"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


Dienstendpunkte für den Papierkorb

Ein Endpunkt ist eine URL, die als Einstiegspunkt für einen AWS Webdienst dient. Der Papierkorb unterstützt die folgenden Endpunkttypen:

- IPv4-Endpunkte
- Dual-stack Endpunkte, die sowohl IPv4 als auch IPv6 unterstützen
- FIPS-Endpunkte

Wenn Sie eine Anfrage stellen, können Sie den Endpunkt und die Region angeben, die verwendet werden sollen. Wenn Sie keinen Endpunkt festlegen, wird standardmäßig der IPv4-Endpunkt verwendet. Um einen anderen Endpunkttyp zu verwenden, müssen Sie ihn in Ihrer Anforderung angeben. Beispiele für diese Vorgehensweise finden Sie unter Angeben von Endpunkten.

Informationen zum Papierkorb finden Sie unter Papierkorb-Endpunkte im. Allgemeine Amazon Web Services-Referenz

Themen

- IPv4-Endpunkte
- Dual-stack (IPv4 und IPv6) Endpunkte

- FIPS-Endpunkte
- Angeben von Endpunkten

IPv4-Endpunkte

IPv4 Endpunkte unterstützen nur IPv4-Datenverkehr. IPv4-Endpunkte sind für alle Regionen verfügbar.

Sie müssen die Region als Teil des Endpunktnamens angeben. Die Endpunktnamen verwenden die folgende Namenskonvention:

- Robin. *region*.amazonaws.com

Der IPv4-Endpunkt für die Region USA Ost (Nord-Virginia) lautet beispielsweise. `rbin.us-east-1.amazonaws.com`

Dual-stack (IPv4 und IPv6) Endpunkte

Dual-stack Endpunkte unterstützen sowohl IPv4- als auch IPv6-Verkehr. Dual-stack Endpunkte sind für alle Regionen verfügbar.

Um IPv6 verwenden zu können, müssen Sie einen Dual-Stack-Endpunkt verwenden. Wenn Sie eine Anfrage an einen Dual-Stack-Endpunkt stellen, löst die Endpunkt-URL eine IPv6- oder eine IPv4-Adresse auf, je nachdem, welches Protokoll Ihr Netzwerk und Ihr Client verwendet.

Sie müssen die Region als Teil des Endpunktnamens angeben. Dual-stack Bei Endpunktnamen wird die folgende Namenskonvention verwendet:

- `rbin.`*region*`.api.aws`

Der Dual-Stack-Endpunkt für die Region USA Ost (Nord-Virginia) lautet `rbin.us-east-1.api.aws` beispielsweise.

FIPS-Endpunkte

Der Papierkorb bietet FIPS-validated IPv4- und Dual-Stack-Endpunkte (IPv4 und IPv6) für die folgenden Regionen:

- `us-east-1` – USA Ost (Nord-Virginia)
- `us-east-2` – USA Ost (Ohio)
- `us-west-1` – USA West (Nordkalifornien)
- `us-west-2` – USA West (Oregon)
- `ca-central-1` – Kanada (Zentral)
- `ca-west-1`— Kanada West (Calgary)
- `us-gov-east-1` — AWS GovCloud (US-East)
- `us-gov-west-1` — AWS GovCloud (US-West)

FIPS-IPv4-Endpunkte verwenden die folgende Namenskonvention: `rbin-fips.`*`region`*`.amazonaws.com`. Der FIPS-IPv4-Endpunkt für die Region USA Ost (Nord-Virginia) lautet beispielsweise. `rbin-fips.us-east-1.amazonaws.com`

FIPS-Dual-Stack-Endpunkte verwenden die folgende Namenskonvention: `rbin-fips.`*`region`*`.api.aws`. Der FIPS-Dual-Stack-Endpunkt für die Region USA Ost (Nord-Virginia) lautet beispielsweise. `rbin-fips.us-east-1.api.aws`

Angeben von Endpunkten

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS CLI einen Endpunkt für die `us-east-2`-Region angeben.

- Dual-stack

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.us-east-2.api.aws
```

- IPv4

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.us-east-2.amazonaws.com
```

Erstellen Sie eine private Verbindung zwischen einer VPC und dem Papierkorb

Sie können eine private Verbindung zwischen Ihrer VPC und dem Papierkorb herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen, unterstützt von. AWS PrivateLink Sie können auf den Papierkorb zugreifen, als ob er sich in Ihrer VPC befinde, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung zu verwenden. Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit dem Papierkorb zu kommunizieren.

Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren.

Weitere Informationen finden Sie im Handbuch unter Greifen Sie über AWS PrivateLink auf AWS Dienste zu. AWS PrivateLink

Erstellen Sie einen Schnittstellen-VPC-Endpunkt für den Papierkorb

Sie können einen VPC-Endpunkt für den Papierkorb erstellen, indem Sie entweder die Amazon VPC-Konsole oder die verwenden. AWS CLI Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen VPC-Endpunkt für den Papierkorb mit dem folgenden Servicenamen: `com.amazonaws.region.rbin`

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an den Papierkorb richten, indem Sie beispielsweise den Standard-DNS-Namen für die Region verwenden. `rbin.us-east-1.amazonaws.com`

Erstellen Sie eine VPC-Endpunktrichtlinie für den Papierkorb

Standardmäßig ist der vollständige Zugriff auf den Papierkorb über den Endpunkt zulässig. Sie können den Zugriff auf den Schnittstellenendpunkt mithilfe von VPC-Endpunktrichtlinien steuern. Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf den Papierkorb steuert. Die Richtlinie gibt die folgenden Informationen an:

- Der Prinzipal, der Aktionen ausführen kann.
- Die Aktionen, die ausgeführt werden können.
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

```
{
    "Statement": [
    {
        "Effect": "Allow",
        "Action": "rbin:*",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Effect": "Deny",
        "Action": "rbin:DeleteRule",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "StringEquals" : {
                "rbin:Attribute/ResourceType": "EBS_SNAPSHOT"
            }
        }
    }]
}
```

Sicherheit in Amazon EBS

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen 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. Third-party Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Elastic Block Store gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon EBS anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon EBS konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Amazon EBS-Ressourcen zu überwachen und zu sichern.

Topics

- Datenschutz in Amazon EBS
- Identitäts- und Zugriffsmanagement für Amazon EBS
- Konformitätsüberprüfung für Amazon EBS
- Datenstabilität in Amazon EBS

Datenschutz in Amazon EBS

Das Modell der AWS geteilten Verantwortung (Modell der gilt für den Datenschutz im Amazon Elastic Block Store. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen

Infrastruktur verantwortlich, auf der alle ausgeführt AWS Cloud werden. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz in der Region . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, AWS-Konto Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten findest du unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon EBS oder anderen AWS-Services über die Konsole, die API oder die SDKs arbeiten. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen

- Datensicherheit bei Amazon EBS
- Verschlüsselung bei Speicherung und Übertragung
- KMS-Schlüsselverwaltung

Datensicherheit bei Amazon EBS

Amazon-EBS-Volumes werden Ihnen als unformatierte Blockgeräte präsentiert. Bei diesen Geräten handelt es sich um logische Geräte, die auf der EBS-Infrastruktur erstellt wurden. Der Amazon EBS-Dienst stellt sicher, dass die Geräte logisch leer sind (das heißt, die Rohblöcke sind auf Null gesetzt oder enthalten kryptografisch pseudozufällige Daten), bevor der Kunde sie verwendet oder wiederverwendet.

Wenn Ihre Verfahren das Löschen aller Daten mit einer bestimmten Methode erfordern, wie sie beispielsweise in DoD 5220.22-M (National Industrial Security Program Operating Manual) oder NIST 800-88 (Guidelines for Media Sanitization) beschrieben sind, können Sie dies auf Amazon EBS tun. Je nach den Anforderungen des Verfahrens können Sie die Daten vor oder nach der Verwendung oder beides löschen. Diese Aktivität auf Blockebene wird auf die zugrunde liegenden Speichermedien im Amazon EBS-Service übertragen.

Verschlüsselung bei Speicherung und Übertragung

Die Amazon EBS-Verschlüsselung ist eine Verschlüsselungslösung, mit der Sie Ihre Amazon EBS-Volumes und Amazon EBS-Snapshots mithilfe kryptografischer Schlüssel verschlüsseln können. AWS Key Management Service EBS-Verschlüsselungsvorgänge finden auf den Servern statt, die Amazon EC2-Instances hosten. Dadurch wird die Sicherheit sowohl der Daten im Ruhezustand als auch der Daten während der Übertragung zwischen einer Instance und dem zugehörigen Volume sowie allen nachfolgenden Snapshots gewährleistet. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung.

KMS-Schlüsselverwaltung

Wenn Sie ein verschlüsseltes Amazon EBS-Volume oder einen verschlüsselten Snapshot erstellen, geben Sie einen AWS Key Management Service Schlüssel an. Standardmäßig verwendet Amazon EBS den AWS verwalteten KMS-Schlüssel für Amazon EBS in Ihrem Konto und Ihrer Region (). `aws/ebs` Sie können jedoch einen vom Kunden verwalteten KMS-Schlüssel angeben, den Sie erstellen und verwalten. Die Verwendung eines vom Kunden verwalteten KMS-Schlüssels bietet Ihnen mehr Flexibilität, einschließlich der Möglichkeit, KMS-Schlüssel zu erstellen, zu rotieren und zu deaktivieren.

Um einen vom Kunden verwalteten KMS-Schlüssel verwenden zu können, müssen Sie Benutzern die Erlaubnis geben, den KMS-Schlüssel zu verwenden. Weitere Informationen finden Sie unter Berechtigungen für --Benutzer.

> **Important**
>
> Amazon EBS unterstützt nur symmetrische KMS-Schlüssel. Sie können keine asymmetrischen KMS-Schlüssel verwenden, um ein Amazon EBS-Volume und Snapshots zu verschlüsseln. Hilfe bei der Bestimmung, ob ein KMS-Schlüssel symmetrisch oder asymmetrisch ist, finden Sie unter Identifizieren asymmetrischer KMS-Schlüssel. https://docs.aws.amazon.com/kms/latest/developerguide/identify-key-types.html#identify-asymm-keys

Für jedes Volume fordert Amazon EBS auf, einen eindeutigen Datenschlüssel AWS KMS zu generieren, der unter dem von Ihnen angegebenen KMS-Schlüssel verschlüsselt ist. Amazon EBS speichert den verschlüsselten Datenschlüssel mit dem Volume. Wenn Sie das Volume dann an eine Amazon EC2-Instance anhängen, ruft Amazon EBS auf, AWS KMS um den Datenschlüssel zu entschlüsseln. Amazon EBS verwendet den Klartext-Datenschlüssel im Hypervisor-Speicher, um alles auf dem Volume zu verschlüsseln. I/O Weitere Informationen finden Sie unter So funktioniert die Amazon EBS-Verschlüsselung.

Identitäts- und Zugriffsmanagement für Amazon EBS

AWS Identity and Access Management (IAM) ist ein Programm AWS-Service , das einem Administrator hilft, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon EBS-Ressourcen zu nutzen. IAM ist ein Dienst AWS-Service , den Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie Amazon EBS mit IAM funktioniert
- Beispiel für IAM-Richtlinien für Amazon EBS

- Beheben Sie Probleme mit der Amazon EBS-Autorisierung

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Beheben Sie Probleme mit der Amazon EBS-Autorisierung).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie Amazon EBS mit IAM funktioniert).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiel für IAM-Richtlinien für Amazon EBS).

Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich AWS mit Ihren Identitätsdaten an. Sie müssen als IAM-Benutzer oder als IAM-Benutzer authentifiziert sein, indem Sie eine IAM-Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich mit Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen als Verbundidentität anmelden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Stellt für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen bereit. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, menschliche Benutzer dazu zu verpflichten, einen Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen darauf zuzugreifen.

Bei einer Verbundidentität handelt es sich um einen Benutzer aus Ihrem Unternehmensverzeichnis, einem Web-Identitätsanbieter oder Directory Service einem Benutzer, der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer einen Verbund mit einem Identitätsanbieter verwenden, um AWS mithilfe temporärer Anmeldeinformationen auf den Zugriff zuzugreifen.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder eine AWS API-Operation aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie einer Identität oder Ressource zugeordnet sind. AWS wertet diese Richtlinien aus, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können integrierte Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximale Anzahl von Berechtigungen festgelegt werden kann, die von gängigeren Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen komplizierter zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Logik zur Richtlinienauswertung.

Wie Amazon EBS mit IAM funktioniert

Bevor Sie IAM verwenden, um den Zugriff auf Amazon EBS zu verwalten, erfahren Sie, welche IAM-Funktionen für Amazon EBS verfügbar sind.

IAM-Funktionen, die Sie mit Amazon Elastic Block Store verwenden können

IAM-Feature	Amazon EBS-Unterstützung
Identity-based Richtlinien	Ja

IAM-Feature	Amazon EBS-Unterstützung
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-linked Rollen	Nein

Einen allgemeinen Überblick darüber, wie Amazon EBS und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren.

Identity-based Richtlinien für Amazon EBS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie

in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Identity-based Beispiele für Richtlinien für Amazon EBS

Beispiele für identitätsbasierte Amazon EBS-Richtlinien finden Sie unter. Beispiel für IAM-Richtlinien für Amazon EBS

Resource-based Richtlinien innerhalb von Amazon EBS

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Principals können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Amazon EBS

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu gewähren.

Eine Liste der Amazon EBS-Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 und Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EBS in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen in Amazon EBS wird entweder das Präfix `ec2` oder das `ebs` Präfix vor der Aktion verwendet.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
  "ec2:action1",
  "ec2:action2"
]
```

Beispiele für identitätsbasierte Amazon EBS-Richtlinien finden Sie unter. Beispiel für IAM-Richtlinien für Amazon EBS

Richtlinienressourcen für Amazon EBS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Einige Amazon EBS-API-Aktionen unterstützen mehrere Ressourcen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander. `DescribeVolumes`Greift beispielsweise auf vol-01234567890abcdef und vol-09876543210fedcba zu, sodass ein Principal über Berechtigungen für den Zugriff auf beide Ressourcen verfügen muss.

```
"Resource": [
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"
]
```

Richtlinien-Bedingungsschlüssel für Amazon EBS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Alle AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Die folgende Bedingung ermöglicht es dem Principal beispielsweise, eine Aktion auf einem Volume nur auszuführen, wenn der Datenträgertyp lautet`gp2`.

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

Eine Liste der Amazon EBS-Bedingungsschlüssel finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel in der Serviceautorisierungsreferenz.

ACLs in Amazon EBS

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Amazon EBS

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Principals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Amazon EBS

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen den kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für Amazon EBS

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon EBS

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Amazon EBS-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon EBS dazu eine Anleitung gibt.

Service-linked Rollen für Amazon EBS

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstgebundene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie einen Dienst in der Tabelle, die eine Yes in der Service-linked Rollenspalte enthält. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiel für IAM-Richtlinien für Amazon EBS

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon EBS-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS-Managementkonsole, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien
- Erlauben Sie Benutzern, die Amazon EBS-Konsole zu verwenden
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

- Erlauben Sie Benutzern, mit Volumes zu arbeiten
- Erlauben Sie Benutzern, mit Snapshots zu arbeiten

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Amazon EBS-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, folgen Sie diesen Richtlinien und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese im Rahmen einer bestimmten Aktion verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON)

und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Mehrstufige Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, in dem IAM-Benutzer oder ein Root-Benutzer in Ihrem System erforderlich sind AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Erlauben Sie Benutzern, die Amazon EBS-Konsole zu verwenden

Für den Zugriff auf die Amazon Elastic Block Store-Konsole benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon EBS-Ressourcen in Ihrem AWS-Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon EBS-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die Amazon EBS-Richtlinie `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlauben Sie Benutzern, mit Volumes zu arbeiten

Beispiele

- Beispiel: Anhängen und Trennen von Volumes
- Beispiel: Erstellen eines Volumes
- Beispiel: Erstellen eines Volumes mit Tags (Markierungen)
- Beispiel: Arbeiten Sie mit Volumes mithilfe der Amazon EC2-Konsole

Beispiel: Anhängen und Trennen von Volumes

Wenn ein Aufrufer mehrere Ressourcen für eine API-Aktion angeben muss, erstellen Sie eine Richtlinienanweisung, die den Benutzern den Zugriff auf alle erforderlichen Ressourcen ermöglicht. Falls ein `Condition`-Element mit einem oder mehreren dieser Ressourcen erforderlich ist, müssen Sie mehrere Anweisungen erstellen, wie in diesem Beispiel gezeigt.

Die folgende Richtlinie erlaubt Benutzern das Anfügen von Volumes mit dem Tag (Markierungen) `volume_user`=IAM-Benutzername an Instances mit dem Tag (Markierungen) `department=dev` und das Trennen dieser Volumes von diesen Instances. Wenn Sie einer IAM-Gruppe diese Richtlinie anfügen, erteilt die `aws:username`-Richtlinienvariable jedem IAM-Benutzer in der Gruppe die Berechtigung zum Anfügen bzw. Trennen von Volumes von Instances, die ein Tag mit dem Namen `volume_user` haben, das den entsprechenden IAM-Benutzernamen als Wert aufweist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceTag/volume_user": "${aws:username}"
                }
            }
        }
    ]
}
```

Beispiel: Erstellen eines Volumes

Die folgende Richtlinie ermöglicht Benutzern die Verwendung der CreateVolume API-Aktion. Die Benutzer dürfen nur ein Volume erstellen, wenn das Volume verschlüsselt und nicht größer als 20 GiB ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVolume"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:VolumeSize": "20"
                },
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        }
    ]
}
```

Beispiel: Erstellen eines Volumes mit Tags (Markierungen)

Die folgende Richtlinie umfasst den `aws:RequestTag`-Bedingungsschlüssel. Die Benutzer müssen daher alle Volumes, die sie erstellen, mit den Tags `costcenter=115` und `stack=prod`

versehen. Werden nicht genau diese Tags (Markierungen) übergeben oder überhaupt keine Tags (Markierungen) angegeben, schlägt die Anforderung fehl.

Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen die Benutzer zudem über Berechtigungen für die Aktion `CreateTags` verfügen. Die zweite Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Benutzer Tags nur im Kontext von `CreateVolume` erstellen können. Die Benutzer können keine vorhandenen Volumes oder andere Ressourcen markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedVolumes",
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/costcenter": "115",
                    "aws:RequestTag/stack": "prod"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVolume"
                }
            }
        }
    ]
}
```

Die folgende Richtline erlaubt den Benutzern die Erstellung eines Volumes, ohne Tags (Markierungen) angeben zu müssen. Die `CreateTags`-Aktion wird nur ausgewertet, wenn Tags in der `CreateVolume`-Anforderung festgelegt werden. Wenn Benutzer Tags (Markierungen) hinzufügen, muss das Tag (Markierungen) `purpose=test` sein. Andere Tags (Markierungen) sind in der Anforderung nicht zulässig.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "test",
                    "ec2:CreateAction": "CreateVolume"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "purpose"
                }
            }
        }
    ]
}
```

Beispiel: Arbeiten Sie mit Volumes mithilfe der Amazon EC2-Konsole

Die folgende Richtlinie gewährt Benutzern mithilfe der Amazon EC2-Konsole die Erlaubnis, Volumes anzusehen und zu erstellen sowie Volumes an bestimmte Instances anzuhängen und zu trennen.

Die Benutzer können Instances, die über den `purpose=test`-Tag (Markierung) verfügen, beliebige Volumes anfügen und außerdem Volumes von diesen Instances trennen. Zum Anfügen eines Volumes mithilfe der Amazon EC2-Konsole ist es praktisch, Benutzern die Berechtigung zum Verwenden der `ec2:DescribeInstances`-Aktion zu gewähren, damit sie eine Instance aus einer vorausgefüllten Liste im Dialogfeld Attach Volume auswählen können. Allerdings dürfen die Benutzer dadurch außerdem alle Instances auf der Seite Instances in der Konsole ansehen. Sie können diese Aktion daher auch auslassen.

In der ersten Anweisung ist die `ec2:DescribeAvailabilityZones` Aktion erforderlich, um sicherzustellen, dass ein Benutzer beim Erstellen eines Volumes eine Availability Zone auswählen kann.

Benutzer können die von ihnen erstellten Volumes nicht mit Tags (Markierungen) versehen (entweder während oder nach der Erstellung eines Volumes).

Erlauben Sie Benutzern, mit Snapshots zu arbeiten

Dieser Abschnitt enthält Beispielrichtlinien für `CreateSnapshot` (zeitpunktbezogener Snapshot eines EBS-Volumes) und `CreateSnapshots` (Multi-Volume-Snapshots).

Beispiele

- Beispiel: Erstellen eines Snapshots
- Beispiel: Erstellen von Snapshots
- Beispiel: Erstellen eines Snapshots mit Tags (Markierungen)
- Beispiel: Erstellen von Multi-Volume-Snapshots mit Tags
- Beispiel: Snapshots kopieren
- Beispiel: Ändern der Berechtigungseinstellungen für Snapshots

Beispiel: Erstellen eines Snapshots

Die folgende Richtlinie ermöglicht es Kunden, die CreateSnapshot API-Aktion zu verwenden. Die Kunden können nur dann Snapshots erstellen, wenn das Volume verschlüsselt und nicht größer als 20 GiB ist.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:VolumeSize": "20"
                },
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        }
    ]
}
```

Beispiel: Erstellen von Snapshots

Die folgende Richtlinie ermöglicht es Kunden, die CreateSnapshots API-Aktion zu verwenden. Die Kunden können nur Snapshots erstellen, wenn alle Volumes in der Instance den Typ GP2 aufweisen.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
```

```
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
             }
     }

      }
   ]
}
```

Beispiel: Erstellen eines Snapshots mit Tags (Markierungen)

Die folgende Richtlinie umfasst den `aws:RequestTag`-Bedingungsschlüssel. Er fordert, dass die Kunden die Tags `costcenter=115` und `stack=prod` auf jeden neuen Snapshot anwenden. Werden nicht genau diese Tags (Markierungen) übergeben oder überhaupt keine Tags (Markierungen) angegeben, schlägt die Anforderung fehl.

Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen die Kunden zudem über die Berechtigungen für die `CreateTags`-Aktion verfügen. Die dritte Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Kunden Tags nur im Kontext von `CreateSnapshot` erstellen können. Kunden können keine vorhandenen Volumes oder andere Ressourcen markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*"
        },
        {
            "Sid": "AllowCreateTaggedSnapshots",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
```

```
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/costcenter": "115",
                    "aws:RequestTag/stack": "prod"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        }
    ]
}
```

Beispiel: Erstellen von Multi-Volume-Snapshots mit Tags

Die folgende Richtlinie enthält den Bedingungsschlüssel `aws:RequestTag`, der verlangt, dass der Kunde die Tags `costcenter=115` und `stack=prod` anwendet, wenn er ein Multi-Volume-Snapshot-Satz erstellt. Werden nicht genau diese Tags (Markierungen) übergeben oder überhaupt keine Tags (Markierungen) angegeben, schlägt die Anforderung fehl.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"
```

```
   ]
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erlaubt den Kunden die Erstellung eines Snapshots, ohne Tags (Markierungen) angeben zu müssen. Die `CreateTags`-Aktion wird nur ausgewertet, wenn Tags in der `CreateSnapshot`- oder `CreateSnapshots`-Anforderung angegeben werden. In der Anforderung können Tags weggelassen werden. Wenn ein Tags (Markierungen) angegeben ist, muss das Tag (Markierungen) `purpose=test` sein. Andere Tags (Markierungen) sind in der Anforderung nicht zulässig.

JSON

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

```
            "Action":"ec2:CreateSnapshot",
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":"ec2:CreateTags",
            "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
            "Condition":{
                "StringEquals":{
                    "aws:RequestTag/purpose":"test",
                    "ec2:CreateAction":"CreateSnapshot"
                },
                "ForAllValues:StringEquals":{
                    "aws:TagKeys":"purpose"
                }
            }
        }
    ]
}
```

Die folgende Richtlinie ermöglicht es Kunden, Multi-Volume-Snapshot-Sätze zu erstellen, ohne Tags angeben zu müssen. Die `CreateTags`-Aktion wird nur ausgewertet, wenn Tags in der `CreateSnapshot`- oder `CreateSnapshots`-Anforderung angegeben werden. In der Anforderung können Tags weggelassen werden. Wenn ein Tags (Markierungen) angegeben ist, muss das Tag (Markierungen) `purpose=test` sein. Andere Tags (Markierungen) sind in der Anforderung nicht zulässig.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Action":"ec2:CreateSnapshots",
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":"ec2:CreateTags",
            "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
```

```
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erlaubt nur dann, einen Snapshot zu erstellen, wenn das Quell-Volume das Tag (Markierungen) `User:`*`username`* für den Kunden hat, und wenn der eigentliche Snapshot mit den Tags (Markierungen) `Environment:Dev` und `User:`*`username`* gekennzeichnet ist. Der Kunde kann dem Snapshot weitere Tags (Markierungen) hinzufügen.

Die folgende Richtlinie für `CreateSnapshots` erlaubt nur dann, Snapshots zu erstellen, wenn das Quell-Volume mit `User:`*`username`* für den Kunden markiert ist und der eigentliche Snapshot mit `Environment:Dev` und `User:`*`username`* markiert ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1:*:instance/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/User": "${aws:username}"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Environment": "Dev",
                    "aws:RequestTag/User": "${aws:username}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
        }
    ]
}
```

Die folgende Richtlinie erlaubt nur dann, einen Snapshot zu löschen, wenn der Snapshot mit User:Benutzername für den Kunden markiert ist.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erlaubt einem Kunden, einen Snapshot zu erstellen, weist die Aktion jedoch ab, wenn der zu erstellende Snapshot den Tag (Markierung)-Schlüssel `value=stack` hat.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erlaubt einem Kunden, Snapshots zu erstellen, weist die Aktion jedoch ab, wenn die zu erstellenden Snapshots den Tag (Markierung)-Schlüssel `value=stack` haben.

JSON

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

```
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erlaubt es Ihnen, mehrere Aktionen in einer Richtlinie zu kombinieren. Sie können nur einen Snapshot erstellen (im Kontext von`CreateSnapshots`), wenn der Snapshot in der Region `us-east-1` erstellt wird. Sie können nur Snapshots erstellen (im Kontext von `CreateSnapshots`) wenn die Snapshots in der Region `us-east-1` erstellt werden und der Instance-Typ `t2*` lautet.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
```

```
         "Condition":{
            "StringEqualsIgnoreCase": {
              "ec2:Region": "us-east-1"
            },
            "StringLikeIfExists": {
              "ec2:InstanceType": ["t2.*"]
            }
         }
      }
   ]
}
```

Beispiel: Snapshots kopieren

Resource-level Die für die CopySnapshot Aktion angegebenen Berechtigungen gelten sowohl für den neuen Snapshot als auch für den Quell-Snapshot.

Die folgende Beispielrichtlinie ermöglicht es Prinzipalen, Snapshots nur zu kopieren, wenn der neue Snapshot mit dem Tag (Markierung)-Schlüssel von `purpose` und einem Tag (Markierung)-Wert von `production` (`purpose=production`) erstellt wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:111122223333:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

Die folgende Beispielrichtlinie ermöglicht es Principals, Snapshots nur zu kopieren, wenn der Quell-Snapshot einem AWS Konto gehört. `123456789012`

Die folgende Beispielrichtlinie ermöglicht es Principals, Snapshots nur zu kopieren, wenn der Quell-Snapshot mit dem Tag-Schlüssel von erstellt wurde. `CSISnapshotName`

```
{
    "Effect": "Allow",
    "Action": "ec2:CopySnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/${*}",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/CSISnapshotName": "*"
         }
     }
},

{
    "Effect": "Allow",
    "Action": "ec2:CopySnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/snap-*"
}
```

Beispiel: Ändern der Berechtigungseinstellungen für Snapshots

Die folgende Richtlinie erlaubt das Ändern eines Snapshots nur, wenn der Snapshot mit `User:`*`username`* dem Tag „Wo *`username`* ist der AWS Kontonutzername des Kunden“ gekennzeichnet ist. Die Anforderung schlägt fehl, wenn diese Bedingungen nicht erfüllt ist.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
```

```
            }
        }
    ]
}
```

Beheben Sie Probleme mit der Amazon EBS-Autorisierung

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon EBS und IAM auftreten können.

Problembereiche

- Ich bin nicht berechtigt, eine Aktion in Amazon EBS auszuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Amazon EBS-Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Amazon EBS auszuführen

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie Ihren Administrator um Unterstützung bitten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu einem Volume anzuzeigen, aber nicht über die `ec2:DescribeVolumes` erforderlichen Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeVolumes on resource: volume-id
```

In diesem Fall bittet Mateo seinen AWS Administrator, ihm die Beschreibung des Volumes zu gestatten.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon EBS übergeben können.

In einigen AWS-Services Fällen können Sie eine vorhandene Rolle an diesen Service übergeben, anstatt eine neue Servicerolle oder eine serviceverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon EBS auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Amazon EBS-Ressourcen zuzugreifen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon EBS diese Funktionen unterstützt, finden Sie unterWie Amazon EBS mit IAM funktioniert.
- Weitere Informationen zum Bereitstellen des Zugriffs auf Ihre Ressourcen in Ihrem eigenen AWS-Konten Bereich finden Sie im IAM-Benutzerhandbuch unter Bereitstellen des Zugriffs für einen IAM-Benutzer in einem anderen Benutzer AWS-Konto , dessen Eigentümer Sie sind.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf Ressourcen, die Dritten AWS-Konten gehören.

- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsüberprüfung für Amazon EBS

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen für AWS Ihre Umgebung anmelden oder diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme, .

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen im Abschnitt Berichte AWS Artifact .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Datenstabilität in Amazon EBS

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen 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. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Amazon EBS mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

- Automatisierung von EBS-Snapshots mit Amazon Data Lifecycle Manager
- Kopieren von EBS-Snapshots über Regionen hinweg

Überwachungstools für Amazon EBS

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Elastic Block Store und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Amazon EBS zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Die APIs zur Verwaltung Ihrer EBS-Volumes und -Snapshots sind Teil der Amazon EC2 EC2-API. Weitere Informationen CloudTrail zur Amazon EC2 EC2-API finden Sie unter Protokollieren von Amazon EC2 EC2-API-Aufrufen AWS CloudTrail im Amazon EC2 EC2-Benutzerhandbuch.
- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie unter the section called “Amazon CloudWatch”.
- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie unter the section called “Amazon EventBridge”.
- Detaillierte Leistungsstatistiken von Amazon EBS bieten Leistungsstatistiken in Echtzeit I/O für Amazon EBS-Volumes, die an Amazon EC2 EC2-Instances Nitro-based angehängt sind. Weitere Informationen finden Sie unter Detaillierte Leistungsstatistiken von Amazon EBS.
- Amazon GuardDuty hilft bei der Erkennung potenziell bösartiger Aktivitäten in Ihren EC2-Instances. GuardDuty Malware Protection for EC2 scannt die EBS-Volumes, die an Ihre EC2-Instances angehängt sind. Weitere Informationen finden Sie unter the section called “Amazon GuardDuty”.

CloudWatch Amazon-Metriken für Amazon EBS

CloudWatch Amazon-Metriken sind statistische Daten, die Sie verwenden können, um das Betriebsverhalten Ihrer Volumes einzusehen, zu analysieren und Alarme dafür einzustellen.

Die Daten werden automatisch in 1-Minuten-Intervallen kostenlos zur Verfügung gestellt.

Wenn Sie Daten von abrufen CloudWatch, können Sie einen `Period` Anforderungsparameter angeben, um die Granularität der zurückgegebenen Daten anzugeben. Dies unterscheidet sich von dem Zeitraum, den EBS zur Erfassung der Daten verwendet (Zeiträume von 1 Minute). Wir empfehlen Ihnen, in Ihrer Anfrage einen Zeitraum anzugeben, der dem Erfassungszeitraum entspricht oder diesen überschreitet, um sicherzustellen, dass die zurückgegebenen Daten gültig sind.

Sie können die Daten entweder über die CloudWatch API oder die Amazon EC2-Konsole abrufen. Die Konsole nimmt die Rohdaten aus der CloudWatch API und zeigt eine Reihe von Diagrammen an, die auf den Daten basieren. Je nach Anforderungen können Sie entweder die Daten aus der API oder die Diagramme in der Konsole verwenden.

Themen

- Metriken für Amazon-EBS-Volumes
- Metriken für Amazon EBS-Snapshots
- Metriken für Nitro-Instances
- Metriken für die schnelle Snapshot-Wiederherstellung
- Diagramme der Amazon-EC2-Konsole

Metriken für Amazon-EBS-Volumes

Der `AWS/EBS`-Namespace enthält die folgenden Metriken für EBS-Volumes, die allen Instance-Typen angefügt sind. Alle Amazon EBS-Volume-Typen senden automatisch 1-Minuten-Metriken an CloudWatch, aber nur, wenn das Volume an eine Instance angehängt ist.

Informationen zum verfügbaren Festplattenspeicher aus dem Betriebssystem auf einer Instance finden Sie unter Anzeigen von freiem Festplattenspeicher.

> **Note**
>
> Einige Metriken weisen Unterschiede bei Instances auf, die auf dem Nitro-System basieren. Eine Liste dieser Instance-Typen finden Sie unter Instances, die auf dem Nitro-System erstellt wurden.

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeAvgIOPS *`	**Note** Wird für alle EBS-Volume-Typen unterstützt, die an Nitro-Instances angehängt sind. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Die durchschnittlichen IOPS beim Lesen und Schreiben, die dem Volume in einer Minute zugewiesen wurden. Wurden innerhalb der letzten Minute keine Operationen auf das Volume ausgeführt, ist der Wert für die Metrik	Ops/s	`VolumeId` | `InstanceId`	• `Sum` • `Average` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	Null (0). Weitere Informationen finden Sie unter Überwachen Sie die Eigenschaften I/O mit CloudWatch. Verwenden Sie für Multi-Attach aktivierte Volumes die `InstanceId` Dimension, um die durchschnittlichen IOPS für ein bestimmtes Volume-Instance-Attachement anzuzeigen.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeAvgThroughput *`	**Note** Wird für alle EBS-Volume-Typen unterstützt, die an Nitro-Instances angehängt sind. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Der durchschnittliche Lese- und Schreibdurchsatz, der in einer Minute auf das Volume übertragen wird. Wenn innerhalb der letzten Minute keine Operationen auf das Volume ausgeführt wurden, ist der Wert für die Metrik Null (`0`). Weitere Informationen finden Sie unter Überwachen Sie die Eigenschaften I/O mit CloudWatch.	KiB/s	`VolumeId` | `InstanceId`	• `Sum` • `Average` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	Verwenden Sie für Multi-Attach aktivierte Volumes die `InstanceId` Dimension, um den durchschnittlichen Durchsatz für ein bestimmtes Volume-Instance-Attachement anzuzeigen.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeAvgReadLatency *`	**Note** Wird für alle Volume-Typen unterstützt, die an Nitro-Instances angehängt sind. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Die durchschnittliche Zeit, die benötigt wird, um Lesevorgänge in einer Minute abzuschließen. Verwenden Sie diese Metrik, um die durchschnittliche I/O Latenz der EBS-Volumes zu überwachen, die an Ihre Amazon EC2-Instances angeschlossen sind. Der Durchschnitt wird auf der Grundlage von I/O Vorgängen berechnet, die in der letzten Minute abgeschlossen wurden. Wenn innerhalb der	Millisekunden	`VolumeId` | `InstanceId`	`Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	letzten Minute keine Operationen abgeschlossen wurden, ist der Wert für die Metrik Null. Verwenden Sie für Multi-Attach aktivierte Volumes die `InstanceId` Dimension, um die durchschnittliche Latenz für ein bestimmtes Volume-Instance-Attachement anzuzeigen.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeAvgWriteLatency *`	**Note** Wird für alle Volume-Typen unterstützt, die an Nitro-Instances angehängt sind. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Die durchschnittliche Zeit, die benötigt wird, um Schreibvorgänge in einer Minute abzuschließen. Verwenden Sie diese Metrik, um die durchschnittliche I/O Latenz der EBS-Volumes zu überwachen, die an Ihre Amazon EC2-Instances angeschlossen sind. Der Durchschnitt wird auf der Grundlage von I/O Vorgängen berechnet, die in der letzten Minute abgeschlossen wurden. Wenn innerhalb der	Millisekunden	`VolumeId` | `InstanceId`	`Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	letzten Minute keine Operationen abgeschlossen wurden, ist der Wert für die Metrik Null. Verwenden Sie für Multi-Attach aktivierte Volumes die `InstanceId` Dimension, um die durchschnittliche Latenz für ein bestimmtes Volume-Instance-Attachement anzuzeigen.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeIOPSExceededCheck *`	**Note** Wird für alle Volume-Typen unterstützt, mit Ausnahme von magnetic (`standard`), die an Nitro-Instances angehängt sind. Wird bei Multi-Attach aktivierten Volumes nicht unterstützt. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Meldet, ob eine Anwendung innerhalb der letzten Minute wiederholt versucht hat, IOPS zu erreichen, die die für das Volume bereitgestellte IOPS-Leistung übersteigen. Diese Metrik kann entweder	Keine	`VolumeId` | `InstanceId`	• `Sum` • `Average` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	`0` (bereitgestellte IOPS nicht überschritten) oder 1 (bereitgestellte IOPS überschritten) sein. Weitere Informationen finden Sie unter Überwachen Sie die Eigenschaften I/O mit CloudWatch.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeThroughputExceededCheck *`	**Note** Wird für alle Volume-Typen unterstützt, mit Ausnahme von magnetic (`standard`), die an Nitro-Instances angeschlossen sind. Wird bei Multi-Attach aktivierten Volumes nicht unterstützt. Nicht veröffentlicht für Volumes, die an Amazon ECS und AWS Fargate Aufgaben angehängt sind. Meldet, ob eine Anwendung innerhalb der letzten Minute wiederholt versucht hat, einen Durchsatz zu erzielen, der die für das Volume bereitgestellte Durchsatzleistung übersteigt. Diese Metrik kann	Keine	`VolumeId` | `InstanceId`	• `Sum` • `Average` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	entweder 0 (bereitgestellter Durchsatz wurde nicht überschritten) oder 1 (bereitgestellter Durchsatz wurde überschritten) lauten. Weitere Informationen finden Sie unter. Überwachen Sie die Eigenschaften I/O mit CloudWatch			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeReadBytes`	Stellt Informationen über Leseoperationen in einem bestimmten Zeitraum zur Verfügung. • Die `Sum`-Statistik enthält die Gesamtbytezahl, die während des Zeitraums übertragen wurde. • Die `Average` Statistik gibt die durchschnittliche Anzahl der im angegebenen Zeitraum gelesenen Byte an. • Die `SampleCount` Statistik stellt die Anzahl der Datenpunkte dar, die bei der statistischen Berechnung verwendet wurden. **Note** Für Xen-Instances werden Daten nur dann gemeldet, wenn eine Lesetätigkeit	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum`|`Maximum` — nur für Volumes, die an Instanzen Nitro-based angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	auf dem Volume stattfindet.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeWriteBytes`	Stellt Informationen über Schreibvorgänge in einem bestimmten Zeitraum zur Verfügung • Die `Sum`-Statistik enthält die Gesamtbytezahl, die während des Zeitraums übertragen wurde. • Die `Average` Statistik gibt die durchschnittliche Anzahl der im angegebenen Zeitraum geschriebenen Byte an. • Die `SampleCount` Statistik stellt die Anzahl der Datenpunkte dar, die bei der statistischen Berechnung verwendet wurden. **Note** Für Xen-Instances werden Daten nur dann gemeldet, wenn eine Schreibtätigkeit auf dem	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum`|`Maximum` — nur für Volumes, die an Instanzen Nitro-based angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	Volume stattfindet.			
`VolumeReadOps`	Die Gesamtzahl der Leseoperationen in einem bestimmten Zeitraum. Lesevorgänge werden nach Abschluss gezählt. Zum Berechnen der durchschnittlichen Leseoperationen pro Sekunde (Lese-IOPS, Ein- und Ausgabe-Befehle pro Sekunde) für einen Zeitraum dividieren Sie die Gesamt-Lesevorgänge im Zeitraum durch die Anzahl der Sekunden im Zeitraum.	Anzahl	`VolumeId`	• `Average` • `Sum` • `Minimum`|`Maximum` — nur für Volumes, die an Nitro-based Instanzen angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeWriteOps`	Die Gesamtzahl der Schreiboperationen in einem bestimmten Zeitraum. Schreibvorgänge werden nach Abschluss gezählt. Zum Berechnen der durchschnittlichen Schreiboperationen pro Sekunde (Schreib-IOPS, Ein- und Ausgabe-Befehle pro Sekunde) für einen Zeitraum dividieren Sie die Gesamt-Schreibvorgänge im Zeitraum durch die Anzahl der Sekunden im Zeitraum.	Anzahl	`VolumeId`	• `Average` • `Sum` • `Minimum`|`Maximum` — nur für Volumes, die an Nitro-based Instanzen angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeTotalReadTime`	**Note** Wird bei Multi-Attach aktivierten Volumes nicht unterstützt. Für Xen-Instances werden Daten nur dann gemeldet, wenn eine Lesetätigkeit auf dem Volume stattfindet. Die Gesamtzahl von Sekunden, die von allen innerhalb eines bestimmten Zeitraums abgeschlossenen Leseoperationen aufgewendet wurden. Wenn mehrere Anfragen gleichzeitig übertragen werden, kann diese Gesamtzahl größer sein als die Länge des Zeitraums. Beispiel für einen Zeitraum von 1 Minute (60 Sekunden): Wenn 150 Operationen während dieses	Sekunden	`VolumeId`	• `Average` — nicht relevant für Volumes, die an Nitro-based Instances angehängt sind • `Sum` • `Minimum`|`Maximum` — nur für Volumes, die an Nitro-based Instanzen angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	Zeitraums abgeschlossen wurden und jede Operation 1 Sekunde dauerte, ergibt sich ein Wert von 150 Sekunden.			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeTotalWriteTime`	**Note** Wird bei Multi-Attach aktivierten Volumes nicht unterstützt. Für Xen-Instances werden Daten nur dann gemeldet, wenn eine Schreibtätigkeit auf dem Volume stattfindet. Die Gesamtzahl von Sekunden, die von allen innerhalb eines bestimmten Zeitraums abgeschlossenen Schreiboperationen aufgewendet wurden. Wenn mehrere Anfragen gleichzeitig übertragen werden, kann diese Gesamtzahl größer sein als die Länge des Zeitraums. Beispiel für einen Zeitraum von 1 Minute (60 Sekunden): Wenn 150 Operation	Sekunden	`VolumeId`	• `Average` — nicht relevant für Volumes, die an Nitro-based Instances angehängt sind • `Sum` • `Minimum` | `Maximum` — nur für Volumes, die an Nitro-based Instanzen angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	en während dieses Zeitraums abgeschlossen wurden und jede Operation 1 Sekunde dauerte, ergibt sich ein Wert von 150 Sekunden.			
`VolumeIdleTime`	**Note** Wird bei Multi-Attach aktivierten Volumes nicht unterstützt. Die Gesamtzahl von Sekunden in einem bestimmten Zeitraum, wenn keine Lese- oder Schreiboperationen übertragen wurden.	Sekunden	`VolumeId`	• `Average`— nicht relevant für Volumes, die an Nitro-based Instances angehängt sind • `Sum` • `Minimum`| `Maximum` — nur für Volumes, die an Nitro-based Instanzen angehängt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeQueueLength`	Die Anzahl von Lese- und Schreiboperationsanfragen, die innerhalb eines bestimmten Zeitraums auf Abschluss warten.	Anzahl	`VolumeId`	• `Average` • `Sum` – nicht relevant für Volumes, die an Nitro-Instances angefügt sind • `Minimum` | `Maximum` – nur für Volumes, die Nitro-Instances angefügt sind

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeStalledIOCheck *`	**Note** Nur für Nitro-Instanzen. Nicht veröffentlicht für Bände, die Amazon ECS und AWS Fargate -Aufgaben angehängt sind. Meldet, ob ein Volume in der letzten Minute eine ins Stocken geratene I/O-Prüfung bestanden hat oder nicht bestanden hat. Diese Metrik kann entweder `0` (bestanden) oder (nicht bestanden) lauten. 1 Weitere Informationen finden Sie unter Überwachen Sie die Eigenschaften I/O mit CloudWatch.	Keine	`VolumeId` | `InstanceId`	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeThroughputPercentage`	**Note** Nur bereitgestellte IOPS-SSD-Volumes. Wird bei aktivierten Volumes nicht unterstützt. Multi-Attach Der Prozentsatz der I/O ausgeführten Operationen pro Sekunde (IOPS) an den gesamten bereitgestellten IOPS für ein Amazon EBS-Volume. Bereitgestellte IOPS SSD-Volumes liefern in 99,9 % der Zeit über ein bestimmtes Jahr bis zu 99,9 % der bereitgestellten IOPS-Leistung. Wenn während eines Schreibvorgangs innerhalb einer Minute keine weiteren ausstehenden I/O Anfragen vorliegen, beträgt der Metrikwert 100 Prozent. Außerdem kann die I/O Leistung	Prozent	`VolumeId`	• `Average` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
	eines Volumes aufgrund einer von Ihnen ergriffen en Aktion vorübergehend beeinträchtigt werden (z. B. Erstellen eines Snapshots eines Volumes bei Spitzenauslastung, Ausführung des Volumes auf einer EBS-optim ized Nicht-Instance oder erstmaliger Zugriff auf Daten auf dem Volume).			

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`VolumeConsumedReadWriteOps`	**Note** Nur bereitgestellte IOPS-SSD-Volumes. Die Gesamtmenge der Lese- und Schreibvorgänge (normalisiert auf 256.000 Kapazitätseinheiten), die in einem bestimmten Zeitraum verbraucht wurden. I/O Operationen, die jeweils kleiner als 256 K sind, zählen als 1 verbrauchte IOPS. I/O Operationen, die größer als 256 K sind, werden in Einheiten mit 256 K Kapazität gezählt. Beispielsweise I/O würden 1024K als 4 verbrauchte IOPS gezählt.	Anzahl	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`BurstBalance`	**Note** gp2, und st1 nur Volumes. sc1 Stellt Informationen über den Prozentsatz der I/O Credits (fürgp2) oder Durchsatzgutschriften (für st1 undsc1) bereit, die im Burst-Bucket verbleiben. Daten werden CloudWatch nur gemeldet, wenn das Volume aktiv ist. Wenn das Volume nicht angefügt ist, werden keine Daten gemeldet. Wenn die Basisleistung des Volumes die maximale Burst-Leistung übersteigt, werden die Guthaben nie ausgegeben. Bei anderen Instances beträgt die gemeldete Burst-Balance 100%. Weitere Informationen finden Sie unter GP2-Volumen-Leistung .	Prozent	`VolumeId`	• `Average` • `Sum` – nicht relevant für Volumes, die an Nitro-Instances angefügt sind. • `Minimum` | `Maximum`

* Sie können diese Metriken nicht in Außenposten, lokalen Zonen oder Wellenlängenzonen verwenden.

Metriken für Amazon EBS-Snapshots

Der `AWS/EBS` Namespace enthält die folgenden Metriken für Amazon EBS-Snapshots.

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
`SnapshotCopyBytesTransferred`	Die Menge der Snapshot-Daten, die in eine AWS Region kopiert wurden.	Bytes	`sourceRegion`	`Sum`

Metriken für Nitro-Instances

Der `AWS/EC2` Namespace enthält zusätzliche Amazon EBS-Metriken für Volumes, die an Instances angehängt sind, bei denen es sich nicht um Nitro-based Bare-Metal-Instances handelt.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`InstanceEBSIOPSExceededCheck *`	Meldet, ob eine Anwendung innerhalb der letzten Minute versucht hat, IOPS zu treiben, die die maximalen EBS-IOPS-Limits für die Instance überschritten hat. Diese Metrik kann entweder `0` (IOPS nicht überschritten) oder 1 (IOPS überschritten) sein.	Keine	• Summe • Durchschnitt • Minimum • Maximum
`InstanceEBSThroughputExceededCheck *`	Meldet, ob eine Anwendung innerhalb der letzten Minute versucht hat, einen Durchsatz zu treiben, der die maximalen EBS-Durchsatzlimits für die Instance überschreitet. Diese Metrik	Keine	• Summe • Durchschnitt • Minimum

Metrik	Description	Einheit	Aussagekräftige Statistiken
	kann entweder `0` (Durchsatz nicht überschritten) oder 1 (Durchsatz überschritten) sein.		• Maximum
`EBSReadOps`	Abgeschlossene Lesevorgänge von allen an die Instance angefügten Amazon EBS-Volumes in einem angegebenen Zeitraum. Um die durchschnittlichen I/O Lesevorgänge pro Sekunde (Read IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Operationen in dem Zeitraum durch die Anzahl der Sekunden in diesem Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Lese-IOPS zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME` , um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSReadOps` haben`m1`, gibt die metrische mathematische Formel die Metrik in `m1/(DIFF_TIME(m1))` operations/second zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Verwenden der metrischen Mathematik.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSWriteOps`	Abgeschlossene Schreibvorgänge in alle an die Instance angehängten EBS-Volumes in einem angegebenen Zeitraum. Um die durchschnittlichen I/O Schreibvorgänge pro Sekunde (Write-IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Operationen in der Periode durch die Anzahl der Sekunden in diesem Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Schreib-IOPS zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME`, um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSWriteOps` haben`m1`, gibt die metrische mathematische Formel die Metrik in `m1/(DIFF_TIME(m1))` operations/second zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Verwenden der metrischen Mathematik.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSReadBytes`	Die aus allen an die Instance angefügten EBS-Volumes gelesenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums gelesenen Bytes. Wenn Sie eine einfache Überwachung (5 Minuten) verwenden, können Sie diese Zahl durch 300 teilen, um Read zu erhalten Bytes/second. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSReadBytes` haben`m1`, gibt die metrische mathematische Formel die Metrik in `m1/(DIFF_TIME(m1))` bytes/second zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Verwenden der metrischen Mathematik.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSWriteBytes`	Die in alle an die Instance angefügten EBS-Volumes geschriebenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums geschriebenen Bytes. Wenn Sie eine einfache Überwachung (5 Minuten) verwenden, können Sie diese Zahl durch 300 teilen, um Write zu finden Bytes/second. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME`, um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSWriteBytes` haben `m1`, gibt die metrische mathematische Formel die Metrik in `m1/(DIFF_TIME(m1))` bytes/second zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Verwenden der metrischen Mathematik.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
EBSIOBalance%	Stellt Informationen über den Prozentsatz der im Burst-Bucket verbleibenden I/O Credits bereit. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige *.4xlarge -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Weitere Informationen finden Sie unter Standardmäßig optimiertes EBS. Die Sum-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum
EBSByteBalance%	Bietet Informationen über den Prozentanteil der verbleibenden Durchsatz-Guthaben im Burst-Bucket. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige *.4xlarge -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Weitere Informationen finden Sie unter Standardmäßig für EBS optimiert. Die Sum-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum

* Sie können diese Metriken nicht in Outposts, Local Zones oder Wavelength Zones verwenden.

Metriken für die schnelle Snapshot-Wiederherstellung

Der AWS/EBS-Namespace enthält die folgenden Metriken für die schnelle Snapshot-Wiederherstellung.

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
FastSnapshotRestoreCreditsBucketSize	Die maximale Menge an Guthaben für die Volume-Erstellung, die angesammelt werden kann. Diese Metrik wird pro Snapshot pro Availability Zone gemeldet.	Keine	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** Die aussagekräftigste Statistik ist Average. Die Ergebnisse für die Statistiken Minimum und Maximum sind identisch mit denen für Average und können stattdessen verwendet werden.
FastSnapshotRestoreCreditsBalance	Die Menge an verfügbarem Guthaben für die Volume-Erstellung. Diese Metrik wird pro Snapshot pro Availability Zone gemeldet.	Keine	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** Die aussagekräftigste Statistik ist Average.

Metrik	Description	Einheiten	Dimensionen	Aussagekräftige Statistiken
				Die Ergebnisse für die Statistiken `Minimum` und `Maximum` sind identisch mit denen für `Average` und können stattdessen verwendet werden.

Diagramme der Amazon-EC2-Konsole

Wenn Sie ein Volume erstellt haben, können Sie die Überwachungsdiagramme des Volumes in der Amazon EC2-Konsole anzeigen. Wählen Sie ein Volume auf der Seite Volumes in der Konsole aus und klicken Sie auf Monitoring. In der folgenden Tabelle sind die Diagramme aufgelistet, die angezeigt werden. Die Spalte auf der rechten Seite beschreibt, wie die Rohdatenmetriken aus der CloudWatch API verwendet werden, um jedes Diagramm zu erstellen. Der Zeitraum für alle Diagramme beträgt 5 Minuten.

Diagramm	Beschreibung mithilfe von Rohmetriken
Durchsatz lesen (KiB/s)	`Sum(VolumeReadBytes) / Period / 1024`
Durchsatz schreiben (KiB/s)	`Sum(VolumeWriteBytes) / Period / 1024`
Operationen lesen (Ops/s)	`Sum(VolumeReadOps) / Period`
Operationen schreiben (Ops/s)	`Sum(VolumeWriteOps) / Period`
Durchschnittliche Warteschlangenlänge (Operationen)	`Avg(VolumeQueueLength)`
Zeit im Leerlauf (%)	`Sum(VolumeIdleTime) / Period × 100`

Diagramm	Beschreibung mithilfe von Rohmetriken

Durchschnittliche Lesegröße (KiB/op)	`Avg(VolumeReadBytes) / 1024`
	
	Zum Beispiel Nitro-based leitet die folgende Formel die durchschnittliche Lesegröße mithilfe von CloudWatch Metric Math ab:
	
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024`
	
	Die `VolumeReadOps` Metriken `VolumeReadBytes` und sind in der EBS-Konsole CloudWatch verfügbar.

Durchschnittliche Schreibgröße () KiB/op	`Avg(VolumeWriteBytes) / 1024`
	
	Zum Nitro-based Beispiel leitet die folgende Formel die durchschnittliche Schreibgröße mithilfe von CloudWatch Metric Math ab:
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`
	
	Die `VolumeWriteOps` Metriken `VolumeWriteBytes` und sind in der EBS-Konsole CloudWatch verfügbar.

Durchschnittliche Leselatenz () ms/op	`Avg(VolumeTotalReadTime) × 1000`
	
	Beispielsweise Nitro-based leitet die folgende Formel die durchschnittliche Leselatenz mithilfe von CloudWatch Metric Math ab:
	
	`(Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000`
	
	Die `VolumeReadOps` Metriken `VolumeTotalReadTime` und sind in der EBS-Konsole CloudWatch verfügbar.

Diagramm	Beschreibung mithilfe von Rohmetriken

Durchschnittliche Schreiblatenz () ms/op	`Avg(VolumeTotalWriteTime) × 1000`
	
	Beispielsweise Nitro-based leitet die folgende Formel die durchschnittliche Schreiblatenz mithilfe von CloudWatch Metric Math ab:
	
	`(Sum(VolumeTotalWriteTime) / Sum(Volum eWriteOps)) * 1000`
	
	Die `VolumeTotalWriteTime` und `VolumeWriteOps` - Metriken sind in der EBS-Konsole CloudWatch verfügbar.

Für die Diagramme der durchschnittlichen Latenz und der durchschnittlichen Größe wird der Durchschnitt über die Gesamtzahl der Operationen (Lese- oder Schreiboperationen, je nachdem, welcher Wert für das Diagramm gilt) berechnet, die während des Zeitraums abgeschlossen wurden.

EventBridge Amazon-Ereignisse für Amazon EBS

Amazon EBS sendet Ereignisse an Amazon EventBridge für Aktionen, die auf Volumes und Snapshots ausgeführt werden. Mit können Sie Regeln festlegen EventBridge, die als Reaktion auf diese Ereignisse programmatische Aktionen auslösen. Sie können beispielsweise eine Regel erstellen, die eine Benachrichtigung an Ihre E-Mailadresse sendet, wenn ein Snapshot für die schnelle Snapshot-Wiederherstellung aktiviert wurde.

Ereignisse in EventBridge werden als JSON-Objekte dargestellt. Die Felder, die für das Ereignis einzigartig sind, sind im Abschnitt "Detail" des JSON-Objekt enthalten. Im Feld "Ereignis" ist der Name des Ereignisses enthalten. Das Feld "Ergebnis" enthält den vollständigen Status der Aktion, die zur Auslösung des Ereignisses führte. Weitere Informationen finden Sie unter EventBridge Amazon-Ereignismuster im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch.

Ereignisse

- EBS-Volume-Ereignisse
- Ereignis zur Initialisierung des EBS-Volumes

- Ereignisse der EBS-Volume-Änderung
- EBS-Snapshot-Ereignisse
- Archivereignisse von EBS-Snapshots
- EBS – schnelle Snapshot-Wiederherstellungsereignisse
- Verwenden AWS Lambda um Ereignisse zu verarbeiten EventBridge

EBS-Volume-Ereignisse

Amazon EBS sendet Ereignisse an, EventBridge wenn die folgenden Volume-Ereignisse eintreten.

Ereignisse

- Volume erstellen (createVolume)
- Volume löschen (deleteVolume)
- Volume anhängen oder erneut anhängen (attachVolume, reattachVolume)
- Volume trennen (DetachVolume)

Volume erstellen (createVolume)

Das `createVolume` Ereignis wird an Ihr AWS Konto gesendet, wenn eine Aktion zum Erstellen eines Volumes abgeschlossen ist. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Für dieses Ereignis kann als Ergebnis entweder `available` oder `failed` eintreten. Die Erstellung schlägt fehl, wenn ein ungültiger Wert angegeben AWS KMS key wurde, wie in den folgenden Beispielen gezeigt.

Ereignisdaten

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS für ein erfolgreiches Ereignis `createVolume` ausgestellt wird.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
```

```
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "available",
      "cause": "",
      "event": "createVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS nach einem fehlgeschlagenen Ereignis `createVolume` ausgestellt wird. Die Ursache für den Fehler war ein deaktivierter Verschlüsselung.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Nachstehend finden Sie ein Beispiel eines JSON-Objekts, das von EBS nach einem fehlgeschlagenen Ereignis `createVolume` ausgestellt wird. Die Ursache für den Fehler war ein ausstehender Import des Verschlüsselung.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
```

```
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Volume löschen (deleteVolume)

Das `deleteVolume` Ereignis wird an Ihr AWS Konto gesendet, wenn eine Aktion zum Löschen eines Volumes abgeschlossen ist. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Dieses Ereignis hat das Ergebnis `deleted`. Wenn das Löschen nicht abgeschlossen wird, wird das Ereignis nie gesendet.

Ereignisdaten

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS für ein erfolgreiches Ereignis `deleteVolume` ausgestellt wird.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
```

```
      "event": "deleteVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Volume anhängen oder erneut anhängen (attachVolume, reattachVolume)

Das `reattachVolume` Ereignis `attachVolume` oder wird an Ihr AWS Konto gesendet, wenn ein Volume an eine Instance angehängt oder erneut angehängt wird. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Wenn Sie einen Verschlüsselung zur Verschlüsselung eines EBS-Volumes verwenden und der Verschlüsselung ungültig wird, löst EBS ein Ereignis aus, wenn dieser Verschlüsselung später zum Zuweisen oder erneuten Zuweisen an eine Instance verwendet wird, wie in den folgenden Beispielen gezeigt.

Ereignisdaten

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS nach einem fehlgeschlagenen Ereignis `attachVolume` ausgestellt wird. Die Ursache für den Fehler war eine ausstehende Löschung des Verschlüsselung.

> **Note**
>
> AWS versucht möglicherweise, nach einer routinemäßigen Serverwartung erneut eine Verbindung zu einem Volume herzustellen.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
```

```
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS nach einem fehlgeschlagenen Ereignis `reattachVolume` ausgestellt wird. Die Ursache für den Fehler war eine ausstehende Löschung des Verschlüsselung.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Volume trennen (DetachVolume)

Das `detachVolume` Ereignis wird an Ihr AWS Konto gesendet, wenn ein Volume von einer Amazon EC2-Instance getrennt wird.

Ereignisdaten

Das Folgende ist ein Beispiel für ein erfolgreiches `detachVolume` Ereignis.

```
{
  "version":"0",
  "id":"2ec37298-1234-e436-70fc-c96b1example",
```

```
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.ec2",
  "account":"123456789012",
  "time":"2024-03-18T16:35:52Z",
  "region":"us-east-1",
  "resources":[],
  "detail":
  {
    "eventVersion":"1.09",
    "userIdentity":
    {
      "type":"IAMUser",
      "principalId":"AIDAJT12345SQ2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/administrator",
      "accountId":"123456789012",
      "accessKeyId":"AKIAJ67890A6EXAMPLE",
      "userName":"administrator"
    },
    "eventTime":"2024-03-18T16:35:52Z",
    "eventSource":"ec2.amazonaws.com",
    "eventName":"DetachVolume",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"12.12.123.12",
    "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ec2.detach-volume",
    "requestParameters":
    {
      "volumeId":"vol-072577c46bexample",
      "force":false
    },
    "responseElements":
    {
      "requestId":"1234513a-6292-49ea-83f8-85e95example",
      "volumeId":"vol-072577c46bexample",
      "instanceId":"i-0217f7eb3dexample",
      "device":"/dev/sdb",
      "status":"detaching",
      "attachTime":1710776815000
    },
    "requestID":"1234513a-6292-49ea-83f8-85e95example",
    "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
```

```
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":
    {
      "tlsVersion":"TLSv1.3",
      "cipherSuite":"TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
    }
  }
}
```

Ereignis zur Initialisierung des EBS-Volumes

Wenn Sie ein Amazon EBS-Volume aus einem Snapshot erstellen und die Standard-Volume-Initialisierungsrate oder eine Amazon EBS-Provisioned Rate für die Volumeninitialisierung verwenden, wird das `initializeVolume` Ereignis innerhalb von fünf Minuten nach Abschluss der Volume-Initialisierung an Ihr AWS Konto gesendet. Weitere Informationen finden Sie unter Verwenden Sie eine von Amazon EBS bereitgestellte Rate für die Volumeninitialisierung.

Das Ereignis wird nicht für Volumes gesendet, die mit Fast Snapshot Restore erstellt wurden.

> **Important**
>
> `completionTime`gibt an, wann das Ereignis generiert wurde. Da das Ereignis innerhalb von 5 Minuten nach Abschluss der Initialisierung generiert wird, `completionTime` kann es bis zu fünf Minuten dauern, bis die Initialisierung abgeschlossen ist.

Es folgt ein Beispielereignis.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567890abcdef"
   ],
```

```
   "detail": {
      "event": " initializeVolume",
      "result": "succeeded",
      "completionTime": "yyyy-mm-ddThh:mm:ssZ",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Ereignisse der EBS-Volume-Änderung

Amazon EBS sendet `modifyVolume` Ereignisse, EventBridge wenn ein Volume geändert wird. Es wird jedoch nicht gespeichert, protokolliert oder archiviert.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

EBS-Snapshot-Ereignisse

Amazon EBS sendet Ereignisse an, EventBridge wenn die folgenden Volume-Ereignisse eintreten.

Ereignisse

- Snapshot erstellen (createSnapshot)
- Snapshots erstellen (createSnapshots)
- Snapshot kopieren (copySnapshot)
- Snapshot freigeben (shareSnapshot)

Snapshot erstellen (createSnapshot)

Das `createSnapshot` Ereignis wird an Ihr AWS Konto gesendet, wenn eine Aktion zum Erstellen eines Snapshots abgeschlossen ist. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Für dieses Ereignis kann als Ergebnis entweder `succeeded` oder `failed` eintreten.

Ereignisdaten

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS für ein erfolgreiches Ereignis `createSnapshot` ausgestellt wird. Im Abschnitt `detail` enthält das Feld `source` die ARN des Quellvolumes. Die Felder `startTime` und `endTime` zeigen an, wann die Erstellung des Snapshot begann und abgeschlossen war.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

Snapshots erstellen (createSnapshots)

Das `createSnapshots` Ereignis wird an Ihr AWS Konto gesendet, wenn eine Aktion zum Erstellen eines Snapshots mit mehreren Volumes abgeschlossen ist. Für dieses Ereignis kann als Ergebnis entweder `succeeded` oder `failed` eintreten.

Ereignisdaten

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS für ein erfolgreiches Ereignis `createSnapshots` ausgestellt wird. Im Abschnitt `detail` sind im Feld `source` die ARNs der Quellvolumes des festgelegten Multi-Volume-Snapshots angegeben. Die Felder `startTime` und `endTime` zeigen an, wann die Erstellung des Snapshot begann und abgeschlossen war.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

Die nachstehende Liste ist ein Beispiel eines JSON-Objekts, das von EBS nach einem fehlgeschlagenen Ereignis `createSnapshots` ausgestellt wird. Der Fehler wurde verursacht, da ein oder mehrere Snapshots für den Multi-Volume-Snapshot nicht abgeschlossen werden konnten.

Bei den Werten für `snapshot_id` handelt es sich um die ARNs der fehlgeschlagenen Snapshots. `startTime` und `endTime` geben den Zeitpunkt an, zu dem die Aktion zum Erstellen des Snapshots begonnen und beendet wurde.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

Snapshot kopieren (copySnapshot)

Das `copySnapshot` Ereignis wird an Ihr AWS Konto gesendet, wenn eine Aktion zum Kopieren eines Snapshots abgeschlossen ist. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Für dieses Ereignis kann als Ergebnis entweder `succeeded` oder `failed` eintreten.

In `detail` diesem Abschnitt `source` ist der ARN des Quell-Snapshots und `snapshot_id` der ARN der Snapshot-Kopie angegeben. `startTime`und `endTime` geben an, wann der Kopiervorgang gestartet und beendet wurde. `incremental`gibt an, ob es sich bei der Snapshot-Kopie um einen inkrementellen Snapshot (`true`) oder um einen vollständigen Snapshot (`false`) handelt. `transferType`gibt an, ob der Snapshot-Kopiervorgang ein Standardkopiervorgang oder ein zeitbasierter Kopiervorgang war. Weitere Informationen finden Sie unter Time-based Kopien für Amazon EBS-Snapshots und AMIs EBS-backed.

Wenn Sie den Snapshot regionsübergreifend kopieren, wird das Ereignis in der Zielregion ausgegeben.

Szenario 1: Der standardmäßige Snapshot-Kopiervorgang ist abgeschlossen

Das Folgende ist ein Beispiel für ein Ereignis, das an Ihr Konto gesendet wird, wenn ein Standard-Snapshot-Kopiervorgang erfolgreich abgeschlossen wurde. Beachten Sie, dass `transferType` gleich `standard` ist.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
```

```
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true",
    "transferType": "standard"
  }
}
```

Szenario 2: Der Time-based Snapshot-Kopiervorgang wird innerhalb der Abschlussdauer abgeschlossen

Das Folgende ist ein Beispiel für ein Ereignis, das an Ihr Konto gesendet wird, wenn ein zeitbasierter Snapshot-Kopiervorgang innerhalb seiner Abschlussdauer abgeschlossen wird. Beachten Sie, dass `transferType` dies `time-based` darauf hinweist, dass es sich um einen zeitbasierten Snapshot-Kopiervorgang handelte. `completionDurationStartTime`gibt an, wann die Abschlussdauer begonnen hat.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "transferType": "time-based"
  }
}
```

Szenario 3: Der Time-based Snapshot-Kopiervorgang wird abgeschlossen, die angeforderte Abschlussdauer wird jedoch nicht eingehalten

Wenn ein zeitbasierter Snapshot-Kopiervorgang abgeschlossen wird, die angeforderte Abschlussdauer jedoch nicht eingehalten wird, werden zwei Ereignisse an Ihr Konto CloudWatch gesendet. Im Folgenden finden Sie Beispiele für diese Ereignisse.

- Das erste Ereignis wird an Ihr Konto gesendet, sobald die Abschlussdauer nicht eingehalten wird, auch wenn der Kopiervorgang noch nicht abgeschlossen ist. Für dieses Ereignis `detail-type` ist `EBS Copy Snapshot Missed Completion Duration` und `missedCompletionDurationCause` gibt den Grund an.

```
{
 "version":"0",
 "id":"fd90eb95-0938-e02c-cf55-b81363b8ac12",
 "detail-type":"EBS Copy Snapshot Missed Completion Duration",
 "source":"aws.ec2",
 "account":"123456789012",
 "time":"2024-11-19T18:17:08Z",
 "region":"us-east-1",
 "resources": ["arn:aws:ec2:us-east-1:123456789012:snapshot/snap-01234567890abcedf"],
 "detail":{
   "event":"copySnapshot",
   "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
   "snapshot_id":"arn:aws:ec2:us-
east-1:123456789012:snapshot/snap-01234567890abcedf",
   "source":"arn:aws:ec2:us-east-1:123456789012:snapshot/snap-00987654321fedcba",
   "startTime": "Sun Nov 24 22:32:55 UTC 2024",
   "transferType": "time-based"
   }
}
```

- Das zweite Ereignis wird erst an Ihr Konto gesendet, wenn der Snapshot abgeschlossen ist. Das Ereignis beinhaltet`missedCompletionDurationCause`, was den Grund dafür liefert.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
```

```
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
    "transferType": "time-based"
  }
}
```

Szenario 4: Der Snapshot-Kopiervorgang schlägt fehl

Das Folgende ist ein Beispiel für ein Ereignis, das an Ihr Konto gesendet wird, wenn ein Snapshot-Kopiervorgang fehlschlägt. Beachten Sie, dass `result` dies `failed` darauf hinweist, dass der Vorgang fehlgeschlagen ist.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
```

```
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Snapshot freigeben (shareSnapshot)

Das `shareSnapshot` Ereignis wird an Ihr AWS Konto gesendet, wenn ein anderes Konto einen Snapshot mit ihm teilt. Es wird jedoch nicht gespeichert, protokolliert oder archiviert. Das Ergebnis ist immer `succeeded`.

Ereignisdaten

Es folgt ein Beispiel eines JSON-Objekts, das nach einem abgeschlossenen `shareSnapshot`-Ereignis von EBS ausgegeben wird. In `detail` diesem Abschnitt `source` ist der Wert von die AWS Kontonummer des Benutzers, der den Snapshot mit Ihnen geteilt hat. `startTime`und `endTime` stellen dar, wann die Aktion „Snapshot teilen“ gestartet und beendet wurde. Das Ereignis `shareSnapshot` wird nur dann gesendet, wenn ein privater Snapshot mit einem anderen Benutzer geteilt wird. Durch das Teilen eines öffentlichen Snapshot wird das Ereignis noch nicht ausgelöst.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
```

```
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Archivereignisse von EBS-Snapshots

Amazon EBS sendet Ereignisse im Zusammenhang mit Snapshot-Archivierungsaktionen aus. Weitere Informationen finden Sie unter Überwachen Sie die Amazon EBS-Snapshot-Archivierung mithilfe von Events CloudWatch.

EBS – schnelle Snapshot-Wiederherstellungsereignisse

Amazon EBS sendet Ereignisse, EventBridge wenn sich der Status der schnellen Snapshot-Wiederherstellung für einen Snapshot ändert. Ereignisse werden auf bestmögliche Weise ausgegeben.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

Die möglichen Werte für `state` sind `enabling`, `optimizing`, `enabled`, `disabling` und `disabled`.

Die möglichen Werte für `message` sind wie folgt:

`Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)`

Eine Anfrage zur Aktivierung der schnellen Snapshot-Wiederherstellung ist fehlgeschlagen und der Status hat zu `disabling` oder `disabled` gewechselt. Die schnelle Snapshot-Wiederherstellung kann für diesen Snapshot nicht aktiviert werden.

`Client.UserInitiated`

Der Status hat erfolgreich zu `enabling` oder `disabling` gewechselt.

`Client.UserInitiated - Lifecycle state transition`

Der Status hat erfolgreich zu `optimizing`, `enabled` oder `disabled` gewechselt.

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

Eine Anfrage zur Aktivierung der schnellen Snapshot-Wiederherstellung ist aufgrund von unzureichender Kapazität fehlgeschlagen und der Status hat zu `disabling` oder `disabled` gewechselt. Warten Sie und versuchen Sie es dann erneut.

`Server.InternalError - An internal error caused the operation to fail`

Eine Anfrage zur Aktivierung der schnellen Snapshot-Wiederherstellung ist aufgrund eines internen Fehlers fehlgeschlagen und der Status hat zu `disabling` oder `disabled` gewechselt. Warten Sie und versuchen Sie es dann erneut.

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

Der Status für die schnelle Snapshot-Wiederherstellung für den Snapshot hat zu `disabling` oder `disabled` gewechselt, weil der Snapshot vom Snapshot-Besitzer gelöscht oder die Freigabe aufgehoben wurde. Die schnelle Snapshot-Wiederherstellung kann nicht für einen Snapshot aktiviert werden, der gelöscht wurde oder nicht mehr für Sie freigegeben ist.

Verwenden AWS Lambda um Ereignisse zu verarbeiten EventBridge

Sie können Amazon EBS und Amazon verwenden, EventBridge um Ihren Datensicherungsworkflow zu automatisieren. Dazu müssen Sie eine IAM-Richtlinie, eine AWS Lambda Funktion zur

Behandlung des Ereignisses und eine EventBridge Regel erstellen, die eingehende Ereignisse abgleicht und sie an die Lambda-Funktion weiterleitet.

Für das folgende Verfahren wird das Ereignis `createSnapshot` verwendet, um einen abgeschlossenen Snapshot zur Notfallwiederherstellung automatisch in eine andere Region zu kopieren.

Kopieren eines abgeschlossenen Snapshots in eine andere Region

1. Erstellen Sie eine IAM-Richtlinie, wie sie im folgenden Beispiel gezeigt wird, um Berechtigungen zur Verwendung der `CopySnapshot` Aktion und zum Schreiben in das Protokoll bereitzustellen. EventBridge Weisen Sie die Richtlinie dem Benutzer zu, der das EventBridge Ereignis verarbeiten wird.

   JSON

   ```
   {
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": [
           "logs:CreateLogGroup",
           "logs:CreateLogStream",
           "logs:PutLogEvents"
         ],
         "Resource": "arn:aws:logs:*:*:*"
       },
       {
         "Effect": "Allow",
         "Action": [
           "ec2:CopySnapshot"
         ],
         "Resource": "*"
       }
     ]
   }
   ```

2. Definieren Sie eine Funktion in Lambda, die von der EventBridge Konsole aus verfügbar sein wird. Die unten angegebene Beispiel-Lambda-Funktion wird aufgerufen Node.js, EventBridge wenn von Amazon EBS ein entsprechendes `createSnapshot` Ereignis ausgesendet wird (was

bedeutet, dass ein Snapshot abgeschlossen wurde). Nach der Auslösung kopiert die Funktion den Snapshot von `us-east-2` nach `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
```

```
        } else {
            const successMessage = `Successfully started copy of snapshot
 ${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

Um sicherzustellen, dass Ihre Lambda-Funktion von der EventBridge Konsole aus verfügbar ist, erstellen Sie sie in der Region, in der das Ereignis eintreten wird. EventBridge Weitere Informationen finden Sie im AWS Lambda -Entwicklerhandbuch.

3. Öffnen Sie die EventBridge Amazon-Konsole unter. https://console.aws.amazon.com/events/
4. Wählen Sie im Navigationsbereich Rules (Regeln) und anschließend Create rule (Regel erstellen) aus.
5. Gehen Sie bei Schritt 1: Regeldetail festlegen folgendermaßen vor:
   a. Geben Sie einen Name (Namen) und eine Description (Beschreibung) ein.
   b. Behalten Sie für Event bus (Event Bus) default (Standard) bei.
   c. Vergewissern Sie sich, dass die Option Regel auf dem ausgewählten Event-Bus aktivieren aktiviert ist.
   d. Bei Event type (Ereignistyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
   e. Wählen Sie Weiter aus.
6. Bei Schritt 2: Ereignismuster erstellen gehen Sie wie folgt vor:
   a. Wählen Sie als Eventquelle die Option AWS Ereignisse oder EventBridge Partnerereignisse aus.
   b. Vergewissern Sie sich, dass im Abschnitt Event-Muster für Eventquelle AWS Service ausgewählt ist, und wählen Sie für AWS Service EC2 aus.
   c. Wählen Sie für Event type (Ereignistyp) EBS Snapshot Notification (EBS-Snapshot-Benachrichtigung) aus, dann Specific event(s) (Spezifische Ereignisse) und dann createSnapshot.
   d. Wählen Sie Spezifische(s) Ergebnis(se) und dann Erfolgreich aus.
   e. Wählen Sie Weiter aus.

7. Gehen Sie bei Schritt 3: Ziele auswählen wie folgt vor:
   a. Bei Zieltypen wählen Sie AWS -Service aus.
   b. Wählen Sie bei Select target (Ziel auswählen) Lambda function (Lamda-Funktion) und bei Function (Funktion) die zuvor von Ihnen erstellte Funktion aus.
   c. Wählen Sie Next (Weiter)
8. Bei Step 4: Configure tags (Schritt 4: Tags konfigurieren) geben Sie bei Bedarf Tags für die Regel an und wählen Sie dann Next (Weiter).
9. Bei Step 5: Review and create (Schritt 5: Überprüfen und erstellen) überprüfen Sie die Regel und wählen Sie dann Create rule (Regel erstellen).

Ihre Regel sollte jetzt auf der Registerkarte Rules (Regeln) erscheinen. Im gezeigten Beispiel sollte das von Ihnen konfigurierte Ereignis von EBS beim nächsten Kopieren eines Snapshot gesendet werden.

Detaillierte Leistungsstatistiken von Amazon EBS

Amazon EBS-NVMe-Blockgeräte senden in Echtzeit hochauflösende I/O Leistungsstatistiken für Amazon EBS-Volumes, die an Amazon EC2-Instances angeschlossen sind. Nitro-based Diese Statistiken werden als aggregierte Zähler dargestellt, die so lange aufbewahrt werden, wie das Volume an die Instance angehängt ist. Die Statistiken enthalten Details über die Gesamtzahl der Operationen, die gesendeten und empfangenen Byte und die für Lese- und I/O Schreibvorgänge aufgewendete Zeit. Darüber hinaus enthalten die Statistiken Histogramme für Lese- und Schreibvorgänge. I/O Sie geben auch an, wie lange Ihre Anwendung die bereitgestellten IOPS- oder Durchsatzgrenzwerte des EBS-Volumes oder der angehängten Instance insgesamt überschritten hat.

Sie können diese Statistiken mit einer Genauigkeit von Intervallen von bis zu 1 Sekunde erfassen. Wenn Anfragen häufiger als 1-Sekunden-Intervalle gestellt werden, kann der NVMe-Treiber die Anfragen zusammen mit anderen Administratorbefehlen in eine Warteschlange stellen, damit sie zu einem späteren Zeitpunkt verarbeitet werden können.

Überlegungen

- Die Statistiken werden für alle Amazon EBS-Volume-Typen unterstützt.
- Die Statistiken werden nur für Volumes unterstützt, die an Instances angehängt sind, die auf dem AWS Nitro-System erstellt wurden.

- Die Statistiken sind für Multi-Attach aktivierte Volumes verfügbar. Wenn Sie Statistiken für ein Multi-Attach aktiviertes Volume anzeigen, beziehen sich die Statistiken auf diesen Instanzanhang und geben nur die Nutzung dieser Instanz wieder.
- Die Statistiken sind ohne zusätzliche Kosten verfügbar.

Statistiken

Das Amazon EBS NVMe-Blockgerät verkauft die folgenden Statistiken:

Name der Statistik	Vollständiger Name	Typ	Description
`total_rea d_ops`	Gesamtzahl an Lesevorgängen	Zähler	Die Gesamtzahl der abgeschlossenen Lesevorgänge.
`total_wri te_ops`	Gesamtzahl an Schreibvorgängen	Zähler	Die Gesamtzahl der abgeschlossenen Schreibvorgänge.
`total_rea d_bytes`	Gesamtzahl der gelesenen Bytes	Zähler	Die Gesamtzahl der übertragenen und gelesenen Bytes.
`total_wri te_bytes`	Gesamtzahl der Schreibbytes	Zähler	Die Gesamtzahl der übertragenen und geschriebenen Bytes.
`total_rea d_time`	Gesamte Lesezeit	Zähler	Die Gesamtzeit für alle abgeschlossenen Lesevorgänge in Mikrosekunden.
`total_wri te_time`	Gesamte Schreibzeit	Zähler	Die Gesamtzeit für alle abgeschlossenen Schreibvorgänge in Mikrosekunden.
`ebs_volu e_perfor ance_exc eded_iop`	Die Gesamtzeit, in der der Bedarf das bereitgestellte Volumen (IOPS) überstieg	Zähler	Die Gesamtzeit in Mikrosekunden, in welcher der IOPS-Bedarf die vom Volume bereitges tellte IOPS-Leistung überstiegen hat.

Name der Statistik	Vollständiger Name	Typ	Description
ebs_volu e_perfor ance_exc eded_tp	Gesamtzeit, in der der Bedarf den Durchsatz des bereitgestellten Volumens überstieg	Zähler	Die Gesamtzeit in Mikrosekunden, in welcher der Durchsatzbedarf die vom Volume bereitgestellte Durchsatzleistung überstiegen hat.
ec2_inst nce_ebs_ erforman e_exceed d_iops	Der Gesamtzeitbedarf überstieg die IOPS-Leistung der EC2-Instanz	Zähler	Die Gesamtzeit in Mikrosekunden, in der das EBS-Volume die maximale IOPS-Leistung der angeschlossenen Amazon-EC2-Instance überschritten hat.
ec2_inst nce_ebs_ erforman e_exceed d_tp	Der Gesamtzeitbedarf überstieg die Durchsatzleistung der EC2-Instance	Zähler	Die Gesamtzeit in Mikrosekunden, in der das EBS-Volume die maximale Durchsatzleistung der angeschlossenen Amazon-EC2-Instance überschritten hat.
volume_qu eue_leng h	Länge der Volume-Warteschlange	Zeitpunkt	Die Anzahl der Lese- und Schreibvorgänge, die auf Abschluss warten.
read_io_ atency_h stogram	Histogramm lesen I/O	Histogramm *	Die Anzahl der innerhalb der einzelnen Latenzbereiche abgeschlossenen Lesevorgänge in Mikrosekunden.
write_io_ latency_h istogram	Histogramm schreiben I/O	Histogramm *	Die Anzahl der innerhalb der einzelnen Latenzbereiche abgeschlossenen Schreibvorgänge in Mikrosekunden.

Note

* Die Histogrammstatistik stellt nur I/O Operationen dar, die erfolgreich abgeschlossen wurden. I/O Betriebsabläufe, die ins Stocken geraten oder beeinträchtigt sind, sind nicht

enthalten, werden aber in den `volume_queue_length` Statistiken deutlich, die als Zeitpunktstatistik dargestellt werden.

Auf die Statistiken zugreifen

Auf die Statistiken muss direkt von der Instance aus zugegriffen werden, an die das Amazon EBS-Volume angehängt ist. Sie können mit einer der folgenden Methoden auf die Statistik zugreifen.

Linux-Instances

Amazon CloudWatch

Sie können den CloudWatch Amazon-Agenten so konfigurieren, dass er die Statistiken aus Ihrer Instance sammelt und sie als benutzerdefinierte Metriken in CloudWatch verfügbar macht. Anschließend können Sie die Metriken verwenden, CloudWatch um I/O Muster zu analysieren, Leistungstrends zu verfolgen, benutzerdefinierte Dashboards zu erstellen und automatische Alarme auf der Grundlage von Leistungsschwellenwerten einzurichten.

Weitere Informationen zur Konfiguration des CloudWatch Agenten finden Sie unter den folgenden Links:

- Erstellen Sie die CloudWatch Agenten-Konfigurationsdatei
- Erfassen Sie die Amazon EBS-NVMe-Treibermetriken

Mit der Amazon CloudWatch Observability EKS-Add-on-Version `4.1.0` und höher werden die Statistiken automatisch erfasst, wenn die Amazon EBS-CSI-Treibermetriken aktiviert werden. Weitere Informationen finden Sie unter Amazon EBS NVMe-Treibermetriken.

ebsnvme script

Das `ebsnvme` Skript befindet sich im Github-Repo von amazon-ec2-utils.

So greifen Sie auf die Statistiken zu

1. Stellen Sie eine Verbindung zu der Instance her, der das Volume angehängt ist.
2. Laden Sie das `ebsnvme` Skript aus dem Github-Repo herunter. `amazon-ec2-utils`

```
wget https://raw.githubusercontent.com/amazonlinux/amazon-ec2-utils/refs/heads/
main/ebsnvme
```

3. Ändern Sie die Berechtigungen für das Skript, um es ausführbar zu machen.

```
sudo chmod +x ./ebsnvme
```

4. Führen Sie das `ebsnvme` Skript aus und geben Sie den Gerätenamen für das Volume an.

```
sudo ./ebsnvme stats /dev/nvme0n1
```

nvme-cli tool

So greifen Sie auf die Statistiken zu

1. Stellen Sie eine Verbindung zu der Instance her, der das Volume angehängt ist.
2. Amazon Linux-AMIs, die nach dem 12. November 2024 veröffentlicht wurden, enthalten die neueste Version des `nvme-cli` Tools. Wenn Sie ein älteres Amazon Linux AMI verwenden, aktualisieren Sie das `nvme-cli`-Tool.

```
sudo yum install nvme-cli
```

3. Führen Sie den folgenden Befehl aus und geben Sie den Gerätenamen für das Volume an.

```
nvme amzn stats /dev/nvme0n1
```

Prometheus

Sie können die Statistiken mit Prometheus, einer Open-Source-Überwachungsanwendung, und Amazon Managed Service for Prometheus überwachen. Dies erleichtert die skalierbare Überwachung von Amazon EBS-Volumes in Container- und Kubernetes-Umgebungen. Mit der Amazon EBS-CSI-Treiberversion v1.37.0 und höher werden die detaillierten Leistungsstatistiken als Endpunkt für den Export nach Prometheus bereitgestellt. Prometheus-compatible `/metrics`

Weitere Informationen finden Sie unter Ingest Metrics in Ihren Amazon Managed Service for Prometheus-Workspace im Amazon Managed Service for Prometheus-Benutzerhandbuch.

Windows-Instances

nvme_amzn.exe tool

So greifen Sie auf die Statistiken zu

1. Stellen Sie eine Verbindung zu der Instance her, der das Volume angehängt ist.
2. Stellen Sie sicher, dass Sie die AWSNVMe-Treiberversion `1.7.0` oder höher verwenden. Weitere Informationen zur Aktualisierung des AWSNVMe-Treibers finden Sie unter AWS - NVMe-Treiber.
3. Rufen Sie die Festplattennummer für das EBS-Volume ab. Weitere Informationen finden Sie unter Zuordnen von Amazon EBS-Volumes zu NVMe-Gerätenamen
4. Führen Sie den folgenden Befehl als Administrator aus und geben Sie die Festplattennummer für das Volume an.

```
.\nvme_amzn.exe stats disk_number
```

Amazon GuardDuty für Amazon EBS

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der Ihnen hilft, Ihre Konten, Container, Workloads und die Daten in Ihrer AWS Umgebung zu schützen. Mithilfe von Modellen für maschinelles Lernen (ML) und Funktionen zur Erkennung von Anomalien und Bedrohungen werden GuardDuty kontinuierlich verschiedene Protokollquellen und Laufzeitaktivitäten überwacht, um potenzielle Sicherheitsrisiken und böswillige Aktivitäten in Ihrer Umgebung zu identifizieren und zu priorisieren.

Die darin enthaltene Malware-Schutzfunktion GuardDuty scannt die Amazon EBS-Volumes, die Ihren Amazon EC2 EC2-Instances und Container-Workloads zugeordnet sind, um potenzielle Bedrohungen zu erkennen. GuardDuty bietet zwei Möglichkeiten, dies zu tun:

- Malware-Schutz aktivieren — Wenn ein Ergebnis GuardDuty generiert wird, das auf das potenzielle Vorhandensein von Malware in einer Amazon EC2 EC2-Instance oder einem Container-Workload hinweist, wird automatisch ein Malware-Scan auf der potenziell gefährdeten Ressource initiiert.
- Verwenden Sie den On-Demand-Malware-Scan, ohne den Malware-Schutz zu aktivieren — Geben Sie den Amazon-Ressourcennamen (ARN) Ihrer Amazon EC2-Instance an, um einen On-Demand-Scan zu starten.

Weitere Informationen finden Sie im GuardDuty Amazon-Benutzerhandbuch.

Verstehen Sie die Codes für Amazon EBS in Abrechnungs- und Nutzungsberichten

Wenn Sie Amazon EBS verwenden, nehmen wir entsprechende Codes in Ihre AWS Abrechnungs- und Nutzungsberichte auf. Die Überprüfung dieser Codes hilft Ihnen, Ihre Kosten und Nutzungsmuster für Amazon EBS zu verstehen. Die Nachverfolgung und Verwaltung Ihrer Ausgaben ist für die Optimierung Ihrer Kosten unerlässlich.

In den folgenden Tabellen werden die Codes für Amazon EBS beschrieben, die in Ihren Abrechnungs- und Nutzungsberichten erscheinen. Eine Liste der Regionscodes in den Fakturierungs- und Nutzungsberichten finden Sie unter AWS -Regions-Fakturierungscodes.

Fakturierungscodes für:

- -Snapshots
- Volume-Speicher
- Bereitgestellte Leistung
- Direkte EBS-APIs
- Schnelle Snapshot-Wiederherstellung (FSR)

Zugehörige Ressourcen

- Amazon EBS-Preise
- the section called “Preisgestaltung”

-Snapshots

Code	Description	Einheiten	Granularity
region-EBS:SnapshotUsage	Snapshots der Standardebene (inkrementelle Kopien).	GB-Month	Stündlich

Code	Description	Einheiten	Granularity
region-EBS:SnapshotArchiveStorage	Snapshots der Archivierungsebene (vollständige Kopien).	GB-Month	Stündlich
region-EBS:SnapshotArchiveEarlyDelete	Löschen archivierter Snapshots vor Ablauf der Mindestaufbewahrungsdauer.	GB	Pro Löschung
region-EBS:SnapshotArchiveRetrieval	Archivierte Snapshots werden abgerufen.	GB	Pro GB

Volume-Speicher

Code	Description	Einheiten	Granularity
region-EBS:VolumeUsage.gp3	Speicher für Allzweck-SSD-Volumes (GP3).	GB-Month	Stündlich
region-EBS:VolumeUsage.gp2	Speicher für Allzweck-SSD-Volumes (g2).	GB-Month	Stündlich
region-EBS:Volu	Speicher für bereitgestellte IOPS-SSD-Volumes (io2).	GB-Month	Stündlich

Code	Description	Einheiten	Granularity
meUsage.io2			
region-EBS:VolumeUsage.piops	Speicher für bereitgestellte IOPS-SSD-Volumes (io1).	GB-Month	Stündlich
region-EBS:VolumeUsage.st1	Speicher für durchsatzoptimierte HDD-Volumes.	GB-Month	Stündlich
region-EBS:VolumeUsage.sc1	Speicher für Cold HDD-Volumes.	GB-Month	Stündlich
region-EBS:VolumeUsage	Speicher für magnetische Volumen.	GB-Month	Stündlich

Bereitgestellte Leistung

Code	Description	Einheiten	Granularity
region-EBS:VolumeP-Throughput.gp3	Bereitgestellter Durchsatz für GP3-Volumes über 125. MB/s	MB/s-Month	Stündlich
region-EBS:Volu	Bereitgestellte IOPS für GP3-Volumes über 3.000.	IOPS-Month	Stündlich

Code	Description	Einheiten	Granularity
meP-IOPS.gp3			
region-EBS:VolumeP-IOPS.io2	Bereitgestellte IOPS für io2-Volumes bis zu 32.000.	IOPS-Month	Stündlich
region-EBS:VolumeP-IOPS.io2.tier2	Bereitgestellte IOPS für io2-Volumes von 32.001 bis 64.000.	IOPS-Month	Stündlich
region-EBS:VolumeP-IOPS.io2.tier3	Bereitgestellte IOPS für io2-Volumes über 64.000.	IOPS-Month	Stündlich
region-EBS:VolumeP-IOPS.piops	Bereitgestellte IOPS für io1-Volumes.	IOPS-Month	Stündlich
region-EBS:VolumeIOUsage	Ältere IOPS.	IOPS-Month	Stündlich

Direkte EBS-APIs

Code	Description	Einheiten	Granularity
region-EBS:dire	Aufrufe der `ListChangedBlocks` und `ListSnapshotBlocks` API-Aktionen.	Pro 1.000 Anfragen	Pro Anfrage

Code	Description	Einheiten	Granularity
`ctAPI.snapshot.List`			
region-`EBS:directAPI.snapshot.Get`	Von der `GetSnapshotBlock` API-Aktion zurückgegebene Blöcke.	Pro 1.000 zurückgegebenen Blöcken	Pro Anfrage
region-`EBS:directAPI.snapshot.Put`	Von der `PutSnapshotBlock` API-Aktion geschriebene Blöcke.	Pro 1.000 geschriebenen Blöcken	Pro Anfrage

Schnelle Snapshot-Wiederherstellung (FSR)

Code	Description	Einheiten	Granularity
region-`EBS:FastSnapshotRestore`	Datendienste Unit-Hours (DSU-Hours) für Snapshots sind für eine schnelle Snapshot-Wiederherstellung aktiviert (pro AZ).	DSU-Hours	Pro Minute (mindestens eine Stunde)

Erstellen Sie ein Inventar Ihrer EBS-Volumes

Amazon EBS bietet skalierbare, leistungsstarke Blockspeicherressourcen, die mit EC2-Instances verwendet werden können. Sie können ein EBS-Volume an eine EC2-Instance anhängen. Sie können ein EBS-Volume auch von einer EC2-Instance trennen.

Im Folgenden sind die wichtigsten Merkmale des EBS-Speichers aufgeführt. Ein Systemadministrator kann Informationen über diese Eigenschaften Ihrer EBS-Ressourcen abrufen und sie verwenden, um funktionell äquivalenten Speicher für Server zu konfigurieren, die Sie vor Ort betreiben, oder für Server von einem anderen Cloud-Anbieter. Ein Systemadministrator kann auch die in Ihren

EBS-Ressourcen gespeicherten Daten abrufen und die Daten dann vor Ort oder im Speicher eines anderen Cloud-Anbieters speichern.

Merkmal	Description
Datenträger	Ein EBS-Volume ist ein robustes Speicherg erät auf Blockebene, das Sie an eine Instance anhängen, formatieren und mounten können.
I/O Leistung	Amazon EBS bietet mehrere Volumentypen, die sich in Bezug auf Leistungsmerkmale und Preis unterscheiden.
Inhalt Ihrer EBS-Datenvolumen	Die einzige Möglichkeit, direkt auf die Daten auf einem Volume zuzugreifen, ist von der Instance aus.
Snapshots	Ein EBS-Snapshot ist eine Point-in-Time-Kopie der Daten auf einem EBS-Volume. Snapshots werden in Amazon S3 in Buckets gespeichert, auf die Sie nicht direkt zugreifen können.
Inhalt Ihrer EBS-Snapshots	Sie können Daten aus Ihren Snapshots lesen oder sie zum Erstellen von Volumes verwenden .

Datenträger

Wenn Sie ein EBS-Volume erstellen, wählen Sie eine Availability Zone für das Volume aus. Sie müssen ein EBS-Volume an eine EC2-Instance in derselben Availability Zone anhängen. Sie können Volumes erstellen, wenn Sie eine EC2-Instance starten, oder sie zuerst erstellen und dann an eine Instance anhängen. Wenn ein Volume an eine Instance angehängt ist, lautet `in-use` sein Status. Wenn ein Volume nicht an eine Instance angehängt ist, lautet sein Status`available`.

Warum diese wichtig sind

EBS-Root-Volumes enthalten das Betriebssystem für Ihre EC2-Instances. EBS-Datenvolumes können geschäftskritische Daten enthalten. Sie können Ihre EBS-Volumes in allen Regionen auflisten und angeben, ob sie an EC2-Instances angehängt sind.

Um eine Zusammenfassung Ihrer EBS-Volumes in allen Regionen zu erhalten

Sie können Amazon EC2 Global View verwenden, um Ihre EBS-Volumes in allen Regionen aufzulisten.

1. Öffnen Sie die Amazon EC2 Global View-Konsole unter. https://console.aws.amazon.com/ec2globalview/home
2. Überprüfen Sie auf der Registerkarte Regions-Explorer unter Zusammenfassung die Anzahl der Ressourcen für Volumes, einschließlich der Anzahl der Volumes und der Anzahl der Regionen. Wählen Sie den unterstrichenen Text aus, um zu sehen, wie sich die Volumenzahl auf die Regionen verteilt.
3. Wählen Sie auf der Registerkarte Globale Suche den Client-Filter Ressourcentyp = Volume aus. Sie können die Ergebnisse weiter filtern, indem Sie eine Region oder ein Tag angeben.

Um die EBS-Volumes zu beschreiben, die verwendet werden

Verwenden Sie den Befehl describe-volumes. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie EBS-Volumes haben. Der `--filters` Parameter beschränkt die Ergebnisse auf Volumes, die `in-use` Der `--query` Parameter zeigt nur die angegebenen Felder in der Ausgabe an. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-volumes \
    --filters Name=status,Values=in-use \
    --query "Volumes[].[VolumeId,Size,Attachments[0].InstanceId]" \
    --output table
```

Es folgt eine Beispielausgabe. Die Spalten enthalten die Volume-ID, die Volume-Größe, die ID der angehängten Instanz und den Gerätenamen.

```
-------------------------------------------------------------------
|                         DescribeVolumes                         |
+-------------------------+-----+----------------------+-----------+
|  vol-0992ee65bec96de19 |  8  |  i-00a7d9ec76a46a49f  |  /dev/xvda |
|  vol-04d631d22047db1cb |  30 |  i-0b1bf24fd4f297ab9  |  /dev/sda1 |
   ...
```

```
   ...
|  vol-0b811be5cbd1425cc | 100 |  i-0a8d998154b320257  |  /dev/xvde |
+------------------------+-----+-----------------------+------------+
```

Zur Beschreibung der EBS-Volumes, die nicht verwendet werden

Ändern Sie im vorherigen Befehl den Filter, um Volumes mit dem folgenden Status `available` zu finden.

```
--filters Name=status,Values=available
```

Wenn ein Volume unbenutzt ist, sollten Sie ermitteln, ob es Daten enthält, die Sie benötigen. Sie können beispielsweise Volumes löschen, die zu Testzwecken oder zur Behebung eines Problems erstellt wurden. Ein Volume ist möglicherweise auch verfügbar, wenn das Blockgerät, das das Volume an die Instance angeschlossen hat, so konfiguriert wurde, dass es auch nach dem Beenden der Instance bestehen bleibt. Wenn dies der Fall ist, überprüfen Sie, ob die Daten auf dem Volume noch benötigt werden.

I/O Leistung

Der Volumetyp, den Sie für ein EBS-Volume angeben, bestimmt dessen Leistung. Je nach Volume-Typ können Sie eine Kombination aus Größe, IOPS und Durchsatz für Ihre Volumes angeben. Informationen zu den maximal bereitgestellten IOPS und zum Durchsatz für jeden Volume-Typ finden Sie unter Amazon EBS-Volume-Typen.

Warum das wichtig ist

Nachdem Sie die Leistung Ihrer EBS-Volumes bestimmt haben, können Sie die Mindestanforderungen festlegen, die für einen funktionell gleichwertigen Speicher erforderlich sind.

Um Informationen über die Leistung Ihrer Volumes zu erhalten

Verwenden Sie den Befehl describe-volumes, um die Leistung Ihrer verwendeten Volumes zu beschreiben. Der `--query` Parameter zeigt nur die angegebenen Felder in der Ausgabe an. Sie können nach Bedarf weitere Felder hinzufügen. Informationen zur EBS-optimized Leistung finden Sie in den Spezifikationen für den Amazon EC2-Instance-Typ im Amazon EC2-Instance-Types-Handbuch.

```
aws ec2 describe-volumes \
    --filters Name=status,Values=in-use \
```

```
    --query "Volumes[].[VolumeId,VolumeType,Iops,Throughput]" \
    --output table
```

Es folgt eine Beispielausgabe. Die Spalten lauten Volume-ID, Volume-Typ, IOPS und Durchsatz (). MiB/s

```
-------------------------------------------------
|                DescribeVolumes                |
+------------------------+------+-------+-------+
|  vol-0992ee65bec96de19 |  gp3 |  3000 |  125  |
|  vol-04d631d22047db1cb |  gp2 |  100  |  None |
   ...
   ...
|  vol-0b811be5cbd1425cc |  gp3 |  3000 |  125  |
+------------------------+------+-------+-------+
```

Inhalt Ihrer EBS-Datenvolumes

Amazon EBS hat keinen Zugriff auf die Daten, die Sie auf Ihren EBS-Volumes speichern. Sie sind für die Sicherung Ihrer Datenvolumen verantwortlich. Sie können beispielsweise Point-in-Time-Snapshots, sogenannte EBS-Snapshots, erstellen.

Sie können auch eine Verbindung zu Ihren EC2-Instances herstellen und Dateien von Ihren EBS-Volumes auf Ihren eigenen Computer übertragen. Es gibt viele Tools, die Ihnen dabei helfen. Im Folgenden sind einige Beispiele aufgeführt.

Warum das wichtig ist

Wenn sich auf Ihren EBS-Volumes geschäftskritische Daten befinden, können Sie diese auf einen funktionell gleichwertigen Speicher kopieren.

Um Dateien von einem Volume zu übertragen, das an eine Linux-Instance angehängt ist

Stellen Sie eine Verbindung zu Ihrer Linux-Instance her und verwenden Sie SCP. Weitere Informationen finden Sie unter Dateien mit SCP übertragen.

Um Dateien von einem Volume zu übertragen, das an eine Windows-Instanz angehängt ist

Stellen Sie eine Verbindung zu Ihrer Windows-Instanz her und verwenden Sie RDP. Weitere Informationen finden Sie unter Dateien mit RDP https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-to-linux-instanceWindowsFileTransfer.html übertragen.

-Snapshots

Sie können Ihre EBS-Datenvolumes sichern, indem Sie EBS-Snapshots erstellen. Sie können EBS-Snapshots mit Amazon EBS, Amazon Data Lifecycle Manager oder erstellen. AWS Backup

Warum das wichtig ist

Wenn Sie geschäftskritische Daten auf Ihren EBS-Volumes haben, erstellen Sie höchstwahrscheinlich Backups in Form von EBS-Snapshots. Sie können die neuesten Snapshots Ihrer Volumes finden und überprüfen, ob sie die aktuellen Daten auf den Volumes widerspiegeln.

Um die Snapshots für ein bestimmtes Volume zu beschreiben

Verwenden Sie den Befehl describe-snapshots. Der `--filters` Parameter beschränkt die Ergebnisse auf Schnappschüsse für das angegebene Volume. Der `--query` Parameter zeigt nur die angegebenen Felder in der Ausgabe an. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-snapshots \
    --filters Name=volume-id,Values=vol-00622ef8c2ac8b762 \
    --query Snapshots[*].[SnapshotId,CompletionTime,Description] --output table
```

Es folgt eine Beispielausgabe. Die Spalten enthalten die Snapshot-ID, das Abschlussdatum und ob das Volume verschlüsselt ist.

```
-------------------------------------------------------------------------
|                            DescribeSnapshots                          |
+-------------------------+-----------------------------------+--------+
|  snap-0ad439c50efabb47c |  2024-07-12T03:36:27.952000+00:00  |  False |
+-------------------------+-----------------------------------+--------+
```

Inhalt Ihrer EBS-Snapshots

Sie können den Inhalt eines EBS-Snapshots nicht herunterladen oder in ein anderes Format exportieren. Sie können jedoch mithilfe der direkten EBS-APIs auf die Daten in Ihren Snapshots zugreifen oder indem Sie aus dem Snapshot ein EBS-Volume erstellen und die Dateien übertragen.

Warum das wichtig ist

Wenn Sie geschäftskritische Daten auf Ihren EBS-Volumes haben, erstellen Sie höchstwahrscheinlich Backups in Form von EBS-Snapshots. Sie können diese Daten abrufen und in einen funktionell gleichwertigen Speicher kopieren.

Option 1: Um Daten aus Ihren Snapshots zu lesen

Verwenden Sie die direkten EBS-APIs.

Option 2: Um ein Volume aus einem Snapshot zu erstellen und die Daten zu übertragen

1. Verwenden Sie den Befehl create-volume, um aus dem Snapshot ein Volume zu erstellen.

```
aws ec2 create-volume \
   --volume-type gp3 \
   --snapshot-id snap-0ad439c50efabb47c \
   --iops 6000 \
   --availability-zone us-east-2b
```

2. Verwenden Sie den Befehl attach-volume, um das Volume an eine Instance anzuhängen.

```
aws ec2 attach-volume \
   --device /dev/sdf \
   --instance-id i-0b1bf24fd4f297ab9 \
   --volume-id vol-1234567890abcdef0
```

3. Stellen Sie eine Verbindung zu Ihrer Instance her und formatieren und mounten Sie das Volume.
4. Übertragen Sie die Dateien auf dem Volume auf Ihren eigenen Computer.

Kontingente für Amazon EBS

Für jede AWS-Konto AWS-Service dieser Kontingente gelten Standardkontingente, die früher als Limits bezeichnet wurden. Sofern nicht anders angegeben, gilt für jedes Kontingent Folgendes Region-specific. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für Amazon EBS anzuzeigen, öffnen Sie die Service Quotas Console. Wählen Sie im Navigationsbereich AWS Services und dann Amazon Elastic Block Store (Amazon EBS) aus. Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS-Konto hat die folgenden Kontingente in Bezug auf Amazon EBS.

Name	Standard	Anpas	Description
Archivierte Snapshots pro Volume	Jede unterstützte Region: 25	Ja	Die maximale Anzahl archivierter Snapshots pro Volume.
CompleteSnapshot Anfragen pro Konto	Jede unterstützte Region: 10 pro Sekunde	Nein	Die maximal zulässige Anzahl von CompleteSnapshot Anfragen pro Konto.
Gleichzeitige Snapshot-Kopien pro Zielregion	Jede unterstützte Region: 20	Nein	Die maximale Anzahl gleichzeitiger Snapshot-Kopien in eine einzelne Zielregion.
Gleichzeitige Snapshots pro Cold-HDD-Volume (sc1)	Jede unterstützte Region: 1	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Cold-HDD-Volume (sc1) in dieser Region.
Gleichzeitige Snapshots pro Universelle-SSD-Volume (gp2)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Universelle-SSD-

Name	Standard	Anpas	Description
			Volume (gp2) in dieser Region.
Gleichzeitige Snapshots pro Universelle-SSD-Volume (gp3)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Universelle-SSD-Volume (gp3) in dieser Region.
Gleichzeitige Snapshots pro Magnetfestplatten-Volume (Standard)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Magnetfestplatten-Volume (Standard) in dieser Region.
Gleichzeitige Snapshots pro Bereitgestellte-IOPS-SSD-Volume (io1)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Bereitgestellte-IOPS-SSD-Volume (io1) in dieser Region.
Gleichzeitige Snapshots pro Bereitgestellte-IOPS-SSD-Volume (io2)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Bereitgestellte-IOPS-SSD-Volume (io2) in dieser Region.
Gleichzeitige Snapshots pro Durchsatzoptimierte-HDD-Volume (st1)	Jede unterstützte Region: 1	Nein	Die maximale Anzahl gleichzeitiger Snapshots pro Durchsatzoptimierte-HDD-Volume (st1) in dieser Region.

Name	Standard	Anpas	Description
Schnelle Snapshot-Wiederherstellung	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von Snapshots, die für die schnelle Snapshot-Wiederherstellung in dieser Region aktiviert werden können.
GetSnapshotBlock Anfragen pro Konto	us-east-1:5.000 pro Sekunde us-east-2:5.000 pro Sekunde us-west-2:5.000 pro Sekunde ap-southeast-1:5.000 pro Sekunde eu-west-1:5.000 pro Sekunde Jede der anderen unterstützten Regionen: 1.000 pro Sekunde	Ja	Die maximal zulässige Anzahl von GetSnapshotBlock Anfragen pro Konto.
GetSnapshotBlock Anfragen pro Snapshot	Jede unterstützte Region: 1000 pro Sekunde	Nein	Die maximal zulässige Anzahl von GetSnapshotBlock Anfragen pro Snapshot.

Name	Standard	Anpas	Description
IOPS für bereitgestellte IOPS-SSD-Volumes (io1)	Jede unterstützte Region: 300 000	Ja	Die maximale aggregierte Anzahl von IOPS, die für bereitgestellte IOPS-SSD-Volumes (io1) in dieser Region bereitgestellt werden können.
IOPS für Bereitgestellte-IOPS-SSD-Volumes (io2)	Jede unterstützte Region: 100 000	Ja	Die maximale aggregierte Anzahl von IOPS, die für bereitgestellte IOPS-SSD-Volumes (io2) in dieser Region bereitgestellt werden können.
IOPS-Änderungen für Bereitgestellte-IOPS-SSD-Volumes (io1)	Jede unterstützte Region: 500 000	Ja	Die maximale aggregierte Anzahl von IOPS, die über Bereitgestellte-IOPS-SDD-Volumes (io1) in dieser Region durch Volume-Änderungen angefordert werden können.
IOPS-Änderungen für Bereitgestellte-IOPS-SSD-Volumes (io2)	Jede unterstützte Region: 100 000	Ja	Die maximalen aktuellen (von) und angeforderten (bis) IOPS für Volume-Änderungsanfragen über bereitgestellte IOPS-SSD (io2)-Volumes in dieser Region.
In-progress Snapshot-Archive pro Konto	Jede unterstützte Region: 25	Ja	Die maximale Anzahl aktiver Snapshot-Archiven pro Konto.

Name	Standard	Anpas	Description
In-progress Snapshot-Wiederher stellungen aus dem Archiv pro Konto	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl aktiver Snapshot-Wiederherstellungen aus dem Archiv pro Konto.
ListChangedBlocks Anfragen pro Konto	Jede unterstützte Region: 50 pro Sekunde	Nein	Die maximal zulässige Anzahl von ListChang edBlocks Anfragen pro Konto.
ListSnapshotBlocks Anfragen pro Konto	Jede unterstützte Region: 50 pro Sekunde	Nein	Die maximal zulässige Anzahl von ListSnaps hotBlocks Anfragen pro Konto.
Maximale Anzahl gleichzeitiger Kopiervolumenvorgänge pro Konto	Jede unterstützte Region: 5	Yes (Ja)	Maximale Anzahl gleichzeitiger Kopiervol umen-Operationen, die pro Konto in dieser Region zulässig sind.
Bereitgestellte Rate für die Volumenin itialisierung bei gleichzeitigen Anfragen zur Volumenerstellung pro Region	Jede unterstützte Region: 5 000	Ja	Die maximale aggregier te Rate für die Volumenin itialisierung, in MiB/s, die für gleichzeitige Volume-Erstellungsanfragen in dieser Region angefordert werden kann.

Name	Standard	Anpas	Description
PutSnapshotBlock Anfragen pro Konto	us-east-1:5.000 pro Sekunde us-east-2:5.000 pro Sekunde us-west-2:5.000 pro Sekunde ap-southeast-1:5.000 pro Sekunde eu-west-1:5.000 pro Sekunde Jede der anderen unterstützten Regionen: 1.000 pro Sekunde	Ja	Die maximal zulässige Anzahl von PutSnapshotBlock Anfragen pro Konto.
PutSnapshotBlock Anfragen pro Snapshot	Jede unterstützte Region: 1000 pro Sekunde	Nein	Die maximal zulässige Anzahl von PutSnapshotBlock Anfragen pro Snapshot.
Snapshots pro Region	Jede unterstützte Region: 100 000	Ja	Die maximale Anzahl von Snapshots pro Region.
StartSnapshot ausstehende Snapshots pro Konto	Jede unterstützte Region: 100	Nein	Die maximale Anzahl ausstehender Snapshots pro Konto, die mithilfe der StartSnapshot API erstellt werden können.
StartSnapshot Anfragen pro Konto	Jede unterstützte Region: 10 pro Sekunde	Nein	Die maximal zulässige Anzahl von StartSnapshot Anfragen pro Konto.

Name	Standard	Anpas	Description
Speicher für Cold-HDD-Volumes (sc1), in TiB	us-east-1:50 US-Ost-2:50 US-West-1:50 US-West-2:50 ap-northeast-1:50 ap-northeast-2:50 AP-Süd-1:50 AP-Southeast-1:50 AP-Southeast-2:50 ca-central-1:50 EU-Zentral-1:50 EU-Nord-1:50 EU-West-1:50 eu-west-2:50 EU-West-3:50 sa-ost-1:50 Jede der anderen unterstützten Regionen: 300	Ja	Die maximale aggregierte Speichermenge in TiB, die über Cold-HDD-Volumes (sc1) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Universelle-SSD-Volumes (gp2), in TiB	us-east-1:50 US-Ost-2:50 US-West-1:50 US-West-2:50 ap-northeast-1:50 ap-northeast-2:50 AP-Süd-1:50 AP-Southeast-1:50 AP-Southeast-2:50 ca-central-1:50 EU-Zentral-1:50 EU-Nord-1:50 EU-West-1:50 eu-west-2:50 EU-West-3:50 sa-ost-1:50 Jede der anderen unterstützten Regionen: 300	Ja	Die maximale aggregierte Speichermenge in TiB, die über Universelle-HDD-Volumes (gp2) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Universelle-SSD-Volumes (gp3), in TiB	af-south-1: 300 ap-east-1: 300 ap-east-2:300 ap-Nordost-3:300 AP-Süd-2:300 AP-Soudost-4:300 AP-Southeast-5:300 AP-Soudost-6:300 AP-Soudost-7:300 ca-west-1:300 eu-central-2:300 eu-south-1: 300 EU-Süd-2:300 il-Central-1:300 mx-central-1:300 Jede der anderen unterstützten Regionen: 50	Ja	Die maximale aggregierte Speichermenge in TiB, die über Universelle-HDD-Volumes (gp3) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Magnetfestplatten-Volumes (Standard), in TiB	us-east-1:50 US-Ost-2:50 US-West-1:50 US-West-2:50 ap-northeast-1:50 ap-northeast-2:50 AP-Süd-1:50 AP-Southeast-1:50 AP-Southeast-2:50 ca-central-1:50 EU-Zentral-1:50 EU-Nord-1:50 EU-West-1:50 eu-west-2:50 EU-West-3:50 sa-ost-1:50 Jede der anderen unterstützten Regionen: 300	Ja	Die maximale aggregierte Speichermenge in TiB, die über Magnetfestplatten-Volumes (Standard) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Bereitgestellte-IOPS-SSD-Volumes (io1), in TiB	us-east-1:50 US-Ost-2:50 US-West-1:50 US-West-2:50 ap-northeast-1:50 ap-northeast-2:50 AP-Süd-1:50 AP-Southeast-1:50 AP-Southeast-2:50 ca-central-1:50 EU-Zentral-1:50 EU-Nord-1:50 EU-West-1:50 eu-west-2:50 EU-West-3:50 sa-ost-1:50 Jede der anderen unterstützten Regionen: 300	Ja	Die maximale aggregierte Speichermenge in TiB, die über Bereitgestellte-IOPS-SSD-Volumes (io1) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Bereitgestellte-IOPS-SSD-Volumes (io2), in TiB	Jede unterstützte Region: 20	Ja	Die maximale aggregierte Speichermenge in TiB, die über Bereitgestellte-IOPS-SSD-Volumes (io2) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicher für Durchsatzoptimierte-HDD-Volumes (st1), in TiB	us-east-1:50 US-Ost-2:50 US-West-1:50 US-West-2:50 ap-northeast-1:50 ap-northeast-2:50 AP-Süd-1:50 AP-Southeast-1:50 AP-Southeast-2:50 ca-central-1:50 EU-Zentral-1:50 EU-Nord-1:50 EU-West-1:50 eu-west-2:50 EU-West-3:50 sa-ost-1:50 Jede der anderen unterstützten Regionen: 300	Ja	Die maximale aggregierte Speichermenge in TiB, die über Durchsatzoptimierte-HDD-Volumes (st1) in dieser Region bereitgestellt werden kann.

Name	Standard	Anpas	Description
Speicheränderungen für Cold-HDD-Volumes (sc1), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Cold-HDD-Volumes (sc1) durch Volume-Änderungen in dieser Region angefordert werden kann.
Speicheränderungen für Universelle-SSD-Volumes (gp2), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Universelle-SSD-Volumes (gp2) durch Volume-Änderungen in dieser Region angefordert werden kann.
Speicheränderungen für Universelle-SSD-Volumes (gp3), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Universelle-SSD-Volumes (gp3) durch Volume-Änderungen in dieser Region angefordert werden kann.
Speicheränderungen für Magnetfestplatten-Volumes (Standard), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Magnetfestplatten-Volumes (Standard) durch Volume-Änderungen in dieser Region angefordert werden kann.

Name	Standard	Anpas	Description
Speicheränderungen für Bereitgestellte-IOPS-SSD-Volumes (io1), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Bereitgestellte-IOPS-SSD-Volumes (io1) durch Volume-Änderungen in dieser Region angefordert werden kann.
Speicheränderungen für Bereitgestellte-IOPS-SSD-Volumes (io2), in TiB	Jede unterstützte Region: 20	Ja	Die maximale aggregierte Speichermenge in TiB, die über Bereitgestellte-IOPS-SSD-Volumes (io2) durch Volume-Änderungen in dieser Region angefordert werden kann.
Speicheränderungen für Durchsatz optimierte-HDD-Volumes (st1), in TiB	Jede unterstützte Region: 500	Ja	Die maximale aggregierte Speichermenge in TiB, die über Durchsatz optimierte-HDD-Volumes (st1) durch Volume-Änderungen in dieser Region angefordert werden kann.
Time-based Snapshot-Kopierdurchsatz pro Zielregion	Jede unterstützte Region: 2.000	Ja	Der maximale Durchsatz auf Kontoebene, in MiB/sec, für zeitbasierte Snapshot-Kopiervorgänge pro Zielregion.

Überlegungen

- Ihre Kontingente können sich im Laufe der Zeit ändern. Amazon EBS überwacht ständig Ihren bereitgestellten Speicher und Ihre IOPS-Nutzung in jeder Region und kann Ihre Kontingente je nach Nutzung automatisch pro Region erhöhen. Obwohl Amazon EBS Ihre Kontingente automatisch auf Grundlage Ihrer Nutzung erhöhen kann, können Sie bei Bedarf eine Kontingenterhöhung beantragen. Wenn Sie beispielsweise planen, in den USA Ost (Nord-Virginia) mehr gp3 Speicherplatz als Ihr aktuelles Kontingent zu nutzen, können Sie vor Ihrer geplanten Nutzung eine Kontingenterhöhung für diesen Volumentyp in dieser Region beantragen.
- Das Kontingent für gleichzeitige Snapshot-Kopien pro Zielregion kann mithilfe von Service Quotas nicht angepasst werden. Sie können jedoch eine Erhöhung dieses Kontingents beantragen, indem Sie sich an den AWS Support wenden.
- Die Kontingente für IOPS-Änderungen und Speicheränderungen gelten für den aggregierten aktuellen Wert (für Größe oder IOPS, je nach Kontingent) von Volumes, die gleichzeitig geändert werden können. Sie können gleichzeitig Änderungsanfragen für Volumes stellen, die einen kombinierten aktuellen Wert (für Größe oder IOPS) in Höhe des Kontingents haben. Wenn Ihr Kontingent für IOPS-Änderungen für bereitgestellte IOPS-SSD (io1)-Volumes beispielsweise `50,000` beträgt, können Sie gleichzeitige IOPS-Änderungsanforderungen für eine beliebige Anzahl von `io1`-Volumes stellen, sofern deren aktuelle IOPS-Gesamtanzahl gleich oder kleiner als `50,000` ist. Wenn Sie drei `io1`-Volumes mit jeweils `20,000` IOPS bereitgestellt haben, können Sie IOPS-Änderungen für zwei Volumes gleichzeitig beantragen (`20,000 * 2 < 50,000`). Wenn Sie eine gleichzeitige IOPS-Änderungsanforderung für das dritte Volume einreichen, überschreiten Sie Ihr Kontingent und diese Anfrage schlägt fehl (`20,000 * 3 > 50,000`).
- Amazon EBS hat die folgenden, nicht anpassbaren Grenzwerte für die Anzahl der EBS-Volumes pro Instance-Startanforderung.
  - `2500`—`us-east-1`,, und `us-west-2` `eu-west-1` `ap-northeast-1`
  - `500`— alle anderen Regionen

  Dieses Limit gilt für Instance-Startanfragen, die Sie stellen, und für Instance-Startanfragen, die von AWS Diensten wie Amazon EMR in Ihrem Namen gestellt werden. Wenn Ihre Instance-Startanfrage aufgrund der Überschreitung dieses Limits fehlschlägt, passen Sie die EBS-Volume-Konfiguration in der Startanforderung an, um die Anzahl der Volumes unter das Limit zu reduzieren. Sie können auch mit Ihrem Technical Account Manager (TAM) zusammenarbeiten, um andere Optionen für den Start Ihres Clusters zu prüfen.

Dokumentenverlauf für das Amazon EBS-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon EBS beschrieben.

Änderung	Beschreibung	Datum
Aktualisierung der Elastic Volumes-Änderungen	Sie können jetzt eine neue Elastic Volumes-Änderung initiieren, sobald die vorherige abgeschlossen ist, bis zu viermal innerhalb von 24 Stunden.	15. Januar 2026
Papierkorb für EBS-Volumes	Mit dem Papierkorb können Sie Amazon EBS-Volumes vor versehentlichem Löschen schützen.	20. November 2025
Kopieren Sie ein EBS-Volume	Sie können sofort eine Point-in-Time-Kopie eines Amazon EBS-Volumes innerhalb derselben Availability Zone erstellen.	14. Oktober 2025
GP3-Volumenaktualisierungen	Sie können jetzt Allzweck-SSD-Volumes (GP3) mit Größen bis zu 64 TiB, IOPS bis zu 80.000 IOPS und einem Durchsatz von bis zu 2.000 bereitstellen. MiB/s	26. September 2025
Aktualisierungen der Latenzrichtlinien für io2-Volumes	`io2`Block Express-Volumes sind so konzipiert, dass sie bei I/O 16-KB-Vorgängen eine durchschnittliche Latenz von unter 500 Mikrosekunden bieten. `io2` Block Express-	26. September 2025

	Volumes bieten im Vergleich zu Allzweck-Volumes auch eine bessere Ausreißerlatenz, wodurch die Häufigkeit von I/Os Überschreitungen von 800 Mikrosekunden um mehr als das Zehnfache reduziert wird.	
Latenzinjektion	Verwenden Sie die Aktion AWS FIS Latency Injection, um eine erhöhte I/O Latenz auf Ihren Amazon EBS-Volumes zu simulieren.	16. September 2025
`io2`Erweiterung der Region	Bereitgestellte IOPS SSD (`io2`) -Volumes sind jetzt in allen kommerziellen und AWS GovCloud (US) Regionen verfügbar.	22. Juli 2025
Lokale Schnappschüsse in lokalen Zonen	Sie können jetzt lokale Snapshots in Local Zones erstellen.	15. Mai 2025
Von Amazon EBS bereitgestellte Rate für die Volume-Initialisierung	Sie können jetzt eine Volume-Initialisierungsrate angeben, wenn Sie Amazon EBS-Volumes erstellen, um sicherzustellen, dass diese innerhalb einer vorhersehbaren Zeit vollständig initialisiert werden.	6. Mai 2025
Amazon Data Lifecycle Manager VPC-Endpunkte	Sie können jetzt eine private Verbindung zwischen Ihrer VPC und Amazon Data Lifecycle Manager herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen.	28. Februar 2025

Time-based AMI-Kopien	Sie können jetzt eine Bearbeitungsdauer für EBS-backed AMI-Kopiervorgänge anfordern, um sicherzustellen, dass AMI-Kopien innerhalb eines bestimmten Zeitrahmens abgeschlossen werden.	25. Februar 2025
Volle Snapshot-Größe	Sie können jetzt die volle Größe eines Amazon EBS-Snapshots mithilfe der Amazon EC2-Konsole anzeigen und. AWS CLI	11. Februar 2025
IPv6-Unterstützung für Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager bietet jetzt Dual-Stack-Endpunkte, die sowohl IPv4- als auch IPv6-Verkehr unterstützen.	7. Februar 2025
IPv6-Unterstützung für den Papierkorb	Der Papierkorb bietet jetzt Dual-Stack-Endpunkte, die sowohl IPv4- als auch IPv6-Verkehr unterstützen.	19. Dezember 2024
Lokale Snapshots in dediziert en lokalen Zonen	Sie können jetzt lokale Snapshots in Dedicated Local Zones erstellen.	16. Dezember 2024
AWSDataLifecycleMa nagerServiceRole AWS Die verwaltete Richtlinie wurde aktualisiert	Die AWSDataLifecycleMa nagerServiceRole AWS verwaltete Richtlinie wurde aktualisiert und enthält nun auch die Genehmigung für die `ec2:DescribeAvaila bilityZones` Aktion.	16. Dezember 2024

Deklarative Richtlinien zur Sperrung des öffentlichen Zugriffs auf EBS-Schnappschüsse	Sie können jetzt deklarative Richtlinien verwenden, um Einstellungen auf Kontoebene anzuwenden, um den öffentlichen Zugriff für Snapshots in mehreren Regionen und Konten gleichzeitig zu blockieren. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.	01. Dezember 2024
Time-based Snapshot-Kopien	Sie können jetzt eine Abschlussdauer für Snapshot-Kopiervorgänge anfordern, um sicherzustellen, dass Snapshot-Kopien innerhalb eines bestimmten Zeitrahmens abgeschlossen werden.	26. November 2024
Ausschluss-Tags für den Papierkorb	Sie können den Region-level Aufbewahrungsregeln jetzt Ausschluss-Tags hinzufügen, um Ressourcen mit bestimmten Stichwörtern auszuschließen.	19. November 2024
CloudFormation Unterstützung für den Papierkorb	Sie können jetzt Aufbewahrungsregeln für den Papierkorb mithilfe von erstellen und verwalten. AWS CloudFormation	18. November 2024

Detaillierte Leistungsstatistiken von Amazon EBS	Amazon EBS NVMe-Blockgeräte senden in Echtzeit hochauflösende I/O Leistungsstatistiken für Amazon EBS-Volumes, die mit Amazon EC2-Instances verbunden sind. Nitro-based	12. November 2024
Neue Metriken für Amazon EBS-Volumes CloudWatch	Sie können jetzt die CloudWatch Metriken`VolumeAvgReadLatency`, `VolumeAvgWriteLatency`, und `VolumeThroughputExceededCheck` Amazon verwenden`VolumeIOPSExceededCheck`, um die Volume-Leistung zu überwachen.	30. Oktober 2024
Aktivieren Sie die Amazon Data Lifecycle Manager-Standardrichtlinien für alle Konten	Sie können CloudFormation StackSets die Amazon Data Lifecycle Manager-Standardrichtlinien für eine AWS Organisation oder für bestimmte AWS Konten verwenden.	26. April 2024
AWSDataLifecycleManagerSSMFullAccess AWS Verwaltete Richtlinie	Die Richtlinie wurde aktualisiert, um anwendungskonsistente Snapshots für SAP HANA unter Verwendung des SSM-Dokuments `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` zu unterstützen.	17. November 2023

VolumeStalledIOCheck Metrik	Mithilfe der Metrik `VolumeStalledIOCheck` können Sie überprüfen, ob ein Volume in der letzten Minute eine unterbrochene E/A-Überprüfung bestanden hat.	16. November 2023
Standardrichtlinien für Amazon Data Lifecycle Manager	Sie können jetzt Amazon Data Lifecycle Manager-Standardrichtlinien für EBS-Snapshots und EBS-backed AMIs erstellen, um alle Volumes und Instances in einer Region zu sichern.	16. November 2023
Amazon-EBS-Snapshot-Sperre	Sie können Ihre Amazon-EBS-Snapshots sperren, um sie vor versehentlichem oder böswilligem Löschen zu schützen oder um sie für eine bestimmte Dauer im WORM-Format zu speichern.	15. November 2023
Öffentlichen Zugriff auf Snapshots sperren	Sie können jetzt den öffentlichen Zugriff auf Snapshots blockieren, um zu verhindern, dass Ihre Snapshots öffentlich freigegeben werden.	9. November 2023
Vor- und Nachskripte für Amazon Data Lifecycle Manager	Sie können jetzt Vor- und Nachskripte in Ihren Snapshot-Richtlinien von Amazon Data Lifecycle Manager verwenden, um den Lebenszyklus anwendungskonsistenter Snapshots zu automatisieren.	7. November 2023

NVMe-Reservierungen	Multi-Attach aktivierte `io2` Volumes unterstützen NVMe-Reservierungen, eine Reihe von Storage-Fencing-Protokollen nach Industriestandard.	18. September 2023
Fehlertests auf Amazon EBS	Verwenden Sie diese AWS FIS Option, um vorübergehend I/O zwischen einem EBS-Volume und den Instances, an die es angeschlossen ist, zu unterbrechen, um zu testen, wie Ihre Workloads mit Unterbrechungen umgehen. I/O	27. Januar 2023
Sperrung der Aufbewahrungsregel für den Papierkorb	Sie können Aufbewahrungsregeln sperren, um sie vor versehentlichen oder böswilligen Änderungen und Löschungen zu schützen.	23. November 2022
Bedingungsschlüssel für den Papierkorb	Sie können die Bedingungsschlüssel `rbin:Request/ResourceType` und `rbin:Attribute/ResourceType` zum Filtern des Zugriffs auf Papierkorb-Anforderungen verwenden.	14. Juni 2022
`io2`-Block-Express-Volumes	Sie können die Größe und die bereitgestellten IOPS von `io2`-Block-Express-Volumes ändern und Sie können sie für eine schnelle Snapshot-Wiederherstellung aktivieren.	31. Mai 2022

Papierkorb für AMIs	Über den Papierkorb können Sie versehentlich gelöschte AMIs wiederherstellen.	3. Februar 2022
Papierkorb für Amazon-EBS-Snapshots	Der Papierkorb für Amazon-EBS-Snapshots ist ein Snapshot-Wiederherstellungsfeature, mit dem Sie versehentlich gelöschte Snapshots wiederherstellen können.	29. November 2021
Amazon EBS Snapshots Archive	Amazon EBS Snapshots Archive ist eine neue Speicherstufe, die Sie für eine kostengünstige und langfristige Speicherung Ihrer selten aufgerufenen Snapshots verwenden können.	29. November 2021
Unterstützung für AMI-Veralterung für Amazon Data Lifecycle Manager	Durch die AMI-Richtlinien von Amazon Data Lifecycle Manager können EBS-backed AMIs veraltet sein. Die AWSDataLifecycleManagerServiceRoleForAMIManagement AWS verwaltete Richtlinie wurde aktualisiert, um diese Funktion zu unterstützen.	23. August 2021
CloudWatch Metriken für Amazon Data Lifecycle Manager	Sie können Ihre Amazon Data Lifecycle Manager-Richtlinien mithilfe von Amazon überwachen CloudWatch.	28. Juli 2021

CloudTrail Datenereignisse für direkte EBS-APIs	In den PutSnapshotBlock APIs ListSnapshotBlocks ListChangedBlocks, GetSnapshotBlock, und können Datenereignisse protokolliert werden. CloudTrail	27. Juli 2021
io2-Block-Express-Volumes	io2Block Express-Volumes sind jetzt allgemein verfügbar.	19. Juli 2021
Lokale Amazon-EBS-Snapshots auf Outposts	Sie können jetzt lokale Amazon EBS-Snapshots auf Outposts verwenden, um Snapshots von Volumes Outpost lokal in Amazon S3 auf dem Computer selbst zu speichern. Outpost	4. Februar 2021
Multi-Attach Unterstützung für io2-Volumes	Sie können jetzt bereitgestellte IOPS SSD (io2) -Volumes für Amazon EBS aktivieren. Multi-Attach	18. Dezember 2020
Amazon Data Lifecycle Manager	Verwenden Sie Amazon Data Lifecycle Manager, um den Prozess der gemeinsamen Nutzung und des kontoüber greifenden Kopierens von Snapshots zu automatisieren. AWS	17. Dezember 2020
gp3-Volumes	Ein neuer Volume-Typ Amazon EBS Allzweck-SSD. Sie können bereitgestellte IOPS und einen Durchsatz angeben, wenn Sie das Volume erstellen oder ändern.	1. Dezember 2020

Volume-Größen von durchsatzoptimierten HDDs und Cold-HDDs	Throughput Optimized HDD(`st1`) und Cold HDD(`sc1`)-Volumes können in der Größe von 125 GiB bis 16 TiB reichen.	30. November 2020
Amazon Data Lifecycle Manager	Sie können Amazon Data Lifecycle Manager verwenden, um die Erstellung, Aufbewahrung und Löschung von EBS-backed AMIs zu automatisieren.	9. November 2020
Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager-Richtlinien können mit bis zu vier Zeitplänen konfiguriert werden.	17. September 2020
Bereitgestellte IOPS SSD (io2)-Volumes für Amazon EBS	Bereitgestellte IOPS-SSD-(`io2`)-Volumes sind so konzipiert, dass sie eine Volume-Haltbarkeit von 99,999 Prozent mit einem AFR von höchstens 0,001 Prozent bieten.	24. August 2020
Schnelle Snapshot-Wiederherstellung	Sie können die schnelle Snapshot-Wiederherstellung für Snapshots aktivieren, die mit Ihnen geteilt werden.	21. Juli 2020
Amazon EBS Multi-Attach	Sie können jetzt ein einzelnes Provisioned IOPS SSD (io1) -Volume an bis zu 16 Nitro-based Instances anhängen, die sich in derselben Availability Zone befinden.	14. Februar 2020

Schnelle Amazon-EBS-Snapshot-Wiederherstellungen	Sie können schnelle Snapshot-Wiederherstellungen auf einem EBS-Snapshot aktivieren, um sicherzustellen, dass die aus dem Snapshot erstellten EBS-Volumes bei der Erstellung vollständig initialisiert werden und sofort die gesamte bereitgestellte Leistung bereitstellen.	20. November 2019
Amazon-EBS-Multi-Volume-Snapshots	Sie können exakte zeitpunkt bezogene Snapshots, datenkoordinierte Snapshots und absturzkonsistente Snapshots über mehrere einer EC2-Instance angefügte EBS-Volumes hinweg erstellen.	29. Mai 2019
Standardmäßige Amazon-EBS-Verschlüsselung	Nachdem Sie die standardmäßige Verschlüsselung in einer Region aktiviert haben, werden alle neuen EBS-Volumes, die Sie in der Region erstellt haben, mit dem Standard-Verschlüsselung für die EBS-Verschlüsselung verschlüsselt.	23. Mai 2019
Automatisieren Sie den Snapshot-	Sie können mit Amazon Data Lifecycle Manager das Erstellen und Löschen von Snapshots für Ihre EBS-Volumes automatisieren.	12. Juli 2018

Nehmen Sie Änderungen an den angeschlossenen EBS-Volumes vor	Bei den meisten an EC2-Instances angefügten EBS-Volumes können Sie Volume-Größe, -Typ und -IOPS modifizieren, ohne das Volume zu trennen oder die Instance anzuhalten.	13. Februar 2017
Kopieren Sie verschlüsselte Amazon EBS-Snapshots zwischen AWS-Konten	Sie können jetzt verschlüsselte EBS-Snapshots dazwischen kopieren. AWS-Konten	21. Juni 2016
Für den Durchsatz optimierte HDD- und Cold HDD-Volumetypen	Sie können jetzt Throughput Optimized HDD(st1)- und Cold HDD(sc1)-Volumes erstellen.	19. April 2016
Allzweck-SSD-Volumetyp	Allzweck-SSD-Volumes bieten kostengünstigen Speicher, der für ein breites Spektrum an Workloads gedacht ist. Diese Volumes bieten Latenzen im einstelligen Millisekundenbereich, die Fähigkeit, über längere Zeiträume auf 3.000 IOPS zu explodieren, und bieten eine Grundleistung von 3. IOPS/GiB Universelle SSD-Volumes verfügen über Größen von 1 GiB bis 1 TiB.	16. Juni 2014

Amazon-EBS-Verschlüsselung	Amazon EBS-Verschlüsselung bietet nahtlose Verschlüsselung von EBS-Daten-Volumes und Snapshots, wodurch die Notwendigkeit entfällt, eine sichere Infrastruktur zur Schlüsselverwaltung aufzubauen und zu unterhalten. Die EBS-Verschlüsselung gewährleistet die Sicherheit gespeicherter Daten, indem Ihre Daten mithilfe von Von AWS verwaltete Schlüssel verschlüsselt werden. Die Verschlüsselung erfolgt auf den Servern, die EC2-Instances hosten, was für die Verschlüsselung von Daten sorgt, die zwischen EC2-Instances und EBS-Speicher übertragen werden.	21. Mai 2014
Inkrementelle Snapshot-Kopien	Sie können jetzt inkrementelle Snapshot-Kopien erstellen.	11. Juni 2013
EBS-Snapshot-Kopie	Sie können Snapshot-Kopien zum Erstellen von Daten-Backups, neuen Amazon EBS-Volumes oder Amazon Machine Images (AMIs) verwenden.	17. Dezember 2012

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.