



Unable to locate subtitle

AWS Snowball Edge Leitfaden für Entwickler



AWS Snowball Edge Leitfaden für Entwickler: ***Unable to locate subtitle***

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

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

Table of Contents

Was ist Snowball Edge?	1
Funktionen von Snowball Edge	1
Verwandte Dienstleistungen	2
Zugreifen auf den Snowball Edge-Dienst	3
Auf ein AWS Snowball Edge Gerät zugreifen	4
Preise für den Snowball Edge	4
AWS Überwachung von Snowball Edge	4
Ressourcen für Erstanwender AWS Snowball Edge	4
Informationen zur Gerätehardware	5
Gerätekonfigurationen	5
Gerätespezifikationen	7
Unterstützte Netzwerkhardware	11
Voraussetzungen für die Verwendung von Snowball Edge	14
Melden Sie sich an für ein AWS-Konto	15
Erstellen eines Benutzers mit Administratorzugriff	16
Über deine Umgebung	17
Mit Sonderzeichen arbeiten	18
Amazon S3 S3-Verschlüsselung mit AWS KMS	19
Amazon S3 S3-Verschlüsselung mit serverseitiger Verschlüsselung	24
Voraussetzungen für die Verwendung des Amazon S3 S3-Adapters auf Snowball Edge für Import- und Exportaufträge	24
Voraussetzungen für die Verwendung von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge	25
Voraussetzungen für die Verwendung von Compute-Instanzen auf Snowball Edge	26
So funktioniert Snowball Edge	28
Wie funktionieren Importaufträge	30
Wie funktionieren Exportaufträge	31
Wie funktionieren lokale Rechen- und Speicherjobs	32
So funktionieren geclusterte lokale Rechen- und Speicherjobs	32
Videos und Blogs zu Snowball Edge	33
Langfristige Preisgestaltung für Snowball Edge-Geräte	35
Austausch von Geräten während des langfristigen Preiszeitraums	36
Überlegungen zum Versand	37
Regionale Versandbeschränkungen	37

Erste Schritte	39
Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen	40
Wählen Sie einen Jobtyp	41
Wählen Sie Ihre Rechen- und Speicheroptionen	42
Wählen Sie Ihre Funktionen und Optionen	46
Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen	47
Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job	51
Einen Job stornieren	51
Einen Job klonen, um einen Snowball Edge zu bestellen	52
Erhalt des Snowball Edge	53
Stellen Sie eine Verbindung zu Ihrem lokalen Netzwerk her	55
Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen	57
Den Snowball Edge freischalten	58
Problembehebung beim Entsperren eines Snowball Edge	61
Lokale Benutzer einrichten	62
Das Snowball Edge-Gerät neu starten	64
Snowball Edge ausschalten	68
Rückgabe des Geräts	72
Rückversand	73
Spediteure	73
Überwachung des Importstatus	83
Erhalten Sie einen Bericht und Protokolle zum Abschluss des Auftrags	84
Migration großer Datenmengen	87
Planen Sie Ihren großen Transfer	87
Schritt 1: Verstehen Sie, was Sie in die Cloud verlagern	88
Schritt 2: Berechnen Sie Ihre Zielübertragungsrate	88
Schritt 3: Ermitteln Sie, wie viele Snowball Edge Sie benötigen	89
Schritt 4: Erstellen Sie Ihre Jobs	89
Schritt 5: Teilen Sie Ihre Daten in Übertragungssegmente auf	89
Kalibrieren einer großen Datenübertragung	90
Erstellung eines Migrationsplans für große Datenmengen	91
Schritt 1: Wählen Sie Ihre Migrationsdetails	92
Schritt 2: Wählen Sie Ihre Versand-, Sicherheits- und Benachrichtigungseinstellungen	98
Schritt 3: Überprüfen und erstellen Sie Ihren Plan	98
Verwenden des Migrationsplans für große Datenmengen	99
Empfohlener Zeitplan für die Auftragsbestellung	99

Liste der bestellten Jobs	101
Dashboard zur Überwachung	102
AWS OpsHub Zur Verwaltung von Geräten verwenden	103
Wird heruntergeladen AWS OpsHub	104
Ein Gerät entsperren	104
Lokales Entsperren eines Geräts	105
Ein Gerät aus der Ferne entsperren	108
Überprüfung der Signatur von AWS OpsHub	111
Dienste verwalten AWS	115
Starten einer EC2 Amazon-kompatiblen Instance	116
Stoppen einer Amazon EC2 -kompatiblen Instance	120
Starten einer EC2 Amazon-kompatiblen Instance	120
Arbeiten mit Schlüsselpaaren	121
Beenden einer EC2 Amazon-kompatiblen Instance	121
Verwaltung von EBS-Volumes	123
Ein Bild als EC2 Amazon-kompatibles AMI auf Ihr Gerät importieren	125
Löschen eines Snapshots	129
Ein AMI abmelden	130
Verwalten von -Clustern	131
Richten Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ein mit AWS OpsHub	132
Verwaltung von S3-Speicher	139
Verwaltung der NFS-Schnittstelle	143
Das Gerät neu starten	152
Profile verwalten mit AWS OpsHub	155
Gerät herunterfahren	155
Den Gerätealias bearbeiten	158
Verwaltung von Public-Key-Zertifikaten mit OpsHub	158
Laden Sie das Public-Key-Zertifikat herunter mit OpsHub	159
Erneuerung des Public-Key-Zertifikats mit OpsHub	159
Geräte-Updates erhalten	160
Aktualisierung AWS OpsHub	161
Automatisieren Sie Ihre Verwaltungsaufgaben mit AWS OpsHub	162
Eine Aufgabe erstellen und starten	162
Details einer Aufgabe anzeigen	166
Eine Aufgabe löschen	166

Einstellung der NTP-Zeitserver für das Gerät	166
Konfiguration und Verwendung des Snowball Edge-Clients	169
Den Snowball Edge-Client herunterladen und installieren	169
Konfiguration eines Profils für den Snowball Edge-Client	171
Snowball Edge-Clientversion finden	174
Abrufen von Anmeldeinformationen	175
Einen Dienst auf einem Snowball Edge starten	176
Beenden eines Dienstes auf einem Snowball Edge	176
Protokolle anzeigen und herunterladen	177
Gerätestatus anzeigen	179
Status von Diensten anzeigen	180
Status von Funktionen anzeigen	186
Zeitserver einrichten	186
Zeitquellen werden überprüft	187
Zeitserver werden aktualisiert	188
Validierung von NFC-Tags	189
Die MTU-Größe wird aktualisiert	189
Übertragung von Dateien mit dem S3-Adapter	191
Herunterladen und Installieren von AWS CLI	192
Installieren Sie das AWS CLI auf Linux-Betriebssystemen	192
Installieren Sie das AWS CLI auf Windows-Betriebssystemen	193
Verwenden der API-Operationen AWS CLI und auf Snowball Edge-Geräten	193
Autorisierung mit der Amazon S3 S3-API-Schnittstelle für AWS Snowball Edge	193
Lokale Amazon S3 S3-Anmeldeinformationen abrufen und verwenden	194
Konfiguration des S3-Adapters als Endpunkt AWS CLI	195
Nicht unterstützte Amazon S3 S3-Funktionen für den S3-Adapter	196
Kleine Dateien stapeln	197
Unterstützte AWS CLI Befehle für die Datenübertragung	199
Unterstützte AWS CLI Befehle für Amazon S3	200
Unterstützte Amazon S3 S3-REST-API-Aktionen für die Datenübertragung	204
Verwaltung der NFS-Schnittstelle	207
NFS-Konfiguration für Snowball Edge	208
Snowball Edge für die NFS-Schnittstelle konfigurieren	209
Den NFS-Dienst auf dem Snowball Edge starten	210
Mounten von NFS-Endpunkten auf Client-Computern	212
Stoppen der NFS-Schnittstelle	213

Verwenden von EC2 Amazon-kompatiblen Recheninstanzen	214
Erläuterung Amazon EC2 Amazon-kompatiblen Instances	215
Preisgestaltung für Instanzen EC2	216
Verwendung AMIs auf Snowball Edge	216
Hinzufügen eines AMI bei der Bestellung	218
Hinzufügen eines AMI von AWS Marketplace	219
Hinzufügen eines AMI nach Erhalt des Geräts	223
Hinzufügen eines Microsoft Windows-AMI zu einem Snowball Edge	224
Importieren eines VM-Images in einen Snowball Edge	226
Exportieren des neuesten Amazon Linux 2-AMI für einen Snowball Edge	226
Importieren eines VM-Images auf ein Snowball Edge-Gerät	227
Schritt 1: Bereiten Sie das VM-Image vor und laden Sie es auf das Snowball Edge-Gerät hoch	228
Schritt 2: Richten Sie die erforderlichen Berechtigungen auf dem Snowball Edge ein	230
Schritt 3: Importieren Sie das VM-Image als Snapshot auf Snowball Edge	236
Schritt 4: Registrieren Sie den Snapshot als AMI auf dem Snowball Edge	238
Schritt 5: Starten Sie eine Instance über das AMI auf dem Snowball Edge	239
Zusätzliche AMI-Aktionen für einen Snowball Edge	240
Verwendung der AWS CLI und API-Operationen	244
Netzwerkkonfigurationen für Recheninstanzen	245
DNI- und VNI-Voraussetzungen	246
Einrichtung einer virtuellen Netzwerkschnittstelle (VNI)	247
Ein DNI einrichten	248
SSH verwenden, um eine Verbindung zu einer Recheninstanz herzustellen	252
Übertragung von Daten von Recheninstanzen in Buckets auf demselben Gerät	253
Automatisches Starten von Instanzen	253
Erstellen einer EC2 -kompatiblen Startkonfiguration	254
Aktualisierung einer EC2 -kompatiblen Startkonfiguration	254
Löschen einer EC2 -kompatiblen Startkonfiguration	255
Listing-kompatible Startkonfigurationen EC2	255
Erstellen einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge	255
Beschreibung Ihrer virtuellen Netzwerkschnittstellen	256
Aktualisieren einer virtuellen Netzwerkschnittstelle	258
Löschen einer virtuellen Netzwerkschnittstelle	258
Verwenden des EC2 Amazon-kompatiblen Endpunkts	259
Den EC2 -kompatiblen Endpunkt als Endpunkt angeben AWS CLI	259

Unterstützte EC2 -kompatible Befehle AWS CLI	260
Unterstützte EC2 Amazon-kompatible API-Operationen	277
Automatisches Starten von -kompatiblen Instanzen EC2	280
Verwenden von IMDS for Snow mit -kompatiblen Instances EC2	282
IMDS-Versionen auf einem Snowball Edge	283
Beispiele für das Abrufen von Instanz-Metadaten mit und IMDSv1 IMDSv2	287
Blockspeicher mit -kompatiblen Instances EC2 verwenden	292
Steuern des Netzwerkverkehrs mit Sicherheitsgruppen	293
Unterstützt EC2 — kompatible Instanzmetadaten und Benutzerdaten	294
Benutzerdaten der Computerinstanz	295
Stoppen EC2 von -kompatiblen Instanzen	296
Verwendung auf -kompatiblen Instances AWS IoT Greengrass EC2	297
Einrichtung von -compatible für EC2 AWS IoT Greengrass	297
Installation AWS IoT Greengrass auf einer EC2 -kompatiblen Instanz auf einem Snowball Edge	298
Benutzen AWS Lambda	301
Erste Schritte mit Lambda	301
Voraussetzungen für AWS IoT Greengrass	301
Voraussetzungen für Lambda	302
Stellen Sie eine Lambda-Funktion auf einem Snowball Edge-Gerät bereit	303
Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge	305
Amazon S3 S3-kompatiblen Speicher auf Snowball Edge bestellen	308
Amazon S3 S3-kompatiblen Speicher auf Snowball Edge einrichten und starten	309
Voraussetzungen	309
Richten Sie Ihre lokale Umgebung ein	309
Starten des Amazon S3 S3-kompatiblen Speichers auf dem Snowball Edge-Service	311
Informationen zu Endpunkten anzeigen	313
Arbeiten mit S3-Buckets	315
Verwenden des AWS CLI	316
Verwenden des Java-SDK	317
Bucket-ARN-Format	317
Format des Bucket-Speicherorts	318
Ermitteln des Bucket-Zugriffs	318
Eine Liste von Buckets oder regionalen Buckets wird abgerufen	318
Abrufen eines Buckets	320
Erstellen eines S3-Buckets	321

Löschen eines Buckets	322
Erstellen und Verwalten einer Objektlebenszykluskonfiguration mit dem AWS CLI	323
PUT eine Lebenszykluskonfiguration auf einen Snowball Edge-Bucket	323
Kopieren eines Objekts	325
Auflisten von Objekten	326
Abrufen eines Objekts	328
Löschen von Objekten	330
Unterstützte REST-API-Aktionen für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge	332
Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit einem Cluster von Snow-Geräten	333
Snowball Edge-Cluster-Quoren	336
Einen nicht verfügbaren Clusterknoten erneut verbinden	337
Einen Knoten in einem Cluster ersetzen	338
Konfiguration von Amazon S3 S3-kompatiblen Speicher für Snowball Edge-Ereignisbenachrichtigungen	351
Konfiguration lokaler SMTP-Benachrichtigungen	354
Snowball Edge für lokale Benachrichtigungen konfigurieren	354
Verwenden von Amazon EKS Anywhere auf Snowball Edge	356
Vor der Bestellung eines Snowball Edge-Geräts für Amazon EKS Anywhere on AWS Snow auszuführende Aktionen	358
Erstellen Sie ein Ubuntu EKS Distro AMI	359
Baue ein Harbor-AMI	359
Bestellung eines Snowball Edge-Geräts zur Verwendung mit Amazon EKS Anywhere on AWS Snow	359
Konfiguration und Ausführung von Amazon EKS Anywhere auf Snowball Edge-Geräten	360
Erstes Einrichten	361
Automatisches Konfigurieren und Ausführen von Amazon EKS Anywhere	361
Manuelles Konfigurieren und Ausführen von Amazon EKS Anywhere	362
Konfiguration von Amazon EKS Anywhere on AWS Snow für den Betrieb ohne Internetverbindung	372
Konfigurieren Sie die Harbor-Registrierung auf einem Snowball Edge-Gerät	372
Verwenden Sie die Harbor-Registrierung auf der Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge	372
Cluster erstellen und verwalten	372
Bewährte Methoden für die Erstellung von Clustern auf einem Snowball Edge	372

Aktualisieren von Clustern auf einem Snowball Edge	373
Bereinigen von Clusterressourcen auf einem Snowball Edge	373
Lokales Verwenden von IAM	374
Verwendung der AWS CLI und API-Operationen	375
Unterstützte IAM-Befehle AWS CLI	375
Unterstützte IAM-API-Operationen auf Snowball Edge	377
Unterstützte IAM-Richtlinienversion und Grammatik auf Snowball Edge	379
Beispiele für IAM-Richtlinien auf Snowball Edge	380
Zulassen des GetUser Aufrufs für einen Beispielbenutzer auf einem Snowball Edge über die IAM-API	380
Vollzugriff auf die Amazon S3 S3-API auf einem Snowball Edge zulassen	380
Lese- und Schreibzugriff auf einen Amazon S3 S3-Bucket auf einem Snowball Edge zulassen	381
.....	382
Zulassen des Auflisten-, Abruf- und Platzzugriffs auf einen Amazon S3 S3-Bucket auf einem Snowball Edge	382
Vollzugriff auf die EC2 Amazon-API auf einem Snowball Edge zulassen	382
Zulassen des Zugriffs zum Starten und Beenden von EC2 Amazon-kompatiblen Instances auf einem Snowball Edge	383
Anrufe an einen Snowball Edge ablehnen, DescribeLaunchTemplates DescribeImages aber alle Anrufe zulassen	383
Richtlinie für API-Aufrufe auf einem Snowball Edge	384
TrustPolicy Beispiel auf einem Snowball Edge	385
Benutzen AWS STS	386
Verwenden der API-Operationen AWS CLI und auf einem Snowball Edge	386
Unterstützte AWS STSAWS CLI Befehle auf einem Snowball Edge	387
Beispielbefehl zum Übernehmen einer Rolle auf einem Snowball Edge	387
Unterstützte AWS STS API-Operationen auf einem Snowball Edge	387
Verwaltung von Public-Key-Zertifikaten	389
Das Zertifikat auflisten	389
Zertifikate erhalten	390
Löschen von Zertifikaten	391
Portanforderungen für Dienste AWS	392
Geräte mit Snowball Edge Device Management verwalten	394
Auswahl des Snowball Edge-Geräteverwaltungsstatus bei der Bestellung eines Snowball Edge	395

Aktivieren der Snowball Edge-Geräteverwaltung auf einem Snowball Edge	396
Hinzufügen von Berechtigungen für Snowball Edge Device Management zu einer IAM-Rolle auf einem Snowball Edge	397
CLI-Befehle für die Snowball Edge-Geräteverwaltung	398
Eine Snowball Edge-Geräteverwaltungsaufgabe erstellen	399
Überprüfen des Status einer Snowball Edge-Geräteverwaltungsaufgabe	400
Überprüfen von Geräteinformationen mit Snowball Edge Device Management	401
Status EC2 kompatibler Instanzen mit Snowball Edge Device Management überprüfen	402
Metadaten der Snowball Edge-Geräteverwaltungsaufgabe anzeigen	404
Abbrechen einer Snowball Edge-Geräteverwaltungsaufgabe	405
Befehle und Syntax der Snowball Edge-Geräteverwaltung auflisten	406
Snowball Edge auflisten, die für die Fernverwaltung verfügbar sind	407
Geräteübergreifendes Auflisten des Status von Aufgaben	408
Verfügbare Ressourcen auf Geräten auflisten	409
Geräte- oder Aufgaben-Tags auflisten	410
Aufgaben nach Status auflisten	411
Anwenden von Tags auf Aufgaben oder Geräte	412
Entfernen von Tags aus Aufgaben oder Geräten	413
Snowball Edge-Geräte aktualisieren	414
Voraussetzungen für die Aktualisierung von Software	415
Updates werden heruntergeladen	416
Updates werden installiert	419
Aktualisierung des SSL-Zertifikats	426
Aktualisieren Sie Ihr Amazon Linux 2 AMIs	427
Jobs verstehen	429
Angaben zum Job	430
Auftragsstatus	433
Status von Snowball Edge-Cluster-Jobs	436
Importaufträge	437
Exportaufträge	438
Verwenden von Amazon S3 S3-Objektschlüsseln mit Exportaufträgen	439
Bewährte Methoden für Exportaufträge	448
Informationen zu lokalen Rechen- und Speicheraufträgen	448
Informationen zu lokalen Speicheraufträgen	449
Informationen zum lokalen Speicher auf einem Gerätecluster	449
Bewährte Methoden	450

Sicherheitsempfehlungen	450
Bewährte Methoden für das Ressourcenmanagement	451
Empfehlungen zur Leistung der Datenübertragung	452
Verbesserung der Datenübertragungsgeschwindigkeit	453
Sicherheit	455
Datenschutz	456
Schützen von Daten in der Cloud	457
Schützen von Daten auf Ihrem Gerät	461
Identitäts- und Zugriffsverwaltung	464
Zugriffskontrolle für Konsole und Aufgaben	465
Protokollieren und Überwachen	509
Compliance-Validierung	510
Ausfallsicherheit	511
Sicherheit der Infrastruktur	511
Datenvalidierung	513
Lokaler Dateibestand	513
Häufige Ursachen für Datenvalidierungsfehler mit Snowball Edge	514
Manuelles Überprüfen von Daten nach dem Import in Amazon S3	514
Benachrichtigungen	516
So verwendet Snow Amazon SNS	516
Verschlüsselung von SNS-Themen bei Änderungen des Jobstatus	516
Einrichtung einer vom Kunden verwalteten KMS-Schlüsselrichtlinie	517
Beispiele für SNS-Benachrichtigungen	519
Protokollierung mit AWS CloudTrail	541
AWS Snowball Edge Informationen in CloudTrail	541
Grundlagen zu -Protokolldateieinträgen	542
Kontingente	544
Verfügbarkeit in der Region für AWS Snowball Edge	544
Einschränkungen für Jobs AWS Snowball Edge	545
Ratenbegrenzungen für AWS Snowball Edge	546
Verbindungslimit für Amazon Snow S3 Adapter	546
Einschränkungen bei der Übertragung von Daten vor Ort	546
Kontingente für Recheninstanzen	547
Ressourcenspeicherkontingente auf Snowball Edge berechnen	547
Einschränkungen gemeinsam genutzter Rechenressourcen auf Snowball Edge	549
Einschränkungen beim Versand	550

Einschränkungen bei der Verarbeitung zurückgesendeter Geräte für Importaufträge	551
Fehlerbehebung	552
Identifizieren Sie ein Gerät	554
Behebung von Startproblemen	554
Behebung von Problemen mit dem LCD-Display während des Startvorgangs	555
Behebung von Problemen mit dem E-Ink-Display beim Systemstart	557
Behebung von Verbindungsproblemen	557
Behebung von unlock-device Befehlsproblemen	558
Behebung von Problemen mit Manifestdateien	559
Behebung von Problemen mit Anmeldeinformationen	559
Fehlerbehebung: Anmeldeinformationen konnten nicht gefunden AWS CLI werden	559
Fehlerbehebung bei der Fehlermeldung: Überprüfen Sie Ihren geheimen Zugriffsschlüssel und Ihre Signatur	560
Behebung von Datenübertragungsproblemen	560
Behebung von Problemen mit Importaufträgen	561
Behebung von Problemen mit Exportaufträgen	561
Behebung von Problemen mit der NFS-Schnittstelle	562
Fehler „Zugriff verweigert“ über die S3-Schnittstelle	564
403 unzulässiger Fehler von der S3-Schnittstelle	567
Behebung von Problemen AWS CLI	571
Fehlerbehebung bei der AWS CLI Fehlermeldung: „Das Profil kann nicht Null sein“	571
Behebung eines Nullzeigerfehlers bei der Übertragung von Daten mit dem AWS CLI	572
Fehlerbehebung bei Recheninstanzen	572
Virtuelle Netzwerkschnittstelle hat die IP-Adresse 0.0.0.0	573
Das Snowball Edge-Gerät reagiert nicht mehr, wenn eine große Recheninstanz gestartet wird	573
Meine Instanz auf dem Snowball Edge hat ein Root-Volume	573
Fehler in der ungeschützten privaten Schlüsseldatei	574
Dokumentverlauf	575
.....	dlxxxiii

Was ist Snowball Edge?

Snowball Edge ist ein Gerät mit integriertem Speicher und Rechenleistung für ausgewählte AWS Funktionen. Snowball Edge kann Daten lokal verarbeiten, Edge-Computing-Workloads ausführen und Daten an oder von der übertragen. AWS Cloud

Jedes Snowball Edge-Gerät kann Daten schneller als das Internet übertragen. Die Geräte mit den Daten werden durch einen regionalen Kurierdienst transportiert. Die Geräte sind robust und mit E-Ink-Versandetiketten versehen.

Snowball Edge-Geräte bieten zwei Optionen für Gerätekonfigurationen: Speicheroptimiert mit 210 TB und Compute Optimized. Wenn sich dieses Handbuch auf Snowball Edge-Geräte bezieht, bezieht es sich auf alle Optionen des Geräts. Wenn spezifische Informationen nur für eine oder mehrere optionale Gerätekonfigurationen gelten, wird ausdrücklich darauf hingewiesen. Weitere Informationen finden Sie unter [Snowball Edge-Gerätekonfigurationen](#).

Themen

- [Funktionen von Snowball Edge](#)
- [Dienstleistungen im Zusammenhang mit Snowball Edge](#)
- [Zugreifen auf den Snowball Edge-Dienst](#)
- [Preise für den Snowball Edge](#)
- [AWS Überwachung von Snowball Edge](#)
- [Ressourcen für Erstanwender AWS Snowball Edge](#)
- [AWS Snowball Edge Informationen zur Gerätehardware](#)
- [Voraussetzungen für die Verwendung von Snowball Edge](#)

Funktionen von Snowball Edge

Snowball Edge-Geräte verfügen über die folgenden Funktionen:

- Große Mengen an Speicherkapazität oder Rechenfunktionen für Geräte. Das hängt von den Optionen ab, die Sie bei der Erstellung Ihres Jobs wählen.
- Netzwerkadapter mit Übertragungsgeschwindigkeiten von bis zu 100 Gbit/s.
- Die Verschlüsselung wird erzwungen, sodass Ihre Daten im Ruhezustand und bei der Übertragung geschützt sind.

- Sie können Daten zwischen Ihren lokalen Umgebungen und Amazon S3 importieren oder exportieren und die Daten physisch mit einem oder mehreren Geräten transportieren, ohne das Internet zu verwenden.
- Snowball Edge-Geräte sind ihre eigene robuste Box. Das integrierte E-Ink-Display ändert sich und zeigt nun Ihr Versandetikett an, wenn das Gerät versandbereit ist.
- Snowball Edge-Geräte verfügen über ein integriertes LCD-Display, das zur Verwaltung von Netzwerkverbindungen und zum Abrufen von Dienststatusinformationen verwendet werden kann.
- Sie können Snowball Edge-Geräte für lokale Speicher- und Rechenaufträge clustern, um Datenbeständigkeit auf 3 bis 16 Geräten zu erreichen und den Speicher bei Bedarf lokal zu vergrößern oder zu verkleinern.
- Sie können Amazon EKS Anywhere auf Snowball Edge-Geräten für Kubernetes-Workloads verwenden.
- Snowball Edge-Geräte verfügen über Amazon S3- und EC2 Amazon-kompatible Endpunkte, die programmatische Anwendungsfälle ermöglichen.
- Snowball Edge-Geräte unterstützen die neuen sbe-g Instance-Typen sbe1sbe-c, und, mit denen Sie Compute-Instances auf dem Gerät mithilfe von Amazon Machine Images (AMIs) ausführen können.
- Snowball Edge unterstützt die folgenden Datenübertragungsprotokolle für die Datenmigration:
 - NFSv3
 - NFSv4
 - NFSv4.1.
 - Amazon S3 über HTTP oder HTTPS (über eine API, die mit AWS CLI Version 1.16.14 und früher kompatibel ist)

Dienstleistungen im Zusammenhang mit Snowball Edge

Sie können ein AWS Snowball Edge Gerät mit den folgenden zugehörigen AWS Diensten verwenden:

- Amazon S3 S3-Adapter — Wird für die programmatische Datenübertragung in und aus der Amazon S3 S3-API für Snowball Edge AWS verwendet, die eine Teilmenge der Amazon S3 S3-API-Operationen unterstützt. In dieser Rolle werden Daten in Ihrem Namen AWS auf das Snow-Gerät übertragen und das Gerät wird an Sie versendet (für einen Exportauftrag), oder AWS es wird

Ihnen ein leeres Snow-Gerät gesendet und Sie übertragen Daten von Ihren lokalen Quellen auf das Gerät und senden es zurück an AWS (für einen Importauftrag).

- Amazon S3 S3-kompatibler Speicher auf Snowball Edge — Wird verwendet, um die Datenanforderungen von Rechendiensten wie Amazon EC2, Amazon EKS Anywhere on Snow und anderen zu unterstützen. Diese Funktion ist auf Snowball Edge-Geräten verfügbar und bietet ein erweitertes Amazon S3 S3-API-Set sowie Funktionen wie erhöhte Ausfallsicherheit mit flexiblem Cluster-Setup für 3 bis 16 Knoten, lokales Bucket-Verwaltung und lokale Benachrichtigungen.
- Amazon EC2 — Führen Sie Compute-Instances auf einem Snowball Edge-Gerät mithilfe des EC2 Amazon-kompatiblen Endpunkts aus, der eine Teilmenge der EC2 Amazon-API-Operationen unterstützt. Weitere Informationen zur Verwendung von Amazon EC2 in AWS finden Sie unter [Erste Schritte mit Amazon EC2 Linux-Instances](#).
- Amazon EKS Anywhere on Snow — Erstellen und betreiben Sie Kubernetes-Cluster auf Snowball Edge-Geräten. Siehe [Verwenden von Amazon EKS Anywhere auf AWS Schnee](#).
- AWS Lambda powered by AWS IoT Greengrass — Rufen Sie Lambda-Funktionen auf, die auf Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Speicheraktionen basieren, die auf einem Gerät ausgeführt wurden. AWS Snowball Edge Weitere Informationen zur Verwendung von Lambda finden Sie unter [Verwendung AWS Lambda mit einem AWS Snowball Edge](#) und im [AWS Lambda Developer Guide](#).
- Amazon Elastic Block Store (Amazon EBS) — Stellt Speichervolumes auf Blockebene zur Verwendung mit EC2 -kompatiblen Instances bereit. Weitere Informationen finden Sie unter [Amazon Elastic Block Store \(Amazon EBS\)](#).
- AWS Identity and Access Management (IAM) — Verwenden Sie diesen Service, um den Zugriff auf Ressourcen sicher zu kontrollieren. AWS Weitere Informationen finden Sie unter [Was ist IAM?](#)
- AWS -Security-Token-Service (AWS STS) — Fordern Sie temporäre Anmeldeinformationen mit eingeschränkten Rechten für IAM-Benutzer oder für Benutzer an, die Sie authentifizieren (Verbundbenutzer). Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).
- Amazon EC2 Systems Manager — Verwenden Sie diesen Service, um Ihre Infrastruktur einzusehen und zu steuern AWS. Weitere Informationen finden Sie unter [Was ist AWS Systems Manager?](#)

Zugreifen auf den Snowball Edge-Dienst

Sie können die [Managementkonsole für die AWS Snow-Familie](#) oder die Job-Management-API verwenden, um Jobs zu erstellen und zu verwalten. Weitere Informationen zur Verwendung der

[Managementkonsole für die AWS Snow-Familie](#) finden Sie unter [Erste Schritte mit Snowball Edge](#). Informationen zur Job-Management-API finden Sie unter [Job Management API-Referenz für Snowball Edge](#).

Auf ein AWS Snowball Edge Gerät zugreifen

Nachdem Ihr Snowball Edge-Gerät vor Ort ist, können Sie es über den LCD-Bildschirm mit einer IP-Adresse konfigurieren und dann das Gerät mit dem Snowball Edge-Client entsperren oder. AWS OpsHub Anschließend können Sie Datenübertragungs- oder Edge-Computing-Aufgaben ausführen. Weitere Informationen finden Sie unter [Snowball Edge erhalten](#).

Preise für den Snowball Edge

Informationen zu den Preisen und Gebühren im Zusammenhang mit dem Dienst und seinen Geräten finden Sie unter [AWS Snowball Edge Preise](#).

AWS Überwachung von Snowball Edge

AWS überwacht das Snow-Gerät und kann Messwerte und Nutzungsinformationen sammeln, wenn das Snow-Gerät mit einem verbunden ist AWS-Region. Wenn das Snow-Gerät nicht an das angeschlossen ist AWS-Region, AWS wird das Snow-Gerät nicht überwacht.

Wenn AWS ein irreparables Problem festgestellt wird und die physische Ausrüstung ausgetauscht werden muss, AWS werden Sie darüber informiert. Sie können dann einen Ersatzauftrag vergeben, den wir an Ihren Standort versenden. Dafür fallen keine zusätzlichen Kosten an, da die Überwachung von Snow-Geräten in der Servicegebühr für Snow-Geräte enthalten ist.

Ressourcen für Erstanwender AWS Snowball Edge

Wenn Sie den AWS Snowball Edge-Dienst zum ersten Mal verwenden, empfehlen wir Ihnen, die folgenden Abschnitte der Reihe nach zu lesen:

1. Informationen zu Gerätetypen und Optionen finden Sie unter. [AWS Snowball Edge Informationen zur Gerätehardware](#)
2. Weitere Informationen zu den Arten von Aufträgen finden Sie unter [Snowball Edge-Jobs verstehen](#).
3. Eine end-to-end Übersicht über die Verwendung eines AWS Snowball Edge Geräts finden Sie unter [Wie AWS Snowball Edge funktioniert](#).

4. Wenn Sie bereit sind, sehen Sie sich [Erste Schritte mit Snowball Edge](#) an.
5. Informationen zur Verwendung von Datenverarbeitungs-Instances auf einem Gerät finden Sie unter [Verwenden von EC2 Amazon-kompatiblen Compute-Instances auf Snowball Edge](#).

AWS Snowball Edge Informationen zur Gerätehardware

Alle Snowball Edge-Geräte haben dieselben physikalischen Eigenschaften wie Größe und Gewicht, enthalten jedoch je nach Verwendungszweck unterschiedliche Hardwaretypen. Geräte, die für die Datenübertragung konzipiert sind, sind mit mehr Speicherplatz konfiguriert, und Geräte, die für die Datenverarbeitung konzipiert sind, sind mit mehr virtuellem Speicher CPUs und mehr Arbeitsspeicher konfiguriert. Dieser Abschnitt enthält Informationen zu den physikalischen Eigenschaften von Snowball Edge-Geräten sowie zu ihren Rechen- und Speicherspezifikationen.

Themen

- [Snowball Edge-Gerätekonfigurationen](#)
- [AWS Snowball Edge Gerätespezifikationen](#)
- [Von Snowball Edge unterstützte Netzwerkhardware](#)

Snowball Edge-Gerätekonfigurationen

Snowball Edge-Geräte bieten die folgenden Optionen für Gerätekonfigurationen:

- Speicheroptimierte 210 TB für Snowball Edge — Diese Snowball Edge-Geräteoption verfügt über 210 TB nutzbare Speicherkapazität.
- Rechenoptimiert für Snowball Edge — Dieses Snowball Edge-Gerät (mit AMD EPYC Gen2) bietet mit bis zu 104 VCPUs, 416 GB Arbeitsspeicher und 28 TB dedizierter SSD für Recheninstanzen die meisten Rechenfunktionen. NVMe

Note

Wenn Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf diesen Geräten verwenden, variiert der nutzbare Speicherplatz. Informationen zur Speicherkapazität [mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#) finden Sie unter Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge.

Weitere Informationen über die Datenverarbeitungsfunktionalität dieser drei Optionen finden Sie unter [Verwenden von EC2 Amazon-kompatiblen Compute-Instances auf Snowball Edge](#). [Die Unterschiede bei der Erstellung von Job und der Festplattenkapazität in Terabyte werden hier beschrieben.](#)

Note

Wenn wir uns auf Snowball Edge-Geräte beziehen, umfasst dies alle optionalen Varianten des Geräts. Wenn sich Informationen auf eine oder mehrere spezifische optionale Konfigurationen beziehen, erwähnen wir dies ausdrücklich.

In der folgenden Tabelle werden die Unterschiede zwischen den verschiedenen Geräteoptionen zusammengefasst. Informationen zu Hardwarespezifikationen finden Sie unter [AWS Snowball Edge Gerätespezifikationen](#).

	Snowball Edge, speicheroptimiert, 210 TB	Snowball Edge rechneroptimiert mit AMD EPYC Gen2 und NVME
CPU	AMD Rom, 64 Kerne, 2 GHz	AMD Rom, 64 Kerne, 2 GHz
v CPUs	104	104
Verwendbarer Speicher	416 GB	416 GB
Sicherheitskarte	Ja	Ja
SSD	210 TB NVMe	28 TB NVMe
Verwendbare Festplatte	Nicht zutreffend	Nicht zutreffend
Netzwerkschnittstellen	• 2x 10 Gbit — RJ45 (eines nutzbar) • 1 x 25 Gbit — SFP28 • 1 x 100 Gbit — QSFP28	• 2x 10 Gbit — RJ45 (eines nutzbar) • 1 x 25 Gbit — SFP28 • 1 x 100 Gbit — QSFP28
Physische Sicherheitsfunktionen	• Versteckte Magnetschlösser • Eindringungsschalter	• Versteckte Magnetschlösser • Eindringungsschalter

	Snowball Edge, speicheroptimiert, 210 TB	Snowball Edge rechneroptimiert mit AMD EPYC Gen2 und NVME
	• NFC-Tags • Antimanipulationseinsätze • Android-App zur Erkennung von Manipulationen • Konforme Beschichtung	• NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • Konforme Beschichtung

AWS Snowball Edge Gerätespezifikationen

In diesem Abschnitt finden Sie Spezifikationen für AWS Snowball Edge Gerätetypen und Hardware.

Themen

- [Snowball Edge-Spezifikationen für speicheroptimierte 210 TB](#)
- [Snowball Edge Compute Optimized Gerätespezifikationen](#)

Snowball Edge-Spezifikationen für speicheroptimierte 210 TB

Die folgende Tabelle enthält Hardwarespezifikationen für Snowball Edge-Geräte mit einer Speicheroptimierung von 210 TB.

Item	Snowball Edge-Spezifikationen für speicheroptimierte 210 TB
Rechen- und Speicherspezifikationen	
CPU	104 v CPUs
RAM	416 GB
Speicherspezifikationen	

Item	Snowball Edge-Spezifikationen für speicheroptimierte 210 TB
NVME-Speicherkapazität	210 TB nutzbar (für Objekt- und NFS-Datenübertragung)
SSD-Speicherkapazität	Keine
Technische Daten der Stromversorgung	
Stromversorgung	AWS-Regionen In den USA: NEMA 5—15p 100—220 Volt. In allen Regionen ist ein Stromkabel im Lieferumfang enthalten AWS
Stromverbrauch	304 Watt für einen durchschnittlichen Anwendungsfall, obwohl das Netzteil für 1200 Watt ausgelegt ist
Spannung	100 – 240 V AC
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit — RJ45 (eines nutzbar) 1 x 25 Gbit — SFP28 1 x 100 Gbit — QSFP28
Kabel	Jedes AWS Snowball Edge Gerät wird mit landesspezifischen Stromkabeln geliefert. Es werden keine weiteren Kabel oder optischen Stecker mitgeliefert. Weitere Informationen finden Sie unter Von Snowball Edge unterstützte Netzwerkhardware .
Thermische Anforderungen	AWS Snowball Edge Geräte sind für den Bürobetrieb konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät einen Ton von 68 Dezibel und ist damit in der Regel leiser als ein Staubsauger oder Musik im Wohnzimmer.

Item	Snowball Edge-Spezifikationen für speicheroptimierte 210 TB
Abmessungen und Gewichtsangaben	
Gewicht	22,54 Kilogramm
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Spezifikationen für die Umgebung	
Vibration	Einsatz bei Nichtbetrieb entspricht ASTM D4169 Lkw Level I 0,73 GRMS
Schock	Betriebsgebrauch entspricht 70G (MIL-S-901) Nichtbetrieblicher Einsatz entspricht 50 G (ISTA-3A)
Höhe	Betriebsnutzung entspricht 0—3.000 Metern (0—10.000 Fuß) Nutzung bei Nichtbetrieb entspricht 0—12.000 Metern
Temperaturbereich	0—30 °C (betriebsbereit)

Snowball Edge Compute Optimized Gerätespezifikationen

Item	Technische Daten für Snowball Edge Compute Optimized
Rechen- und Speicherspezifikationen	
CPU	104 v CPUs
RAM	512 GB RAM (Bis zu 416 GB RAM — vom Kunden nutzbar)
Speicherspezifikationen	

Item	Technische Daten für Snowball Edge Compute Optimized
SSD-Speicherkapazität	28 TB NVMe SSD
Technische Daten der Stromversorgung	
Stromversorgung	AWS-Regionen In den USA: NEMA 5—15p 100—220 Volt. In allen Regionen ist ein Stromkabel im Lieferumfang enthalten AWS
Stromverbrauch	304 Watt für einen durchschnittlichen Anwendungsfall, obwohl das Netzteil für 1200 Watt ausgelegt ist
Spannung	100 – 240 V AC
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit — RJ45 (eines nutzbar) 1 x 25 Gbit — SFP28 1 x 100 Gbit — QSFP28
Kabel	Jedes AWS Snowball Edge Gerät wird mit landesspezifischen Stromkabeln geliefert. Es werden keine weiteren Kabel oder optischen Stecker mitgeliefert. Weitere Informationen finden Sie unter Von Snowball Edge unterstützte Netzwerkhardware .
Thermische Anforderungen	AWS Snowball Edge Geräte sind für den Bürobetrieb konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät einen Ton von 68 Dezibel und ist damit in der Regel leiser als ein Staubsauger oder Musik im Wohnzimmer.
Abmessungen und Gewichtsangaben	

Item	Technische Daten für Snowball Edge Compute Optimized
Gewicht	22,54 Kilogramm
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Spezifikationen für die Umgebung	
Vibration	Einsatz bei Nichtbetrieb entspricht ASTM D4169 Lkw Level I 0,73 GRMS
Schock	Betriebsgebrauch entspricht 70G (MIL-S-901)
	Nichtbetrieblicher Einsatz entspricht 50 G (ISTA-3A)
Höhe	Betriebsnutzung entspricht 0—3.000 Metern (0—10.000 Fuß)
	Nutzung bei Nichtbetrieb entspricht 0—12.000 Metern
Temperaturbereich	0—45 °C (betriebsbereit)

Von Snowball Edge unterstützte Netzwerkhardware

Um das AWS Snowball Edge Gerät verwenden zu können, benötigen Sie Ihre eigenen Netzkabel. Für RJ45 Kabel gibt es keine spezifischen Empfehlungen. Es wurde verifiziert, dass SFP+- und QSFP+-Kabel und -Module von Mellanox und Finisar mit dem Gerät kompatibel sind.

Nachdem Sie die Rückseite des AWS Snowball Edge Geräts geöffnet haben, sehen Sie die Netzwerkanschlüsse, die den im folgenden Screenshot gezeigten Anschlüssen ähneln.



Es kann jeweils nur eine Netzwerkschnittstelle auf dem AWS Snowball Edge Gerät verwendet werden. Verwenden Sie daher einen der Anschlüsse, um die folgende Netzwerkhardware zu unterstützen.

SFP

Dieser Anschluss bietet eine SFP28 10G/25G-Schnittstelle, die mit SFP+-Transceivermodulen SFP28 und DAC-Kabeln (Direct Attach Copper) kompatibel ist. Sie müssen Ihre eigenen Transceiver- oder DAC-Kabel bereitstellen.

- Für den 10G-Betrieb können Sie eine beliebige SFP+-Option verwenden. Beispiele sind unter anderem:
 - 10Gbase-LR-Transceiver (Monomodefaser)
 - 10Gbase-SR-Transceiver (Multimodefaser)
 - SFP+-DAC-Kabel
- Für den 25G-Betrieb können Sie jede Option verwenden. SFP28 Beispiele sind unter anderem:
 - 25Gbase-LR-Transceiver (Monomodefaser)
 - 25Gbase-SR-Transceiver (Multimodefaser)
 - SFP28 DAC-Kabel



QSFP

Dieser Anschluss bietet auf speicheroptimierten Geräten eine 40G QSFP+-Schnittstelle und auf für die Datenverarbeitung optimierten Geräten eine 40/50/100G QSFP+-Schnittstelle. Beide sind mit QSFP+-Transceiver-Modulen und DAC-Kabeln kompatibel. Sie müssen Ihre eigenen Transceiver- oder DAC-Kabel bereitstellen. Beispiele sind unter anderem:

- 40Gbase- LR4 (Einmode-Glasfaser) -Transceiver
- 40Gbase- SR4 (Multimode-Glasfaser) -Transceiver
- QSFP+ DAC

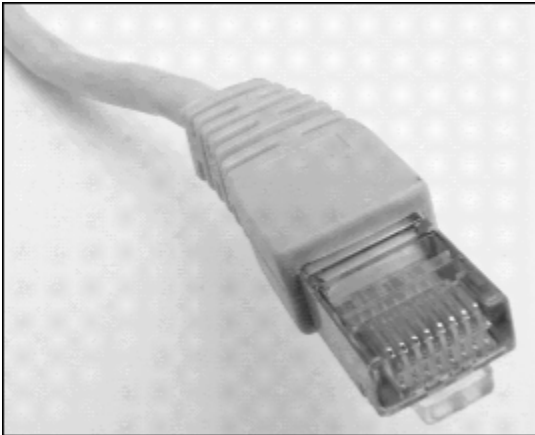


RJ45

Dieser Port unterstützt einen 1Gbase TX/10Gbase-TX-Betrieb. Der Anschluss erfolgt über ein UTP-Kabel, das mit einem Stecker abgeschlossen ist. RJ45 Snowball Edge-Geräte haben zwei RJ45 Anschlüsse. Wählen Sie einen Port aus, den Sie verwenden möchten.

1G-Betrieb wird durch eine gelb blinkende Lampe angezeigt. Der 1G-Betrieb wird für umfangreiche Datenübertragungen auf das Snowball Edge-Gerät nicht empfohlen, da dadurch die für die Datenübertragung benötigte Zeit erheblich verlängert wird.

10G-Betrieb wird durch eine grün blinkende Lampe angezeigt. Dafür ist ein Cat6A UTP-Kabel mit einer maximalen Betriebsdistanz von 55 m (180 ft) erforderlich.



Voraussetzungen für die Verwendung von Snowball Edge

Bevor Sie mit einem Snowball Edge beginnen, müssen Sie sich für ein AWS Konto registrieren, falls Sie noch keines haben. Wir empfehlen außerdem, zu lernen, wie Sie Ihre Daten und Recheninstanzen für die Verwendung mit Snowball Edge konfigurieren.

AWS Snowball Edge ist ein regionsspezifischer Dienst. Bevor Sie also Ihren Job planen, stellen Sie sicher, dass der Service in Ihrem Land verfügbar ist. AWS-Region Stellen Sie sicher, dass sich Ihr Standort und Ihr Amazon S3 S3-Bucket im selben AWS-Region oder im selben Land befinden, da dies Ihre Möglichkeit beeinträchtigt, das Gerät zu bestellen.

Um Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit rechenoptimierten Geräten für lokale Edge-Rechen- und Speicherjobs zu verwenden, müssen Sie bei der Bestellung S3-Kapazität auf dem Gerät oder den Geräten bereitstellen. Amazon S3 S3-kompatibler Speicher auf Snowball Edge unterstützt die lokale Bucket-Verwaltung, sodass Sie S3-Buckets auf dem Gerät oder Cluster erstellen können, nachdem Sie das Gerät oder die Geräte erhalten haben.

Im Rahmen des Bestellvorgangs erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle und einen AWS Key Management Service (AWS KMS) -Schlüssel. Der KMS-Schlüssel wird verwendet, um den Entsperrcode für Ihren Job zu verschlüsseln. Weitere Informationen zum Erstellen von IAM-Rollen und KMS-Schlüsseln finden Sie unter [Erstellen eines Auftrags zur Bestellung eines Snowball Edge-Geräts](#).

Note

Im asiatisch-pazifischen Raum (Mumbai) wird der AWS-Region Service von Amazon über Internet Services Private Limited (AISPL) bereitgestellt. Informationen zur Registrierung für Amazon Web Services im asiatisch-pazifischen Raum (Mumbai) AWS-Region finden Sie unter [Registrierung für AISPL](#).

Themen

- [Melden Sie sich an für ein AWS-Konto](#)
- [Erstellen eines Benutzers mit Administratorzugriff](#)
- [Über Ihre Umgebung](#)
- [Arbeiten Sie mit Dateinamen, die Sonderzeichen enthalten](#)
- [Amazon S3 S3-Verschlüsselung mit AWS KMS](#)
- [Amazon S3 S3-Verschlüsselung mit serverseitiger Verschlüsselung](#)
- [Voraussetzungen für die Verwendung des Amazon S3 S3-Adapters auf Snowball Edge für Import- und Exportaufträge](#)
- [Voraussetzungen für die Verwendung von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#)
- [Voraussetzungen für die Verwendung von Compute-Instanzen auf Snowball Edge](#)

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/die-Anmeldung>.
2. Folgen Sie den Online-Anweisungen.

Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscode auf der Telefontastatur.

Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS-Managementkonsole](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter [Benutzerzugriff mit der Standardeinstellung konfigurieren](#). AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal](#).

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

Anweisungen hierzu finden Sie unter [Berechtigungssatz erstellen](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Eine genaue Anleitung finden Sie unter [Gruppen hinzufügen](#) im AWS IAM Identity Center Benutzerhandbuch.

Über Ihre Umgebung

Wenn Sie Ihren Datensatz verstehen und wissen, wie die lokale Umgebung eingerichtet ist, können Sie Ihre Datenübertragung abschließen. Beachten Sie Folgendes, bevor Sie Ihre Bestellung aufgeben.

Welche Daten übertragen Sie?

Das Übertragen einer großen Anzahl kleiner Dateien funktioniert nicht gut mit AWS Snowball Edge. Das liegt daran, dass Snowball Edge jedes einzelne Objekt verschlüsselt. Zu den

kleinen Dateien gehören Dateien mit einer Größe von weniger als 1 MB. Wir empfehlen, sie vor der Übertragung auf das AWS Snowball Edge Gerät zu komprimieren. Wir empfehlen außerdem, dass Sie nicht mehr als 500.000 Dateien oder Verzeichnisse in jedem Verzeichnis haben.

Wird während der Übertragung auf die Daten zugegriffen?

Es ist wichtig, über einen statischen Datensatz zu verfügen (d. h., dass während der Übertragung keine Benutzer oder Systeme auf die Daten zugreifen). Andernfalls kann die Dateiübertragung aufgrund einer nicht übereinstimmenden Prüfsumme fehlschlagen. Die Dateien werden nicht übertragen und die Dateien werden als markiert. `Failed`

Um zu verhindern, dass Ihre Daten beschädigt werden, sollten Sie während der Übertragung keine Verbindung zu einem AWS Snowball Edge Gerät trennen oder dessen Netzwerkeinstellungen ändern. Dateien müssen beim Schreiben auf das Gerät in statischem Zustand sein. Dateien, die während des Schreibens auf das Gerät geändert werden, können zu Lese-/Schreibkonflikten führen.

Unterstützt das Netzwerk die Datenübertragung AWS Snowball Edge ?

Snowball Edge unterstützt die Netzwerkadapter RJ45SFP+ oder QSFP+. Stellen Sie sicher, dass es sich bei Ihrem Switch um einen Gigabit-Switch handelt. Je nach Switch-Marke könnte es Gigabit oder 10/100/1000 sein. Snowball Edge-Geräte unterstützen keinen Megabit-Switch oder 10/100-Switch.

Arbeiten Sie mit Dateinamen, die Sonderzeichen enthalten

Beachten Sie bitte, dass Fehler auftreten können, wenn die Namen Ihrer Objekte Sonderzeichen enthalten. Amazon S3 erlaubt zwar Sonderzeichen, wir empfehlen jedoch dringend, die folgenden Zeichen zu vermeiden:

- Umgekehrter Schrägstrich ("`\`")
- Linke geschweifte Klammer ("`{`")
- Rechte geschweifte Klammer ("`}`")
- Linke eckige Klammer ("`[`")
- Rechte eckige Klammer ("`]`")
- Kleiner als-Zeichen ("`<`")
- Größersymbol ("`>`")
- Nicht darstellbare ASCII-Zeichen (128-255 Dezimalzeichen)

- Caret ("^")
- Prozentzeichen ("%")
- Accent Grave ("`")
- Anführungszeichen
- Tilde ("~")
- Pfundzeichen ("£")
- Vertikaler Strich ("|")

Wenn Ihre Dateien eines oder mehrere dieser Zeichen in Objektnamen enthalten, benennen Sie die Objekte um, bevor Sie sie auf das AWS Snowball Edge Gerät kopieren. Windows-Benutzer, deren Dateinamen Leerzeichen enthalten, sollten vorsichtig sein, wenn sie einzelne Objekte kopieren oder einen rekursiven Befehl ausführen. Setzen Sie in Befehlen die Namen von Objekten, die Leerzeichen enthalten, in Anführungszeichen. Im Folgenden finden Sie Beispiele für solche Dateien.

Betriebssystem	Dateiname: test file.txt
Windows	"C:\Users\ <username>\desktop\test file.txt"</username>
iOS	/Users/<username>/test\ file.txt
Linux	/home/<username>/test\ file.txt

Note

Die einzigen Objektmetadaten, die übertragen werden, sind der Objektname und die Größe.

Amazon S3 S3-Verschlüsselung mit AWS KMS

Sie können die standardmäßig AWS verwalteten oder kundenverwalteten Verschlüsselungsschlüssel verwenden, um Ihre Daten beim Import oder Export von Daten zu schützen.

Verwenden der standardmäßigen Amazon S3 S3-Bucket-Verschlüsselung mit AWS KMS verwalteten Schlüsseln

Um die AWS verwaltete Verschlüsselung zu aktivieren mit AWS KMS

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie den Amazon S3 S3-Bucket aus, den Sie verschlüsseln möchten.
3. Wählen Sie im Assistenten, der auf der rechten Seite angezeigt wird, Eigenschaften aus.
4. Wählen Sie im Feld Standardverschlüsselung die Option Deaktiviert (diese Option ist ausgegraut), um die Standardverschlüsselung zu aktivieren.
5. Wählen Sie AWS-KMS als Verschlüsselungsmethode und wählen Sie dann den KMS-Schlüssel aus, den Sie verwenden möchten. Dieser Schlüssel wird verwendet, um Objekte zu verschlüsseln, die in den Bucket eingefügt werden.
6. Wählen Sie Speichern.

Nachdem der Snowball Edge-Job erstellt wurde und bevor die Daten importiert werden, fügen Sie der vorhandenen IAM-Rollenrichtlinie eine Anweisung hinzu. Dies ist die Rolle, die Sie während des Bestellvorgangs erstellt haben. Je nach Jobtyp sieht der Standard-Rollenname ähnlich aus wie `Snowball-import-s3-only-role` oder `Snowball-export-s3-only-role`.

Im Folgenden finden Sie Beispiele für eine solche Aussage.

Für den Import von Daten

Wenn Sie serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln (SSE-KMS) verwenden, um die Amazon S3 S3-Buckets zu verschlüsseln, die Ihrem Importauftrag zugeordnet sind, müssen Sie Ihrer IAM-Rolle auch die folgende Anweisung hinzufügen.

Example Beispiel für eine IAM-Rolle für den Snowball-Import

```
{
  "Effect": "Allow",
  "Action": [
    "kms: GenerateDataKey",
    "kms: Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
```

```
}
```

Zum Exportieren von Daten

Wenn Sie serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln verwenden, um die Amazon S3 S3-Buckets zu verschlüsseln, die Ihrem Exportauftrag zugeordnet sind, müssen Sie Ihrer IAM-Rolle auch die folgende Anweisung hinzufügen.

Example IAM-Rolle „Snowball-Export“

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Verwendung der S3-Standard-Bucket-Verschlüsselung mit AWS KMS Kundenschlüsseln

Sie können die standardmäßige Amazon S3 S3-Bucket-Verschlüsselung mit Ihren eigenen KMS-Schlüsseln verwenden, um Daten zu schützen, die Sie importieren und exportieren.

Für den Import von Daten

Um die vom Kunden verwaltete Verschlüsselung zu aktivieren mit AWS KMS

1. Melden Sie sich bei der AWS Key Management Service (AWS KMS) -Konsole an AWS-Managementkonsole und öffnen Sie sie 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 linken Navigationsbereich die Option Vom Kunden verwaltete Schlüssel und dann den KMS-Schlüssel aus, der den Buckets zugeordnet ist, die Sie verwenden möchten.
4. Erweitern Sie Key Policy, falls es nicht bereits erweitert ist.
5. Wählen Sie im Bereich Key Users die Option Hinzufügen aus und suchen Sie nach der IAM-Rolle. Wählen Sie die IAM-Rolle und dann Hinzufügen aus.

- Alternativ können Sie „Zur Richtlinienansicht wechseln“ wählen, um das Dokument mit den wichtigsten Richtlinien anzuzeigen und der wichtigen Richtlinie eine Erklärung hinzuzufügen. Im Folgenden finden Sie ein Beispiel für die Richtlinie.

Example einer Richtlinie für den vom AWS KMS Kunden verwalteten Schlüssel

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/snowball-import-s3-only-role"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Nachdem diese Richtlinie dem vom AWS KMS Kunden verwalteten Schlüssel hinzugefügt wurde, ist sie auch erforderlich, um die mit dem Snowball-Job verknüpfte IAM-Rolle zu aktualisieren. Standardmäßig ist die Rolle `snowball-import-s3-only-role`

Example der IAM-Rolle „Snowball-Import“

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Weitere Informationen finden Sie unter [Verwenden identitätsbasierter Richtlinien \(IAM-Richtlinien\) für AWS Snowball Edge](#).

Der verwendete KMS-Schlüssel sieht wie folgt aus:

"Resource": "arn:aws:kms:*region*:*AccountID*:key/*"

Für den Export von Daten

Example einer Richtlinie für den vom AWS KMS Kunden verwalteten Schlüssel

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/snowball-import-s3-only-role"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Nachdem diese Richtlinie dem vom AWS KMS Kunden verwalteten Schlüssel hinzugefügt wurde, ist sie auch erforderlich, um die mit dem Snowball-Job verknüpfte IAM-Rolle zu aktualisieren. Standardmäßig sieht die Rolle wie folgt aus:

snowball-export-s3-only-role

Example der IAM-Rolle Snowball-Export

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Nachdem diese Richtlinie dem vom AWS KMS Kunden verwalteten Schlüssel hinzugefügt wurde, ist sie auch erforderlich, um die mit dem Snowball-Job verknüpfte IAM-Rolle zu aktualisieren. Standardmäßig ist die Rolle. snowball-export-s3-only-role

Amazon S3 S3-Verschlüsselung mit serverseitiger Verschlüsselung

AWS Snowball Edge unterstützt serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Verschlüsselungsschlüsseln (SSE-S3). Bei der serverseitigen Verschlüsselung geht es darum, Daten im Ruhezustand zu schützen, und SSE-S3 verfügt über eine starke Multifaktor-Verschlüsselung, um Ihre Daten im Ruhezustand in Amazon S3 zu schützen. Weitere Informationen zu SSE-S3 finden Sie unter [Schützen von Daten mithilfe serverseitiger Verschlüsselung mit Amazon S3-Managed Encryption Keys \(SSE-S3\) im Amazon Simple Storage Service-Benutzerhandbuch](#).

Note

Unterstützt derzeit AWS Snowball Edge keine serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C). Sie möchten diesen SSE-Typ möglicherweise jedoch zum Schutz von importierten Daten verwenden oder setzen ihn möglicherweise auch bereits für zu exportierende Daten ein. Beachten Sie in diesem Fall jedoch die folgenden Punkte:

- Import — Wenn Sie die Objekte, die Sie in S3 importiert haben, mit SSE-C verschlüsseln möchten, kopieren Sie diese Objekte in einen anderen Bucket, für den die SSE-KMS- oder SSE-S3-Verschlüsselung als Teil der Bucket-Richtlinie dieses Buckets eingerichtet wurde.
- Export — Wenn Sie Objekte exportieren möchten, die mit SSE-C verschlüsselt sind, kopieren Sie diese Objekte zunächst in einen anderen Bucket, der entweder keine serverseitige Verschlüsselung hat oder für den SSE-KMS oder SSE-S3 in der Bucket-Richtlinie dieses Buckets angegeben sind.

Voraussetzungen für die Verwendung des Amazon S3 S3-Adapters auf Snowball Edge für Import- und Exportaufträge

Sie können den S3-Adapter auf Snowball Edge verwenden, wenn Sie die Geräte verwenden, um Daten aus lokalen Datenquellen in die Cloud oder von der Cloud in den lokalen Datenspeicher zu verschieben. Weitere Informationen finden Sie unter [Übertragung von Dateien mithilfe des Amazon S3 S3-Adapters für die Datenmigration zu oder von Snowball Edge](#).

Der dem Auftrag zugeordnete Amazon S3 S3-Bucket muss die Amazon S3 S3-Standardspeicherkategorie verwenden. Bevor Sie Ihren ersten Auftrag anlegen, sollten Sie die folgenden Informationen beachten.

Gehen Sie für Jobs, die Daten in Amazon S3 importieren, wie folgt vor:

- Vergewissern Sie sich, dass die zu übertragenden Dateien und Ordner gemäß den [Richtlinien zur Benennung von Objektschlüsseln](#) für Amazon S3 benannt sind. Dateien oder Ordner mit Namen, die diese Richtlinien nicht erfüllen, werden nicht in Amazon S3 importiert.
- Planen Sie, welche Daten Sie in Amazon S3 importieren möchten. Weitere Informationen finden Sie unter [Planen Sie Ihren großen Transfer mit Snowball Edge](#).

Gehen Sie vor dem Exportieren von Daten aus Amazon S3 wie folgt vor:

- Überlegen Sie, welche Daten exportiert wurden, als Sie den Auftrag erstellten. Weitere Informationen finden Sie unter [Verwenden von Amazon S3 S3-Objektschlüsseln beim Exportieren von Daten auf ein Snowball Edge-Gerät](#).
- Ändern Sie für alle Dateien mit einem Doppelpunkt (:) im Dateinamen die Dateinamen in Amazon S3, bevor Sie den Exportauftrag zum Abrufen dieser Dateien erstellen. Dateien mit einem Doppelpunkt im Dateinamen werden nicht zu Microsoft Windows Server exportiert.

Voraussetzungen für die Verwendung von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge

Sie verwenden Amazon S3 S3-kompatiblen Speicher auf Snowball Edge, wenn Sie Daten auf dem Gerät an Ihrem Edge-Standort speichern und die Daten für lokale Rechenoperationen verwenden. Daten, die für lokale Rechenoperationen verwendet werden, werden nicht in Amazon S3 importiert, wenn das Gerät zurückgegeben wird.

Beachten Sie bei der Bestellung eines Snow-Geräts für lokale Datenverarbeitung und Speicherung mit Amazon S3 S3-kompatiblen Speicher Folgendes.

- Sie stellen Amazon S3 S3-Speicherkapazität bereit, wenn Sie das Gerät bestellen. Berücksichtigen Sie also Ihren Speicherbedarf, bevor Sie ein Gerät bestellen.
- Sie können Amazon S3 S3-Buckets auf dem Gerät erstellen, nachdem Sie es erhalten haben, anstatt ein Snowball Edge-Gerät zu bestellen.
- Sie müssen die neueste Version des Snowball Edge-Clients AWS CLI (v2.11.15 oder höher) herunterladen oder AWS OpsHub auf Ihrem Computer installieren, um Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden zu können.
- Nachdem Sie Ihr Gerät erhalten haben, konfigurieren, starten und verwenden Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge gemäß [Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#) in diesem Handbuch.

Voraussetzungen für die Verwendung von Compute-Instanzen auf Snowball Edge

Sie können EC2 Amazon-kompatible Compute-Instances ausführen, die auf einer AWS Snowball Edge mit den sbe-g Instance-Typen sbe1, sbe-c, und gehostet werden:

- Der sbe1 Instanztyp funktioniert auf Geräten mit der Option Snowball Edge Storage Optimized.
- Der sbe-c Instanztyp funktioniert auf Geräten mit der Option Snowball Edge Compute Optimized.

Alle Compute-Instanztypen, die in den Snowball Edge Edge-Geräteoptionen unterstützt werden, sind AWS Snowball Edge gerätespezifisch. Wie ihre cloudbasierten Gegenstücke benötigen diese Instances Amazon Machine Images (AMIs), um gestartet zu werden. Sie wählen das AMI für eine Instance aus, bevor Sie Ihren Snowball Edge Edge-Job erstellen.

Um eine Recheninstanz auf einem Snowball Edge Edge zu verwenden, erstellen Sie einen Job, um ein Snowball Edge-Gerät zu bestellen, und geben Sie Ihre an. AMIs Sie können dazu die AWS Snowball Edge Managementkonsole, die AWS Command Line Interface (AWS CLI) oder eine der folgenden Optionen verwenden. AWS SDKs Um Ihre Instances verwenden zu können, müssen Sie in der Regel einige Voraussetzungen erfüllen, bevor Sie Ihren Job erstellen können.

Für Jobs, die Compute-Instances verwenden, müssen Sie, bevor Sie Ihrem Job irgendwelche hinzufügen können, ein AMI in Ihrem haben AWS-Konto und es muss sich AMIs um einen unterstützten Image-Typ handeln. Derzeit AMIs basieren die unterstützten Betriebssysteme auf den folgenden Betriebssystemen:

- [Amazon Linux 2](#)
- [CentOS 7 \(x86_64\) - mit Updates HVM](#)
- Ubuntu 16.04 LTS - Xenial (HVM)
- [Ubuntu 20.04 LTS - Fokus](#)
- [Ubuntu 22.04 LTS - Jammy](#)
- [Microsoft Windows Server 2012 R2](#)
- [Microsoft Windows Server 2016](#)
- [Microsoft Windows Server 2019](#)

 Note

Ubuntu 16.04 LTS — Xenial (HVM) -Images werden in der nicht mehr unterstützt AWS Marketplace, werden aber weiterhin für die Verwendung auf Snowball Edge-Geräten über Amazon EC2 VM und die lokale Ausführung in unterstützt. Import/Export AMIs

Sie können diese Bilder von erhalten. [AWS Marketplace](#)

Wenn Sie SSH verwenden, um eine Verbindung zu den Instances herzustellen, die auf einem Snowball Edge ausgeführt werden, können Sie Ihr eigenes key pair verwenden oder eines auf dem Snowball Edge erstellen. Informationen AWS OpsHub zum Erstellen eines key pair auf dem Gerät finden Sie unter [Arbeiten mit Schlüsselpaaren für EC2 -kompatible Instanzen in AWS OpsHub](#). Informationen zur Verwendung von AWS CLI , um ein key pair auf dem Gerät zu erstellen, finden Sie `create-key-pair` unter [Liste der unterstützten EC2 -kompatiblen AWS CLI Befehle auf einem Snowball Edge](#). Weitere Informationen zu Schlüsselpaaren und Amazon Linux 2 finden Sie unter [EC2 Amazon-Schlüsselpaare und Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch.

Informationen zur Verwendung von Datenverarbeitungs-Instances auf einem Gerät finden Sie unter [Verwenden von EC2 Amazon-kompatiblen Compute-Instances auf Snowball Edge](#).

Wie AWS Snowball Edge funktioniert

AWS Snowball Edge Geräte gehören Ihnen und befinden sich an Ihrem lokalen Standort, solange sie verwendet werden. AWS

Es gibt drei Auftragsstypen, die Sie mit einem AWS Snowball Edge Gerät verwenden können. Die Auftragsstypen unterscheiden sich zwar in ihren Anwendungsfällen, doch verfügt jeder Auftragsstyp über denselben Workflow zum Bestellen, Empfangen und Zurückgeben von Geräten. Unabhängig vom Auftragsstyp erfolgt bei jedem Auftrag nach Abschluss des Auftrags eine Datenlöschung gemäß der Norm 800-88 des National Institute of Standards and Technology (NIST).

Der gemeinsame Workflow

1. Job erstellen — Jeder Job wird in der Managementkonsole für die AWS Snow-Familie oder programmgesteuert über die Job-Management-API erstellt. Der Status eines Jobs kann in der Konsole oder über die API nachverfolgt werden.
2. Ein Gerät ist für Ihren Job vorbereitet — Wir bereiten ein AWS Snowball Edge Gerät für Ihren Job vor, und der Status Ihres Jobs lautet jetzt Preparing Snowball. Dieser Vorbereitungsprozess kann ab dem Zeitpunkt, an dem der Auftrag zur Bestellung des Geräts erstellt wurde, bis zu 4 Wochen dauern. Dieser Zeitplan sollte in Ihrem Projektplan berücksichtigt werden, um einen reibungslosen Übergang zu gewährleisten.
3. Ein Gerät wird vom Mobilfunkanbieter Ihrer Region an Sie versandt. Der Mobilfunkanbieter übernimmt von hier aus, und der Status Ihres Auftrags lautet jetzt In Bearbeitung zu Ihnen. Sie finden die Sendungsverfolgungsnummer und einen Link zur Webseite zur Sendungsverfolgung auf der Konsole oder in der API zur Auftragsverwaltung. Informationen darüber, wer der Mobilfunkanbieter Ihrer Region ist, finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).
4. Gerät erhalten — Wenige Tage später liefert der Mobilfunkanbieter Ihrer Region das AWS Snowball Edge Gerät an die Adresse, die Sie bei der Erstellung des Auftrags angegeben haben, und der Status Ihres Auftrags ändert sich in Zugestellt an Sie. Das Gerät wird nicht in einem Paket angeliefert, da das Gerät einen eigenen Transportbehälter umfasst.
5. Holen Sie sich Ihre Anmeldeinformationen und laden Sie den Snowball Edge-Client herunter — Machen Sie sich bereit, mit der Datenübertragung zu beginnen, indem Sie Ihre Anmeldeinformationen, Ihr Auftragsmanifest und den Entsperrcode des Manifests abrufen und dann den Snowball Edge-Client herunterladen.
 - Der Snowball Edge-Client ist das Tool, mit dem Sie den Datenfluss vom Gerät zu Ihrem lokalen Datenziel verwalten.

Sie können den Snowball Edge-Client von der [AWS Snowball Edge Ressourcenseite](#) herunterladen und installieren.

Sie müssen den Snowball Edge-Client von der Seite [AWS Snowball Edge Ressourcen](#) herunterladen und auf einer leistungsstarken Workstation installieren, die Sie besitzen.

- Das Manifest wird zum Authentifizieren Ihres Zugangs auf das Gerät verwendet. Es ist verschlüsselt und kann nur mit dem Entsperrcode entschlüsselt werden. Sie erhalten das Manifest in der Konsole oder über die API zur Auftragsverwaltung, wenn sich das Gerät an Ihrem Standort vor Ort befindet.
 - Der Entsperrcode umfasst 29 Zeichen und dient zum Entschlüsseln des Manifests. Sie erhalten den Entsperrcode in der Konsole; oder über die API zur Auftragsverwaltung. Wir empfehlen Ihnen, den Entsperrcode nicht zusammen mit dem Manifest aufzubewahren. Auf diese Weise verhindern Sie jeden unautorisierten Zugriff auf das Gerät, während sich dieses in Ihrem Gebäude befindet.
6. Platzieren Sie die Hardware — Platzieren Sie das Gerät in Ihrem Rechenzentrum und öffnen Sie es gemäß den Anweisungen auf dem Gehäuse. Schließen Sie das Gerät an eine Stromquelle an und verbinden Sie sie mit Ihrem lokalen Netzwerk.
 7. Gerät einschalten — Als Nächstes schalten Sie das Gerät ein, indem Sie den Netzschalter über dem LCD-Display drücken. Nach einigen Minuten erscheint im Display die Meldung Ready (Bereit).
 8. Rufen Sie die IP-Adresse für das Gerät ab — Auf dem LCD-Display befindet sich die Registerkarte CONNECTION. Tippen Sie auf diese Registerkarte und rufen Sie die IP-Adresse für das AWS Snowball Edge Gerät ab.
 9. Verwenden Sie den Snowball Edge-Client, um das Gerät zu entsperren — Wenn Sie den Snowball Edge-Client verwenden, um das AWS Snowball Edge Gerät zu entsperren, geben Sie die IP-Adresse des Geräts, den Pfad zu Ihrem Manifest und den Entsperrcode ein. Der Snowball Edge-Client entschlüsselt das Manifest und authentifiziert damit Ihren Zugriff auf das Gerät.
 10. Gerät verwenden — Das Gerät ist betriebsbereit. Sie können es verwenden, um Daten mit dem Amazon S3 S3-Adapter oder dem NFS-Mountpoint (Network File System) zu übertragen oder für lokale Datenverarbeitung und Speicherung mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge.
 11. Bereiten Sie das Gerät für die Rückreise vor — Wenn Sie mit dem Gerät an Ihrem Standort vor Ort fertig sind, drücken Sie den Netzschalter über dem LCD-Display. Das Herunterfahren des Geräts dauert ca. 20 Sekunden. Trennen Sie das Gerät von der Stromversorgung und legen Sie das

Stromkabel in die Halterung an der Oberseite des Geräts. Schließen Sie dann alle drei Klappen des Geräts. Das Gerät ist nun versandfertig für die Rückgabe.

12Der Mobilfunkanbieter Ihrer Region sendet das Gerät zurück an AWS — Wenn der Mobilfunkanbieter das AWS Snowball Edge Gerät hat, lautet der Status für den Auftrag auf Auf dem Weg zu AWS.

Note

Für Export- und Cluster-Jobs gibt es zusätzliche Schritte. Weitere Informationen erhalten Sie unter [So funktionieren Snowball Edge-Exportaufträge](#) und [So funktionieren geclusterte lokale Rechen- und Speicherjobs mit Snowball Edge](#).

Themen

- [So funktionieren Snowball Edge-Importaufträge](#)
- [So funktionieren Snowball Edge-Exportaufträge](#)
- [So funktionieren lokale Rechen- und Speicherjobs in Snowball Edge](#)
- [Videos und Blogs zu Snowball Edge](#)

So funktionieren Snowball Edge-Importaufträge

Jeder Importauftrag verwendet eine einzelne Snowball-Appliance. Nachdem Sie in der Managementkonsole für die AWS Snow-Familie oder der Job-Management-API einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellt haben, senden wir Ihnen einen Snowball zu. Wenn es in ein paar Tagen ankommt, verbinden Sie das Snowball Edge-Gerät mit Ihrem Netzwerk und übertragen die Daten, die Sie in Amazon S3 importieren möchten, auf das Gerät. Wenn Sie mit der Datenübertragung fertig sind, senden Sie den Snowball zurück an AWS, und wir importieren Ihre Daten in Amazon S3.

Important

Der Importvorgang kann vom Snow-Gerät aus nicht in Buckets in Amazon S3 schreiben, wenn Sie S3 Object Lock aktiviert und die Standard-Aufbewahrungseinstellungen aktiviert haben. Nachdem Amazon S3 Object Lock aktiviert wurde, können Sie es nicht deaktivieren oder die Bucket-Versionierung für den Bucket aussetzen. Wenn in Ihren Buckets S3 Object Lock mit aktivierten Standard-Aufbewahrungseinstellungen aktiviert ist, deaktivieren

Sie vor der Rückgabe von Snowball Edge die Aufbewahrungseinstellung von S3 Object Lock. Nachdem die Daten vom Gerät importiert wurden AWS, aktivieren Sie erneut die Aufbewahrungseinstellung für den Bucket. Weitere Informationen finden Sie unter [Einen Aufbewahrungszeitraum für ein S3-Objekt festlegen oder ändern](#).

Der Importvorgang kann auch nicht in Ihren Bucket in Amazon S3 schreiben, wenn die IAM-Richtlinien für den Bucket das Schreiben in den Bucket verhindern. Weitere Informationen finden Sie unter [Identity and Access Management für Amazon S3](#).

So funktionieren Snowball Edge-Exportaufträge

Jeder Exportauftrag kann eine beliebige Anzahl von AWS Snowball Edge Geräten verwenden. Wenn die Liste mehr Daten enthält, als auf ein einzelnes Gerät passen, werden Ihnen mehrere Geräte zur Verfügung gestellt. Jedem Teilauftrag wird genau einem Gerät zugeordnet. Nachdem Ihre Auftragsteile erstellt wurden, wechselt Ihr erster Auftragsteil in den Status Preparing Snowball.

Note

Der Angebotsvorgang, mit dem Ihr Auftrag in Teile aufgeteilt wurde, ist eine Funktion von Amazon S3, und er wird Ihnen auf die gleiche Weise in Rechnung gestellt wie jeder andere Amazon S3 S3-Vorgang.

Kurz darauf beginnen wir mit dem Exportieren Ihrer Daten in ein Gerät. Die für den Export Ihrer Daten benötigte Zeit hängt von der Art Ihres Datensatzes ab. Beispielsweise dauert der Export vieler kleiner Dateien (weniger als 10 MB) deutlich länger. Wenn der Export abgeschlossen ist, AWS wird das Gerät für die Abholung durch den Mobilfunkanbieter Ihrer Region bereit gemacht. Wenn es ankommt, verbinden Sie das AWS Snowball Edge Gerät mit Ihrem Netzwerk und übertragen die Daten vom Gerät in den Speicher in Ihrem Netzwerk.

Wenn Sie mit der Datenübertragung fertig sind, senden Sie das Gerät zurück an AWS. Wenn wir das Gerät für Ihren Exportauftrag erhalten haben, löschen wir es vollständig. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88. Dieser Schritt kennzeichnet den Abschluss dieses bestimmten Teilauftrags.

- Für die Keylisting

Bevor wir die Objekte im S3-Bucket exportieren, scannen wir den Bucket. Wenn der Bucket nach dem Scan geändert wird, kann es beim Job zu Verzögerungen kommen, da wir nach fehlenden oder veränderten Objekten suchen.

- Für S3 Glacier Flexible Retrieval

Es ist wichtig zu beachten, dass AWS Snowball Edge keine Objekte exportiert werden können, die sich in der S3 Glacier-Speicherkategorie befinden. Diese Objekte müssen wiederhergestellt werden, bevor die Objekte im Bucket erfolgreich exportiert werden können AWS Snowball Edge.

So funktionieren lokale Rechen- und Speicherjobs in Snowball Edge

Sie können die lokalen Rechen- und Speicherfunktionen eines AWS Snowball Edge Geräts nutzen, indem Sie AWS EC2 -kompatible Compute-Instances oder Kubernetes-Container in Amazon EKS Anywhere on Snow ausführen. Für Rechenfunktionen wird der Datenspeicher durch Amazon S3 S3-kompatiblen Speicher auf Snowball Edge bereitgestellt.

Sie können Amazon S3 S3-Buckets auf den Snowball Edge-Geräten erstellen, um Objekte vor Ort für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Amazon S3-kompatibler Speicher auf Snowball Edge bietet eine neue Speicherkategorie `SNOW`, die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Snowball Edge-Geräten zu speichern. Sie können für Snowball Edge-Buckets dieselben APIs Funktionen wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte zurückgegeben werden, werden alle Daten gelöscht AWS, die in einem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge erstellt oder gespeichert wurden. Weitere Informationen finden Sie unter Jobs [nur für lokale Datenverarbeitung und Speicherung](#).

Weitere Informationen finden Sie unter [Informationen zur Verwendung von Snowball Edge-Geräten zur Bereitstellung lokaler Rechen- und Speicherfunktionen](#).

So funktionieren geclusterte lokale Rechen- und Speicherjobs mit Snowball Edge

Bei einem Cluster-Job handelt es sich um eine spezielle Art von Job, der ausschließlich für lokale Speicher- und Rechenaufgaben bestimmt ist. Er eignet sich für Workloads, die eine höhere

Datenbeständigkeit und Speicherkapazität erfordern. Weitere Informationen finden Sie unter [Informationen zu Aufträgen, die lokalen Speicher auf einem Cluster von Snowball Edge-Geräten bereitstellen](#).

Note

Wie bei eigenständigen lokalen Speicher- und Rechenaufträgen können die in einem Cluster gespeicherten Daten nicht in Amazon S3 importiert werden, ohne zusätzliche Geräte als Teil separater Importaufträge zu bestellen. Wenn Sie diese Geräte bestellen, können Sie die Daten aus dem Cluster auf die Geräte übertragen und bei der Rückgabe der Geräte für die Import-Aufträge importieren.

Cluster haben 3 bis 16 AWS Snowball Edge Geräte, sogenannte Knoten. Wenn Sie die Knoten von Ihrem regionalen Mobilfunkanbieter erhalten, verbinden Sie alle Knoten mit Strom und Ihrem Netzwerk, um ihre IP-Adressen zu erhalten. Sie verwenden diese IP-Adressen, um alle Knoten des Clusters gleichzeitig mit einem einzigen Entsperrbefehl zu entsperren, wobei Sie die IP-Adresse eines der Knoten verwenden. Weitere Informationen finden Sie unter [Konfiguration und Verwendung des Snowball Edge-Clients](#).

Sie können Daten in einen entsperrten Cluster schreiben, indem Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge und die auf die anderen Knoten verteilten Daten verwenden oder verwenden.

Wenn Sie mit Ihrem Cluster fertig sind, senden Sie alle Knoten zurück an AWS. Wenn wir den Clusterknoten erhalten, löschen wir den Snowball vollständig. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Videos und Blogs zu Snowball Edge

- [Migrieren gemischter Dateigrößen mit den snow-transfer-tool auf AWS Snowball Edge-Geräten](#)
- [AWS Snowball Edge Datenmigration](#)
- [AWS OpsHub for Snow Family](#)
- [Novetta stellt in der Katastrophenhilfe auch an den abgelegensten Orten IoT und Machine Learning bereit.](#)
- [Ermöglichen Sie umfangreiche Datenbankmigrationen mit DMS und AWS Snowball Edge](#)
- [Bewährte Methoden zur Datenmigration mit AWS Snowball Edge](#)

- [AWS Snowball Edge Ressourcen](#)
- [Amazon S3 S3-kompatibler Speicher auf AWS Snowball Edge rechenoptimierten Geräten jetzt allgemein verfügbar](#)
- [Erste Schritte mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf AWS Snowball Edge-Geräten](#)

Langfristige Preisgestaltung für Snowball Edge-Geräte

Wenn Sie ein Snowball Edge-Gerät bestellen, können Sie die Preisoption wählen, die am besten zu Ihrem Anwendungsfall passt. Die Preisgestaltung ist auf zwei Arten verfügbar: auf Abruf für jeden Tag, an dem Sie das Gerät besitzen, oder im Voraus bezahlt, langfristige Preise mit monatlichen, ein- oder dreijährigen Laufzeiten, je nach Gerätetyp. Sie können sich dafür entscheiden, Ihre langfristige Preisoption automatisch für ein oder drei Jahre zu verlängern, sodass ein neuer Prepaid-Zeitraum beginnt, wenn der vorherige Zeitraum endet, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Die monatliche langfristige Preisoption verlängert sich automatisch, solange sich das Gerät in Ihrem Besitz befindet. Weitere Informationen zur Bestellung eines Geräts finden Sie unter [Erstellen eines Auftrags zur Bestellung eines Snowball Edge-Geräts](#) in diesem Handbuch.

Die langfristige Preisgestaltung bietet nicht nur ein günstiges Budget, sondern ermöglicht es Ihnen auch, Snowball Edge-Geräte während des Preiszeitraums auszutauschen, wenn sich Ihre betrieblichen Anforderungen ändern. Sie können beispielsweise beantragen, Geräte auszutauschen, sodass das neue Gerät ein neues AMI oder neue Daten von Amazon S3 enthält, oder dass ein ausgefallenes Gerät ersetzt wird. Siehe [Austausch von Snowball Edge-Geräten während des langfristigen Preiszeitraums](#).

Note

Wenn Sie aus einem anderen Grund als einem Hardware- oder Softwareproblem, das auf den Snow-Service zurückzuführen ist, den Austausch oder den Austausch eines Snowball Edge-Geräts im Rahmen des 1- oder 3-jährigen Commit-Preisplans beantragen, wird Ihnen eine Gerätezyklusgebühr berechnet. AWS Diese Gerätezyklusgebühr wird als monatliche Gebühr (für Snowball Edge Compute Optimized) oder als On-Demand-Jobgebühr für Ihre Konfiguration festgelegt.

Weitere Informationen zur langfristigen Preisgestaltung finden Sie unter [Kostenoptimierung mit langfristigen Preisoptionen für AWS Snowball Edge](#). AWS Snowball Edge Die Preise für Sie AWS-Region finden Sie unter [AWS Snowball Edge Preisgestaltung](#).

Austausch von Snowball Edge-Geräten während des langfristigen Preiszeitraums

Der Austausch von Snowball Edge-Geräten während des langfristigen Preiszeitraums beinhaltet die Bestellung eines neuen Geräts und die sofortige Rückgabe des aktuellen Geräts.

1. Erstellen Sie einen neuen Auftrag für das Snowball Edge-Ersatzgerät. Das Ersatzgerät muss für denselben Auftragsstyp bestimmt sein und über dieselben Rechen- und Speicheroptionen verfügen wie das Gerät, das Sie haben. Weitere Informationen finden Sie in diesem Handbuch unter [Erstellen eines Auftrags zur Bestellung eines Snowball Edge-Geräts](#).
2. Senden Sie das Gerät, das Sie haben, sofort zurück. Siehe [Snowball Edge ausschalten](#) und [Rückgabe des Snowball Edge-Geräts](#). AWS kümmert sich um die Logistik für den Austausch von Geräten, und für diesen Austausch wird eine Gebühr für den Gerätewechsel erhoben.

Überlegungen zum Versand für Snowball Edge

Wenn Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen, geben Sie eine Lieferadresse an und wählen die Versandgeschwindigkeit. Beachten Sie, dass die Versandgeschwindigkeit nicht angibt, wie schnell Sie das Gerät ab dem Tag, an dem Sie den Auftrag erstellt haben, erwarten können. Sie gibt vielmehr die Uhrzeit an, zu der sich das Gerät auf dem Transportweg zwischen AWS und Ihrer Lieferadresse befindet.

Es kann bis zu 4 Wochen dauern, bis das Gerät bereitgestellt und für Ihre Arbeit vorbereitet ist, bevor es versendet wird. Dieser Zeitplan sollte in Ihrem Projektplan berücksichtigt werden, um einen reibungslosen Übergang zu gewährleisten. Während Ihr Gerät für den Versand vorbereitet AWS wird, können Sie den Status Ihres Auftrags über den verfolgen. Managementkonsole für die AWS Snow-Familie Weitere Informationen finden Sie unter [Status von Snowball Edge-Jobs](#).

Note

Die von Ihnen gewählte Versandgeschwindigkeit gilt, wenn das Gerät an Sie AWS gesendet wird und wenn Sie das Gerät an zurücksenden AWS.

Snowball Edge-Geräte können nur zum Import oder Export von Daten innerhalb der AWS Region verwendet werden, in der die Geräte bestellt wurden.

Weitere Informationen zur Auswahl der Versandgeschwindigkeit und zur Eingabe Ihrer Lieferadresse bei der Erstellung eines Auftrags zur Bestellung eines Snowball Edge-Geräts finden Sie unter [Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen](#). Weitere Informationen zur Rückgabe eines Snowball Edge-Geräts an finden Sie AWS unter [Rückgabe des Snowball Edge-Geräts](#).

Informationen zu den Versandkosten finden Sie unter [AWS Snowball Edge Preise](#).

Regionale Versandbeschränkungen für Snowball Edge

Bevor Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen, sollten Sie sich mit Ihren Amazon S3 S3-Daten AWS-Region bei der Konsole anmelden. AWS versendet Snowball Edge nicht zwischen Ländern innerhalb desselben Landes, z. AWS-Region B. vom asiatisch-pazifischen Raum (Indien) nach dem asiatisch-pazifischen Raum (Australien).

Eine Ausnahme beim Versand zwischen Ländern besteht zwischen Mitgliedsländern der Europäischen Union (EU). Für Datenübertragungen in den europäischen AWS Regionen versenden wir Geräte nur in die aufgeführten EU-Mitgliedsländer:

Österreich, Belgien, Bulgarien, Kroatien, Republik Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Italien, Irland, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien und Schweden.

Snowball Edge kann nur in dieselbe AWS Region zurückgegeben werden, in der die Geräte bestellt wurden.

Lieferungen im Inland innerhalb desselben Landes sind zulässig. Beispiele:

- Für Datenübertragungen in der Region Vereinigtes Königreich versenden wir Geräte im Inland innerhalb des Vereinigten Königreichs.
- Für Datenübertragungen im asiatisch-pazifischen Raum (Mumbai) versenden wir Geräte innerhalb Indiens.

 Note

AWS versendet Snowball Edge nicht an Postfächer.

Erste Schritte mit Snowball Edge

Mit einem AWS Snowball Edge Gerät können Sie AWS Cloud lokal und kostengünstig an Orten, an denen eine Verbindung zum Internet möglicherweise nicht möglich ist, auf die Speicher- und Rechenleistung des Geräts zugreifen. Sie können auch Hunderte von Terabyte oder Petabyte an Daten zwischen Ihren lokalen Rechenzentren und Amazon Simple Storage Service (Amazon S3) übertragen.

Im Folgenden finden Sie allgemeine Anweisungen zum Erstellen und Abschließen Ihres ersten AWS Snowball Edge Gerätejobs im Managementkonsole für die AWS Snow-Familie. In der Konsole sind die häufigsten Workflows enthalten, nach Auftragsarten getrennt. Weitere Informationen zu bestimmten Komponenten des AWS Snowball Edge Geräts finden Sie in dieser Dokumentation. Eine Übersicht über den Service insgesamt erhalten Sie unter [Wie AWS Snowball Edge funktioniert](#).

Es kann bis zu 4 Wochen dauern, bis der Snowball Edge bereitgestellt und für Ihren Job vorbereitet ist, bevor er versendet wird. Dieser Zeitplan sollte in Ihrem Projektplan berücksichtigt werden, um einen reibungslosen Übergang zu gewährleisten.

Bevor Sie beginnen können, müssen Sie in AWS Identity and Access Management (IAM) einen Administratorbenutzer AWS-Konto und einen Administratorbenutzer erstellen. Weitere Informationen finden Sie unter [Voraussetzungen für die Verwendung von Snowball Edge](#).

Themen

- [Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen](#)
- [Einen Auftrag stornieren, um einen Snowball Edge zu bestellen](#)
- [Einen Job klonen, um einen Snowball Edge in der Managementkonsole für die AWS Snow-Familie](#)
- [Erhalt des Snowball Edge](#)
- [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#)
- [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#)
- [Den Snowball Edge freischalten](#)
- [Lokale Benutzer auf einem Snowball Edge einrichten](#)
- [Das Snowball Edge-Gerät neu starten](#)
- [Snowball Edge ausschalten](#)
- [Rückgabe des Snowball Edge-Geräts](#)
- [Rückversand für Snowball Edge](#)

- [Überwachen des Importstatus vom Snowball Edge](#)
- [Sie erhalten den Abschlussbericht und die Protokolle Ihres Datenübertragungsauftrags](#)

Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen

Um ein Snowball Edge-Gerät zu bestellen, erstellen Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts in der Managementkonsole für die AWS Snow-Familie. Ein Job ist ein Begriff, der AWS verwendet wird, um den Lebenszyklus der Nutzung eines Snowball Edge-Geräts durch einen Kunden zu beschreiben. Ein Auftrag beginnt, wenn Sie ein Gerät bestellen, wird fortgesetzt, wenn das Gerät AWS vorbereitet und an Sie versendet wird und Sie es verwenden, und wird abgeschlossen, nachdem Sie das Gerät AWS erhalten und bearbeitet haben, nachdem Sie es zurückgesendet haben. Jobs sind nach Typ kategorisiert: Export, Import und lokale Datenverarbeitung und Speicherung. Weitere Informationen finden Sie unter [Grundlegendes zu AWS Snowball Edge-Jobs](#).

Nachdem Sie den Auftrag zur Bestellung eines Geräts erstellt haben, können Sie Managementkonsole für die AWS Snow-Familie den Auftragsstatus anzeigen und den Status des bestellten Geräts überwachen, während das Gerät für den Versand an Sie AWS vorbereitet wird und nach der Rücksendung. Weitere Informationen finden Sie unter [Jobstatus](#). Nachdem das Gerät zurückgegeben und von bearbeitet wurde AWS, können Sie über den Abschluss des Auftrags hinzugefügte Berichte und Protokolle zugreifen. Managementkonsole für die AWS Snow-Familie Weitere Informationen finden Sie unter [Abrufen Ihres Auftragsabschlussberichts und Ihrer Protokolle auf der Konsole](#).

Sie können Jobs auch mithilfe der Job-Management-API erstellen und verwalten. Weitere Informationen finden Sie in der [AWS Snowball Edge -API-Referenz](#).

Themen

- [Wählen Sie einen Jobtyp](#)
- [Wählen Sie Ihre Rechen- und Speicheroptionen](#)
- [Wählen Sie Ihre Funktionen und Optionen](#)
- [Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen](#)
- [Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job](#)

Wählen Sie einen Jobtyp

Der erste Schritt bei der Erstellung eines Jobs besteht darin, die Art des Jobs zu bestimmen, den Sie benötigen, und mit der Planung zu beginnen Managementkonsole für die AWS Snow-Familie.

Um Ihren Jobtyp auszuwählen

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#). Wenn Sie in diesem Bereich zum ersten Mal einen Job erstellen AWS-Region, wird die AWS Snowball Edge-Seite angezeigt. Andernfalls wird die Liste der vorhandenen Jobs angezeigt.
2. Wenn Sie zum ersten Mal ein Gerät bestellen möchten, wählen Sie AWS Snowball Edge-Gerät bestellen. Wenn Sie davon ausgehen, dass mehrere Jobs mehr als 500 TB an Daten migrieren, wählen Sie Create your large data migration plan more than 500 TB. Andernfalls wählen Sie in der linken Navigationsleiste Job erstellen. Wählen Sie „Nächster Schritt“, um die Seite „Job planen“ zu öffnen.
3. Geben Sie im Abschnitt Jobname im Feld Jobname einen Namen für Ihren Job ein.
4. Wählen Sie je nach Bedarf einen der folgenden Jobtypen aus:
 - In Amazon S3 importieren — Wählen Sie diese Option, um sich AWS ein leeres Snowball Edge-Gerät zusenden zu lassen. Sie verbinden das Gerät mit Ihrem lokalen Netzwerk und führen den Snowball Edge-Client aus. Sie kopieren Daten mit NFS Share oder dem S3-Adapter auf das Gerät, senden sie zurück an AWS und Ihre Daten werden hochgeladen. AWS
 - Aus Amazon S3 exportieren — Wählen Sie diese Option, um Daten aus Ihrem Amazon S3 S3-Bucket auf Ihr Gerät zu exportieren. AWS lädt Ihre Daten auf das Gerät und versendet sie an Sie. Sie verbinden das Gerät mit Ihrem lokalen Netzwerk und führen den Snowball Edge-Client aus. Sie kopieren Daten von Ihrem Gerät auf Ihre Server. Wenn Sie fertig sind, senden Sie das Gerät an AWS, und Ihre Daten werden vom Gerät gelöscht.
 - Nur lokale Datenverarbeitung und Speicherung — Führen Sie Rechen- und Speicher-Workloads auf dem Gerät aus, ohne Daten zu übertragen.

Choose a job type

☒ **Import into Amazon S3** [Info](#)

AWS will ship an empty device to you for storage and compute workloads. You'll transfer your data onto it, and ship it back. After AWS gets it, your data will be moved.

☐ **Export from Amazon S3** [Info](#)

Choose what data you want to export from your S3 buckets for storage and compute workloads. AWS will load that data onto a device and ship it to you. When you're done ship the device back for erasing.

☐ **Local compute and storage only** [Info](#)

Perform local compute and storage workloads without transferring data. You can order multiple devices in a cluster for increased durability and storage capacity. Includes rugged and rack-mountable devices.

5. Wählen Sie Next (Weiter), um fortzufahren.

Wählen Sie Ihre Rechen- und Speicheroptionen

Wählen Sie die Hardwarespezifikationen für Ihr Snowball Edge-Gerät aus, welche Ihrer EC2 Amazon-kompatiblen Instances darauf enthalten sein sollen, wie die Daten gespeichert werden und welche Preise gelten.

Um die Rechen- und Speicheroptionen Ihres Geräts auszuwählen

1. Wählen Sie im Bereich Schneegeräte das Snowball Edge-Gerät aus, das Sie bestellen möchten.

Note

Je nachdem, bei welchem Anbieter Sie bestellen und welchen Jobtyp AWS-Region Sie ausgewählt haben, sind einige Snowball Edge möglicherweise nicht verfügbar.

2. Wählen Sie im Abschnitt Wählen Sie Ihre Preisoption im Menü Wählen Sie Ihre Preisoption aus, welche Art von Preisgestaltung für diese Stelle gelten soll. Wenn Sie sich für ein Jahr oder 3 Jahre mit verbindlicher Vorauszahlung entscheiden, wählen Sie unter Automatische Verlängerung die Option An, um den Preis am Ende des aktuellen Zeitraums automatisch zu verlängern, oder Aus, um den Preis nicht automatisch zu verlängern, wenn der aktuelle Zeitraum

endet. Weitere Informationen zu langfristigen Preisoptionen für Snowball Edge-Geräte finden Sie unter [Langfristige Preisgestaltung für Snowball Edge-Geräte](#) in diesem Handbuch. [Die Gerätepreise für Ihr Gerät finden Sie AWS-Region unter AWS Snowball Edge Preise.](#)

3. Treffen Sie im Abschnitt Speichertyp auswählen eine Auswahl, die Ihren Anforderungen entspricht:
 - S3 Adapter: Verwenden Sie den S3-Adapter, um Daten mithilfe von Amazon S3 S3-REST-API-Aktionen programmgesteuert zu und von Snowball Edge zu übertragen.
 - Amazon S3 S3-kompatibler Speicher: Verwenden Sie Amazon S3 S3-kompatiblen Speicher, um S3-kompatiblen, dauerhaften, skalierbaren Objektspeicher auf einem einzelnen Snowball Edge-Gerät oder in einem Cluster mit mehreren Geräten bereitzustellen.
 - NFS-basierte Datenübertragung: Verwenden Sie die auf dem Network File System (NFS) basierende Datenübertragung, um Dateien per Drag-and-Drop von Ihrem Computer in Amazon S3 S3-Buckets auf Snowball Edge zu ziehen.

 Warning

Die NFS-basierte Datenübertragung unterstützt den S3-Adapter nicht. Wenn Sie mit der NFS-basierten Datenübertragung fortfahren, müssen Sie die NFS-Freigabe bereitstellen, um Objekte zu übertragen. Die Verwendung von AWS CLI zum Übertragen von Objekten schlägt fehl.

Weitere Informationen finden Sie [unter Verwenden von NFS für die Offline-Datenübertragung](#) im AWS Snowball Edge Edge-Entwicklerhandbuch.

 Note

Die verfügbaren Speichertyp-Optionen hängen vom Jobtyp und dem ausgewählten Snow-Gerät ab.

4. Wenn Sie S3 Adapter als Speichertyp ausgewählt haben oder wenn Sie ein Gerät ausgewählt haben, das Blockspeicher unterstützt, gehen Sie wie folgt vor, um einen oder mehrere S3-Buckets auszuwählen, die auf dem Gerät enthalten sein sollen:

- Führen Sie im Abschnitt Wählen Sie Ihre S3-Buckets aus einen oder mehrere der folgenden Schritte aus, um einen oder mehrere S3-Buckets auszuwählen:

1. Wählen Sie den S3-Bucket, den Sie verwenden möchten, in der Liste der S3-Bucket-Namen aus.
2. Geben Sie im Feld Nach einem Artikel suchen einen Bucketnamen ganz oder teilweise ein, um die Liste der verfügbaren Buckets nach Ihrem Eintrag zu filtern, und wählen Sie dann den Bucket aus.
3. Wählen Sie Neuen S3-Bucket erstellen, um einen neuen S3-Bucket zu erstellen. Der neue Bucket-Name wird in der Liste der Bucket-Namen angezeigt. Wählen Sie diese aus.

Sie können einen oder mehrere S3-Buckets hinzufügen. Diese Buckets werden auf Ihrem Gerät als lokale S3-Buckets angezeigt.

Select your S3 buckets [Info](#)

The S3 buckets you select will appear as directories on your device. Data stored in these buckets on the device will not be transferred to S3 on return.

Create a new S3 bucket

Q Search for an item

☐	S3 bucket name	Date created
☐	my-gobally-unique-bucket-name	3/15/2023, 5:20:20 PM EDT
☐	do-not-delete-gatedgarden-audit-669419309129	3/11/2023, 5:13:13 PM EST

5. Wenn Sie Amazon S3 S3-kompatiblen Speicher als Speichertyp ausgewählt haben, gehen Sie im Abschnitt S3-Speicherkapazität wie folgt vor:
 - a. Wählen Sie aus, ob Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem einzelnen Gerät oder einem Gerätecluster verwenden möchten. Weitere Informationen finden Sie [unter Verwenden eines AWS Snowball Edge Clusters](#) in diesem Handbuch.
 - b. Wählen Sie die Menge an Gerätespeicher aus, die für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwendet werden soll.

Note

Wenn Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden, können Sie Amazon S3 S3-Buckets verwalten und erstellen, nachdem Sie das Gerät erhalten

haben, sodass Sie sie nicht bei der Bestellung auswählen müssen. In diesem Handbuch finden Sie Informationen zu [Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#).

S3 storage capacity

Select device type

☒ Single device

☐ Cluster

Select storage amount

2.5 TB Single device ▼

Single device

Block storage: 41 TB

6. Wenn Sie NFS-basierte Datenübertragung als Speichertyp ausgewählt haben, führen Sie im Abschnitt Wählen Sie Ihre S3-Buckets einen oder mehrere der folgenden Schritte aus, um einen oder mehrere S3-Buckets auszuwählen:
 - a. Wählen Sie den S3-Bucket, den Sie verwenden möchten, in der Liste der S3-Bucket-Namen aus.
 - b. Geben Sie im Feld Nach einem Artikel suchen einen Bucketnamen ganz oder teilweise ein, um die Liste der verfügbaren Buckets nach Ihrem Eintrag zu filtern, und wählen Sie dann den Bucket aus.
 - c. Wählen Sie Neuen S3-Bucket erstellen, um einen neuen S3-Bucket zu erstellen. Der neue Bucket-Name wird in der Liste der Bucket-Namen angezeigt. Wählen Sie diese aus.
 - d. Nachdem Sie S3-Buckets für die NFS-Datenübertragung ausgewählt haben, wählen Sie auch einen S3-Bucket aus, für den Sie als Blockspeicher verwenden möchten. AMLs Sehen Sie sich die Schritte zur Auswahl eines Buckets an [S3](#).

Sie können einen oder mehrere S3-Buckets hinzufügen. Diese Buckets werden auf Ihrem Gerät als lokale S3-Buckets angezeigt.

Choose your NFS storage

These S3 buckets will appear on directories on your device. You can transfer data onto these buckets using NFS.

 Only data stored in these directories will be ingested to your S3 buckets in the cloud.

The NFS storage limit is 80 TB

Create a new S3 bucket

☐	S3 bucket name	Date created
☐	this-unique-bucket-name	6/14/2023, 12:20:08 PM EDT

- Wählen Sie im Abschnitt Compute EC2 using -compatible instances — optional Amazon EC2 - compatible AMIs aus Ihrem Konto aus, um es auf das Gerät aufzunehmen. Oder geben Sie in das Suchfeld den Namen eines AMI ganz oder teilweise ein, um die Liste der verfügbaren AMIs zu filtern, und wählen Sie dann das AMI aus.

Informationen zur Konfiguration eines AMI für Secure Shell (SSH) finden Sie unter [Konfiguration eines AMI für Snowball Edge](#) und SSH

Weitere Informationen finden Sie unter [Hinzufügen eines AMI bei der Bestellung Ihres Geräts](#) in diesem Handbuch.

Für diese Funktion fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS Snowball Edge – Preise](#).

- Klicken Sie auf die Schaltfläche Next.

Wählen Sie Ihre Funktionen und Optionen

Wählen Sie die Funktionen und Optionen aus, die Sie in Ihren AWS Snowball Edge-Geräteauftrag aufnehmen möchten, einschließlich Amazon EKS Anywhere for Snow, einer AWS IoT Greengrass Instance und Funktionen zur Remote-Geräteverwaltung.

Um Ihre Funktionen und Optionen auszuwählen

- Wählen Sie im Abschnitt Amazon EKS Anywhere on AWS Snow die Option Amazon EKS Anywhere on AWS Snow einbeziehen aus, um Amazon EKS Anywhere on Snow einzubeziehen, und gehen Sie dann wie folgt vor.

 Note

Wir empfehlen Ihnen, Ihren Kubernetes-Cluster mit der neuesten verfügbaren Kubernetes-Version zu erstellen, die von Amazon EKS Anywhere unterstützt wird. Weitere Informationen finden Sie unter [Amazon EKS-Anywhere Versioning](#). Wenn Ihre Anwendung eine bestimmte Version von Kubernetes erfordert, verwenden Sie eine beliebige Version von Kubernetes, die im Standard- oder erweiterten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten der Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust der Unterstützung für die Version von Kubernetes, die Sie verwenden möchten, vermeiden. Weitere Informationen finden Sie im [Amazon EKS Kubernetes-Veröffentlichungskalender](#).

- a. Wählen Sie im Abschnitt Erstellen Sie Ihr eigenes AMI das aus, das AMIs Sie für Amazon EKS Anywhere erstellt haben. Siehe [Vor der Bestellung eines Snowball Edge-Geräts für Amazon EKS Anywhere on AWS Snow auszuführende Aktionen](#).
- b. Um Amazon EKS Anywhere Anywhere-Cluster auf mehreren Snowball Edge-Geräten zu betreiben, wählen Sie im Abschnitt Hochverfügbarkeit die Anzahl der Geräte aus, die in Ihrer Bestellung enthalten sein sollen.
2. Um ein validiertes AMI für IoT-Workloads hinzuzufügen, wählen Sie im Abschnitt AWS IoT Greengrass On Snow die Option AWS IoT Greengrass Validiertes AMI auf meinem Snow-Gerät installieren aus.
3. Um die Fernverwaltung Ihres Snowball Edge-Geräts durch AWS OpsHub oder den Snowball Edge-Client zu aktivieren, wählen Sie Ihr Snow-Gerät remote verwalten mit AWS OpsHub oder Snowball Edge Client aus.
4. Wählen Sie die Schaltfläche Weiter.

Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen

Themen

- [Wählen Sie die Sicherheitseinstellungen für Snowball Edge](#)

- [Wählen Sie Ihre Versandpräferenzen für den Empfang und die Rücksendung des Snowball Edge](#)
- [Wählen Sie Einstellungen für Benachrichtigungen über den Snowball Edge-Job](#)

Wählen Sie die Sicherheitseinstellungen für Snowball Edge

Durch die Einstellung der Sicherheit werden die Berechtigungen und Verschlüsselungseinstellungen für Ihren AWS Snowball Edge-Job hinzugefügt, um Ihre Daten während der Übertragung zu schützen.

Um die Sicherheit für Ihren Job festzulegen

1. Wählen Sie im Abschnitt Verschlüsselung den KMS-Schlüssel aus, den Sie verwenden möchten.
 - Wenn Sie den Standardschlüssel AWS Key Management Service (AWS KMS) verwenden möchten, wählen Sie AWS/importexport (Standard). Dies ist der Standardschlüssel, der Ihre Import- und Exportaufträge schützt, wenn kein anderer Schlüssel definiert ist.
 - Wenn Sie Ihren eigenen AWS KMS Schlüssel angeben möchten, wählen Sie Einen Schlüssel-ARN eingeben, geben Sie den Amazon-Ressourcennamen (ARN) in das Schlüssel-ARN-Feld ein und wählen Sie Diesen KMS-Schlüssel verwenden aus. Der Schlüssel ARN wird der Liste hinzugefügt.
2. Führen Sie im Abschnitt Servicezugriffstyp auswählen einen der folgenden Schritte aus:
 - Die Konsole „Choose Snow“ erstellt und verwendet eine serviceverknüpfte Rolle, um in Ihrem Namen auf AWS Ressourcen zuzugreifen. um AWS Snowball Edge die Erlaubnis zu erteilen, Amazon S3 und Amazon Simple Notification Service (Amazon SNS) in Ihrem Namen zu nutzen. Die Rolle gewährt dem Snow-Service AssumeRole Vertrauen in den AWS Security Token Service (AWS STS)
 - Wählen Sie Zu verwendende bestehende Servicerolle hinzufügen aus, um den gewünschten Rollen-ARN anzugeben, oder Sie können die Standardrolle verwenden.
3. Wählen Sie Weiter aus.

Wählen Sie Ihre Versandpräferenzen für den Empfang und die Rücksendung des Snowball Edge

Der Empfang und die Rückgabe eines Snowball Edge-Geräts beinhalten den Hin- und Rückversand des Geräts. Daher ist es wichtig, dass Sie genaue Versandinformationen angeben.

Um Versanddetails bereitzustellen

1. Wählen Sie im Abschnitt Lieferadresse eine bestehende Adresse aus oder fügen Sie eine neue Adresse hinzu.
 - Wenn Sie Letzte Adresse verwenden wählen, werden die hinterlegten Adressen angezeigt. Wählen Sie die gewünschte Adresse sorgfältig aus der Liste aus.
 - Wenn Sie Neue Adresse hinzufügen wählen, geben Sie die angeforderten Adressinformationen ein. Das Managementkonsole für die AWS Snow-Familie speichert Ihre neuen Versandinformationen.

Note

Das Land, das Sie in der Adresse angeben, muss mit dem Zielland des Geräts übereinstimmen und für dieses Land gültig sein.

2. Wählen Sie im Abschnitt Versandgeschwindigkeit eine Versandgeschwindigkeit für den Auftrag aus. Die Versandgeschwindigkeit gibt nicht an, wie schnell Sie ab dem Tag, an dem Sie den Auftrag erstellt haben, mit dem Erhalt des Geräts rechnen können. Sie gibt vielmehr die Uhrzeit an, zu der sich das Gerät auf dem Transportweg zwischen AWS und Ihrer Lieferadresse befindet.

Es kann bis zu 4 Wochen dauern, bis das Gerät bereitgestellt und für Ihre Arbeit vorbereitet ist, bevor es versendet wird. Dieser Zeitplan sollte in Ihrem Projektplan berücksichtigt werden, um einen reibungslosen Übergang zu gewährleisten.

Die Versandgeschwindigkeiten, die Sie wählen können, sind:

- Versand innerhalb eines Tages (1 Werktag)
- Zweitägiger Versand (2 Arbeitstage)

Wählen Sie Einstellungen für Benachrichtigungen über den Snowball Edge-Job

Benachrichtigungen informieren Sie über den neuesten Status Ihrer AWS Snowball Edge-Jobs. Sie erstellen ein SNS-Thema und erhalten E-Mails von Amazon Simple Notification Service (Amazon SNS), wenn sich Ihr Jobstatus ändert.

Richten Sie Benachrichtigungen wie folgt ein

- Führen Sie im Abschnitt Benachrichtigungen einrichten eine der folgenden Aktionen aus:
 - Wenn Sie ein vorhandenes SNS-Thema verwenden möchten, wählen Sie Bestehendes SNS-Thema verwenden und wählen Sie das Thema Amazon Resource Name (ARN) aus der Liste aus.
 - Wenn Sie ein neues SNS-Thema erstellen möchten, wählen Sie Neues SNS-Thema erstellen. Geben Sie einen Namen für Ihr Thema ein und geben Sie eine E-Mail-Adresse ein.

Note

Aufträge zur Bestellung von Snow-Geräten, die in den Regionen USA West (Nordkalifornien) und USA West (Oregon) hergestellt wurden, werden über die Region USA Ost (Nord-Virginia) weitergeleitet. Aus diesem Grund werden Serviceanrufe wie Amazon SNS auch über den Osten der USA (Nord-Virginia) geleitet. Wir empfehlen, alle neuen SNS-Themen in der Region USA Ost (Nord-Virginia) zu erstellen, um ein optimales Erlebnis zu erzielen.

Die Benachrichtigungen beziehen sich auf einen der folgenden Status Ihres Jobs:

- Job created
- Vorbereitung des Geräts
- Preparing shipment
- In transit to you
- Delivered to you
- Auf dem Weg nach AWS
- Im Sortierzentrum
- Bei AWS
- Importing
- Completed
- Canceled

Weitere Informationen zu Benachrichtigungen über Jobstatusänderungen und Themen zu verschlüsselten SNS-Themen finden Sie unter [Benachrichtigungen für Snowball Edge](#) in diesem Handbuch.

Wählen Sie „Weiter“.

Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job

Nachdem Sie alle erforderlichen Informationen für Ihren AWS Snowball Edge-Job angegeben haben, überprüfen Sie den Job und erstellen Sie ihn. Nachdem Sie den Auftrag erstellt haben, AWS wird mit der Vorbereitung des Snowball Edge für den Versand an Sie begonnen.

Jobs unterliegen in bestimmten Ländern den Exportkontrollgesetzen und erfordern möglicherweise eine Exportlizenz. Es gelten auch die Export- und Reexportgesetze der USA. Abweichungen von den Gesetzen und Vorschriften des Landes und der USA sind verboten.

1. Überprüfen Sie auf der Seite mit der Jobübersicht alle Abschnitte, bevor Sie den Job erstellen. Wenn Sie Änderungen vornehmen möchten, wählen Sie Bearbeiten für den entsprechenden Abschnitt und bearbeiten Sie die Informationen.
2. Wenn Sie mit der Überprüfung und Bearbeitung fertig sind, wählen Sie Job erstellen.

Note

Nachdem Sie einen Job zur Bestellung eines Snowball Edge-Geräts erstellt haben, können Sie ihn stornieren, solange er sich im Status Auftrag erstellt befindet, ohne dass Gebühren anfallen. Weitere Informationen finden Sie unter [Stornieren eines](#) Jobs über den Managementkonsole für die AWS Snow-Familie

Nachdem Ihr Job erstellt wurde, können Sie den Status des Jobs im Abschnitt Jobstatus sehen. Ausführliche Informationen zum Jobstatus finden Sie unter [Jobstatus](#).

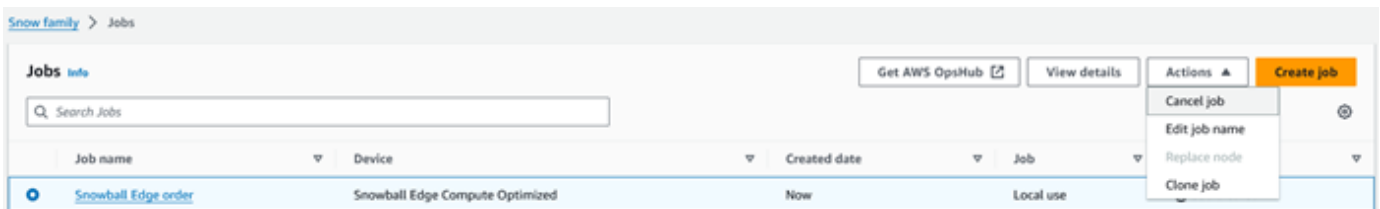
Einen Auftrag stornieren, um einen Snowball Edge zu bestellen

Nachdem Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellt haben, können Sie den Auftrag über den Managementkonsole für die AWS Snow-Familie stornieren. Wenn Sie den Auftrag stornieren, erhalten Sie das bestellte Gerät nicht. Sie können den Job nur stornieren, solange

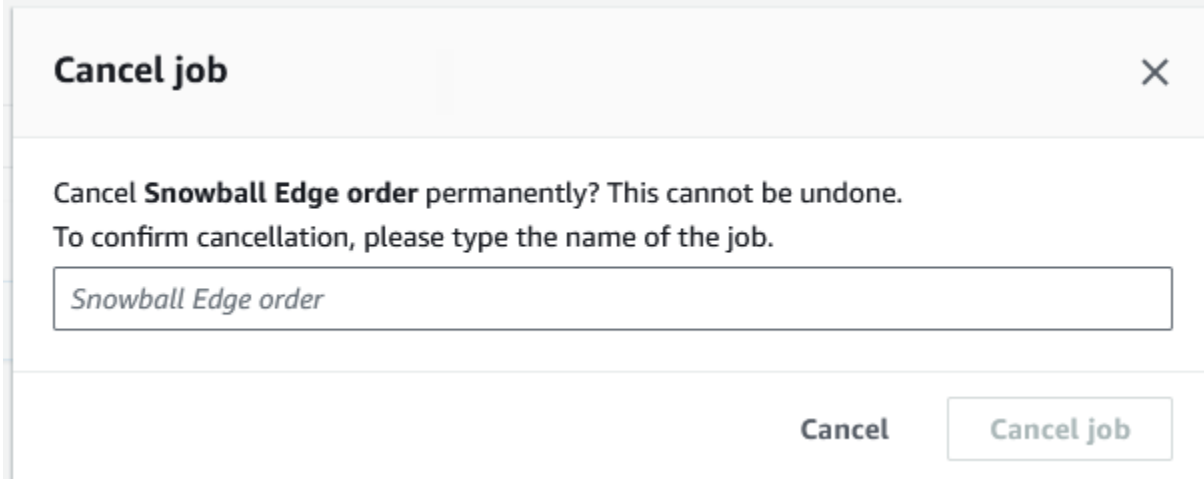
der Jobstatus Job created lautet. Sobald der Job diesen Status überschritten hat, können Sie ihn nicht mehr stornieren. Weitere Informationen finden Sie unter [Jobstatus](#).

Wenn Sie einen Job stornieren, während er sich im Status Job created befindet, wird Ihnen das Snowball Edge-Gerät nicht in Rechnung gestellt. Die Abrechnung beginnt erst, nachdem das Gerät vorbereitet und an Sie versandt wurde.

1. Melden Sie sich bei den [Managementkonsole für die AWS Snow-Familie](#) an.
2. Wählen Sie den Job aus, den Sie stornieren möchten.
3. Wählen Sie Aktionen. Wählen Sie im daraufhin angezeigten Menü die Option Auftrag stornieren aus.



4. Das Fenster „Auftrag stornieren“ wird angezeigt. Um das Abbrechen des Jobs zu bestätigen, geben Sie den ein **job name** und wählen Sie Job stornieren. In der Liste der Jobs wird in der Spalte Status der Eintrag Storniert angezeigt.



Einen Job klonen, um einen Snowball Edge in der Managementkonsole für die AWS Snow-Familie

Wenn Sie zum ersten Mal einen Importauftrag oder einen lokalen Rechen- und Speicherauftrag erstellen, stellen Sie möglicherweise fest, dass Sie mehr als ein AWS Snowball Edge Gerät

benötigen. Da Importaufträge und lokale Datenverarbeitungs- und Speicheraufträge einem einzelnen Gerät zugeordnet sind, bedeutet dies, dass Sie mehr als einen Auftrag erstellen müssen, wenn Sie mehrere Geräte benötigen. Zum Erstellen zusätzlicher Aufträge können Sie wieder den Assistenten in der Konsole verwenden oder einen vorhandenen Auftrag klonen.

Note

Das Klonen eines Auftrags ist ein in der Konsole verfügbarer Schnellzugang, der das Erstellen zusätzlicher Aufträge vereinfacht. Wenn Sie Aufträge mit der API zur Auftragsverwaltung erstellen, können Sie einfach den Befehl zur Auftragserstellung erneut ausführen.

Das Klonen eines Jobs bedeutet, ihn exakt neu zu erstellen, mit Ausnahme eines automatisch geänderten Namens. Das Klonen ist ein einfacher Vorgang.

So klonen Sie einen Auftrag in der Konsole

1. Wählen Sie in der Managementkonsole für die AWS Snow-Familie Ihren Job aus der Tabelle aus.
2. Wählen Sie für Actions (Aktionen) die Option Clone job (Auftrag klonen).

Der Create job-Assistent wird auf der Seite Step 6: Review (letzte Seite) geöffnet.

3. Überprüfen Sie die Informationen und nehmen Sie ggf. Änderungen durch Auswahl der entsprechenden Schaltfläche Edit (Bearbeiten) vor.
4. Erstellen Sie den geklonten Auftrag mit Create job (Auftrag erstellen).

Geklonte Jobs werden im Format **Job Name**-clone- benannt. *number* Die Nummer wird automatisch an den Auftragsnamen angehängt und gibt an, wie oft Sie diesen Auftrag nach dem ersten Klonen erneut geklont haben. Beispielsweise steht AprilFinanceReports-clone für den ersten geklonten AprilFinanceReportsJob des Jobs und DataCenterMigration-clone-42 für den zweiundvierzigsten Klon des Jobs. DataCenterMigration

Erhalt des Snowball Edge

Wenn Sie das AWS Snowball Edge Gerät erhalten, stellen Sie möglicherweise fest, dass es nicht in einer Box geliefert wird. Das Gerät ist selbst ein robuster Transportbehälter. Nachdem Sie das

Gerät erhalten haben, sollten Sie nach Beschädigungen und offensichtlichen Manipulationen suchen. Wenn Ihnen am Gerät irgendetwas Verdächtiges auffällt, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie sich stattdessen an die [AWS Support](#) und informieren Sie sie über das Problem, damit Ihnen ein neues Gerät zugeschickt werden kann.

 Important

Das AWS Snowball Edge Gerät ist Eigentum von AWS. Die Manipulation eines AWS Snowball Edge Geräts stellt einen Verstoß gegen die AWS Nutzungsbedingungen dar. Weitere Informationen finden Sie unter [AWS Nutzungsbedingungen](#).

Das Gerät sieht aus wie in der folgenden Abbildung gezeigt.



Wenn Sie dazu bereit sind, das Gerät mit Ihrem internen Netzwerk zu verbinden, fahren Sie mit dem nächsten Abschnitt fort.

Weiter: [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#)

Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden

Mit dem folgenden Verfahren verbinden Sie das AWS Snowball Edge Gerät mit Ihrem lokalen Netzwerk. Das Gerät muss nicht mit dem Internet verbunden sein. Das Gerät hat drei Türen: eine Vordertür, eine Hintertür und eine Oberseite.

So verbinden Sie das Gerät mit dem Netzwerk

1. Öffnen Sie die vordere und hintere Klappe, indem Sie diese in die dafür vorgesehenen Schlitze im Gerät schieben. So erhalten Sie Zugang zum Touchscreen auf dem LCD-Display, das in die Front des Gerät eingelassen ist, und auf die Strom- und Netzwerkanschlüsse auf der Rückseite.

Note

Schließen Sie nicht die Vorder- und Hintertüren, während Sie das Snowball Edge-Gerät verwenden. Durch die geöffneten Türen kann das Gerät mit Luft gekühlt werden. Das Schließen der Türen während der Verwendung des Geräts kann dazu führen, dass das Gerät heruntergefahren wird, um eine Überhitzung zu vermeiden.

2. Öffnen Sie die obere Klappe. Nehmen Sie das mitgelieferte Stromkabel aus der Halterung und schließen Sie das Gerät an die Stromversorgung an.
3. Wählen Sie eines Ihrer RJ45 SFP+- oder QSFP+-Netzwerkkabel und schließen Sie das Gerät an Ihr Netzwerk an. Die Netzwerkanschlüsse befinden sich an der Rückseite des Geräts.
4. Schalten Sie das AWS Snowball Edge Gerät ein, indem Sie den Netzschalter über dem LCD-Display drücken.
5. Wenn das Gerät bereit ist, wird auf der LCD-Anzeige ein kurzes Video angezeigt, während das Gerät für den Start vorbereitet wird. Nach etwa 10 Minuten kann das Gerät entsperrt werden.
6. (Optional) Sie können die Standardnetzwerkeinstellungen über das LCD-Display ändern, indem Sie CONNECTION (VERBINDUNG) auswählen.

Im Folgenden wird erläutert, wie Sie Ihre IP-Adresse durch eine andere statische Adresse ersetzen können, die Sie mit dem folgenden Verfahren angeben.

Informationen zur Behebung von Startproblemen finden Sie unter [Behebung von Startproblemen mit Snowball Edge](#).

So ändern Sie die IP-Adresse eines Geräts AWS Snowball Edge

1. Wählen Sie auf dem LCD-Display CONNECTION (VERBINDUNG).

Es wird ein Bildschirm mit den aktuellen Netzwerkeinstellungen für das AWS Snowball Edge Gerät angezeigt. Die IP-Adresse unter dem Dropdown-Feld wird automatisch aktualisiert, sodass sie die vom AWS Snowball Edge Gerät angeforderte DHCP-Adresse wiedergibt.

2. (Optional) Ändern Sie die IP-Adresse in eine statische IP-Adresse. Sie können sie auch beibehalten.

Das Gerät ist mit dem Netzwerk verbunden.

 Important

Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie das AWS Snowball Edge Gerät nicht vom Computer und ändern Sie nicht die Verbindungseinstellungen, während es verwendet wird.

Weiter: [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#)

Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen

Jeder Job hat eine Reihe von Anmeldeinformationen, die Sie von der Managementkonsole für die AWS Snow-Familie oder der Job-Management-API abrufen müssen, um Ihren Zugriff auf Snowball Edge zu authentifizieren. Bei diesen Anmeldeinformationen handelt es sich um eine verschlüsselte Manifestdatei und einen zugehörigen Entsperrcode. Die Manifestdatei enthält wichtige Informationen zu dem Auftrag und zu den damit verbundenen Berechtigungen.

 Note

Sie erhalten Ihre Anmeldeinformationen, nachdem das Gerät zu Ihnen übertragen wurde. Sie können den Status Ihres Jobs in der sehen Managementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter [Status von Snowball Edge-Jobs](#).

Um Ihre Anmeldeinformationen über die Konsole abzurufen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#).
2. Suchen Sie auf der Konsole in der Tabelle nach dem spezifischen Job, für den Sie das Auftragsmanifest herunterladen möchten, und wählen Sie dann diesen Job aus.
3. Erweitern Sie den Bereich Jobstatus und wählen Sie Jobdetails anzeigen aus.

4. Erweitern Sie im angezeigten Detailbereich die Option Credentials (Anmeldeinformationen) und führen Sie dann die folgenden Schritte aus:
 - Notieren Sie sich den Entsperrcode (einschließlich der Bindestriche), da Sie alle 29 Zeichen eingeben müssen, um das Gerät zu entsperren.
 - Wählen Sie im Dialogfeld die Option Manifest herunterladen aus und folgen Sie den Anweisungen, um die Job-Manifest-Datei auf Ihren Computer herunterzuladen. Der Name Ihrer Manifestdatei enthält Ihre Job ID (Auftrags-ID).

Note

Es wird empfohlen, keine Kopie des Entsperrcodes an derselben Stelle auf dem Computer zu speichern wie das Manifest für diesen Job. Weitere Informationen finden Sie unter [Bewährte Methoden für die Verwendung eines Snowball Edge-Geräts](#).

Nachdem Sie Ihre Anmeldeinformationen haben, müssen Sie im nächsten Schritt den Snowball Edge-Client herunterladen, mit dem das AWS Snowball Edge Gerät entsperrt wird.

Weiter: [Den Snowball Edge-Client herunterladen und installieren](#)

Den Snowball Edge freischalten

In diesem Abschnitt wird das Entsperren des Snowball Edge-Geräts mithilfe des Snowball Edge-Clients beschrieben. Informationen zum Entsperren des Geräts mithilfe AWS OpsHub eines grafischen Benutzeroberflächentools (GUI) für Snowball Edge finden Sie unter Gerät [entsperren Gerät](#) .

Bevor Sie ein Snowball Edge-Gerät zum Übertragen von Daten oder zum Ausführen von Edge-Computing-Aufgaben verwenden können, müssen Sie das Gerät entsperren. Wenn Sie das Gerät entsperren, authentifizieren Sie Ihre Zugriffsfähigkeit, indem Sie zwei Arten von Anmeldeinformationen angeben: einen 29-stelligen Entsperrcode und eine Manifestdatei. Nachdem Sie das Gerät entsperrt haben, können Sie das Gerät weiter konfigurieren, Daten dorthin oder vom Gerät verschieben, EC2 Amazon-kompatible Instances einrichten und verwenden und vieles mehr.

Bevor Sie ein Gerät entsperren, muss es an die Stromversorgung und das Netzwerk angeschlossen, eingeschaltet und eine IP-Adresse zugewiesen werden. Weitere Informationen finden Sie unter [Einen](#)

[Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#) . Sie benötigen die folgenden Informationen zum Snowball Edge-Gerät:

- Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Den Snowball Edge-Client herunterladen und installieren](#).
- Holen Sie sich die Anmeldeinformationen von der Managementkonsole für die AWS Snow-Familie. Für ein oder mehrere eigenständige Geräte die Entsperrcodes und die Manifestdatei für jeden Snowball Edge. Für einen Cluster von Snowball Edge-Geräten der eine Entsperrcode und eine Manifestdatei für den Cluster. Weitere Informationen zum Herunterladen von Anmeldeinformationen finden Sie unter [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#).
- Schalten Sie jedes Gerät ein und verbinden Sie es mit Ihrem Netzwerk. Weitere Informationen finden Sie unter [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#).

So entsperren Sie ein eigenständiges Gerät mit dem Snowball Edge Client

1. Suchen Sie die IP-Adresse für das AWS Snowball Edge Gerät auf dem LCD-Display des AWS Snowball Edge Geräts unter der Registerkarte Verbindungen. Notieren Sie die IP-Adresse.
2. Verwenden Sie den `unlock-device` Befehl, um Ihren Zugriff auf Snowball Edge mit der IP-Adresse von Snowball Edge und Ihren Anmeldeinformationen wie folgt zu authentifizieren.

```
snowballEdge unlock-device --endpoint https://ip-address-of-device --manifest-file /Path/to/manifest/file.bin --unlock-code 29-character-unlock-code
```

Das Gerät gibt mit der folgenden Meldung an, dass es erfolgreich entsperrt wurde.

```
Your Snowball Edge device is unlocking. You may determine the unlock state of your device using the describe-device command. Your Snowball Edge device will be available for use when it is in the UNLOCKED state.
```

Wenn der Befehl zurückkehrt `connection refused`, finden Sie weitere Informationen unter [Problembehebung beim Entsperren eines Snowball Edge](#).

Example des **unlock-device** Befehls

In diesem Beispiel lautet die IP-Adresse für das Gerät `192.0.2.0`, der Name der Manifestdatei ist `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` und der 29-stellige Entsperrcode lautet `12345-abcde-12345-ABCDE-12345`.

```
snowballEdge unlock-device --endpoint https://192.0.2.0 --manifest-file /
Downloads/JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin /
--unlock-code 12345-abcde-12345-ABCDE-12345
```

So entsperren Sie einen Cluster von Snowball Edge-Geräten mit dem Snowball Edge-Client

1. Suchen Sie die IP-Adressen der einzelnen Geräte im Cluster auf dem LCD-Display jedes AWS Snowball Edge Geräts auf der Registerkarte Verbindungen. Notieren Sie sich die IP-Adressen.
2. Verwenden Sie den `snowballEdge unlock-cluster` Befehl, um Ihren Zugriff auf den AWS Snowball Edge Gerätecluster anhand der IP-Adresse eines der Geräte im Cluster, Ihren Anmeldeinformationen und den IP-Adressen aller Geräte im Cluster wie folgt zu authentifizieren.

```
snowballEdge unlock-cluster --endpoint https://ip-address-of-device --manifest-
file Path/to/manifest/file.bin --unlock-code 29-character-unlock-code --device-ip-
addresses ip-address-of-cluster-device-1 ip-address-of-cluster-device-2 ip-address-
of-cluster-device-3
```

Der Gerätecluster gibt mit der folgenden Meldung an, dass er erfolgreich entsperrt wurde.

```
Your Snowball Edge Cluster is unlocking. You may determine the unlock state of your
cluster using the describe-cluster command. Your Snowball Edge Cluster will be
available for use when your Snowball Edge devices are in the UNLOCKED state.
```

Wenn der Befehl zurückkehrt `connection refused`, finden Sie weitere Informationen unter [Problembehebung beim Entsperren eines Snowball Edge](#).

Example des **unlock-cluster** Befehls

In diesem Beispiel für einen Cluster mit fünf Geräten lautet die IP-Adresse für eines der Geräte im Cluster, der Name der Manifestdatei lautet `192.0.2.0JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin`, und der 29-stellige Entsperrcode lautet `12345-abcde-12345-ABCDE-12345`.

```
snowballEdge unlock-cluster --endpoint https://192.0.2.0 --manifest-file /
Downloads/JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin /

--unlock-code 12345-abcde-12345-ABCDE-12345 --device-ip-addresses 192.0.2.0
192.0.2.1 192.0.2.2 192.0.2.3 192.0.2.4
```

Problembehebung beim Entsperren eines Snowball Edge

Wenn der `unlock-device` Befehl zurückgegeben wird `connection refused`, haben Sie möglicherweise die Befehlssyntax falsch eingegeben, oder die Konfiguration Ihres Computers oder Netzwerks verhindert möglicherweise, dass der Befehl das Snow-Gerät erreicht. Ergreifen Sie die folgenden Maßnahmen, um das Problem zu lösen:

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.
 - a. Überprüfen Sie anhand des LCD-Bildschirms des Geräts, ob die im Befehl verwendete IP-Adresse korrekt ist.
 - b. Stellen Sie sicher, dass der Pfad zur im Befehl verwendeten Manifestdatei korrekt ist, einschließlich des Dateinamens.
 - c. Verwenden Sie die [AWS Snowball Edge Management Console](#), um zu überprüfen, ob der im Befehl verwendete Entsperrcode korrekt ist.
2. Stellen Sie sicher, dass sich der Computer, den Sie verwenden, im selben Netzwerk und Subnetz wie das Snow-Gerät befindet.
3. Stellen Sie sicher, dass der Computer, den Sie verwenden, und das Netzwerk so konfiguriert sind, dass der Zugriff auf das Snow-Gerät möglich ist. Ermitteln Sie anhand des `ping` Befehls für Ihr

Betriebssystem, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen der Antivirensoftware, der Firewall-Konfiguration, des virtuellen privaten Netzwerks (VPN) oder anderer Konfigurationen Ihres Computers und Netzwerks.

Jetzt können Sie mit der Verwendung von Snowball Edge beginnen.

Weiter: [Lokale Benutzer auf einem Snowball Edge einrichten](#)

Lokale Benutzer auf einem Snowball Edge einrichten

Im Folgenden finden Sie die Schritte zum Einrichten eines lokalen Administrators auf Ihrem AWS Snowball Edge Gerät.

1. Abruf der Stammbenutzer-Anmeldeinformationen

Verwenden Sie die `snowballEdge list-access-keys` und den `snowballEdge get-secret-access-key`, um die lokalen Anmeldeinformationen abzurufen. Weitere Informationen finden Sie unter [Anmeldeinformationen für einen Snowball Edge abrufen](#).

2. Konfigurierung der Stammbenutzer-Anmeldeinformationen mithilfe von **aws configure**

Geben Sie AWS Access Key ID, AWS Secret Access Key und Default region name ein. Der Name der Region muss snow sein. Geben Sie optional ein Default output format ein. Weitere Informationen zur Konfiguration von finden Sie unter [Konfiguration von AWS CLI im AWS Command Line Interface](#) Benutzerhandbuch. AWS CLI

3. Erstellung eines oder mehrerer lokaler Benutzer auf Ihrem Gerät

Mit dem Befehl `create-user` können Sie Ihrem Gerät Benutzer hinzufügen.

```
aws iam create-user --endpoint endpointIPAddress:6078 --region snow --user-name UserName --profile ProfileID
```

Nachdem Sie Benutzer entsprechend Ihren Geschäftsanforderungen hinzugefügt haben, können Sie Ihre AWS Root-Anmeldeinformationen an einem sicheren Ort speichern und sie nur für Konto- und Dienstverwaltungsaufgaben verwenden. Weitere Informationen zum Erstellen von IAM-Benutzern finden Sie unter [Erstellen eines IAM-Benutzers in Ihrem AWS-Konto](#) im IAM-Benutzerhandbuch.

4. Erstellung eines Zugriffsschlüssels für Ihren Benutzer

Warning

Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Die Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Zugriffsschlüssel aktualisieren](#).

Mit dem Befehl `create-access-key` können Sie einen Zugriffsschlüssel für Ihren Benutzer erstellen.

```
aws iam create-access-key --endpoint endpointIPAddress:6078 --region snow --user-name UserName --profile ProfileID
```

Speichern Sie die Zugriffsschlüsseldaten in einer Datei und verteilen Sie diese an Ihre Benutzer.

5. Erstellung einer -Zugriffsrichtlinie

Möglicherweise möchten Sie, dass verschiedene Benutzer verschiedene Zugriffsstufen für die Funktionalität auf Ihrem Gerät besitzen. Im folgenden Beispiel wird ein Richtliniendokument mit dem Namen `s3-only-policy` erstellt und an einen Benutzer angefügt.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

```
}
```

```
aws iam create-policy --endpoint endpointIPAddress:6078 --region snow --policy-name  
s3-only-policy --policy-document file://s3-only-policy --profile ProfileID
```

6. Anfügung der Richtlinie an Ihren Benutzer

Mit `attach-user-policy` können Sie die `s3-only-policy` an einen Benutzer anfügen.

```
aws iam attach-user-policy --endpoint endpointIPAddress:6078 --region snow  
--user-name UserName --policy-arn arn:aws:iam::AccountID:policy/POLICYNAME --  
profile ProfileID
```

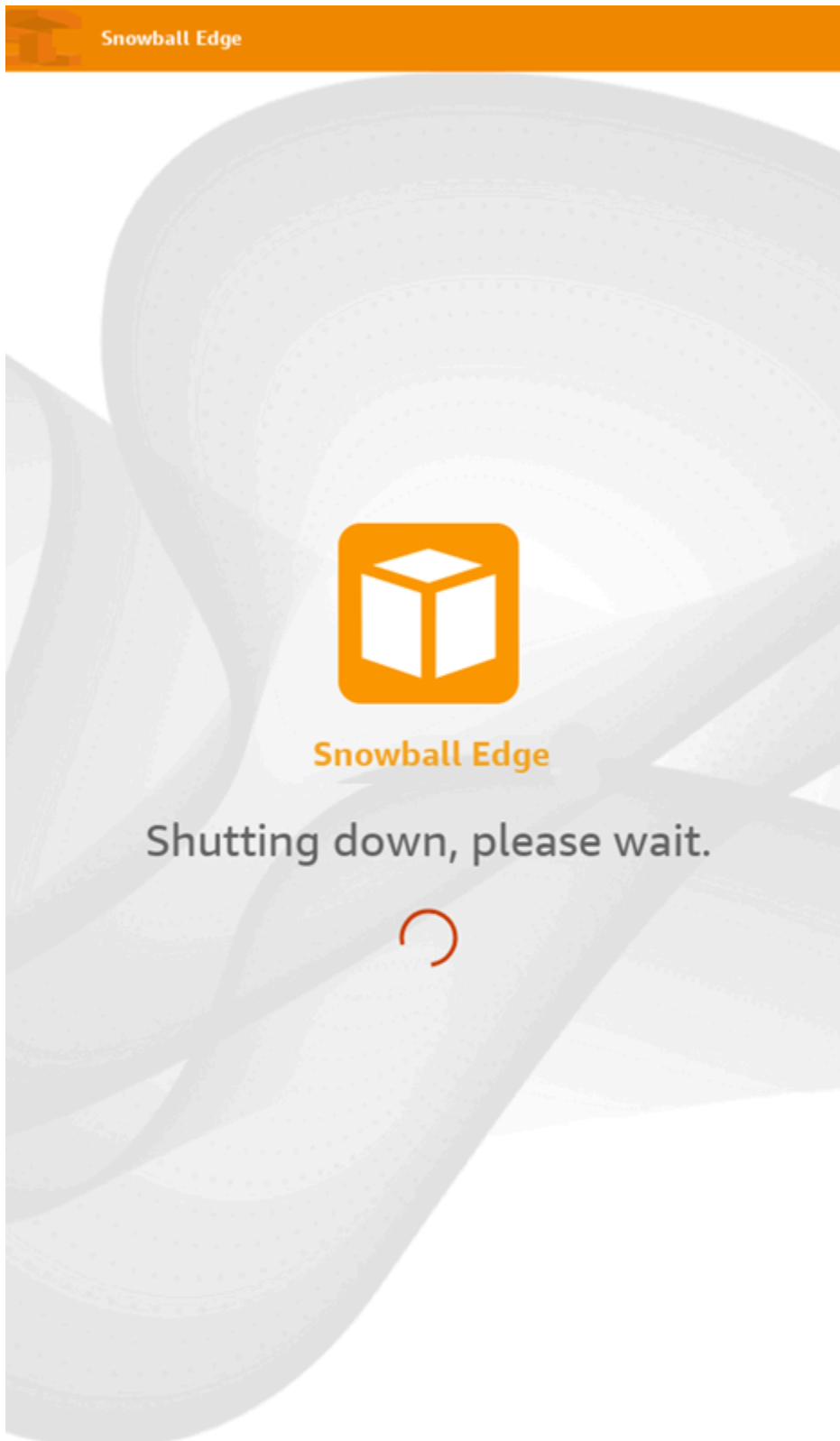
Weitere Informationen zur lokalen Verwendung von IAM finden Sie unter. [Lokales Verwenden von IAM auf einem Snowball Edge](#)

Das Snowball Edge-Gerät neu starten

Bevor Sie ein Snowball Edge-Gerät neu starten, stellen Sie sicher, dass die gesamte Datenübertragung zum Gerät gestoppt wurde.

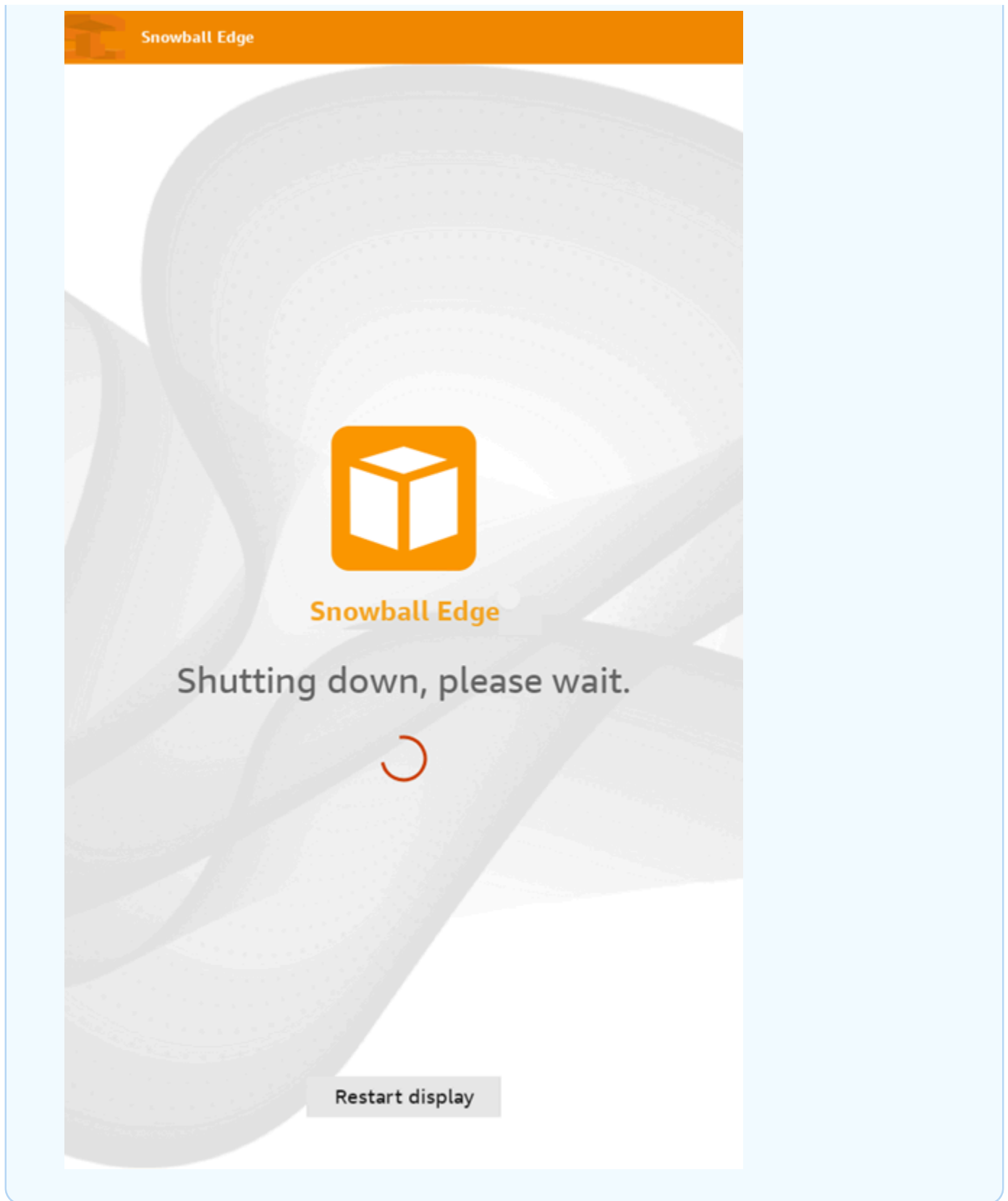
Um das Gerät mit dem Netzschalter neu zu starten:

1. Wenn die gesamte Kommunikation mit dem Gerät beendet ist, schalten Sie es aus, indem Sie den Netzschalter über dem LCD-Bildschirm drücken. Das Herunterfahren des Geräts dauert ca. 20 Sekunden. Während das Gerät heruntergefahren wird, wird auf dem LCD-Bildschirm eine Meldung angezeigt, die darauf hinweist, dass das Gerät heruntergefahren wird.



 Note

Wenn auf dem LCD-Bildschirm die Meldung zum Herunterfahren angezeigt wird, obwohl das Gerät nicht wirklich heruntergefahren wird, drücken Sie auf dem Bildschirm die Taste Display neu starten, um den Bildschirm wieder in den Normalbetrieb zu versetzen.



2. Drücken Sie den Betriebsschalter. Wenn das Gerät bereit ist, wird auf der LCD-Anzeige ein kurzes Video angezeigt, während das Gerät für den Start vorbereitet wird. Nach etwa 10 Minuten kann das Gerät entsperrt werden.
3. Entsperren Sie das Gerät. Siehe [Den Snowball Edge freischalten](#).

Um das Gerät mit dem Snowball Edge-Client neu zu starten:

1. Wenn die gesamte Kommunikation mit dem Gerät beendet ist, verwenden Sie den `reboot-device` Befehl, um es neu zu starten. Wenn das Gerät bereit ist, wird auf der LCD-Anzeige ein kurzes Video angezeigt, während das Gerät für den Start vorbereitet wird. Nach etwa 10 Minuten kann das Gerät entsperrt werden.

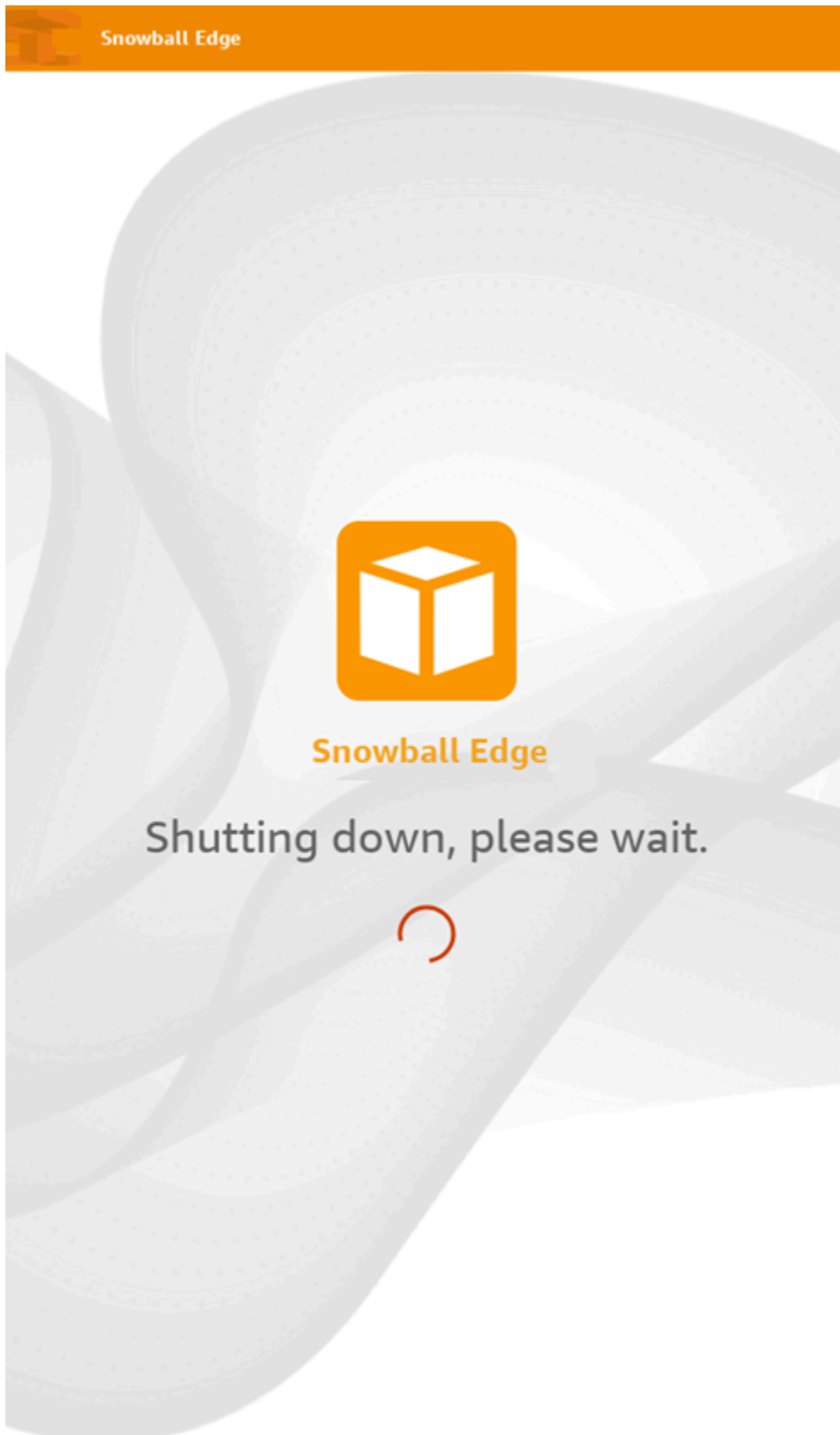
```
snowballEdge reboot-device --profile profile-name
```

2. Entsperren Sie das Gerät. Siehe [Den Snowball Edge freischalten](#).

Snowball Edge ausschalten

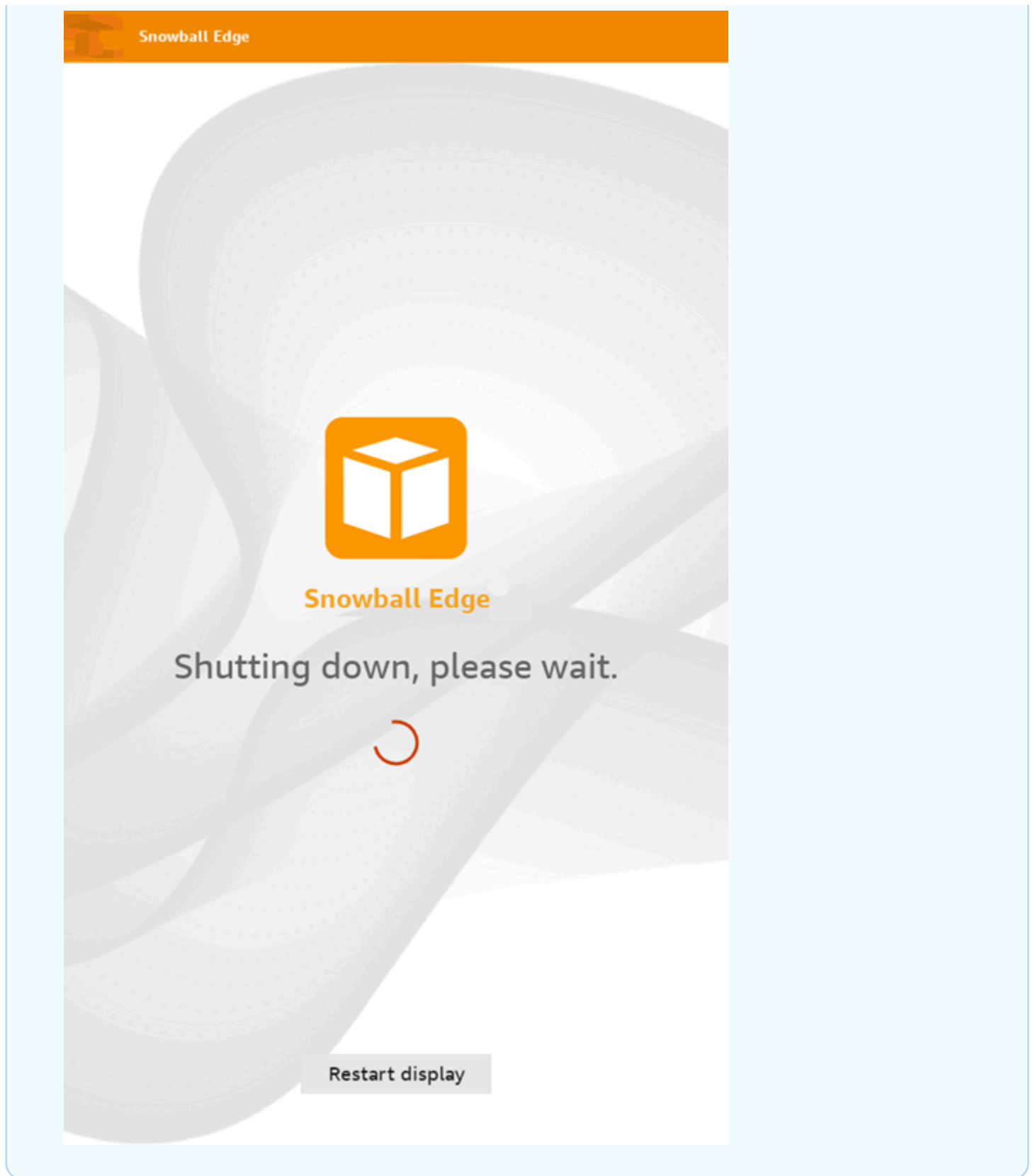
Wenn Sie mit der Übertragung von Daten auf das AWS Snowball Edge Gerät fertig sind, bereiten Sie es für die Rückreise nach vor AWS. Vergewissern Sie sich vorher, dass alle Datenübertragungen an das Gerät zum Abschluss gebracht wurden. Wenn Sie die NFS-Schnittstelle zum Übertragen von Daten verwendet haben, deaktivieren Sie sie, bevor Sie das Gerät ausschalten. Weitere Informationen finden Sie unter [Verwaltung der NFS-Schnittstelle](#).

Wenn die gesamte Kommunikation mit dem Gerät beendet ist, schalten Sie es aus, indem Sie den Netzschalter über dem LCD-Bildschirm drücken. Das Herunterfahren des Geräts dauert ca. 20 Sekunden. Während das Gerät heruntergefahren wird, wird auf dem LCD-Bildschirm eine Meldung angezeigt, die darauf hinweist, dass das Gerät heruntergefahren wird.



 Note

Wenn auf dem LCD-Bildschirm die Meldung zum Herunterfahren angezeigt wird, obwohl das Gerät nicht wirklich heruntergefahren wird, drücken Sie auf dem Bildschirm die Taste Display neu starten, um den Bildschirm wieder in den Normalbetrieb zu versetzen.



Nach dem Herunterfahren des Geräts werden die Versandinformationen auf dem E Ink-Display angezeigt. Wenn die Informationen zur Rücksendung nicht auf dem E Ink-Display angezeigt werden, wenden Sie sich an Support.

Weiter: [Rückgabe des Snowball Edge-Geräts](#)

Rückgabe des Snowball Edge-Geräts

Wenn Sie den Snowball Edge nicht mehr verwenden und ihn ausgeschaltet haben, sendet ihn ein Spediteur an AWS zurück. Der Transporteur stellt automatisch eine Sendungsverfolgungsnummer für den Versand des Geräts zur Verfügung. Die Tracking-Nummer erscheint in der Managementkonsole für die AWS Snow-Familie. Sie können auf die Sendungsverfolgungsnummer und einen Link zur Tracking-Website des Transporteurs zugreifen, indem Sie sich die Statusdetails des Auftrags in der Konsole ansehen. Weitere Informationen finden Sie unter [Rückversand für Snowball Edge-Geräte](#).

Der Transporteur liefert das Gerät an eine AWS Sortiereinrichtung und das Gerät wird an das AWS Rechenzentrum weitergeleitet. Im Rechenzentrum AWS wird sichergestellt, dass das Gerät während des Transports nicht manipuliert wurde und dass das Gerät fehlerfrei ist. Wenn das Gerät Daten enthält, die in Amazon S3 importiert werden sollen, wird mit dem Import begonnen. Andernfalls werden die Daten auf dem Gerät sicher gelöscht. Sie können die Statusänderungen verfolgen, während das Gerät AWS verarbeitet wird Managementkonsole für die AWS Snow-Familie. Sie erhalten Amazon SNS Benachrichtigungen über Statusänderungen, wenn Sie diese Option bei der Erstellung des Auftrags zur Bestellung des Geräts ausgewählt haben. Weitere Informationen finden Sie unter [Überwachung des Importstatus](#).

Zu den endgültigen Statuswerten gehört, wann das AWS Snowball Edge Gerät empfangen wurde, wann der Datenimport beginnt und wann der Job abgeschlossen ist.

Note

Wenn das Gerät Daten enthält, die Sie in Amazon S3 importieren wollten, und Sie nicht möchten, dass die Daten auf dem Gerät importiert werden, wenden Sie sich an Support um die Stornierung des Snow-Auftrags zu beantragen. Wenn Sie den Auftrag stornieren, überspringen wir die Datenübertragung und löschen das Gerät gemäß den festgelegten Verfahren auf sichere Weise. Aufgrund unserer strengen Aufbewahrungskette und unserer strengen Betriebsverfahren können wir kein Gerät mit Ihren Daten in unseren Einrichtungen aufbewahren.

Um ein AWS Snowball Edge Gerät für den Rückversand vorzubereiten

1. Schalten Sie das Gerät aus. Weitere Informationen finden Sie unter [Snowball Edge ausschalten](#).
2. Trennen Sie alle Netzkabel, die an das Gerät angeschlossen sind.
3. Trennen Sie das Netzkabel. Verstauen Sie es in der Kabelecke auf der Oberseite des AWS Snowball Edge Geräts.
4. Schließen Sie die Türen an der Rück-, Ober- und Vorderseite des AWS Snowball Edge Geräts. Drücken Sie jede Tür nach innen, bis Sie ein Klicken hören und fühlen.

Weiter: [Rückversand für Snowball Edge](#)

Rückversand für Snowball Edge

Das AWS Snowball Edge Gerät wird von einem AWS Rechenzentrum aus versandt und an dieses geliefert. Die vorausbezahlten Versandinformationen auf dem E Ink-Bildschirm des Geräts enthalten die Adresse für die Rücksendung des AWS Snowball Edge Geräts. Die Versandgeschwindigkeit für die Rücksendung entspricht der ursprünglichen Versandgeschwindigkeit, als Sie das Gerät erhalten haben. Sie können Statusänderungen mit der Managementkonsole für die AWS Snow-Familie verfolgen und den Status des Pakets über den Transporteur Ihrer Region verfolgen.

Weitere Informationen zur Rückgabe Ihres AWS Snowball Edge Geräts finden Sie unter [Versanddienstleister für Snowball Edge](#).

Important

Kleben Sie niemals ein separates Versandetikett auf dem Gerät an AWS, sofern Sie nicht anders angewiesen haben. AWS Snowball Edge Verwenden Sie immer die Versandinformationen, die auf dem E-Ink-Display des AWS Snowball Edge Geräts angezeigt werden.

Versanddienstleister für Snowball Edge

Wenn Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen, geben Sie die Adresse an, an die das AWS Snowball Edge Gerät versendet werden soll. Der Transporteur, der Ihre Region unterstützt, kümmert sich um den Versand der Geräte von AWS zu Ihnen und von Ihnen zurück zu

AWS. Sie können die Informationen zum ausgehenden Versand einsehen, wenn Ihr Auftrag den Status Sendung wird vorbereitet erreicht.

Für jedes AWS Snowball Edge Gerät, das versendet wird, gibt es eine Sendungsverfolgungsnummer. Sie finden die Tracking-Nummer und einen Link zur Tracking-Website über das [Managementkonsole für die AWS Snow-Familie](#) Job-Dashboard oder die Job-Management-API.

Diese Mobilfunkanbieter werden für folgende AWS Snowball Edge Geräte unterstützt:

- Für Indien ist Blue Dart die Fluggesellschaft.
- Für Korea, Japan, Australien und Indonesien ist Kühne + Nagel die Fluggesellschaft.
- Für China und Hongkong ist S.F. Express die Fluggesellschaft.
- In allen anderen Regionen erfolgt der Versand per [UPS](#).

Themen

- [Snowball Edge UPS-Abholungen in der EU, den USA, Großbritannien, Südafrika und Kanada](#)
- [Snowball Edge-Tonabnehmer im Vereinigten Königreich](#)
- [Pickups von Snowball Edge in Brasilien](#)
- [Pickups von Snowball Edge in Australien](#)
- [Snowball Edge-Tonabnehmer in Indien](#)
- [Tonabnehmer von Snowball Edge in Korea](#)
- [Pickups von Snowball Edge in Hongkong](#)
- [Snowball Edge-Abholungen in Singapur, Japan und Indonesien](#)
- [Empfang und Rückgabe von Snowball Edge in Dubai, Vereinigte Arabische Emirate](#)
- [Versandgeschwindigkeiten für Snowball Edge](#)

Snowball Edge UPS-Abholungen in der EU, den USA, Großbritannien, Südafrika und Kanada

UPS kann Ihr Gerät häufig in der EU, den USA, Großbritannien, Südafrika und Kanada abholen. Hier sind einige hilfreiche Richtlinien:

- Vereinbaren Sie direkt mit UPS eine Abholung oder bringen Sie das AWS Snowball Edge Gerät zu einer UPS-Paketabgabestelle, an die es versendet werden soll. AWS

- Das vorausbezahlte UPS-Versandetikett auf dem E Ink-Display enthält die Absenderadresse für das AWS Snowball Edge Gerät.
- Das AWS Snowball Edge Gerät wird an eine AWS Sortieranlage geliefert und an ein AWS Rechenzentrum weitergeleitet. UPS stellt Ihnen eine Sendungsverfolgungsnummer zur Verfügung.

Important

Sofern nicht anders angegeben AWS, kleben Sie niemals ein separates Versandetikett auf dem AWS Snowball Edge Gerät an. Verwenden Sie immer die Versandinformationen, die auf dem E-Ink-Display des Geräts angezeigt werden.

UPS versendet Snowball Edge-Geräte in die folgenden EU-Mitgliedstaaten: Österreich, Belgien, Bulgarien, Kroatien, Republik Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Italien, Irland, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien und Schweden.

Note

Bestellungen zwischen dem Vereinigten Königreich und Ländern der Europäischen Union gelten nun als international und müssen in einem speziellen internationalen Verfahren genehmigt werden. Wenn Sie Ihr Gerät zwischen Großbritannien und der EU versenden müssen, senden Sie uns eine E-Mail an <snowball-shipping@amazon.com>, um eine Handelsrechnung anzufordern, bevor Sie die Abholung oder Rückgabe mit UPS vereinbaren.

UPS-Services für Snowball Edge-Produkte sind nur innerhalb eines Landes verfügbar.

Snowball Edge-Tonabnehmer im Vereinigten Königreich

Beachten Sie im Vereinigten Königreich die folgenden Informationen, damit UPS einen Snowball Edge abholen kann:

- Sie veranlassen, dass UPS das AWS Snowball Edge Gerät abholt, indem Sie direkt eine Abholung mit UPS vereinbaren oder das AWS Snowball Edge Gerät zu einer UPS-Paketabgabestelle bringen, an die es versendet werden soll. AWS
- Das vorausbezahlte UPS-Versandetikett auf dem E Ink-Display enthält die richtige Adresse für die Rücksendung des AWS Snowball Edge Geräts.

- Das AWS Snowball Edge Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. UPS übermittelt Ihnen automatisch eine Sendungsverfolgungsnummer zu Ihrem Auftrag.

Important

Bringen Sie niemals ein separates Versandetikett auf dem Gerät an AWS, sofern Sie nicht persönlich etwas anderes angewiesen haben. AWS Snowball Edge Verwenden Sie immer die Versandinformationen, die auf dem E-Ink-Display des Geräts angezeigt werden.

UPS-Services für Snowball Edge-Produkte sind nur innerhalb eines Landes im Inland verfügbar.

Note

Seit Januar 2021 ist Großbritannien nicht mehr Teil der EU. Bestellungen zwischen Großbritannien und anderen EU-Ländern sind internationale Bestellungen, ein nicht allgemeiner Verfügbarkeitsprozess, der nur im Rahmen eines speziellen internationalen Verfahrens genehmigt wird. Wenn ein Kunde eine Genehmigung erhalten hat und ein Gerät aus einem EU-Land an LHR oder aus Großbritannien zurück in ein EU-Land zurücksendet, muss er zunächst eine Rücksendung an <snowball-shipping@amazon.com> beantragen, damit eine Handelsrechnung ausgestellt werden kann, bevor die Abholung mit UPS vereinbart werden kann. up/drop

Pickups von Snowball Edge in Brasilien

Hier sind einige Richtlinien für UPS zur Abholung eines Snowball Edge-Geräts in Brasilien:

- Wenn Sie bereit sind, ein Snowball Edge-Gerät zurückzugeben, rufen Sie 0800-770-9035 an, um eine Abholung mit UPS zu vereinbaren.
- Snowball Edge ist im Inland in Brasilien erhältlich, das 26 Bundesstaaten und den Distrito Federal umfasst.
- Halten Sie, sofern vorhanden, Ihre Betriebszulassungsnummer (Cadastro Nacional de Pessoa Juridica, CNPJ) bereit, bevor Sie einen Auftrag erstellen.
- Sie sollten das entsprechende Dokument ausstellen, um das Snowball Edge-Gerät zurückzugeben. Erkundigen Sie sich bei Ihrer Steuerbehörde, welche der folgenden Dokumente in Ihrem

Bundesstaat gemäß Ihrer Imposto sobre Circulação de Mercadorias e Serviços (ICMS) - Registrierung erforderlich sind:

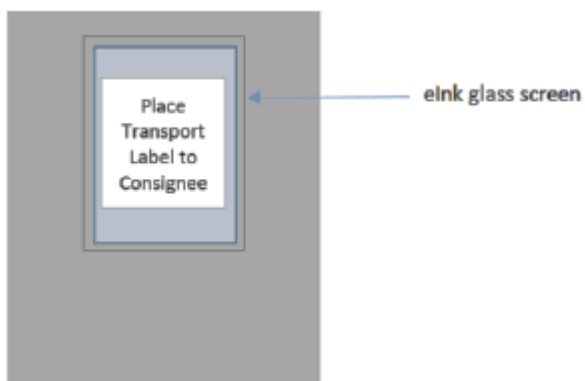
- Innerhalb von São Paulo sind in der Regel eine Nicht-ICMS-Erklärung und eine elektronische Steuerrechnung (NF-e) erforderlich.
- Außerhalb von São Paulo — Folgendes ist in der Regel erforderlich:
 - Eine Erklärung zur Befreiung von der Warenumlaufsteuer
 - Eine Nota Fiscal
 - Elektronische Steuerrechnung (NF-e)

Note

Für Steuererklärungen, die nicht dem ICMS angehören, empfehlen wir Ihnen, vier Kopien der Erklärung zu erstellen: eine für Ihre Unterlagen und die anderen drei für den Transport.

Pickups von Snowball Edge in Australien

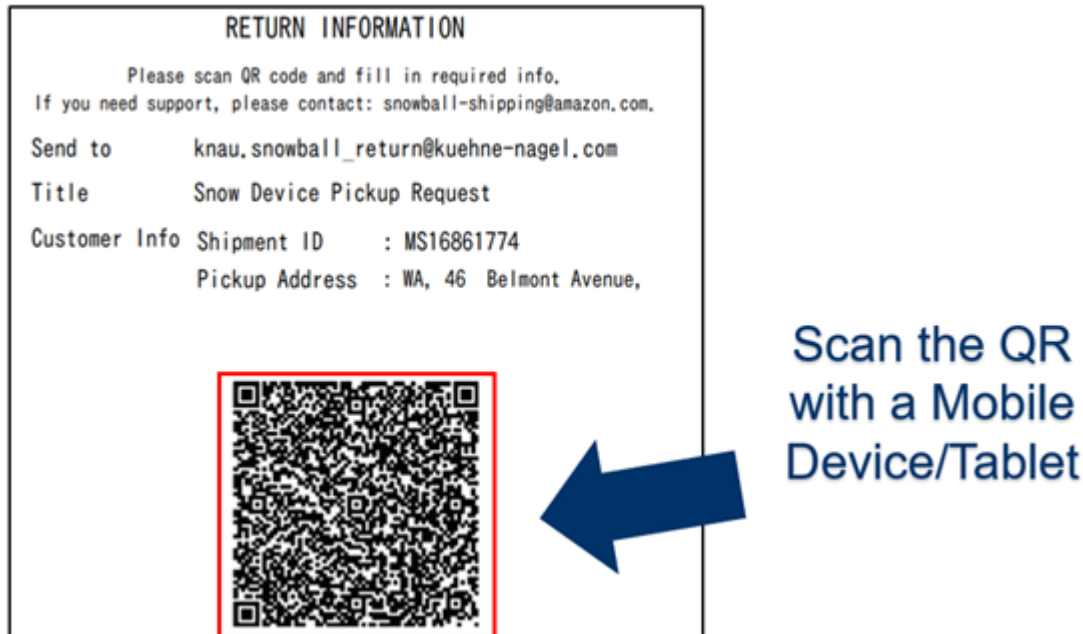
Wenn Sie in Australien ein AWS Snowball Edge Gerät zurückschicken AWS, kleben Sie das Rücksendetikett (befindet sich in dem Beutel mit diesen Anweisungen) über dem E-Ink-Etikett auf dem Snow-Gerät.



Note

Wenn Sie mit Ihrem Gerät kein Rücksendetikett erhalten haben, senden Sie eine E-Mail mit Ihrer Geräteseriennummer oder Referenznummer an knau.snowball_return@kuehne-nagel.com.

Um die Rückgabe des Snowball Edge zu arrangieren, scannen Sie den QR-Code auf den Rückgabeanweisungen mit Ihrem Mobilgerät. Auf Ihrem Gerät erscheint ein Hyperlink zu einer E-Mail-Nachricht. Die Nachricht enthält Informationen wie E-Mail-Adresse, Betreff und Kontrollnummer oder Sendungsnummer. Geben Sie das Abholdatum, den Namen und die Kontaktdaten ein oder geben Sie eine neue Abholadresse an, falls sich Änderungen ergeben.



Snowball Edge-Tonabnehmer in Indien

In Indien holt Blue Dart das Snowball-Gerät ab. Wenn Sie bereit sind, Ihr Snowball-Gerät zurückzugeben, schalten Sie es aus und bereiten Sie es für den Rückversand vor. Um die Abholung zu planen, senden Sie eine E-Mail an snowball-pickup@amazon.com mit der Betreffzeile Snowball Pickup Request. Geben Sie in der E-Mail folgende Informationen an:

- Job-ID — Die Job-ID, die dem Snowball zugeordnet ist, zu dem Sie zurückkehren möchten AWS.
- AWS-Konto ID — Die ID für das AWS Konto, das den Job erstellt hat.
- Gewünschtes Datum — Der Tag, an dem das Snowball-Gerät abgeholt werden soll.
- Früheste Abholzeit (Ihre Ortszeit) — Die früheste Tageszeit, zu der Sie den Snowball abholen möchten.
- Letzte Abholzeit (Ihre Ortszeit) — Die späteste Tageszeit, zu der Sie den Snowball abholen möchten.
- Besondere Anweisungen (optional) — Alle speziellen Anweisungen für die Abholung des Snowball, einschließlich der Kontaktdaten für die Koordination der Abholung.

Das Snowball Edge-Team arrangiert die Abholung mit Blue Dart und sendet Ihnen eine Bestätigungse-Mail. Blue Dart stellt Ihnen ein Versandetikett in paper zur Verfügung und holt das Snowball Edge-Gerät ab.

 Important

- Wenn Sie einen Snowball in Indien verwenden, denken Sie daran, alle relevanten Steuerunterlagen bei Ihrem Bundesstaat einzureichen.
- AWS benötigt mindestens 72 Stunden Vorlaufzeit, um Rücksendeanfragen in Indien zu bearbeiten. AWS kann keine Tagesgebühren für Rücksendeanfragen erstatten, die weniger als 72 Stunden im Voraus eingehen.

Tonabnehmer von Snowball Edge in Korea

In Korea verwaltet Kühne+Nagel Ihre Abholungen. Wenn Sie für die Rückgabe Ihres Geräts bereit sind, senden Sie eine E-Mail an snowball-shipping@amazon.com mit dem Betreff Snowball Pickup Request, damit wir die Abholung für Sie organisieren können. Geben Sie im Text der E-Mail folgende Informationen an:

- Job-ID — Die Job-ID, die dem Snowball zugeordnet ist, zu dem Sie zurückkehren möchten AWS.
- Abholadresse — Die Adresse, an der das Gerät abgeholt wird.
- Abholdatum — Der früheste Tag, an dem Sie das Gerät abholen möchten.
- Kontaktdetails — Der Name, die E-Mail-Adresse und die lokale Telefonnummer, über die Kühne + Nagel bei Bedarf Kontakt mit Ihnen aufnehmen kann.

Kurze Zeit später erhalten Sie eine E-Mail vom Snowball-Team mit Informationen zur Abholung unter der von Ihnen angegebenen Adresse. Führen Sie einen Power Cycle für das Gerät aus; in der Regel werden die Geräte zwischen 13:00 und 15:00 Uhr abgeholt.

Pickups von Snowball Edge in Hongkong

In Hongkong kümmert sich S.F. Express um Ihre Abholung. Wenn Sie bereit sind, Ihr Gerät zurückzugeben, senden Sie eine E-Mail an snowball-shipping-ap-east-1@amazon.com mit dem Betreff Snowball Pickup Request, damit wir die Abholung für Sie vereinbaren können. Geben Sie im Text der E-Mail folgende Informationen an:

- Auftrags-ID
- AWS-Konto Ausweis
- Name des Ansprechpartners
- Telefonnummer des Ansprechpartners
- E-Mail-Adresse des Ansprechpartners
- Der Tag, an dem die Geräte abgeholt werden sollen
- Früheste Abholzeit
- Späteste Abholzeit
- Abholadresse

Sobald Sie mit S.F. Express einen Abholungstermin vereinbart haben, kann dieser nicht mehr umgeplant werden.

Das Gerät wird AWS von S.F. Express geliefert. Die S.F. Express-Sendungsverfolgungsnummer für die Rücksendung informiert Sie über das Lieferdatum.

Snowball Edge-Abholungen in Singapur, Japan und Indonesien

Wenn Sie in Singapur, Japan und Indonesien bereit sind, Ihr Gerät zurückzugeben, scannen Sie den QR-Code, der auf dem E-Ink-Rücksendeetikett angezeigt wird, mit Ihrem Handy. Dadurch gelangen Sie direkt zu einer E-Mail-Vorlage. Bitte geben Sie die Abhol date/time - und Kontaktdaten ein.

RETURN

AWS Jobs ID QF6LNZGKTZPF
 シリアル番号 2R 207138750022
 管理番号 MS14003547



返送のご案内

“以下のQRコードをスキャンし情報を入力の上、メールにてご連絡をお願い致します。”

送信先アドレス knjp.snowball_return@kuehne-nagel.com
 件名 Snow Ball Pickup Request
 お客様情報
 管理番号 : MS14003547
 引取希望日 : 要記入
 お名前 : 要記入
 お電話番号 : 要記入



Cancel Snowball Pickup Request

To: knjp.snowball_return@kuehne-nagel.c...

Cc/Bcc:

Subject: Snowball Pickup Request

お客様情報
 管理番号 : MS11968270
 引取希望日 :
 お名前 :
 お電話番号 :

 Note

Wenn sich Ihre Abholadresse von der Adresse unterscheidet, an die das Gerät geliefert wurde, fügen Sie bitte die neue Adresse in den E-Mail-Text ein, damit der beauftragte Transporteur informiert werden kann.

 Note

In Japan erhebt die Reederei eine Versandgebühr von 120,00 USD. In der Beschreibung der Gebühr ist Snowball Edge angegeben, die Gebühr gilt jedoch für den Versand aller Snowball Edge-Produkte.

Empfang und Rückgabe von Snowball Edge in Dubai, Vereinigte Arabische Emirate

Hier sind einige Richtlinien, die Sie beachten müssen, wenn Sie ein AWS Snowball Edge Gerät in Dubai erhalten oder zurücksenden.

Empfangen eines Snowball Edge-Geräts

Wenn Sie ein Snowball Edge-Gerät in einer Freizone erhalten und von UPS darüber informiert werden, dass das Paket versandbereit ist, beantragen Sie den Gate-Pass für Ihre Freizone, holen Sie sich ihn und teilen Sie ihn mit anderen.

Wenn Sie sich in einer Freizone oder auf dem Festland befinden, unterschreiben Sie den Liefernachweis (POD), wenn Sie das Gerät erhalten.

Rückgabe eines Snowball Edge-Geräts

Wenn Sie ein Snowball Edge-Gerät zurücksenden, veranlassen Sie, dass UPS das Gerät abholt, indem Sie eine Abholung direkt mit UPS unter 600 544 743 oder über die UPS-Website vereinbaren. Vergewissern Sie sich, dass die Informationen zur Rücksendung auf dem E Ink-Display angezeigt werden, bevor das Gerät abgeholt wird. Siehe [Rückgabe des Snowball Edge-Geräts](#). Wenn Sie in einer Freizone darüber informiert werden, dass ein UPS-Fahrer mit der Abholung des Geräts beauftragt wurde, beantragen Sie den Gate Pass für Ihre Freizone, besorgen Sie sich ihn und teilen Sie ihn mit anderen.

Die vorausbezahlten UPS-Versandinformationen auf dem E Ink-Display enthalten die richtige Adresse für die Rücksendung des Snowball Edge-Geräts.

Das Snowball Edge-Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. UPS stellt automatisch eine Sendungsverfolgungsnummer für Ihren Auftrag zur Verfügung.

 Important

Kleben Sie niemals ein separates Versandetikett auf dem Snowball Edge-Gerät an AWS, sofern Sie nicht persönlich etwas anderes angewiesen haben. Verwenden Sie immer das Versandetikett, das auf dem E-Ink-Display des Geräts angezeigt wird.

UPS-Services für Snowball Edge-Produkte sind nur innerhalb eines Landes im Inland verfügbar.

Versandgeschwindigkeiten für Snowball Edge

Die Versandzeiten sind in jedem Land unterschiedlich. Diese Versandgeschwindigkeiten hängen von dem Land ab, in das Sie ein AWS Snowball Edge Gerät versenden. Von folgenden Versandzeiten können Sie ausgehen:

- Australien, Japan, Singapur, Indonesien, Südkorea — Beim Versand innerhalb dieser Länder haben Sie Zugriff auf die Standardversandgeschwindigkeit von 1 — 3 Tagen.
- Brasilien — Beim Versand innerhalb Brasilien haben Sie Zugriff auf den UPS Domestic Express Saver-Versand, der während der Geschäftszeiten innerhalb von zwei Werktagen zustellt. Die Transportdauer kann durch Verspätungen an den zwischenstaatlichen Grenzen verlängert werden.
- Europäische Union (EU) — Beim Versand in eines der Länder innerhalb der EU haben Sie Zugang zum Expressversand. In der Regel werden AWS Snowball Edge Geräte, die per Express versendet werden, innerhalb von etwa einem Tag geliefert. Außerdem ist in den meisten EU-Ländern der Standardversand möglich. In der Regel dauert dieser für einen Weg weniger als eine Woche.
- Hongkong — Beim Versand innerhalb Hongkong haben Sie Zugang zum Expressversand.
- Indien — Beim Versand innerhalb Indien werden Snowball Edge-Geräte innerhalb von 7 Arbeitstagen nach AWS Erhalt aller zugehörigen Steuerdokumente versandt.
- Dubai, Vereinigte Arabische Emirate - Sie haben Zugriff auf den Courier Express Saver-Versand.
- Vereinigtes Königreich (UK) — Beim Versand innerhalb des Vereinigten Königreichs haben Sie Zugriff auf Expressversand. In der Regel werden Snowball Edge-Geräte, die per Express versendet werden, innerhalb von etwa einem Tag geliefert. Darüber hinaus haben Sie Zugriff auf den Standardversand, der in der Regel weniger als eine Woche dauert, und zwar in einer Richtung.

- Vereinigte Staaten von Amerika (USA) und Kanada: Innerhalb der USA oder Kanadas ist Versand innerhalb von 24 und 48 Stunden möglich.

Überwachen des Importstatus vom Snowball Edge

Um den Status Ihres Importauftrags in der Konsole zu überwachen, melden Sie sich in dem Bereich an, [Managementkonsole für die AWS Snow-Familie](#) in AWS-Region dem der Job erstellt wurde. Wählen Sie den Auftrag, den Sie verfolgen möchten, in der Tabelle aus, oder suchen Sie mit den ausgewählten Parametern in der Suchleiste oberhalb der Tabelle danach. Nachdem Sie den Job ausgewählt haben, werden detaillierte Informationen zu diesem Job in der Tabelle angezeigt, einschließlich einer Leiste, die den Status Ihres Jobs in Echtzeit anzeigt.

Note

Wenn wir aufgrund eines Problems mit den von Ihnen konfigurierten Zugriffsberechtigungen keine Daten vom Snow-Gerät in unsere Rechenzentren importieren können, werden wir versuchen, Sie zu benachrichtigen, und Sie haben ab dem Datum, an dem wir die Benachrichtigung erhalten, 30 Tage Zeit, um das Problem zu lösen. Wenn das Problem nicht behoben ist, stornieren wir möglicherweise Ihren Snowball Edge-Job und löschen Daten vom Gerät.

Nachdem Ihr Gerät bei uns eingetroffen ist AWS, ändert sich Ihr Auftragsstatus von Im Transit AWS zu At AWS. Im Durchschnitt dauert es einen Tag, bis Ihr Datenimport in Amazon S3 beginnt. Der Status Ihres Auftrags wechselt dann zu Importing (Wird importiert). Das Importieren Ihrer Daten vom Snowball Edge dauert ungefähr genauso lange wie das Verschieben auf Snowball Edge. AWS Nachdem Ihre Daten importiert wurden, ändert sich der Auftragsstatus in den Status Abgeschlossen.

Jetzt ist Ihr erster Datenimportauftrag in Amazon S3 AWS Snowball Edge abgeschlossen. Sie können einen Bericht über die Datenübertragung von der Konsole abrufen. Zum Öffnen dieses Berichts über die Konsole wählen Sie den Auftrag in der Tabelle aus und erweitern Sie ihn, sodass die ausführlichen Auftragsinformationen angezeigt werden. Wählen Sie Get report (Bericht abrufen), um Ihren Auftragsabschlussbericht als PDF-Datei herunterzuladen. Weitere Informationen finden Sie unter [Sie erhalten den Abschlussbericht und die Protokolle Ihres Datenübertragungsauftrags](#).

Weiter: [Sie erhalten den Abschlussbericht und die Protokolle Ihres Datenübertragungsauftrags](#)

Sie erhalten den Abschlussbericht und die Protokolle Ihres Datenübertragungsauftrags

Wenn Sie einen Snowball Edge verwenden, um Daten in Amazon S3 zu importieren oder Daten aus Amazon S3 zu exportieren, erhalten Sie einen herunterladbaren PDF-Auftragsbericht. Bei Importaufträgen steht dieser Bericht am Ende des Importvorgangs zur Verfügung. Bei Exportaufträgen steht Ihnen Ihr Auftragsbericht in der Regel zur Verfügung, während Ihnen das AWS Snowball Edge Gerät für Ihren Auftragsteil geliefert wird. Berichte zum Abschluss von Aufträgen sind nicht nur für lokale Rechen- und Speicheraufträge verfügbar.

Der Jobbericht gibt Ihnen Einblick in den Status Ihrer Amazon S3 S3-Datenübertragung. Der Bericht enthält zudem Details zu Ihrem Auftrag oder Teilauftrag. Der Jobbericht enthält auch eine Tabelle, die einen allgemeinen Überblick über die Gesamtzahl der Objekte und Byte bietet, die zwischen dem Gerät und Amazon S3 übertragen wurden.

Einen tieferen Einblick in den Status Ihrer übertragenen Objekte ermöglichen die beiden zugehörigen Protokolle – ein Erfolgsprotokoll und ein Fehlerprotokoll. Die Protokolle sind im CSV-Dateiformat (durch Kommas getrennte Werte) gespeichert, und der Name jedes Protokolls enthält die ID des Auftrags oder Auftragsteils, zu dem das Protokoll gehört.

Sie können die Berichte und Protokolle in der Managementkonsole für die AWS Snow-Familie herunterladen. Im Folgenden finden Sie einen Beispielbericht.

Snow Family Job Completion Report



Region: us-gov-east-1(OSU)

Job ID: JIDd6d95004-fe1a-42d3-895d-684f357ef840

Snow Device Serial ID: 207117851234

Job type: IMPORT

Device type: Snowball Edge Storage Optimized

Storage type: S3

Job creation date: 2022-06-02 19:32:27.831 GMT

Job state: Completed

Customer address:

123 Any Street
Any Town, USA

Transfer details:

Transfer type	Total	Success	Failed
Objects	2,635	2,635	0
Bytes	32.2 TB	32.2 TB	0 B

Job state transition details:

The job was created on 2022-06-02 19:32:27.831 GMT
The snowball got allocated on 2022-06-06 19:10:43.670 GMT
The snowball was shipped on 2022-06-07 21:59:50.937 GMT
The snowball was at customer on 2022-06-08 14:04:45.856 GMT
The snowball was shipped to AWS on 2022-06-28 20:57:42.246 GMT
The snowball was at our sorting facility on 2022-06-29 14:06:20.737 GMT
The snowball was at AWS on 2022-06-30 23:12:45.017 GMT
The data transfer started on 2022-06-30 23:21:34.805 GMT
The data transfer was completed on +54473-09-10 22:23:46 GMT

Please review your job's status from the console.

For Snow job details, please see: <https://docs.aws.amazon.com/snowball/>

Abrufen von Abschlussberichten und Protokollen für Aufträge

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie den [Managementkonsole für die AWS Snow-Familie](#).
2. Wählen Sie Ihren Job oder Ihren Jobteil aus der Tabelle aus und erweitern Sie den Statusbereich.

Zum Abrufen der Berichte und Protokolle werden drei Optionen angezeigt: Get job report (Auftragsbericht abrufen), Download success log (Erfolgsprotokoll herunterladen) und Download failure log (Fehlerprotokoll herunterladen).

3. Wählen Sie das gewünschte Protokoll für den Download aus.

Der Bericht kann die folgende Werte besitzen:

- Abgeschlossen — Die Übertragung wurde erfolgreich abgeschlossen. Weitere detaillierte Informationen finden Sie im Erfolgsprotokoll.
- Fehlerhaft abgeschlossen — Einige oder alle Ihre Daten wurden nicht übertragen. Weitere detaillierte Informationen finden Sie im Fehlerprotokoll.

Migration großer Datenmengen mit Snowball Edge

Die Migration großer Datenmengen von lokalen Standorten erfordert eine sorgfältige Planung, Orchestrierung und Ausführung, um sicherzustellen, dass Ihre Daten erfolgreich migriert werden.

AWS

Wir empfehlen, dass Sie vor Beginn der Migration über eine Datenmigrationsstrategie verfügen, um mögliche Terminüberschreitungen, Budgetüberschreitungen und Migrationsfehler zu vermeiden. AWS Snow Services hilft Ihnen dabei, Ihre großen Datenmigrationsprojekte über die Snowball Edge Large Data Migration Manager (LDMM) -Funktion in der zu platzieren, zu bestellen und zu verfolgen. Managementkonsole für die AWS Snow-Familie

Die Themen [Planen Sie Ihren großen Transfer mit Snowball Edge](#) und [Kalibrieren einer großen Übertragung mit Snowball Edge](#) beschreiben einen manuellen Datenmigrationsprozess. Sie können die manuellen Schritte mithilfe des Snowball Edge LDMM-Migrationsplans optimieren.

Themen

- [Planen Sie Ihren großen Transfer mit Snowball Edge](#)
- [Kalibrieren einer großen Übertragung mit Snowball Edge](#)
- [Erstellen eines Migrationsplans für große Datenmengen mit Snowball Edge](#)
- [Verwenden des Migrationsplans für große Datenmengen mit Snowball Edge](#)

Planen Sie Ihren großen Transfer mit Snowball Edge

Wir empfehlen Ihnen, große Datenübertragungen zwischen den AWS Snowball Edge Geräten, die Sie vor Ort haben, und Ihren Servern anhand der Richtlinien in den folgenden Abschnitten zu planen und zu kalibrieren.

Themen

- [Schritt 1: Verstehen Sie, was Sie in die Cloud verlagern](#)
- [Schritt 2: Berechnen Sie Ihre Zielübertragungsrate](#)
- [Schritt 3: Ermitteln Sie, wie viele Snowball Edge Sie benötigen](#)
- [Schritt 4: Erstellen Sie Ihre Jobs](#)
- [Schritt 5: Teilen Sie Ihre Daten in Übertragungssegmente auf](#)

Schritt 1: Verstehen Sie, was Sie in die Cloud verlagern

Bevor Sie Ihren ersten Job mit der erstellen Managementkonsole für die AWS Snow-Familie, sollten Sie sich Gedanken über die Datenmenge machen, die Sie übertragen müssen, wo sie derzeit gespeichert sind und an welches Ziel Sie sie übertragen möchten. Bei Datenübertragungen, die ein Petabyte oder mehr umfassen, erleichtert diese administrative Verwaltung die Ankunft Ihres Snowball Edge erheblich.

Wenn Sie Daten AWS Cloud zum ersten Mal in die migrieren, empfehlen wir Ihnen, ein Cloud-Migrationsmodell zu entwerfen. Die Cloud-Migration erfolgt nicht über Nacht. Es erfordert einen sorgfältigen Planungsprozess, um sicherzustellen, dass alle Systeme wie erwartet funktionieren.

Nach diesem Schritt sollten Sie wissen, welche Menge an Daten Sie insgesamt in die Cloud verschieben werden.

Schritt 2: Berechnen Sie Ihre Zielübertragungsrate

Es ist wichtig, abzuschätzen, wie schnell Sie Daten auf den Snowball Edge übertragen können, die mit jedem Ihrer Server verbunden sind. Diese geschätzte Geschwindigkeit in MB/s bestimmt, wie schnell Sie die Daten mithilfe Ihrer lokalen Netzwerkinfrastruktur von Ihrer Datenquelle auf Snowball Edge-Geräte übertragen können.

Note

Für große Datenübertragungen empfehlen wir die Verwendung der Amazon S3 S3-Datenübertragungsmethode. Sie müssen diese Option auswählen, wenn Sie Geräte in der bestellen Managementkonsole für die AWS Snow-Familie.

Um eine Basisübertragungsrate zu ermitteln, übertragen Sie einen kleinen Teil Ihrer Daten auf das Snowball Edge-Gerät oder übertragen Sie eine 10-GB-Beispieldatei und beobachten Sie den Durchsatz.

Denken Sie bei der Festlegung Ihrer Zielübertragungsgeschwindigkeit daran, dass Sie den Durchsatz verbessern können, indem Sie Ihre Umgebung, einschließlich der Netzwerkkonfiguration, optimieren, indem Sie die Netzwerkgeschwindigkeit, die Größe der zu übertragenden Dateien und die Geschwindigkeit, mit der Daten von Ihren lokalen Servern gelesen werden können, ändern. Der Amazon S3 S3-Adapter kopiert Daten so schnell nach Snowball Edge, wie es Ihre Bedingungen zulassen.

Schritt 3: Ermitteln Sie, wie viele Snowball Edge Sie benötigen

Ermitteln Sie anhand der Gesamtmenge der Daten, die Sie in die Cloud verschieben möchten, der geschätzten Übertragungsgeschwindigkeit und der Anzahl der Tage, in die Sie die Daten verschieben möchten AWS, wie viele Snowball Edge Sie für Ihre groß angelegte Datenmigration benötigen. Je nach Gerätetyp verfügen Snowball Edge-Geräte über etwa 39,5 TB oder 210 TB nutzbaren Speicherplatz. Wenn Sie beispielsweise 300 TB Daten auf AWS mehr als 10 Tage verschieben möchten und eine Übertragungsgeschwindigkeit von 250 MB/s haben, benötigen Sie 2 Snowball Edge-Geräte mit 210 TB Speicher.

Note

Das Snowball Edge LDMM bietet einen Assistenten zur Schätzung der Anzahl von Snowball Edge, die gleichzeitig unterstützt werden können. Weitere Informationen finden Sie unter [Erstellen eines Migrationsplans für große Datenmengen mit Snowball Edge](#).

Schritt 4: Erstellen Sie Ihre Jobs

Nachdem Sie wissen, wie viele Snowball Edge Sie benötigen, müssen Sie für jedes Gerät einen Importauftrag erstellen. Die Erstellung mehrerer Jobs wird durch das Snowball Edge LDMM vereinfacht. Weitere Informationen finden Sie unter [Platzieren Sie Ihren nächsten Auftrag](#).

Note

Sie können Ihre nächste Auftragsbestellung aufgeben und sie direkt über den Zeitplan für empfohlene Auftragsbestellungen automatisch zu Ihrem Plan hinzufügen. Weitere Informationen finden Sie unter [Empfohlener Zeitplan für die Auftragsbestellung](#).

Schritt 5: Teilen Sie Ihre Daten in Übertragungssegmente auf

Als bewährte Methode für große Datenübertragungen mit mehreren Aufträgen empfehlen wir, dass Sie Ihre Daten logisch in mehrere kleinere, besser verwaltbare Datensätze aufteilen. Auf diese Weise können Sie jede Partition gleichzeitig oder mehrere Partitionen parallel übertragen. Stellen Sie bei der Planung Ihrer Partitionen sicher, dass die Daten für die Partitionen zusammen auf den Snowball Edge für den Job passen. Sie können Ihre Übertragung beispielsweise auf eine der folgenden Arten in Partitionen unterteilen:

- Sie können beispielsweise 10 Partitionen mit jeweils 20 TB für die Verwendung mit einem Snowball Edge-Gerät mit 210 TB Speicher erstellen.
- Bei großen Dateien kann jede Datei bis zur Größenbeschränkung von 5 TB für Objekte in Amazon S3 eine individuelle Partition sein.
- Jede Partition kann eine andere Größe haben, und jede einzelne Partition kann aus derselben Art von Daten bestehen, z. B. kleine Dateien in einer Partition, komprimierte Archive in einer anderen, große Dateien in einer anderen Partition usw. Dieser Ansatz kann Ihnen helfen, Ihre durchschnittliche Übertragungsrate für verschiedene Dateitypen zu ermitteln.

Note

Metadatenoperationen werden für jede übertragene Datei ausgeführt. Dieser Aufwand ist derselbe, unabhängig von der Dateigröße. Daher erzielen Sie eine schnellere Leistung, wenn Sie kleine Dateien zu einem größeren Paket komprimieren, Ihre Dateien stapeln oder größere Einzeldateien übertragen.

Das Erstellen von Datenübertragungssegmenten kann es Ihnen erleichtern, Übertragungsprobleme schnell zu lösen, da es komplex sein kann, eine große, heterogene Übertragung zu beheben, nachdem die Übertragung einen Tag oder länger andauert.

Wenn Sie mit der Planung Ihrer Datenübertragung im Petabyte-Bereich fertig sind, empfehlen wir Ihnen, einige Segmente von Ihrem Server auf das Snowball Edge-Gerät zu übertragen, um Ihre Geschwindigkeit und Gesamtübertragungszeit zu kalibrieren.

Kalibrieren einer großen Übertragung mit Snowball Edge

Sie können die Übertragungsleistung kalibrieren, indem Sie einen repräsentativen Satz Ihrer Datenpartitionen übertragen. Wählen Sie mehrere Partitionen aus, die Sie definiert haben, und übertragen Sie sie auf ein Snowball Edge-Gerät. Notieren Sie die Übertragungsgeschwindigkeit und die Gesamtübertragungszeit für jeden Vorgang. Wenn die Ergebnisse der Kalibrierung unter der Zielübertragungsrate liegen, können Sie möglicherweise mehrere Teile Ihrer Datenübertragung gleichzeitig kopieren. In diesem Fall wiederholen Sie die Kalibrierung mit den zusätzlichen Partitionen Ihres Datensatzes.

Fügen Sie während der Kalibrierung weitere parallel Kopiervorgänge hinzu, bis Sie feststellen, dass die Summe der Übertragungsgeschwindigkeit aller Instanzen, die derzeit Daten übertragen, abnimmt. Beenden Sie die letzte aktive Instanz und notieren Sie sich Ihre neue Zielübertragungsrate.

Sie können Daten schneller an Snowball Edge übertragen, indem Sie Daten mithilfe eines der folgenden Szenarien parallel übertragen:

- Verwendung mehrerer Sitzungen des S3-Adapters auf einer Workstation gegen ein einzelnes Snowball Edge-Gerät.
- Verwendung mehrerer Sitzungen des S3-Adapters auf mehreren Workstations auf einem einzigen Snowball Edge-Gerät.
- Verwenden mehrerer Sitzungen der S3-Oberfläche (mit einer oder mehreren Workstations), die auf mehrere Snowball Edge abzielen.

Wenn Sie diese Schritte abgeschlossen haben, sollten Sie wissen, wie schnell Sie Daten auf ein Snowball Edge-Gerät übertragen können.

Erstellen eines Migrationsplans für große Datenmengen mit Snowball Edge

Mit der Snowball Edge-Migrationsplanfunktion für große Datenmengen können Sie große Datenmigrationen von 500 TB bis zu mehreren Petabyte mithilfe mehrerer Snowball Edge-Serviceprodukte planen, verfolgen, überwachen und verwalten.

Verwenden Sie die Funktion zum Migrationsplan für große Datenmengen, um Informationen über Datenmigrationsziele zu sammeln, z. B. die Größe der Daten, in die migriert werden soll, AWS und die Anzahl der Snowball Edge-Geräte, die für die gleichzeitige Migration der Daten benötigt werden. Verwenden Sie den Plan, um einen voraussichtlichen Zeitplan für Ihr Datenmigrationsprojekt und den empfohlenen Zeitplan für die Auftragsbestellung zu erstellen, um Ihre Ziele zu erreichen.

Note

Derzeit ist der Datenmigrationsplan für Importaufträge mit einer Größe von mehr als 500 TB verfügbar.

Themen

- [Schritt 1: Wählen Sie Ihre Migrationsdetails](#)
- [Schritt 2: Wählen Sie Ihre Versand-, Sicherheits- und Benachrichtigungseinstellungen](#)
- [Schritt 3: Überprüfen und erstellen Sie Ihren Plan](#)

Schritt 1: Wählen Sie Ihre Migrationsdetails

Note

Für Datenmigrationen von mehr als 500 TB ist ein umfangreicher Datenmigrationsplan verfügbar. Erstellen Sie individuelle Auftragsaufträge auf Snowball Edge für Ihre Datenübertragungsprojekte mit einer Größe von weniger als 500 TB. Weitere Informationen finden Sie in diesem Handbuch unter [Erstellen eines Auftrags zur Bestellung eines Snowball Edge-Geräts](#).

1. Melden Sie sich an der [Managementkonsole für die AWS Snow-Familie](#) an. Wenn Sie das zum ersten Mal verwenden AWS-Region, wird die Managementkonsole für die AWS Snow-Familie Snowball Edge-Seite angezeigt. Andernfalls wird die Liste der vorhandenen Jobs angezeigt.
2. Wenn dies Ihr erster Datenmigrationsplan ist, wählen Sie auf der Hauptseite Create your large data migration plan aus. Wählen Sie andernfalls Migrationsplan für große Datenmengen aus. Wählen Sie Datenmigrationsplan erstellen, um den Assistenten zur Planerstellung zu öffnen.
3. Geben Sie im Feld Name Ihres Datenmigrationsplans einen Namen für den Datenmigrationsplan ein. Der Name des Plans kann bis zu 64 Zeichen lang sein. Gültige Zeichen sind A-Z, a-z, 0-9 und . (Bindestrich). Ein Planname darf nicht mit **aws** beginnen.
4. Geben Sie unter Gesamtzahl der zu AWS migrierenden Daten die Datenmenge ein, zu der Sie migrieren möchten AWS.
5. Wählen Sie unter Snow-Geräte ein Snowball Edge-Gerät aus.

Note

Die unterstützten Geräteoptionen können je nach Geräteverfügbarkeit in einigen AWS-Regionen variieren.

6. Geben Sie für Concurrent-Geräte die Anzahl der Snowball Edge-Geräte ein, auf die Sie gleichzeitig Daten an Ihrem Standort kopieren können. Wenn Sie sich nicht sicher sind, fahren

Sie mit dem nächsten Abschnitt fort, um Informationen darüber zu erhalten, wie Sie dies mithilfe des Assistenten zur Schätzung von gleichzeitigen Geräten ermitteln können.

7. Wählen Sie Weiter.

Verwenden Sie den Assistenten für die Schätzung von Concurrent-Devices

Der Assistent zur Schätzung paralleler Geräte hilft Ihnen dabei, die Anzahl der gleichzeitigen Geräte zu ermitteln, die Sie bei umfangreichen Datenmigrationen verwenden können.

Voraussetzungen:

- Sie haben eine Machbarkeitsstudie durchgeführt, um Ihre Datenübertragungsmethodik zu testen und die Leistung mit einem Snowball Edge-Gerät in Ihrer Umgebung zu messen.
- Sie kennen das Netzwerk und die Verbindung zum Back-End-Speicher.

Schritt 1: Geben Sie Datenquelleninformationen ein

Ermitteln Sie zunächst den maximalen theoretischen Durchsatz für das Kopieren von Daten aus Ihrer Speicherquelle.

1. Geben Sie unter Gesamtzahl der zu migrierenden Daten die Datenmenge ein, die Sie migrieren möchten.

Wählen Sie unter Einheit die Maßeinheit (GB oder TB) für die Datenmenge aus, die Sie migrieren möchten.

2. Geben Sie unter Anzahl der aktiven Netzwerkschnittstellen die Anzahl der aktiven Netzwerkschnittstellen ein, die Ihnen für die Datenmigration von der Speicherquelle zur Verfügung stehen.

Number of active network interfaces [Info](#)
The number of network interfaces that can be used for migrations

Number of active network interfaces used for data migration

3. Wählen Sie unter Geschwindigkeit der Netzwerkschnittstelle die Geschwindigkeit der Netzwerkschnittstelle für die Speicherquelle aus. Die Netzwerkgeschwindigkeiten werden in GB/s angegeben.

Network interface speed [Info](#)
The speed of the network interfaces used for migrations

Network interface speed (Gb/s)

10 ▼

4. Geben Sie für Maximaler Netzwerkdurchsatz den maximalen getesteten Netzwerkdurchsatz für Ihre Speicherquelle ein, den Sie während der Machbarkeitsstudie ermittelt haben. Der Durchsatz wird in MB/S angegeben.

Maximum network throughput [Info](#)
The maximum sustainable throughput for the data source

Maximum tested throughput of data source (MB/s)

5. Geben Sie unter Netzwerknutzung im Speicher-Backend an, ob sich die Speicherquelle ein Netzwerk mit dem Back-End-Speicher teilt.
- Wählen Sie Ja, wenn das Netzwerk nicht gemeinsam genutzt wird. Sie müssen die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream nicht eingeben.
 - Wählen Sie Nein, wenn das Netzwerk gemeinsam genutzt wird. Geben Sie die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream in MB/s ein.

Je nach Ihrer Wahl aktualisiert der Assistent den Wert für den maximalen Migrationsdurchsatz für die Datenquelle (MB/s) unten auf der Seite.

Storage backend network usage [Info](#)**Network shared with storage backend traffic?**

Is the network used for migration being shared with your storage backend?

Yes

Speed of storage interconnection for single stream (MB/s)

This is a single connection throughput that can be sustained from source to destination

6. Wählen Sie Weiter.

Schritt 2: Geben Sie die Workstation-Parameter für die Migration ein

Sie können Ihren Snowball Edge direkt mit Ihrer Speicherquelle (z. B. einem Microsoft Windows-Server) verbinden. Sie können sich stattdessen dafür entscheiden, Ihren Snowball Edge mit einer oder mehreren Workstations zu verbinden, um Daten aus der Speicherquelle zu kopieren.

1. Geben Sie für die Nutzung der Migrations-Workstation Ihre bevorzugte Workstation-Nutzung an.
 - Wählen Sie Keine — Datenquelle direkt verwenden, um Daten direkt aus einer Datenquelle zu übertragen, ohne eine Arbeitsstation zu verwenden, und wählen Sie dann Weiter.
 - Wählen Sie Andere — Kopierarbeitsstation (en) verwenden, um eine oder mehrere Arbeitsstationen für die Datenübertragung zu verwenden.

Migration workstation usage [Info](#)

Type of migration source used

Other - Use copy workstation(s)

2. Geben Sie unter Anzahl der aktiven Netzwerkschnittstellen die Anzahl der Ports ein, die für die Datenmigration verwendet werden sollen.

Number of active network interfaces [Info](#)

The number of network interfaces that can be used for migrations

Number of active network interfaces on the migration workstation

3. Wählen Sie für Geschwindigkeit der Netzwerkschnittstelle die Geschwindigkeit der Netzwerkschnittstellen in GB/s aus.

Network interface speed [Info](#)

Your workstations Network card speeds

Network interface speed (Gb/s)

4. Geben Sie unter Netzwerknutzung im Speicher-Backend an, ob das Netzwerk, in dem sich die Workstations befinden, mit dem Back-End-Speicher gemeinsam genutzt wird.
- Wählen Sie Ja, wenn es gemeinsam genutzt wird.
 - Wähle Nein, wenn es nicht geteilt wird. Geben Sie die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream in MB/s ein.

Storage backend network usage [Info](#)

Network shared with storage backend traffic?

Is the network used for migration being shared with your storage backend?

Speed of storage interconnection for single stream (MB/s)

This is a single connection throughput that can be sustained from source to destination

Basierend auf Ihren Eingaben zeigt der Assistent unter Anzahl der Migrations-Workstations eine Empfehlung an. Sie können die Anzahl manuell ändern, wenn Sie mit der Empfehlung nicht einverstanden sind. Diese Nummer wird im Migrationsplan für große Datenmengen unter Gleichzeitige Geräte angezeigt.

Number of migration workstations [Info](#)

Recommended number of migration workstations used

Schritt 3: Geben Sie den durchschnittlichen Übertragungsdurchsatz von Snowball Edge ein

1. Geben Sie im Feld Average Snow Device Transfer Throughput den Übertragungsdurchsatz in MB/s ein, den Sie während Ihrer Machbarkeitsstudie festgestellt haben.

Average Snow device transfer throughput [Info](#)

This is the throughput from your migration workstation to the Snow device you saw during the proof of concept

Average Snow device transfer throughput (MB/s)

Basierend auf Ihrem durchschnittlichen Durchsatz aktualisiert der Assistent in den Details zum Migrationsplan die empfohlene Anzahl gleichzeitiger Snow-Geräte und die maximale Anzahl gleichzeitiger Geräte.

2. Wählen Sie Diese Anzahl verwenden, um fortzufahren und zur Auswahl Ihrer Migrationsdetails zurückzukehren. Wählen Sie Weiter und fahren Sie mit dem nächsten Schritt fort ([Schritt 2: Wählen Sie Ihre Versand-, Sicherheits- und Benachrichtigungseinstellungen](#)).

Note

Sie können bis zu 5 Snow-Geräte gleichzeitig verwenden.

Schritt 2: Wählen Sie Ihre Versand-, Sicherheits- und Benachrichtigungseinstellungen

1. Wählen Sie im Abschnitt Lieferadresse eine bestehende Adresse aus oder erstellen Sie eine neue.

- Note

Das Land in der Adresse muss mit dem Zielland des Geräts übereinstimmen und für dieses Land gültig sein.

2. Führen Sie unter Servicezugriffstyp auswählen einen der folgenden Schritte aus:
 - Erlauben Sie Snowball Edge, für Sie eine neue serviceverknüpfte Rolle mit allen erforderlichen Berechtigungen zum Veröffentlichen von CloudWatch Metriken und Amazon SNS SNS-Benachrichtigungen für Ihre Snowball Edge-Jobs zu erstellen.
 - Fügen Sie eine bestehende Servicerolle hinzu, die über die erforderlichen Berechtigungen verfügt. Ein Beispiel für die Einrichtung dieser Rolle finden Sie unter [Beispiel 4: Erwartete Rollenberechtigungen und Vertrauensrichtlinie](#).
3. Wählen Sie unter Benachrichtigungen senden aus, ob Benachrichtigungen gesendet werden sollen. Beachten Sie, dass Sie, wenn Sie „Keine Benachrichtigung über Datenmigrationspläne senden“ auswählen, keine Benachrichtigungen von diesem Plan erhalten, aber Sie erhalten trotzdem Jobbenachrichtigungen.
4. Für Benachrichtigungen festlegen
 - Wählen Sie „Bestehendes SNS-Thema verwenden“
 - oder Neues SNS-Thema erstellen.

Schritt 3: Überprüfen und erstellen Sie Ihren Plan

1. Überprüfe deine Informationen in den Tarifdetails und Einstellungen für Versand, Sicherheit und Benachrichtigungen und bearbeite sie gegebenenfalls.
2. Wählen Sie Datenmigrationsplan erstellen aus, um den Plan zu erstellen.

Verwenden des Migrationsplans für große Datenmengen mit Snowball Edge

Nachdem Sie Ihren Migrationsplan für große Datenmengen erstellt haben, können Sie den daraus resultierenden Zeitplan und das Dashboard verwenden, um Sie durch den weiteren Migrationsprozess zu führen.

Empfohlener Zeitplan für die Auftragsbestellung

Nachdem Sie einen großen Snowball Edge-Migrationsplan erstellt haben, können Sie den empfohlenen Zeitplan für die Auftragsbestellung verwenden, um neue Jobs zu erstellen.

Note

Manuelle Aktualisierungen, die Sie an der Datengröße oder der Anzahl gleichzeitiger Geräte vornehmen, führen zu einer Anpassung des Zeitplans. Der Zeitplan passt sich automatisch an, wenn ein Auftrag nicht bis zum empfohlenen Bestelldatum oder vor dem empfohlenen Bestelldatum bestellt wurde. Wenn ein Auftrag vor dem empfohlenen Bestelldatum zurückgegeben wird, passt sich der Zeitplan automatisch an.

Recommended job ordering schedule						Jobs ordered
Recommended job ordering schedule						Actions
This list provides an estimated schedule to place Snow jobs in order to achieve your data migration goals. The estimated ordering schedule is automatically adjusted based on your data migration speed.						
Filter by a date and time range 🔄 ☒ Hide Ordered						< 1 >
Recommended date to order	Number of devices to order	Number of ordered devices	Device type	Status		
☐ Thu Mar 23 2023	2	-	Snowball Edge Storage Optimized with 210TB	☒ Not Ordered		
☐ Fri Mar 31 2023	2	-	Snowball Edge Storage Optimized with 210TB	☒ Not Ordered		
☐ Sat Apr 08 2023	2	-	Snowball Edge Storage Optimized with 210TB	☒ Not Ordered		
☐ Sun Apr 16 2023	2	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Mon Apr 24 2023	2	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Tue May 02 2023	2	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Wed May 10 2023	2	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Thu May 18 2023	2	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Fri May 26 2023	1	-	Snowball Edge Storage Optimized with 80TB	☒ Not Ordered		
☐ Fri May 26 2023	1	-	Snowcone SSD	☒ Not Ordered		

Platzieren Sie Ihren nächsten Auftrag

Um Ihre nächste Bestellung aufzugeben, haben Sie die Möglichkeit, entweder einen zuvor bestellten Job zu klonen oder einen bereits ausgefüllten Job zu erstellen, anstatt manuell einen Job zu erstellen und ihn dann zu Ihrem Plan hinzuzufügen.

So klonen Sie einen Job:

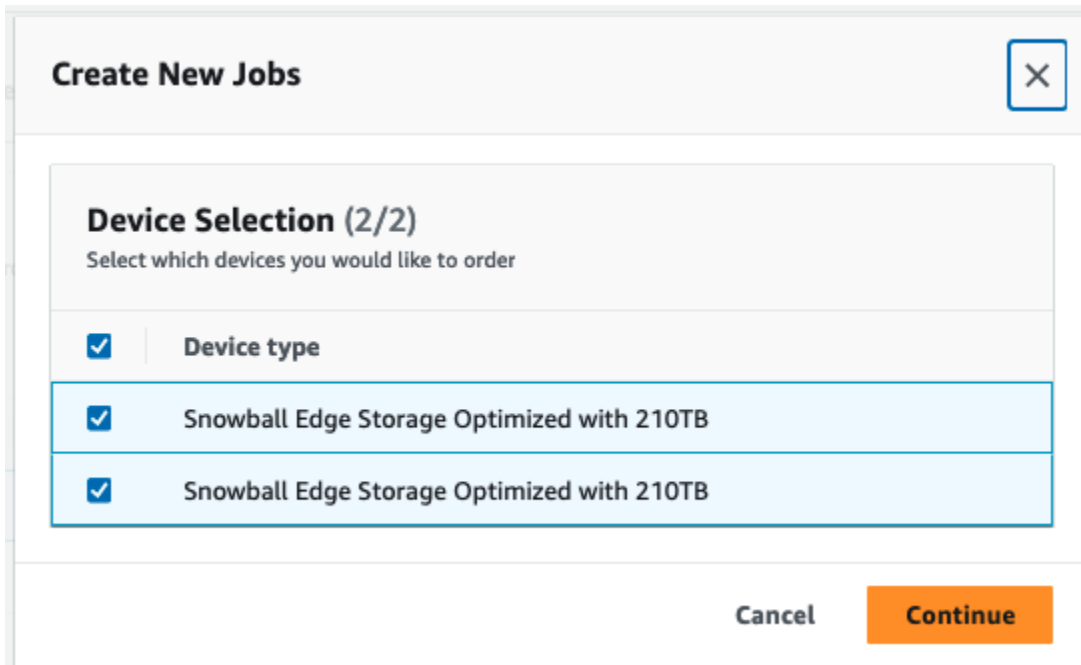
1. Wählen Sie die nächste Bestellung (die erste Empfehlung mit dem Status Nicht bestellt) aus dem Bestellplan für empfohlene Jobs aus und wählen Sie dann im Menü Aktionen die Option Job klonen. Das Fenster Clone Job wird angezeigt.
2. Wählen Sie im Fenster „Job klonen“ im Abschnitt „Geordnete Jobs“ den Job aus, den Sie klonen möchten.
3. Wählen Sie im Abschnitt „Details zu neuen Aufträgen“ die Geräte aus, die Sie bestellen möchten. Für jedes gewählte Gerät wird der Auftragsname automatisch auf der Grundlage des ausgewählten Auftrags ausgefüllt. Sie können den Jobnamen überschreiben.
4. Wählen Sie Bestätigen, um den Auftrag für die ausgewählten Geräte aufzugeben. Das System klonet den Job für jedes Gerät.

Um neue Jobs zu erstellen:

1. Wählen Sie den nächsten Auftrag (die erste Empfehlung mit dem Status „Nicht bestellt“) aus dem Bestellplan „Empfohlene Jobs“ aus und wählen Sie dann im Menü „Aktionen“ die Option „Neue Jobs erstellen“. Das Fenster Neue Jobs erstellen wird angezeigt.

Recommended job ordering schedule					
This list provides an estimated schedule to place Snow Jobs in order to achieve your data migration goals. The estimated ordering schedule is automatically adjusted based on your data migration speed.					
Filter by a date and time range		Hide Ordered		Actions View Details Create New Jobs Clone Job	
Recommended date to order	Number of devices to order	Number of ordered devices	Device type	Status	
☒ Thu Mar 23 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Fri Mar 31 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Sat Apr 08 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Sun Apr 16 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Mon Apr 24 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Tue May 02 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Wed May 10 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Thu May 18 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Fri May 26 2023	1	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Fri May 26 2023	1	-	Snowcone SSD	⊗ Not Ordered	

2. Wählen Sie im Bereich Geräteauswahl die Geräte aus, die Sie bestellen möchten. Klicken Sie auf Weiter.



Create New Jobs

Device Selection (2/2)
Select which devices you would like to order

☒	Device type
☒	Snowball Edge Storage Optimized with 210TB
☒	Snowball Edge Storage Optimized with 210TB

Cancel Continue

3. Die Seite „Neues erstellen“ wird angezeigt. Die meisten Parameter, wie der Auftragstyp, die Lieferadresse und der Gerätetyp, werden auf der Grundlage des Plans festgelegt. Das System erstellt den Job für jedes Gerät.

Sie können sehen, ob der Job oder die Jobs erfolgreich erstellt wurden oder nicht. Erfolgreich erstellte Jobs werden automatisch zum Plan hinzugefügt.

Liste der bestellten Jobs

Für jeden Plan wird eine Liste mit der Reihenfolge der Aufträge angezeigt. Diese ist zunächst leer. Wenn Sie anfangen, Jobs zu bestellen, können Sie Jobs zu Ihrem Plan hinzufügen, indem Sie im Menü Aktionen die Option Job hinzufügen auswählen. Jobs, die Sie hier hinzufügen, werden im Monitoring-Dashboard nachverfolgt.

Ebenso können Sie den Job aus der Liste der bestellten Jobs entfernen, indem Sie im Menü Aktionen die Option Job entfernen auswählen.

Wir empfehlen, den im Plan enthaltenen Zeitplan für die Auftragsbestellung zu verwenden, um eine reibungslose Datenmigration zu gewährleisten.

Dashboard zur Überwachung

Nachdem Sie Jobs zu Ihrem Plan hinzugefügt haben, können Sie auf dem Dashboard die Metriken sehen, zu denen die Jobs AWS zur Aufnahme zurückkehren. Diese Kennzahlen können dir helfen, deinen Fortschritt zu verfolgen:

- Daten migriert nach AWS — Die Datenmenge, zu der bisher migriert wurde AWS ..
- Durchschnittlich migrierte Daten pro Auftrag — Die durchschnittliche Datenmenge pro Auftrag in Terabyte.
- Schneeaufträge insgesamt — Die Anzahl der bestellten Snowball Edge-Aufträge im Vergleich zu den verbleibenden zu bestellenden Aufträgen.
- Durchschnittliche Dauer eines Migrationsauftrags — Die durchschnittliche Dauer eines Jobs in Tagen.
- Snow Job Status — Die Anzahl der Jobs in jedem Status.

AWS OpsHub Zur Verwaltung von Geräten verwenden

Snowball Edge bietet jetzt ein benutzerfreundliches Tool AWS OpsHub, mit dem Sie Ihre Geräte und lokalen AWS Dienste verwalten können. Sie verwenden es AWS OpsHub auf einem Client-Computer, um Aufgaben wie das Entsperren und Konfigurieren einzelner oder geclusterter Geräte, das Übertragen von Dateien und das Starten und Verwalten von Instanzen auszuführen, die auf Snowball Edge ausgeführt werden. Sie können AWS OpsHub damit die beiden Gerätetypen Storage Optimized und Compute Optimized Snow verwalten. Die AWS OpsHub Anwendung steht Ihnen ohne zusätzliche Kosten zur Verfügung.

AWS OpsHub nimmt alle vorhandenen Operationen, die in der Snowball-API verfügbar sind, und präsentiert sie als grafische Benutzeroberfläche. Diese Schnittstelle hilft Ihnen, Daten schnell zu den Edge-Computing-Anwendungen auf Snowball Edge zu migrieren AWS Cloud und bereitzustellen.

AWS OpsHub bietet eine einheitliche Ansicht der AWS Dienste, die auf Snowball Edge ausgeführt werden, und automatisiert betriebliche Aufgaben durch. AWS Systems Manager Mit AWS OpsHub können Benutzer mit unterschiedlichem technischen Fachwissen eine große Anzahl von Snowball Edge verwalten. Mit wenigen Klicks können Sie Geräte entsperren, Dateien übertragen, EC2 Amazon-kompatible Instances verwalten und Gerätemetriken überwachen.

Wenn Ihr Snow-Gerät an Ihrem Standort eintrifft, laden Sie die AWS OpsHub -Anwendung herunter und installieren und starten sie auf einem Client-Computer, z. B. einem Laptop. Nach der Installation können Sie das Gerät entsperren und damit beginnen, es lokal zu verwalten und unterstützte AWS Dienste zu nutzen. AWS OpsHub bietet ein Dashboard, das wichtige Kennzahlen wie Speicherkapazität und aktive Instanzen auf Ihrem Gerät zusammenfasst. Es bietet auch eine Auswahl von AWS Diensten, die auf dem Snowball Edge unterstützt werden. Innerhalb weniger Minuten können Sie mit der Übertragung von Dateien zum Gerät beginnen.

Themen

- [AWS OpsHub Für Snowball Edge wird heruntergeladen](#)
- [Entsperren eines Snowball Edge-Geräts mit AWS OpsHub](#)
- [Überprüfung der PGP-Signatur von AWS OpsHub \(optional\)](#)
- [Verwaltung von AWS Diensten auf dem Snowball Edge mit AWS OpsHub](#)
- [Starten Sie das Gerät neu mit AWS OpsHub](#)
- [Profile verwalten mit AWS OpsHub](#)
- [Das Gerät herunterfahren mit AWS OpsHub](#)

- [Den Gerätealias bearbeiten mit AWS OpsHub](#)
- [Verwaltung von Public-Key-Zertifikaten mit OpsHub](#)
- [Updates für Snowball Edge abrufen](#)
- [Aktualisierung der AWS OpsHub Anwendung](#)
- [Automatisieren Sie Ihre Verwaltungsaufgaben mit AWS OpsHub](#)
- [Einstellung der NTP-Zeitserver für das Gerät mit AWS OpsHub](#)

AWS OpsHub Für Snowball Edge wird heruntergeladen

Zum Herunterladen AWS OpsHub

1. Rufen Sie die [AWS Snowball-Ressourcen-Website](#) auf.

The screenshot shows the AWS OpsHub website. On the left is a sidebar with navigation links: 'What's New', 'OpsHub', 'Snowball Edge Client', 'Featured Content', 'Documentation', 'Webinars', 'Videos', 'Blog Posts', and 'Free Training'. The main content area is titled 'OpsHub' and contains a description: 'OpsHub is a graphical user interface you can use to manage Snowball devices. OpsHub makes it easy to setup and manage Snowball devices enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. With just a few clicks in OpsHub, you have the full functionality of the Snow Family of devices at your fingertips; you can unlock and configure devices, drag-and-drop data to devices, launch applications, and monitor device metrics.' Below this is a link to 'OpsHub documentation'. At the bottom, there is a table with download links for different operating systems.

	OpsHub
Windows 7 or higher	Download
Mac OS X 10.10 or higher	Download
Linux (Ubuntu version 14 or higher, and Fedora version 24 or higher)	Download
	(Signature)

2. Wählen Sie in AWS OpsHubdiesem Abschnitt die Option Herunterladen für Ihr Betriebssystem aus und folgen Sie den Installationsschritten.

Entsperren eines Snowball Edge-Geräts mit AWS OpsHub

Wenn Ihr Gerät an Ihrem Standort ankommt, besteht der erste Schritt darin, es zu verbinden und zu entsperren. AWS OpsHub ermöglicht es Ihnen, Geräte mithilfe der folgenden Methoden anzumelden, zu entsperren und zu verwalten:

- **Lokal** — Um sich lokal bei einem Gerät anzumelden, müssen Sie das Gerät einschalten und mit Ihrem lokalen Netzwerk verbinden. Geben Sie dann einen Entsperrcode und eine Manifestdatei ein.
- **Fernzugriff** — Um sich remote bei einem Gerät anzumelden, müssen Sie das Gerät einschalten und sicherstellen, dass es *device-order-region*.amazonaws.com über Ihr Netzwerk eine Verbindung herstellen kann. Geben Sie dann die AWS Identity and Access Management (IAM-) Anmeldeinformationen (Zugriffsschlüssel und geheimer Schlüssel) für das Gerät ein AWS-Konto, das mit Ihrem Gerät verknüpft ist.

Informationen zur Aktivierung der Fernverwaltung und zum Erstellen eines zugehörigen Kontos finden Sie unter [Aktivieren der Snowball Edge-Geräteverwaltung auf einem Snowball Edge](#).

Themen

- [Lokales Entsperren eines Snowball Edge-Geräts mit AWS OpsHub](#)
- [Ein Snowball Edge-Gerät aus der Ferne entsperren mit AWS OpsHub](#)

Lokales Entsperren eines Snowball Edge-Geräts mit AWS OpsHub

Um Ihr Gerät lokal zu verbinden und zu entsperren

1. Öffnen Sie die Klappe an Ihrem Gerät, suchen Sie das Netzkabel und schließen Sie es an eine Stromquelle an.
2. Connect das Gerät über ein Netzkabel (normalerweise ein RJ45 Ethernet-Kabel) mit Ihrem Netzwerk, öffnen Sie dann die Frontplatte und schalten Sie das Gerät ein.
3. Öffnen Sie die AWS OpsHub Anwendung. Wenn Sie zum ersten Mal Benutzer sind, werden Sie aufgefordert, eine Sprache auszuwählen. Wählen Sie anschließend Weiter.
4. Wählen Sie auf der OpsHub Seite Erste Schritte mit die Option Auf lokalen Geräten anmelden und dann Anmelden aus.



Get started with OpsHub

☒ Sign into local devices
You'll need an unlock code and
manifest file

☐ Sign into remote devices
You'll need an access key & secret
key

Sign in

5. Wählen Sie auf der Seite Bei lokalen Geräten anmelden Ihren Snowball Edge-Typ und dann Anmelden aus.
6. Geben Sie auf der Anmeldeseite die Geräte-IP-Adresse und den Entsperrcode ein. Um das Gerätemanifest auszuwählen, wählen Sie Datei auswählen und dann Anmelden aus.



Sign into your Snowball Edge

Sign in with an unlock code and manifest file

Device IP address

Eg 12.34.45.678

Unlock code

7c0e1-bab84-f7675-0a2b6-bfcc3

Manifest file

 Choose file

No file chosen

Back

Sign in

7. (Optional) Speichern Sie die Anmeldeinformationen Ihres Geräts als Profil. Benennen Sie das Profil und wählen Sie Save profile name (Profilname speichern) aus. Weitere Informationen zu Profilen finden Sie unter [Profile verwalten mit AWS OpsHub](#).
8. Wählen Sie auf der Registerkarte Lokale Geräte ein Gerät aus, um dessen Details zu sehen, z. B. die Netzwerkschnittstellen und AWS Dienste, die auf dem Gerät ausgeführt werden. Auf dieser Registerkarte können Sie auch Details für Cluster einsehen oder Ihre Geräte genauso verwalten, wie Sie es mit dem AWS Command Line Interface (AWS CLI) tun. Weitere Informationen finden Sie unter [Verwaltung von AWS Diensten auf dem Snowball Edge mit AWS OpsHub](#).

Für Geräte, die bereits AWS Snowball Edge Device Management installiert sind, können Sie Fernverwaltung aktivieren wählen, um die Funktion zu aktivieren. Weitere Informationen finden Sie unter [AWS Snowball Edge Device Management Zur Verwaltung von Snowball Edge verwenden](#).

Ein Snowball Edge-Gerät aus der Ferne entsperren mit AWS OpsHub

Um einen Snowball Edge zu entsperren, nicht

Um Ihr Gerät aus der Ferne zu verbinden und zu entsperren

1. Öffnen Sie die Klappe an Ihrem Gerät, suchen Sie das Netzkabel und schließen Sie es an eine Stromquelle an.
2. Connect das Gerät über ein Ethernet-Kabel (normalerweise ein RJ45 Kabel) mit Ihrem Netzwerk, öffnen Sie dann die Frontplatte und schalten Sie das Gerät ein.

Note

Damit das Gerät aus der Ferne entsperrt werden kann, muss es eine Verbindung herstellen können `device-order-region`.amazonaws.com.

3. Öffnen Sie die AWS OpsHub Anwendung. Wenn Sie zum ersten Mal Benutzer sind, werden Sie aufgefordert, eine Sprache auszuwählen. Wählen Sie anschließend Weiter.
4. Wählen Sie auf der OpsHub Seite Erste Schritte mit die Option Bei Remote-Geräten anmelden und dann Anmelden aus.



Get started with OpsHub

☐ Sign into local devices
You'll need an unlock code and manifest file

☒ Sign into remote devices
You'll need an access key & secret key

Sign in

5. Geben Sie auf der Seite „Bei Remote-Geräten anmelden“ die AWS Identity and Access Management (IAM-) Anmeldeinformationen (Zugriffsschlüssel und geheimer Schlüssel) für das Gerät ein AWS-Konto , das mit Ihrem Gerät verknüpft ist, und wählen Sie dann Anmelden aus.



Sign into remote devices

Sign in with an access key and secret key

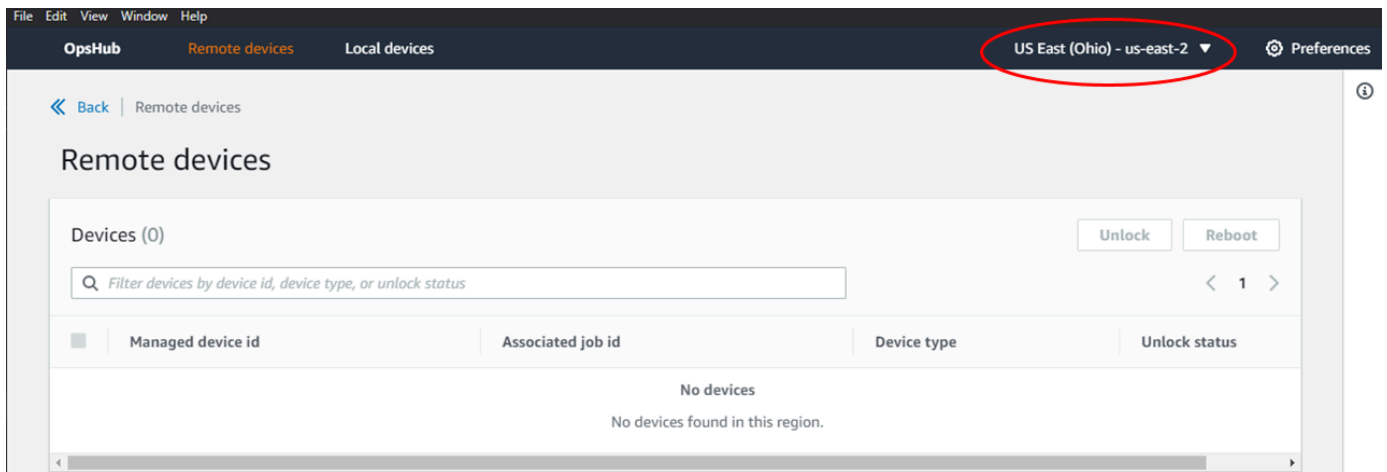
Access key

Secret key

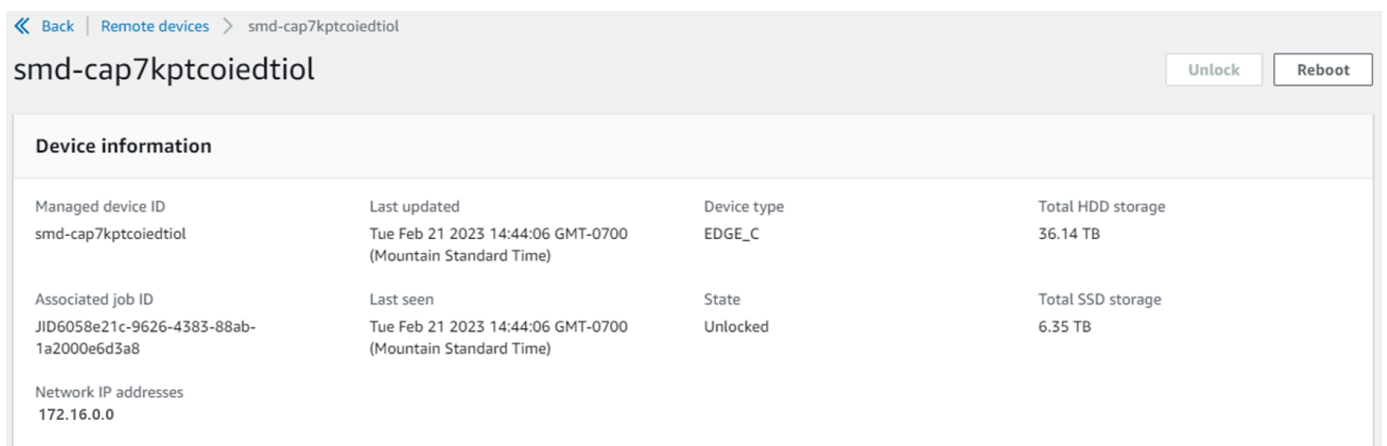
Back

Sign in

6. Wählen Sie oben auf der Registerkarte „Remote-Geräte“ die Region des Snow-Geräts aus, das per Fernzugriff entsperrt werden soll.



7. Wählen Sie auf der Registerkarte Remote-Geräte Ihr Gerät aus, um dessen Details wie Status und Netzwerkschnittstellen anzuzeigen. Wählen Sie dann Entsperren, um das Gerät zu entsperren.



Auf der Detailseite des Remote-Geräts können Sie Ihre Geräte auch neu starten und verwalten, genauso wie Sie es mit dem AWS Command Line Interface (AWS CLI) tun. Um Remote-Geräte in verschiedenen Kategorien anzuzeigen AWS-Regionen, wählen Sie in der Navigationsleiste die aktuelle Region und dann die Region aus, die Sie anzeigen möchten. Weitere Informationen finden Sie unter [Verwaltung von AWS Diensten auf dem Snowball Edge mit AWS OpsHub](#).

Überprüfung der PGP-Signatur von AWS OpsHub (optional)

Das Installationsprogramm der AWS OpsHub Anwendung für das Linux-Betriebssystem ist kryptografisch signiert. Sie können einen öffentlichen Schlüssel verwenden, um zu überprüfen, ob das Installationspaket original und unverändert ist. Wenn die Dateien beschädigt oder verändert sind, schlägt die Überprüfung fehl. Sie können die Signatur des Installationspakets mit GNU Privacy Guard

(GPG) überprüfen. Diese Überprüfung ist optional. Wenn Sie die Signatur der Anwendung überprüfen möchten, können Sie dies jederzeit tun.

Sie können die SIGNATURE-Datei für das Linux-Betriebssystem-Installationsprogramm von [AWS Snowball Edge Resources](#) oder [Snowball Edge Resources](#) herunterladen.

Um das AWS OpsHub Installationspaket für das Linux-Betriebssystem zu überprüfen

1. Kopieren Sie den folgenden öffentlichen Schlüssel, speichern Sie ihn in einer Datei und geben Sie der Datei einen Namen. Beispiel, `opshub-public-key.pgp`.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBF/hGf8BEAC9HCDV8uljDX02Jxspi6kmPu4xqf4ZZLQsSqJcHU61oL/c
/zAN+mUqJT9aJ1rr0QFGVD1bMogecUPf1TWlDkEEpG8ZbX5P8vR+EE10/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmI07j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZxcI/+u+99YLaugJIP6ZYIeDfpxnghqyVtaappBFTAyfG67Y
N/5mea1VqJzd8liFpIFQnl+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvfTb47bbv9Z28V1284
4lw2w1B1007Fo02v/Y0ukrN3VHCpmJQS1IiqZbYRa0DVK6UR5QNvUlj5fwWs
4qW9UDPhT/HDuaMrMFcejEn/7wvRUrGVtzCT9F56Al/dwRSxBejQQEb1AC8j
uuyi7gJaPdyNntR0EFTD7i02L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTp0ry/
Wvw0iKZFbo4AkiI0aLyBCK9HBXhUKa9x06g0nhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90w1RBuAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZIenrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQS4NAwARAQABzTlBV1MgT3BzSHVi
IGZvcibTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFAl/hGf8GCwkHCAMCBUIcGIEFgIBAAIZAQIBAwIeAQAh
CRAhgC9adPNF8RYhBDcvpelIaY930b0vqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIaw0SXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmXWbG
cxg1g0GXNXCM4lAd68CmbA0LoLTaWSQX30ZbswzhbtX2ADAlOpV8RLBik7fm
bS9FyuubDRhfYRQq0fpjUGXFiEgwg6aMFxsrlLlV4QD7t+6ftFie/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+FOVMmPeEN5JRazEeUr1
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDW0q/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty25lo8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4ED119Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEza/2upDJ1m+40HK4p
8DrEzP/3jTahT8q5ofFWSRDL17d31TSU+JBmPE3mz311FNXgi08w+taY320z
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
07vxM05xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFVzT/tDi5FiEEi+09
V+UAYN9Gnw36EVm/NP+00LnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvg0tUBxqmC0jr+8AKH00tiBWSu0
lsS8JU5rindEsKUrKTwcG2wyZFoe1z1E8xPkLRSRN5ZbbgKsTz1611HgCCId
Do+WJdDkWGwXmtDvzjM32EI/PVBd108ga9aPwXdhLw0dKAjZ4JrJXLUQJjRI
```

```

IVDSyM0bEH0UM6a/+mWNZazNfo0LSGWqGva6Xn5WJWlwR1S78vPNf03BQYU0
YRjaVQR+kPtB9aSAZni5sWfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7X103o/VjblneZ0hJK6kAKU172tnPJTJ31Jb0xX73wsMWDYZRZVcK
9X9+GFrpwhKHKKPjpM0t/FRxNepvqR172TkgBPqGH2TM0FdB1f/uQprvqge
PBbS0JrmBIH9/anIqgtMdtcNQB/0erLdCDqI5af0uD10LcLwdJwG9/bSrfwT
TVEE3WbXmJ8pZgMz1HUizE6V2DSadV/YItk50I0jJR0VH0Hv1FMwGCEAIFzf
9P/pNi8hpEm1RphRi0VVcdQ30bH0M0gPHu5V9f1IhyCL1zU3LjYTHkq0yJD5
YDA1x01MYq3DcSM5130VBbLmuVS2GpcsTCYqlgQA6h/zzMwz+/70wU0EX+EZ
/wEQA0AY8ULmcJIQWIr14V0jylpJeD3qwJ7wd+QsBzJ+mOp0B/3ZFAhQiN01
9yCD1HeiZeAmWYX90IXrNiIdcHy+WTAp4G+NaMpqE52qhbDjz+IbvLp11yDH
bYEHpJnTHXEy21bvKAJ0Kkw/2RcQ0i4dodGnq5icyYj+9gcuHvnVwbrQ96Ia
0D7c+b5T+bzFqk90nIcztMRuhDLJnJpi70jpvQwfq/TkkZA+mzupxfSkq/Y
N9qXNEToT/VI2gn/LS0X4Ar112KxBjzNESQkwGSiWSYtMA5J+Tj5ED0uZ/que
omNblAlD4bm7Na8NAoLxCtAiDq/f3To9Xb18lHsnd0mFLCb/BVgP4edQKTii
C/OZHy9QJ1fmN0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXM0d3I
e6NUvU7pW0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQqYZe0
jXD3Ij7T+X2XA8M/BmypoMw0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcPxzehwsSVq1lzaL2ureJBL0KkBgYxUJYXpbS01ax1TsFG
091dAN0s9Ej8CND37GsNnuygj0gWXB6MNgbvPs3H3zi/AbMunQ1VB1w07JX
zdM1hBQZh6w+NeiEsK1T6wHi7IhxABEBAAHCwXYEGAEIAAkFAl/hGf8CGwwA
IQkQIYHPWnTzRfEWIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PVbF
ywKvwi3GL0lpY7BXn8lQaHyunMGUavm080faRR0ynkH0ZqLHCp6bIajF0fvF
b7c0Jamzx8Hg+SIId16yRpRY+fA4RQ6PNnmT93ZgWW3EbjPyJGlm0/rt03SR
+0yn4/ldlg2KfBX4pqMoPCMKUdWxGmDETXsGihwZ0gmCZqXe8lK122PYkSN
JQQ+L1fjKvCaxfPKEjXYTbIbfyyhCR6NzA0VZxCrzSz2xDrYwP/V002K1xda
0ix6r2aEHf+xYEUh0aBt80HY5nXTuRReCVU789MUVtCMqD2u6amdo4BR0kWA
QNg4yavKwV+LVtyYh2Iju9VSyv4xL1Q4xKHvcAUrSH73bHG7b7jkUJckD0f4
twhjJk/Lfwe6RdnVo2WoeTvE93w+NAq2FXmvbiG7eltl0XfQecvQU3QNbRvH
U8B96W0w8UXJdvTKg4f0NbjSw7iJ3x5naixQ+rA8hLV8x0gn2LX6wvxT/SEu
mn20KX+fPtJELK7v/NheFLX1jsKLXYo4jHrkfIXNsNUhg/x2E71kAjbET3s+
t9kCtxt2iXDDZvpIbmG04QkvLFvoroASmN6+8fupe3e+e2yN0e6xGTuE60gX
I2+X1p1g9IduDYTpoI20XleHyyMqGEEIb4g0iisloTp5oi3EuAYRGf1XuqAT
VA19bKnpkBsJ0A==
=tD2T
-----END PGP PUBLIC KEY BLOCK-----

```

2. Verwenden Sie eine kryptografische Softwaresuite wie GNU Privacy Guard, um den öffentlichen Schlüssel in Ihren Schlüsselbund zu importieren, und notieren Sie sich den zurückgegebenen Schlüsselwert.

```
gpg --import opshub-public-key.gpg
```

Example Ausgabe des Befehls

```
gpg: key 1655BBDE2B770256: public key "AWS OpsHub for Snowball Edge <aws-opshub-  
signer@amazon.com>" imported  
gpg: Total number processed: 1  
gpg:             imported: 1
```

- Überprüfen Sie den Fingerprint Achten Sie darauf, *key-value* durch den Wert aus dem vorherigen Schritt zu ersetzen. Wir empfehlen, dass Sie GPG verwenden, um den Fingerabdruck zu verifizieren.

```
gpg --fingerprint key-value
```

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

```
pub   rsa4096 2020-12-21 [SC]  
      372F A5E9 4869 8F77 D1B3  AFAA 2181 CF5A 74F3 45F1  
uid           [ unknown] AWS OpsHub for Snowball Edge <aws-opshub-  
signer@amazon.com>  
sub   rsa4096 2020-12-21 [E]
```

Der Fingerabdruck sollte folgenden Angaben entsprechen:

372F A5E9 4869 8F77 D1B3 AFAA 2181 CF5A 74F3 45F1

Wenn der Fingerabdruck nicht übereinstimmt, installieren Sie die AWS OpsHub Anwendung nicht. Wenden Sie sich an Support.

- Überprüfen Sie das Installationspaket und laden Sie die SIGNATURE-Datei entsprechend der Architektur und dem Betriebssystem Ihrer Instanz herunter, falls Sie dies noch nicht getan haben.
- Überprüfen Sie die Installer-Paketsignatur. Achten Sie darauf, *signature-filename* und *OpsHub-download-filename* durch die Werte zu ersetzen, die Sie beim Herunterladen der SIGNATURE-Datei und der AWS OpsHub Anwendung angegeben haben.

GPG

```
gpg --verify signature-filename OpsHub-download-filename
```

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

GPG

```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snowball Edge <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9C93 4C3B 61F8 C434 9F94 5CA0 1655 BBDE 2B77 0256
```

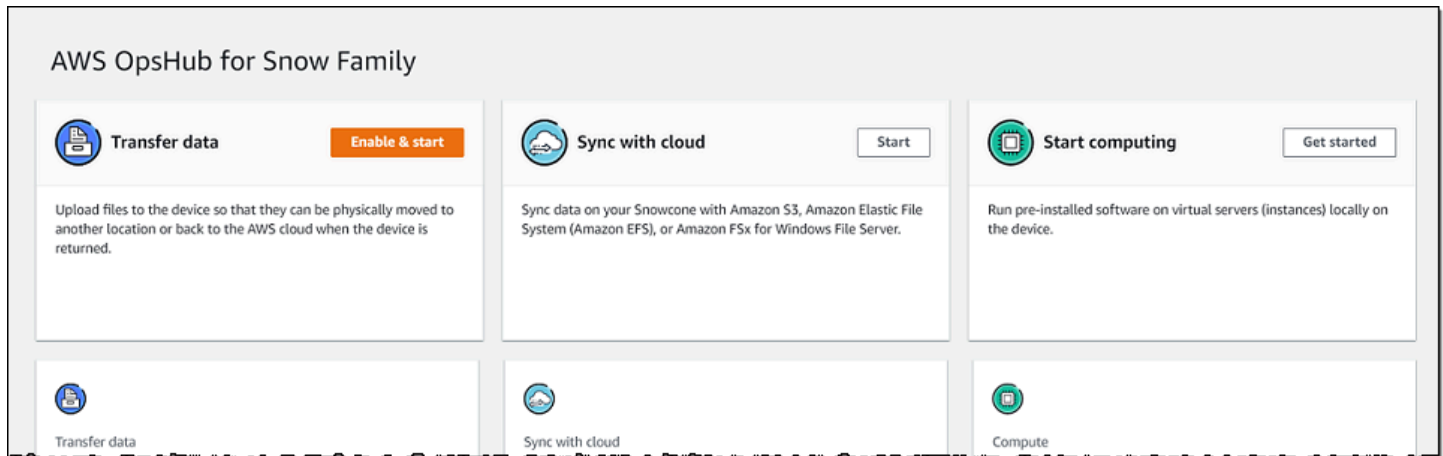
Wenn Sie GPG verwenden und die Ausgabe den Ausdruck enthält `BAD signature`, überprüfen Sie, ob Sie das Verfahren korrekt ausgeführt haben. Wenn Sie weiterhin diese Antwort erhalten, wenden Sie sich an den Agenten Support und installieren Sie ihn nicht. Die Warnmeldung bezüglich des Vertrauens bedeutet nicht, dass die Signatur nicht gültig ist, sondern nur, dass Sie den öffentlichen Schlüssel nicht verifiziert haben. Beachten Sie die Warnung zu vertrauenswürdigen Inhalten.

Verwaltung von AWS Diensten auf dem Snowball Edge mit AWS OpsHub

Mit AWS OpsHub können Sie AWS Dienste auf Ihrem Snowball Edge verwenden und verwalten. AWS OpsHub Unterstützt derzeit die folgenden Ressourcen:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instances — Verwenden Sie EC2 Amazon-kompatible Instances, um auf einem virtuellen Server installierte Software auszuführen, ohne sie AWS Cloud zur Verarbeitung an den zu senden.
- Network File System (NFS) — Verwenden Sie Dateifreigaben, um Daten auf Ihr Gerät zu verschieben. Sie können das Gerät versenden, AWS an das Ihre Daten übertragen werden AWS Cloud, oder es für die Übertragung DataSync an andere AWS Cloud Standorte verwenden.
- Amazon S3 S3-kompatibler Speicher auf Snowball Edge — Bietet sicheren Objektspeicher mit erhöhter Stabilität, Skalierbarkeit und erweiterten Amazon S3 S3-API-Funktionen für robuste, mobile Edge-Umgebungen und unverbundene Umgebungen. Mithilfe von Amazon S3 S3-

kompatiblen Speicher auf Snowball Edge können Sie Daten speichern und hochverfügbare Anwendungen auf Snowball Edge für Edge-Computing ausführen.



Themen

- [Starten einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub](#)
- [Stoppen einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub](#)
- [Starten einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub](#)
- [Arbeiten mit Schlüsselpaaren für EC2 -kompatible Instanzen in AWS OpsHub](#)
- [Beenden einer Amazon EC2 -kompatiblen Instance mit AWS OpsHub](#)
- [Lokales Verwenden von Speichervolumes auf Snowball Edge mit AWS OpsHub](#)
- [Import eines Images als EC2 Amazon-kompatibles AMI mit AWS OpsHub](#)
- [Löschen eines Snapshots aus einem Snowball Edge mit AWS OpsHub](#)
- [Abmeldung eines AMI auf einem Snowball Edge mit AWS OpsHub](#)
- [Verwaltung eines EC2 Amazon-Clusters auf Snowball Edge mit AWS OpsHub](#)
- [Richten Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ein mit AWS OpsHub](#)
- [Verwaltung des Amazon S3 S3-Adapterspeichers mit AWS OpsHub](#)
- [Verwaltung der NFS-Schnittstelle mit AWS OpsHub](#)

Starten einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub

Gehen Sie wie folgt vor, um eine Amazon EC2 -kompatible Instance mit AWS OpsHub zu starten.

Um eine EC2 Amazon-kompatible Instance zu starten

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wenn Sie EC2 Amazon-kompatible Instances auf Ihrem Gerät ausführen, werden diese in der Spalte Instanzname unter Instances angezeigt. Sie können auf dieser Seite Details zu den einzelnen Instances anzeigen.
4. Wählen Sie Launch Instance (Instance starten) aus. Der Launch Instance Wizard wird geöffnet.
5. Wählen Sie unter Gerät das Snow-Gerät aus, auf dem Sie das Amazon EC2 -kompatible Gerät starten möchten.

Launch instance

×

Device

192.0.2.0

Image (AMI)

snow-al2-test-ami-1.0.2

Instance type

sbe-c.small

☒ Create public IP address (VNI)

☐ Use existing IP address (VNI)

☐ Do not attach IP address

Physical network interface

SFP+:a.bc-1d2ef456gg678gi9j

IP Address assignment

DHCP

☒ Create key pair

☐ Use existing key pair

☐ Do not attach key pair

Name

test-instance-key-pair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Create key pair

Cancel

Launch

6. Wählen Sie in Image (AMI) (Abbild (AMI)) ein Amazon Machine Image (AMI) aus der Liste aus. Dieses AMI wird zum Starten Ihrer Instance verwendet.
7. Wählen Sie in Instance type (Instance-Typ) einen Instance-Typ aus der Liste aus.
8. Legen Sie fest, wie der Instance eine IP-Adresse angefügt werden soll. Ihnen stehen folgende Optionen zur Verfügung:
 - Öffentliche IP-Adresse (VNI) erstellen — Wählen Sie diese Option, um eine neue IP-Adresse mithilfe einer physischen Netzwerkschnittstelle zu erstellen. Wählen Sie eine physische Netzwerkschnittstelle und eine IP-Adresszuweisung aus.
 - Bestehende IP-Adresse (VNI) verwenden — Wählen Sie diese Option, um eine vorhandene IP-Adresse und anschließend vorhandene virtuelle Netzwerkschnittstellen zu verwenden. Wählen Sie eine physische und eine virtuelle Netzwerkschnittstelle aus.
 - Keine IP-Adresse anhängen — Wählen Sie diese Option, wenn Sie keine IP-Adresse anhängen möchten.
9. Wählen Sie aus, wie Sie ein key pair an die Instance anhängen möchten. Ihnen stehen folgende Optionen zur Verfügung:

key pair erstellen — Wählen Sie diese Option, um ein neues key pair zu erstellen und die neue Instance mit diesem key pair zu starten.

Bestehendes key pair verwenden — Wählen Sie diese Option, um ein vorhandenes key pair zum Starten der Instance zu verwenden.

IP-Adresse nicht anhängen — Wählen Sie diese Option, wenn Sie kein key pair anhängen möchten. Sie müssen sich darüber im Klaren sein, dass Sie keine Verbindung zu dieser Instance herstellen können, es sei denn, Sie kennen das Passwort, das in dieses AMI integriert ist.

Weitere Informationen finden Sie unter [Arbeiten mit Schlüsselpaaren für EC2 -kompatible Instanzen in AWS OpsHub](#).
10. Wählen Sie Launch (Starten) aus. Die Instance sollte im Abschnitt Compute instances (Datenverarbeitungs-Instances) gestartet werden. Der State (Status) ist Pending (Ausstehend) und wird nach Abschluss in Running (Wird ausgeführt) geändert.

Stoppen einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub

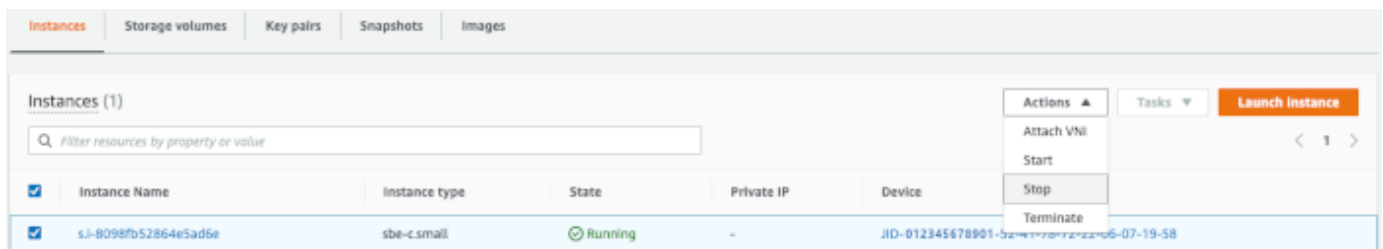
Gehen Sie wie folgt vor, um eine Amazon EC2 -kompatible Instance AWS OpsHub zu beenden.

So beenden Sie eine EC2 Amazon-kompatible Instance

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen.

Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.

3. Wenn Sie EC2 Amazon-kompatible Instances auf Ihrem Gerät ausführen, werden diese in der Spalte Instanzname unter Instances angezeigt.
4. Wählen Sie die Instance aus, die Sie beenden möchten, wählen Sie das Menü Aktionen und dann Stopp. Der State (Status) wird in Stopping (Wird angehalten) und anschließend nach Abschluss in Stopped (Angehalten) geändert.



Starten einer EC2 Amazon-kompatiblen Instance auf einem Snowball Edge mit AWS OpsHub

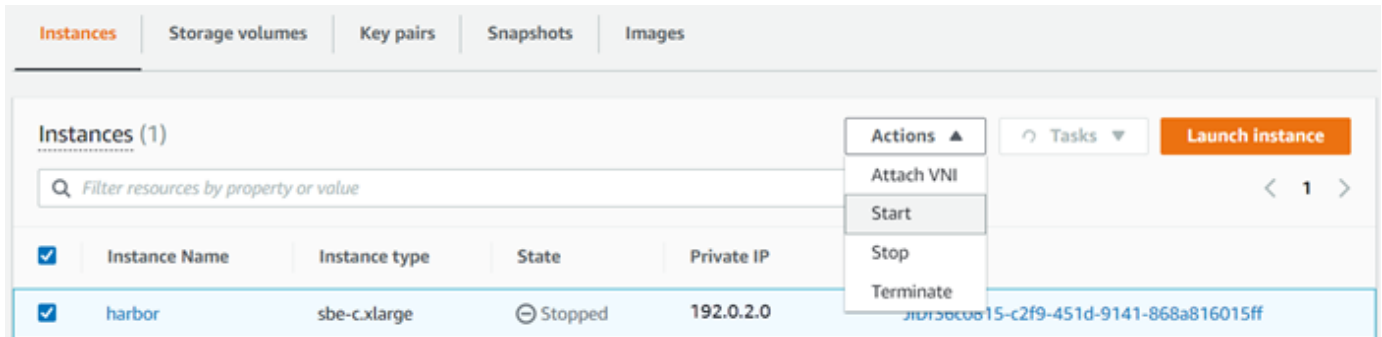
Gehen Sie wie folgt vor, um eine Amazon EC2 -kompatible Instance mit AWS OpsHub zu starten.

Um eine EC2 Amazon-kompatible Instance zu starten

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen.

Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.

- Suchen Sie in der Spalte Instance name (Instance-Name) unter Instances (Instanzen) die Instance, die Sie starten möchten.
- Wählen Sie die Instance und anschließend Start (Starten) aus. Der State (Status) wird in Pending (Ausstehend) und anschließend nach Abschluss in Running (Wird ausgeführt) geändert.



Arbeiten mit Schlüsselpaaren für EC2 -kompatible Instanzen in AWS OpsHub

Wenn Sie eine EC2 Amazon-kompatible Instance starten und beabsichtigen, über SSH eine Verbindung zu ihr herzustellen, müssen Sie ein key pair angeben. Sie können Amazon verwenden, EC2 um ein neues key pair zu erstellen, oder Sie können ein vorhandenes key pair importieren oder Ihre Schlüsselpaare verwalten.

Um Schlüsselpaare zu erstellen, zu importieren oder zu verwalten

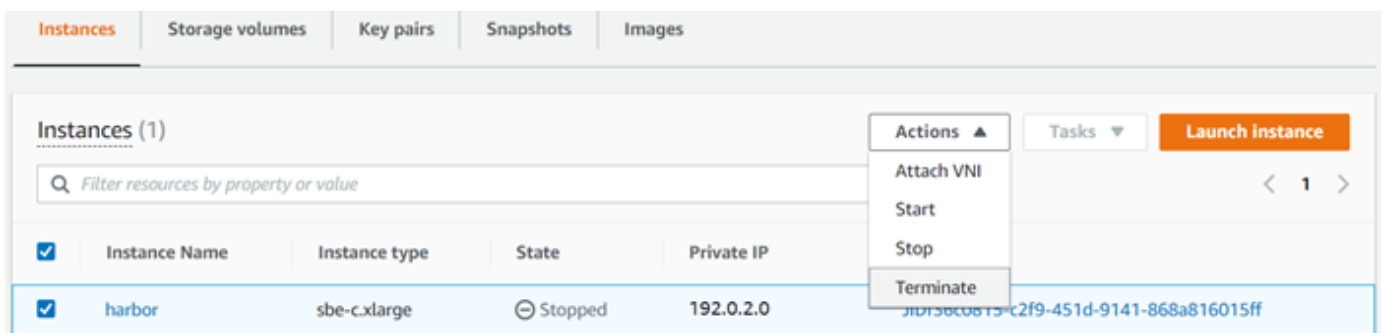
- Öffnen Sie Compute im AWS OpsHub Dashboard.
- Wählen Sie im Navigationsbereich die Seite Compute (EC2) und dann die Registerkarte Key Pairs aus. Sie werden zur EC2 Amazon-Konsole weitergeleitet, wo Sie Ihre Schlüsselpaare erstellen, importieren oder verwalten können.
- Anweisungen zum Erstellen und Importieren von Schlüsselpaaren finden Sie unter [EC2 Amazon-Schlüsselpaare und Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch.

Beenden einer Amazon EC2 -kompatiblen Instance mit AWS OpsHub

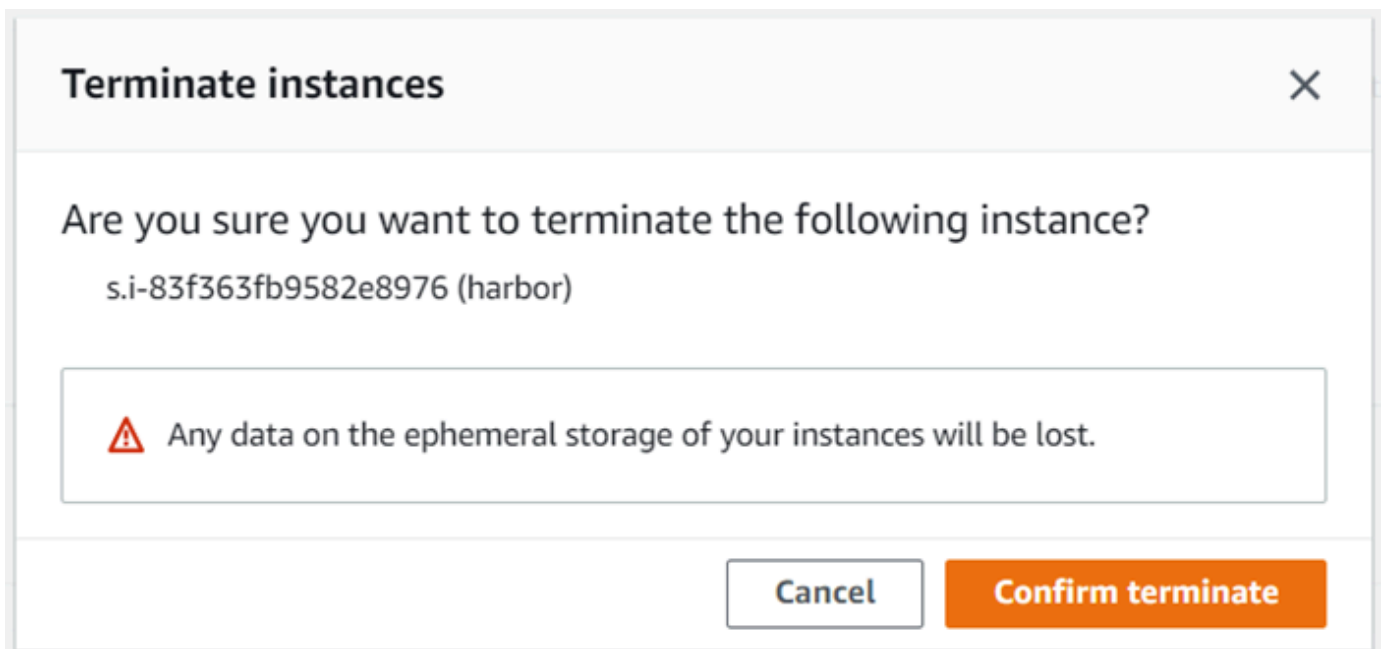
Nachdem Sie eine EC2 Amazon-kompatible Instance beendet haben, können Sie die Instance nicht neu starten.

Um eine EC2 Amazon-kompatible Instance zu beenden

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Sie können alle Ihre Datenverarbeitungsressourcen im Abschnitt Resources (Ressourcen) anzeigen.
3. Suchen Sie in der Spalte Instance name (Instance-Name) unter Instances (Instanzen) die Instance aus, die Sie beenden möchten.
4. Wählen Sie die Instanz und anschließend das Menü „Aktionen“ aus. Wählen Sie im Menü „Aktionen“ die Option „Beenden“.



5. Wählen Sie im Fenster „Instanzen beenden“ die Option „Beenden bestätigen“.



Note

Wenn die Instance beendet wurde, können Sie sie nicht neu starten.

Der State (Status) wird in Terminating (Wird beendet) und anschließend nach Abschluss in Terminated (Beendet) geändert.

Lokales Verwenden von Speichervolumes auf Snowball Edge mit AWS OpsHub

EC2Amazon-kompatible Instances verwenden Amazon EBS-Volumes für die Speicherung. In diesem Verfahren erstellen Sie ein Speicher-Volume und fügen es Ihrer Instance mithilfe von hinzu. AWS OpsHub

So erstellen Sie ein Speichervolume

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen.
3. Wählen Sie die Registerkarte Storage volumes (Speichervolumes) aus. Wenn auf Ihrem Gerät Speichervolumes vorhanden sind, werden die Details zu den Volumes unter Storage volumes (Speichervolumes) angezeigt.
4. Wählen Sie Create volume (Volume erstellen) aus, um die Seite Create volume (Volume erstellen) zu öffnen.

<< Back | Compute (EC2) > Create volume

Create Volume

Device
Select the device on which you wish to create the volume.

JID5a11d1db-8b98-4f37-80bf-97af46e45eb2 - 10.24.34.0 ▼

Size
Define the size of the volume, in GiBs.

100

Volume Type
Select a performance type for your volume.

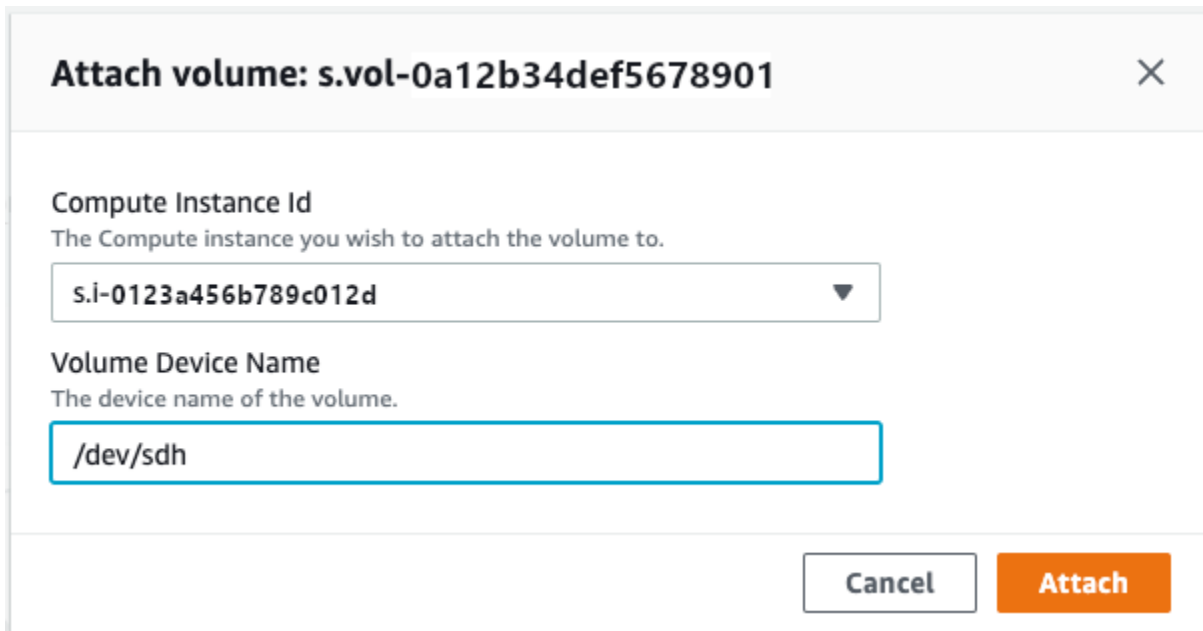
Capacity-optimized HDD volume (sbg1) ▼

Cancel Submit

5. Wählen Sie das Gerät aus, auf dem Sie das Volume erstellen möchten, geben Sie die Größe (in GiBs) ein, die Sie erstellen möchten, und wählen Sie den Typ des Volumes aus.
6. Wählen Sie Absenden aus. Der State (Status) wird Creating (Wird erstellt) und anschließend nach Abschluss in Available (Verfügbar) geändert. Sie können das Volume und dessen Details auf der Registerkarte Volumes (Volumes) anzeigen.

So fügen Sie Ihrer Instance ein Speichervolume an

1. Wählen Sie das Volume, das Sie erstellt haben, und anschließend Attach volume (Volume anfügen) aus.



The screenshot shows a dialog box titled "Attach volume: s.vol-0a12b34def5678901" with a close button (X) in the top right corner. Inside the dialog, there are two sections: "Compute Instance Id" and "Volume Device Name". The "Compute Instance Id" section has a description "The Compute instance you wish to attach the volume to." and a dropdown menu showing "s.i-0123a456b789c012d". The "Volume Device Name" section has a description "The device name of the volume." and a text input field containing "/dev/sdh". At the bottom right of the dialog, there are two buttons: "Cancel" and "Attach".

2. Wählen Sie unter Compute instance ID (Datenverarbeitungs-Instance-ID) die Instance aus, der Sie das Volume anfügen möchten.
3. Geben Sie in Volume Device Name (Volume-Gerätenamen) den Gerätenamen Ihres Volumes ein (z. B. **/dev/sdh** oder **xvdh**).
4. Wählen Sie Anfügen aus.

Wenn Sie das Volume nicht mehr benötigen, können Sie es von der Instance trennen und anschließend löschen.

Import eines Images als EC2 Amazon-kompatibles AMI mit AWS OpsHub

Sie können einen Snapshot Ihres Images in Ihr Snowball Edge-Gerät importieren und es als EC2 Amazon-kompatibles Amazon Machine Image (AMI) registrieren. Ein Snapshot ist im Grunde eine Kopie Ihres Speichervolumens, mit der Sie ein AMI oder ein anderes Speichervolume erstellen können. Auf diese Weise können Sie Ihr eigenes Bild von einer externen Quelle auf Ihr Gerät laden und es als EC2 Amazon-kompatible Instanz starten.

Folgen Sie diesen Schritten, um den Import Ihres Bildes abzuschließen.

1. Laden Sie Ihren Snapshot in einen Amazon S3 S3-Bucket auf Ihrem Gerät hoch.
2. Richten Sie die erforderlichen Berechtigungen ein, um Zugriff auf Amazon S3 EC2, Amazon und VM Import/Export zu gewähren, die Funktion, die zum Import und Export von Snapshots verwendet wird.
3. Importieren Sie den Snapshot aus dem S3-Bucket als Image auf Ihr Gerät.
4. Registrieren Sie das Image als EC2 Amazon-kompatibles AMI.
5. Starten Sie das AMI als EC2 Amazon-kompatible Instance.

Note

Beachten Sie beim Hochladen von Snapshots auf Snowball Edge die folgenden Einschränkungen.

- Snowball Edge unterstützt derzeit nur den Import von Schnappschüssen im RAW-Bildformat.
- Snowball Edge unterstützt derzeit nur den Import von Snapshots mit Größen von 1 GB bis 1 TB.

Schritt 1: Laden Sie einen Snapshot in einen S3-Bucket auf Ihrem Gerät hoch

Sie müssen Ihren Snapshot auf Ihrem Gerät auf Amazon S3 hochladen, bevor Sie ihn importieren. Dies liegt daran, dass Snapshots nur aus Amazon S3 importiert werden können, das auf Ihrem Gerät oder Cluster verfügbar ist. Während des Importvorgangs wählen Sie den S3-Bucket auf Ihrem Gerät aus, in dem das Bild gespeichert werden soll.

Um einen Snapshot auf Amazon S3 hochzuladen

- Informationen zum Erstellen eines S3-Buckets finden Sie unter [Amazon S3 S3-Speicher erstellen](#).

Informationen zum Hochladen eines Snapshots in einen S3-Bucket finden Sie unter [Dateien in Amazon S3 S3-Speicher hochladen](#).

Schritt 2: Importieren Sie den Snapshot aus einem S3-Bucket

Wenn Ihr Snapshot auf Amazon S3 hochgeladen wurde, können Sie ihn auf Ihr Gerät importieren. Alle Snapshots, die importiert wurden oder gerade importiert werden, werden auf der Registerkarte Schnappschüsse angezeigt.

Um den Snapshot auf Ihr Gerät zu importieren

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie den Tab „Schnappschüsse“, um alle Schnappschüsse zu sehen, die auf Ihr Gerät importiert wurden. Die Bilddatei in Amazon S3 ist eine RAW-Datei, die als Snapshot auf Ihr Gerät importiert wird. Sie können nach der Snapshot-ID oder dem Status des Snapshots filtern, um bestimmte Snapshots zu finden. Sie können eine Snapshot-ID wählen, um Details zu diesem Snapshot zu sehen.
4. Wählen Sie den Snapshot aus, den Sie importieren möchten, und wählen Sie Snapshot importieren, um die Seite Snapshot importieren zu öffnen.
5. Wählen Sie unter Gerät die IP-Adresse des Snow Family-Geräts aus, auf das Sie importieren möchten.
6. Geben Sie unter Beschreibung importieren und Beschreibung des Snapshots jeweils eine Beschreibung ein.
7. Wählen Sie in der Rollenliste eine Rolle aus, die für den Import verwendet werden soll. Snowball Edge verwendet VM, um Snapshots Import/Export zu importieren. AWS übernimmt diese Rolle und verwendet sie, um den Snapshot in Ihrem Namen zu importieren. Wenn Sie auf Ihrem keine Rolle konfiguriert haben AWS Snowball Edge, öffnen Sie das AWS Identity and Access Management (IAM), in AWS OpsHub dem Sie eine lokale IAM-Rolle erstellen können. Für die

Rolle ist außerdem eine Richtlinie erforderlich, die über die erforderlichen Import/Export VM-Berechtigungen verfügt, um den Import durchzuführen. Sie müssen diese Richtlinie an die Rolle anhängen. Weitere Informationen dazu finden Sie unter [Lokales Verwenden von IAM](#).

Im Folgenden finden Sie ein Beispiel für die Richtlinie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vmie.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.

Die von Ihnen erstellte Rolle sollte über Mindestberechtigungen für den Zugriff auf Amazon S3 verfügen. Im Folgenden finden Sie ein Beispiel für eine Mindestrichtlinie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetMetadata"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
        "arn:aws:s3:::import-snapshot-bucket-name",
        "arn:aws:s3:::import-snapshot-bucket-name/*"
    ]
}
]
```

8. Wählen Sie Browse S3 und wählen Sie den S3-Bucket aus, der den Snapshot enthält, den Sie importieren möchten. Wählen Sie den Snapshot aus und klicken Sie auf Senden. Der Snapshot wird auf Ihr Gerät heruntergeladen. Sie können die Snapshot-ID wählen, um die Details zu sehen. Sie können den Importvorgang von dieser Seite aus abbrechen.

Schritt 3: Registrieren Sie den Snapshot als EC2 Amazon-kompatibles AMI

Das Erstellen eines EC2 Amazon-kompatiblen AMI aus einem als Snapshot importierten Image wird als Registrierung bezeichnet. Bilder, die auf Ihr Gerät importiert werden, müssen registriert werden, bevor sie als EC2 Amazon-kompatible Instances gestartet werden können.

Um ein als Snapshot importiertes Bild zu registrieren

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie die Registerkarte Images. Sie können die Bilder nach Name, ID oder Bundesland filtern, um ein bestimmtes Bild zu finden.
4. Wählen Sie das Bild aus, das Sie registrieren möchten, und wählen Sie Bild registrieren.

	Name	Id	State	Description
☐	test-image	s.ami-8087a170e24a3124d	Available	test-image-oopshub-1.15.6
☐	SnowAL2	s.ami-88833957b18097f46	Available	-
☐	test for 1.15.2	s.ami-8c4d8b29618568414	Available	-
☒	testing	s.ami-8de47d2e397937318	Available	tesing
☐	test-windows	s.ami-8f12682f18b1de4e2	Available	windows-test

5. Geben Sie auf der Seite Bild registrieren einen Namen und eine Beschreibung ein.
6. Geben Sie für Root-Volume den Namen des Root-Geräts an.

Im Abschnitt Gerät blockieren können Sie die Größe des Volumes und den Volumetyp ändern.

7. Wenn Sie möchten, dass das Volume gelöscht wird, wenn die Instance beendet wird, wählen Sie Bei Kündigung löschen.
8. Wenn Sie weitere Volumes hinzufügen möchten, wählen Sie Neues Volume hinzufügen.
9. Wenn Sie fertig sind, wählen Sie Submit.

Schritt 4: Starten Sie das EC2 Amazon-kompatible AMI

- Weitere Informationen finden Sie unter [Starten einer Amazon EC2 -kompatiblen Instance](#).

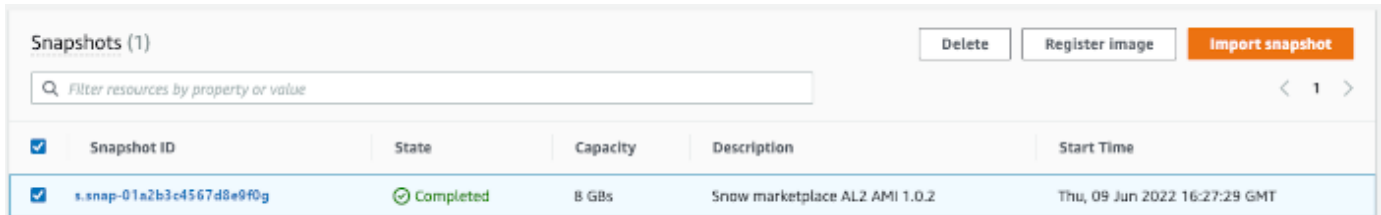
Löschen eines Snapshots aus einem Snowball Edge mit AWS OpsHub

Wenn Sie einen Snapshot nicht mehr benötigen, können Sie ihn von Ihrem Gerät löschen. Die Bilddatei in Amazon S3 ist eine RAW-Datei, die als Snapshot auf Ihr Gerät importiert wird. Wenn der Snapshot, den Sie löschen, von einem Image verwendet wird, kann er nicht gelöscht werden. Nach Abschluss des Imports können Sie auch die RAW-Datei, die Sie auf Amazon S3 hochgeladen haben, auf Ihrem Gerät löschen.

So löschen Sie einen Snapshot

1. Öffnen Sie die AWS OpsHub Anwendung.

2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie den Tab Snapshot, um alle importierten Snapshots zu sehen. Sie können nach Snapshot-ID oder Status des Snapshots filtern, um bestimmte Snapshots zu finden.
4. Wählen Sie den Snapshot aus, den Sie löschen möchten, und klicken Sie auf Löschen. Sie können mehrere Schnappschüsse auswählen.



The screenshot shows the 'Snapshots (1)' section of the AWS console. At the top, there are buttons for 'Delete', 'Register image', and 'Import snapshot'. Below these is a search bar with the placeholder text 'Filter resources by property or value'. A table below the search bar lists the snapshots. The table has columns for 'Snapshot ID', 'State', 'Capacity', 'Description', and 'Start Time'. One snapshot is listed with ID 's.snap-01a2b3c4567d8e9f0g', state 'Completed', capacity '8 GBs', description 'Snow marketplace AL2 AMI 1.0.2', and start time 'Thu, 09 Jun 2022 16:27:29 GMT'.

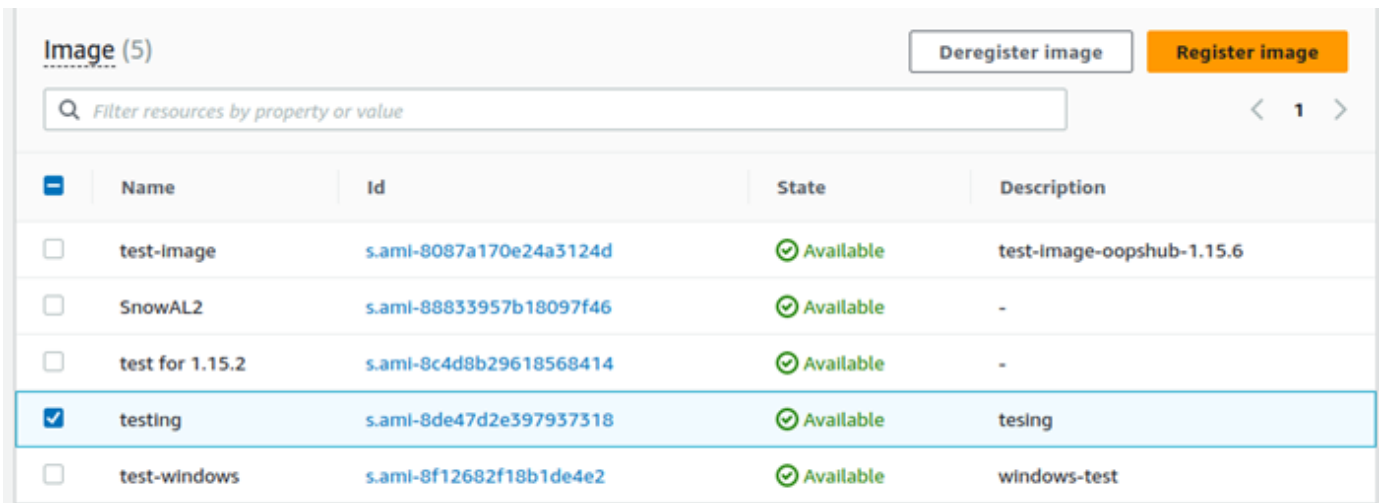
Snapshot ID	State	Capacity	Description	Start Time
s.snap-01a2b3c4567d8e9f0g	Completed	8 GBs	Snow marketplace AL2 AMI 1.0.2	Thu, 09 Jun 2022 16:27:29 GMT

5. Wählen Sie im Bestätigungsfeld „Snapshot löschen“ die Option Snapshot löschen aus. Wenn das Löschen erfolgreich ist, wird der Snapshot aus der Liste auf der Registerkarte Schnappschüsse entfernt.

Abmeldung eines AMI auf einem Snowball Edge mit AWS OpsHub

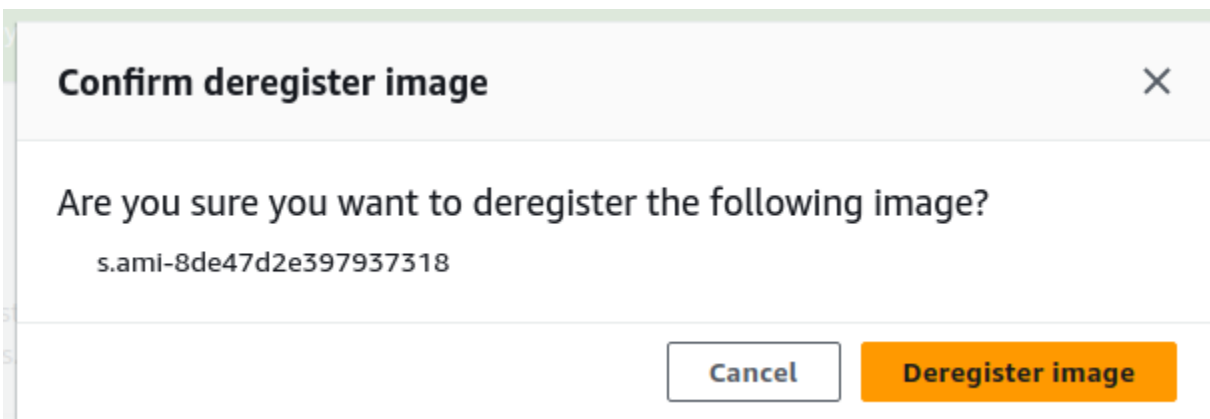
So heben Sie die Registrierung eines AMI auf

1. Öffnen Sie die Anwendung. AWS OpsHub
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Oder wählen Sie oben das Menü Dienste und dann Compute (EC2), um die Compute-Seite zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie die Registerkarte Images. Alle Ihre Bilder werden aufgelistet. Sie können die Bilder nach Name, ID oder Bundesland filtern, um ein bestimmtes Bild zu finden.
4. Wählen Sie das Bild aus, dessen Registrierung Sie aufheben möchten, und wählen Sie Abmelden.



	Name	Id	State	Description
☐	test-image	s.ami-8087a170e24a3124d	Available	test-image-oopshub-1.15.6
☐	SnowAL2	s.ami-88833957b18097f46	Available	-
☐	test for 1.15.2	s.ami-8c4d8b29618568414	Available	-
☒	testing	s.ami-8de47d2e397937318	Available	tesing
☐	test-windows	s.ami-8f12682f18b1de4e2	Available	windows-test

5. Bestätigen Sie im Fenster Bild abmelden bestätigen die Bild-ID und wählen Sie Bild abmelden. Wenn die Abmeldung erfolgreich ist, wird das Bild aus der Bilderliste entfernt.



Verwaltung eines EC2 Amazon-Clusters auf Snowball Edge mit AWS OpsHub

Ein EC2 Amazon-Cluster ist eine Gruppe von Geräten, die zusammen als Gerätecluster bereitgestellt werden. Um einen Cluster verwenden zu können, müssen die AWS Dienste auf Ihrem Gerät auf Ihrem Standardendpunkt ausgeführt werden. Sie müssen auch das spezifische Gerät im Cluster auswählen, mit dem Sie kommunizieren möchten. Sie verwenden einen Cluster auf Gerätebasis.

Um einen EC2 Amazon-Cluster zu erstellen

1. Stellen Sie eine Verbindung her und melden Sie sich an Ihrem Snow-Gerät an. Anleitungen zur Anmeldung an Ihrem Gerät finden Sie unter [Entsperren eines Snowball Edge-Geräts mit AWS OpsHub](#).

2. Wählen Sie auf der Seite Gerät auswählen die Option Snowball Edge-Cluster und dann Weiter aus.
3. Geben Sie auf der Seite Connect to your device (Mit ihrem Gerät verbinden) die IP-Adresse des Geräts und die IP-Adressen weiterer Geräte im Cluster an.
4. Wählen Sie Add another device (Weiteres Gerät hinzufügen) aus, um weitere Geräte hinzuzufügen. Wählen Sie anschließend Next (Weiter) aus.
5. Geben Sie auf der Seite Provide the keys (Schlüssel angeben) den Entsperrungscode des Geräte-Clients ein, laden Sie das Gerätemanifest hoch und wählen Sie Unlock device (Gerät entsperren) aus.

Snowball Edge-Geräte verwenden eine 256-Bit-Verschlüsselung, um sowohl die Sicherheit als auch die Vollständigkeit Ihrer Daten chain-of-custody zu gewährleisten.

6. (Optional) Geben Sie einen Namen ein, um ein Profil zu erstellen, und wählen Sie dann Profilname speichern. Sie werden zum Dashboard weitergeleitet, in dem alle Ihre Cluster angezeigt werden.

Sie können jetzt damit beginnen, AWS Dienste zu nutzen und Ihren Cluster zu verwalten. Sie verwalten die Instances im Cluster genau wie einzelne Instances. Detaillierte Anweisungen finden Sie unter [Verwaltung von AWS Diensten auf dem Snowball Edge mit AWS OpsHub](#).

Richten Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ein mit AWS OpsHub

Der Amazon S3 S3-kompatible Speicher im Snowball Edge-Service ist standardmäßig nicht aktiv. Um den Service auf einem Gerät oder einem Cluster zu starten, müssen Sie auf jedem Gerät zwei virtuelle Netzwerkschnittstellen (VNICs) erstellen, die mit den `s3api` Endpunkten `s3control` und verbunden werden.

Themen

- [Voraussetzungen für Amazon S3 S3-kompatibler Speicher auf Snowball Edge AWS OpsHub](#)
- [Verwenden des Amazon S3 S3-kompatiblen Speichers auf Snowball Edge \(einfache Einrichtungsoption\) in AWS OpsHub](#)
- [Verwenden der erweiterten Einrichtungsoption für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mithilfe von AWS OpsHub](#)

- [Konfiguration von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge für den automatischen Start der Verwendung AWS OpsHub](#)
- [Erstellen eines Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit AWS OpsHub](#)
- [Laden Sie Dateien und Ordner in einen Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets hoch mit AWS OpsHub](#)
- [Entfernen Sie Dateien und Ordner aus dem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets mit AWS OpsHub](#)
- [Löschen Sie Buckets aus dem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#)

Voraussetzungen für Amazon S3 S3-kompatibler Speicher auf Snowball Edge AWS OpsHub

Bevor Sie Ihr Gerät oder Ihren Cluster mit einrichten können AWS OpsHub, gehen Sie wie folgt vor:

- Schalten Sie Ihr Snowball Edge-Gerät ein und verbinden Sie es mit Ihrem Netzwerk.
- Laden Sie auf Ihrem lokalen Computer die neueste Version von [AWS OpsHub](#) herunter und installieren Sie sie. Connect zum Gerät oder Cluster her, um es mit einer Manifestdatei zu entsperren. Weitere Informationen finden Sie unter [Entsperren eines Geräts](#).

Verwenden des Amazon S3 S3-kompatiblen Speichers auf Snowball Edge (einfache Einrichtungsoption) in AWS OpsHub

Verwenden Sie die einfache Einrichtungsoption, wenn Ihr Netzwerk DHCP verwendet. Mit dieser Option VNICs werden sie automatisch auf jedem Gerät erstellt, wenn Sie den Dienst starten.

1. Melden Sie sich an AWS OpsHub und wählen Sie dann Speicher verwalten.

Dadurch gelangen Sie zur Landingpage mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge.

2. Wählen Sie für den Setup-Typ „Service starten“ die Option Simple aus.
3. Wählen Sie Dienst starten.

Note

Dieser Vorgang dauert einige Minuten und hängt von der Anzahl der verwendeten Geräte ab.

Nach dem Start des Dienstes ist der Dienststatus aktiv und es gibt Endpunkte.

The screenshot displays the AWS OpsHub interface for 'Amazon S3 compatible storage on Snow'. At the top, there are buttons for 'Stop service' and 'Start service setup'. Below this, a section titled 'Amazon S3 compatible storage on Snow resources' includes a refresh button and an 'Enable service auto-start' button. The status section shows: Service state is 'Active' (green checkmark), Service auto-start is 'Disabled' (grey circle), S3 storage available is '-', S3 endpoint status is 'Active' (green checkmark), S3 endpoint is '10.0.0.8', S3Control endpoint status is 'Active' (green checkmark), and S3Control endpoint is '10.0.0.1'. Below the status section, the 'Buckets (8)' section shows a search bar, 'Empty', 'Delete', and 'Create bucket' buttons. A table lists one bucket named '1bucket' created on 'Thu, 16 Mar 2023 00:51:53 GMT'.

Verwenden der erweiterten Einrichtungsoption für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mithilfe von AWS OpsHub

Verwenden Sie die erweiterte Einrichtungsoption, wenn Ihr Netzwerk statische IP-Adressen verwendet oder wenn Sie vorhandene VNIs wiederverwenden möchten. Mit dieser Option erstellen Sie VNIs für jedes Gerät manuell.

1. Melden Sie sich an AWS OpsHub und wählen Sie dann Speicher verwalten.

Dadurch gelangen Sie zur Landingpage mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge.

2. Wählen Sie für den Setup-Typ „Service starten“ die Option Erweitert aus.
3. Wählen Sie die Geräte aus, VNIs für die Sie etwas erstellen müssen.

Für Cluster benötigen Sie ein Mindestquorum an Geräten, um den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Service zu starten. Das Quorum beträgt zwei für einen Cluster mit drei Knoten.

 Note

Für den ersten Start des Dienstes in einem Cluster-Setup müssen alle Geräte im Cluster konfiguriert und verfügbar sein, damit der Dienst gestartet werden kann. Für nachfolgende Starts können Sie eine Teilmenge der Geräte verwenden, wenn Sie das Quorum erreichen, der Dienst wird jedoch in einem heruntergestuften Zustand gestartet.

4. Wählen Sie für jedes Gerät eine vorhandene VNIC oder wählen Sie Create VNI aus.

Jedes Gerät benötigt eine VNIC für den S3-Endpunkt für Objektoperationen und eine weitere für den S3Control-Endpunkt für Bucket-Operationen.

5. Wenn Sie eine VNIC erstellen, wählen Sie eine physische Netzwerkschnittstelle aus, geben Sie die Status-IP-Adresse und die Subnetzmaske ein und wählen Sie dann Virtuelle Netzwerkschnittstelle erstellen.
6. Nachdem Sie Ihre VNICS erstellt haben, wählen Sie Dienst starten.

 Note

Dieser Vorgang dauert einige Minuten und hängt von der Anzahl der verwendeten Geräte ab.

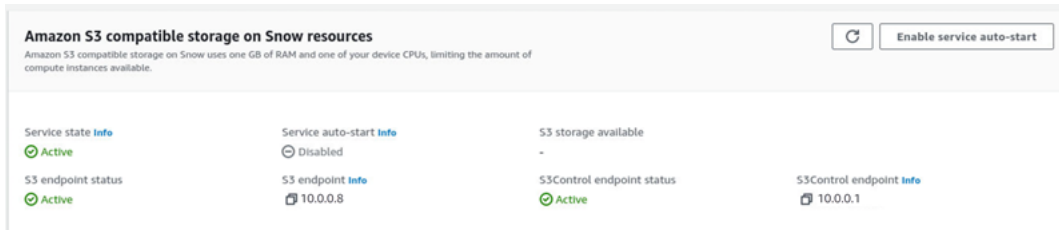
Nach dem Start des Dienstes ist der Dienststatus aktiv und es gibt Endpunkte.

Konfiguration von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge für den automatischen Start der Verwendung AWS OpsHub

1. Melden Sie sich an AWS OpsHub und wählen Sie dann Speicher verwalten.

Dadurch gelangen Sie zur Landingpage mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge.

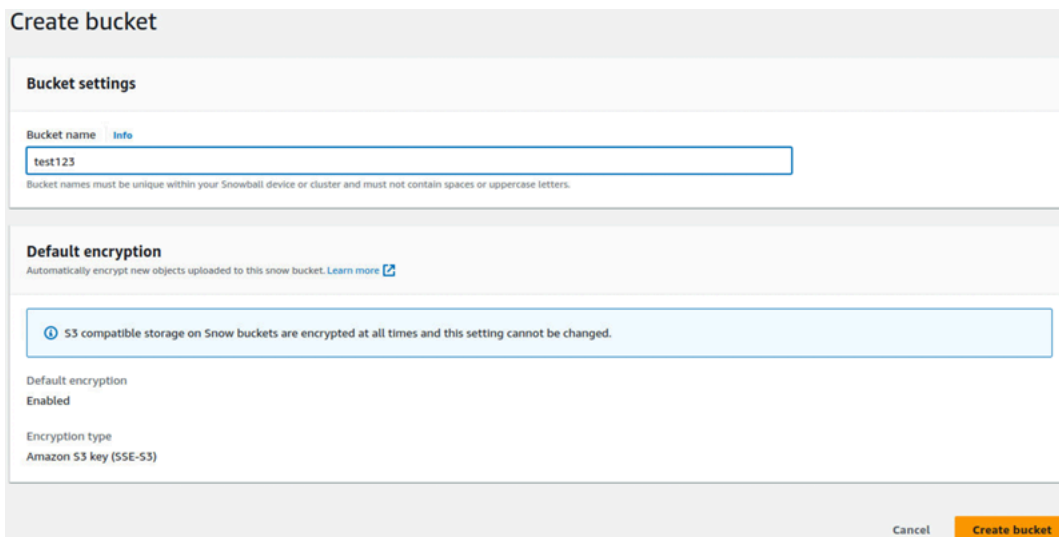
2. Wählen Sie im Amazon S3 S3-kompatiblen Speicher auf Snow-Ressourcen die Option Automatischen Start des Dienstes aktivieren aus. Das System konfiguriert den Dienst so, dass er in future automatisch gestartet wird.



Erstellen eines Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit AWS OpsHub

Verwenden Sie die AWS OpsHub Benutzeroberfläche, um einen Amazon S3 S3-Bucket auf Ihrem Snowball Edge-Gerät zu erstellen.

1. Öffnen AWS OpsHub.
2. Wählen Sie unter Speicher verwalten die Option Erste Schritte aus. Die Seite Amazon S3 S3-kompatibler Speicher auf Snow wird angezeigt.
3. Wählen Sie unter Buckets die Option Create Bucket aus. Der Bildschirm Create Bucket wird angezeigt.



4. Geben Sie im Feld Bucket-Name einen Namen für den Bucket ein.

Note

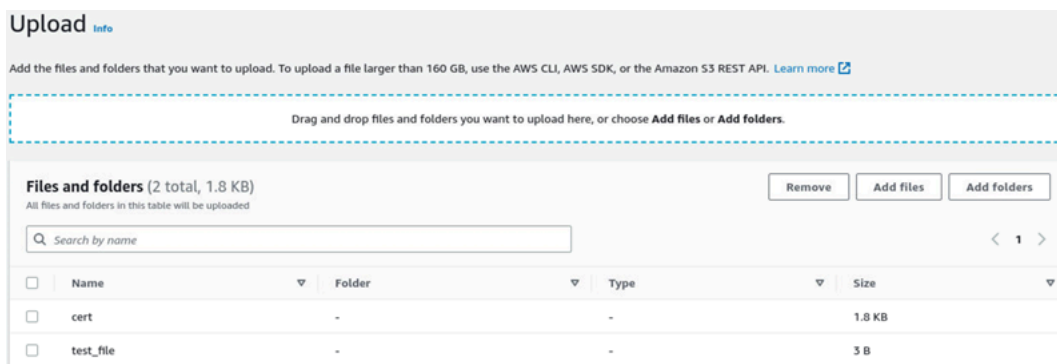
Bucket-Namen müssen innerhalb Ihres Snowball-Geräts oder -Clusters eindeutig sein und dürfen keine Leerzeichen oder Großbuchstaben enthalten.

5. Wählen Sie Create Bucket (Bucket erstellen) aus. Das System erstellt den Bucket und er erscheint unter Buckets auf der Amazon S3 S3-kompatiblen Speicherseite auf der Snow-Seite.

Laden Sie Dateien und Ordner in einen Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets hoch mit AWS OpsHub

Verwenden Sie die AWS OpsHub Schnittstelle, um Dateien und Ordner in einen Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets hochzuladen. Dateien und Ordner können separat oder zusammen hochgeladen werden.

1. Öffnen AWS OpsHub
2. Wählen Sie unter Speicher verwalten unter Buckets einen Bucket aus, in den Dateien hochgeladen werden sollen. Die Seite für diesen Bucket wird angezeigt.
3. Wählen Sie auf der Bucket-Seite die Option Dateien hochladen aus. Die Upload-Seite wird angezeigt.



4. Laden Sie Dateien oder Ordner hoch, indem Sie sie aus dem Dateimanager des Betriebssystems in das AWS OpsHub Fenster ziehen, oder gehen Sie wie folgt vor:
 - a. Wählen Sie Dateien hinzufügen oder Ordner hinzufügen aus.
 - b. Wählen Sie eine oder mehrere Dateien oder Ordner zum Hochladen aus. Wählen Sie Öffnen aus.

Das System lädt die ausgewählten Dateien und Ordner in den Bucket auf dem Gerät hoch. Nach Abschluss des Uploads werden die Namen der Dateien und Ordner in der Liste Dateien und Ordner angezeigt.

Entfernen Sie Dateien und Ordner aus dem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets mit AWS OpsHub AWS OpsHub

Verwenden Sie die AWS OpsHub Benutzeroberfläche, um Dateien und Ordner aus Buckets auf dem Snowball Edge-Gerät zu entfernen und dauerhaft zu löschen.

1. Öffnen. AWS OpsHub
2. Wählen Sie unter Speicher verwalten unter Buckets den Namen eines Buckets aus, aus dem Dateien und Ordner gelöscht werden sollen. Die Seite für diesen Bucket wird angezeigt.
3. Aktivieren Sie unter Dateien und Ordner die Kontrollkästchen der Dateien und Ordner, die dauerhaft gelöscht werden sollen.
4. Wählen Sie Entfernen aus. Das System entfernt die Dateien oder Ordner aus dem Bucket auf dem Gerät.

Löschen Sie Buckets aus dem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge

Bevor Sie einen Bucket von einem Gerät löschen können, muss der Bucket leer sein. Entfernen Sie entweder Dateien und Ordner aus dem Bucket oder verwenden Sie das Tool „Bucket leeren“. Informationen zum Entfernen von Dateien und Ordnern finden Sie unter [Entfernen Sie Dateien und Ordner aus dem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Buckets mit AWS OpsHub AWS OpsHub](#).

So verwenden Sie das Tool „Bucket leeren“

1. Öffnen AWS OpsHub.
2. Wählen Sie unter Speicher verwalten unter Buckets das Optionsfeld des Buckets aus, den Sie leeren möchten.
3. Wählen Sie Leer aus. Die Seite „Bucket leeren“ wird angezeigt.

4. Geben Sie in das Textfeld auf der Seite Leerer Bucket den Text ein. **permanently delete**
5. Wählen Sie Leer aus. Das System leert den Bucket.

Um einen leeren Bucket zu löschen

1. Wählen Sie unter Speicher verwalten unter Buckets das Optionsfeld des Buckets aus, den Sie löschen möchten.
2. Wählen Sie Löschen aus. Die Seite „Bucket löschen“ wird angezeigt.

3. Geben Sie in das Textfeld auf der Seite „Bucket löschen“ den Namen des Buckets ein.
4. Wählen Sie Löschen aus. Das System löscht den Bucket vom Gerät.

Verwaltung des Amazon S3 S3-Adapterspeichers mit AWS OpsHub

Sie können es verwenden AWS OpsHub , um Amazon Simple Storage Service (Amazon S3) - Speicher auf Ihrem Snowball Edge mithilfe des S3-Adapters für Import- und Exportaufträge zu erstellen und zu verwalten.

Themen

- [Zugreifen auf Amazon S3 S3-Speicher mit AWS OpsHub](#)
- [Hochladen von Dateien in den Amazon S3 S3-Speicher mit AWS OpsHub](#)
- [Dateien aus dem Amazon S3 S3-Speicher herunterladen mit AWS OpsHub](#)

- [Löschen von Dateien aus dem Amazon S3 S3-Speicher mit AWS OpsHub](#)

Zugreifen auf Amazon S3 S3-Speicher mit AWS OpsHub

Sie können Dateien zu Ihrem Gerät hochladen und lokal auf die Dateien zugreifen. Sie können sie physisch an einen anderen Ort auf dem Gerät verschieben oder sie wieder dorthin importieren, AWS Cloud wenn das Gerät zurückgegeben wird.

Snowball Edge verwendet Amazon S3 S3-Buckets, um Dateien auf Ihrem Gerät zu speichern und zu verwalten.

Um auf einen S3-Bucket zuzugreifen

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Manage file storage (Dateispeicher verwalten) die Option Get started (Erste Schritte) aus.

Wenn Ihr Gerät mit dem Amazon S3 S3-Übertragungsmechanismus bestellt wurde, werden sie im Bereich Buckets auf der Datei- und Objektspeicherseite angezeigt. Auf der Seite Datei- und Objektspeicher können Sie Details zu jedem Bucket einsehen.

Note

Wenn das Gerät mit dem NFS-Übertragungsmechanismus bestellt wurde, erscheint der Bucket-Name nach der Konfiguration und Aktivierung des NFS-Dienstes im Bereich Mount-Points. Weitere Informationen zur Verwendung der NFS-Schnittstelle finden Sie unter. [Verwaltung der NFS-Schnittstelle mit AWS OpsHub](#)

File & object storage

Use Amazon S3 to manage files and objects stored on your device. Add files to the device so they can be accessed locally. For import jobs, the files will be transferred to AWS when the device is sent back.

Resources

Storage available

925.85 GB available of 925.93 GB

99%

Select a bucket below to start transferring files to your device.

Buckets (7)

Filter buckets

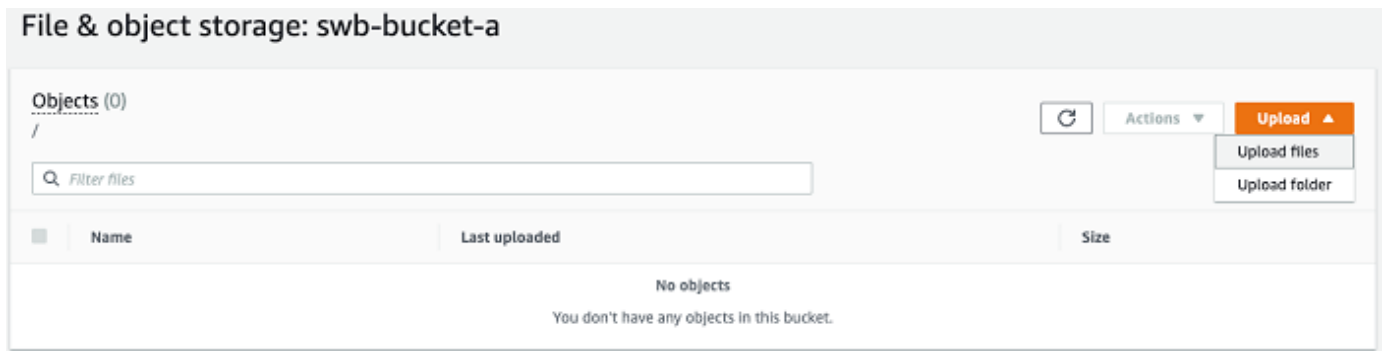
< 1 >

Bucket name	Date created
sbw-output	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-a	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-b	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-c	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-d	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-e	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-f	Mon, 12 Oct 2009 17:50:30 GMT

Hochladen von Dateien in den Amazon S3 S3-Speicher mit AWS OpsHub

So laden Sie eine Datei hoch

1. Wählen Sie im Abschnitt Manage file storage (Dateispeicher verwalten) die Option Get started (Erste Schritte) aus. Wenn Sie Amazon S3 S3-Buckets auf Ihrem Gerät haben, werden diese im Abschnitt Buckets auf der Dateispeicherseite angezeigt. Sie können auf der Seite Details zu den einzelnen Buckets anzeigen.
2. Wählen Sie den Bucket aus, zu dem Sie Dateien hochladen möchten.
3. Wählen Sie Hochladen und dann Dateien hochladen oder ziehen Sie die Dateien per Drag-and-Drop in den Bucket und wählen Sie OK.



Note

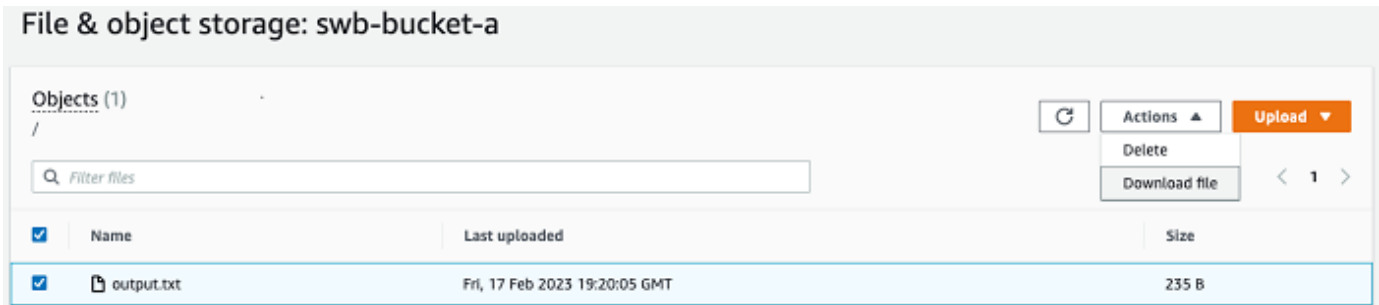
Um größere Dateien hochzuladen, können Sie die Funktion für den mehrteiligen Upload in Amazon S3 verwenden, indem Sie AWS CLI Weitere Informationen zur Konfiguration der S3-CLI-Einstellungen finden Sie unter [CLI S3-Konfiguration](#). Weitere Informationen zum mehrteiligen Upload finden Sie unter [Überblick über mehrteilige Uploads](#) im Amazon Simple Storage Service-Benutzerhandbuch

Das Hochladen eines Ordners von einem lokalen Computer auf Snowball Edge mithilfe von AWS OpsHub wird unterstützt. Wenn der Ordner sehr groß ist, dauert es einige Zeit, OpsHub bis die file/folder Auswahl gelesen ist. Beim Lesen der Dateien und Ordner OpsHub wird kein Fortschritts-Tracker angezeigt. Es wird jedoch angezeigt, dass ein Fortschritts-Tracker angezeigt wird, sobald der Upload-Vorgang beginnt.

Dateien aus dem Amazon S3 S3-Speicher herunterladen mit AWS OpsHub

So laden Sie eine Datei herunter

1. Wählen Sie im Abschnitt Manage file storage (Dateispeicher verwalten) die Option Get started (Erste Schritte) aus. Wenn Sie auf Ihrem Gerät S3-Buckets verwenden, werden sie im Abschnitt Buckets (Buckets) auf der Seite File storage (Dateispeicher) angezeigt. Sie können auf der Seite Details zu den einzelnen Buckets anzeigen.
2. Wählen Sie den Bucket aus, aus dem Sie Dateien herunterladen möchten, und navigieren Sie zu der Datei, die Sie herunterladen möchten. Wählen Sie eine oder mehrere Dateien aus.



3. Wählen Sie im Menü Actions (Aktionen) die Option Download (Herunterladen) aus.
4. Wählen Sie einen Speicherort aus, zu dem die Datei heruntergeladen werden soll. Wählen Sie anschließend OK aus.

Löschen von Dateien aus dem Amazon S3 S3-Speicher mit AWS OpsHub

Wenn Sie eine Datei nicht mehr benötigen, können Sie sie aus Ihrem Amazon S3 S3-Bucket löschen.

Löschen Sie eine Datei wie folgt:

1. Wählen Sie im Abschnitt Manage file storage (Dateispeicher verwalten) die Option Get started (Erste Schritte) aus. Wenn Sie Amazon S3 S3-Buckets auf Ihrem Gerät haben, werden diese im Abschnitt Buckets auf der Dateispeicherseite angezeigt. Sie können auf der Seite Details zu den einzelnen Buckets anzeigen.
2. Wählen Sie den Bucket, aus dem Sie Dateien löschen möchten, und navigieren Sie zu der Datei, die Sie löschen möchten.
3. Wählen Sie im Menü Actions die Option Delete.
4. Wählen Sie im jetzt angezeigten Dialogfeld Confirm delete (Löschen bestätigen) aus.

Verwaltung der NFS-Schnittstelle mit AWS OpsHub

Verwenden Sie die NFS-Schnittstelle (Network File System), um Dateien auf den Snowball Edge hochzuladen, als ob das Gerät ein lokaler Speicher Ihres Betriebssystems wäre. Dies ermöglicht einen benutzerfreundlicheren Ansatz für die Übertragung von Daten, da Sie Funktionen Ihres Betriebssystems wie das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche verwenden können. Jeder S3-Bucket auf dem Gerät ist als Endpunkt der NFS-Schnittstelle verfügbar und kann für das Kopieren von Daten bereitgestellt werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

Sie können die NFS-Schnittstelle verwenden, wenn das Snowball Edge-Gerät so konfiguriert wurde, dass es bei der Erstellung des Auftrags zur Bestellung des Geräts berücksichtigt wurde. Wenn das Gerät nicht so konfiguriert ist, dass es die NFS-Schnittstelle enthält, verwenden Sie den S3-Adapter oder Amazon S3 S3-kompatible Speicher auf Snowball Edge, um Daten zu übertragen. Weitere Informationen zum S3-Adapter finden Sie unter [Verwaltung des Amazon S3 S3-Adapterspeichers mit AWS OpsHub](#). Weitere Informationen zu Amazon S3 S3-kompatiblen Speicher auf Snowball Edge finden Sie unter [Richten Sie Amazon S3 S3-kompatible Speicher auf Snowball Edge ein mit AWS OpsHub](#).

Beim Start verwendet die NFS-Schnittstelle 1 GB Arbeitsspeicher und 1 CPU. Dies kann die Anzahl anderer Dienste, die auf dem Snowball Edge ausgeführt werden, oder die Anzahl der EC2 - kompatiblen Instanzen, die ausgeführt werden können, einschränken.

Daten, die über die NFS-Schnittstelle übertragen werden, werden bei der Übertragung nicht verschlüsselt. Bei der Konfiguration der NFS-Schnittstelle können Sie CIDR-Blöcke bereitstellen, und Snowball Edge schränkt den Zugriff auf die NFS-Schnittstelle von Client-Computern mit Adressen in diesen Blöcken aus.

Dateien auf dem Gerät werden nach der Rückgabe an Amazon S3 übertragen AWS. Weitere Informationen finden Sie unter [Jobs in Amazon S3 importieren](#).

Weitere Informationen zur Verwendung von NFS mit Ihrem Computerbetriebssystem finden Sie in der Dokumentation zu Ihrem Betriebssystem.

Beachten Sie bei der Verwendung der NFS-Schnittstelle die folgenden Details.

- Die NFS-Schnittstelle stellt einen lokalen Bucket für die Datenspeicherung auf dem Gerät bereit. Bei Importaufträgen werden keine Daten aus dem lokalen Bucket in Amazon S3 importiert.
- Dateinamen sind Objektschlüssel in Ihrem lokalen S3-Bucket auf dem Snowball Edge. Der Schlüsselname ist eine Folge von Unicode-Zeichen, deren UTF-8-Kodierung maximal 1.024 Byte lang ist. Wir empfehlen, möglichst NFSv4 .1 zu verwenden und Dateinamen mit Unicode-UTF-8 zu codieren, um einen erfolgreichen Datenimport sicherzustellen. Dateinamen, die nicht mit UTF-8 codiert sind, werden je nach verwendeter NFS-Kodierung möglicherweise nicht nach S3 oder mit einem anderen Dateinamen nach S3 hochgeladen.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Snowball Edge unterstützt keine Dateipfade mit mehr als 1024 Zeichen. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateiimport.
- Weitere Informationen finden Sie unter [Objektschlüssel](#) im Amazon Simple Storage Service-Benutzerhandbuch.

- Bei NFS-basierten Übertragungen werden Ihren Objekten Metadaten im POSIX-Stil hinzugefügt, wenn sie von Snowball Edge in Amazon S3 importiert werden. Darüber hinaus werden Sie die Metadaten „x-amz-meta-user-agent aws-datasync“ sehen, wie wir sie derzeit AWS DataSync als Teil des internen Importmechanismus nach Amazon S3 für den Snowball Edge-Import mit NFS-Option verwenden.
- Sie können bis zu 40 Millionen Dateien mit einem einzigen Snowball Edge-Gerät übertragen. Wenn Sie mehr als 40 Millionen Dateien in einem einzigen Auftrag übertragen müssen, stapeln Sie die Dateien, um die Anzahl der Dateien pro Übertragung zu reduzieren. Einzelne Dateien können eine beliebige Größe mit einer maximalen Dateigröße von 5 TB für Snowball Edge-Geräte mit der erweiterten NFS-Schnittstelle oder der S3-Schnittstelle haben.

Sie können die NFS-Schnittstelle auch mit dem Snowball Edge-Client, einem Befehlszeilenschnittstellentool (CLI), konfigurieren und verwalten. Weitere Informationen finden Sie unter [Verwaltung der NFS-Schnittstelle](#).

Themen

- [Den NFS-Dienst auf einem Windows-Betriebssystem starten](#)
- [Automatische Konfiguration der NFS-Schnittstelle mit AWS OpsHub](#)
- [Manuelles Konfigurieren der NFS-Schnittstelle mit AWS OpsHub](#)
- [Verwaltung von NFS-Endpunkten auf dem Snowball Edge mit AWS OpsHub](#)
- [Mounten von NFS-Endpunkten auf Client-Computern](#)
- [Stoppen der NFS-Schnittstelle mit AWS OpsHub](#)

Den NFS-Dienst auf einem Windows-Betriebssystem starten

Wenn Ihr Client-Computer das Betriebssystem Windows 10 Enterprise oder Windows 7 Enterprise verwendet, starten Sie den NFS-Dienst auf dem Client-Computer, bevor Sie NFS in der Anwendung konfigurieren. AWS OpsHub

1. Öffnen Sie auf dem Client-Computer Start, wählen Sie Systemsteuerung und anschließend Programme aus.
2. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren.

Note

Um die Windows-Funktionen zu aktivieren, müssen Sie möglicherweise einen Administratorbenutzernamen und ein Administratorkennwort für Ihren Computer angeben.

3. Wählen Sie unter Services for NFS (Dienste für NFS) die Option Client for NFS (Client für NFS) aus und klicken Sie auf OK.

Automatische Konfiguration der NFS-Schnittstelle mit AWS OpsHub

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snowball Edge-Gerät ausgeführt. Sie müssen sie daher starten, um die Datenübertragung auf dem Gerät zu aktivieren. Mit wenigen Klicks kann Ihr Snowball Edge die NFS-Schnittstelle schnell und automatisch für Sie konfigurieren. Sie können die NFS-Schnittstelle auch selbst konfigurieren. Weitere Informationen finden Sie unter [Manuelles Konfigurieren der NFS-Schnittstelle mit AWS OpsHub](#).

1. Wählen Sie im Dashboard im Abschnitt Transfer data (Daten übertragen) die Option Enable & start (Aktivieren und starten). Der Vorgang kann ein oder zwei Minuten dauern.



2. Wenn der NFS-Dienst gestartet wird, wird die IP-Adresse der NFS-Schnittstelle auf dem Dashboard angezeigt, und im Bereich Daten übertragen wird angezeigt, dass der Dienst aktiv ist.
3. Wählen Sie Im Explorer öffnen (wenn Sie ein Windows- oder ein Linux-Betriebssystem verwenden), um die Dateifreigabe im Dateibrowser Ihres Betriebssystems zu öffnen und mit der Übertragung von Dateien auf Snowball Edge zu beginnen. Sie können Dateien von Ihrem Client-Computer kopieren und einfügen oder per Drag-and-Drop in die Dateifreigabe ziehen. Im Windows-Betriebssystem sieht Ihre Dateifreigabe wie folgt aus: `\\12.123.45.679` (Z:).

 Note

In Linux-Betriebssystemen erfordert das Mounten von NFS-Endpunkten Root-Rechte.

Manuelles Konfigurieren der NFS-Schnittstelle mit AWS OpsHub

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snowball Edge-Gerät ausgeführt. Sie müssen sie daher starten, um die Datenübertragung auf dem Gerät zu aktivieren. Sie können die NFS-Schnittstelle manuell konfigurieren, indem Sie die IP-Adresse einer virtuellen Netzwerkschnittstelle (VNI) angeben, die auf dem Snowball Edge-Gerät ausgeführt wird, und den Zugriff auf Ihre Dateifreigabe bei Bedarf einschränken. Bevor Sie die NFS-Schnittstelle manuell konfigurieren, richten Sie eine virtuelle Netzwerkschnittstelle (VNI) auf Ihrem Snowball Edge-Gerät ein. Weitere Informationen finden Sie unter [Netzwerkconfiguration für Compute-Instances](#).

Sie können auch festlegen, dass das Snowball Edge-Gerät die NFS-Schnittstelle automatisch konfiguriert. Weitere Informationen finden Sie unter [Automatische Konfiguration der NFS-Schnittstelle mit AWS OpsHub](#).

1. Wählen Sie unten im Abschnitt Transfer data (Daten übertragen) im Dashboard die Option Configure manually (Manuell konfigurieren) aus.

2. Wählen Sie **Enable & start** (Aktivieren und starten), um den Start NFS-Assistenten zu öffnen. Das Feld **Physikalische Netzwerkschnittstelle** ist gefüllt.

Start NFS

Physical network interface

RJ45: s.ni-8459d6c7273eed333

☒ Create IP address (VNI)

☐ Use existing IP address (VNI)

IP Address assignment

DHCP

☒ Restrict NFS to allowed hosts

☐ Allow all hosts

Allowed hosts

Provide a set of CIDR blocks allowed to connect to the NFS service.

192.0.2.0/24

0.0.0.0/0

Add allowed hosts

Allow instances on this device to access NFS

☒ Enable

Cancel

Start NFS

3. Wählen Sie **Create IP address (VNI)** (IP-Adresse erstellen) oder **Use existing IP address** (Vorhandene IP-Adresse verwenden).

4. Wenn Sie Create IP Address (VNI) wählen, wählen Sie DHCP oder Static IP im Listenfeld IP-Adresszuweisung aus.

 Important

Wenn Sie ein DHCP-Netzwerk verwenden, ist es möglich, dass die IP-Adresse der NFS-Schnittstelle vom DHCP-Server neu zugewiesen wird. Dies kann passieren, nachdem das Gerät getrennt und die IP-Adressen recycelt wurden. Wenn Sie einen zulässigen Hostbereich festlegen und sich die Adresse des Clients ändert, kann ein anderer Client diese Adresse abrufen. In diesem Fall hat der neue Client Zugriff auf den Share. Um dies zu verhindern, verwenden Sie DHCP-Reservierungen oder statische IP-Adressen.

Wenn Sie Bestehende IP-Adresse verwenden wählen, wählen Sie im Listenfeld Virtuelle Netzwerkschnittstelle eine virtuelle Netzwerkschnittstelle aus.

5. Sie können den Zugriff auf die NFS-Schnittstelle einschränken und einen Block zulässiger Netzwerkadressen bereitstellen oder allen Geräten im Netzwerk den Zugriff auf die NFS-Schnittstelle auf dem Snowball Edge ermöglichen.
 - Um den Zugriff auf die NFS-Schnittstelle auf dem Snowball Edge einzuschränken, wählen Sie „NFS auf erlaubte Hosts beschränken“. Geben Sie im Feld Zulässige Hosts eine Reihe von CIDR-Blöcken ein. Wenn Sie den Zugriff auf mehr als einen CIDR-Block zulassen möchten, geben Sie einen anderen Satz von Blöcken ein. Um eine Gruppe von Blöcken zu entfernen, wählen Sie X neben dem Feld, das die Blöcke enthält. Wählen Sie Zulässige Hosts hinzufügen.

 Note

Wenn Sie „NFS auf erlaubte Hosts beschränken“ wählen und keine zulässigen CIDR-Blöcke angeben, lehnt Snowball Edge alle Anfragen zum Mounten der NFS-Schnittstelle ab.

- Um jedem Gerät im Netzwerk den Zugriff auf die NFS-Schnittstelle zu ermöglichen, wählen Sie Alle Hosts zulassen aus.
6. Um EC2 -kompatiblen Instances, die auf dem Snowball Edge ausgeführt werden, den Zugriff auf den NFS-Adapter zu ermöglichen, wählen Sie Enable.

7. Wählen Sie Start NFS (NFS starten). Der Start des Vorgangs kann etwa eine oder zwei Minuten dauern.

 Important

Schalten Sie Snowball Edge nicht aus, während die NFS-Schnittstelle gestartet wird.

Im Bereich Network File System (NFS) -Ressourcen wird der Status der NFS-Schnittstelle als Aktiv angezeigt. Sie benötigen die angegebene IP-Adresse, um die Schnittstelle als lokalen Speicher auf Client-Computern bereitzustellen.

Verwaltung von NFS-Endpunkten auf dem Snowball Edge mit AWS OpsHub

Jeder S3-Bucket auf dem Snowball Edge wird als Endpunkt dargestellt und in Mount-Pfaden aufgeführt. Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie einen Endpunkt, um Dateien zu oder von diesem Endpunkt zu übertragen. Es kann jeweils nur ein Endpunkt gemountet werden. Um einen anderen Endpunkt zu mounten, müssen Sie zuerst den aktuellen Endpunkt aushängen.

Um einen Endpunkt zu mounten

1. Wählen Sie im Abschnitt Bereitstellungspfade einen der folgenden Schritte aus, um einen Endpunkt auszuwählen:
 - Geben Sie im Feld Endpunkte filtern einen Bucketnamen ganz oder teilweise ein, um die Liste der verfügbaren Endpunkte nach Ihrem Eintrag zu filtern, und wählen Sie dann den Endpunkt aus.
 - Wählen Sie in der Liste der Bereitstellungspfade den zu mountenden Endpunkt aus.
2. Wählen Sie NFS-Endpunkt mounten aus. Der Snowball Edge montiert den Endpunkt zur Verwendung.

Um die Bereitstellung eines Endpunkts aufzuheben

1. Wählen Sie im Abschnitt Bereitstellungspfade den Endpunkt aus, für den die Bereitstellung aufgehoben werden soll.

2. Wählen Sie Endpoint unmount aus. Snowball Edge hebt die Bereitstellung des Endpunkts auf und kann nicht mehr verwendet werden.

 Note

Bevor Sie die Bereitstellung eines Endpunkts aufheben, stellen Sie sicher, dass keine Daten von oder dorthin kopiert werden.

Mounten von NFS-Endpunkten auf Client-Computern

Nachdem die NFS-Schnittstelle gestartet und ein Endpunkt bereitgestellt wurde, mounten Sie den Endpunkt als lokalen Speicher auf den Client-Computern.

1. Wählen Sie unter Bereitstellungspfade das Kopiersymbol des Endpunkts aus, den Sie mounten möchten. Fügen Sie es in Ihr Betriebssystem ein, wenn Sie den Endpunkt mounten.
2. Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und MacOS-Betriebssysteme aufgeführt.

- Windows:

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/  
buckets/BucketName *
```

- Linux:

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsize=131072,wsize=131072,nolocks,hard,retrans=2 nfs-  
interface-ip-address:/buckets/$bucketname mount_point
```

Stoppen der NFS-Schnittstelle mit AWS OpsHub

Beenden Sie die NFS-Schnittstelle auf dem Snowball Edge-Gerät, wenn Sie mit der Übertragung von Dateien zum oder vom Snowball Edge-Gerät fertig sind.

1. Wählen Sie im Dashboard Services und anschließend File Storage (Dateispeicher) aus.
2. Wählen Sie auf der Seite File storage (Dateispeicher) die Option Disable data transfer (Datentransfer deaktivieren). Normalerweise dauert es bis zu 2 Minuten, bis die NFS-Endpunkte aus dem Dashboard verschwinden.

Starten Sie das Gerät neu mit AWS OpsHub

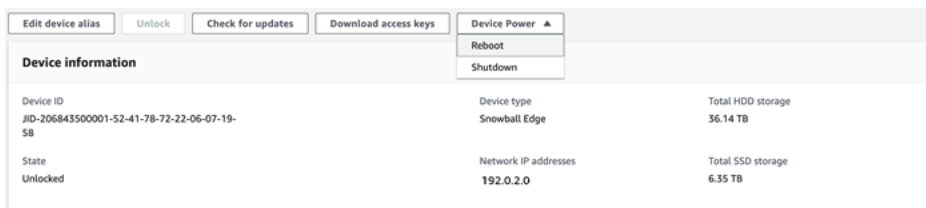
Gehen Sie wie folgt vor, um Ihr Snow-Gerät neu AWS OpsHub zu starten.

Important

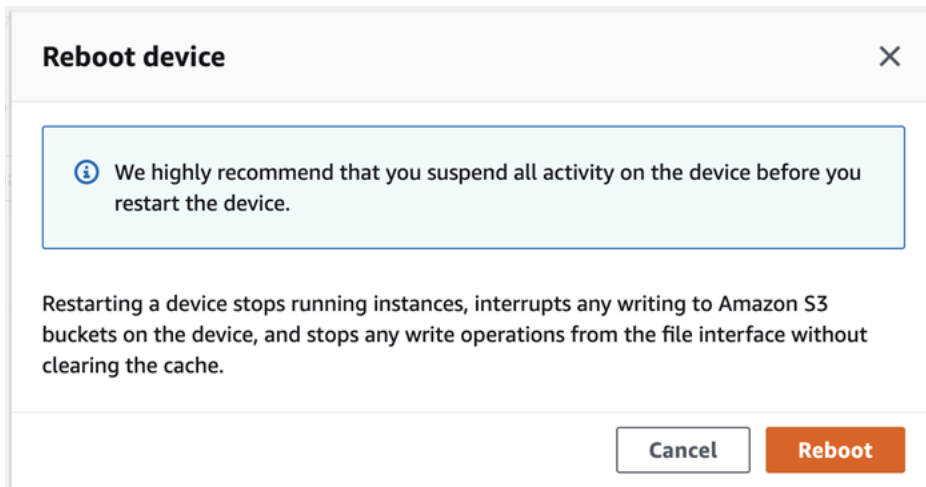
Es wird nachdrücklich empfohlen, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät neu starten. Durch den Neustart eines Geräts werden die laufenden Instances gestoppt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen.

So starten Sie ein Gerät neu

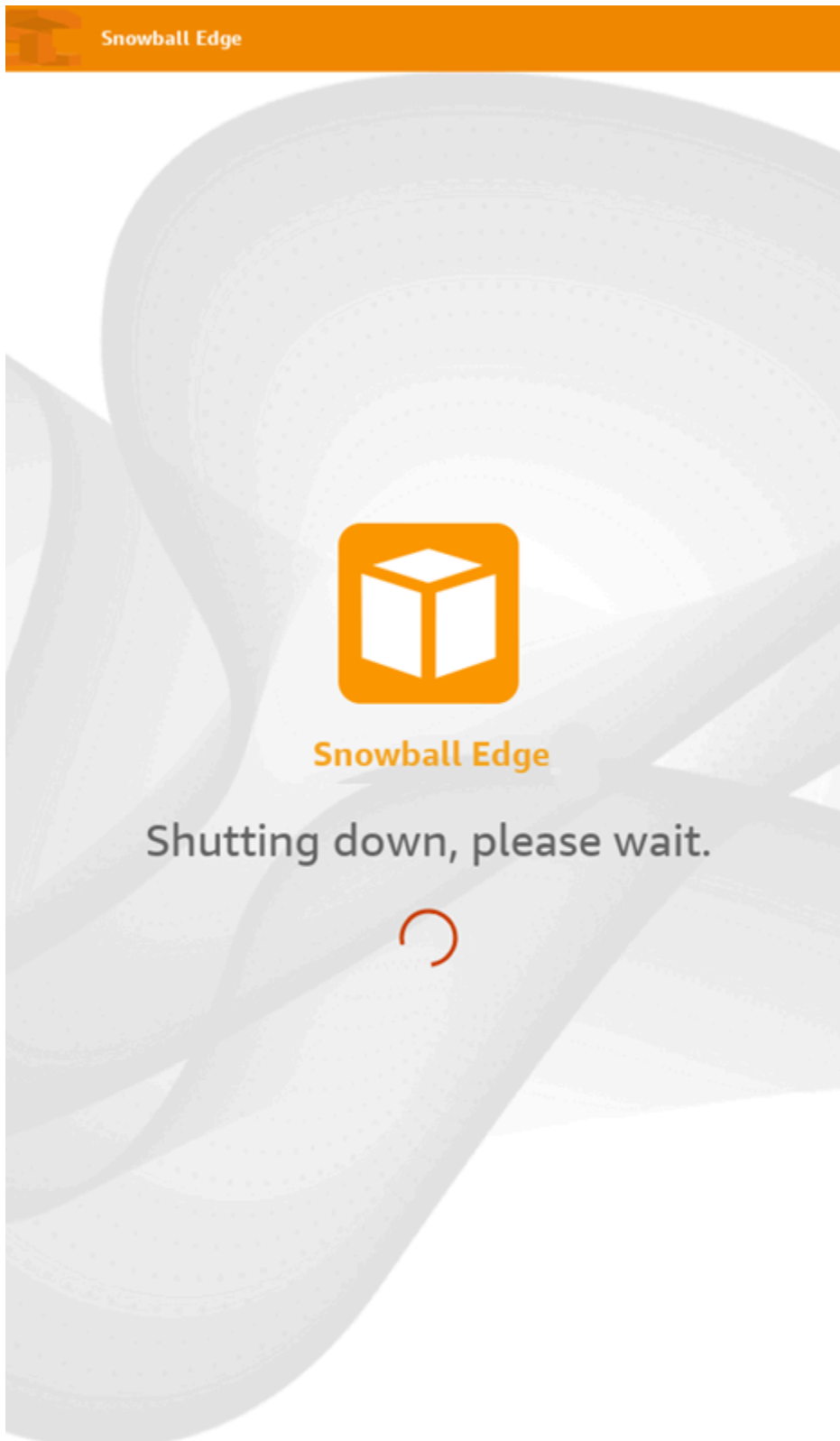
1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie anschließend das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie das Menü „Gerätebetrieb“ und anschließend „Neustart“. Ein Dialogfeld wird angezeigt.



3. Wählen Sie im Dialogfeld „Neustart“ aus. Ihr Gerät beginnt mit dem Neustart.



Während das Gerät heruntergefahren wird, wird auf dem LCD-Bildschirm eine Meldung angezeigt, die darauf hinweist, dass das Gerät heruntergefahren wird.



Profile verwalten mit AWS OpsHub

Sie können ein Profil für die persistente Speicherung Ihrer Anmeldeinformationen in Ihrem lokalen Dateisystem erstellen. Mit dieser Option haben Sie die Möglichkeit AWS OpsHub, jedes Mal, wenn Sie das Gerät entsperren, ein neues Profil mithilfe der Geräte-IP-Adresse, des Entsperrcodes und der Manifestdatei zu erstellen.

Sie können den Snowball Edge-Client auch verwenden, um jederzeit ein Profil zu erstellen. Siehe [Konfiguration eines Profils für den Snowball Edge-Client](#).

So erstellen Sie ein Profil

1. Entsperren Sie Ihr Gerät lokal und melden Sie sich gemäß den Anweisungen unter an. [Entsperren eines Snowball Edge-Geräts mit AWS OpsHub](#)
2. Benennen Sie das Profil und wählen Sie Save profile name (Profilname speichern) aus.

Das Gerät herunterfahren mit AWS OpsHub

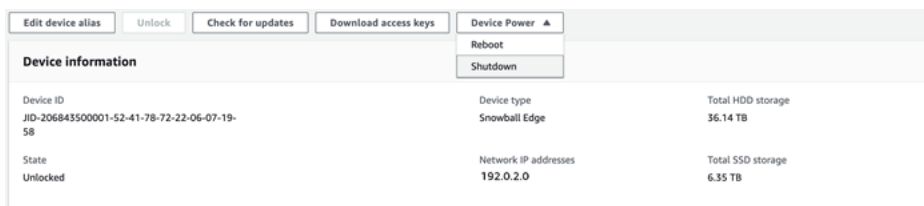
Gehen Sie wie folgt vor, AWS OpsHub um Ihr Snow-Gerät herunterzufahren.

Important

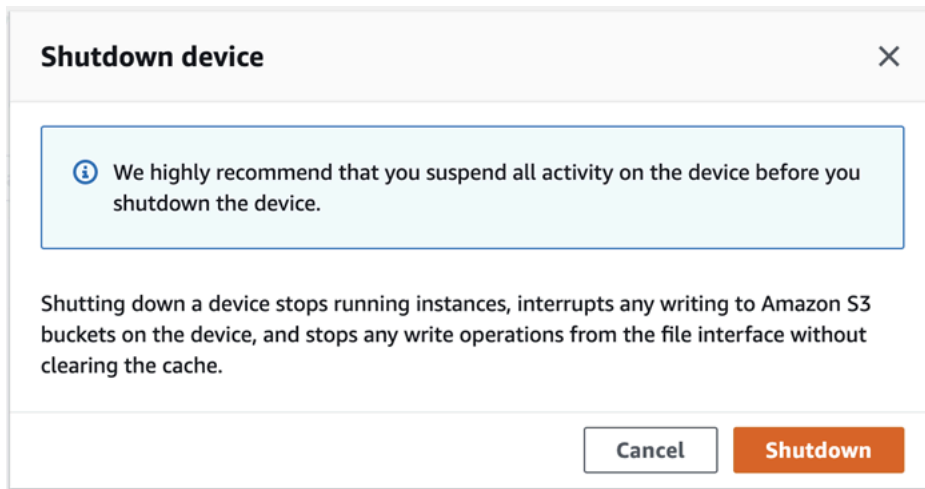
Wir empfehlen dringend, alle Aktivitäten auf dem Gerät zu unterbrechen, bevor Sie das Gerät herunterfahren. Beim Herunterfahren eines Geräts werden Instances nicht mehr ausgeführt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät werden unterbrochen.

Um ein Gerät herunterzufahren

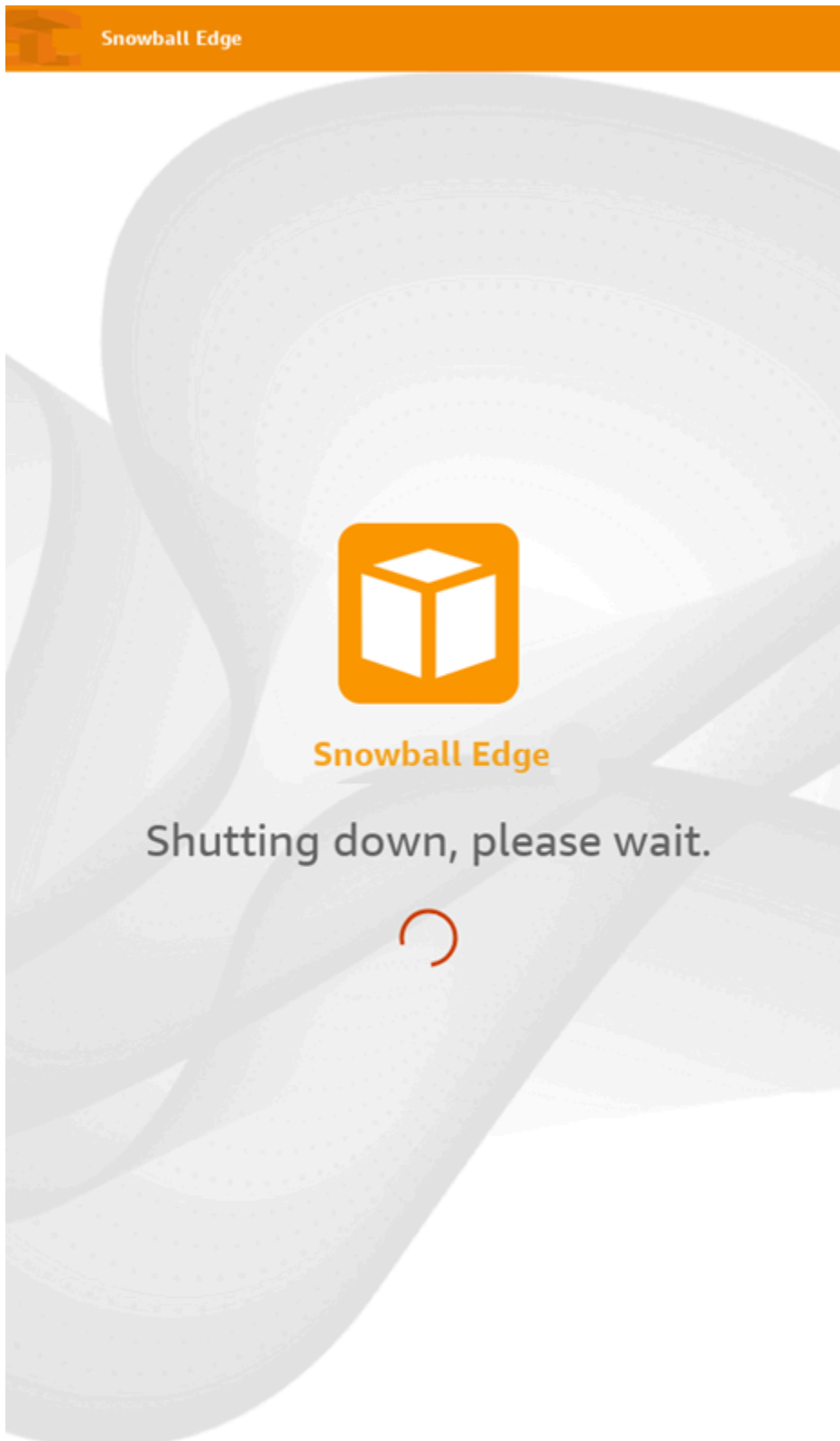
1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie anschließend das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wähle das Menü „Gerätebetrieb“ und dann „Herunterfahren“. Ein Dialogfeld wird angezeigt.



3. Wählen Sie im Dialogfeld „Herunterfahren“. Ihr Gerät wird heruntergefahren.



Während das Gerät heruntergefahren wird, wird auf dem LCD-Bildschirm eine Meldung angezeigt, die darauf hinweist, dass das Gerät heruntergefahren wird.

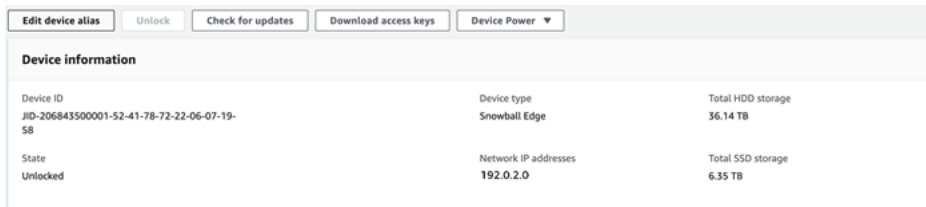


Den Gerätealias bearbeiten mit AWS OpsHub

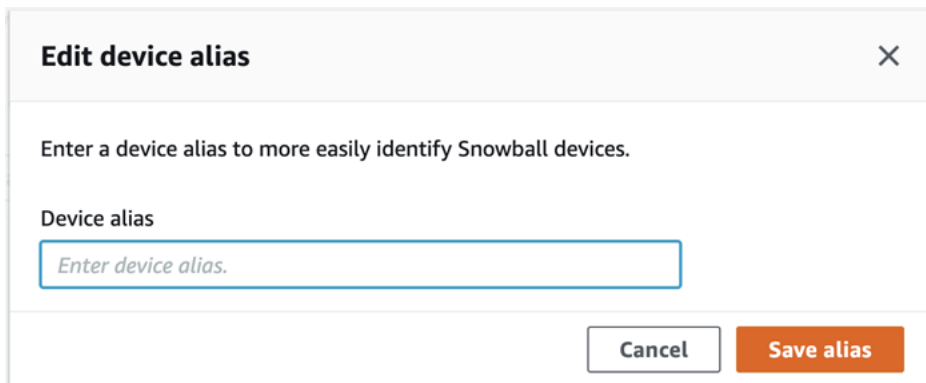
Gehen Sie wie folgt vor, um Ihren Gerätealias mit zu bearbeiten AWS OpsHub.

So bearbeiten Sie den Alias Ihres Geräts

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie die Registerkarte Edit device alias (Gerätealias bearbeiten) aus.



3. Geben Sie in Device alias (Gerätealias) einen neuen Namen ein. Wählen Sie anschließend Save alias (Alias speichern) aus.



Edit device alias [X]

Enter a device alias to more easily identify Snowball devices.

Device alias

[Cancel] [Save alias]

Verwaltung von Public-Key-Zertifikaten mit OpsHub

Sie können über das HTTPS-Protokoll sicher mit AWS Diensten interagieren, die auf einem Snowball Edge-Gerät oder einem Cluster von Snowball Edge-Geräten ausgeführt werden, indem Sie ein Public-Key-Zertifikat bereitstellen. Sie können das HTTPS-Protokoll verwenden, um mit AWS Diensten wie IAM, Amazon EC2, S3-Adapter und Amazon S3 S3-kompatiblen Speicher auf Snowball Edge, Amazon EC2 Systems Manager und Snowball AWS STS Edge-Geräten zu interagieren. Bei einem Gerätecluster ist ein einzelnes Zertifikat erforderlich, das von jedem Gerät im Cluster generiert werden kann. Sobald ein Snowball Edge-Gerät das Zertifikat generiert hat und Sie das Gerät entsperren, können Sie Snowball Edge-Clientbefehle verwenden, um das Zertifikat aufzulisten, abzurufen und zu löschen.

Ein Snowball Edge-Gerät generiert ein Zertifikat, wenn die folgenden Ereignisse eintreten:

- Das Snowball Edge-Gerät oder -Cluster wird zum ersten Mal entsperrt.
- Das Snowball Edge-Gerät oder -Cluster wird nach dem Löschen des Zertifikats entsperrt (mit dem `delete-certificate` Befehl oder Zertifikat erneuern in AWS OpsHub).
- Das Snowball Edge-Gerät oder -Cluster wird nach Ablauf des Zertifikats neu gestartet und entsperrt.

Immer wenn ein neues Zertifikat generiert wird, ist das alte Zertifikat nicht mehr gültig. Ein Zertifikat ist ab dem Tag, an dem es generiert wurde, für einen Zeitraum von einem Jahr gültig.

Sie können den Snowball Edge-Client auch verwenden, um Public-Key-Zertifikate zu verwalten. Weitere Informationen finden Sie unter [Verwaltung von Zertifikaten mit öffentlichen Schlüsseln](#).

Themen

- [Laden Sie das Public-Key-Zertifikat herunter mit OpsHub](#)
- [Erneuerung des Public-Key-Zertifikats mit OpsHub](#)

Laden Sie das Public-Key-Zertifikat herunter mit OpsHub

Sie können das aktive Public-Key-Zertifikat auf Ihren Computer herunterladen.

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie auf der Seite mit den Gerätedetails das Menü Zertifikat verwalten aus. Wählen Sie im Menü die Option Zertifikat herunterladen.
3. Es erscheint ein Fenster, in dem Sie der herunterzuladenden Zertifikatsdatei einen Namen geben und den Speicherort auf Ihrem Computer auswählen können, an den sie heruntergeladen werden soll. Wählen Sie Speichern.

Erneuerung des Public-Key-Zertifikats mit OpsHub

Bevor Sie das Public-Key-Zertifikat erneuern, beenden Sie alle Datenübertragungen zum oder vom Snowball Edge-Gerät und beenden Sie alle laufenden EC2 -kompatiblen Datenübertragungen.

Weitere Informationen finden Sie unter [Stoppen einer Amazon EC2 -kompatiblen Instance](#) in diesem Handbuch.

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie auf der Seite mit den Gerätedetails das Menü Zertifikat verwalten aus. Wählen Sie im Menü die Option Zertifikat erneuern aus.
3. Geben Sie im Fenster Zertifikat erneuern das **Renew** Feld ein und wählen Sie Erneuern. Das Snowball Edge-Gerät löscht das vorhandene Public-Key-Zertifikat und startet das Gerät oder den Cluster neu.

Renew certificate



The following certificate will be deleted:

arn:aws:snowball-device:::certificate/example



Stop all activity on the Snow device or cluster before proceeding.

Clicking **Renew** will automatically reboot **all devices attached to this certificate** and terminate any ongoing data transfers and other running processes. A new certificate will be generated when you unlock the device or cluster after it reboots.

To confirm, enter **Renew** in the field and then choose **Renew**

Cancel

Renew

Updates für Snowball Edge abrufen

Sie können nach Updates für Ihr Gerät suchen und diese installieren. Version.

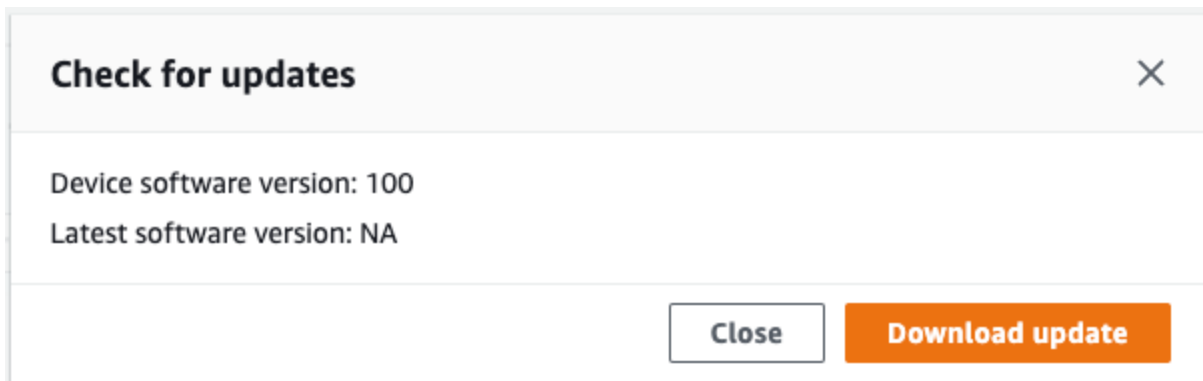
Das Gerät wird aktualisiert

Gehen Sie wie folgt vor, AWS OpsHub um Ihr Snow-Gerät zu aktualisieren.

Um das Gerät zu aktualisieren

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie die Registerkarte Check for updates (Nach Updates suchen) aus.

Auf der Seite Check for updates (Nach Updates suchen) werden die aktuelle Softwareversion auf Ihrem Gerät und die neueste Softwareversion angezeigt, wenn vorhanden.

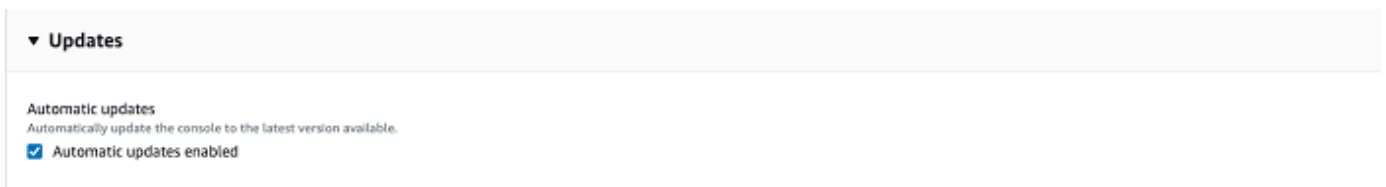


3. Wenn es ein Update gibt, wählen Sie Update herunterladen. Wählen Sie andernfalls Close aus.

Aktualisierung der AWS OpsHub Anwendung

Um zu überprüfen, ob automatische Updates aktiviert sind für AWS OpsHub

1. Wählen Sie im AWS OpsHub Dashboard Einstellungen aus.
2. Öffnen Sie den Tab Updates.
3. Vergewissern Sie sich, dass Automatische Updates aktiviert ausgewählt ist. Automatisches Update ist standardmäßig aktiviert.



Wenn die Option Automatische Updates aktiviert nicht ausgewählt ist, erhalten Sie nicht die neueste Version der AWS OpsHub Anwendung.

Automatisieren Sie Ihre Verwaltungsaufgaben mit AWS OpsHub

Sie können AWS OpsHub damit betriebliche Aufgaben automatisieren, die Sie häufig auf Ihrem Snowball Edge ausführen. Sie können eine Aufgabe für wiederkehrende Aktionen erstellen, die Sie möglicherweise an Ressourcen ausführen möchten, z. B. das Neustarten virtueller Server, das Stoppen von EC2 Amazon-kompatiblen Instances usw. Sie stellen ein Automatisierungsdokument bereit, das betriebliche Aufgaben sicher ausführt und den Vorgang auf mehreren AWS Ressourcen ausführt. Sie können auch allgemeine IT-Workflows planen.

Note

Die Automatisierung von Aufgaben wird in Clustern nicht unterstützt.

Um Aufgaben verwenden zu können, muss zuerst der Amazon EC2 Systems Manager Manager-Service gestartet werden. Weitere Informationen finden Sie unter [Snowball Edge-Geräteverwaltung auf einem Snowball Edge aktivieren](#).

Themen

- [Eine Aufgabe erstellen und starten mit AWS OpsHub](#)
- [Details einer Aufgabe anzeigen in AWS OpsHub](#)
- [Löschen einer Aufgabe in AWS OpsHub](#)

Eine Aufgabe erstellen und starten mit AWS OpsHub

Wenn Sie eine Aufgabe erstellen, geben Sie die Arten von Ressourcen an, für die die Aufgabe ausgeführt werden soll. Anschließend stellen Sie ein Aufgabendokument bereit, das die Anweisungen enthält, nach denen die Aufgabe ausgeführt wird. Das Aufgabendokument hat entweder YAML- oder das JSON-Format. Anschließend geben Sie die erforderlichen Parameter für die Aufgabe an und starten die Aufgabe.

So erstellen Sie eine Aufgabe

1. Wählen Sie im Abschnitt Launch tasks (Aufgaben starten) des Dashboards die Option Get started (Erste Schritte) aus, um die Seite Tasks (Aufgaben) zu öffnen. Wenn Sie Aufgaben erstellt haben, werden diese unter Tasks (Aufgaben) angezeigt.
2. Wählen Sie Create task (Aufgabe erstellen) aus und geben Sie Details für die Aufgabe an.

3. Geben Sie in Name (Rollenname) einen eindeutigen Namen für die Aufgabe ein.

 Tip

Der Name muss 3 bis 128 Zeichen enthalten. Gültige Zeichen sind a-z, A-Z, 0-9, ., _ und -.

4. Optional können Sie aus der Liste Target type-optional (Zieltyp – optional) einen Zieltyp auswählen. Dies ist der Typ der Ressource, auf der die Aufgabe ausgeführt werden soll.

Sie können **/AWS::EC2::Instance** beispielsweise angeben, dass die Aufgaben auf einer EC2 Amazon-kompatiblen Instance oder auf allen Ressourcentypen ausgeführt werden / sollen.

5. Wählen Sie im Bereich Inhalt YAML oder JSON und geben Sie das Skript an, das die Aufgabe ausführt. Es gibt zwei Optionen, das YAML- oder das JSON-Format. Beispiele finden Sie unter [Beispiele für Aufgaben in AWS OpsHub](#).
6. Wählen Sie Erstellen aus. Die von Ihnen erstellte Aufgabe wird anschließend auf der Seite Tasks (Aufgaben) angezeigt.

So starten Sie eine Aufgabe

1. Wählen Sie im Abschnitt Launch tasks (Aufgaben starten) des Dashboards die Option Get started (Erste Schritte) aus, um die Seite Tasks (Aufgaben) zu öffnen. Ihre Aufgaben werden unter Tasks (Aufgaben) angezeigt.
2. Wählen Sie Ihre Aufgabe aus, um die Seite Start task (Aufgabe starten) zu öffnen.
3. Wählen Sie Simple execution (Einfache Ausführung) zur Ausführung auf Zielen aus.

Wählen Sie Rate control (Ratensteuerung) für die sichere Ausführung auf mehreren Zielen aus. Definieren Sie Schwellenwerte für Gleichzeitigkeit und Fehler. Für diese Option geben Sie die zusätzlichen Ziel- und Fehler-Schwellenwertinformationen im Abschnitt Rate control (Ratensteuerung) an.

4. Geben Sie die erforderlichen Eingabeparameter an. Wählen Sie anschließend Start task (Aufgabe starten) aus.

Der Status der Aufgabe ist Pending (Ausstehend). Dieser wird nach erfolgreicher Ausführung der Aufgabe in Success (Erfolg) geändert.

Beispiele für Aufgaben in AWS OpsHub

Im folgenden Beispiel wird eine Amazon EC2 -kompatible Instance neu gestartet. Hierfür sind zwei Eingabeparameter erforderlich: endpoint und instance ID.

YAML-Beispiel

```
description: Restart EC2 instance
schemaVersion: '0.3'
parameters:
  Endpoint:
    type: String
    description: (Required) EC2 Service Endpoint URL
  Id:
    type: String
    description: (Required) Instance Id
mainSteps:
- name: restartInstance
  action: aws:executeScript
  description: Restart EC2 instance step
  inputs:
    Runtime: python3.7
    Handler: restart_instance
    InputPayload:
      Endpoint: "{{ Endpoint }}"
      Id: "{{ Id }}"
    TimeoutSeconds: 30
  Script: |-
    import boto3
    import time
    def restart_instance(payload, context):
        ec2_endpoint = payload['Endpoint']
        instance_id = payload['Id']
        ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)
        instance = ec2.Instance(instance_id)
        if instance.state['Name'] != 'stopped':
            instance.stop()
            instance.wait_until_stopped()
        instance.start()
        instance.wait_until_running()
        return {'InstanceState': instance.state}
```

JSON-Beispiel

```
{
  "description" : "Restart EC2 instance",
  "schemaVersion" : "0.3",
  "parameters" : {
    "Endpoint" : {
      "type" : "String",
      "description" : "(Required) EC2 Service Endpoint URL"
    },
    "Id" : {
      "type" : "String",
      "description" : "(Required) Instance Id"
    }
  },
  "mainSteps" : [ {
    "name" : "restartInstance",
    "action" : "aws:executeScript",
    "description" : "Restart EC2 instance step",
    "inputs" : {
      "Runtime" : "python3.7",
      "Handler" : "restart_instance",
      "InputPayload" : {
        "Endpoint" : "{{ Endpoint }}",
        "Id" : "{{ Id }}"
      },
      "TimeoutSeconds" : 30,
      "Script" : "import boto3\nimport time\ndef restart_instance(payload, context):\n\n    ec2_endpoint = payload['Endpoint']\n    instance_id = payload['Id']\n    ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)\n    instance = ec2.Instance(instance_id)\n    if instance.state['Name'] != 'stopped':\n        instance.stop()\n        instance.wait_until_stopped()\n    instance.start()\n    instance.wait_until_running()\n    return {'InstanceState': instance.state}"
    }
  ]
}
```

Details einer Aufgabe anzeigen in AWS OpsHub

Sie können die Details einer Verwaltungsaufgabe anzeigen, z. B. die Beschreibung und die Parameter, die zum Ausführen der Aufgabe erforderlich sind.

So zeigen Sie Details für eine Aufgabe an

1. Wählen Sie im Abschnitt Launch tasks (Aufgaben starten) des Dashboards die Option Get started (Erste Schritte) aus, um die Seite Tasks (Aufgaben) zu öffnen.
2. Suchen Sie auf der Seite Tasks (Aufgaben) die Aufgabe, deren Details Sie anzeigen möchten, und wählen Sie diese Aufgabe aus.
3. Wählen Sie View details (Details anzeigen) aus. Wählen Sie anschließend eine der Registerkarten aus, um die Details anzuzeigen. Auf der Registerkarte Parameters (Parameter) werden Ihnen beispielsweise die Eingabeparameter im Skript angezeigt.

Löschen einer Aufgabe in AWS OpsHub

Führen Sie die folgenden Schritte aus, um eine Verwaltungsaufgabe zu löschen.

So löschen Sie eine Aufgabe

1. Wählen Sie im Abschnitt Launch tasks (Aufgaben starten) des Dashboards die Option Get started (Erste Schritte) aus, um die Seite Tasks (Aufgaben) zu öffnen.
2. Suchen Sie die Aufgabe, die Sie löschen möchten. Wählen Sie die Aufgabe und anschließend Delete (Löschen) aus.

Einstellung der NTP-Zeitserver für das Gerät mit AWS OpsHub

Gehen Sie wie folgt vor, um anzuzeigen und zu aktualisieren, mit welchen Zeitservern Ihr Gerät die Uhrzeit synchronisieren muss.

Um Zeitquellen zu überprüfen

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. In der Tabelle Zeitquellen wird eine Liste der Zeitquellen angezeigt, mit denen Ihr Gerät die Zeit synchronisiert.

Die Tabelle mit den Zeitquellen besteht aus vier Spalten:

- **Adresse:** Der DNS-Name/die IP-Adresse der Zeitquelle
- **Status:** Der aktuelle Verbindungsstatus zwischen dem Gerät und dieser Zeitquelle. Es gibt 5 mögliche Zustände:
 - **AKTUELL:** Die Zeitquelle wird derzeit zum Synchronisieren der Uhrzeit verwendet
 - **KOMBINIERT:** Die Zeitquelle wird mit der aktuellen Quelle kombiniert
 - **AUSGESCHLOSSEN:** Die Zeitquelle ist durch den Kombinationsalgorithmus ausgeschlossen
 - **VERLOREN:** Die Verbindung mit der Zeitquelle wurde unterbrochen
 - **UNVERFÜGBARKEIT:** Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder ein falscher Ticker oder eine zu große Variabilität erkannt hat
- **Typ:** Bei den NTP-Quellen (Network Time Protocol) kann es sich um einen Server oder einen Peer handeln. Ein Server kann vom Benutzer mithilfe des `update-time-server` Befehls eingerichtet werden, wohingegen ein Peer nur mit anderen Snowball Edge-Geräten im Cluster eingerichtet werden kann und automatisch eingerichtet wird, wenn der Cluster zugeordnet wird.
- **Schicht:** Die Schicht der Quelle. Stratum 1 weist auf eine Quelle mit einer lokal angeschlossenen Referenzuhr hin. Eine Quelle, die mit einer Stratum 1-Quelle synchronisiert ist, ist auf Stratum 2 eingestellt. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert ist, wird auf Stratum 3 gesetzt usw.

Um die Zeitserver zu aktualisieren

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. In der Tabelle Zeitquellen wird eine Liste der Zeitquellen angezeigt, mit denen Ihr Gerät die Zeit synchronisiert.
3. Wählen Sie in der Tabelle Zeitquellen die Option Zeitserver aktualisieren aus.
4. Geben Sie den DNS-Namen oder die IP-Adresse der Zeitserver ein, mit denen Ihr Gerät die Uhrzeit synchronisieren soll, und wählen Sie Aktualisieren aus.

Update time servers

Update time servers on JID-206843500001-52-41-78-72-22-06-07-19-58

Overriding Existing Settings
Updating the time servers will override existing time server settings.

NTP server IP address or DNS name

Enter NTP server IP address or DNS name

You can add up to 4 more time servers.

Unterstützte NTP-Gerätetypen und Softwareversionen

NTP ist auf keinem Speicher- und Computergerätetyp der Version 2 verfügbar. Speicher- und Rechengenrätetypen der Version 3 von Snowball Edge mit Softwareversion 77 oder höher unterstützen jedoch NTP. Verwenden Sie den Snowball Edge-CLI-Befehl, um zu überprüfen, ob NTP aktiviert ist. `describe-time-sources`

Konfiguration und Verwendung des Snowball Edge-Clients

Der Snowball Edge-Client ist ein Befehlszeilenschnittstellentool (CLI) AWS, mit dem Sie mit einem Snowball Edge oder einem Snowball Edge-Cluster arbeiten können. Sie können den Client verwenden, um einen Snowball Edge oder einen Gerätecluster zu entsperren, Snowball Edge einzurichten, Dienste auf Geräten zu starten und zu beenden und Daten zu oder von Geräten zu übertragen. Der Snowball Edge-Client ist mit Computern kompatibel, die unter Linux-, MacOS- und Windows-Betriebssystemen ausgeführt werden.

Themen

- [Den Snowball Edge-Client herunterladen und installieren](#)
- [Konfiguration eines Profils für den Snowball Edge-Client](#)
- [Snowball Edge-Clientversion finden](#)
- [Anmeldeinformationen für einen Snowball Edge abrufen](#)
- [Einen Dienst auf einem Snowball Edge starten](#)
- [Beenden eines Dienstes auf einem Snowball Edge](#)
- [Protokolle von Snowball Edge anzeigen und herunterladen](#)
- [Status eines Snowball Edge anzeigen](#)
- [Status von Diensten anzeigen, die auf Snowball Edge ausgeführt werden](#)
- [Status der Funktionen von Snowball Edge anzeigen](#)
- [Zeitserver für Snowball Edge einrichten](#)
- [Einen QR-Code zur Validierung von Snowball Edge NFC-Tags erhalten](#)
- [Die MTU-Größe wird aktualisiert](#)

Den Snowball Edge-Client herunterladen und installieren

Sie können den Snowball Edge-Client unter [AWS Snowball Edge Ressourcen](#) herunterladen. Auf dieser Seite finden Sie das Installationspaket für Ihr Betriebssystem.

Installieren und konfigurieren Sie den Client gemäß den nachstehenden Anweisungen.

Linux

Note

Der Snowball Edge-Client wird nur auf 64-Bit-Linux-Distributionen unterstützt.

1. Extrahieren Sie die `snowball-client-linux.tar.gz`-Datei. Er erstellt die `/snowball-client-linux-build_number/bin` Ordnerstruktur und extrahiert die Dateien dort.
2. Führen Sie die folgenden Befehle aus, um die Ordner zu konfigurieren.

```
chmod u+x snowball-client-linux-build_number/bin/snowballEdge
```

```
chmod u+x snowball-client-linux-build_number/jre/bin/java
```

3. Fügen Sie `/snowball-client-linux-build_number/bin` die Umgebungsvariable `$PATH` Ihres Betriebssystems hinzu, um Snowball Edge-Client-Befehle von einem beliebigen Verzeichnis aus auszuführen. Weitere Informationen finden Sie in der Dokumentation zum Betriebssystem Ihres Geräts oder Ihrer Shell.

macOS

1. Extrahieren Sie die `snowball-client-mac.tar.gz`-Datei. Es erstellt die `/snowball-client-linux-build_number/bin` Ordnerstruktur und extrahiert die Dateien dort.
2. Führen Sie die folgenden Befehle aus, um die Ordner zu konfigurieren.

```
chmod u+x snowball-client-mac-build_number/bin/snowballEdge
```

```
chmod u+x snowball-client-mac-build_number/jre/bin/java
```

3. Fügen Sie `/snowball-client-mac-build_number/bin` die Umgebungsvariable `$PATH` Ihres Betriebssystems hinzu, um Snowball Edge-Client-Befehle von einem beliebigen Verzeichnis aus auszuführen. Weitere Informationen finden Sie in der Dokumentation zum Betriebssystem Ihres Geräts oder Ihrer Shell.

Windows

Der Client ist als Microsoft Software Installer (MSI) -Datei gepackt. Öffnen Sie die Datei und folgen Sie den Anweisungen des Installationsassistenten. Wenn der Client installiert wurde, können Sie ihn ohne zusätzliche Vorbereitung von jedem Verzeichnis aus ausführen.

Konfiguration eines Profils für den Snowball Edge-Client

Jedes Mal, wenn Sie einen Befehl für den Snowball Edge-Client ausführen, geben Sie Ihre Manifestdatei, den Entsperrcode und die IP-Adresse von Snowball Edge an. Anstatt diese bei jeder Ausführung eines Befehls anzugeben, können Sie den `configure` Befehl verwenden, um den Pfad zur Manifestdatei, den 29-stelligen Entsperrcode und den Endpunkt (die IP-Adresse von Snowball Edge) als Profil zu speichern. Nach der Konfiguration können Sie Snowball Edge Client-Befehle verwenden, ohne diese Werte für jeden Befehl manuell eingeben zu müssen, indem Sie den Profilnamen in den Befehl aufnehmen. Nachdem Sie den Snowball Edge-Client konfiguriert haben, werden die Informationen in einem Klartext-JSON-Format unter gespeichert. `home directory/.aws/snowball/config/snowball-edge.config` Stellen Sie sicher, dass Ihre Umgebung so konfiguriert ist, dass Sie diese Datei erstellen können.

Important

Jeder, der auf die Konfigurationsdatei zugreifen kann, kann auf die Daten auf Ihren Snowball Edge-Geräten oder -Clustern zugreifen. Zu Ihren administrativen Verantwortlichkeiten zählt auch die Verwaltung der lokalen Zugriffssteuerung für diese Datei.

Sie können es auch verwenden AWS OpsHub , um ein Profil zu erstellen. In AWS OpsHub erstellte Profile können mit dem Snowball Edge-Client verwendet werden, und die in erstellten Profile können mit dem Snowball Edge-Client verwendet werden. Weitere Informationen finden Sie unter Profile [verwalten](#).

So erstellen Sie ein Profil

1. Geben Sie den Befehl in der Befehlszeilenschnittstelle Ihres Betriebssystems ein. Der Wert des `profile-name` Parameters ist der Name des Profils. Sie werden es in future bereitstellen, wenn Sie Snowball Edge Client-Befehle ausführen.

```
snowballEdge configure --profile profile-name
```

2. Der Snowball Edge-Client fordert Sie zur Eingabe jedes Parameters auf. Wenn Sie dazu aufgefordert werden, geben Sie die Informationen für Ihre Umgebung und Snowball Edge ein.

Note

Der Wert des `endpoint` Parameters ist die IP-Adresse von Snowball Edge mit dem Präfix. `https://` Sie können die IP-Adresse für das Snowball Edge-Gerät auf dem LCD-Bildschirm an der Vorderseite des Geräts finden.

Example Ausgabe des Befehls **configure**

```
Configuration will stored at home directory\.aws\snowball\config\snowball-  
edge.config  
Snowball Edge Manifest Path: /Path/to/manifest/file  
Unlock Code: 29 character unlock code  
Default Endpoint: https://192.0.2.0
```

Der Snowball Edge-Client überprüft, ob der Entsperrcode für die Manifestdatei korrekt ist. Wenn sie nicht übereinstimmen, wird der Befehl beendet und das Profil wird nicht erstellt. Überprüfen Sie den Entsperrcode und die Manifestdatei und führen Sie den Befehl erneut aus.

Um das Profil zu verwenden, fügen Sie es `--profile profile-name` nach der Befehlssyntax ein.

Wenn Sie mehrere eigenständige Snowball Edge verwenden, können Sie für jeden ein Profil erstellen. Um ein anderes Profil zu erstellen, führen Sie den `configure` Befehl erneut aus, geben Sie einen anderen Wert für den `--profile` Parameter und die Informationen für ein anderes Gerät ein.

Example **snowball-edge.config**-Beispieldatei

Dieses Beispiel zeigt eine Profildatei mit drei Profilen—

SnowDevice1profile, SnowDevice2profile, und SnowDevice3profile.

```
{
  "version": 1,
  "profiles": [
    {
      "SnowDevice1profile": {
        "name": "SnowDevice1profile",
        "jobId": "JID12345678-136f-45b4-b5c2-847db8adc749",
        "unlockCode": "db223-12345-dbe46-44557-c7cc2",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-136f-45b4-b5c2-847db8adc749_manifest-1670622989203.bin",
        "defaultEndpoint": "https://10.16.0.1",
        "isCluster": false,
        "deviceIps": []
      }
    },
    {
      "SnowDevice2profile": {
        "name": "SnowDevice2profile",
        "jobId": "JID12345678-fdb2-436a-a4ff-7c510dec1bae",
        "unlockCode": "b893b-54321-0f65c-6c5e1-7f748",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-fdb2-436a-a4ff-7c510dec1bae_manifest-1670623746908.bin",
        "defaultEndpoint": "https://10.16.0.2",
        "isCluster": false,
        "deviceIps": []
      }
    },
    {
      "SnowDevice3profile": {
        "name": "SnowDevice3profile",
        "jobId": "JID12345678-c384-4a5e-becd-ab5f38888463",
        "unlockCode": "64c89-13524-4d054-13d93-c1b80",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-c384-4a5e-becd-ab5f38888463_manifest-1670623999136.bin",
        "defaultEndpoint": "https://10.16.0.3",
        "isCluster": false,
        "deviceIps": []
      }
    }
  ]
}
```

Um Profile zu bearbeiten oder zu löschen, bearbeiten Sie die Profildatei in einem Texteditor.

So bearbeiten Sie ein Profil

1. Öffnen Sie in einem Texteditor `snowball-edge.config` von *home directory* \.aws \snowball\config.

 Note

Stellen Sie sicher, dass Ihre Umgebung so konfiguriert ist, dass Sie auf diese Datei zugreifen und sie lesen und schreiben können.

2. Bearbeiten Sie die Datei nach Bedarf. Um beispielsweise die IP-Adresse des Snowball Edge zu ändern, der dem Profil zugeordnet ist, ändern Sie den `defaultEndpoint` Eintrag.
3. Speichern und schließen Sie die Datei.

So löschen Sie ein Profil

1. Öffnen Sie mit einem Texteditor `snowball-edge.config` von *home directory* \.aws \snowball\config.

 Note

Stellen Sie sicher, dass Ihre Umgebung so konfiguriert ist, dass Sie auf diese Datei zugreifen und sie lesen und schreiben können.

2. Löschen Sie die Zeile, die den Profilnamen, die geschweiften Klammern {}, die auf den Profilnamen folgen, und den Inhalt innerhalb dieser Klammern enthält.
3. Speichern und schließen Sie die Datei.

Snowball Edge-Clientversion finden

Verwenden Sie den `version` Befehl, um die Version des Snowball Edge-Clients für die Befehlszeilenschnittstelle (CLI) anzuzeigen.

Usage

```
snowballEdge version
```

Beispielausgabe

```
Snowball Edge client version: 1.2.0 Build 661
```

Anmeldeinformationen für einen Snowball Edge abrufen

Mit den `snowballEdge get-secret-access-key` Befehlen `snowballEdge list-access-keys` und können Sie die Anmeldeinformationen des Admin-Benutzers AWS-Konto auf Ihrem Snowball Edge abrufen. Sie können diese Anmeldeinformationen verwenden, um AWS Identity and Access Management (IAM-Benutzer) und Rollen zu erstellen und Ihre Anfragen zu authentifizieren, wenn Sie das AWS CLI oder mit einem SDK verwenden. AWS Diese Anmeldeinformationen sind nur mit einem einzelnen Auftrag für Snowball Edge verknüpft, und Sie können sie nur auf dem Gerät oder Gerätecluster verwenden. Das Gerät oder die Geräte haben keine IAM-Berechtigungen in der. AWS Cloud

Note

Wenn Sie den AWS CLI mit Snowball Edge verwenden, müssen Sie diese Anmeldeinformationen bei der Konfiguration der CLI verwenden. Informationen zur Konfiguration der AWS CLI Anmeldeinformationen für finden Sie unter [Konfiguration von AWS CLI im AWS Command Line Interface](#) Benutzerhandbuch.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-access-keys
```

Example Output

```
{
  "AccessKeyIds" : [ "AKIAIOSFODNN7EXAMPLE" ]
}
```

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge get-secret-access-key --access-key-id Access Key
```

Example Output

```
[snowballEdge]  
aws_access_key_id = AKIAIOSFODNN7EXAMPLE  
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Einen Dienst auf einem Snowball Edge starten

Snowball Edge-Geräte unterstützen mehrere Dienste. Dazu gehören Recheninstanzen, die NFS-Schnittstelle (Network File System), Snowball Edge Device Management und AWS IoT Greengrass. Der Amazon S3 S3-Adapterservice EC2 AWS STS, Amazon und IAM werden standardmäßig gestartet und können nicht gestoppt oder neu gestartet werden. Die NFS-Schnittstelle, Snowball Edge Device Management, AWS IoT Greengrass kann jedoch mithilfe ihrer Dienst-ID mit dem `start-service` Befehl gestartet werden. Um die Service-ID für den jeweiligen Service zu erhalten, können Sie den Befehl `list-services` verwenden.

Bevor Sie diesen Befehl ausführen, erstellen Sie eine einzige virtuelle Netzwerkschnittstelle, die Sie an den Service bindet, den Sie gerade starten. Weitere Informationen finden Sie unter [Erstellen einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge](#).

```
snowballEdge start-service --service-id service_id --virtual-network-interface-  
arns virtual-network-interface-arn --profile profile-name
```

Example Ausgabe des Befehls **start-service**

```
Starting the AWS service on your Snowball Edge. You can determine the status of the AWS  
service using the describe-service command.
```

Beenden eines Dienstes auf einem Snowball Edge

Um einen Dienst zu beenden, der auf einem Snowball Edge ausgeführt wird, können Sie den `stop-service` Befehl verwenden.

Der Amazon S3 S3-Adapter EC2 AWS STS, Amazon und die IAM-Dienste können nicht gestoppt werden.

Warning

Datenverlust kann auftreten, wenn der Network File System (NFS) -Service gestoppt wird, bevor die verbleibenden gepufferten Daten auf das Gerät geschrieben werden. Weitere Informationen zur Verwendung des NFS-Dienstes finden Sie unter [Verwaltung der NFS-Schnittstelle auf Snowball Edge](#)

Note

Wenn Sie den Amazon S3 S3-kompatiblen Speicher auf dem Snowball Edge-Service beenden, wird der Zugriff auf die in Ihren S3-Buckets auf dem Gerät oder Cluster gespeicherten Daten deaktiviert. Der Zugriff wird wiederhergestellt, wenn der Amazon S3 S3-kompatible Speicher auf Snowball Edge erneut gestartet wird. Für Geräte, die mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge aktiviert sind, wird empfohlen, den Service nach dem Einschalten des Snowball Edge-Geräts zu starten. Weitere Informationen finden Sie in diesem Handbuch unter [Einrichtung von Snowball Edge](#).

```
snowballEdge stop-service --service-id service_id --profile profile-name
```

Example Ausgabe des Befehls **stop-service**

```
Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.
```

Protokolle von Snowball Edge anzeigen und herunterladen

Wenn Sie Daten zwischen Ihrem lokalen Rechenzentrum und einem Snowball Edge übertragen, werden automatisch Protokolle generiert. Sollten während der Datenübertragung auf das Gerät unerwartete Fehler auftreten, können Sie mit den folgenden Befehlen eine Kopie der Protokolle auf Ihrem lokalen Server speichern.

Im Zusammenhang mit Protokollen gibt es drei verschiedene Befehle:

- **list-logs**— Gibt eine Liste von Protokollen im JSON-Format zurück. In dieser Liste sind die Größe der Protokolle in Byte, die ARNs und die Service-ID für die Protokolle sowie die Art der Protokolle enthalten.

Usage

```
snowballEdge list-logs --profile profile-name
```

Example Ausgabe des **list-logs** Befehls

```
{
  "Logs" : [ {
    "LogArn" : "arn:aws:snowball-device::log/s3-storage-JIEXAMPLE2f-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "SUPPORT",
    "ServiceId" : "s3",
    "EstimatedSizeBytes" : 53132614
  }, {
    "LogArn" : "arn:aws:snowball-device::log/fileinterface-JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "CUSTOMER",
    "ServiceId" : "fileinterface",
    "EstimatedSizeBytes" : 4446
  } ]
}
```

- **get-log**— Lädt eine Kopie eines bestimmten Protokolls von Snowball Edge unter einem angegebenen Pfad auf Ihr Gerät herunter. CUSTOMERProtokolle werden in diesem .zip Format gespeichert, und Sie können diesen Protokolltyp extrahieren, um seinen Inhalt anzuzeigen. SUPPORTProtokolle sind verschlüsselt und können nur von gelesen werden AWS Support. Sie haben die Möglichkeit, einen Namen und einen Pfad für das Protokoll anzugeben.

Usage

```
snowballEdge get-log --log-arn arn:aws:snowball-device::log/fileinterface-JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709 --profile profile-name
```

Example Ausgabe des **get-log** Befehls

```
Logs are being saved to download/path/snowball-edge-logs-1515EXAMPLE88.bin
```

- **get-support-logs**— Lädt eine Kopie aller SUPPORT Protokolltypen von Snowball Edge unter einem angegebenen Pfad auf Ihren Service herunter.

Usage

```
snowballEdge get-support-logs --profile profile-name
```

Example Ausgabe des Befehls **get-support-logs**

```
Logs are being saved to download/path/snowball-edge-logs-1515716135711.bin
```

Important

CUSTOMER-Protokolle enthalten möglicherweise vertrauliche Informationen über Ihre Daten. Um solche potenziell sensiblen Daten zu schützen, empfehlen wir dringend, diese Protokolle zu löschen, sobald Sie sie nicht mehr verwenden.

Status eines Snowball Edge anzeigen

Mit dem **describe-device** Befehl können Sie den Status und den allgemeinen Zustand von Snowball Edge ermitteln.

```
snowballEdge describe-device --profile profile-name
```

Example Ausgabe des Befehls **describe-device**

```
{
  "DeviceId": "JID-EXAMPLE12345-123-456-7-890",
  "UnlockStatus": {
    "State": "UNLOCKED"
  },
  "ActiveNetworkInterface": {
```



```

    "IpAddress": "192.0.2.0"
  },
  "PhysicalNetworkInterfaces": [
    {
      "PhysicalNetworkInterfaceId": "s.ni-EXAMPLEd9ecbf03e3",
      "PhysicalConnectorType": "RJ45",
      "IpAddressAssignment": "STATIC",
      "IpAddress": "0.0.0.0",
      "Netmask": "0.0.0.0",
      "DefaultGateway": "192.0.2.1",
      "MacAddress": "EX:AM:PL:E0:12:34"
    },
    {
      "PhysicalNetworkInterfaceId": "s.ni-EXAMPLE4c3840068f",
      "PhysicalConnectorType": "QSFP",
      "IpAddressAssignment": "STATIC",
      "IpAddress": "0.0.0.0",
      "Netmask": "0.0.0.0",
      "DefaultGateway": "192.0.2.2",
      "MacAddress": "EX:AM:PL:E0:56:78"
    },
    {
      "PhysicalNetworkInterfaceId": "s.ni-EXAMPLE0a3a6499fd",
      "PhysicalConnectorType": "SFP_PLUS",
      "IpAddressAssignment": "DHCP",
      "IpAddress": "192.168.1.231",
      "Netmask": "255.255.255.0",
      "DefaultGateway": "192.0.2.3",
      "MacAddress": "EX:AM:PL:E0:90:12"
    }
  ]
}

```

Status von Diensten anzeigen, die auf Snowball Edge ausgeführt werden

Mit dem `describe-service` Befehl können Sie den Status und den allgemeinen Zustand der Dienste ermitteln, die auf Snowball Edge-Geräten ausgeführt werden. Sie können zunächst den `list-services`-Befehl ausführen, um zu sehen, welche Services ausgeführt werden.

- `list-services`

Usage

```
snowballEdge list-services --profile profile-name
```

Example Ausgabe des Befehls **list-services**

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

• describe-service

Dieser Befehl gibt einen Statuswert für einen Service zurück. Er enthält außerdem Statusinformationen, die Ihnen bei der Lösung von Problemen mit dem Service behilflich sein können. Diese Statuswerte lauten wie folgt.

- **ACTIVE** – Der Service wird ausgeführt und steht zur Verfügung.
- **ACTIVATING** – Der Service wird gestartet, steht aber noch nicht zur Verfügung.
- **DEACTIVATING** – Der Service wird gerade heruntergefahren.
- **DEGRADED**— Für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge bedeutet dieser Status, dass eine oder mehrere Festplatten oder Geräte im Cluster ausgefallen sind. Der Amazon S3 S3-kompatible Speicher auf dem Snowball Edge-Service läuft ununterbrochen, aber Sie sollten das betroffene Gerät wiederherstellen oder austauschen, bevor das Cluster-Quorum verloren geht, um das Risiko eines Datenverlusts zu minimieren. Weitere Informationen finden Sie in [diesem Handbuch im Überblick über Clustering](#).
- **INACTIVE** – Der Service wird nicht ausgeführt und steht nicht zur Verfügung.

Usage

```
snowballEdge describe-service --service-id service-id --profile profile-name
```

Example Ausgabe des Befehls **describe-service**

```
{
  "ServiceId": "s3",
  "Status": {
    "State": "ACTIVE"
  }
}
```

```

},
"Storage": {
  "TotalSpaceBytes": 99608745492480,
  "FreeSpaceBytes": 99608744468480
},
"Endpoints": [
  {
    "Protocol": "http",
    "Port": 8080,
    "Host": "192.0.2.0"
  },
  {
    "Protocol": "https",
    "Port": 8443,
    "Host": "192.0.2.0",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
    }
  }
]
}

```

Example Amazon S3 S3-kompatibler Speicher auf der Snowball Edge-Serviceausgabe

Der `describe-service` Befehl liefert die folgende Ausgabe für den *s3-snow* Wert des `service-id` Parameters.

```

{
  "ServiceId" : "s3-snow",
  "Autostart" : false,
  "Status" : {
    "State" : "ACTIVE"
  },
  "ServiceCapacities" : [ {
    "Name" : "S3 Storage",
    "Unit" : "Byte",
    "Used" : 640303104,
    "Available" : 219571981512
  } ],
  "Endpoints" : [ {
    "Protocol" : "https",

```

```

    "Port" : 443,
    "Host" : "10.0.2.123",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.202",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.63",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.243",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"

```

```

    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.220",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.55",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
        "State" : "ACTIVE"
    }
}, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.213",
    "CertificateAssociation" : {
        "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
        "State" : "ACTIVE"
    }
}

```

```

    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.144",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.143",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.224",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  }
]
}

```

Status der Funktionen von Snowball Edge anzeigen

Verwenden Sie den `describe-features` Befehl, um den Status der auf einem Snowball Edge verfügbaren Funktionen aufzulisten.

`RemoteManagementState` zeigt den Status von Snowball Edge Device Management an und gibt einen der folgenden Zustände zurück:

- `INSTALLED_ONLY`— Die Funktion ist installiert, aber nicht aktiviert.
- `INSTALLED_AUTOSTART`— Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu ihrer herzustellen AWS-Region, wenn es eingeschaltet ist.
- `NOT_INSTALLED`— Das Gerät unterstützt die Funktion nicht oder war vor der Markteinführung bereits im Einsatz.

Usage

```
snowballEdge describe-features --profile profile-name
```

Example Ausgabe des **describe-features** Befehls

```
{  
  "RemoteManagementState" : String  
}
```

Zeitserver für Snowball Edge einrichten

Sie können Snowball Edge-Client-Befehle verwenden, um die aktuelle NTP-Konfiguration (Network Time Protocol) anzuzeigen und einen Server oder Peer für die Bereitstellung von Zeit auszuwählen. Sie können die Snowball Edge Client-Befehle verwenden, wenn sich das Gerät sowohl im gesperrten als auch im entsperrten Zustand befindet.

Es liegt in Ihrer Verantwortung, einen sicheren NTP-Zeitserver bereitzustellen. Verwenden Sie den Befehl, um festzulegen, mit welchen NTP-Zeitservern das Gerät eine Verbindung herstellt. `update-time-servers`

Überprüfen der Zeitquellen von Snowball Edge

Verwenden Sie den `describe-time-sources` Befehl, um zu sehen, mit welchen NTP-Zeitquellen das Gerät derzeit verbunden ist.

```
snowballEdge describe-time-sources --profile profile-name
```

Example Ausgabe des Befehls **describe-time-sources**

```
{
  "Sources" : [ {
    "Address" : "172.31.2.71",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.3.203",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.0.178",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.3.178",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "216.239.35.12",
    "State" : "CURRENT",
    "Type" : "SERVER",
    "Stratum" : 1
  } ]
}
```

Der `describe-time-sources` Befehl gibt eine Liste von Zeitquellenzuständen zurück. Jeder Zeitquellenstatus enthält die Stratum Felder Address StateType,, und. Im Folgenden sind die Bedeutungen dieser Felder aufgeführt.

- **Address**— Der DNS-Name/die IP-Adresse der Zeitquelle.
- **State**— Der aktuelle Verbindungsstatus zwischen dem Gerät und dieser Zeitquelle. Es gibt fünf mögliche Zustände:
 - **CURRENT**— Die Zeitquelle wird derzeit verwendet, um die Zeit zu synchronisieren.
 - **COMBINED**— Die Zeitquelle wird mit der aktuellen Quelle kombiniert.
 - **EXCLUDED**— Die Zeitquelle wird durch den Kombinationsalgorithmus ausgeschlossen.
 - **LOST**— Die Verbindung mit der Zeitquelle wurde unterbrochen.
 - **UNACCEPTABLE**— Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder als Falselticker oder als zu stark variabel eingestuft wurde.
- **Type**— Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Server können mit dem `update-time-servers` Befehl festgelegt werden. Peers können nur andere Snowball Edge Edge-Geräte im Cluster sein und werden automatisch eingerichtet, wenn der Cluster verknüpft wird.
- **Stratum**— Dieses Feld zeigt die Schicht der Quelle. Stratum 1 weist auf eine Quelle mit einer lokal angeschlossenen Referenzuhr hin. Eine Quelle, die mit einer Stratum-1-Quelle synchronisiert ist, befindet sich in Stratum 2. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert ist, befindet sich in Stratum 3 usw.

Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Ein Server kann vom Benutzer mit dem `update-time-servers` Befehl eingerichtet werden, wohingegen ein Peer nur andere Snowball Edge Edge-Geräte im Cluster sein kann. In der Beispielausgabe `describe-time-sources` wird auf einem Snowball Edge Edge aufgerufen, der sich in einem Cluster von 5 befindet. Die Ausgabe enthält 4 Peers und 1 Server. Die Peers haben eine Schicht von 10, während der Server eine Schicht von 1 hat. Daher wird der Server als aktuelle Zeitquelle ausgewählt.

Zeitserver werden aktualisiert

Verwenden Sie den `update-time-servers` Befehl und die Adresse des Zeitserver, um Snowball Edge für die Verwendung eines NTP-Servers oder -Peers für NTP zu konfigurieren.

```
snowballEdge update-time-servers time-server-address --profile profile-name
```

Note

Der `update-time-servers` Befehl überschreibt die vorherigen NTP-Zeitserver-Einstellungen.

Example Ausgabe des Befehls `update-time-servers`

```
Updating time servers now.
```

Einen QR-Code zur Validierung von Snowball Edge NFC-Tags erhalten

Mit diesem Befehl können Sie einen gerätespezifischen QR-Code für die Verwendung mit der AWS Snowball Edge Verifizierungs-App generieren. Weitere Informationen zur NFC-Validierung finden Sie unter. [Validieren von NFC-Tags](#)

Usage

```
snowballEdge get-app-qr-code --output-file ~/downloads/snowball-qr-code.png --  
profile profile-name
```

Example Output

```
QR code is saved to ~/downloads/snowball-qr-code.png
```

Die MTU-Größe wird aktualisiert

Verwenden Sie den `update-mtu-size` Befehl, um die Größe der MTU (Maximum Transmission Unit) einer physikalischen Schnittstelle eines Snowball Edge-Geräts in Byte zu ändern. Alle virtuellen Netzwerkschnittstellen und direkten Netzwerkschnittstellen, die dieser physischen Netzwerkschnittstelle zugeordnet sind, werden mit derselben MTU-Größe konfiguriert.

Note

Die minimale MTU-Größe beträgt 1500 Byte und die maximale Größe beträgt 9216 Byte.

Sie können den `describe-device` Befehl verwenden, um die physische Netzwerkschnittstelle IDs und die aktuellen MTU-Größen dieser Schnittstellen abzurufen. Weitere Informationen finden Sie unter [Status eines Snowball Edge anzeigen](#).

Sie können die `describe-virtual-network-interface` Befehle `describe-direct-network-interface` und verwenden, um die aktuellen MTU-Größen dieser Schnittstellen abzurufen.

Usage

```
snowballEdge update-mtu-size --physical-network-interface-id physical-network-interface-id --mtu-size size-in-bytes --profile profile-name
```

Example der Ausgabe **update-mtu-size**

```
{
  "PhysicalNetworkInterface": {
    "PhysicalNetworkInterfaceId": "s.ni-8c1f891d7f5b87cfe",
    "PhysicalConnectorType": "SFP_PLUS",
    "IpAddressAssignment": "DHCP",
    "IpAddress": "192.0.2.0",
    "Netmask": "255.255.255.0",
    "DefaultGateway": "192.0.2.255",
    "MacAddress": "8A:2r:5G:9p:6Q:4s",
    "MtuSize": "5743"
  }
}
```

Übertragung von Dateien mithilfe des Amazon S3 S3-Adapters für die Datenmigration zu oder von Snowball Edge

Im Folgenden finden Sie eine Übersicht über den Amazon S3 S3-Adapter, mit dem Sie mithilfe von Amazon S3 S3-REST-API-Aktionen Daten programmgesteuert zu und von S3-Buckets übertragen können, die sich bereits auf dem AWS Snowball Edge Gerät befinden. Diese Amazon S3 S3-REST-API-Unterstützung ist auf eine Teilmenge von Aktionen beschränkt. Sie können diese Teilmenge von Aktionen mit einer der Aktionen verwenden, um Daten AWS SDKs programmgesteuert zu übertragen. Sie können auch die Teilmenge der unterstützten Befehle AWS Command Line Interface (AWS CLI) für Amazon S3 verwenden, um Daten programmgesteuert zu übertragen.

Wenn Ihre Lösung die AWS SDK für Java Version 1.11.0 oder neuer verwendet, müssen Sie Folgendes verwenden: `S3ClientOptions`

- `disableChunkedEncoding()`— Zeigt an, dass die Chunk-Codierung von der Schnittstelle nicht unterstützt wird.
- `setPathStyleAccess(true)`— Konfiguriert die Schnittstelle so, dass sie für alle Anfragen den Zugriff im Pfadstil verwendet.

Weitere Informationen finden Sie unter [Class S3 ClientOptions .Builder](#) im Amazon AppStream SDK for Java.

Important

Wir empfehlen, jeweils nur eine Methode zu verwenden, um Daten in einen lokalen Bucket auf einem AWS Snowball Edge Gerät zu lesen und zu schreiben. Die gleichzeitige Verwendung der NFS-Schnittstelle und des Amazon S3 S3-Adapters auf demselben Bucket kann zu read/write Konflikten führen.

[AWS Snowball Edge Kontingente](#) beschreibt die Grenzwerte.

Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter [Portanforderungen für AWS Dienste auf einem Snowball Edge](#).

- [Herunterladen und Installieren der AWS CLI Version 1.16.14 zur Verwendung mit dem Amazon S3 S3-Adapter](#)
- [Verwenden der API-Operationen AWS CLI und auf Snowball Edge-Geräten](#)
- [Abrufen und Verwenden lokaler Amazon S3 S3-Anmeldeinformationen auf Snowball Edge](#)
- [Nicht unterstützte Amazon S3 S3-Funktionen für den Amazon S3 S3-Adapter auf Snowball Edge](#)
- [Batching kleiner Dateien zur Verbesserung der Datenübertragungsleistung an Snowball Edge](#)
- [Unterstützte AWS CLI Befehle für die Datenübertragung zu oder von Snowball Edge](#)
- [Unterstützte Amazon S3 S3-REST-API-Aktionen auf Snowball Edge für die Datenübertragung](#)

Herunterladen und Installieren der AWS CLI Version 1.16.14 zur Verwendung mit dem Amazon S3 S3-Adapter

Derzeit unterstützen Snowball Edge-Geräte nur Version 1.16.14 und frühere Versionen von AWS CLI für die Verwendung mit dem Amazon S3 S3-Adapter. Neuere Versionen von AWS CLI sind nicht mit dem Amazon S3 S3-Adapter kompatibel, da sie nicht alle Funktionen des S3-Adapters unterstützen.

Note

Wenn Sie Amazon S3 S3-kompatible Speicher auf Snowball Edge verwenden, können Sie die neueste Version von verwenden. AWS CLI Informationen zum Herunterladen und Verwenden der neuesten Version finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

Installieren Sie das AWS CLI auf Linux-Betriebssystemen

Führen Sie diesen verketteten Befehl aus:

```
curl "https://s3.amazonaws.com/aws-cli/awscli-bundle-1.16.14.zip" -o "awscli-bundle.zip";unzip awscli-bundle.zip;sudo ./awscli-bundle/install -i /usr/local/aws -b /usr/local/bin/aws;/usr/local/bin/aws --version;
```

Installieren Sie das AWS CLI auf Windows-Betriebssystemen

Laden Sie die Installationsdatei für Ihr Betriebssystem herunter und führen Sie sie aus:

- [32-Bit-Installationsprogramm im Paket mit Python 2](#)
- [32-Bit-Installationsprogramm im Paket mit Python 3](#)
- [64-Bit-Installer im Paket mit Python 2](#)
- [64-Bit-Installer im Paket mit Python 3](#)
- [Setup-Datei mit 32- und 64-Bit-Installationsprogrammen, die automatisch die richtige Version installieren](#)

Verwenden der API-Operationen AWS CLI und auf Snowball Edge-Geräten

Wenn Sie die API-Operationen AWS CLI oder verwenden, um IAM-, Amazon S3- und EC2 Amazon-Befehle auf Snowball Edge auszugeben, müssen Sie die Region als "" snow angeben. Sie können dies mithilfe `aws configure` oder innerhalb des Befehls selbst tun, wie in den folgenden Beispielen.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Oder

```
aws s3 ls --endpoint http://192.0.2.0:8080 --region snow --profile snowballEdge
```

Autorisierung mit der Amazon S3 S3-API-Schnittstelle für AWS Snowball Edge

Wenn Sie den Amazon S3 S3-Adapter verwenden, wird jede Interaktion standardmäßig mit dem AWS Signature Version 4-Algorithmus signiert. Diese Autorisierung wird nur verwendet, um die Daten zu verifizieren, die von der Quelle zur Schnittstelle übertragen werden. Die gesamte Ver- und Entschlüsselungen erfolgt auf dem Gerät. Es werden zu keiner Zeit unverschlüsselte Daten auf dem Gerät gespeichert.

Beachten Sie bei der Verwendung der Schnittstelle Folgendes:

- Um die lokalen Amazon S3 S3-Anmeldeinformationen zum Signieren Ihrer Anfragen auf dem AWS Snowball Edge Gerät zu erhalten, führen Sie die Client-Befehle `snowballEdge list-access-keys` und `snowballEdge get-secret-access-keys` Snowball Edge aus. Weitere Informationen finden Sie unter [Konfiguration und Verwendung des Snowball Edge-Clients](#). Diese lokalen Amazon S3 S3-Anmeldeinformationen umfassen ein Schlüsselpaar: einen Zugriffsschlüssel und einen geheimen Schlüssel. Diese Schlüssel sind nur für die Geräte gültig, die Ihrem Auftrag zugeordnet sind. Sie können nicht in der verwendet werden AWS Cloud , da sie kein AWS Identity and Access Management (IAM-) Gegenstück haben.
- Der Verschlüsselungsschlüssel wird nicht durch die von Ihnen verwendeten AWS Anmeldeinformationen geändert. Das Signieren mit dem Signature Version 4-Algorithmus wird nur zur Überprüfung der Daten verwendet, die von der Quelle zur Schnittstelle übertragen werden. Daher berücksichtigt diese Signatur niemals die Verschlüsselungsschlüssel, die zur Verschlüsselung Ihrer Daten auf dem Snowball verwendet werden.

Abrufen und Verwenden lokaler Amazon S3 S3-Anmeldeinformationen auf Snowball Edge

Jede Interaktion mit einem Snowball Edge wird mit dem AWS Signature Version 4-Algorithmus signiert. Weitere Informationen zum Algorithmus finden Sie unter [Signature Version 4-Signierungsprozess](#) in der Allgemeine AWS-Referenz.

Sie können die lokalen Amazon S3 S3-Anmeldeinformationen abrufen, um Ihre Anfragen auf dem Edge-Gerät des Snowball Edge-Clients zu signieren, indem Sie die `snowballEdge list-access-keys` und `snowballEdge get-secret-access-key` Snowball Edge-Client-Informationen ausführen, siehe. [Anmeldeinformationen für einen Snowball Edge abrufen](#) Diese lokalen Amazon S3 S3-Anmeldeinformationen umfassen ein Schlüsselpaar: eine Zugriffsschlüssel-ID und einen geheimen Schlüssel. Diese Anmeldeinformationen sind nur für die Geräte gültig, die Ihrer Aufgabe zugeordnet sind. Sie können in der nicht verwendet werden AWS Cloud , da sie kein IAM-Gegenstück haben.

Sie können diese Anmeldeinformationen zur AWS Anmeldeinformationsdatei auf Ihrem Server hinzufügen. Die Datei mit den Standard-Anmeldeinformationsprofilen befindet sich in der Regel in `~/.aws/credentials`, der Speicherort kann aber je nach Plattform abweichen. Diese Datei wird von vielen gemeinsam genutzt AWS SDKs und von den AWS CLI. Sie können lokale Anmeldeinformationen mit einem Profilnamen speichern, wie im folgenden Beispiel.

```
[snowballEdge]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Konfiguration des AWS CLI für die Verwendung des S3-Adapters auf einem Snowball Edge als Endpunkt

Wenn Sie den verwenden AWS CLI , um einen Befehl an das AWS Snowball Edge Gerät zu senden, geben Sie an, dass der Endpunkt der Amazon S3 S3-Adapter ist. Sie können den HTTPS-Endpunkt oder einen ungesicherten HTTP-Endpunkt, wie hier gezeigt, verwenden.

Gesicherter HTTPS-Endpunkt

```
aws s3 ls --endpoint https://192.0.2.0:8443 --ca-bundle path/to/certificate --profile
snowballEdge
```

Ungesicherter HTTP-Endpunkt

```
aws s3 ls --endpoint http://192.0.2.0:8080 --profile snowballEdge
```

Wenn Sie den HTTPS-Endpunkt von verwenden 8443, werden Ihre Daten sicher von Ihrem Server zum Snowball Edge übertragen. Diese Verschlüsselung wird durch ein Zertifikat gewährleistet, das vom Snowball Edge generiert wird, wenn er eine neue IP-Adresse erhält. Nachdem Sie Ihr Zertifikat erhalten haben, können Sie es in einer lokalen `ca-bundle.pem`-Datei speichern. Anschließend können Sie Ihr AWS CLI Profil so konfigurieren, dass es den Pfad zu Ihrem Zertifikat enthält, wie im Folgenden beschrieben.

Um Ihr Zertifikat dem Schnittstellenendpunkt zuzuordnen

1. Connect den Snowball Edge mit der Stromversorgung und dem Netzwerk und schalten Sie ihn ein.
2. Notieren Sie nach dem Start des Gerätes seine IP-Adresse auf dem lokalen Netzwerk.
3. Stellen Sie sicher, dass Sie Snowball Edge von einem Terminal in Ihrem Netzwerk aus pingen können.
4. Führen Sie den `snowballEdge get-certificate`-Befehl in Ihrem Terminal aus. Weitere Informationen zu diesem Befehl finden Sie unter [Verwaltung von Public-Key-Zertifikaten auf Snowball Edge](#).

5. Speichern Sie die Ausgabe des `snowballEdge get-certificate`-Befehls in einer Datei, z. B. `ca-bundle.pem`.
6. Führen Sie im Terminal den folgenden Befehl aus:

```
aws configure set profile.snowballEdge.ca_bundle /path/to/ca-bundle.pem
```

Wenn das Verfahren abgeschlossen ist, können Sie CLI-Befehle mit diesen lokalen Anmeldeinformationen, Ihrem Zertifikat und dem angegebenen Endpunkt wie im folgenden Beispiel dargestellt ausführen.

```
aws s3 ls --endpoint https://192.0.2.0:8443 --profile snowballEdge
```

Nicht unterstützte Amazon S3 S3-Funktionen für den Amazon S3 S3-Adapter auf Snowball Edge

Mithilfe des Amazon S3 S3-Adapters können Sie mit Amazon S3 S3-API-Aktionen programmgesteuert Daten zu und von einem Snowball Edge übertragen. Allerdings werden nicht alle Amazon S3 S3-Übertragungsfunktionen und API-Aktionen für die Verwendung mit einem Snowball Edge-Gerät unterstützt, wenn der Amazon S3 S3-Adapter verwendet wird. Beispielsweise werden die folgenden Funktionen und Aktionen für die Verwendung mit Snowball Edge nicht unterstützt:

- [TransferManager](#)— Dieses Tool überträgt Dateien mit dem SDK for Java aus einer lokalen Umgebung nach Amazon S3. Erwägen Sie stattdessen, die unterstützten API-Aktionen oder AWS CLI -Befehle mit der Schnittstelle zu verwenden.
- [GET Bucket \(List Objects\) Version 2](#) — Diese Implementierung der GET-Aktion gibt einige oder alle (bis zu 1.000) Objekte in einem Bucket zurück. Erwägen Sie, die Aktion [GET Bucket \(List Objects\) Version 1](#) oder den AWS CLI Befehl `ls` zu verwenden.
- [ListBuckets](#)— Der Endpunkt ListBuckets mit dem Objekt wird nicht unterstützt. Der folgende Befehl funktioniert nicht mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge:

```
aws s3 ls --endpoint https://192.0.2.0 --profile profile
```

Batching kleiner Dateien zur Verbesserung der Datenübertragungsleistung an Snowball Edge

Bei jeder Kopieroperation entsteht ein zusätzlicher verschlüsselungsbedingter Overhead. Um die Übertragung kleiner Dateien auf Ihr AWS Snowball Edge Gerät zu beschleunigen, können Sie sie in einem einzigen Archiv zusammenfassen. Wenn Sie Dateien stapeln, können sie beim Import in Amazon S3 automatisch extrahiert werden, sofern sie in einem der unterstützten Archivformate gebündelt wurden.

In der Regel sollten Dateien, die 1 MB oder kleiner sind, in Stapeln gespeichert werden. Es gibt keine Begrenzung für die Anzahl der Dateien, die in Stapeln gespeichert werden können. Wir empfehlen jedoch, dass Sie Ihre Stapel auf ca. 10 000 Dateien begrenzen. Wenn Sie mehr als 100.000 Dateien in einem Stapel haben, kann dies beeinflussen, wie schnell diese Dateien nach der Rückgabe des Geräts in Amazon S3 importiert werden. Wir empfehlen, die Gesamtgröße der einzelnen Stapel auf max. 100 GB zu beschränken.

Das Stapeln von Dateien ist ein manueller Prozess, den Sie verwalten. Nachdem Sie Ihre Dateien gebündelt haben, übertragen Sie sie mithilfe des AWS CLI `cp` Befehls mit der `--metadata snowball-auto-extract=true` Option auf ein Snowball Edge-Gerät. Wenn Sie angeben, wird der Inhalt der archivierten Dateien `snowball-auto-extract=true` automatisch extrahiert, wenn die Daten in Amazon S3 importiert werden, sofern die Größe der Batchdatei nicht größer als 100 GB ist.

Note

Stapel, die größer als 100 GB sind, werden nicht extrahiert, wenn sie in Amazon S3 importiert werden.

So stapeln Sie kleine Dateien

1. Bestimmen Sie, in welchem Format die kleinen Dateien gestapelt werden sollen. Die Funktion zum automatischen Extrahieren unterstützt die Formate TAR, ZIP, `tar.gz`.
2. Identifizieren Sie, welche kleinen Dateien zusammen gestapelt werden sollen. Schließen Sie deren Größe und die Gesamtzahl der Dateien ein, die zusammen gestapelt werden sollen.
3. Stapeln Sie Ihre Dateien in der Befehlszeile, wie in den folgenden Beispielen gezeigt.

- Unter Linux können Sie die Dateien in derselben Befehlszeile stapeln, mit der Sie Ihre Dateien auf das Gerät übertragen haben.

```
tar -cf - /Logs/April | aws s3 cp - s3://amzn-s3-demo-bucket/batch01.tar --  
metadata snowball-auto-extract=true --endpoint http://192.0.2.0:8080
```

Note

Alternativ können Sie ein Archivierungsprogramm Ihrer Wahl verwenden, um Dateien in einem oder mehreren großen Archiven zu stapeln. Dieser Ansatz erfordert jedoch zusätzlichen lokalen Speicher, um die Archive zu speichern, bevor Sie sie auf den Snowball Edge übertragen.

- Verwenden Sie für Windows den folgenden Beispielbefehl, um die Dateien zu stapeln, wenn sich alle Dateien in demselben Verzeichnis befinden, von dem aus der Befehl ausgeführt wird:

```
7z a -tzip -so "test" | aws s3 cp - s3://amzn-s3-demo-bucket/batch01.zip --  
metadata snowball-auto-extract=true --endpoint http://192.0.2.0:8080
```

Verwenden Sie den folgenden Beispielbefehl, um Dateien aus einem anderen Verzeichnis zu stapeln, von dem aus der Befehl ausgeführt wird:

```
7z a -tzip -so "test" "c:\temp" | aws s3 cp - s3://amzn-s3-demo-bucket/  
batch01.zip --metadata snowball-auto-extract=true --endpoint http://10.x.x.x:8080
```

Note

Für Microsoft Windows 2016 ist Tar nicht verfügbar, Sie können es jedoch von der Tar for Windows-Website herunterladen.

Sie können 7 ZIP von der 7ZIP-Website herunterladen.

4. Wiederholen Sie den Vorgang, bis Sie alle kleinen Dateien archiviert haben, die Sie mit einem Snowball Edge auf Amazon S3 übertragen möchten.
5. Übertragen Sie die archivierten Dateien auf den Snowball. Wenn Sie möchten, dass die Daten automatisch extrahiert werden, und Sie eines der zuvor in Schritt 1 genannten unterstützten

Archivformate verwendet haben, verwenden Sie den AWS CLI cp Befehl mit der `--metadata snowball-auto-extract=true` Option.

 Note

Wenn es Dateien gibt, die keine Archivdateien sind, verwenden Sie diesen Befehl nicht.

Beim Erstellen der Archivdateien wird bei der Extraktion die aktuelle Datenstruktur beibehalten. Das heißt, wenn Sie eine Archivdatei erstellen, die Dateien und Ordner enthält, erstellt Snowball Edge diese während der Aufnahme in Amazon S3 neu.

Die Archivdatei wird in dasselbe Verzeichnis extrahiert, in dem sie gespeichert ist, und die Ordnerstrukturen werden entsprechend aufgebaut. Beachten Sie, dass es beim Kopieren von Archivdateien wichtig ist, die Markierung zu setzen `--metadata snowball-auto-extract=true`. Andernfalls extrahiert Snowball Edge die Daten nicht, wenn sie in Amazon S3 importiert werden.

Verwenden Sie das Beispiel in Schritt 3, wenn Sie die Ordnerstruktur `/Logs/April/` haben, die Dateien enthält, und `a.txt b.txt c.txt`. Wenn diese Archivdatei im Stammverzeichnis von `/amzn-s3-demo-bucket/` platziert würde, würden die Daten nach dem Extrahieren wie folgt aussehen:

```
/amzn-s3-demo-bucket/Logs/April/a.txt  
/amzn-s3-demo-bucket/Logs/April/b.txt  
/amzn-s3-demo-bucket/Logs/April/c.txt
```

Wenn die Archivdatei in `/amzn-s3-demo-bucket/Test/` platziert würde, würde die Extraktion wie folgt aussehen:

```
/amzn-s3-demo-bucket/Test/Logs/April/a.txt  
/amzn-s3-demo-bucket/Test/Logs/April/b.txt  
/amzn-s3-demo-bucket/Test/Logs/April/c.txt
```

Unterstützte AWS CLI Befehle für die Datenübertragung zu oder von Snowball Edge

Im Folgenden finden Sie Informationen dazu, wie Sie den Amazon S3-Adapter oder den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge als Endpunkt für die entsprechenden AWS Command Line Interface (AWS CLI) -Befehle angeben. Die Liste der AWS CLI Befehle für Amazon S3, die für

die Übertragung von Daten auf das AWS Snowball Edge Gerät mit dem Adapter oder Amazon S3 S3-kompatiblen Speicher unterstützt werden, finden Sie auch auf Snowball Edge.

 Note

Informationen zur Installation und Einrichtung von AWS CLI, einschließlich der Angabe, in welche Regionen Sie AWS CLI telefonieren möchten, finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

Derzeit unterstützen Snowball Edge-Geräte nur Version 1.16.14 und frühere Versionen von, AWS CLI wenn der Amazon S3 S3-Adapter verwendet wird. Siehe [Snowball Edge-Clientversion finden](#). Wenn Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden, können Sie die neueste Version von verwenden. AWS CLI Informationen zum Herunterladen und Verwenden der neuesten Version finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

 Note

Sie müssen die Python-Versionen 2.6.5+ oder 3.4+ installieren, bevor Sie die Version 1.16.14 der AWS CLI installieren.

Unterstützte AWS CLI Befehle für die Datenübertragung mit Amazon S3 und Snowball Edge

Im Folgenden finden Sie eine Beschreibung der Teilmenge der AWS CLI Befehle und Optionen für Amazon S3, die das AWS Snowball Edge Gerät unterstützt. Wenn ein Befehl oder eine Option nicht aufgeführt ist, wird sie nicht unterstützt. Sie können einige nicht unterstützte Optionen in Kombination mit einem Befehl angeben, z. B. `--sse` oder `--storage-class`. Diese werden jedoch ignoriert und haben keine Auswirkung auf die Art und Weise, wie Daten importiert werden.

- [cp](#) — Kopiert eine Datei oder ein Objekt auf das oder vom AWS Snowball Edge Gerät. Im Folgenden werden die Optionen für diesen Befehl aufgeführt:
 - `--dryrun(Boolean)` — Die Operationen, die mit dem angegebenen Befehl ausgeführt würden, werden angezeigt, ohne dass sie ausgeführt wurden.
 - `--quiet(Boolean)` — Operationen, die mit dem angegebenen Befehl ausgeführt wurden, werden nicht angezeigt.

- `--include(string)` — Schließt keine Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen. Einzelheiten finden Sie in der AWS CLI Befehlsreferenz unter [Verwendung von Ausschließ- und Einschlussfiltern](#).
- `--exclude(string)` — Schließt alle Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen.
- `--follow-symlinks` | `--no-follow-symlinks(Boolean)` — Symbolischen Links (Symlinks) wird nur gefolgt, wenn aus dem lokalen Dateisystem auf Amazon S3 hochgeladen wird. Amazon S3 unterstützt keine symbolischen Links, daher werden die Inhalte des Linkziels unter dem Namen des Links hochgeladen. Wenn keine Option angegeben ist, wird symbolischen Links standardmäßig gefolgt.
- `--only-show-errors(Boolean)` — Es werden nur Fehler und Warnungen angezeigt. Jede sonstige Ausgabe wird unterdrückt.
- `--recursive(Boolean)` — Der Befehl wird für alle Dateien oder Objekte im angegebenen Verzeichnis oder Präfix ausgeführt.
- `--page-size(Ganzzahl)` — Die Anzahl der Ergebnisse, die in jeder Antwort auf eine Listenoperation zurückgegeben werden sollen. Der Standardwert lautet 1000 (das zulässige Maximum). Ein niedrigerer Wert kann bei einem Timeout einer Operation hilfreich sein.
- `--metadata(map)` — Eine Karte mit Metadaten, die zusammen mit den Objekten in Amazon S3 gespeichert werden sollen. Diese Map wird auf jedes Objekt angewendet, das Teil dieser Anforderung ist. Bei einer Synchronisierung bedeutet diese Funktionalität, dass unveränderte Dateien die neuen Metadaten nicht erhalten. Beim Kopieren zwischen zwei Amazon S3 Standorten ist das `metadata-directive` Argument standardmäßig auf, REPLACE sofern nicht anders angegeben.
- `ls` — Listet Objekte auf dem AWS Snowball Edge Gerät auf. Im Folgenden werden die Optionen für diesen Befehl aufgeführt:
 - `--human-readable(Boolean)` — Dateigrößen werden in einem für Menschen lesbaren Format angezeigt.
 - `--summarize(Boolean)` — Zusammenfassungsinformationen werden angezeigt. Diese Information stellt die Anzahl der Objekte und deren Gesamtgröße dar.
 - `--recursive(Boolean)` — Der Befehl wird für alle Dateien oder Objekte im angegebenen Verzeichnis oder Präfix ausgeführt.
 - `--page-size(Ganzzahl)` — Die Anzahl der Ergebnisse, die in jeder Antwort auf eine Listenoperation zurückgegeben werden sollen. Der Standardwert lautet 1000 (das zulässige Maximum). Ein niedrigerer Wert kann bei einem Timeout einer Operation hilfreich sein.

- [rm](#) — Löscht ein Objekt auf dem AWS Snowball Edge Gerät. Im Folgenden werden die Optionen für diesen Befehl aufgeführt:
 - `--dryrun(Boolean)` — Die Operationen, die mit dem angegebenen Befehl ausgeführt würden, werden angezeigt, ohne dass sie ausgeführt wurden.
 - `--include(string)` — Schließt keine Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen. Einzelheiten finden Sie in der AWS CLI Befehlsreferenz unter [Verwendung von Ausschließ- und Einschlussfiltern](#).
 - `--exclude(string)` — Schließt alle Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen.
 - `--recursive(Boolean)` — Der Befehl wird für alle Dateien oder Objekte im angegebenen Verzeichnis oder Präfix ausgeführt.
 - `--page-size(Ganzzahl)` — Die Anzahl der Ergebnisse, die in jeder Antwort auf eine Listenoperation zurückgegeben werden sollen. Der Standardwert lautet 1000 (das zulässige Maximum). Ein niedrigerer Wert kann bei einem Timeout einer Operation hilfreich sein.
 - `--only-show-errors(Boolean)` — Es werden nur Fehler und Warnungen angezeigt. Jede sonstige Ausgabe wird unterdrückt.
 - `--quiet(Boolean)` — Mit dem angegebenen Befehl ausgeführte Operationen werden nicht angezeigt.
- [sync](#) — [Synchronisiert](#) Verzeichnisse und Präfixe. Mit diesem Befehl werden neue und aktualisierte Dateien aus dem Quellverzeichnis in das Ziel kopiert. Dieser Befehl erstellt nur Verzeichnisse im Ziel, wenn sie eine oder mehrere Dateien enthalten.

 Important

Die Synchronisierung von einem Verzeichnis zu einem anderen Verzeichnis auf demselben Snowball Edge wird nicht unterstützt.

Die Synchronisierung von einem AWS Snowball Edge Gerät zu einem anderen AWS Snowball Edge Gerät wird nicht unterstützt.

Sie können diese Option nur verwenden, um den Inhalt zwischen Ihrem lokalen Datenspeicher und einem Snowball Edge zu synchronisieren.

- `--dryrun(Boolean)` — Die Operationen, die mit dem angegebenen Befehl ausgeführt würden, werden angezeigt, ohne ausgeführt zu werden.

- `--quiet(Boolean)` — Operationen, die mit dem angegebenen Befehl ausgeführt wurden, werden nicht angezeigt.
- `--include(string)` — Schließt keine Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen. Einzelheiten finden Sie in der AWS CLI Befehlsreferenz unter [Verwendung von Ausschließ- und Einschlussfiltern](#).
- `--exclude(string)` — Schließt alle Dateien oder Objekte aus dem Befehl aus, die dem angegebenen Muster entsprechen.
- `--follow-symlinks` oder `--no-follow-symlinks (Boolean)` — Symbolischen Links (Symlinks) wird nur gefolgt, wenn vom lokalen Dateisystem auf Amazon S3 hochgeladen wird. Amazon S3 unterstützt keine symbolischen Links, daher werden die Inhalte des Linkziels unter dem Namen des Links hochgeladen. Wenn keine Option angegeben ist, wird symbolischen Links standardmäßig gefolgt.
- `--only-show-errors(Boolean)` — Es werden nur Fehler und Warnungen angezeigt. Jede sonstige Ausgabe wird unterdrückt.
- `--no-progress(Boolean)` — Der Fortschritt der Dateiübertragung wird nicht angezeigt. Diese Option wird nur angewendet, wenn die Optionen `--quiet` und `--only-show-errors` nicht verwendet werden.
- `--page-size(Ganzzahl)` — Die Anzahl der Ergebnisse, die in jeder Antwort auf einen Listenvorgang zurückgegeben werden sollen. Der Standardwert lautet 1000 (das zulässige Maximum). Ein niedrigerer Wert kann bei einem Timeout einer Operation hilfreich sein.
- `--metadata(map)` — Eine Karte mit Metadaten, die zusammen mit den Objekten in Amazon S3 gespeichert werden sollen. Diese Map wird auf jedes Objekt angewendet, das Teil dieser Anforderung ist. Bei einer Synchronisierung bedeutet diese Funktionalität, dass unveränderte Dateien die neuen Metadaten nicht erhalten. Beim Kopieren zwischen zwei Amazon S3 S3-Standorten ist das `metadata-directive` Argument standardmäßig auf, REPLACE sofern nicht anders angegeben.

 Important

Die Synchronisierung von einem Verzeichnis zu einem anderen Verzeichnis auf demselben Snowball Edge wird nicht unterstützt.

Die Synchronisierung von einem AWS Snowball Edge Gerät zu einem anderen AWS Snowball Edge Gerät wird nicht unterstützt.

Sie können diese Option nur verwenden, um den Inhalt zwischen Ihrem lokalen Datenspeicher und einem Snowball Edge zu synchronisieren.

- `--size-only(Boolean)` — Bei dieser Option ist die Größe jedes Schlüssels das einzige Kriterium, anhand dessen entschieden wird, ob von der Quelle zum Ziel synchronisiert werden soll.
- `--exact-timestamps(Boolean)` — Bei der Synchronisierung von Amazon S3 mit dem lokalen Speicher werden Elemente gleicher Größe nur ignoriert, wenn die Zeitstempel exakt übereinstimmen. Standardmäßig werden Artikel gleicher Größe ignoriert, es sei denn, die lokale Version ist neuer als die Amazon S3 S3-Version.
- `--delete(Boolean)` — Dateien, die im Ziel, aber nicht in der Quelle existieren, werden während der Synchronisierung gelöscht.

Sie können Dateien oder Ordner mit Leerzeichen in den Namen verwenden, z. B. `my photo.jpg` oder `My Documents`. Stellen Sie jedoch sicher, dass Sie die Leerzeichen in den AWS CLI Befehlen richtig behandeln. Weitere Informationen finden Sie unter [Angaben von Parameterwerten für die AWS CLI](#) im AWS Command Line Interface Benutzerhandbuch.

Unterstützte Amazon S3 S3-REST-API-Aktionen auf Snowball Edge für die Datenübertragung

Im Folgenden finden Sie die Liste der Amazon S3 S3-REST-API-Aktionen, die für die Verwendung des Amazon S3 S3-Adapters unterstützt werden. Die Liste enthält Links zu Informationen darüber, wie die API-Aktionen mit Amazon S3 funktionieren. Die Liste deckt auch alle Verhaltensunterschiede zwischen der Amazon S3 S3-API-Aktion und dem Gegenstück auf dem AWS Snowball Edge Gerät ab. Alle Antworten, die von einem AWS Snowball Edge Gerät zurückkommen `AWSSnowball`, Server werden als deklariert, wie im folgenden Beispiel.

```
HTTP/1.1 201 OK
x-amz-id-2: JuKZqmXuiwFeDQxhD7M8KtsKobSzWA1QEjLbTMTagkKdBX2z7I1/jGhDeJ3j6s80
x-amz-request-id: 32FE2CEB32F5EE25
Date: Fri, 08 2016 21:34:56 GMT
Server: AWSSnowball
```

Amazon S3 S3-REST-API-Aufrufe erfordern eine SigV4-Signatur. Wenn Sie das AWS CLI oder ein AWS SDK für diese API-Aufrufe verwenden, wird die SigV4-Signatur für Sie übernommen.

Andernfalls müssen Sie Ihre eigene SigV4 Signatur-Lösung implementieren. Weitere Informationen finden Sie unter [Authentifizieren von Anfragen \(AWS Signature Version 4\)](#) im Amazon Simple Storage Service-Benutzerhandbuch.

- [GET Bucket \(Objekte auflisten\) Version 1](#) — Unterstützt. In dieser Implementierung der GET-Operation wird Folgendes jedoch nicht unterstützt:
 - Paginierung
 - Marker
 - Trennzeichen
 - Wenn die Liste zurückgegeben wird, ist die Liste nicht sortiert

Es wird nur Version 1 unterstützt. GET Bucket (List Objects) Version 2 wird nicht unterstützt.

- [GET-Dienst](#)
- [HEAD Eimer](#)
- [HEAD Object](#)
- [GET Object](#) — ist ein DOWNLOAD eines Objekts aus dem S3-Bucket des Snow-Geräts.
- [PUT-Object](#) — Wenn ein Objekt mithilfe von auf ein AWS Snowball Edge Gerät hochgeladen wirdPUT Object, ETag wird ein generiert.

Das ETag ist ein Hash des Objekts. Das ETag spiegelt nur Änderungen am Inhalt eines Objekts wider, nicht an seinen Metadaten. Dies ETag kann eine MD5 Zusammenfassung der Objektdaten sein oder auch nicht. Weitere Informationen ETags finden Sie unter [Common Response Headers](#) in der Amazon Simple Storage Service API-Referenz.

- [DELETE Object](#)
- [Mehrteiligen Upload initiieren](#) — In dieser Implementierung wird durch das Initiieren einer mehrteiligen Upload-Anfrage für ein Objekt, das sich bereits auf dem AWS Snowball Edge Gerät befindet, dieses Objekt zuerst gelöscht. Anschließend wird es in Teilen auf das Gerät kopiert. AWS Snowball Edge
- [List Multipart Uploads](#)
- [Upload Part](#)
- [Abschließen eines mehrteiligen Uploads](#)
- [Abort Multipart Upload](#)

 Note

Alle hier nicht aufgeführten Amazon S3 S3-Adapter-REST-API-Aktionen werden nicht unterstützt. Wenn Sie nicht unterstützte REST-API-Aktionen mit Ihrem Snowball Edge verwenden, wird eine Fehlermeldung zurückgegeben, die besagt, dass die Aktion nicht unterstützt wird.

Verwaltung der NFS-Schnittstelle auf Snowball Edge

Verwenden Sie die NFS-Schnittstelle (Network File System), um Dateien auf den Snowball Edge hochzuladen, als ob das Gerät ein lokaler Speicher Ihres Betriebssystems wäre. Dies ermöglicht einen benutzerfreundlicheren Ansatz für die Übertragung von Daten, da Sie Funktionen Ihres Betriebssystems wie das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche verwenden können. Jeder S3-Bucket auf dem Gerät ist als Endpunkt der NFS-Schnittstelle verfügbar und kann für das Kopieren von Daten bereitgestellt werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

Sie können die NFS-Schnittstelle verwenden, wenn das Snowball Edge-Gerät so konfiguriert wurde, dass es bei der Erstellung des Auftrags zur Bestellung des Geräts berücksichtigt wurde. Wenn das Gerät nicht so konfiguriert ist, dass es die NFS-Schnittstelle enthält, verwenden Sie den S3-Adapter oder Amazon S3 S3-kompatiblen Speicher auf Snowball Edge, um Daten zu übertragen. Weitere Informationen zum S3-Adapter finden Sie unter [Verwaltung des Amazon S3 S3-Adapterspeichers mit AWS OpsHub](#). Weitere Informationen zu Amazon S3 S3-kompatiblen Speicher auf Snowball Edge finden Sie unter [Richten Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ein mit AWS OpsHub](#).

Beim Start verwendet die NFS-Schnittstelle 1 GB Arbeitsspeicher und 1 CPU. Dies kann die Anzahl anderer Dienste, die auf dem Snowball Edge ausgeführt werden, oder die Anzahl der EC2 - kompatiblen Instanzen, die ausgeführt werden können, einschränken.

Daten, die über die NFS-Schnittstelle übertragen werden, werden bei der Übertragung nicht verschlüsselt. Bei der Konfiguration der NFS-Schnittstelle können Sie CIDR-Blöcke bereitstellen, und Snowball Edge schränkt den Zugriff auf die NFS-Schnittstelle von Client-Computern mit Adressen in diesen Blöcken aus.

Dateien auf dem Gerät werden nach der Rückgabe an Amazon S3 übertragen AWS. Weitere Informationen finden Sie unter [Jobs in Amazon S3 importieren](#).

Weitere Informationen zur Verwendung von NFS mit Ihrem Computerbetriebssystem finden Sie in der Dokumentation zu Ihrem Betriebssystem.

Beachten Sie bei der Verwendung der NFS-Schnittstelle die folgenden Details.

- Die NFS-Schnittstelle stellt einen lokalen Bucket für die Datenspeicherung auf dem Gerät bereit. Bei Importaufträgen werden keine Daten aus dem lokalen Bucket in Amazon S3 importiert.

- Dateinamen sind Objektschlüssel in Ihrem lokalen S3-Bucket auf dem Snowball Edge. Der Schlüsselname ist eine Folge von Unicode-Zeichen, deren UTF-8-Kodierung maximal 1.024 Byte lang ist. Wir empfehlen, möglichst NFSv4 .1 zu verwenden und Dateinamen mit Unicode-UTF-8 zu codieren, um einen erfolgreichen Datenimport sicherzustellen. Dateinamen, die nicht mit UTF-8 codiert sind, werden je nach verwendeter NFS-Kodierung möglicherweise nicht nach S3 oder mit einem anderen Dateinamen nach S3 hochgeladen.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Snowball Edge unterstützt keine Dateipfade mit mehr als 1024 Zeichen. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateimport.
- Weitere Informationen finden Sie unter [Objektschlüssel](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Bei NFS-basierten Übertragungen werden Ihren Objekten Metadaten im POSIX-Stil hinzugefügt, wenn sie von Snowball Edge in Amazon S3 importiert werden. Darüber hinaus werden Sie die Metadaten „x-amz-meta-user-agent aws-datasync“ sehen, wie wir sie derzeit AWS DataSync als Teil des internen Importmechanismus nach Amazon S3 für den Snowball Edge-Import mit NFS-Option verwenden.
- Sie können bis zu 40 Millionen Dateien mit einem einzigen Snowball Edge-Gerät übertragen. Wenn Sie mehr als 40 Millionen Dateien in einem einzigen Auftrag übertragen müssen, stapeln Sie die Dateien, um die Anzahl der Dateien pro Übertragung zu reduzieren. Einzelne Dateien können eine beliebige Größe mit einer maximalen Dateigröße von 5 TB für Snowball Edge-Geräte mit der erweiterten NFS-Schnittstelle oder der S3-Schnittstelle haben.

Sie können die NFS-Schnittstelle auch mit AWS OpsHub einem GUI-Tool konfigurieren und verwalten. Weitere Informationen finden Sie unter [Verwaltung der NFS-Schnittstelle mithilfe von NFS](#).

NFS-Konfiguration für Snowball Edge

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snowball Edge-Gerät ausgeführt. Sie müssen sie daher starten, um die Datenübertragung zum Gerät zu ermöglichen. Sie können die NFS-Schnittstelle konfigurieren, indem Sie die IP-Adresse eines Virtual Network Interface (VNI) angeben, das auf dem Snowball Edge ausgeführt wird, und den Zugriff auf Ihre Dateifreigabe bei Bedarf einschränken. Bevor Sie die NFS-Schnittstelle konfigurieren, richten Sie eine virtuelle Netzwerkschnittstelle (VNI) auf Ihrem Snowball Edge ein. Weitere Informationen finden Sie unter [Netzwerkkonfiguration für](#) Compute-Instances.

Snowball Edge für die NFS-Schnittstelle konfigurieren

- Verwenden Sie den `describe-service` Befehl, um festzustellen, ob die NFS-Schnittstelle aktiv ist.

```
snowballEdge describe-service --service-id nfs
```

Der Befehl gibt den Status des NFS-Dienstes zurück, `ACTIVE` oder `INACTIVE`

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  }
}
```

Wenn der Wert des `State` Namens lautet `ACTIVE`, ist der NFS-Schnittstellendienst aktiv und Sie können das Snowball Edge-NFS-Volume mounten. Weitere Informationen finden Sie unter

[Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie den Endpunkt als lokalen Speicher auf den Client-Computern.](#)

[Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und MacOS-Betriebssysteme aufgeführt.](#)

- **Windows:**

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/
buckets/BucketName *
```

- **Linux:**

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsz=131072,wsz=131072,nolocks,hard,retrans=2 nfs-  
interface-ip-address:/buckets/$bucketname mount_point
```

. Wenn der Wert lautet INACTIVE, müssen Sie den Dienst starten.

Den NFS-Dienst auf dem Snowball Edge starten

Starten Sie bei Bedarf eine virtuelle Netzwerkschnittstelle (VNI) und starten Sie dann den NFS-Dienst auf dem Snowball Edge. Falls erforderlich, geben Sie beim Starten des NFS-Dienstes einen Block zulässiger Netzwerkadressen an. Wenn Sie keine Adressen angeben, ist der Zugriff auf die NFS-Endpunkte uneingeschränkt.

1. Verwenden Sie den `describe-virtual-network-interface` Befehl, um die auf Snowball Edge VNIs verfügbaren anzuzeigen.

```
snowballEdge describe-virtual-network-interfaces
```

Wenn einer oder mehrere auf Snowball Edge aktiv VNIs sind, gibt der Befehl Folgendes zurück.

```
snowballEdge describe-virtual-network-interfaces  
[  
  {  
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/  
s.ni-8EXAMPLE8EXAMPLE8",  
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",  
    "IpAddressAssignment" : "DHCP",  
    "IpAddress" : "192.0.2.0",  
    "Netmask" : "255.255.255.0",  
    "DefaultGateway" : "192.0.2.1",  
    "MacAddress" : "EX:AM:PL:E1:23:45"  
  }, {  
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/  
s.ni-1EXAMPLE1EXAMPLE1",
```

```

    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.2",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "12:34:5E:XA:MP:LE"
  }
]

```

Notieren Sie sich den Wert des `VirtualNetworkInterfaceArn` Namens des VNI, der mit der NFS-Schnittstelle verwendet werden soll.

2. Wenn keine verfügbar VNIs sind, verwenden Sie den `create-virtual-network-interface` Befehl, um ein VNI für die NFS-Schnittstelle zu erstellen. Weitere Informationen finden Sie unter [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\)](#).
3. Verwenden Sie den `start-service` Befehl, um den NFS-Dienst zu starten und ihn dem VNI zuzuordnen. Um den Zugriff auf die NFS-Schnittstelle einzuschränken, fügen Sie die `AllowedHosts` Parameter `service-configuration` und in den Befehl ein.

```

snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id
nfs --service-configuration AllowedHosts=CIDR-address-range

```

4. Verwenden Sie den `describe-service` Befehl, um den Dienststatus zu überprüfen. Es läuft, wenn der Wert des `State` Namens ist `ACTIVE`.

```

snowballEdge describe-service --service-id nfs

```

Der Befehl gibt den Dienststatus sowie die IP-Adresse und Portnummer des NFS-Endpunkts sowie die CIDR-Bereiche zurück, die für den Zugriff auf den Endpunkt zulässig sind.

```

{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  },

```



```
"Endpoints" : [ {  
  "Protocol" : "nfs",  
  "Port" : 2049,  
  "Host" : "192.0.2.0"  
} ],  
"ServiceConfiguration" : {  
  "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]  
}  
}
```

Mounten von NFS-Endpunkten auf Client-Computern

Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie den Endpunkt als lokalen Speicher auf den Client-Computern.

Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und MacOS-Betriebssysteme aufgeführt.

- Windows:

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/  
buckets/BucketName *
```

- Linux:

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsize=131072,wsize=131072,nolocks,hard,retrans=2 nfs-  
interface-ip-address:/buckets/$bucketname mount_point
```

Stoppen der NFS-Schnittstelle auf Snowball Edge

Wenn Sie mit der Übertragung von Dateien über die NFS-Schnittstelle fertig sind und bevor Sie Snowball Edge ausschalten, beenden Sie den `stop-service` NFS-Dienst mit dem Befehl.

```
snowballEdge stop-service --service-id nfs
```

Verwenden von EC2 Amazon-kompatiblen Compute-Instances auf Snowball Edge

Sie können EC2 Amazon-kompatible Compute-Instances, die auf einem Snowball Edge gehostet werden, mit den `sbe1` `sbe-g` Instance-Typen `sbe-c`, und ausführen. Der `sbe1` Instanztyp funktioniert auf Geräten mit der Option Snowball Edge Storage Optimized. Der `sbe-c` Instanztyp funktioniert auf Geräten mit der Snowball Edge-Option Compute Optimized. Eine Liste mit unterstützten Instance-Typen finden Sie unter [Kontingente für Recheninstanzen auf einem Snowball Edge-Gerät](#).

Alle drei Compute-Instance-Typen, die für die Verwendung auf Snowball Edge-Geräteoptionen unterstützt werden, gelten nur für Snowball Edge-Geräte. Wie ihre cloudbasierten Gegenstücke benötigen diese Instances Amazon Machine Images (AMIs), um gestartet zu werden. Sie wählen das AMI als Basis-Image für eine Instanz in der Cloud aus, bevor Sie Ihren Snowball Edge-Job erstellen.

Um eine Recheninstanz auf einem Snowball Edge zu verwenden, erstellen Sie einen Job, um ein Snowball Edge-Gerät zu bestellen, und geben Sie Ihre an. AMIs Sie können dies mit dem [Managementkonsole für die AWS Snow-Familie](#) AWS CLI, dem oder einem der tun. AWS SDKs In der Regel gibt es einige organisatorische Voraussetzungen, die Sie vor dem Erstellen Ihres Auftrags umsetzen müssen, um Ihre Instances nutzen zu können.

Sobald Ihr Gerät bei uns eingetroffen ist, können Sie mit der Verwaltung Ihrer AMIs und -Instanzen beginnen. Sie können Ihre Compute-Instances auf einem Snowball Edge über einen EC2 Amazon-kompatiblen Endpunkt verwalten. Dieser Endpunkttyp unterstützt viele der EC2 Amazon-kompatiblen CLI-Befehle und -Aktionen für. AWS SDKs Sie können den AWS-Managementkonsole auf dem Snowball Edge nicht verwenden, um Ihre Instanzen AMIs und Recheninstanzen zu verwalten.

Wenn Sie mit Ihrem Gerät fertig sind, geben Sie es an AWS zurück. Wenn das Gerät in einem Importauftrag verwendet wurde, werden die mit dem Amazon S3-Adapter oder der NFS-Schnittstelle übertragenen Daten in Amazon S3 importiert. Andernfalls führen wir eine vollständige Löschung des Geräts durch, wenn es zurückgegeben wird. AWS Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Important

- Die Verwendung von verschlüsselt AMIs auf Snowball Edge Edge-Geräten wird nicht unterstützt.

- Daten in Compute-Instances, die auf einem Snowball Edge ausgeführt werden, werden nicht importiert AWS.

Themen

- [Unterschied zwischen Amazon EC2 - und EC2 Amazon-kompatiblen Instances auf Snowball Edge](#)
- [Preise für Compute-Instances auf Snowball Edge](#)
- [Verwenden eines EC2 Amazon-kompatiblen AML auf Snowball Edge](#)
- [Importieren eines VM-Images auf ein Snowball Edge-Gerät](#)
- [Verwenden der AWS CLI und API-Operationen auf dem Snowball Edge-Gerät](#)
- [Netzwerkconfigurationen für Recheninstanzen auf Snowball Edge](#)
- [Verwenden von SSH zum Herstellen einer Verbindung zu Recheninstanzen auf einem Snowball Edge](#)
- [Übertragung von Daten von EC2 -kompatiblen Recheninstanzen in S3-Buckets auf demselben Snowball Edge](#)
- [Automatisches Starten von EC2 -kompatiblen Instances](#)
- [Verwenden des EC2 Amazon-kompatiblen Endpunkts auf einem Snowball Edge](#)
- [EC2Autostart-kompatible Instances mit Startvorlagen auf einem Snowball Edge](#)
- [Verwenden von Instance Metadata Service for Snow mit EC2 Amazon-kompatiblen Instances auf einem Snowball Edge](#)
- [Blockspeicher mit EC2 Amazon-kompatiblen Instances auf Snowball Edge verwenden](#)
- [Steuern des Netzwerkverkehrs mit Sicherheitsgruppen auf Snowball Edge](#)
- [Unterstützte EC2 -kompatible Instanzmetadaten und Benutzerdaten auf Snowball Edge](#)
- [Stoppen von EC2 -kompatiblen Instanzen, die auf Snowball Edge ausgeführt werden](#)

Unterschied zwischen Amazon EC2 - und EC2 Amazon-kompatiblen Instances auf Snowball Edge

AWS Snowball EC2 Edge-kompatible Instances ermöglichen es Kunden, EC2 Amazon-kompatible Instances mit einer Teilmenge von und einer Teilmenge von zu verwenden EC2 APIs und zu verwalten. AMLs

Preise für Compute-Instances auf Snowball Edge

Die Verwendung von Datenverarbeitungs-Instances verursacht zusätzliche Kosten. Weitere Informationen finden Sie unter [AWS Snowball Edge – Preise](#).

Verwenden eines EC2 Amazon-kompatiblen AMI auf Snowball Edge

Um ein Amazon Machine Image (AMI) auf Ihrem AWS Snowball Edge-Gerät zu verwenden, müssen Sie es zuerst dem Gerät hinzufügen. Sie können ein AMI auf folgende Weise hinzufügen:

- Laden Sie das AMI hoch, wenn Sie das Gerät bestellen.
- Fügen Sie das AMI hinzu, wenn Ihr Gerät an Ihrem Standort ankommt.

EC2 Amazon-Compute-Instances, die mit Ihrem Snowball Edge geliefert werden, werden basierend auf dem Amazon gestarteten EC2 AMIs, das Sie Ihrem Gerät hinzufügen. EC2 Amazon-kompatible AMIs unterstützen sowohl Linux- als auch Microsoft Windows-Betriebssysteme.

Linux

Die folgenden Linux-Betriebssysteme werden unterstützt:

- [Amazon Linux 2 für Snowball Edge](#)

Note

Die neueste Version dieses AMI wird zu dem Zeitpunkt bereitgestellt, zu dem Ihr Snowball Edge für den Versand vorbereitet wird. AWS Informationen zum Ermitteln der Version dieses AMI auf dem Gerät, wenn Sie es erhalten, finden Sie unter [Ermitteln der Version des Amazon Linux 2 AMI für Snowball Edge](#).

- [CentOS 7 \(x86_64\) - mit Updates HVM](#)
- Ubuntu 16.04 LTS - Xenial (HVM)

 Note

Ubuntu 16.04 LTS — Xenial (HVM) -Images werden in der nicht mehr unterstützt AWS Marketplace, werden aber weiterhin für die Verwendung auf Snowball Edge-Geräten über Amazon EC2 VM und die lokale Ausführung in unterstützt. Import/Export AMIs

- [Ubuntu 20.04 LTS — Focal](#)
- [Ubuntu 22.04 LTS - Jammy](#)

Als bewährte Methode zur Sicherheit sollten Sie Ihr Amazon Linux 2 AMIs up-to-date auf Snowball Edge verwenden, sobald neue Amazon Linux 2 veröffentlicht AMIs werden. Siehe [Aktualisieren Sie Ihr Amazon Linux 2 AMIs auf Snowball Edge](#).

Windows

Die folgenden Windows-Betriebssysteme werden unterstützt:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Sie können Windows AMIs zu Ihrem Gerät hinzufügen, indem Sie Ihr Windows Virtual Machine (VM) -Image AWS mithilfe von VM Import/Export importieren. Oder Sie können das Image direkt nach der Bereitstellung des Geräts auf Ihrer Site auf Ihr Gerät importieren. Weitere Informationen finden Sie unter [Hinzufügen eines Microsoft Windows-AMI zu einem Snowball Edge](#).

 Note

Windows AMIs , das ursprünglich von stammt, AWS kann Ihrem Gerät nicht hinzugefügt werden.

AMIs Lokal importierte Dateien müssen sich im BIOS-Startmodus befinden, da UEFI nicht unterstützt wird.

Snowball Edge unterstützt das Modell Bring Your Own License (BYOL). Weitere Informationen finden Sie unter [Hinzufügen eines Microsoft Windows-AMI zu einem Snowball Edge](#).

 Note

AWS Snowball EC2 Edge-kompatible Instances ermöglichen es Kunden, EC2 Amazon-kompatible Instances zu verwenden und zu verwalten, indem sie eine Teilmenge von EC2 APIs und eine Teilmenge von verwenden. AMIs

Themen

- [Hinzufügen eines AMI bei der Erstellung eines Auftrags zur Bestellung eines Snowball Edge](#)
- [Hinzufügen eines AMIs von AWS Marketplace zu einem Snowball Edge](#)
- [Hinzufügen eines AMI zu Snowball Edge nach Erhalt des Geräts](#)
- [Hinzufügen eines Microsoft Windows-AMI zu einem Snowball Edge](#)
- [Importieren eines VM-Images in einen Snowball Edge](#)
- [Exportieren des neuesten Amazon Linux 2-AMI für einen Snowball Edge](#)

Hinzufügen eines AMI bei der Erstellung eines Auftrags zur Bestellung eines Snowball Edge

Wenn Sie Ihr Gerät bestellen, können Sie es dem Gerät AMIs hinzufügen, indem Sie es im Abschnitt Compute using EC2 instances — optional unter auswählen. Managementkonsole für die AWS Snow-Familie. Unter EC2 Instanzen berechnen — optional sind alle Funktionen aufgeführt AMIs, die auf Ihr Gerät geladen werden können. Sie AMIs lassen sich in die folgenden Kategorien einteilen:

- AMIs von AWS Marketplace — Diese werden aus der Liste der unterstützten AMIs erstellt AMIs. Informationen zum Erstellen eines AMI aus dem vom AWS Marketplace unterstützten AMIs Bereich finden Sie unter [Hinzufügen eines AMIs von AWS Marketplace zu einem Snowball Edge](#).
- AMIs mit VM Import/Export hochgeladen — Wenn Sie Ihr Gerät bestellen, Import/Export werden AMIs die mit VM hochgeladenen Geräte in der Konsole aufgeführt. Weitere Informationen finden Sie unter [Importieren einer VM als Image mithilfe von VM Import/Export](#) im Import/Export VM-Benutzerhandbuch. Informationen zu unterstützten Virtualisierungsumgebungen finden Sie unter [VM Import/Export Requirements](#).

Hinzufügen eines AMIs von AWS Marketplace zu einem Snowball Edge

Sie können Ihrem Snowball Edge-Gerät viele AMIs von AWS Marketplace hinzufügen, indem Sie die AWS Marketplace Instance starten, daraus ein AMI erstellen und das AMI in derselben Region konfigurieren, aus der Sie das Snow-Gerät bestellen. Anschließend können Sie wählen, ob das AMI auf dem Gerät enthalten sein soll, wenn Sie einen Auftrag zur Bestellung des Geräts erstellen. Wenn Sie ein AMI aus dem Marketplace auswählen, stellen Sie sicher, dass es über einen unterstützten Produktcode und eine unterstützte Plattform verfügt.

Themen

- [Überprüfung der Produktcodes und Plattformdetails von AWS Marketplace AMIs Snowball Edge](#)
- [Ermitteln der Version des Amazon Linux 2 AMI für Snowball Edge](#)
- [Konfigurieren Sie das AMI für das Snowball Edge-Gerät](#)

Überprüfung der Produktcodes und Plattformdetails von AWS Marketplace AMIs Snowball Edge

Bevor Sie mit dem Hinzufügen eines AMI von AWS Marketplace zu Ihrem Snowball Edge-Gerät beginnen, stellen Sie sicher, dass der Produktcode und die Plattformdetails des AMI in Ihrem AWS-Region unterstützt werden.

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten und von der aus Sie den Auftrag zur Bestellung des Snowball Edge-Geräts erstellen. Sie können jede Region auswählen, die Ihnen zur Verfügung steht, unabhängig von Ihrem Standort.
3. Wählen Sie im Navigationsbereich AMIs aus.
4. Verwenden Sie die Filter- und Suchoptionen, um die angezeigte Liste so einzuschränken AMIs , AMIs dass nur diejenigen angezeigt werden, die Ihren Kriterien entsprechen. Wählen Sie beispielsweise Öffentliche Bilder aus AWS Marketplace, die von AMIs bereitgestellt werden. Verwenden Sie dann die Suchoptionen, um die Liste der angezeigten Objekte weiter einzugrenzen AMIs:
 - (Neue Konsole) Wählen Sie in der Suchleiste aus dem Menü die Option Owner-Alias, dann den Operator = und anschließend den Wert amazon aus.
 - (Alte Konsole) Wählen Sie die Search bar (Suchleiste) aus und anschließend im Menü den Punkt Owner (Besitzer). Wählen Sie dann den Wert Amazon Images (Amazon-Images) aus.

 Note

AMIs wählen Sie in der Spalte Quelle die Option aws-marketplace mit AWS Marketplace einschließen.

5. Wählen Sie in der Spalte AMI-ID die AMI-ID des AMI aus.
6. Stellen Sie in der Bildübersicht des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der Tabelle unten.

Unterstützte AWS Marketplace AMI-Produktcodes

AMI-Betriebssystem	Produktcode
Ubuntu Server 14.04 LTS	b3dl4415quatdndl4qa6kcu45
CentOS 7 (x86_64)	aw0evgkw8e5c1q413zgy5pjce
Ubuntu 16.04 LTS	csv6h7oyg29b7epjzg7qdr7no
Amazon Linux 2	avyfzznywektml5qv5f57ska
Ubuntu 20.04 LTS	a8jyyfn4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkkjt189a13aqe

7. Stellen Sie anschließend sicher, dass die Plattformdetails einen der Einträge aus der folgenden Liste enthalten.
 - Amazon Linux, Ubuntu oder Debian
 - Red Hat Linux bring-your-own-license
 - Amazon RDS for Oracle bring-your-own-license
 - Windows bring-your-own-license

Ermitteln der Version des Amazon Linux 2 AMI für Snowball Edge

Gehen Sie wie folgt vor, um die Version des Amazon Linux 2-AMI für Snowball Edge auf dem Snowball Edge zu ermitteln. Installieren Sie die neueste Version von, AWS CLI bevor Sie fortfahren.

Weitere Informationen finden Sie im [AWS Command Line Interface Benutzerhandbuch unter Installation oder Aktualisierung AWS CLI auf die neueste Version von](#).

- Verwenden Sie den `describe-images` AWS CLI Befehl, um die Beschreibung des AMI anzuzeigen. Die Version ist in der Beschreibung enthalten. Stellen Sie das Public-Key-Zertifikat aus dem vorherigen Schritt bereit. Weitere Informationen finden Sie unter [describe-images](#) in der AWS CLI Befehlsreferenz.

```
aws ec2 describe-images --endpoint http://snow-device-ip:8008 --region snow
```

Example der Ausgabe des Befehls **describe-images**

```
{
  "Images": [
    {
      "CreationDate": "2024-02-12T23:24:45.705Z",
      "ImageId": "s.ami-02ba84cb87224e16e",
      "Public": false,
      "ProductCodes": [
        {
          "ProductCodeId": "avyfzznywektkgl5qv5f57ska",
          "ProductCodeType": "marketplace"
        }
      ],
      "State": "AVAILABLE",
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/xvda",
          "Ebs": {
            "DeleteOnTermination": true,
            "Iops": 0,
            "SnapshotId": "s.snap-0efb49f2f726fde63",
            "VolumeSize": 8,
            "VolumeType": "sbp1"
          }
        }
      ],
    }
  ],
}
```

```
    "Description": "Snow Family Amazon Linux 2 AMI 2.0.20240131.0 x86_64  
    HVM gp2",  
    "EnaSupport": false,  
    "Name": "amzn2-ami-snow-family-hvm-2.0.20240131.0-x86_64-gp2-  
    b7e7f8d2-1b9e-4774-a374-120e0cd85d5a",  
    "RootDeviceName": "/dev/xvda"  
  }  
]  
}
```

In diesem Beispiel ist die Version des Amazon Linux 2-AMI für Snowball Edge.
2.0.20240131.0 Sie ist im Wert des Description Namens enthalten.

Konfigurieren Sie das AMI für das Snowball Edge-Gerät

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Starten Sie eine neue Instanz eines unterstützten AMI in AWS Marketplace.

Note

Wenn Sie Ihre Instance starten, stellen Sie sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihren Anwendungsfall geeignet ist. In der EC2 Amazon-Konsole tun Sie dies im Schritt Speicher hinzufügen.

3. Installieren und konfigurieren Sie die Anwendungen, die Sie auf Snowball Edge ausführen möchten, und stellen Sie sicher, dass sie erwartungsgemäß funktionieren.

Important

- Es AMIs werden nur einzelne Volumes unterstützt.
- Das EBS-Volume in Ihrem AMI sollte 10 TB oder weniger betragen. Wir empfehlen, dass Sie die EBS-Volumegröße bereitstellen, die für die Daten im AMI erforderlich ist. Dies wird dazu beitragen, die Zeit zu verkürzen, die zum Exportieren Ihres AMI und zum Laden auf Ihr Gerät benötigt wird. Sie können die Größe Ihrer Instance ändern oder weitere Volumes hinzufügen, nachdem Ihr Gerät bereitgestellt wurde.
- Der EBS-Snapshot in Ihrem AMI darf nicht verschlüsselt sein.

4. Erstellen Sie eine Kopie der PEM- oder PPK-Datei, die Sie für das SSH-Schlüsselpaar verwendet haben, als Sie diese Instanz erstellt haben. Speichern Sie diese Datei auf dem Server, den Sie für die Kommunikation mit dem Snowball Edge-Gerät verwenden möchten. Notieren Sie sich den Pfad zu dieser Datei, da Sie ihn benötigen, wenn Sie SSH verwenden, um eine Verbindung mit der EC2 -kompatiblen Instanz auf Ihrem Gerät herzustellen.

 Important

Wenn Sie dieses Verfahren nicht befolgen, können Sie mit SSH keine Verbindung zu Ihren Instances herstellen, wenn Sie Ihr Snowball Edge-Gerät erhalten.

5. Speichern Sie die Instance als AMI. Weitere Informationen finden Sie im [EC2 Amazon-Benutzerhandbuch für Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch.
6. Wiederholen Sie die Schritte 1—4 für jede Instance, zu der Sie über SSH eine Verbindung herstellen möchten. Stellen Sie sicher, dass Sie Kopien der einzelnen SSH-Schlüsselpaare erstellen und verfolgen Sie, mit welchen Schlüsselpaaren sie AMIs verknüpft sind.
7. Wenn Sie Ihr Gerät jetzt bestellen, können AMIs Sie diese Ihrem Gerät hinzufügen.

Hinzufügen eines AMI zu Snowball Edge nach Erhalt des Geräts

Wenn das Gerät auf Ihrer Site ankommt, können Sie ihm neue AMIs hinzufügen. Detaillierte Anweisungen finden Sie unter [Importieren eines VM-Images auf ein Snowball Edge-Gerät](#). Beachten Sie, dass zwar alle unterstützt VMs werden, aber nur die unterstützten AMIs Produkte auf ihre volle Funktionalität getestet wurden.

 Note

Wenn Sie VM verwenden Import/Export , AMIs um Ihrem Gerät eine VM hinzuzufügen oder eine VM zu importieren, nachdem Ihr Gerät bereitgestellt wurde, können Sie VMs diese unter Verwendung eines beliebigen Betriebssystems hinzufügen. Auf Snowball Edge wurden jedoch nur unterstützte Betriebssysteme getestet und validiert. Sie sind dafür verantwortlich, die Nutzungsbedingungen aller Betriebssysteme oder Software einzuhalten, die sich in dem virtuellen Image befinden, das Sie auf Ihr Gerät importieren.

 Important

Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter [Portanforderungen für AWS Dienste auf einem Snowball Edge](#).

Hinzufügen eines Microsoft Windows-AMI zu einem Snowball Edge

Für virtuelle Maschinen (VMs), die ein unterstütztes Windows-Betriebssystem verwenden, können Sie das AMI hinzufügen, indem Sie Ihr Windows-VM-Image AWS mithilfe von VM Import/Export importieren oder indem Sie es direkt nach der Bereitstellung auf Ihrer Site in Ihr Gerät importieren.

Bring Your Own License (BYOL)

Snowball Edge unterstützt den Import von Microsoft Windows AMIs auf Ihr Gerät mit Ihrer eigenen Lizenz. Bring Your Own License (BYOL) ist der Prozess, bei dem ein AMI, das Sie besitzen, mit seiner lokalen Lizenz installiert wird. AWS bietet sowohl gemeinsame als auch dedizierte Bereitstellungsoptionen für die BYOL-Option.

Sie können Ihr Windows-VM-Image zu Ihrem Gerät hinzufügen, indem Sie es in AWS eine virtuelle Maschine importieren Import/Export oder indem Sie es direkt nach der Bereitstellung auf Ihrer Site in Ihr Gerät importieren. Sie können kein Windows hinzufügen AMIs , das seinen Ursprung in hat AWS. Daher müssen Sie Ihr eigenes Windows-VM-Image erstellen und importieren und Ihre eigene Lizenz mitbringen, wenn Sie das AMI auf Ihrem Snowball Edge-Gerät verwenden möchten. Weitere Informationen zur Windows-Lizenzierung und BYOL finden Sie unter [Amazon Web Services und Microsoft: Häufig gestellte Fragen](#).

Erstellen eines Windows-VM-Images für den Import in einen Snowball Edge

Um ein Windows-VM-Image zu erstellen, benötigen Sie beispielsweise eine Virtualisierungsumgebung VirtualBox, die für die Betriebssysteme Windows und macOS unterstützt wird. Wenn Sie eine VM für Snow-Geräte erstellen, empfehlen wir, dass Sie mindestens zwei Kerne mit mindestens 4 GB RAM zuweisen. Wenn die VM betriebsbereit ist, müssen Sie Ihr Betriebssystem installieren (Windows Server 2012, 2016 oder 2019). Folgen Sie den Anweisungen in diesem Abschnitt, um die erforderlichen Treiber für das Snowball Edge-Gerät zu installieren.

Damit ein Windows-AMI auf einem Snow-Gerät ausgeführt werden kann, müssen Sie VirtIO, FLR, NetVCM, Vioinput, Viorng, Vioscsi, Vioserial und Treiber hinzufügen. VioStor Sie können [einen Microsoft Software Installer \(virtio-win-guest-tools-installer\) für die Installation dieser Treiber auf Windows-Images aus dem virtio-win-pkg-scripts Repository unter herunterladen](#). GitHub

 Note

Wenn Sie Ihr VM-Image direkt auf Ihr bereitgestelltes Snow-Gerät importieren möchten, muss die VM-Imagedatei im RAW-Format vorliegen.

Um ein Windows-Image zu erstellen

1. Wählen Sie auf Ihrem Microsoft Windows-Computer Start und Enter, **devmgmt.msc** um den Geräte-Manager zu öffnen.
2. Wählen Sie im Hauptmenü Aktionen und anschließend Legacy-Hardware hinzufügen aus.

 Note

Wählen Sie für Windows 11 zunächst ein beliebiges Gerät im unteren Bereich aus, bevor die Option Legacy-Hardware hinzufügen im Aktionsmenü angezeigt wird.

3. Wählen Sie im Assistenten „Weiter“.
4. Wählen Sie Hardware installieren, die ich manuell aus einer Liste ausgewählt habe (erweitert), und klicken Sie auf Weiter.
5. Wählen Sie „Alle Geräte anzeigen“ und dann „Weiter“.
6. Wählen Sie „Festplatte haben“, öffnen Sie die Liste „Herstellerdateien aus kopieren“ und suchen Sie nach der ISO-Datei.
7. Suchen Sie in der ISO-Datei nach dem `Driver\W2K8R2\amd64` Verzeichnis und suchen Sie dann nach der `.INF` Datei.
8. Wählen Sie die INF-Datei aus, klicken Sie auf Öffnen und anschließend auf OK.
9. Wenn der Treibername angezeigt wird, wählen Sie Weiter und dann noch zweimal Weiter. Klicken Sie auf Finish (Fertig stellen).

Dadurch wird ein Gerät installiert, das den neuen Treiber verwendet. Die tatsächliche Hardware ist nicht vorhanden, daher wird ein gelbes Ausrufezeichen angezeigt, das auf ein Problem mit dem Gerät hinweist. Sie müssen dieses Problem beheben.

Um das Hardwareproblem zu beheben

1. Öffnen Sie das Kontextmenü (Rechtsklick) für das Gerät mit dem Ausrufezeichen.
2. Wählen Sie Deinstallieren, deaktivieren Sie die Option Treibersoftware für dieses Gerät löschen und wählen Sie OK.

Der Treiber ist installiert und Sie sind bereit, das AMI auf Ihrem Gerät zu starten.

Importieren eines VM-Images in einen Snowball Edge

Nachdem Sie Ihr VM-Image vorbereitet haben, können Sie eine der Optionen verwenden, um das Image auf Ihr Gerät zu importieren.

- In der Cloud mithilfe von VM Import/Export — Wenn Sie Ihr VM-Image in ein AMI importieren AWS und es als AMI registrieren, können Sie es Ihrem Gerät hinzufügen, wenn Sie eine Bestellung bei der aufgeben. Managementkonsole für die AWS Snow-Familie Weitere Informationen finden Sie unter [Importieren einer VM als Image mithilfe von VM Import/Export](#) im Import/Export VM-Benutzerhandbuch.
- Lokal auf Ihrem Gerät, das an Ihrem Standort bereitgestellt wird — Sie können Ihr VM-Image mit AWS OpsHub oder AWS Command Line Interface (AWS CLI) direkt in Ihr Gerät importieren.

Informationen zur Verwendung finden Sie unter AWS OpsHub [Lokales Verwenden von EC2 Amazon-kompatiblen Compute-Instances](#).

Informationen zur Verwendung von finden Sie AWS CLI unter [Importieren eines VM-Images auf ein Snowball Edge-Gerät](#).

Exportieren des neuesten Amazon Linux 2-AMI für einen Snowball Edge

Um Ihr Amazon Linux 2 AMIs auf die neueste Version zu aktualisieren, exportieren Sie zuerst das neueste Amazon Linux 2-VM-Image von AWS Marketplace und importieren Sie dieses VM-Image dann in das Snow-Gerät.

1. Verwenden Sie den `ssm get-parameters` AWS CLI Befehl, um die neueste Image-ID des Amazon Linux 2-AMI in der zu finden AWS Marketplace.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Der Befehl gibt die neueste Image-ID des AMI zurück. Beispiel, `ami-0ccb473bada910e74`.

2. Exportieren Sie das neueste Amazon Linux 2-Image. Weitere Informationen finden Sie unter [Exportieren einer VM direkt aus einem Amazon Machine Image \(AMI\)](#) im EC2 Amazon-Benutzerhandbuch. Verwenden Sie die neueste Image-ID des Amazon Linux 2-AMI als Wert für den `image-id` Parameter des `ec2 export-image` Befehls.
3. Importieren Sie das VM-Image mit dem AWS CLI oder in das Snow-Gerät AWS OpsHub.
 - Informationen zur Verwendung von AWS CLI finden Sie unter [Importieren eines VM-Images auf ein Snowball Edge-Gerät](#).
 - Informationen zur Verwendung von AWS OpsHub finden Sie unter [Import eines Images als EC2 Amazon-kompatibles AMI mit AWS OpsHub](#).

Importieren eines VM-Images auf ein Snowball Edge-Gerät

Sie können den AWS CLI und den Import/Export VM-Dienst verwenden, um ein Image einer virtuellen Maschine (VM) als Amazon Machine Image (AMI) auf das Snowball Edge-Gerät zu importieren. Nachdem Sie ein VM-Image importiert haben, registrieren Sie das Image als AMI und starten Sie es als Amazon EC2 -kompatible Instance.

Sie können dem Gerät AMIs etwas von Amazon EC2 hinzufügen, wenn Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen. Gehen Sie wie folgt vor, nachdem Sie das Snowball Edge-Gerät erhalten haben. Weitere Informationen finden Sie unter [Wählen Sie Ihre Rechen- und Speicheroptionen](#).

Sie können es auch verwenden AWS OpsHub , um die VM-Imagedatei hochzuladen. Weitere Informationen finden Sie [in diesem Handbuch unter Importieren eines Images auf Ihr Gerät als EC2 Amazon-kompatibles AMI](#).

Themen

- [Schritt 1: Bereiten Sie das VM-Image vor und laden Sie es auf das Snowball Edge-Gerät hoch](#)
- [Schritt 2: Richten Sie die erforderlichen Berechtigungen auf dem Snowball Edge ein](#)
- [Schritt 3: Importieren Sie das VM-Image als Snapshot auf Snowball Edge](#)
- [Schritt 4: Registrieren Sie den Snapshot als AMI auf dem Snowball Edge](#)

- [Schritt 5: Starten Sie eine Instance über das AMI auf dem Snowball Edge](#)
- [Zusätzliche AMI-Aktionen für einen Snowball Edge](#)

Schritt 1: Bereiten Sie das VM-Image vor und laden Sie es auf das Snowball Edge-Gerät hoch

Bereiten Sie das VM-Image vor, indem Sie ein VM-Image aus einem EC2 Amazon-AMI oder einer Instance in der AWS Cloud benutzenden VM exportieren Import/Export oder indem Sie das VM-Image lokal mit der Virtualisierungsplattform Ihrer Wahl generieren.

Informationen zum Exportieren einer EC2 Amazon-Instance als VM-Image mithilfe von VM Import/Export finden Sie unter [Exportieren einer Instanz als VM mithilfe von VM Import/Export](#) im VM-Benutzerhandbuch. Import/Export Informationen zum Exportieren eines Amazon EC2 AMI als VM-Image mithilfe von VM Import/Export finden Sie unter [Exportieren einer VM direkt aus einem Amazon Machine Image \(AMI\)](#) im Import/Export VM-Benutzerhandbuch.

Wenn Sie ein VM-Image aus Ihrer lokalen Umgebung generieren, stellen Sie sicher, dass das Image für die Verwendung als AMI auf dem Snowball Edge-Gerät konfiguriert ist. Abhängig von Ihrer Umgebung müssen Sie möglicherweise die folgenden Elemente konfigurieren.

- Konfigurieren und aktualisieren Sie das Betriebssystem.
- Legen Sie einen Hostnamen fest.
- Stellen Sie sicher, dass das Network Time Protocol (NTP) konfiguriert ist.
- Fügen Sie, falls erforderlich, öffentliche SSH-Schlüssel hinzu. Erstellen Sie lokale Kopien der Schlüsselpaare. Weitere Informationen finden Sie unter [SSH verwenden, um eine Connect zu Ihren Compute-Instances auf einem Snowball Edge](#) herzustellen.
- Installieren und konfigurieren Sie jegliche Software, die Sie auf dem Snowball Edge-Gerät verwenden möchten.

Note

Beachten Sie die folgenden Einschränkungen, wenn Sie einen Festplatten-Snapshot für ein Snowball Edge-Gerät vorbereiten.

- Snowball Edge unterstützt derzeit nur den Import von Schnappschüssen im RAW-Bildformat.

- Snowball Edge unterstützt derzeit nur den Import von Snapshots mit Größen von 1 GB bis 1 TB.

Hochladen eines VM-Images in einen Amazon S3 S3-Bucket auf dem Snowball Edge-Gerät

Nachdem Sie ein VM-Image vorbereitet haben, laden Sie es in einen S3-Bucket auf dem Snowball Edge-Gerät oder -Cluster hoch. Sie können den S3-Adapter oder Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden, um den Snapshot hochzuladen.

Um das Image der virtuellen Maschine mit dem S3-Adapter hochzuladen

- Verwenden Sie den `cp` Befehl, um die VM-Image-Datei in einen Bucket auf dem Gerät zu kopieren.

```
aws s3 cp image-path s3://S3-bucket-name --endpoint http://S3-object-API-endpoint:443 --profile profile-name
```

Weitere Informationen finden Sie unter [Unterstützte AWS CLI Befehle](#) in diesem Handbuch.

Um das VM-Image mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge hochzuladen

- Verwenden Sie den `put-object` Befehl, um die Snapshot-Datei in einen Bucket auf dem Gerät zu kopieren.

```
aws s3api put-object --bucket bucket-name --key path-to-snapshot-file --body snapshot-file --endpoint-url s3api-endpoint-ip --profile your-profile
```

Weitere Informationen finden Sie unter [Arbeiten mit S3-Objekten auf einem Snowball Edge-Gerät](#).

Schritt 2: Richten Sie die erforderlichen Berechtigungen auf dem Snowball Edge ein

Damit der Import erfolgreich ist, müssen Sie Berechtigungen für VM Import/Export auf dem Snowball Edge-Gerät EC2, Amazon und dem Benutzer einrichten.

Note

Die Servicerollen und Richtlinien, die diese Berechtigungen bereitstellen, befinden sich auf dem Snowball Edge-Gerät.

Erforderliche Berechtigungen für VM Import/Export auf einem Snowball Edge

Bevor Sie den Importvorgang starten können, müssen Sie eine IAM-Rolle mit einer Vertrauensrichtlinie erstellen, die es einer VM Import/Export auf dem Snowball Edge-Gerät ermöglicht, die Rolle zu übernehmen. Der Rolle werden zusätzliche Berechtigungen erteilt, damit virtuelle Maschinen Import/Export auf dem Gerät auf das Bild zugreifen können, das im S3-Bucket auf dem Gerät gespeichert ist.

Erstellen Sie eine JSON-Datei für Vertrauensrichtlinien

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie, die an die Rolle angehängt werden muss, damit die VM auf den Snapshot zugreifen Import/Export kann, der aus dem S3-Bucket importiert werden muss.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vmie.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

}

Erstellen Sie eine Rolle mit der JSON-Datei für die Vertrauensrichtlinie

Der Rollename kann vmimport lauten. Sie können ihn ändern, indem Sie die Option `--role-name` im Befehl verwenden:

```
aws iam create-role --role-name role-name --assume-role-policy-document file:///trust-policy-json-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls. `create-role`

```
{
  "Role":{
    "AssumeRolePolicyDocument":{
      "Version":"2012-10-17",
      "Statement":[
        {
          "Action":"sts:AssumeRole",
          "Effect":"Allow",
          "Principal":{
            "Service":"vmie.amazonaws.com"
          }
        }
      ]
    },
    "MaxSessionDuration":3600,
    "RoleId":"AROACEMGEZDGNBVG3TQ0JQGEZAAAABQBB6NSGNAAAABPSVLTREPY3FPAFOLKJ3",
    "CreateDate":"2022-04-19T22:17:19.823Z",
    "RoleName":"vmimport",
    "Path":"/",
    "Arn":"arn:aws:iam::123456789012:role/vmimport"
  }
}
```

Erstellen Sie eine Richtlinie für die Rolle

Die folgende Beispielrichtlinie enthält die erforderlichen Mindestberechtigungen für den Zugriff auf Amazon S3. Ändern Sie den Namen des Amazon S3 S3-Buckets in den Namen, der Ihre Bilder enthält. Wechseln Sie bei einem eigenständigen Snowball Edge-Gerät *snow-id* zu Ihrer Job-ID.

Wechseln Sie für einen Gerätecluster *snow-id* zur Cluster-ID. Sie können auch Präfixe verwenden, um den Ort, von dem virtuelle Maschinen Snapshots importieren Import/Export können, weiter einzugrenzen. Erstellen Sie eine Richtlinien-JSON-Datei wie diese.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetMetadata"
      ],
      "Resource": [
        "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-bucket-name",
        "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-bucket-name/*"
      ]
    }
  ]
}
```

Erstellen Sie eine Richtlinie mit der Richtliniendatei:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Im Folgenden finden Sie ein Ausgabebeispiel für den Befehl create-policy.

```
{
  "Policy": {
    "PolicyName": "vmimport-resource-policy",
    "PolicyId": "ANPACEMGEZDGNBVG3YTQ0JQGEZAAAAB00EE3IIHAAAABWZJPI2VW4UUTFEDBC2R",
    "Arn": "arn:aws:iam::123456789012:policy/vmimport-resource-policy",
  }
}
```

```
"Path":"/",
"DefaultVersionId":"v1",
"AttachmentCount":0,
"IsAttachable":true,
"CreateDate":"2020-07-25T23:27:35.690000+00:00",
"UpdateDate":"2020-07-25T23:27:35.690000+00:00"
}
}
```

Hängen Sie die Richtlinie an die Rolle an

Fügen Sie der vorherigen Rolle eine Richtlinie hinzu und gewähren Sie Berechtigungen für den Zugriff auf die erforderlichen Ressourcen. Dadurch kann der lokale Import/Export VM-Dienst den Snapshot von Amazon S3 auf das Gerät herunterladen.

```
aws iam attach-role-policy --role-name role-name --policy-arn
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --
region snow --profile profile-name
```

Berechtigungen, die der Anrufer auf einem Snowball Edge benötigt

Zusätzlich zu der Rolle, die die Snowball Edge-VM Import/Export übernehmen muss, müssen Sie auch sicherstellen, dass der Benutzer über die Berechtigungen verfügt, die es ihm ermöglichen, die Rolle an VMIE zu übergeben. Wenn Sie den Standard-Root-Benutzer für den Import verwenden, verfügt der Root-Benutzer bereits über alle erforderlichen Berechtigungen. Sie können diesen Schritt also überspringen und mit Schritt 3 fortfahren.

Ordnen Sie dem Benutzer, der den Import durchführt, die folgenden beiden IAM-Berechtigungen zu.

- `pass-role`
- `get-role`

Erstellen Sie eine Richtlinie für die Rolle

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, mit der ein Benutzer die `pass-role` Aktionen `get-role` und für die IAM-Rolle ausführen kann.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "iam:GetRole",
        "Resource": "*"
      },
      {
        "Sid": "iamPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/snowball*",
        "Condition": {
          "StringEquals": {
            "iam:PassedToService": "importexport.amazonaws.com"
          }
        }
      }
    ]
  }
}

```

Erstellen Sie eine Richtlinie mit der Richtliniendatei:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Im Folgenden finden Sie ein Ausgabebeispiel für den Befehl create-policy.

```

{
  "Policy": {
    "PolicyName": "caller-policy",
    "PolicyId": "ANPACEMGEZDGNBVG3TQ0JQGEZAAAAB000TU0E3AAAAAAPPBEUM7Q7ARPUE53C6R",
    "Arn": "arn:aws:iam::123456789012:policy/caller-policy",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "CreateDate": "2020-07-30T00:58:25.309000+00:00",
    "UpdateDate": "2020-07-30T00:58:25.309000+00:00"
  }
}

```

Nachdem die Richtlinie generiert wurde, hängen Sie die Richtlinie an die IAM-Benutzer an, die die EC2 Amazon-API- oder CLI-Operation aufrufen, um den Snapshot zu importieren.

```
aws iam attach-user-policy --user-name your-user-name --policy-arn
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --
region snow --profile profile-name
```

Erforderliche Berechtigungen, um Amazon EC2 APIs auf einem Snowball Edge aufzurufen

Um einen Snapshot zu importieren, muss der IAM-Benutzer über die `ec2:ImportSnapshot` entsprechenden Berechtigungen verfügen. Wenn eine Beschränkung des Zugriffs auf den Benutzer nicht erforderlich ist, können Sie die `ec2:*` Berechtigungen verwenden, um Amazon vollen EC2 Zugriff zu gewähren. Im Folgenden sind die Berechtigungen aufgeführt, die Amazon EC2 auf Ihrem Gerät gewährt oder eingeschränkt werden können. Erstellen Sie eine Richtliniendatei mit dem angezeigten Inhalt:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:CancelImportTask",
        "ec2:DescribeSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:RegisterImage",
        "ec2:DescribeImages",
        "ec2:DeregisterImage"
      ],
      "Resource": "*"
    }
  ]
}
```


Erstellen Sie eine Richtlinie mit der Richtliniendatei:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Im Folgenden finden Sie ein Ausgabebeispiel für den Befehl create-policy.

```
{  
  "Policy":  
    {  
      "PolicyName": "ec2-import.json",  
      "PolicyId":  
        "ANPACEMGEZDGNBVGY3TQ0JQGEZAAAABQBGPDQC5AAAAATYN62UNBFYTF5WVCSCZS",  
      "Arn": "arn:aws:iam::123456789012:policy/ec2-import.json",  
      "Path": "/",  
      "DefaultVersionId": "v1",  
      "AttachmentCount": 0,  
      "IsAttachable": true,  
      "CreateDate": "2022-04-21T16:25:53.504000+00:00",  
      "UpdateDate": "2022-04-21T16:25:53.504000+00:00"  
    }  
}
```

Nachdem die Richtlinie generiert wurde, hängen Sie die Richtlinie an die IAM-Benutzer an, die die EC2 Amazon-API- oder CLI-Operation aufrufen, um den Snapshot zu importieren.

```
aws iam attach-user-policy --user-name your-user-name --policy-arn  
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --  
region snow --profile profile-name
```

Schritt 3: Importieren Sie das VM-Image als Snapshot auf Snowball Edge

Der nächste Schritt besteht darin, das VM-Image als Snapshot auf das Gerät zu importieren. Der Wert des S3Bucket Parameters ist der Name des Buckets, der das VM-Image enthält. Der Wert des S3Key Parameters ist der Pfad zur VM-Image-Datei in diesem Bucket.

```
aws ec2 import-snapshot --disk-container "Format=RAW,UserBucket={S3Bucket=bucket-  
name,S3Key=image-file}" --endpoint http://snowball-ip:8008 --region snow --  
profile profile-name
```

Weitere Informationen finden Sie unter [import-snapshot](#) in der AWS CLI Befehlsreferenz.

Dieser Befehl unterstützt die folgenden Optionen nicht.

- [--client-datavalue]
- [--client-token] value
- [--Trockenlauf]
- [--no-dry-run]
- [--verschlüsselt]
- [--no-verschlüsselt]
- [--kms-key-id value]
- [--tag-spezifikationen] value

Example Ausgabe des Befehls **import-snapshot**

```
{
  "ImportTaskId": "s.import-snap-1234567890abc",
  "SnapshotTaskDetail": {
    "DiskImageSize": 2.0,
    "Encrypted": false,
    "Format": "RAW",
    "Progress": "3",
    "Status": "active",
    "StatusMessage": "pending",
    "UserBucket": {
      "S3Bucket": "bucket",
      "S3Key": "vmimport/image01"
    }
  }
}
```

Note

Snowball Edge erlaubt derzeit nur die Ausführung eines aktiven Importauftrags gleichzeitig pro Gerät. Um eine neue Importaufgabe zu starten, warten Sie entweder, bis die aktuelle Aufgabe abgeschlossen ist, oder wählen Sie einen anderen verfügbaren Knoten in einem Cluster aus. Sie können den aktuellen Import auch abbrechen, wenn Sie möchten. Um

Verzögerungen zu vermeiden, starten Sie das Snowball Edge-Gerät nicht neu, während der Import läuft. Wenn Sie das Gerät neu starten, schlägt der Import fehl und der Fortschritt wird gelöscht, sobald auf das Gerät zugegriffen werden kann. Verwenden Sie den folgenden Befehl, um den Status Ihrer Snapshot-Importaufgabe zu überprüfen:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --endpoint
http://snowball-ip:8008 --region snow --profile profile-name
```

Schritt 4: Registrieren Sie den Snapshot als AMI auf dem Snowball Edge

Wenn der Snapshot-Import auf das Gerät erfolgreich ist, können Sie ihn mit dem `register-image` Befehl registrieren.

Note

Sie können ein AMI nur registrieren, wenn alle zugehörigen Snapshots verfügbar sind.

Weitere Informationen finden Sie unter [register-image](#) in der AWS CLI Befehlsreferenz.

Example des Befehls **register-image**

```
aws ec2 register-image \
--name ami-01 \
--description my-ami-01 \
--block-device-mappings "[{\"DeviceName\": \"/dev/sda1\", \"Ebs\": {\"Encrypted\": false,
\"DeleteOnTermination\": true, \"SnapshotId\": \"snapshot-id\", \"VolumeSize\": 30}}]" \
--root-device-name /dev/sda1 \
--endpoint http://snowball-ip:8008 \
--region snow \
--profile profile-name
```

Im Folgenden finden Sie ein Beispiel für die Blockgerätezuweisung im JSON-Format. Weitere Informationen finden Sie unter dem [block-device-mapping Parameter von register-image](#) in der AWS CLI Befehlsreferenz.

```
[
  {
```

```

    "DeviceName": "/dev/sda",
    "Ebs": {
        "Encrypted": false,
        "DeleteOnTermination": true,
        "SnapshotId": "snapshot-id",
        "VolumeSize": 30
    }
}
]

```

Example des Befehls **register-image**

```

{
  "ImageId": "s.ami-8de47d2e397937318"
}

```

Schritt 5: Starten Sie eine Instance über das AMI auf dem Snowball Edge

Informationen zum Starten einer Instance finden Sie unter [run-instances](#) in der AWS CLI Befehlsreferenz.

Der Wert des `image-id` Parameters entspricht dem Wert des ImageId Namens als Ausgabe des `register-image` Befehls.

```

aws ec2 run-instances --image-id image-id --instance-type instance-type --endpoint
http://snowball-ip:8008 --region snow --profile profile-name

```

```

{
  "Instances": [
    {
      "SourceDestCheck": false,
      "CpuOptions": {
        "CoreCount": 1,
        "ThreadsPerCore": 2
      },
      "InstanceId": "s.i-12345a73123456d1",
      "EnaSupport": false,
      "ImageId": "s.ami-1234567890abcdefg",
      "State": {
        "Code": 0,

```

```
        "Name": "pending"
    },
    "EbsOptimized": false,
    "SecurityGroups": [
        {
            "GroupName": "default",
            "GroupId": "s.sg-1234567890abc"
        }
    ],
    "RootDeviceName": "/dev/sda1",
    "AmiLaunchIndex": 0,
    "InstanceType": "sbe-c.large"
}
],
"ReservationId": "s.r-1234567890abc"
}
```

Note

Sie können es auch verwenden AWS OpsHub , um die Instance zu starten. Weitere Informationen finden Sie unter [Starten einer EC2 Amazon-kompatiblen Instance](#) in diesem Handbuch.

Zusätzliche AMI-Aktionen für einen Snowball Edge

Sie können zusätzliche AWS CLI Befehle verwenden, um den Status des Snapshot-Imports zu überwachen, Details zu importierten Snapshots abzurufen, den Import eines Snapshots abubrechen und Snapshots nach dem Import zu löschen oder deren Registrierung aufzuheben.

Überwachen des Snapshot-Importstatus auf einem Snowball Edge

Um den aktuellen Status des Importvorgangs zu sehen, können Sie den EC2 `describe-import-snapshot-tasks` Amazon-Befehl ausführen. Dieser Befehl unterstützt Paginierung und Filterung auf dem `task-state`.

Example des Befehls **describe-import-snapshot-tasks**

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Example der **describe-import-snapshot-tasks** Befehlsausgabe

```
{
  "ImportSnapshotTasks": [
    {
      "ImportTaskId": "s.import-snap-8f6bfd7fc9ead9aca",
      "SnapshotTaskDetail": {
        "Description": "Created by AWS-Snowball-VMImport service for
s.import-snap-8f6bfd7fc9ead9aca",
        "DiskImageSize": 8.0,
        "Encrypted": false,
        "Format": "RAW",
        "Progress": "3",
        "SnapshotId": "s.snap-848a22d7518ad442b",
        "Status": "active",
        "StatusMessage": "pending",
        "UserBucket": {
          "S3Bucket": "bucket1",
          "S3Key": "image1"
        }
      }
    }
  ]
}
```

Note

Dieser Befehl zeigt nur Ausgaben für Aufgaben an, die innerhalb der letzten 7 Tage erfolgreich abgeschlossen oder als gelöscht markiert wurden. Die Filterung unterstützt nur `nurName=task-state, Values=active | deleting | deleted | completed`

Dieser Befehl unterstützt die folgenden Parameter nicht.

- `--dry-run`
- `--no-dry-run`

Abbrechen einer Importaufgabe auf einem Snowball Edge

Um eine Importaufgabe abzuberechnen, führen Sie den `cancel-import-task` Befehl aus.

Example des **cancel-import-task** Befehls

```
aws ec2 cancel-import-task --import-task-id import-task-id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Example der **cancel-import-task** Befehlsausgabe

```
{
  "ImportTaskId": "s.import-snap-8234ef2a01cc3b0c6",
  "PreviousState": "active",
  "State": "deleting"
}
```

Note

Nur Aufgaben, die sich nicht in einem abgeschlossenen Zustand befinden, können storniert werden.

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Beschreibung von Schnapsschüssen auf einem Snowball Edge

Nachdem ein Snapshot importiert wurde, können Sie ihn mit diesem Befehl beschreiben. Um die Snapshots zu filtern, können Sie sie `snapshot-ids` mit der Snapshot-ID aus der vorherigen Antwort auf die Importaufgabe übergeben. Dieser Befehl unterstützt Seitennummerierung und Filterung nach `volume-idstatus`, und `start-time`

Example des **describe-snapshots** Befehls

```
aws ec2 describe-snapshots --snapshot-ids snapshot-id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Example der **describe-snapshots** Befehlsausgabe

```
{
```

```
"Snapshots": [  
  {  
    "Description": "Created by AWS-Snowball-VMImport service for s.import-  
snap-8f6bfd7fc9ead9aca",  
    "Encrypted": false,  
    "OwnerId": "123456789012",  
    "SnapshotId": "s.snap-848a22d7518ad442b",  
    "StartTime": "2020-07-30T04:31:05.032000+00:00",  
    "State": "completed",  
    "VolumeSize": 8  
  }  
]  
}
```

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--restorable-by-user-ids value]
- [--dry-run]
- [--no-dry-run]

Löschen eines Snapshots von einem Snowball Edge-Gerät

Um Snapshots zu entfernen, die Ihnen gehören und die Sie nicht mehr benötigen, können Sie den `delete-snapshot` Befehl verwenden.

Example des Befehls **delete-snapshot**

```
aws ec2 delete-snapshot --snapshot-id snapshot-id --endpoint http://snowball-ip:8008 --  
region snow --profile profile-name
```

Note

Snowball Edge unterstützt nicht das Löschen von Snapshots, die sich im Status PENDING befinden oder wenn sie als Root-Gerät für ein AMI vorgesehen sind.

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]

- [--no-dry-run]

Abmeldung eines AMI auf einem Snowball Edge

Um die Registrierung eines nicht mehr benötigten Produkts aufzuheben AMIs , können Sie den Befehl ausführen. `deregister-image` Das Abmelden eines AMI, das sich im Status Ausstehend befindet, wird derzeit nicht unterstützt.

Example des Befehls **deregister-image**

```
aws ec2 deregister-image --image-id image-id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Verwenden der AWS CLI und API-Operationen auf dem Snowball Edge-Gerät

Wenn Sie die Operationen AWS Command Line Interface (AWS CLI) oder API verwenden, um IAM-, Amazon S3- und EC2 Amazon-Befehle auf Snowball Edge auszugeben, müssen Sie das `region` als `"snow"` angeben. Sie können dies mithilfe `AWS configure` oder innerhalb des Befehls selbst tun, wie in den folgenden Beispielen.

```
aws configure --profile ProfileName
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Oder

```
aws s3 ls --endpoint http://192.0.2.0:8080 --region snow --profile ProfileName
```

Netzwerkkonfigurationen für Recheninstanzen auf Snowball Edge

Nachdem Sie Ihre Compute-Instanz auf einem Snowball Edge gestartet haben, müssen Sie ihr eine IP-Adresse zuweisen, indem Sie eine Netzwerkschnittstelle erstellen. Snowball Edges unterstützen zwei Arten von Netzwerkschnittstellen, eine virtuelle Netzwerkschnittstelle und eine direkte Netzwerkschnittstelle.

Virtuelle Netzwerkschnittstelle (VNI) — Eine virtuelle Netzwerkschnittstelle ist die Standard-Netzwerkschnittstelle für die Verbindung mit einer EC2 -kompatiblen Instanz auf Ihrem Snowball Edge. Sie müssen für jede Ihrer EC2 -kompatiblen Instanzen ein VNI erstellen, unabhängig davon, ob Sie auch eine direkte Netzwerkschnittstelle verwenden oder nicht. Der Datenverkehr, der über ein VNI fließt, wird durch die von Ihnen eingerichteten Sicherheitsgruppen geschützt. Sie können nur eine Verbindung zu VNIs dem physischen Netzwerkport herstellen, den Sie zur Steuerung Ihres Snowball Edge verwenden.

Note

VNI verwendet dieselbe physische Schnittstelle (RJ45SFP+ oder QSFP), die für die Verwaltung von Snowball Edge verwendet wird. Das Erstellen eines VNI auf einer anderen physischen Schnittstelle als der, die für die Geräteverwaltung verwendet wird, kann zu unerwarteten Ergebnissen führen.

Direct Network Interface (DNI) — Eine direkte Netzwerkschnittstelle (DNI) ist eine erweiterte Netzwerkfunktion, die Anwendungsfälle wie Multicast-Streams, transitives Routing und Lastenausgleich ermöglicht. Indem Sie Instances mit Layer-2-Netzwerkzugriff ohne zwischengeschaltete Übersetzung oder Filterung bereitstellen, können Sie mehr Flexibilität bei der Netzwerkconfiguration Ihres Snowball Edge und eine verbesserte Netzwerkleistung erzielen. DNIs unterstützt VLAN-Tags und das Anpassen der MAC-Adresse. Weiterer Datenverkehr DNIs ist nicht durch Sicherheitsgruppen geschützt.

DNIs Kann auf Snowball Edge-Geräten mit den RJ45, SFP- oder QSFP-Ports verknüpft werden. Jeder physische Port unterstützt maximal 63. DNIs müssen nicht mit demselben physischen Netzwerkport verknüpft sein, den Sie für die Verwaltung von Snowball Edge verwenden.

 Note

Speicheroptimierte Geräte (mit EC2 Rechenfunktion) von Snowball Edge werden nicht unterstützt DNIs.

Themen

- [Voraussetzungen für DNIs oder VNIs auf Snowball Edge](#)
- [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\) auf einem Snowball Edge](#)
- [Einrichten einer direkten Netzwerkschnittstelle \(DNI\) auf einem Snowball Edge](#)

Voraussetzungen für DNIs oder VNIs auf Snowball Edge

Bevor Sie ein VNI oder ein DNI konfigurieren, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben.

1. Stellen Sie sicher, dass Ihr Gerät mit Strom versorgt wird und dass eine Ihrer physischen Netzwerkschnittstellen, wie der RJ45 Port, mit einer IP-Adresse verbunden ist.
2. Rufen Sie die IP-Adresse ab, die der physischen Netzwerkschnittstelle zugeordnet ist, die Sie auf dem Snowball Edge verwenden.
3. Konfigurieren Sie den Snowball Edge-Client. Weitere Informationen finden Sie unter [Konfiguration eines Profils für den Snowball Edge-Client](#).
4. Konfigurieren Sie AWS CLI. Weitere Informationen finden Sie unter [Erste Schritte mit dem AWS CLI](#) im AWS Command Line Interface Benutzerhandbuch.
5. Entsperren Sie das Gerät.
 - Wird verwendet AWS OpsHub , um das Gerät zu entsperren. Weitere Informationen finden Sie unter [Entsperren eines Snowball Edge](#) mit. AWS OpsHub
 - Verwenden Sie den Snowball Edge-Client, um das Gerät zu entsperren. Weitere Informationen finden Sie unter [Den Snowball Edge freischalten](#).
6. Starten Sie eine EC2 -kompatible Instanz auf dem Gerät. Sie verknüpfen das VNI mit dieser Instanz.

7. Verwenden Sie den Snowball Edge-Client, um den `describe-device` Befehl auszuführen. Die Ausgabe des Befehls liefert eine Liste der physikalischen IDs Netzwerkschnittstellen. Weitere Informationen finden Sie unter [Status eines Snowball Edge anzeigen](#).
8. Identifizieren Sie die ID der physischen Netzwerkschnittstelle, die Sie verwenden möchten. Notieren Sie diese.

Einrichten einer virtuellen Netzwerkschnittstelle (VNI) auf einem Snowball Edge

Nachdem Sie die ID der physischen Netzwerkschnittstelle identifiziert haben, können Sie eine virtuelle Netzwerkschnittstelle (VNI) mit dieser physischen Schnittstelle einrichten. Gehen Sie wie folgt vor, um ein VNI einzurichten. Stellen Sie sicher, dass Sie die erforderlichen Aufgaben ausführen, bevor Sie eine VNI erstellen.

Erstellen Sie ein VNI und ordnen Sie eine IP-Adresse zu

1. Verwenden Sie den Snowball Edge-Client, um den `create-virtual-network-interface` Befehl auszuführen. Die folgenden Beispiele zeigen die Ausführung des Befehls mit den beiden verschiedenen IP-Adressvergabemethoden DHCP oder STATIC. Die DHCP-Methode verwendet das Dynamic Host Configuration Protocol (DHCP).

```
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment DHCP \  
--profile profile-name  
//OR//  
  
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment STATIC \  
--static-ip-address-configuration IpAddress=192.0.2.0,Netmask=255.255.255.0 \  
--profile profile-name
```

Der Befehl gibt eine JSON-Struktur zurück, die die IP-Adresse enthält. Notieren Sie sich die IP-Adresse, die Sie später im Vorgang mit dem `ec2 associate-address` AWS CLI Befehl verwenden möchten.

Wann immer Sie diese IP-Adresse benötigen, können Sie den Snowball Edge-Client-Befehl, den `describe-virtual-network-interfaces` Snowball Edge-Client-Befehl oder den AWS CLI Befehl verwenden, `aws ec2 describe-addresses` um sie abzurufen.

2. Verwenden Sie den AWS CLI , um die IP-Adresse der EC2 -kompatiblen Instanz zuzuordnen, und ersetzen Sie den roten Text durch Ihre Werte:

```
aws ec2 associate-address --public-ip 192.0.2.0 --instance-id s.i-01234567890123456
--endpoint http://Snowball Edge physical IP address:8008
```

Einrichten einer direkten Netzwerkschnittstelle (DNI) auf einem Snowball Edge

Note

Die direkte Netzwerkschnittstellenfunktion ist am oder nach dem 12. Januar 2021 verfügbar und überall verfügbar, AWS-Regionen wo Snowball Edges verfügbar sind.

Voraussetzungen für ein DNI auf einem Snowball Edge

Bevor Sie eine direkte Netzwerkschnittstelle (DNI) einrichten, müssen Sie die Aufgaben im Abschnitt Voraussetzungen ausführen.

1. Führen Sie die erforderlichen Aufgaben aus, bevor Sie das DNI einrichten. Detaillierte Anweisungen finden Sie unter [Voraussetzungen für DNIs oder VNIs auf Snowball Edge](#).
2. Darüber hinaus müssen Sie eine Instanz auf Ihrem Gerät starten, eine VNI erstellen und diese der Instanz zuordnen. Detaillierte Anweisungen finden Sie unter [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\) auf einem Snowball Edge](#).

Note

Wenn Sie Ihrem vorhandenen Gerät durch ein in-the-field Softwareupdate direkte Netzwerke hinzugefügt haben, müssen Sie das Gerät zweimal neu starten, um die Funktion vollständig zu aktivieren.

Erstellen Sie ein DNI und ordnen Sie die IP-Adresse zu

1. Erstellen Sie eine direkte Netzwerkschnittstelle und fügen Sie sie der Amazon EC2 -kompatiblen Instance hinzu, indem Sie den folgenden Befehl ausführen. Für den nächsten Schritt benötigen Sie die MAC-Adresse des Geräts.

```
create-direct-network-interface [--endpoint endpoint] [--instance-id instanceId]
  [--mac macAddress]
                                [--physical-network-interface-
id physicalNetworkInterfaceId]
                                [--unlock-code unlockCode] [--vlan vlanId]
```

OPTIONS

--endpoint <endpoint>Der Endpunkt, an den diese Anfrage gesendet werden soll. Der Endpunkt für Ihre Geräte ist eine URL, die das https Schema verwendet, gefolgt von einer IP-Adresse. Wenn die IP-Adresse für Ihr Gerät beispielsweise 123.0.1.2 lautet, wäre der Endpunkt für Ihr Gerät https://123.0.1.2.

--instance-id <instanceId>Die EC2 -kompatible Instanz-ID, an die die Schnittstelle angehängt werden soll (optional).

--mac <macAddress>Legt die MAC-Adresse der Netzwerkschnittstelle fest (optional).

--physical-network-interface-id <physicalNetworkInterfaceId>Die ID für die physische Netzwerkschnittstelle, auf der eine neue virtuelle Netzwerkschnittstelle erstellt werden soll. Mit dem describe-device Befehl können Sie die auf Ihrem Snowball Edge verfügbaren physischen Netzwerkschnittstellen ermitteln.

--vlan <vlanId>Stellen Sie das zugewiesene VLAN für die Schnittstelle ein (optional). Wenn angegeben, wird der gesamte von der Schnittstelle gesendete Datenverkehr mit der angegebenen VLAN-ID gekennzeichnet. Eingehender Datenverkehr wird nach der angegebenen VLAN-ID gefiltert und alle VLAN-Tags werden entfernt, bevor er an die Instanz weitergeleitet wird.

2. Nachdem Sie ein DNI erstellt und es Ihrer EC2 -kompatiblen Instance zugeordnet haben, müssen Sie zwei Konfigurationsänderungen in Ihrer Amazon EC2 -kompatiblen Instance vornehmen.

- Die erste Änderung besteht darin, sicherzustellen, dass Pakete, die für das mit der EC2 - kompatiblen Instance verknüpfte VNI bestimmt sind, über eth0 gesendet werden.
- Die zweite Änderung konfiguriert Ihre direkte Netzwerkschnittstelle so, dass sie beim Booten entweder DHCP oder statische IP verwendet.

Im Folgenden finden Sie Beispiele für Shell-Skripte für Amazon Linux 2 und CentOS Linux, die diese Konfigurationsänderungen vornehmen.

Amazon Linux 2

```
# Mac address of the direct network interface.
# You got this when you created the direct network interface.
DNI_MAC=[MAC ADDRESS FROM CREATED DNI]

# Configure routing so that packets meant for the VNI always are sent through
eth0.
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo "from $PRIVATE_IP table $ROUTE_TABLE" > /etc/sysconfig/network-scripts/
rule-eth0
echo "default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE" > /etc/
sysconfig/network-scripts/route-eth0
echo "169.254.169.254 dev eth0" >> /etc/sysconfig/network-scripts/route-eth0

# Query the persistent DNI name, assigned by udev via ec2net helper.
# changable in /etc/udev/rules.d/70-persistent-net.rules
DNI=$(ip --oneline link | grep -i $DNI_MAC | awk -F ':' ' '{ print $2 }')

# Configure DNI to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
HWADDR=$DNI_MAC
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
MAINROUTETABLE=no
EOF
```

```
# Make all changes live.
systemctl restart network
```

CentOS Linux

```
# Mac address of the direct network interface. You got this when you created the
direct network interface.
DNI_MAC=[MAC ADDRESS FROM CREATED DNI]
# The name to use for the direct network interface. You can pick any name that
isn't already in use.
DNI=eth1

# Configure routing so that packets meant for the VNIC always are sent through
eth0
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo from $PRIVATE_IP table $ROUTE_TABLE > /etc/sysconfig/network-scripts/rule-
eth0
echo default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE > /etc/sysconfig/
network-scripts/route-eth0

# Configure your direct network interface to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
HWADDR="$DNI_MAC"
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
EOF

# Rename DNI device if needed.
CURRENT_DEVICE_NAME=$(LANG=C ip -o link | awk -F ':' -v IGNORECASE=1 '!/link\/
ieee802\.\.11/ && /'"$DNI_MAC"'/ { print $2 })
ip link set $CURRENT_DEVICE_NAME name $DNI

# Make all changes live.
systemctl restart network
```


Verwenden von SSH zum Herstellen einer Verbindung zu Recheninstanzen auf einem Snowball Edge

Um Secure Shell (SSH) zu verwenden, um eine Verbindung zu Recheninstanzen auf einem Snowball Edge herzustellen, haben Sie die folgenden Optionen für die Bereitstellung oder Erstellung eines SSH-Schlüssels.

- Sie können den SSH-Schlüssel für das Amazon Machine Image (AMI) angeben, wenn Sie einen Auftrag zur Bestellung eines Geräts erstellen. Weitere Informationen finden Sie unter [Einen Job erstellen, um einen Snowball Edge zu bestellen](#).
- Sie können den SSH-Schlüssel für das AMI angeben, wenn Sie ein VM-Image für den Import in einen Snowball Edge erstellen. Weitere Informationen finden Sie unter [Importieren eines VM-Images auf ein Snowball Edge-Gerät](#).
- Sie können ein key pair auf dem Snowball Edge erstellen und wählen, ob Sie eine Instance mit diesem lokal generierten öffentlichen Schlüssel starten möchten. Weitere Informationen finden Sie unter [Erstellen eines key pair mithilfe von Amazon EC2](#) im EC2 Amazon-Benutzerhandbuch.

So stellen Sie über SSH eine Verbindung zu einer Instance her

1. Vergewissern Sie sich, dass Ihr Gerät eingeschaltet, mit dem Netzwerk verbunden und entsperrt ist. Weitere Informationen finden Sie unter [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#).
2. Stellen Sie sicher, dass Sie die Netzwerkeinstellungen für Ihre Datenverarbeitungs-Instances konfiguriert haben. Weitere Informationen finden Sie unter [Netzwerkkonfigurationen für Recheninstanzen auf Snowball Edge](#).
3. Überprüfen Sie Ihre Notizen zum Suchen des PPK- oder PEM-Schlüsselpaars aus, das Sie für diese spezifische Instance verwendet haben. Erstellen Sie eine Kopie dieser Dateien an einem beliebigen Ort auf Ihrem Computer. Notieren Sie sich den Pfad zur PEM-Datei.
4. Verbinden Sie sich wie im folgenden Beispielbefehl per SSH mit Ihrer Instance. Die IP-Adresse ist die IP-Adresse der virtuellen Netzwerkschnittstelle (VNIC), die Sie in [Netzwerkkonfigurationen für Recheninstanzen auf Snowball Edge](#) einrichten.

```
ssh -i path/to/PEM/key/file instance-user-name@192.0.2.0
```

Weitere Informationen finden Sie unter [Herstellen einer Verbindung zu Ihrer Linux-Instance mithilfe von SSH](#) im EC2 Amazon-Benutzerhandbuch.

Übertragung von Daten von EC2 -kompatiblen Recheninstanzen in S3-Buckets auf demselben Snowball Edge

Sie können Daten zwischen Compute-Instances und Amazon S3 S3-Buckets auf demselben Snowball Edge-Gerät übertragen. Dazu verwenden Sie die unterstützten AWS CLI Befehle und die entsprechenden Endpunkte. Nehmen wir zum Beispiel an, dass Sie Daten aus einem Verzeichnis in meiner `sbe1.xlarge` Instanz in den Amazon S3 S3-Bucket `amzn-s3-demo-bucket` auf demselben Gerät verschieben möchten. Gehen Sie davon aus, dass Sie den Amazon S3 S3-kompatiblen Speicher auf dem Snowball Edge-Endpunkt `https://S3-object-API-endpoint:443` verwenden. Sie führen die folgenden Schritte aus.

Um Daten zwischen einer Recheninstanz und einem Bucket auf demselben Snowball Edge zu übertragen

1. Verwenden Sie SSH, um eine Verbindung zu Ihrer Datenverarbeitungs-Instance herzustellen.
2. Laden Sie das herunter und installieren Sie es AWS CLI. Wenn Ihre Instance noch nicht über die AWS CLI verfügt, laden Sie sie herunter und installieren Sie sie. Weitere Informationen finden Sie unter [Installieren der AWS Command Line Interface](#).
3. Konfigurieren Sie die Instance AWS CLI auf Ihrer Recheninstanz so, dass sie mit dem Amazon S3 S3-Endpunkt auf dem Snowball Edge funktioniert. Weitere Informationen finden Sie unter [Abrufen und Verwenden lokaler Amazon S3 S3-Anmeldeinformationen auf Snowball Edge](#).
4. Verwenden Sie den unterstützten Amazon S3 S3-kompatiblen Speicher für Snowball Edge-Befehle, um Daten zu übertragen. Zum Beispiel:

```
aws s3 cp ~/june2018/results s3://amzn-s3-demo-bucket/june2018/results --recursive --endpoint https://S3-object-API-endpoint:443
```

Automatisches Starten von EC2 -kompatiblen Instances

Der Snowball Edge Client ist eine eigenständige CLI (Command Line Interface) -Anwendung, die Sie in Ihrer Umgebung ausführen können. Sie können damit einige Verwaltungsaufgaben auf Ihrem

Snowball Edge-Gerät oder Gerätecluster ausführen. Weitere Informationen zur Verwendung des Snowball Edge-Clients, einschließlich zum Starten und Beenden von Diensten damit, finden Sie unter [Konfiguration und Verwendung des Snowball Edge-Clients](#).

Im Folgenden finden Sie Informationen zu den Snowball Edge-Clientbefehlen, die spezifisch für Recheninstanzen sind, einschließlich Anwendungsbeispielen.

Eine Liste der EC2 Amazon-kompatiblen Befehle, die Sie auf Ihrem AWS Snowball Edge Gerät verwenden können, finden Sie unter [Unterstützte EC2 Amazon-kompatible AWS CLI Befehle auf einem Snowball Edge](#).

Eine EC2 -kompatible Startkonfiguration auf einem Snowball Edge erstellen

Um EC2 Amazon-kompatible Compute-Instances auf Ihrem AWS Snowball Edge Gerät automatisch zu starten, nachdem es entsperrt wurde, können Sie eine Startkonfiguration erstellen. Verwenden Sie dazu den `snowballEdge create-autostart-configuration` Befehl, wie im Folgenden gezeigt.

Usage

```
snowballEdge create-autostart-configuration --physical-connector-type [SFP_PLUS or RJ45 or QSFP] --ip-address-assignment [DHCP or STATIC] [--static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]] --launch-template-id [--launch-template-version]
```

Aktualisierung einer EC2 -kompatiblen Startkonfiguration auf einem Snowball Edge

Verwenden Sie den `snowballEdge update-autostart-configuration` Befehl, um eine bestehende Startkonfiguration auf Ihrem Snowball Edge zu aktualisieren. Im Folgenden wird gezeigt, wie Sie ihn verwenden. Um eine Startkonfiguration zu aktivieren oder zu deaktivieren, geben Sie den Parameter `--enabled` an.

Usage

```
snowballEdge update-autostart-configuration --autostart-configuration-arn [--physical-connector-type [SFP_PLUS or RJ45 or QSFP]] [--ip-address-assignment [DHCP or STATIC]] [--static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]] [--launch-template-id] [--launch-template-version] [--enabled]
```

Löschen einer EC2 -kompatiblen Startkonfiguration auf einem Snowball Edge

Um eine Startkonfiguration zu löschen, die nicht mehr verwendet wird, verwenden Sie den `snowballEdge delete-autostart-configuration` Befehl wie folgt.

Usage

```
snowballEdge delete-autostart-configuration --autostart-configuration-arn
```

EC2Kompatible Startkonfigurationen auf einem Snowball Edge auflisten

Um die Startkonfigurationen aufzulisten, die Sie auf Ihrem Snowball Edge erstellt haben, verwenden Sie den `describe-autostart-configurations` Befehl wie folgt.

Usage

```
snowballEdge describe-autostart-configurations
```

Erstellen einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge

Um eine Recheninstanz auszuführen oder die NFS-Schnittstelle auf einem Snowball Edge zu starten, erstellen Sie zunächst eine virtuelle Netzwerkschnittstelle (VNI). Jeder Snowball Edge hat drei Netzwerkschnittstellen (NICs), die physischen Netzwerkschnittstellen-Controller für das Gerät. Dies sind die RJ45 SFP- und QSFP-Anschlüsse auf der Rückseite des Geräts.

Jedes VNI basiert auf einem physischen VNI, und Sie können jeder NIC eine beliebige Anzahl von VNIs zuordnen. Um eine virtuelle Netzwerkschnittstelle zu erstellen, verwenden Sie den Befehl `snowballEdge create-virtual-network-interface`.

Note

Der Parameter `--static-ip-address-configuration` ist nur gültig, wenn die Option `STATIC` für den Parameter `--ip-address-assignment` verwendet wird.

Verwendung

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge create-virtual-network-interface --ip-address-assignment [DHCP or STATIC]
--physical-network-interface-id [physical network interface id] --static-ip-address-
configuration IPAddress=[IP address],NetMask=[Netmask]
```

Das folgende Anwendungsbeispiel zeigt die Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge create-virtual-network-interface --endpoint https://[ip address]
--manifest-file /path/to/manifest --unlock-code [unlock code] --ip-address-
assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface
id] --static-ip-address-configuration IPAddress=[IP address],NetMask=[Netmask]
```

Example Beispiel: Erstellen VNICs (mit DHCP)

```
snowballEdge create-virtual-network-interface --ip-address-assignment dhcp --physical-
network-interface-id s.ni-8EXAMPLEaEXAMPLEd
{
  "VirtualNetworkInterface" : {
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/
s.ni-8EXAMPLE8EXAMPLEf",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45",
    "MtuSize" : "1500"
  }
}
```

Beschreibung Ihrer virtuellen Netzwerkschnittstellen

Verwenden Sie den `snowballEdge describe-virtual-network-interfaces` Befehl, um VNICs das zu beschreiben, was Sie zuvor auf Ihrem Gerät erstellt haben. Im Folgenden wird gezeigt, wie Sie ihn verwenden.

Verwendung

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge describe-virtual-network-interfaces
```

Das folgende Anwendungsbeispiel zeigt die Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge describe-virtual-network-interfaces --endpoint https://[ip address] --  
manifest-file /path/to/manifest --unlock-code [unlock code]
```

Example Beispiel: Beschreiben VNICs

```
snowballEdge describe-virtual-network-interfaces  
[  
  {  
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/  
s.ni-8EXAMPLE8EXAMPLE8",  
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",  
    "IpAddressAssignment" : "DHCP",  
    "IpAddress" : "192.0.2.0",  
    "Netmask" : "255.255.255.0",  
    "DefaultGateway" : "192.0.2.1",  
    "MacAddress" : "EX:AM:PL:E1:23:45",  
    "MtuSize" : "1500"  
  }, {  
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/  
s.ni-1EXAMPLE1EXAMPLE1",  
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",  
    "IpAddressAssignment" : "DHCP",  
    "IpAddress" : "192.0.2.2",  
    "Netmask" : "255.255.255.0",  
    "DefaultGateway" : "192.0.2.1",  
    "MacAddress" : "12:34:5E:XA:MP:LE",  
    "MtuSize" : "1500"  
  }  
]
```

Aktualisierung einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge

Nachdem Sie eine virtuelle Netzwerkschnittstelle (VNI) erstellt haben, können Sie deren Konfiguration mit dem `snowballEdge update-virtual-network-interface` Befehl aktualisieren. Nachdem Sie den Amazon-Ressourcennamen (ARN) für eine bestimmte VNI angegeben haben, geben Sie nur Werte für die Elemente an, die Sie aktualisieren.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge update-virtual-network-interface --virtual-network-interface-arn [virtual network-interface-arn] --ip-address-assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface id] --static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]
```

Das folgende Anwendungsbeispiel zeigt die Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge update-virtual-network-interface --endpoint https://[ip address] --manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-interface-arn [virtual network-interface-arn] --ip-address-assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface id] --static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]
```

Example Beispiel: Aktualisieren einer VNIC (mit DHCP)

```
snowballEdge update-virtual-network-interface --virtual-network-interface-arn arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd --ip-address-assignment dhcp
```

Löschen einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge

Um eine virtuelle Netzwerkschnittstelle (VNI) zu löschen, können Sie den `snowballEdge delete-virtual-network-interface` Befehl verwenden.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn [virtual network-interface-arn]
```

Das folgende Anwendungsbeispiel zeigt die Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge delete-virtual-network-interface --endpoint https://[ip address] --manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-interface-arn [virtual network-interface-arn]
```

Example Beispiel: Löschen einer VNIC

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd
```

Verwenden des EC2 Amazon-kompatiblen Endpunkts auf einem Snowball Edge

Im Folgenden finden Sie eine Übersicht über den EC2 Amazon-kompatiblen Endpunkt. Mit diesem Endpunkt können Sie Ihre Amazon Machine Images (AMIs) verwalten und Instances mithilfe von EC2 Amazon-kompatiblen API-Operationen programmgesteuert berechnen.

Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben

Wenn Sie den verwenden AWS CLI , um einen Befehl an das AWS Snowball Edge Gerät zu senden, können Sie angeben, dass es sich bei dem Endpunkt um den EC2 Amazon-kompatiblen Endpunkt handelt. Sie können den HTTPS-Endpunkt oder einen ungesicherten HTTP-Endpunkt, wie hier gezeigt, verwenden.

Gesicherter HTTPS-Endpunkt

```
aws ec2 describe-instances --endpoint https://192.0.2.0:8243 --ca-bundle path/to/certificate
```


Ungesicherter HTTP-Endpunkt

```
aws ec2 describe-instances --endpoint http://192.0.2.0:8008
```

Wenn Sie den HTTPS-Endpunkt 8243 verwenden, werden Ihre Daten während der Übertragung verschlüsselt. Diese Verschlüsselung wird durch ein Zertifikat gewährleistet, das von Snowball Edge generiert wird, wenn es entsperrt wird. Nachdem Sie Ihr Zertifikat erhalten haben, können Sie es in einer lokalen `ca-bundle.pem`-Datei speichern. Anschließend können Sie Ihr AWS CLI -Profil so konfigurieren, dass der Pfad zu Ihrem Zertifikat wie unten beschrieben hinzugefügt wird.

So verknüpfen Sie Ihr Zertifikat mit dem EC2 Amazon-kompatiblen Endpunkt

1. Connect den Snowball Edge mit Strom und Netzwerk und schalten Sie ihn ein.
2. Notieren Sie nach dem Entsperren des Geräts seine IP-Adresse im lokalen Netzwerk.
3. Stellen Sie sicher, dass Sie Snowball Edge von einem Terminal in Ihrem Netzwerk aus pingen können.
4. Führen Sie den `snowballEdge get-certificate`-Befehl in Ihrem Terminal aus. Weitere Informationen zu diesem Befehl finden Sie unter [Verwaltung von Public-Key-Zertifikaten auf Snowball Edge](#).
5. Speichern Sie die Ausgabe des `snowballEdge get-certificate`-Befehls in einer Datei, z. B. `ca-bundle.pem`.
6. Führen Sie im Terminal den folgenden Befehl aus:

```
aws configure set profile.snowballEdge.ca_bundle /path/to/ca-bundle.pem
```

Wenn die Vorgehensweise abgeschlossen ist, können Sie CLI-Befehle mit diesen lokalen Anmeldeinformationen, Ihrem Zertifikat und dem angegebenen Endpunkt ausführen.

Unterstützte EC2 Amazon-kompatible AWS CLI Befehle auf einem Snowball Edge

Sie können Ihre Compute-Instances auf einem Snowball Edge-Gerät über einen EC2 Amazon-kompatiblen Endpunkt verwalten. Dieser Endpunkttyp unterstützt viele der Amazon EC2 CLI-Befehle und -Aktionen von AWS SDKs. Informationen zur Installation und Einrichtung von AWS CLI, einschließlich der Angabe, gegen wen AWS-Regionen Sie AWS CLI Anrufe tätigen möchten, finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

Liste der unterstützten EC2 -kompatiblen AWS CLI Befehle auf einem Snowball Edge

Im Folgenden finden Sie eine Beschreibung der Teilmenge der AWS CLI Befehle und Optionen für Amazon EC2 , die auf Snowball Edge-Geräten unterstützt werden. Wenn ein Befehl oder eine Option im Folgenden nicht aufgeführt ist, wird diese(r) nicht unterstützt. Sie können einige nicht unterstützte Optionen in Kombination mit einem Befehl angeben. Diese werden jedoch ignoriert.

- [associate-address](#) – Verknüpft eine virtuelle IP-Adresse mit einer Instance, damit diese über eine der drei physischen Netzwerkschnittstellen auf dem Gerät verwendet werden kann:
 - `--instance-id` – Die ID einer einzelnen sbe-Instance.
 - `--public-ip` – Die virtuelle IP-Adresse, mit der Sie auf Ihre Instance zugreifen möchten.
- [attach-volume](#) — Hängt ein Amazon EBS-Volume an eine gestoppte oder laufende Instance auf Ihrem Gerät an und macht es der Instance mit dem angegebenen Gerätenamen zugänglich.
 - `--device value` Der Gerätename.
 - `--instance-id` — Die ID einer Amazon EC2 -kompatiblen Zielinstanz.
 - `--volume-id value` — Die ID des EBS-Volumes.
- [authorize-security-group-egress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln zur Verwendung mit einem Snowball Edge-Gerät hinzu. Insbesondere ermöglicht diese Aktion Instances, Datenverkehr an einen oder mehrere IPv4 CIDR-Zieladressbereiche zu senden. Weitere Informationen finden Sie unter [Steuern des Netzwerkverkehrs mit Sicherheitsgruppen auf Snowball Edge](#).
 - `--group-id value` — Die ID der Sicherheitsgruppe
 - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
- [authorize-security-group-ingress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Eingangsregeln hinzu. Wenn Sie `authorize-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
 - `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
 - `[--group-idvalue]` — Die ID der Sicherheitsgruppe
 - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
 - `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (-1) angegeben.
 - `[--portvalue]` — Für TCP oder UDP der Bereich der Ports, die zugelassen werden sollen. Dieser Wert kann eine einzelne Ganzzahl oder ein Bereich (Minimum—Maximum) sein.

Für ICMP eine einzelne Ganzzahl oder ein Bereich (type-code), wobei bei type die Nummer des ICMP-Typs und code die ICMP-Codenummer darstellen. Der Wert -1 steht für alle ICMP-Codes für alle ICMP-Typen. Der Wert -1 nur für type gibt alle ICMP-Codes für den angegebenen ICMP-Typ an.

- `--cidrvalue` — Der CIDR-IP-Bereich.
- [create-launch-template](#) — Erstellt eine Startvorlage. Eine Startvorlage enthält die Parameter zum Starten einer Instance. Wenn Sie eine Instance über `RunInstances` starten, können Sie eine Startvorlage angeben, statt die Startparameter in der Anfrage bereitzustellen. Sie können bis zu 100 Vorlagen pro Gerät erstellen.
- `--launch-template-name string` — Ein Name für die Startvorlage.
- `--launch-template-data structure` — Die Informationen für die Startvorlage. Folgende Attribute werden unterstützt:
 - `ImageId`
 - `InstanceType`
 - `SecurityGroupIds`
 - `TagSpecifications`
 - `UserData`

JSON-Syntax:

```
{
  "ImageId":"string",
  "InstanceType":"sbe-c.large",
  "SecurityGroupIds":["string", ...],
  "TagSpecifications":[{"ResourceType":"instance","Tags":
    [{"Key":"Name","Value":"Test"},
     {"Key":"Stack","Value":"Gamma"}]},
  "UserData":"this is my user data"
}
```

- `--version-descriptionstring` — Eine Beschreibung für die erste Version der Startvorlage.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).

- [create-launch-template-version](#) — Erstellt eine neue Version für eine Startvorlage. Sie können eine vorhandene Version einer Startvorlage angeben, auf der die neue Version basieren soll. Die Startvorlagenversionen werden in der Reihenfolge markiert, in der sie erstellt werden. Sie können die Nummerierung von Startvorlagenversionen nicht angeben, ändern oder ersetzen. Sie können bis zu 100 Versionen jeder Startvorlage erstellen.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `-- launch-template-data structure` — Die Informationen für die Startvorlage. Folgende Attribute werden unterstützt:
 - `ImageId`
 - `InstanceType`
 - `SecurityGroupIds`
 - `TagSpecifications`
 - `UserData`

JSON-Syntax:

```
{
  "ImageId":"string",
  "InstanceType":"sbe-c.large",
  "SecurityGroupIds":["string", ...],
  "TagSpecifications":[{"ResourceType":"instance","Tags":
    [{"Key":"Name","Value":"Test"},
     {"Key":"Stack","Value":"Gamma"}]},
  "UserData":"this is my user data"
}
```

- `[--source-versionstring]` — Die Versionsnummer der Startvorlage, auf der die neue Version basieren soll. Die neue Version übernimmt alle Startparameter der Quellversion, ausgenommen der von Ihnen in `launch-template-data` angegebenen Parameter.
- `[--version-descriptionstring]` — Eine Beschreibung für die erste Version der Startvorlage.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).

- [create-tags](#) — **Fügt ein oder mehrere Tags** für die angegebene Ressource hinzu oder überschreibt es. Jede Ressource kann maximal 50 Tags haben. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Tag-Schlüssel müssen für eine Ressource eindeutig sein. Folgende Ressourcen werden unterstützt:
 - AMI
 - Instance
 - Startvorlage
 - Sicherheitsgruppe
 - Schlüsselpaar
- [create-security-group](#) — Erstellt eine Sicherheitsgruppe auf Ihrem Snowball Edge. Sie können bis zu 50 Sicherheitsgruppen erstellen. Wenn Sie eine Sicherheitsgruppe erstellen, geben Sie einen Anzeigenamen Ihrer Wahl an:
 - `--group-name value` — Der Name der Sicherheitsgruppe.
 - `--description value` — Eine Beschreibung der Sicherheitsgruppe. Dies dient nur zu Informationszwecken. Dieser Wert kann bis zu 255 Zeichen lang sein.
- [create-volume](#) — Erstellt ein Amazon EBS-Volume, das an eine Instance auf Ihrem Gerät angehängt werden kann.
 - `[--sizevalue]` — Die Größe des Volumes in GiBs, die zwischen 1 GiB und 1 TB (1000 GiBs) liegen kann.
 - `[--snapshot-idvalue]` — Der Snapshot, aus dem das Volume erstellt werden soll.
 - `[--volume-type]` — Der Volume-Typvalue. Wenn kein Wert angegeben wird, lautet der Standardwert `sbg1`. Die folgenden Werte sind möglich:
 - `sbg1` für magnetische Volumes
 - `sbp1` für SSD-Volumes
 - `[--tag-specificationvalue]` — Eine Liste von Tags, die bei der Erstellung auf das Volume angewendet werden sollen.
- [delete-launch-template](#) — Löscht eine Startvorlage. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.

- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [delete-launch-template-version](#) — Löscht eine oder mehrere Versionen einer Startvorlage. Sie können die Standardversion einer Startvorlage erst löschen, nachdem Sie eine andere Version als Standardversion festgelegt haben. Wenn die Standardversion die einzige Version der Startvorlage ist, löschen Sie die gesamte Startvorlage, indem Sie den Befehl `delete-launch-template` verwenden.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `--launch-template-id string` — Die ID der Startvorlage.
- `--launch-template-name string` — Ein Name für die Startvorlage.
- `--versions (Liste) "string" "string"` — Die Versionsnummern einer oder mehrerer Versionen der Startvorlage, die gelöscht werden sollen.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [delete-security-group](#) — Löscht eine Sicherheitsgruppe.

Wenn Sie versuchen, eine Sicherheitsgruppe zu löschen, die mit einer Instance verknüpft ist, oder auf die von einer anderen Sicherheitsgruppe verwiesen wird, schlägt die Operation mit `DependencyViolation` fehl.

- `--group-name value` — Der Name der Sicherheitsgruppe.
- `--description value` — Eine Beschreibung der Sicherheitsgruppe. Dies dient nur zu Informationszwecken. Dieser Wert kann bis zu 255 Zeichen lang sein.
- [delete-tags](#) — Löscht den angegebenen Satz von Tags aus der angegebenen Ressource (AMI, Compute-Instance, Startvorlage oder Sicherheitsgruppe).
- [delete-volume](#) — Löscht das angegebene Amazon EBS-Volume. Das Volume muss den `available`-Status aufweisen (nicht an eine Instance angefügt).
 - `value--volume-id` — Die ID des Volumes.
- [describe-addresses](#) — Beschreibt eine oder mehrere Ihrer virtuellen IP-Adressen, die derselben Anzahl von sbe Instanzen auf Ihrem Gerät zugeordnet sind.

- `--public-ips` – Eine oder mehrere der virtuellen IP-Adressen, die Ihren Instances zugeordnet sind.
- [`describe-images`](#) — Beschreibt eines oder mehrere der Bilder (AMIs), die Ihnen zur Verfügung stehen. Ihnen zur Verfügung stehende Bilder werden dem Snowball Edge-Gerät bei der Auftragserstellung hinzugefügt.
- `--image-id` — Die Snowball-AMI-ID des AMI.
- [`describe-instance-attribute`](#) — Beschreibt das angegebene Attribut der angegebenen Instance. Sie können jeweils nur ein Attribut angeben. Folgende Attribute werden unterstützt:
 - `instanceInitiatedShutdownBehavior`
 - `instanceType`
 - `userData`
- [`describe-instances`](#) – Beschreibt eine oder mehrere Ihrer Instances. Die Antwort gibt alle Sicherheitsgruppen zurück, die den Instances zugeordnet sind.
 - `--instance-ids` — Die einer oder IDs mehrerer sbe Instanzen, die auf dem Gerät gestoppt wurden.
 - `--page-size` — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
 - `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
 - `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- [`describe-instance-status`](#) — Beschreibt den Status der angegebenen Instances oder all Ihrer Instances. Standardmäßig werden nur laufende Instances beschrieben, es sei denn, Sie geben ausdrücklich an, dass der Status aller Instances zurückgegeben werden soll. Der Instanzstatus umfasst die folgenden Komponenten:
 - **Statuschecks** — Das Snow-Gerät führt Statusprüfungen bei laufenden EC2 Amazon-kompatiblen Instances durch, um Hardware- und Softwareprobleme zu identifizieren.
 - **Instance-Status** — Sie können Ihre Instances vom Start bis zu ihrer Kündigung verwalten.

Mit diesem Befehl werden die folgenden Filter unterstützt.

- `[--filters](Liste)`

Die Filter.

- `instance-state-code`— Der Code für den Instanzstatus als 16-Bit-Ganzzahl ohne Vorzeichen. Das High-Byte wird für interne Serviceberichte verwendet und sollte ignoriert werden. Das Low-Byte wird auf der Grundlage des dargestellten Zustands festgelegt. Die gültigen Werte sind 0 (ausstehend), 16 (läuft), 32 (Herunterfahren), 48 (beendet), 64 (Stopp) und 80 (gestoppt).
- `instance-state-name`— Der Status der Instance (`pending` | `running` | `shutting-down` | `terminated` | `stopping` | `stopped`).
- `instance-status.reachability`— Filtert nach dem Instanzstatus, wobei der Name `reachability` (`passed` | `failed` | `initializing` | `insufficient-data`) lautet.
- `instance-status.status`— Der Status der Instanz (`ok` | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
- `system-status.reachability`— Filtert nach dem Systemstatus, wobei der Name Erreichbarkeit (`passed` | `failed` | `initializing` | `insufficient-data`) lautet.
- `system-status.status`— Der Systemstatus der Instanz (`ok` | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
- JSON-Syntax:

```
[
  {
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
]
```

- `[--instance-ids](Liste)`

Die Instanz IDs.

Standard: Beschreibt alle Ihre Instances.

- `[--dry-run | --no-dry-run](boolescher Wert)`

Überprüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anfrage tatsächlich zu stellen, und gibt eine Fehlermeldung aus. Wenn Sie über die erforderlichen Berechtigungen verfügen, lautet die Fehlerantwort `DryRunOperation`.

Andernfalls ist es `UnauthorizedOperation`.

- `[--include-all-instances | --no-include-all-instances]`(boolescher Wert)

Wenn `true`, beinhaltet den Integritätsstatus für alle Instanzen. Wenn `false`, beinhaltet nur den Integritätsstatus für laufende Instanzen.

Standard: `false`

- `--page-size`(Ganzzahl) — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items`(integer) — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token`(string) — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- [describe-launch-templates](#) — Beschreibt eine oder mehrere Startvorlagen. Beim Befehl `describe-launch-templates` handelt es sich um eine paginierte Operation. Sie können mehrere Aufrufe ausführen, um den gesamten Ergebnissatzen abzurufen.

Geben Sie in der Anfrage entweder die Namen der Startvorlage IDs oder der Startvorlage an.

- `--launch-template-ids` (Liste) "string" "string" — Eine Liste IDs der Startvorlagen.
- `--launch-template-names` (Liste) "string" "string" — Eine Liste mit Namen für die Startvorlagen.
- `--page-size` — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an

das Gerät, wodurch bei jedem Aufruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.

- `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [describe-launch-template-versions](#) — Beschreibt eine oder mehrere Versionen einer bestimmten Startvorlage. Sie können alle Versionen, einzelne Versionen oder eine Reihe von Versionen beschreiben. Beim Befehl `describe-launch-template-versions` handelt es sich um eine paginierte Operation. Sie können mehrere Aufrufe ausführen, um den gesamten Ergebnissatzen abzurufen.

Geben Sie in der Anfrage entweder die Namen der Startvorlage IDs oder der Startvorlage an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `[--versions (Liste)"string" "string"]` — Die Versionsnummern einer oder mehrerer Versionen der Startvorlage, die gelöscht werden sollen.
- `[--min-versionstring]` — Die Versionsnummer, nach der die Versionen der Startvorlagen beschrieben werden sollen.
- `[--max-versionstring]` — Die Versionsnummer, bis zu der die Versionen der Startvorlagen beschrieben werden sollen.
- `--page-size` — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Aufruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert,

wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.

- `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [`describe-security-groups`](#) — Beschreibt eine oder mehrere Ihrer Sicherheitsgruppen.

Beim Befehl `describe-security-groups` handelt es sich um eine paginierte Operation. Sie können mehrere API-Aufrufe ausführen, um den gesamten Ergebnissatz abzurufen.

- `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
- `[--group-idvalue]` — Die ID der Sicherheitsgruppe.
- `[--page-sizevalue]` — Die Größe jeder Seite, die beim Serviceaufruf abgerufen werden soll. AWS Diese Größe hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Die Einstellung einer kleineren Seitengröße führt zu mehr Aufrufen des AWS Dienstes, wodurch bei jedem Aufruf weniger Elemente abgerufen werden. Durch diesen Ansatz kann verhindert werden, dass bei AWS Serviceaufrufen ein Timeout auftritt. Anwendungsbeispiele finden Sie unter [Pagination](#) im AWS Command Line Interface Benutzerhandbuch.
- `[--max-itemsvalue]` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an. Verwenden Sie das `NextToken` Antwortelement nicht direkt außerhalb von. AWS CLI Anwendungsbeispiele finden Sie unter [Pagination](#) im AWS Command Line Interface Benutzerhandbuch.
- `[--starting-tokenvalue]` — Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort. Anwendungsbeispiele finden Sie unter [Pagination](#) im Benutzerhandbuch.AWS Command Line Interface

- [describe-tags](#) — Beschreibt eines oder mehrere der Tags für die angegebene Ressource (image, instance, oder Sicherheitsgruppe). Mit diesem Befehl werden die folgenden Filter unterstützt:
 - launch-template
 - resource-id
 - Ressourcentyp: image oder instance
 - key
 - Wert
- [describe-volumes](#) — Beschreibt die angegebenen Amazon EBS-Volumes.
 - [--max-items value] — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein NextToken in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den NextToken-Wert im starting-token-Argument eines nachfolgenden Befehls an.
 - [--starting-token value] — Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der NextToken-Wert aus einer zuvor abgeschnittenen Antwort.
 - [--volume-ids] — Ein oder mehrere Volumes value. IDs
- [detach-volume](#) — Trennt ein Amazon EBS-Volume von einer gestoppten oder laufenden Instance.
 - [--device] — Der Geräte name value.
 - [--instance-id] — Die ID einer Amazon-Zielinstanz. EC2
 - --volume-id value — Die ID des Volumes.
- [disassociate-address](#) — Entfernt eine virtuelle IP-Adresse von der Instance.
 - --public-ip — Die virtuelle IP-Adresse, die Sie von Ihrer Instance trennen möchten.
- [get-launch-template-data](#) — Ruft die Konfigurationsdaten der angegebenen Instanz ab. Sie können diese Daten verwenden, um eine Startvorlage zu erstellen.
 - --instance-id — Die ID einer einzelnen sbe-Instance.
 - --endpoint snowballEndpoint — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [modify-launch-template](#) — Ändert eine Startvorlage. Sie können angeben, welche Version der Startvorlage als Standardversion festgelegt werden soll. Wenn Sie eine Instance ohne Angabe einer Startvorlagenversion starten, wird die Standardversion der Startvorlage angewendet.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `--default-version string` — Die Versionsnummer der Startvorlage, die als Standardversion festgelegt werden soll.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 -kompatiblen API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den EC2 -kompatiblen Endpunkt als AWS CLI Endpunkt auf einem Snowball Edge angeben](#).
- [modify-instance-attribute](#) — Ändert ein Attribut der angegebenen Instance. Folgende Attribute werden unterstützt:
 - `instanceInitiatedShutdownBehavior`
 - `userData`
- [revoke-security-group-egress](#) — Entfernt eine oder mehrere Ausgangsregeln aus einer Sicherheitsgruppe:
 - `[--group-idvalue]` — Die ID der Sicherheitsgruppe
 - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
- [revoke-security-group-ingress](#) — Widerruft eine oder mehrere Regeln für den Zugriff auf eine Sicherheitsgruppe. Wenn Sie `revoke-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
 - `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
 - `[--group-idvalue]` — Die ID der Sicherheitsgruppe.
 - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
 - `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (`-1`) angegeben.
 - `[--portvalue]` — Für TCP oder UDP der Bereich der Ports, die zugelassen werden sollen. Eine einzelne Ganzzahl oder ein Bereich (Minimum—Maximum).

Für ICMP eine einzelne Ganzzahl oder ein Bereich (`type-code`), wobei bei `type` die Nummer des ICMP-Typs und `code` die ICMP-Codenummer darstellen. Der Wert `-1` steht für alle ICMP-Codes für alle ICMP-Typen. Der Wert `-1` nur für `type` gibt alle ICMP-Codes für den angegebenen ICMP-Typ an.

- `[--cidrvalue]` — Der CIDR-IP-Bereich.

- [run-instances](#) — Startet eine Reihe von Compute-Instances mithilfe einer Snowball-AMI-ID für ein AMI.

 Note

Je nach Größe und Typ der Instanz kann es bis zu anderthalb Stunden dauern, bis eine Compute-Instance auf einem Snowball Edge gestartet wird.

- `[-- block-device-mappings (list)]` — Die blockierten Gerätezuordnungseinträge. Die Parameter `DeleteOnTermination`, `VolumeSize` und `VolumeType` werden unterstützt. Start-Volumes müssen den Typ `sbg1` aufweisen.

Die JSON-Syntax für diesen Befehl lautet wie folgt.

```
{
  "DeviceName": "/dev/sdh",
  "Ebs":
  {
    "DeleteOnTermination": true|false,
    "VolumeSize": 100,
    "VolumeType": "sbg1"|"sbg1"
  }
}
```

- `--count` — Anzahl der zu startenden Instances. Wenn Sie nur eine einzige Zahl angeben, wird davon ausgegangen, dass diese die Mindestanzahl der zu startenden Instances darstellt (der Standardwert ist 1). Wenn ein Bereich in der Form von `min:max` angegeben wird, wird die erste Zahl als die minimale Anzahl der zu startenden Instances und die zweite als die maximale Anzahl der zu startenden Instances interpretiert.
- `--image-id` — Die Snowball-AMI-ID des AMI, die Sie durch einen Anruf abrufen können. `describe-images` Um eine Instance zu starten, wird ein AMI benötigt.
- `-- InstanceInitiatedShutdownBehavior` — Wenn Sie von Ihrer Instance aus ein Herunterfahren einleiten (mit einem Befehl wie `Shutdown` oder `Poweroff`), wird die Instance standardmäßig gestoppt. Sie können das Verhalten stattdessen ändern, sodass sie beendet wird. Die Parameter `stop` und `terminate` werden unterstützt. Der Standardwert ist `stop`. Weitere Informationen finden Sie unter [Ändern des Verhaltens beim initiierten Herunterfahren der Instance](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.

- `--instance-type` – Der sbe-Instance-Typ.
- `--launch-template structure` — Die Startvorlage, die zum Starten der Instances verwendet werden soll. Alle Parameter, die Sie im Befehl `run-instances` angeben, überschreiben die entsprechenden Parameter in der Startvorlage. Sie können den Namen oder die ID einer Einführungsvorlage angeben, jedoch nicht beides.

```
{
  "LaunchTemplateId": "string",
  "LaunchTemplateName": "string",
  "Version": "string"
}
```

- `--security-group-ids` — Eine oder mehrere Sicherheitsgruppen. IDs Sie können eine Sicherheitsgruppe erstellen mit [CreateSecurityGroup](#). Wenn kein Wert angegeben wird, wird die ID für die Standard-Sicherheitsgruppe den erstellten Instances zugewiesen.
- `--tag-specifications` — Die Tags, die beim Start auf die Ressourcen angewendet werden sollen. Instances können nur beim Start markiert werden. Die angegebenen Tags werden auf alle Instances angewendet, die beim Start erstellt werden. Um eine Ressource mit einem Tag zu versehen, nachdem sie erstellt wurde, verwenden Sie `create-tags`.
- `--user-data` — Die Benutzerdaten, die der Instanz zur Verfügung gestellt werden sollen. Wenn Sie die verwenden AWS CLI, wird die Base64-Kodierung für Sie durchgeführt, und Sie können den Text aus einer Datei laden. Andernfalls müssen Sie einen base64-kodierten Text bereitstellen.
- `--key-name (string)` — Der Name des key pair. Sie können ein key pair mit `CreateKeyPair` oder `importKeyPair` erstellen.

Warning

Wenn Sie kein key pair angeben, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI, das so konfiguriert ist, dass Benutzer sich auf andere Weise anmelden können.

- [start-instances](#) — Startet eine sbe Instance, die Sie zuvor gestoppt haben. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.
- `--instance-ids` — Die einer oder IDs mehrerer sbe Instanzen, die auf dem Gerät gestoppt wurden.

- [stop-instances](#) — Stoppt eine Instanz, die gerade läuft. Alle der Instanz zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instanz beendet wird.
- `--instance-ids` — Die IDs mehrerer Instanzen, die auf dem Gerät gestoppt werden sollen.
- [terminate-instances](#) — **Führt** eine oder mehrere Instanzen herunter. Dieser Vorgang ist idempotent. Wenn Sie eine Instanz mehr als einmal beenden, ist jeder Aufruf erfolgreich. Alle der Instanz zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Die Daten werden jedoch gelöscht, wenn die Instanz beendet wird.

Note

Wenn Sie einen Befehl wie `shutdown` oder `poweroff` zum Starten des Herunterfahrens über Ihre Instanz verwenden, wird die Instanz standardmäßig angehalten. Sie können das `InstanceInitiatedShutdownBehavior` Attribut jedoch verwenden, um dieses Verhalten so zu ändern, dass diese Befehle Ihre Instanz beenden. Weitere Informationen finden Sie unter [Ändern des Verhaltens beim initiierten Herunterfahren der Instanz](#) im EC2 Amazon-Benutzerhandbuch für Linux-Instanzen.

- `--instance-ids` — Die IDs mehrerer Instanzen, die auf dem Gerät beendet werden sollen. Alle für diese Instanzen gespeicherten Daten gehen verloren.
- [create-key-pair](#) — Erzeugt ein 2048-Bit-RSA-Schlüsselpaar mit dem angegebenen Namen. Amazon EC2 speichert den öffentlichen Schlüssel und zeigt den privaten Schlüssel an, den Sie in einer Datei speichern können. Der private Schlüssel wird als unverschlüsselter, PEM-codierter PKCS #1 -Schlüssel zurückgegeben. Wenn ein Schlüssel mit dem angegebenen Namen bereits existiert, gibt Amazon einen Fehler zurück.
- `--key-name` (string) — Ein eindeutiger Name für das key pair.

Einschränkungen: Bis zu 255 ASCII-Zeichen.

- `[--tag-specifications]` (Liste) — Die Tags, die auf das neue key pair angewendet werden sollen.

```
{
  "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
  "Tags": [
    {
      "Key": "string",
```



```

        "Value": "string"
    }
    ...
]
}
...

```

- [import-key-pair](#) –

- `--key-name` (string) — Ein eindeutiger Name für das key pair.

Einschränkungen: Bis zu 255 ASCII-Zeichen.

- `--public-key-material` (blob) — Der öffentliche Schlüssel. Für API-Aufrufe muss der Text Base64-codiert sein. Bei Befehlszeilentools wird die Base64-Kodierung für Sie durchgeführt.
- `[--tag-specifications]` (Liste) — Die Tags, die auf das neue key pair angewendet werden sollen.

```

{
  "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
    ...
  ]
}

```

- [describe-key-pairs](#) –

`[--filters]` (Liste) — Die Filter.

- `key-pair-id` — Die ID des key pair.
- Schlüsselname — Der Name des key pair.
- `tag-key` — Der Schlüssel eines Tags, das der Ressource zugewiesen ist. Verwenden Sie diesen Filter, um alle Ressourcen zu finden, denen ein Tag mit einem bestimmten Schlüssel zugewiesen wurde, unabhängig vom Tag-Wert.
- `[--tag-specifications]` (Liste) — Die Tags, die auf das neue key pair angewendet werden sollen.
- `tag:key` — Die key/value Kombination eines der Ressource zugewiesenen Tags. Verwenden Sie den Tag-Schlüssel im Filternamen und den Tag-Wert als Filterwert. Um beispielsweise alle Ressourcen zu finden, die ein Tag mit dem `Owner`-Schlüssel und dem Wert `Team A` haben, geben Sie `tag:Owner` für den Filternamen und `Team A` für den Filterwert an.

```
{
  "Name": "string",
  "Values": ["string", ...]
}
...
```

- `--key-names` (list) — Die Namen der key pair.

Standard: Beschreibt alle Ihre Schlüsselpaare.

- `--key-pair-ids` (Liste) — Das IDs der Schlüsselpaare.
- [delete-key-pair](#) –
 - `--key-name` (string) — Der Name des key pair.
 - `--key-pair-id` (string) — Die ID des key pair.

Unterstützte EC2 Amazon-kompatible API-Operationen auf einem Snowball Edge

Im Folgenden finden Sie EC2 Amazon-kompatible API-Operationen, die Sie mit einem Snowball Edge verwenden können, mit Links zu ihren Beschreibungen in der Amazon EC2 API-Referenz. EC2Amazon-kompatible API-Aufrufe erfordern eine Signatur mit Signature Version 4 (Sigv4). Wenn Sie das AWS CLI oder ein AWS SDK für diese API-Aufrufe verwenden, wird die SigV4-Signatur für Sie übernommen. Andernfalls müssen Sie Ihre eigene SigV4 Signatur-Lösung implementieren. Weitere Informationen finden Sie unter [Abrufen und Verwenden lokaler Amazon S3 S3-Anmeldeinformationen auf Snowball Edge](#).

- [AssociateAddress](#)— Ordnet eine Elastic IP-Adresse einer Instance oder einer Netzwerkschnittstelle zu.
- [AttachVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - Device
 - InstanceId
 - VolumeId
- [AuthorizeSecurityGroupEgress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln zur Verwendung mit einem Snowball Edge-Gerät hinzu. Insbesondere ermöglicht diese Aktion Instances, Datenverkehr an einen oder mehrere IPv4 CIDR-Zieladressbereiche zu senden.

- [AuthorizeSecurityGroupIngress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Eingangsregeln hinzu. Beim Aufrufen `AuthorizeSecurityGroupIngress` müssen Sie entweder einen Wert für `GroupName` oder `GroupId` angeben.
- [CreateVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `SnapshotId`
 - `Size`
 - `VolumeType`
 - `TagSpecification.N`
- [CreateLaunchTemplate](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `ImageId`
 - `InstanceType`
 - `SecurityGroupIds`
 - `TagSpecifications`
 - `UserData`
- [CreateLaunchTemplateVersion](#)
- [CreateTags](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `AMI`
 - `Instance`
 - `Launch template`
 - `Security group`
- [CreateSecurityGroup](#)— Erstellt eine Sicherheitsgruppe auf Ihrem Snowball Edge. Sie können bis zu 50 Sicherheitsgruppen erstellen. Wenn Sie eine Sicherheitsgruppe erstellen, geben Sie einen Anzeigenamen Ihrer Wahl an.
- [DeleteLaunchTemplate](#)
- [DeleteLaunchTemplateVersions](#)
- [DeleteSecurityGroup](#)— Löscht eine Sicherheitsgruppe. Wenn Sie versuchen, eine Sicherheitsgruppe zu löschen, die mit einer Instance verknüpft ist, oder auf die von einer anderen Sicherheitsgruppe verwiesen wird, schlägt die Operation mit `DependencyViolation` fehl.
- [DeleteTags](#)— Löscht den angegebenen Satz von Tags aus dem angegebenen Satz von Ressourcen.
- [DeleteVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `VolumeId`

- [DescribeAddresses](#)
- [DescribeImages](#)
- [DescribeInstanceAttribute](#)— Die folgenden Attribute werden unterstützt:
 - `instanceType`
 - `userData`
- [DescribeInstanceStatus](#)
- [DescribeLaunchTemplates](#)
- [DescribeLaunchTemplateVersions](#)
- [DescribeInstances](#)
- [DescribeSecurityGroups](#)— Beschreibt eine oder mehrere Ihrer Sicherheitsgruppen. `DescribeSecurityGroups` ist eine paginierte Operation. Sie können mehrere API-Aufrufe ausführen, um den gesamten Ergebnissatz abzurufen.
- [DescribeTags](#)— Mit diesem Befehl werden die folgenden Filter unterstützt:
 - `resource-id`
 - `resource-type`— Nur AMI oder Compute-Instance
 - `key`
 - `value`
- [DescribeVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `MaxResults`
 - `NextToken`
 - `VolumeId.N`
- [DetachVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
 - `Device`
 - `InstanceId`
 - `VolumeId`
- [DisassociateAddress](#)
- [GetLaunchTemplateData](#)
- [ModifyLaunchTemplate](#)
- [ModifyInstanceAttribute](#)— Nur das `userData` Attribut wird unterstützt.
- [RevokeSecurityGroupEgress](#)— Entfernt eine oder mehrere Ausgangsregeln aus einer Sicherheitsgruppe.

- [RevokeSecurityGroupIngress](#)— Widerruft eine oder mehrere Eingangsregeln für eine Sicherheitsgruppe. Beim Aufrufen `RevokeSecurityGroupIngress` müssen Sie entweder einen Wert für `group-name` oder angeben. `group-id`
- [RunInstances](#) –

 Note

Je nach Größe und Typ der Instanz kann es bis zu anderthalb Stunden dauern, bis eine Compute-Instance auf einem Snowball Edge gestartet wird.

- [StartInstances](#)
- [StopInstances](#)— Ressourcen, die einer gestoppten Instanz zugeordnet sind, bleiben bestehen. Sie können die Instance beenden, um diese Ressourcen freizugeben. Alle zugehörigen Daten werden jedoch gelöscht.
- [TerminateInstances](#)

EC2Autostart-kompatible Instances mit Startvorlagen auf einem Snowball Edge

Sie können Ihre EC2 Amazon-kompatiblen Instances auf Ihrem AWS Snowball Edge Gerät mithilfe von Startvorlagen und Startkonfigurationsbefehlen für den Snowball Edge-Client automatisch starten.

Eine Startvorlage enthält die Konfigurationsinformationen, die zum Erstellen einer EC2 Amazon-kompatiblen Instance auf Ihrem Snowball Edge erforderlich sind. Sie können eine Startvorlage verwenden, um Startparameter zu speichern, sodass Sie sie nicht jedes Mal angeben müssen, wenn Sie eine EC2 -kompatible Instance auf Ihrem Snowball Edge starten.

Wenn Sie Autostart-Konfigurationen auf Ihrem Snowball Edge verwenden, konfigurieren Sie die Parameter, mit denen Ihre EC2 Amazon-kompatible Instance beginnen soll. Wenn Ihr Snowball Edge nach der Konfiguration neu gestartet und entsperrt wird, verwendet es Ihre Autostart-Konfiguration, um eine Instance mit den von Ihnen angegebenen Parametern zu starten. Wenn eine von Ihnen mithilfe einer Autostart-Konfiguration gestartete Instance angehalten wird, wird die Instance ab dem Moment ausgeführt, in dem Sie Ihr Gerät entsperren.

 Note

Starten Sie Ihr Gerät nach der Konfiguration einer Autostart-Konfiguration neu, um sie zu starten. Alle nachfolgenden Instanzstarts (nach geplanten oder ungeplanten Neustarts) erfolgen automatisch, nachdem Ihr Gerät entsperrt wurde.

Eine Startvorlage kann die Amazon Machine Image (AMI) -ID, den Instance-Typ, Benutzerdaten, Sicherheitsgruppen und Tags für eine EC2 Amazon-kompatible Instance angeben, wenn Sie diese Instance starten. Eine Liste mit unterstützten Instance-Typen finden Sie unter [Kontingente für Recheninstanzen auf einem Snowball Edge-Gerät](#).

Gehen Sie wie folgt vor, um automatisch EC2 -kompatible Instances auf Ihrem Snowball Edge zu starten:

1. Wenn Sie Ihr AWS Snowball Edge Gerät bestellen, erstellen Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts mit Recheninstanzen. Weitere Informationen finden Sie unter [Einen Job erstellen, um einen Snowball Edge zu bestellen](#).
2. Nachdem Sie Ihren Snowball Edge erhalten haben, entsperren Sie ihn.
3. Verwenden Sie den API-Befehl `EC2-compatibleaws ec2 create-launch-template`, um eine Startvorlage zu erstellen.
4. Verwenden Sie den Snowball Edge-Client-Befehl `snowballEdge create-autostart-configuration`, um Ihre EC2 -kompatible Instanzstartvorlage an Ihre Netzwerkkonfiguration zu binden. Weitere Informationen finden Sie unter [Eine EC2 -kompatible Startkonfiguration auf einem Snowball Edge erstellen](#).
5. Starten Sie Ihr Gerät neu und entsperren Sie es anschließend. Ihre EC2 -kompatiblen Instances werden automatisch mit den Attributen gestartet, die in Ihrer Startvorlage und Ihrem Snowball Edge-Client-Befehl angegeben sind. `create-autostart-configuration`

Verwenden Sie den API-Befehl `EC2-compatible`, um den Status Ihrer laufenden Instances anzuzeigen. `describe-autostart-configurations`

 Note

Es gibt keine Konsole oder Job-Management-API zur AWS Snowball Edge Unterstützung von Startvorlagen. Sie verwenden die EC2 CLI-Befehle `-compatible` und Snowball Edge Client, um automatisch EC2 -kompatible Instanzen auf Ihrem Gerät zu starten. AWS Snowball Edge

Verwenden von Instance Metadata Service for Snow mit EC2 Amazon-kompatiblen Instances auf einem Snowball Edge

IMDS for Snow bietet den Instance Metadata Service (IMDS) für EC2 Amazon-kompatible Instances auf Snow. Instance-Metadaten sind Kategorien von Informationen über Instances. Dazu gehören Kategorien wie Hostname, Ereignisse und Sicherheitsgruppen. Mit IMDS for Snow können Sie Instance-Metadaten verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Start Ihrer Amazon EC2 -kompatiblen Instance angegeben haben. Sie können beispielsweise IMDS for Snow verwenden, um Parameter für die Konfiguration Ihrer Instance anzugeben, oder diese Parameter in ein einfaches Skript aufnehmen. Sie können generische Dateien erstellen AMIs und Benutzerdaten verwenden, um die beim Start bereitgestellten Konfigurationsdateien zu ändern.

Informationen zu Instanz-Metadaten und Benutzerdaten sowie EC2 Snow-kompatiblen Instances finden Sie unter [Unterstützte Instanz-Metadaten und Benutzerdaten](#) in diesem Handbuch.

 Important

Sie können nur innerhalb der Instance selbst auf Instance-Metadaten und Benutzerdaten zugreifen. Die Daten sind nicht durch Authentifizierungs- oder kryptografische Verfahren geschützt. Jeder, der direkten Zugriff auf die Instance hat, und möglicherweise auch jede Software, die auf der Instance läuft, kann deren Metadaten einsehen. Daher sollten Sie sensible Daten wie Passwörter oder langlebige Verschlüsselungscodes nicht als Benutzerdaten speichern.

 Note

Die Beispiele in diesem Abschnitt verwenden die IPv4 Adresse des Instanz-Metadatendienstes: 169.254.169.254. Wir unterstützen das Abrufen von Instanz-Metadaten unter Verwendung der Link-Local-Adresse nicht. IPv6

Themen

- [IMDS-Versionen auf einem Snowball Edge](#)
- [Beispiele für das Abrufen von Instanz-Metadaten mit IMDSv1 und IMDSv2 auf einem Snowball Edge](#)

IMDS-Versionen auf einem Snowball Edge

Mit IMDS Version 2 oder IMDS Version 1 können Sie von einer laufenden Instanz aus auf Instanz-Metadaten zugreifen:

- Instance Metadata Service Version 2 (IMDSv2), eine sitzungsorientierte Methode
- Instance Metadata Service Version 1 (IMDSv1), eine Anfrage-Antwort-Methode

Je nach Version Ihrer Snow-Software können Sie IMDSv2, oder IMDSv1 beide verwenden. Dies hängt auch vom Typ des AMI ab, das in der EC2 -kompatiblen Instance ausgeführt wird. Einige AMIs, z. B. solche, auf denen Ubuntu 20.04 ausgeführt wird, erfordern. IMDSv2 Der Instanz-Metadatendienst unterscheidet zwischen IMDSv1 und IMDSv2 Anfragen anhand des Vorhandenseins von PUT Oder-Headern. GET IMDSv2verwendet diese beiden Header. IMDSv1 verwendet nur den GET Header.

AWS befürwortet die Verwendung von IMDSv2 statt IMDSv1 , weil IMDSv2 beinhaltet eine höhere Sicherheit. Weitere Informationen finden [Sie unter Umfassender Schutz vor offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen am Instanz-Metadatendienst](#). EC2

IMDSv2 auf einer Schneeballkante

Wenn Sie IMDSv2 Instanz-Metadaten anfordern, muss die Anfrage diesen Regeln entsprechen:

1. Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance-Metadaten-Service zu starten. Die PUT Anfrage gibt ein Sitzungstoken zurück, das in nachfolgenden GET Anfragen an

den Instanz-Metadatendienst enthalten sein muss. Das Sitzungstoken, das die Sitzungsdauer definiert. Die Sitzungsdauer kann mindestens eine Sekunde und maximal sechs Stunden betragen. Während dieser Dauer können Sie dasselbe Sitzungstoken für nachfolgende Anfragen verwenden. Nach Ablauf dieser Dauer müssen Sie ein neues Sitzungstoken für future Anfragen erstellen. Das Token ist erforderlich, um mithilfe von auf Metadaten zuzugreifen IMDSv2.

2. Nehmen Sie das Token in alle GET-Anfragen an den Instance-Metadaten-Service auf.
 - a. Das Token ist ein instanzspezifischer Schlüssel. Das Token ist auf anderen EC2 -kompatiblen Instances nicht gültig und wird zurückgewiesen, wenn Sie versuchen, es außerhalb der Instanz zu verwenden, auf der es generiert wurde.
 - b. Die PUT-Anfrage muss einen Header enthalten, der die Time To Live (TTL) für das Token in Sekunden bis zu maximal sechs Stunden (21 600 Sekunden) angibt. Das Token stellt eine logische Sitzung dar. Die TTL gibt die Gültigkeitsdauer des Token und damit die Dauer der Sitzung an.
 - c. Nachdem ein Token abgelaufen ist, müssen Sie eine neue Sitzung mit einer anderen PUT-Anfrage erstellen, um auf die Instance-Metadaten zuzugreifen.
 - d. Sie können auswählen, ob Sie ein Token wiederverwenden oder bei jeder Anforderung einen neues Token erstellen möchten. Für eine kleine Anzahl von Anfragen kann es einfacher sein, bei jedem Zugriff auf den Instance-Metadaten-Service ein Token zu generieren und sofort zu verwenden. Aus Effizienzgründen können Sie jedoch eine längere Dauer für das Token festlegen und es wiederverwenden, anstatt jedes Mal eine PUT-Anfrage stellen zu müssen, wenn Sie Instance-Metadaten anfordern müssen. Es gibt keine praktische Begrenzung der Anzahl der gleichzeitigen Tokens, die jeweils eine eigene Sitzung darstellen.

HTTP GET und HEAD Methoden sind in Anfragen zu IMDSv2 Instanz-Metadaten zulässig. PUTAnfragen werden abgelehnt, wenn sie einen X-Forwarded-For Header enthalten.

Standardmäßig hat die Antwort auf PUT Anfragen ein Response-Hop-Limit (Time-to-Live) von 1 auf IP-Protokollebene. IMDS for Snow ist nicht in der Lage, das Hop-Limit für PUT Antworten zu ändern.

Das folgende Beispiel verwendet ein Linux-Shell-Skript und ruft die IMDSv2 Metadatenelemente der Instanz auf oberster Ebene ab. Dieses Beispiel:

1. Erstellt mithilfe der PUT Anfrage ein Sitzungstoken mit einer Dauer von sechs Stunden (21.600 Sekunden).
2. Speichert den Sitzungs-Token-Header in einer Variablen mit dem NamenTOKEN.
3. Fordert mithilfe des Tokens die Metadatenelemente der obersten Ebene an.

Verwenden Sie zwei Befehle, um das EC2 -kompatible Token zu generieren. Sie können die Befehle separat oder als einen Befehl ausführen.

Generieren Sie zuerst ein Token mit dem folgenden Befehl.

 Note

X-aws-ec2-metadata-token-ttl-seconds ist ein erforderlicher Header. Wenn dieser Header nicht enthalten ist, erhalten Sie den Fehlercode 400 — Fehlende oder ungültige Parameter.

```
[ec2-user ~]$ TOKEN=curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"
```

Verwenden Sie dann das Token, um mithilfe des folgenden Befehls Metadatenelemente der obersten Ebene zu generieren.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

 Note

Wenn beim Erstellen des Tokens ein Fehler auftritt, wird in der Variablen statt eines gültigen Tokens eine Fehlermeldung gespeichert und der Befehl funktioniert nicht.

Sie können das Token speichern und die Befehle kombinieren. Das folgende Beispiel kombiniert die beiden obigen Befehle und speichert den Sitzungs-Token-Header in einer Variablen namens `TOKEN`.

Example von kombinierten Befehlen

```
[ec2-user ~]$ TOKEN=curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Der folgende Beispielbefehl ruft die ID des AMI ab, das zum Starten der Instance verwendet wurde, und speichert sie in dem im vorherigen Beispiel \$TOKEN erstellten.

Example der Wiederverwendung eines Tokens

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
```

IMDSv1 auf einer Schneebalkante

IMDSv1 verwendet das Request-Response-Modell. Um Instanz-Metadaten anzufordern, senden Sie eine GET Anfrage an den Instanz-Metadatendienst.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Ihre Instance-Metadaten sind in Ihrer laufenden Instance verfügbar, sodass Sie nicht die EC2 Amazon-Konsole oder die verwenden müssen AWS CLI , um darauf zuzugreifen. Dies kann sehr hilfreich sein, wenn Sie ein Skript schreiben möchten, das in der Instance ausgeführt werden soll. So können Sie z. B. über die Instance-Metadaten auf die lokale IP-Adresse Ihrer Instance zugreifen, um die Verbindung zu einer externen Anwendung zu verwalten. Instance-Metadaten werden in vier Kategorien unterteilt. Eine Beschreibung der einzelnen Instance-Metadatenkategorien finden Sie unter [Unterstützte Instance-Metadaten und Benutzerdaten](#) in diesem Handbuch.

Verwenden Sie den folgenden IPv4 URI, um alle Kategorien von Instanz-Metadaten innerhalb einer laufenden Instance anzuzeigen:

```
http://169.254.169.254/latest/meta-data/
```

Die IP-Adressen sind lokale Adressen (Link-local Addresses) und nur von der Instance aus gültig. Weitere Informationen finden Sie unter [Link-local address](#) in Wikipedia.

Alle Instance-Metadaten werden als Text zurückgegeben (HTTP-Inhaltstyp text/plain).

Eine Anfrage nach einer bestimmten Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode 404 — Not Found zurück, falls die Ressource nicht verfügbar ist.

Eine Anfrage nach einer allgemeinen Metadatenressource (wenn der URI mit einem / Zeichen endet) gibt eine Liste verfügbarer Ressourcen zurück oder einen HTTP-Fehlercode 404 — Not Found, wenn es keine solche Ressource gibt. Die Listenelemente befinden sich in separaten Zeilen, die durch Zeilenvorschübe (ASCII-Zeichencode 10) abgeschlossen werden.

Für Anfragen, die mit gestellt wurden IMDSv1, können die folgenden HTTP-Fehlercodes zurückgegeben werden:

- 400 - Fehlende oder ungültige Parameter — Die PUT Anfrage ist nicht gültig.
- 401 - Nicht autorisiert — Die GET Anfrage verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.
- 403 - Forbidden — Die Anfrage ist nicht zulässig oder der Instanz-Metadatendienst ist deaktiviert.

Beispiele für das Abrufen von Instanz-Metadaten mit IMDSv1 und IMDSv2 auf einem Snowball Edge

Die folgenden Beispiele enthalten Befehle, die Sie für eine Linux-Instance verwenden können.

Example zum Abrufen der verfügbaren Versionen der Instanz-Metadaten

In diesem Beispiel werden die verfügbaren Versionen der Instance-Metadaten abgerufen. Jede Version bezieht sich auf einen Instance-Metadaten-Build, wenn neue Instance-Metadatenkategorien veröffentlicht wurden. Es stehen frühere Versionen zur Verfügung, für den Fall dass Skripte angewendet werden, die auf den Strukturen und Daten dieser früheren Versionen aufbauen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H  
"X-aws-ec2-metadata-token-ttl-seconds: 21600" ` && curl -H "X-aws-ec2-metadata-token:  
$TOKEN" -v http://169.254.169.254/
```

```

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload  Total    Spent    Left  Speed
100      56    100      56      0      0      3733    0    --:--:--
--:--:-- --:--:-- 3733
*   Trying 169.254.169.254...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET / HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.61.1
> Accept: */*
> X-aws-ec2-metadata-token:
MDAXcxNFLbAwJIYx8KzgNckcHTdxT4Tt69TzpKExlXKTULHIQnjEtXvD
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Date: Mon, 12 Sep 2022 21:58:03 GMT
< Content-Length: 274
< Content-Type: text/plain
< Server: EC2ws
<
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27

```

```
2021-01-03
2021-03-23
* Closing connection 0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
latest
```

Example zum Abrufen der Metadatenelemente der obersten Ebene

In diesem Beispiel werden die Metadatenelemente der obersten Ebene abgerufen. Informationen zu Metadatenelementen der obersten Ebene finden Sie in diesem Handbuch unter [Unterstützte Instanz-Metadaten und Benutzerdaten](#).

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
"X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token:
$TOKEN" -v http://169.254.169.254/latest/meta-data/
ami-id
hostname
instance-id
instance-type
local-hostname
local-ipv4
mac
network/
reservation-id
security-groups
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
hostname
instance-id
instance-type
local-hostname
local-ipv4
mac
network/
reservation-id
security-groups
```

Example zum Abrufen von Werten von Metadaten der obersten Ebene

In den folgenden Beispielen werden die Werte einiger der Metadatenelemente der obersten Ebene abgerufen, die im vorherigen Beispiel abgerufen wurden. Die IMDSv2 Anfragen verwenden das gespeicherte Token, das im vorherigen Beispielbefehl erstellt wurde, vorausgesetzt, es ist nicht abgelaufen.

ami-id IMDSv2

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id ami-0abcdef1234567890
```

ami-id IMDSv1

```
curl http://169.254.169.254/latest/meta-data/ami-id ami-0abcdef1234567890
```

reservation-id IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/reservation-id r-0efghijk987654321
```

reservation-id IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id \r-0efghijk987654321
```

local-hostname IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/local-hostname ip-00-000-00-00
```

local-hostname IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname ip-00-000-00-00
```


Blockspeicher mit EC2 Amazon-kompatiblen Instances auf Snowball Edge verwenden

Mit Blockspeicher auf Snowball Edge können Sie Blockspeicher je nach den Anforderungen Ihrer Anwendungen hinzufügen oder entfernen. Volumes, die an eine EC2 Amazon-kompatible Instance angehängt sind, werden als Speichervolumes bereitgestellt, die unabhängig von der Lebensdauer der Instance bestehen bleiben. Sie können Blockspeicher mit der vertrauten Amazon EBS-API verwalten.

Bestimmte Amazon EBS-Befehle werden durch die Verwendung des EC2 -kompatiblen Endpunkts unterstützt. Unterstützte Befehle sind `attach-volume`, `create-volume`, `delete-volume`, `detach-volume` und `describe-volumes`. Weitere Informationen zu diesen Befehlen finden Sie unter [Liste der unterstützten EC2 -kompatiblen AWS CLI Befehle auf einem Snowball Edge](#)

Important

Stellen Sie sicher, dass Sie alle Dateisysteme auf dem Gerät innerhalb Ihres Betriebssystems demounten, bevor Sie das Volume trennen. Andernfalls kann es zu Datenverlusten kommen.

Im Folgenden finden Sie Amazon EBS-Volumenkontingente und Unterschiede zwischen Amazon EBS-Volumes auf Ihrem Gerät und Amazon EBS-Volumes in der Cloud:

- Amazon EBS-Volumes sind nur für EC2 -kompatible Instances verfügbar, die auf dem Gerät laufen, das die Volumes hostet.
- Die Volume-Typen sind entweder auf kapazitätsoptimierte Festplatten (`sbp1`) oder leistungsoptimierte SSDs (`sbp1`) beschränkt. Der Standard-Volume-Typ ist `sbp1`.
- Snowball Edge teilt Festplattenspeicher zwischen Amazon S3 S3-Objekten und Amazon EBS. Wenn Sie HDD-basierten Blockspeicher auf verwenden AWS Snowball Edge, wird dadurch der für Amazon S3 S3-Objekte verfügbare Speicherplatz reduziert. Ebenso reduzieren Amazon S3 S3-Objekte die Menge an Speicher, die für Amazon EBS-Blockspeicher auf HDD-Volumes verfügbar ist.
- Amazon EC2 -kompatible Root-Volumes verwenden immer den IDE-Treiber. Zusätzliche Amazon EBS-Volumes verwenden bevorzugt den Virtio-Treiber, falls verfügbar. Wenn der Virtio-Treiber nicht verfügbar ist, verwendet SBE standardmäßig den IDE-Treiber. Der Virtio-Treiber ermöglicht eine bessere Leistung und wird daher empfohlen.

- Beim Erstellen von Amazon EBS-Volumes wird der encrypted Parameter nicht unterstützt. Jedoch werden alle Daten auf Ihrem Gerät standardmäßig verschlüsselt.
- Volumes können eine Größe zwischen 1 GB und 10 TB aufweisen.
- Bis zu 10 Amazon EBS-Volumes können an eine einzige EC2 kompatible Instance angehängt werden.
- Es gibt kein formelles Limit für die Anzahl der Amazon EBS-Volumes, die Sie auf Ihrem AWS Snowball Edge Gerät haben können. Die gesamte Amazon EBS-Volumenkapazität ist jedoch durch den verfügbaren Speicherplatz auf Ihrem Gerät begrenzt.

Steuern des Netzwerkverkehrs mit Sicherheitsgruppen auf Snowball Edge

Eine Sicherheitsgruppe agiert als virtuelle Firewall, die den Datenverkehr für eine oder mehrere Instances steuert. Beim Start einer Instance verknüpfen Sie diese mit mindestens einer Sicherheitsgruppe. Sie können jeder Sicherheitsgruppe Regeln hinzufügen, um den Datenaustausch mit den ihr zugeordneten Instances zu ermöglichen. Weitere Informationen finden Sie unter [EC2 Amazon-Sicherheitsgruppen für Linux-Instances](#) im EC2 Amazon-Benutzerhandbuch.

Sicherheitsgruppen auf Snowball Edge-Geräten ähneln Sicherheitsgruppen in der AWS Cloud. Virtuelle private Clouds (VPCs) werden auf Snowball Edge-Geräten nicht unterstützt.

Im Folgenden finden Sie die weiteren Unterschiede zwischen Snowball Edge-Sicherheitsgruppen und EC2 VPC-Sicherheitsgruppen:

- Jedes Snowball Edge-Gerät hat ein Limit von 50 Sicherheitsgruppen.
- Die Standard-Sicherheitsgruppe lässt den gesamten ein- und ausgehenden Datenverkehr zu.
- Für den Datenverkehr zwischen lokalen Instances kann entweder die private Instance-IP-Adresse oder eine öffentliche IP-Adresse verwendet werden. Angenommen, Sie möchten per SSH eine Verbindung von Instance A mit Instance B herstellen. In diesem Fall kann Ihre Ziel-IP-Adresse entweder die öffentliche IP-Adresse oder die private IP-Adresse der Instance B sein, sofern die Sicherheitsgruppenregel den Datenverkehr zulässt.
- Nur die für AWS CLI Aktionen und API-Aufrufe aufgelisteten Parameter werden unterstützt. Dabei handelt es sich in der Regel um eine Teilmenge der in EC2 VPC-Instances unterstützten Komponenten.

Weitere Informationen zu unterstützten AWS CLI Aktionen finden Sie unter [Liste der unterstützten EC2 -kompatiblen AWS CLI Befehle auf einem Snowball Edge](#). Weitere Informationen zu unterstützten API-Operationen finden Sie unter [Unterstützte EC2 Amazon-kompatible API-Operationen auf einem Snowball Edge](#).

Unterstützte EC2 -kompatible Instanzmetadaten und Benutzerdaten auf Snowball Edge

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Snowball Edge unterstützt eine Teilmenge von Instanz-Metadatenkategorien für Ihre Recheninstanzen. Weitere Informationen finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im EC2 Amazon-Benutzerhandbuch.

Die folgenden Kategorien werden unterstützt. Bei Verwendung anderer Kategorien wird eine 404 Fehlermeldung zurückgegeben.

Unterstützte Instanz-Metadatenkategorien auf einem Snowball Edge-Gerät

Daten	Beschreibung
<code>ami-id</code>	Die für den Start der Instance verwendete AMI-ID
<code>hostname</code>	Der private IPv4 DNS-Hostname der Instanz.
<code>instance-id</code>	Die ID dieser Instance
<code>instance-type</code>	Der Typ der Instance.
<code>local-hostname</code>	Der private IPv4 DNS-Hostname der Instanz.
<code>local-ipv4</code>	Die private IPv4 Adresse der Instanz.
<code>mac</code>	Die Media Access Control-Adresse (MAC) der Instance.
<code>network/interfaces/macs/ <i>mac</i> /local-hostname</code>	Der lokale Hostname der Schnittstelle

Daten	Beschreibung
network/interfaces/macs/ <i>mac</i> /local-ipv4s	Die privaten IPv4 Adressen, die der Schnittstelle zugeordnet sind.
network/interfaces/macs/ <i>mac</i> /mac	Die MAC-Adresse der Instance
network/interfaces/macs/ <i>mac</i> /public-ipv4s	Die Elastic IP-Adressen, die mit der Schnittstelle verknüpft sind.
public-ipv4	Die öffentliche IPv4 Adresse.
public-keys/0/openssh-key	Der öffentliche Schlüssel. Nur verfügbar, wenn bei der Instance-Startzeit angegeben.
reservation-id	Die ID der Reservierung
userData	Shell-Skripts zum Übermitteln von Anweisungen an eine Instance beim Start.

Unterstützte dynamische Instanzdatenkategorien auf einem Snowball Edge-Gerät

Daten	Beschreibung
instance-identity/document	JSON-Daten mit Instance-Attributen. Nur <code>instanceId</code> , <code>imageId</code> , <code>privateIp</code> und <code>instanceType</code> verfügen über Werte, und die anderen zurückgegebenen Attribute sind auf Null gesetzt. Weitere Informationen finden Sie unter Instance Identity Documents im EC2 Amazon-Benutzerhandbuch.

Benutzerdaten der Computerinstanz auf Snowball Edge

Verwenden Sie Shell-Skripts, um auf Benutzerdaten von Compute-Instanzen auf einem Snowball Edge-Gerät zuzugreifen. Durch die Nutzung von Shell-Skripts können Sie einer Instance beim Start Anweisungen übermitteln. Sie können Benutzerdaten mit dem `modify-instance-attribute` AWS CLI Befehl oder der `ModifyInstanceAttribute` API-Aktion ändern.

So ändern Sie Benutzerdaten

1. Stoppen Sie Ihre Recheninstanz mit dem `stop-instances` AWS CLI Befehl.
2. Ändern Sie das `userData` Attribut mithilfe des `modify-instance-attribute` AWS CLI Befehls.
3. Starten Sie Ihre Compute-Instanz mit dem `start-instances` AWS CLI Befehl neu.

Für Compute-Instances werden nur Shell-Skripte unterstützt. `cloud-init` Paketdirektiven auf Compute-Instances, die auf einem Snowball Edge-Gerät ausgeführt werden, werden nicht unterstützt. Weitere Informationen zum Arbeiten mit AWS CLI Befehlen finden Sie in der [AWS CLI Befehlsreferenz](#).

Stoppen von EC2 -kompatiblen Instanzen, die auf Snowball Edge ausgeführt werden

Um zu verhindern, dass die EC2 Amazon-kompatiblen Instances, die Sie auf einem Gerät erstellen, versehentlich gelöscht werden, sollten Sie Ihre Instances nicht über das Betriebssystem herunterfahren. Beispielsweise dürfen Sie die Befehle `shutdown` oder `reboot` nicht verwenden. Das Herunterfahren einer Instance über das Betriebssystem hat den gleichen Effekt wie der Aufruf des Befehls [terminate-instances](#).

Verwenden Sie stattdessen den Befehl [stop-instances](#), um Amazon EC2 -kompatible Instances zu sperren, die Sie beibehalten möchten.

Wird verwendet AWS IoT Greengrass , um vorinstallierte Software auf EC2 Amazon-kompatiblen Instances auf Snowball Edge auszuführen

AWS IoT Greengrass ist ein Open-Source-Edge-Runtime- und Cloud-Dienst für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können. Sie können AWS IoT Greengrass damit Software entwickeln, die es Ihren Geräten ermöglicht, lokal auf die von ihnen generierten Daten zu reagieren, Vorhersagen auf der Grundlage von Modellen für maschinelles Lernen auszuführen und Gerätedaten zu filtern und zu aggregieren. Ausführliche Informationen zu AWS IoT Greengrass finden Sie unter [Was ist AWS IoT Greengrass?](#) im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

Durch die Verwendung AWS IoT Greengrass auf Ihrem Snowball Edge-Gerät ermöglichen Sie es dem Gerät, Daten näher am Ort ihrer Entstehung zu sammeln und zu analysieren, autonom auf lokale Ereignisse zu reagieren und sicher mit anderen Geräten im lokalen Netzwerk zu kommunizieren.

Einrichtung einer EC2 Amazon-kompatiblen Instance für AWS IoT Greengrass auf einem Snowball Edge

Note

Um die Installation AWS IoT Greengrass Version 2 auf einem Snowball Edge-Gerät durchzuführen, stellen Sie sicher, dass Ihr Gerät mit dem Internet verbunden ist. Nach der Installation ist kein Internet erforderlich, damit ein Snowball Edge-Gerät funktioniert. AWS IoT Greengrass

Um eine EC2 -kompatible Instanz einzurichten für AWS IoT Greengrass V2

1. Starten Sie das AWS IoT Greengrass validierte AMI mit einer öffentlichen IP-Adresse und einem SSH-Schlüssel:
 - a. Verwenden der AWS CLI: [Run-Instances](#).
 - b. Verwenden AWS OpsHub: [Starten einer Amazon EC2 -kompatiblen Instance](#).

 Note

Notieren Sie sich die öffentliche IP-Adresse und den SSH-Schlüsselnamen, die der Instance zugeordnet sind.

2. Stellen Sie mithilfe von SSH eine Connect zur EC2 -kompatiblen Instanz her. Führen Sie dazu den folgenden Befehl auf dem Computer aus, der mit Ihrem Gerät verbunden ist. *ssh-key* Ersetzen Sie ihn durch den Schlüssel, den Sie zum Starten der EC2 -kompatiblen Instanz verwendet haben. *public-ip-address* Ersetzen Sie es durch die öffentliche IP-Adresse der EC2 -kompatiblen Instanz.

```
ssh -i ssh-key ec2-user@ public-ip-address
```

 Important

Wenn Ihr Computer eine frühere Version von Microsoft Windows verwendet, verfügen Sie möglicherweise nicht über den Befehl SSH, oder Sie haben SSH, können aber keine Verbindung zu Ihrer EC2 -kompatiblen Instanz herstellen. Um eine Verbindung zu Ihrer EC2 -kompatiblen Instanz herzustellen, können Sie PuTTY installieren und konfigurieren. Dabei handelt es sich um einen kostenlosen Open-Source-SSH-Client. Sie müssen den SSH-Schlüssel vom .pem Format in das PuTTY-Format konvertieren und eine Verbindung zu Ihrer EC2 Instance herstellen. Anweisungen zur Konvertierung vom .pem PuTTY-Format finden Sie unter [Konvertieren Ihres privaten Schlüssels mithilfe von PuTTYgen](#) im EC2 Amazon-Benutzerhandbuch.

Installation AWS IoT Greengrass auf einer EC2 -kompatiblen Instanz auf einem Snowball Edge

Als Nächstes richten Sie Ihre EC2 -kompatible Instanz als AWS IoT Greengrass Core-Gerät ein, das Sie für die lokale Entwicklung verwenden können.

Um zu installieren AWS IoT Greengrass

1. Verwenden Sie den folgenden Befehl, um die erforderliche Software für zu installieren AWS IoT Greengrass. Dieser Befehl installiert AWS Command Line Interface (AWS CLI) v2, Python 3 und Java 8.

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
&& unzip awscliv2.zip && sudo ./aws/install && sudo yum -y install python3
java-1.8.0-openjdk
```

2. Erteilen Sie dem Root-Benutzer die Berechtigung, die AWS IoT Greengrass Software auszuführen, und ändern Sie die Root-Rechte von root ALL=(ALL) ALL bis root ALL=(ALL:ALL) ALL in der Sudoers-Konfigurationsdatei.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Verwenden Sie den folgenden Befehl, um die AWS IoT Greengrass Core-Software herunterzuladen.

```
curl -s https://d2s8p88vqu9w66.cloudfront.net/releases/greengrass-nucleus-
latest.zip > greengrass-nucleus-latest.zip && unzip greengrass-nucleus-latest.zip -
d GreengrassCore && rm greengrass-nucleus-latest.zip
```

4. Verwenden Sie die folgenden Befehle, um Anmeldeinformationen für die Installation der AWS IoT Greengrass Core-Software bereitzustellen. Ersetzen Sie die Beispielwerte durch Ihre Anmeldeinformationen:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

Note

Dies sind Anmeldeinformationen vom IAM-Benutzer in der AWS Region, nicht vom Snowball Edge-Gerät.

5. Verwenden Sie den folgenden Befehl, um die AWS IoT Greengrass Core-Software zu installieren. Der Befehl erstellt AWS Ressourcen, die die Kernsoftware für den Betrieb benötigt, und richtet die Kernsoftware als Systemdienst ein, der beim Start des AMI ausgeführt wird.

Ersetzen Sie die folgenden Parameter im Befehl:

- **region**: Die AWS Region, in der Ressourcen gesucht oder erstellt werden sollen.
- **MyGreengrassCore**: Der Name der AWS IoT Sache für Ihr AWS IoT Greengrass Kerngerät.
- **MyGreengrassCoreGroup**: Der Name der AWS IoT Dinggruppe für Ihr AWS IoT Greengrass Kerngerät.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE \  
-jar ./GreengrassInstaller/lib/Greengrass.jar \  
--aws-region region \  
--thing-name MyGreengrassCore \  
--thing-group-name MyGreengrassCoreGroup \  
--thing-policy-name GreengrassV2IoTThingPolicy \  
--tes-role-name GreengrassV2TokenExchangeRole \  
--tes-role-alias-name GreengrassCoreTokenExchangeRoleAlias \  
--component-default-user ggc_user:ggc_group \  
--provision true \  
--setup-system-service true \  
--deploy-dev-tools true
```

Note

Dieser Befehl gilt für eine Amazon EC2 -kompatible Instance, auf der ein Amazon Linux 2-AMI ausgeführt wird. Informationen zu einem Windows-AMI finden [Sie unter Installieren der AWS IoT Greengrass Core-Software](#).

Wenn Sie fertig sind, läuft auf Ihrem Snowball Edge-Gerät ein AWS IoT Greengrass Core für Ihren lokalen Gebrauch.

Verwendung AWS Lambda mit einem AWS Snowball Edge

AWS Lambda powered by AWS IoT Greengrass ist ein Rechendienst, mit dem Sie serverlosen Code (Lambda-Funktionen) lokal auf Snowball Edge-Geräten ausführen können. Sie können Lambda verwenden, um Lambda-Funktionen auf einem Snowball Edge-Gerät mit Message Queuing Telemetry Transport (MQTT) -Nachrichten aufzurufen, Python-Code in Lambda-Funktionen auszuführen und damit öffentliche Dienstendpunkte in der Cloud aufzurufen. AWS Um Lambda-Funktionen mit Snowball Edge-Geräten verwenden zu können, müssen Sie Ihre Snowball Edge-Jobs in einem AWS-Region unterstützten von erstellen. AWS IoT Greengrass Eine Liste der gültigen finden Sie [AWS IoT Greengrass](#) in AWS-Regionen der. Allgemeine AWS-Referenz Lambda auf Snowball Edge ist in Regionen verfügbar, in denen Lambda- und Snowball Edge-Geräte verfügbar sind.

Note

Wenn Sie jeder Ihrer Funktionen die empfohlene Mindestspeichermenge von 128 MB zuweisen, können Sie bis zu sieben Lambda-Funktionen in einem einzigen Job haben.

Themen

- [Erste Schritte mit Lambda auf Snowball Edge](#)
- [Stellen Sie eine Lambda-Funktion auf einem Snowball Edge-Gerät bereit](#)

Erste Schritte mit Lambda auf Snowball Edge

Bevor Sie eine Lambda-Funktion in der Sprache Python für die Ausführung auf Ihrem Snowball Edge erstellen, empfehlen wir Ihnen, sich mit den folgenden Diensten, Konzepten und verwandten Themen vertraut zu machen.

Voraussetzungen für AWS IoT Greengrass on Snowball Edge

AWS IoT Greengrass ist Software, die AWS Cloud Funktionen auf lokale Geräte erweitert. AWS IoT Greengrass ermöglicht es lokalen Geräten, Daten näher an der Informationsquelle zu sammeln und zu analysieren und gleichzeitig in lokalen Netzwerken sicher miteinander zu kommunizieren. Genauer gesagt AWS IoT Greengrass können Entwickler, die verwenden, serverlosen Code (Lambda-

Funktionen) in der erstellen. AWS Cloud Sie können diesen Code dann einfach für Geräte zur lokalen Ausführung von Anwendungen bereitstellen.

Bei der Verwendung AWS IoT Greengrass mit einem Snowball Edge sollten Sie unbedingt die folgenden AWS IoT Greengrass Konzepte verstehen:

- AWS IoT Greengrass Anforderungen — Eine vollständige Liste der AWS IoT Greengrass Anforderungen finden Sie unter [Anforderungen](#) im AWS IoT Greengrass Version 2 Entwicklerhandbuch.
- AWS IoT Greengrass core — Laden Sie die AWS IoT Greengrass Kernsoftware herunter und installieren Sie sie auf einer EC2 Instanz, die auf dem Gerät ausgeführt wird. Weitere Informationen finden Sie in diesem Handbuch [unter Verwendung AWS IoT Greengrass auf EC2 Amazon-Instances](#).

Um Lambda-Funktionen auf einem Snowball Edge-Gerät verwenden zu können, müssen Sie zuerst die AWS IoT Greengrass Core-Software auf einer EC2 Amazon-Instance auf dem Gerät installieren. Die Lambda-Funktionen, die Sie auf dem Snowball Edge-Gerät verwenden möchten, müssen mit demselben Konto erstellt werden, das Sie für die Installation AWS IoT Greengrass auf dem Snowball Edge-Gerät verwenden werden. Informationen zur Installation AWS IoT Greengrass auf Ihrem Snowball Edge-Gerät finden Sie unter [Wird verwendet AWS IoT Greengrass , um vorinstallierte Software auf EC2 Amazon-kompatiblen Instances auf Snowball Edge auszuführen](#).

- AWS IoT Greengrass Gruppe — Ein Snowball Edge-Gerät ist Teil einer AWS IoT Greengrass Gruppe als Kerngerät der Gruppe. Weitere Informationen zu Gruppen finden Sie unter [AWS Greengrass IoT Groups](#) im AWS IoT Greengrass Developer Guide.
- MQTT — AWS IoT Greengrass verwendet das einfache, branchenübliche MQTT-Protokoll für die Kommunikation innerhalb einer Gruppe. Jedes mit MQTT kompatible Gerät oder jede Software in Ihrer AWS IoT Greengrass Gruppe kann MQTT-Nachrichten aufrufen. Diese Nachrichten können Lambda-Funktionen aufrufen, wenn Sie die zugehörige MQTT-Nachricht dafür definieren.

Voraussetzungen für AWS Lambda on Snowball Edge

AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es ist wichtig, dass Sie die folgenden Lambda-Konzepte verstehen, wenn Sie Lambda mit einem Snowball Edge verwenden:

- **Lambda-Funktionen** — Ihr benutzerdefinierter Code, der auf Lambda hochgeladen und veröffentlicht und auf einem Snowball Edge verwendet wird. Weitere Informationen finden Sie unter [Lambda-Funktionen](#) im AWS Lambda Entwicklerhandbuch.
- **Lambda-Konsole** — Die Konsole, in der Sie Ihre Lambda-Funktionen in Python-Sprache zur Verwendung auf einem Snowball Edge hochladen, aktualisieren und veröffentlichen. Weitere Informationen zur [Lambda-Konsole](#) finden Sie unter [Lambda-Konsole](#) im AWS Lambda Entwicklerhandbuch.
- **Python** — Die High-Level-Programmiersprache, die für Ihre Lambda-Funktionen verwendet wird und AWS IoT Greengrass auf einem Snowball Edge betrieben wird. AWS IoT Greengrass unterstützt Python-Version 3.8.x.

Stellen Sie eine Lambda-Funktion auf einem Snowball Edge-Gerät bereit

Um eine Lambda-Funktion auf einem Snowball Edge-Gerät in einer AWS IoT Greengrass Gruppe auszuführen, importieren Sie die Funktion als Komponente. Vollständige Informationen zum Importieren einer Funktion als Komponente mithilfe der AWS IoT Greengrass Konsole finden Sie unter [Importieren einer Lambda-Funktion als Komponente \(Konsole\)](#) im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

1. Wählen Sie in der AWS IoT-Konsole auf der Greengrass-Komponentenseite die Option Komponente erstellen aus.
2. Wählen Sie unter Komponentenquelle die Option Lambda-Funktion importieren aus. Wählen Sie in der Lambda-Funktion den Namen Ihrer Funktion aus. Wählen Sie Lambda Lambda-Funktionsversion die Version Ihrer Funktion aus.
3. Um der Funktion Nachrichten zu abonnieren, auf die sie reagieren kann, wählen Sie Ereignisquelle hinzufügen und wählen Sie das Ereignis aus. Geben Sie im Feld Timeout (Sekunden) einen Timeout-Zeitraum in Sekunden an.
4. Wählen Sie unter Fixiert aus, ob Ihre Funktion angeheftet werden soll oder nicht.
5. Wählen Sie Komponente erstellen
6. Wählen Sie Bereitstellen.
7. Wählen Sie unter Deployment die Option Zu vorhandener Bereitstellung hinzufügen und wählen Sie dann Ihre Greengrass-Gruppe aus. Wählen Sie Weiter aus.
8. Wählen Sie unter Öffentliche Komponenten die folgenden Komponenten aus:

- `aws.GreenGrass.cli`
- `aws.greengrass.LambdaLauncher`
- `aws.greengrass.LambdaManager`
- `aws.greengrass.LambdaRuntimes`
- `AWS.Greengrass.Nucleus`

9. Wählen Sie Bereitstellen.

Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge

Amazon S3 S3-kompatibler Speicher auf Snowball Edge bietet sicheren Objektspeicher mit erhöhter Stabilität, Skalierbarkeit und erweiterten Amazon S3 S3-API-Funktionen für robuste, mobile Edge-Umgebungen und unverbundene Umgebungen. Mithilfe von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge können Sie Daten speichern und hochverfügbare Anwendungen auf Snowball Edge für Edge-Computing ausführen.

Sie können Amazon S3 S3-Buckets auf den Snowball Edge-Geräten erstellen, um Objekte vor Ort für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Amazon S3-kompatibler Speicher auf Snowball Edge bietet eine neue Speicherklasse SNOW, die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Snowball Edge-Geräten zu speichern. Sie können für Snowball Edge-Buckets dieselben APIs Funktionen wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte zurückgegeben werden, werden alle Daten gelöscht AWS, die in einem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge erstellt oder gespeichert wurden. Weitere Informationen finden Sie unter [Jobs nur für lokale Datenverarbeitung und Speicherung](#).

Sie können Amazon S3 S3-kompatiblen Speicher auf Snowball Edge in einer eigenständigen Konfiguration oder in einer Cluster-Konfiguration bereitstellen. In der eigenständigen Konfiguration können Sie S3-Kapazität auf dem Gerät bereitstellen, und der Restbetrag ist als Blockspeicher verfügbar. In der Clusterkonfiguration wird die gesamte Kapazität der Datenfestplatte für S3-Speicher verwendet. Ein Cluster kann aus mindestens 3 Geräten bis zu maximal 16 Geräten bestehen. Je nach Größe des Clusters ist der S3-Dienst darauf ausgelegt, die Gerätefehlertoleranz von 1 oder 2 Geräten aufrechtzuerhalten.

Mit AWS DataSync können Sie Objekte zwischen Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge-Gerät und AWS Speicherdiensten übertragen. Weitere Informationen finden Sie unter [Konfiguration von Übertragungen mit S3-kompatiblen Speicher auf Snowball Edge](#) im AWS DataSync Benutzerhandbuch.

Im Folgenden finden Sie die Speicherkapazität für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge und die Blockspeicherkapazität für ein eigenständiges Gerät, das Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwendet. Informationen zur Fehlertoleranz und Speicherkapazität von Clustern finden Sie unter [this table](#)

Snowball Edge Compute Optimized with NVMe storage

Speicherkapazität von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge und Blockspeicher von Snowball Edge Compute Optimized (Compute Optimized with AMD EPYC Gen2 und) -Geräten NVMe

Amazon S3 S3-kompatibler Speicher auf Snowball Edge-Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
3	17,5
5.5	14,5
10.5	8,5
12	6,5
13	5.5
16,5	1.5

Snowball Edge storage optimized 210 TB

Speicherkapazität von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge und Blockspeicher von für Snowball Edge-Speicher optimierten 210-TB-Geräten

Amazon S3 S3-kompatibler Speicher auf Snowball Edge-Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
20	206
40	182
60	158
80	134
100	110
120	86

Amazon S3 S3-kompatibler Speicher auf Snowball Edge-Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
140	62
160	38
180	14
190	2

Spezifikationen für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge:

- Die maximale Anzahl von Snowball Edge-Buckets beträgt 100 pro Gerät oder pro Cluster.
- Das Besitzerkonto des S3 on Snowball Edge-Buckets besitzt alle Objekte im Bucket.
- Nur das Besitzerkonto des S3 on Snowball Edge-Buckets kann Operationen mit dem Bucket ausführen.
- Die Objektgrößenbeschränkungen entsprechen denen in Amazon S3.
- Alle auf S3 auf Snowball Edge gespeicherten Objekte haben SNOW als Speicherklasse.
- Standardmäßig werden alle in der SNOW-Speicherklasse gespeicherten Objekte mit serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) gespeichert. Sie können auch explizit auswählen, Objekte mithilfe serverseitiger Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) zu speichern.
- Wenn nicht genügend Speicherplatz zum Speichern eines Objekts auf Ihrem Snowball Edge vorhanden ist, gibt die API eine Ausnahme mit unzureichender Kapazität (ICE) zurück.

Themen

- [Amazon S3 S3-kompatiblen Speicher auf Snowball Edge bestellen](#)
- [Amazon S3 S3-kompatiblen Speicher auf Snowball Edge einrichten und starten](#)
- [Arbeiten mit S3-Buckets mit Amazon S3 S3-kompatiblem Speicher auf Snowball Edge](#)
- [Feststellen, ob Sie auf einen Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket auf einem Snowball Edge zugreifen können](#)
- [Abrufen einer Liste von Buckets oder regionalen Buckets im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge](#)

- [Einen Bucket mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge abrufen](#)
- [Erstellen eines S3-Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge](#)
- [Löschen eines Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge](#)
- [Erstellen und Verwalten einer Objektlebenszykluskonfiguration mit dem AWS CLI](#)
- [Kopieren eines Objekts in einen Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket auf einem Snowball Edge](#)
- [Objekte in einem Bucket im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge auflisten](#)
- [Ein Objekt aus einem Bucket im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge abrufen](#)
- [Löschen von Objekten in Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#)
- [Unterstützte REST-API-Aktionen für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge](#)
- [Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit einem Cluster von Snow-Geräten](#)
- [Konfiguration von Amazon S3 S3-kompatiblen Speicher für Snowball Edge-Ereignisbenachrichtigungen](#)
- [Konfiguration lokaler SMTP-Benachrichtigungen auf Snowball Edge](#)

Amazon S3 S3-kompatiblen Speicher auf Snowball Edge bestellen

Die Bestellung eines Geräts für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ist dem Bestellvorgang für einen Snowball Edge sehr ähnlich. Informationen zur Bestellung finden Sie [Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen](#) in dieser Anleitung und beachten Sie beim Bestellvorgang die folgenden Punkte:

- Wählen Sie für Jobtyp die Option Nur lokale Datenverarbeitung und Speicher aus.
- Wählen Sie unter Snow-Geräte die Option Snowball Edge Compute Optimized aus.
- Wählen Sie unter Speichertyp auswählen die Option Amazon S3 S3-kompatibler Speicher auf Snowball Edge aus.
- Wählen Sie für ein eigenständiges Gerät unter Speicherkapazität die Option Einzelgerät und dann die gewünschte Speichermenge aus.

- Wählen Sie für einen Cluster unter Speicherkapazität die Option Cluster und dann die gewünschte Speicherkapazität und Fehlertoleranz aus.

Amazon S3 S3-kompatiblen Speicher auf Snowball Edge einrichten und starten

Installieren und konfigurieren Sie Softwaretools von Ihrer lokalen Umgebung aus AWS , um mit dem Snowball Edge-Gerät oder Gerätecluster und Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu interagieren. Verwenden Sie dann diese Tools, um das Snowball Edge-Gerät oder den Snowball Edge-Cluster einzurichten und Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu starten.

Voraussetzungen

Amazon S3 S3-kompatibler Speicher auf Snowball Edge erfordert, dass Sie den Snowball Edge-Client und den in Ihrer lokalen Umgebung AWS CLI installiert haben. Sie können auch AWS Tools für Windows verwenden SDK für .NET , PowerShell um mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu arbeiten. AWS empfiehlt die Verwendung der folgenden Versionen dieser Tools:

- Snowball Edge Client — Verwenden Sie die neueste Version. Weitere Informationen finden Sie in diesem Handbuch unter [Herunterladen und Installieren des Snowball Edge-Clients](#).
- AWS CLI— Version 2.11.15 oder neuer. Weitere Informationen finden Sie unter [Installation, Aktualisierung und Deinstallation von AWS CLI im](#) AWS Command Line Interface Benutzerhandbuch.
- SDK für .NET— AWSSDK .S3Control 3.7.304.8 oder neuer. Weitere Informationen finden Sie unter [AWS SDK für .NET](#).
- AWS Tools für Windows PowerShell — Version 4.1.476 oder neuer. Weitere Informationen finden Sie im [AWS -Tools für PowerShell -Benutzerhandbuch](#).

Richten Sie Ihre lokale Umgebung ein

In diesem Abschnitt wird beschrieben, wie Sie den Snowball Edge-Client und Ihre lokale Umgebung für die Verwendung mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge einrichten und konfigurieren.

1. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Snowball Edge-Client herunterladen und installieren](#).
2. Konfigurieren Sie ein Profil für den Snowball Edge-Client. Weitere Informationen finden Sie unter [Konfiguration eines Profils für den Snowball Edge-Client](#).
3. Wenn Sie verwenden SDK für .NET, legen Sie den `clientConfig.AuthenticationRegion` Parameterwert wie folgt fest:

```
clientConfig.AuthenticationRegion = "snow"
```

Ihr Snowball Edge-Gerät einrichten

IAM auf dem Snowball Edge einrichten

AWS Identity and Access Management (IAM) hilft Ihnen dabei, den granularen Zugriff auf AWS Ressourcen zu ermöglichen, die auf Ihren Snowball Edge-Geräten ausgeführt werden. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.

IAM wird lokal auf dem Snowball Edge unterstützt. Sie können den lokalen IAM-Dienst verwenden, um Rollen zu erstellen und ihnen IAM-Richtlinien zuzuweisen. Sie können diese Richtlinien verwenden, um den für die Ausführung zugewiesener Aufgaben notwendigen Zugriff zu ermöglichen.

Das folgende Beispiel ermöglicht vollen Zugriff auf die Amazon S3 S3-API:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Weitere Beispiele für IAM-Richtlinien finden Sie im [AWS Snowball Edge Developer Guide](#).

Starten des Amazon S3 S3-kompatiblen Speichers auf dem Snowball Edge-Service

Verwenden Sie die folgenden Anweisungen, um den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Dienst auf einem Snowball Edge-Gerät oder -Cluster zu starten.

Wenn Sie eine benutzerfreundlichere Erfahrung bevorzugen, können Sie den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Service für ein eigenständiges Gerät oder einen Gerätecluster starten, indem Sie AWS OpsHub. Siehe [Richten Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ein mit AWS OpsHub](#).

1. Entsperren Sie Ihr Snowball Edge-Gerät oder Ihren Gerätecluster, indem Sie den folgenden Befehl ausführen:

- Für ein einzelnes Gerät:

```
snowballEdge unlock-device --endpoint https://snow-device-ip
```

- Für einen Cluster:

```
snowballEdge unlock-cluster
```

2. Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass das Snowball Edge-Gerät oder der Gerätecluster entsperrt ist:

- Für ein einzelnes Gerät:

```
snowballEdge describe-device --endpoint https://snow-device-ip
```

- Für einen Cluster:

```
snowballEdge describe-cluster --device-ip-addresses [snow-device-1-ip] [snow-device-2-ip] /  
[snow-device-3-ip] [snow-device-4-ip] [snow-device-5-ip] /  
[snow-device-6-ip]
```

3. Gehen Sie für jedes Gerät (unabhängig davon, ob Sie eines oder einen Cluster haben) wie folgt vor, um Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu starten:
 - a. Rufen Sie die Geräte ab, `PhysicalNetworkInterfaceId` indem Sie den folgenden `describe-device` Befehl ausführen:

```
snowballEdge describe-device --endpoint https://snow-device-ip
```

- b. Führen Sie den folgenden `create-virtual-network-interface` Befehl zweimal aus, um die virtuellen Netzwerkschnittstellen (VNIs) für die Endpunkte `s3control` (für Bucket-Operationen) und `s3api` (für Objektoperationen) zu erstellen.

```
snowballEdge create-virtual-network-interface --ip-address-assignment  
dhcp --manifest-file manifest --physical-network-interface-id  
"PhysicalNetworkInterfaceId" --unlock-code unlockcode --endpoint https://snow-  
device-ip
```

Der Befehl gibt eine JSON-Struktur zurück, die die IP-Adresse enthält. Notieren Sie die IP-Adresse.

Einzelheiten zu diesen Befehlen finden Sie unter [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\) auf einem Snowball Edge](#).

 Note

Das Starten von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verbraucht Gerätere Ressourcen.

4. Starten Sie den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Service, indem Sie den folgenden `start-service` Befehl ausführen. Dieser enthält die IP-Adressen Ihrer Geräte und die Amazon-Ressourcennamen (ARNs) der, die Sie für VNIs die Endpunkte `s3control` und `s3api` Endpunkte erstellt haben:

Um den Service auf einem einzelnen Gerät zu starten:

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-device-1-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2
```

Um den Dienst auf einem Cluster zu starten:

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2 vni-arn-3 vni-arn-4 vni-arn-5 vni-arn-6
```

Für `--virtual-network-interface-arns`, schließen ARNs Sie alle ein VNIs, die Sie im vorherigen Schritt erstellt haben. Trennen Sie jeden ARN durch ein Leerzeichen.

5. Führen Sie den folgenden `describe-service` Befehl für ein einzelnes Gerät aus:

```
snowballEdge describe-service --service-id s3-snow
```

Warten Sie, bis der Dienststatus lautet `Active`.

Führen Sie den folgenden `describe-service` Befehl für einen Cluster aus:

```
snowballEdge describe-service --service-id s3-snow \
  --device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip
```

Informationen zu Amazon S3 S3-kompatiblen Speicher auf Snowball Edge-Endpunkten anzeigen

Wenn der Amazon S3 S3-kompatible Speicher auf dem Snowball Edge-Service läuft, können Sie den `describe-service` Snowball Edge-Client-Befehl verwenden, um die IP-Adressen anzuzeigen, die den Endpunkten `s3control` und `s3api` zugeordnet sind.

```
snowballEdge describe-service --service-id s3-snow --endpoint https://snow-device-ip-address --profile profile-name
```

Example Ausgabe des Befehls **describe-service**

In diesem Beispiel lautet die IP-Adresse des s3control-Endpunkts 192.168.1.222 und die IP-Adresse des s3api-Endpunkts 192.168.1.152.

```
{
  "ServiceId": "s3-snow",
  "Autostart": true,
  "Status": {
    "State": "ACTIVATING",
    "Details": "Attaching storage"
  },
  "ServiceCapacities": [
    {
      "Name": "S3 Storage",
      "Unit": "Byte",
      "Used": 148599705600,
      "Available": 19351400294400
    }
  ],
  "Endpoints": [
    {
      "Protocol": "https",
      "Port": 443,
      "Host": "192.168.1.222",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/30c563f1124707705117f57f6c3accd42a4528ed6dba1e35c1822a391a717199d8c49973d3",
      },
      "Description": "s3-snow bucket API endpoint (for s3control SDK)",
      "DeviceId": "JID-beta-207429000001-23-12-28-03-51-11",
      "Status": {
        "State": "ACTIVE"
      }
    },
    {
      "Protocol": "https",
      "Port": 443,
      "Host": "192.168.1.152",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/30c563f1124707705117f57f6c3accd42a4528ed6dba1e35c1822a391a717199d8c49973d3",
      },
    }
  ]
}
```

```
"Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
"DeviceId": "JID-beta-207429000001-23-12-28-03-51-11",
"Status": {
  "State": "ACTIVATING"
}
]
}
```

Arbeiten mit S3-Buckets mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge

Mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge können Sie Amazon S3 S3-Buckets auf Ihren Snowball Edge-Geräten erstellen, um Objekte vor Ort für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Amazon S3-kompatibler Speicher auf Snowball Edge bietet eine neue Speicherklasse SNOW, die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Snowball Edge-Geräten zu speichern. Sie können für Snowball Edge-Buckets dieselben APIs Funktionen wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging.

Sie können Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit AWS Command Line Interface (AWS CLI) oder programmatisch über das AWS Java-SDK verwenden. Mit dem AWS CLI können Sie einen s3api- oder s3control-Endpunkt einrichten und mit ihm über Befehle interagieren. Wir empfehlen die Verwendung des s3api-Endpunkts, da derselbe Endpunkt für Bucket- und Objektoperationen verwendet werden kann.

Note

Der s3api-Endpunkt ist für Version 8004 und neuer der Snowball Edge-Software verfügbar. Verwenden Sie den `snowballEdge check-for-updates` Befehl, um die auf einem Gerät installierte Version der Snowball Edge-Software zu ermitteln. Informationen zum Aktualisieren eines Snowball Edge-Geräts finden Sie unter [Software auf Snowball Edge-Geräten aktualisieren](#).

Verwenden des AWS CLI

Folgen Sie diesen Anweisungen, um mit Amazon S3 S3-Buckets auf Ihrem Gerät zu arbeiten, indem Sie AWS CLI

Um das einzurichten AWS CLI

1. Erstellen Sie ein Profil für Objektpunkte in `~/.aws/config`.

```
[profile your-profile]  
aws_access_key_id = your-access-id  
aws_secret_access_key = your-access-key  
region = snow  
ca_bundle = dev/apps/ca-certs/your-ca_bundle
```

2. Besorgen Sie sich ein Zertifikat von Ihrem Gerät. Weitere Informationen finden Sie im [Snowball Edge Developer Guide](#).
3. Wenn Sie das SDK in einer virtuellen Umgebung installiert haben, aktivieren Sie es mit dem folgenden Befehl:

```
source your-virtual-environment-name/bin/activate
```

Nachdem Sie Ihre Operationen eingerichtet haben, können Sie das s3api SDK oder das s3control SDK verwenden, um mit dem auf S3-Buckets auf Snowball Edge zuzugreifen. AWS CLI

Example des Zugriffs auf den S3-Bucket mithilfe des s3api-SDK

```
aws s3api list-buckets --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Example des Zugriffs auf S3-Buckets mit dem s3control SDK

```
aws s3control list-regional-buckets --account-id bucket-owner --endpoint-url  
https://s3ctrlapi-endpoint-ip --profile your-profile
```

Example des Zugriffs auf S3-Objekte mit dem s3api SDK

```
aws s3api list-objects-v2 --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Verwenden des Java-SDK

Verwenden Sie das folgende Beispiel, um mithilfe des Java-SDK mit Amazon S3 S3-Buckets und -Objekten zu arbeiten.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.auth.credentials.StaticCredentialsProvider;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.regions.Region;

import java.net.URI;

AwsBasicCredentials creds = AwsBasicCredentials.create(accessKey, secretKey); // set
    creds by getting Access Key and Secret Key from snowball edge
SdkHttpClient httpClient =
    ApacheHttpClient.builder().tlsTrustManagersProvider(trustManagersProvider).build(); //
    set trust managers provider with client certificate from snowball edge
String s3SnowEndpoint = "10.0.0.0"; // set s3-snow object api endpoint from describe
    service

S3Client s3Client =
    S3Client.builder().httpClient(httpClient).region(Region.of("snow")).endpointOverride(new
    URI(s3SnowEndpoint)).credentialsProvider(StaticCredentialsProvider.create(creds)).build();
```

Bucket-ARN-Format

Sie können das hier aufgeführte Format Amazon Resource Name (ARN) verwenden, um einen Amazon S3 S3-Bucket auf einem Snowball Edge-Gerät zu identifizieren:

```
arn:partition:s3:snow:account-id:device/device-id/bucket/bucket-name
```

Wo *partition* ist die Partition der Region, in der Sie Ihr Snowball Edge-Gerät bestellt haben. *device-id* ist die `job_id`, wenn es sich bei dem Gerät um ein eigenständiges Snowball Edge-Gerät handelt, oder die, *cluster_id* wenn Sie einen Snowball Edge-Cluster haben.

Format des Bucket-Speicherorts

Das Bucket-Standortformat gibt das Snowball Edge-Gerät an, auf dem der Bucket erstellt wird. Der Bucket-Speicherort hat das folgende Format:

```
/device-id/bucket/bucket-name
```

Weitere Informationen finden Sie unter [create-bucket](#) in der AWS CLI Befehlsreferenz.

Feststellen, ob Sie auf einen Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket auf einem Snowball Edge zugreifen können

Das folgende Beispiel verwendet den `head-bucket` Befehl, um zu ermitteln, ob ein Amazon S3 S3-Bucket vorhanden ist und Sie über Zugriffsberechtigungen mit dem verfügen AWS CLI. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api head-bucket --bucket sample-bucket --endpoint-url https://s3api-endpoint-ip
--profile your-profile
```

Abrufen einer Liste von Buckets oder regionalen Buckets im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge

Verwenden Sie das `list-regional-buckets` oder `list-buckets`, um Amazon S3 S3-kompatiblen Speicher in Snowball Edge-Buckets mithilfe von aufzulisten. AWS CLI

Example des Abrufs einer Liste von Buckets oder regionalen Buckets mit AWS CLI

s3api syntax

```
aws s3api list-buckets --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem `list-buckets` Befehl finden Sie unter [list-buckets](#) in der Befehlsreferenz AWS CLI

s3control syntax

```
aws s3control list-regional-buckets --account-id 123456789012 --endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profiles
```

Weitere Informationen zu dem `list-regional-buckets` Befehl finden Sie [list-regional-buckets](#) in der AWS CLI Befehlsreferenz.

Das folgende Beispiel für ein SDK for Java ruft eine Liste von Buckets auf Snowball Edge-Geräten ab. Weitere Informationen finden Sie [ListBuckets](#) in der Amazon Simple Storage Service API-Referenz.

```
import com.amazonaws.services.s3.model.*;
public void listBuckets() {
    ListBucketsRequest reqListBuckets = new ListBucketsRequest()
        .withAccountId(AccountId)
        ListBucketsResult respListBuckets = s3APIClient.RegionalBuckets(reqListBuckets);
    System.out.printf("ListBuckets Response: %s\n", respListBuckets.toString());
}
```

Im folgenden PowerShell Beispiel wird eine Liste von Buckets auf Snowball Edge-Geräten abgerufen.

```
Get-S3CRegionalBucketList -AccountId 012345678910 -Endpoint "https://snowball_ip" -Region snow
```

Das folgende .NET-Beispiel ruft eine Liste von Buckets auf Snowball Edge-Geräten ab.

```
using Amazon.S3Control;
using Amazon.S3Control.Model;

namespace SnowTest;

internal class Program
{
    static async Task Main(string[] args)
    {
        var config = new AmazonS3ControlConfig
        {
            ServiceURL = "https://snowball_ip",
            AuthenticationRegion = "snow" // Note that this is not RegionEndpoint
        };

        var client = new AmazonS3ControlClient(config);

        var response = await client.ListRegionalBucketsAsync(new
ListRegionalBucketsRequest()
        {
            AccountId = "012345678910"
        });
    }
}
```

Einen Bucket mit Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge abrufen

Im folgenden Beispiel wird mithilfe von ein Amazon S3 S3-kompatibler Speicher auf einem Snowball Edge-Bucket abgerufen. AWS CLI Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3control get-bucket --account-id 123456789012 --bucket amzn-s3-demo-bucket --
endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie unter [get-bucket](#) in der AWS CLI Befehlsreferenz.

Das folgende Beispiel für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ruft mithilfe des SDK for Java einen Bucket ab. Weitere Informationen finden Sie unter [GetBucket](#) in der [API-Referenz zu Amazon Simple Storage Service](#).

```
import com.amazonaws.services.s3control.model.*;

public void getBucket(String bucketName) {

    GetBucketRequest reqGetBucket = new GetBucketRequest()
        .withBucket(bucketName)
        .withAccountId(AccountId);

    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);
    System.out.printf("GetBucket Response: %s\n", respGetBucket.toString());
}
```

Erstellen eines S3-Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge

Sie können Amazon S3 S3-Buckets auf Ihrem Snowball Edge-Gerät erstellen, um Objekte am Edge für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Amazon S3-kompatibler Speicher auf Snowball Edge bietet eine neue Speicherklasse SNOW, die Amazon S3 verwendet und darauf ausgelegt ist, Daten dauerhaft und redundant auf mehreren Geräten zu speichern. Sie können dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Richtlinien für den Bucket-Lebenszyklus, Verschlüsselung und Tagging.

Das folgende Beispiel erstellt einen Amazon S3 S3-Bucket für ein Snowball Edge-Gerät mit dem AWS CLI. Um den Befehl zu verwenden, ersetzen Sie den Platzhaltertext des Benutzers durch Ihre eigenen Informationen.

Example zum Erstellen eines S3-Buckets

s3api syntax

```
aws s3api create-bucket --bucket your-snow-bucket --endpoint-url https://s3api-  
endpoint-ip --profile your-profile
```

s3control syntax

```
aws s3control create-bucket --bucket your-snow-bucket --endpoint-url  
https://s3ctrlapi-endpoint-ip --profile your-profile
```

Löschen eines Buckets in Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge

Sie können das s3api SDK oder das s3control SDK verwenden, um einen Bucket im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu löschen.

Important

- AWS-Konto Derjenige, der den Bucket erstellt, besitzt ihn und ist der einzige, der ihn löschen kann.
- Snowball Edge-Buckets müssen leer sein, bevor sie gelöscht werden können.
- Sie können einen Bucket nicht wiederherstellen, nachdem er gelöscht wurde.

In den folgenden Beispielen wird ein Amazon S3 S3-kompatibler Speicher auf einem Snowball Edge-Bucket mithilfe von gelöscht. AWS CLI Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

Example des Löschens eines Buckets

s3api syntax

```
aws s3api delete-bucket --bucket amzn-s3-demo-bucket --endpoint-url https://s3api-  
endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie unter [delete-bucket](#) in der AWS CLI Befehlsreferenz.

s3control syntax

```
aws s3control delete-bucket --account-id 123456789012 --bucket amzn-s3-demo-bucket  
--endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie unter [delete-bucket](#) in der Befehlsreferenz.
AWS CLI

Erstellen und Verwalten einer Objektlebenszykluskonfiguration mit dem AWS CLI

Sie können Amazon S3 Lifecycle verwenden, um die Speicherkapazität für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge zu optimieren. Sie können Lebenszyklusregeln erstellen, um Objekte ablaufen zu lassen, wenn sie veralten oder durch neuere Versionen ersetzt werden. Sie können eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen. Weitere Informationen zu Amazon S3 Lifecycle finden Sie unter [Verwaltung Ihres Speicherlebenszyklus](#).

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen kann.

Informationen zum Erstellen und Verwalten einer Lebenszykluskonfiguration für einen Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket mithilfe von AWS Command Line Interface (AWS CLI) finden Sie in den folgenden Beispielen.

PUT eine Lebenszykluskonfiguration auf einen Snowball Edge-Bucket

Im folgenden AWS CLI Beispiel wird eine Lebenszykluskonfigurationsrichtlinie auf einen Snowball Edge-Bucket angewendet. Diese Richtlinie gibt an, dass alle Objekte mit dem gekennzeichneten Präfix (*myprefix*) und Tags nach 10 Tagen ablaufen. Ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

Speichern Sie zunächst die Lebenszyklus-Konfigurationsrichtlinie in einer JSON-Datei. In diesem Beispiel wird die Datei benannt **lifecycle-example.json**.


```
{
  "Rules": [{
    "ID": "id-1",
    "Filter": {
      "And": {
        "Prefix": "myprefix",
        "Tags": [{
          "Value": "mytagvalue1",
          "Key": "mytagkey1"
        },
        {
          "Value": "mytagvalue2",
          "Key": "mytagkey2"
        }
      ]
    }
  },
  "Status": "Enabled",
  "Expiration": {
    "Days": 10
  }
}]
}
```

Nachdem Sie die Datei gespeichert haben, senden Sie die JSON-Datei als Teil des `put-bucket-lifecycle-configuration` Befehls. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

Example des **put-bucket-lifecycle** Befehls

s3api syntax

```
aws s3api put-bucket-lifecycle-configuration --bucket example-snow-bucket \\  
  --lifecycle-configuration file://lifecycle-example.json --endpoint-url  
  https://s3api-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie [put-bucket-lifecycle-configuration](#) in der AWS CLI Befehlsreferenz.

s3control syntax

```
aws s3control put-bucket-lifecycle-configuration --bucket example-snow-bucket \\  
--lifecycle-configuration file://lifecycle-example.json \\  
--endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie [put-bucket-lifecycle-configuration](#) in der AWS CLI Befehlsreferenz.

Kopieren eines Objekts in einen Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket auf einem Snowball Edge

Im folgenden Beispiel wird eine Datei mit dem Namen *sample-object.xml* in einen Amazon S3 S3-kompatiblen Speicher im Snowball Edge-Bucket hochgeladen, für dessen Verwendung Sie Schreibberechtigungen haben. AWS CLI Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api put-object --bucket sample-bucket --key sample-object.xml --body sample-object.xml --endpoint-url s3api-endpoint-ip --profile your-profile
```

Das folgende Beispiel für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge kopiert ein Objekt mithilfe des SDK for Java in ein neues Objekt im selben Bucket. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import com.amazonaws.services.s3.AmazonS3;  
import com.amazonaws.services.s3.AmazonS3ClientBuilder;  
import com.amazonaws.services.s3.model.CopyObjectRequest;  
add : import java.io.IOException;  
  
public class CopyObject {  
    public static void main(String[] args) {  
        String bucketName = "**** Bucket name ****";  
        String sourceKey = "**** Source object key ****";
```

```

String destinationKey = "*** Destination object key ***";

try {
    // This code expects that you have AWS credentials set up per:
    // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
    AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
        .enableUseArnRegion()
        .build();

    // Copy the object into a new object in the same bucket.
    CopyObjectRequest copyObjectRequest = new CopyObjectRequest(sourceKey,
destinationKey);
    s3Client.copyObject(copyObjectRequest);
    CopyObjectRequest copyObjectRequest = CopyObjectRequest.builder()
        .sourceKey(sourceKey)
        .destinationKey(destKey)
        .build();
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
}

```

Objekte in einem Bucket im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge auflisten

Das folgende Beispiel listet Objekte in einem Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket unter Verwendung von auf AWS CLI. Der SDK-Befehl lautet `s3-snow:ListObjectsV2`. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```

aws s3api list-objects-v2 --bucket sample-bucket --endpoint-url s3api-endpoint-ip --
profile your-profile

```

Weitere Informationen zu diesem Befehl finden Sie unter [list-objects-v2](#) in der AWS CLI Befehlsreferenz.

Das folgende Beispiel für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge listet Objekte in einem Bucket auf, das das SDK for Java verwendet. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

In diesem Beispiel wird [ListObjectsV2](#) verwendet, die neueste Version des ListObjects API-Vorgangs. Wir empfehlen die Verwendung dieser überarbeiteten API-Operationen für die Anwendungsentwicklung. Aus Gründen der Abwärtskompatibilität unterstützt Amazon S3 weiterhin die vorherige Version dieser API-Operation.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {

    public static void main(String[] args) {
        String bucketName = "**** Bucket name ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .enableUseArnRegion()
                .build();

            System.out.println("Listing objects");

            // maxKeys is set to 2 to demonstrate the use of
            // ListObjectsV2Result.getNextContinuationToken()
            ListObjectsV2Request req = new
            ListObjectsV2Request().withBucketName(bucketName).withMaxKeys(2);
            ListObjectsV2Result result;

            do {
```

```

        result = s3Client.listObjectsV2(req);

        for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
            System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
objectSummary.getSize());
        }
        // If there are more than maxKeys keys in the bucket, get a
continuation token
        // and list the next objects.
        String token = result.getNextContinuationToken();
        System.out.println("Next Continuation Token: " + token);
        req.setContinuationToken(token);
    } while (result.isTruncated());
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
}

```

Ein Objekt aus einem Bucket im Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge abrufen

Im folgenden Beispiel wird mithilfe von ein Objekt abgerufen, das *sample-object.xml* aus einem Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket benannt wurde. AWS CLI Der SDK-Befehl lautet `s3-snow:GetObject`. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api get-object --bucket sample-bucket --key sample-object.xml --endpoint-
url s3api-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie unter [get-object](#) in der AWS CLI Befehlsreferenz.

Das folgende Beispiel für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge ruft ein Objekt mithilfe des SDK for Java ab. Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben

durch Ihre eigenen Informationen. Weitere Informationen finden Sie unter [GetObject](#) in der [API-Referenz zu Amazon Simple Storage Service](#).

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String bucketName = "**** Bucket name ****";
        String key = "**** Object key ****";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .enableUseArnRegion()
                .build();
            GetObjectRequest getObjectRequest = GetObjectRequest.builder()
                .bucket(bucketName)
                .key(key)
                .build();

            s3Client.getObject(getObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
        }
    }
}
```

```

        e.printStackTrace();
    } finally {
        // To ensure that the network connection doesn't remain open, close any
open input streams.
        if (fullObject != null) {
            fullObject.close();
        }
        if (objectPortion != null) {
            objectPortion.close();
        }
        if (headerOverrideObject != null) {
            headerOverrideObject.close();
        }
    }
}

private static void displayTextInputStream(InputStream input) throws IOException {
    // Read the text input stream one line at a time and display each line.
    BufferedReader reader = new BufferedReader(new InputStreamReader(input));
    String line = null;
    while ((line = reader.readLine()) != null) {
        System.out.println(line);
    }
    System.out.println();
}
}

```

Löschen von Objekten in Buckets in Amazon S3 S3-kompatiblem Speicher auf Snowball Edge

Sie können ein oder mehrere Objekte aus einem Amazon S3 S3-kompatiblen Speicher auf einem Snowball Edge-Bucket löschen. Im folgenden Beispiel wird ein Objekt gelöscht, das *sample-object.xml* mit dem benannt wurde. AWS CLI Ersetzen Sie in diesem Befehl jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api delete-object --bucket sample-bucket --key key --endpoint-url s3api-endpoint-ip --profile your-profile
```

Weitere Informationen zu diesem Befehl finden Sie unter [delete-object](#) in der Befehlsreferenz.AWS CLI

Das folgende Beispiel für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge löscht mithilfe des SDK for Java ein Objekt in einem Bucket. Um dieses Beispiel zu verwenden, geben Sie den Schlüsselnamen für das Objekt an, das Sie löschen möchten. Weitere Informationen finden Sie [DeleteObject](#) in der Amazon Simple Storage Service API-Referenz.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String bucketName = "**** Bucket name ****";
        String keyName = "**** key name ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .enableUseArnRegion()
                .build();

            DeleteObjectRequest deleteObjectRequest = DeleteObjectRequest.builder()
                .bucket(bucketName)
                .key(keyName)
                .build());
            s3Client.deleteObject(deleteObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```


Unterstützte REST-API-Aktionen für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge

Die folgenden Listen zeigen die API-Operationen, die von Amazon S3-kompatiblen Speicher auf Snowball Edge unterstützt werden, einschließlich Links zu den zugehörigen Vorgängen für Amazon S3 in AWS-Regionen.

Unterstützte Bucket-API-Operationen für den s3api-Endpunkt:

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycle](#)
- [GetBucketLifecycleConfiguration](#)
- [ListBuckets](#)
- [PutBucketLifecycleConfiguration](#)

Unterstützte Bucket-API-Operationen für den s3control-Endpunkt:

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycle](#)
- [GetBucket](#)
- [GetBucketLifecycleConfiguration](#)
- [ListBuckets](#)
- [PutBucketLifecycleConfiguration](#)

Unterstützte Objekt-API-Operationen:

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)

- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectTagging](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjects](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectTagging](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge mit einem Cluster von Snow-Geräten

Ein Cluster ist eine Sammlung von drei oder mehr Snowball Edge-Geräten, die als eine einzige logische Einheit für lokale Speicher- und Rechenzwecke verwendet werden. Ein Cluster bietet zwei Hauptvorteile gegenüber einem eigenständigen Snowball Edge-Gerät für lokalen Speicher und Datenverarbeitung:

- **Höhere Haltbarkeit** — Die in einem Cluster von Snowball Edge-Geräten gespeicherten S3-Daten weisen eine höhere Datenbeständigkeit auf als ein einzelnes Gerät. Darüber hinaus bleiben die Daten auf dem Cluster trotz möglicher Hardwareausfälle, die sich auf den Cluster auswirken, sicher und funktionsfähig. Cluster können den Verlust eines Geräts in Clustern von 3 und 4 Geräten und von bis zu zwei Geräten in Clustern von 5 bis 16 Geräten aushalten, bevor die Daten gefährdet sind. Sie können fehlerhafte Knoten ersetzen, um die Beständigkeit und Sicherheit der im Cluster gespeicherten Daten zu gewährleisten.
- **Mehr Speicherplatz** — Mit speicheroptimierten Snowball Edge-Geräten können Sie einen einzelnen Cluster mit 16 Knoten und bis zu 2,6 PB nutzbarer S3-kompatibler Speicherkapazität erstellen. Mit den für die Datenverarbeitung optimierten Snowball Edge-Geräten können Sie einen einzelnen Cluster mit 16 Knoten und bis zu 501 TB nutzbarer S3-kompatibler Speicherkapazität erstellen.

Ein Cluster von Snowball Edge-Geräten besteht aus Leaderless-Knoten. Jeder Knoten kann Daten in den gesamten Cluster schreiben und Daten aus dem gesamten Cluster lesen, und alle Knoten sind in der Lage, den Cluster zu behind-the-scenes verwalten.

Beachten Sie bei der Planung der Verwendung eines Clusters von Snowball Edge-Geräten die folgenden Überlegungen:

- Wir empfehlen, dass Sie für alle Geräte im Cluster eine redundante Stromquelle bereitstellen, um mögliche Leistungs- und Stabilitätsprobleme im Cluster zu reduzieren.
- Wie bei eigenständigen lokalen Speicher- und Rechenaufträgen können die in einem Cluster gespeicherten Daten nicht in Amazon S3 importiert werden, ohne zusätzliche Geräte als Teil separater Importaufträge zu bestellen. Wenn Sie zusätzliche Geräte als Importaufträge bestellen, können Sie die Daten vom Cluster auf die Geräte mit den Importaufträgen übertragen.
- Um Daten von Amazon S3 auf einen Cluster zu übertragen, verwenden Sie die Amazon S3 S3-API, um Amazon S3 S3-Buckets auf dem Cluster zu erstellen, um Objekte aus S3 zu speichern und abzurufen. Sie können es auch verwenden, AWS DataSync um Objekte zwischen AWS Speicherdiensten und Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf einem Snowball Edge-Gerät zu übertragen. Weitere Informationen finden Sie unter [Konfiguration von Übertragungen mit S3-kompatiblen Speicher auf Snowball Edge](#).
- Sie können einen Job erstellen, um einen Cluster von Geräten aus der Managementkonsole für die AWS Snow-Familie AWS CLI, dem oder einem der AWS SDKs Geräte zu bestellen. Weitere Informationen finden Sie unter [Erste Schritte mit Snowball Edge](#).
- Jedes Gerät im Cluster hat eine Knoten-ID. Eine Knoten-ID ist eine eindeutige Kennung für jedes Gerät im Cluster, wie eine Job-ID für ein eigenständiges Gerät. Sie können den Knoten IDs von der Managementkonsole für die AWS Snow-Familie, dem AWS CLI AWS SDKs, und dem Snowball Edge-Client abrufen. Der Snowball Edge-Client befiehlt `describe-device` und `describe-cluster` gibt den Knoten IDs mit anderen Informationen über Geräte oder den Cluster zurück.
- Die Lebensdauer eines Clusters wird durch das Sicherheitszertifikat begrenzt, das für die Cluster-Geräte bei der Bereitstellung des Clusters gewährt wird. Standardmäßig können Snowball Edge-Geräte bis zu 360 Tage lang verwendet werden, bevor sie zurückgegeben werden müssen. Nach Ablauf dieser Zeit reagieren die Geräte nicht mehr auf read/write Anfragen. Wenn Sie ein oder mehrere Geräte länger als 360 Tage behalten müssen, wenden Sie sich an AWS Support.
- Wenn AWS Sie ein zurückgesandtes Gerät erhalten, das Teil eines Clusters war, führen wir eine vollständige Löschung des Geräts durch. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Amazon S3 S3-kompatibler Speicher auf Snowball Edge-Cluster, Fehlertoleranz und Speicherkapazität

Cluster-Größe	Fehlertoleranz	Speicherkapazität von Snowball Edge Compute Optimized (Compute Optimized with AMD EPYC Gen2 and NVMe) - Geräten (in TB)	Speicherkapazität von für Snowball Edge-Speicher optimierten 210-TB-Geräten (in TB)
3	Verlust von bis zu einem Knoten	38	438
4	Verlust von bis zu einem Knoten	57	657
5	Verlust von bis zu 2 Knoten	57	657
6	Verlust von bis zu 2 Knoten	76	904
7	Verlust von bis zu 2 Knoten	95	1096
8	Verlust von bis zu 2 Knoten	114	1315
9	Verlust von bis zu 2 Knoten	133	1534
10	Verlust von bis zu 2 Knoten	152	1754
11	Verlust von bis zu 2 Knoten	165	1970
12	Verlust von bis zu 2 Knoten	171	1973

Cluster-Größe	Fehlertoleranz	Speicherkapazität von Snowball Edge Compute Optimized (Compute Optimized with AMD EPYC Gen2 and NVMe) - Geräten (in TB)	Speicherkapazität von für Snowball Edge-Speicher optimierten 210-TB-Geräten (in TB)
13	Verlust von bis zu 2 Knoten	190	2192
14	Verlust von bis zu 2 Knoten	209	2411
15	Verlust von bis zu 2 Knoten	225	2625
16	Verlust von bis zu 2 Knoten	228	2631

Nachdem Sie einen Cluster entsperrt haben, können Sie Daten in diesem Cluster speichern und darauf zugreifen. Sie können den Amazon S3 S3-kompatiblen Endpunkt verwenden, um Daten aus einem Cluster zu lesen und in einen Cluster zu schreiben.

Um Daten aus einem Cluster lesen oder in einen Cluster schreiben zu können, benötigen Sie ein read/write Quorum mit nicht mehr als der zulässigen Anzahl nicht verfügbarer Knoten in Ihrem Gerätecluster.

Snowball Edge-Cluster-Quoren

Ein Quorum stellt die Mindestanzahl von Snowball Edge-Geräten in einem Cluster dar, die miteinander kommunizieren müssen, um ein read/write Quorum aufrechtzuerhalten.

Wenn alle Geräte in einem Cluster fehlerfrei sind, haben Sie ein Lese-/Schreibquorum für Ihren Cluster. Wenn eines oder zwei dieser Geräte offline gehen, reduzieren Sie die Betriebskapazität des Clusters. Sie können jedoch immer noch Lese- und Schreibvorgänge auf dem Cluster durchführen. Wenn der Cluster bis auf ein oder zwei Geräte in Betrieb ist, hat der Cluster immer noch ein read/

write Quorum. Die Anzahl der Knoten, die offline gehen können, bevor die Betriebskapazität des Clusters beeinträchtigt wird, finden Sie in [this table](#).

Quorum kann verloren gehen, wenn ein Cluster mehr als die unter angegebene Anzahl von Geräten verliert. [this table](#) Wenn ein Quorum verloren geht, ist der Cluster offline und die Daten im Cluster sind nicht verfügbar. Je nach Schweregrad des Vorgangs können Sie dies entweder beheben oder die Daten sind möglicherweise dauerhaft verloren. Wenn es sich um ein temporäres externes Stromversorgungsereignis handelt und Sie die Snowball Edge-Geräte wieder einschalten und alle Knoten im Cluster entsperren können, sind Ihre Daten wieder verfügbar.

Important

Wenn kein Mindestquorum an intakten Knoten vorhanden ist, wenden Sie sich an. AWS Support

Sie können den `describe-cluster` Befehl verwenden, um den Sperrstatus und die Erreichbarkeit über das Netzwerk für jeden Knoten einzusehen. Wenn Sie den Clusterspeicher verwenden, müssen Sie sicherstellen, dass die Geräte in Ihrem Cluster ordnungsgemäß funktionieren und verbunden sind. Weitere Informationen finden Sie unter [Gerätestatus abrufen](#).

Wenn Sie feststellen, dass ein oder mehrere Knoten fehlerhaft sind, können Sie die Knoten im Cluster ersetzen, um Quorum und die Integrität und Stabilität Ihrer Daten aufrechtzuerhalten. Weitere Informationen finden Sie unter [Einen Knoten in einem Cluster ersetzen](#).

Einen nicht verfügbaren Clusterknoten erneut verbinden

Ein Knoten oder ein Gerät innerhalb eines Clusters kann aufgrund eines Problems wie Strom- oder Netzausfall vorübergehend nicht verfügbar sein, ohne dass die Daten auf dem Knoten beschädigt werden. Wenn dies geschieht, wirkt sich dies auf den Status Ihres Clusters aus. Die Netzwerkerreichbarkeit und der Sperrstatus eines Knotens werden im Snowball Edge-Client mithilfe des Befehls `snowballEdge describe-cluster` gemeldet.

Wir empfehlen, Ihren Cluster physisch so zu positionieren, dass Sie zur Vorder-, Rück- und Oberseite aller Knoten Zugang haben. Auf diese Weise können Sie auf Strom- und Netzkabel auf der Rückseite, Versandetiketten auf der Oberseite für den Knoten IDs und LCD-Bildschirme auf der Vorderseite der Geräte für die IP-Adressen und andere Verwaltungsinformationen zugreifen.

Wenn Sie feststellen, dass ein Knoten nicht verfügbar ist, empfehlen wir Ihnen, je nach dem Szenario, das dazu geführt hat, dass der Knoten nicht verfügbar ist, eines der folgenden Verfahren auszuprobieren.

So verbinden Sie einen nicht verfügbaren Knoten wieder

1. Stellen Sie sicher, dass der Knoten eingeschaltet ist.
2. Stellen Sie sicher, dass der Knoten mit demselben internen Netzwerk verbunden ist, mit dem der Rest des Clusters verbunden ist.
3. Wenn Sie den Knoten einschalten müssen, warten Sie bis zu 20 Minuten, bis der Vorgang abgeschlossen ist.
4. Führen Sie den `snowballEdge unlock-cluster` Befehl oder den `snowballEdge associate-device` Befehl aus. Ein Beispiel finden Sie unter [Snowball Edge-Geräte entsperren](#).

So stellen Sie die Verbindung zu einem nicht verfügbaren Knoten wieder her, der zwar die Netzwerkkonnektivität, aber nicht die Stromversorgung verloren hat

1. Stellen Sie sicher, dass der Knoten mit demselben internen Netzwerk verbunden ist, in dem sich der Rest des Clusters befindet.
2. Führen Sie den `snowballEdge describe-device`-Befehl aus, um zu sehen, wann der vorher nicht verfügbare Knoten dem Cluster wieder hinzugefügt wird. Ein Beispiel finden Sie unter [Gerätestatus abrufen](#).

Nachdem Sie die oben genannten Verfahren ausgeführt haben, sollten Ihre Knoten normal funktionieren. Sie sollten auch ein read/write Quorum haben. Wenn dies nicht der Fall ist, liegt bei einem oder mehreren Ihrer Knoten möglicherweise ein ernsthafteres Problem vor und diese müssen aus dem Cluster entfernt werden.

Einen Knoten in einem Cluster ersetzen

Um einen Knoten zu ersetzen, müssen Sie zuerst einen Ersatz bestellen. Sie können einen Ersatzknoten über die Konsole AWS CLI, die oder einen der folgenden bestellen AWS SDKs. Wenn Sie einen Ersatzknoten über die Konsole bestellen, können Sie Ersatz für alle Aufträge bestellen, die nicht abgebrochen oder abgeschlossen wurden. Dann trennen Sie den fehlerhaften Knoten vom Cluster, verbinden den Ersatzknoten mit Ihrem Netzwerk und entsperren den Cluster einschließlich

des Ersatzknotens, ordnen den Ersatzknoten dem Cluster zu und starten den Amazon S3 S3-kompatiblen Speicher auf Snowball Edge neu.

So bestellen Sie einen Ersatzknoten über die Konsole

1. Melden Sie sich an der [Managementkonsole für die AWS Snow-Familie](#) an.
2. Suchen und wählen Sie im Auftrags-Dashboard einen Auftrag für einen Knoten, der zu dem Cluster gehört, den Sie erstellt haben.
3. Wählen Sie für Actions (Aktionen) die Option Replace node (Knoten ersetzen) aus.

Dadurch wird der letzte Schritt des Auftragserstellungsassistenten geöffnet. Hierbei sind alle Einstellungen mit denen bei der ursprünglichen Erstellung des Clusters identisch.

4. Wählen Sie Job erstellen aus.

Ihr Ersatz-Snowball Edge ist jetzt auf dem Weg zu Ihnen. Gehen Sie wie folgt vor, um den fehlerhaften Knoten aus dem Cluster zu entfernen.

Um einen Knoten aus einem Cluster zu entfernen

1. Schalten Sie den Knoten aus, der entfernt werden soll. Weitere Informationen finden Sie [unter Snowball Edge ausschalten](#).
2. Verwenden Sie den `describe-cluster` Befehl, um sicherzustellen, dass der fehlerhafte Knoten nicht erreichbar ist. Dies wird durch den Wert von UNREACHABLE für den State Namen des NetworkReachability Objekts angezeigt.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-device-in-cluster
```

Example der **describe-cluster** Ausgabe

```
{
  "ClusterId": "CID12345678-1234-1234-123456789012",
  "Devices": [
    {
      "DeviceId": "JID12345678-1234-1234-123456789012",
      "UnlockStatus": {
```



```

        "State": "UNLOCKED"
    },
    "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.0"
    },
    "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
    },
    "NetworkReachability": {
        "State": "REACHABLE"
    },
    "Tags": []
},
{
    "DeviceId": "JID12345678-1234-1234-1234-123456789013",
    "UnlockStatus": {
        "State": "UNLOCKED"
    },
    "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.1"
    },
    "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
    },
    "NetworkReachability": {
        "State": "REACHABLE"
    },
    "Tags": []
},
{
    "DeviceId": "JID12345678-1234-1234-1234-123456789014",
    "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
    },
    "NetworkReachability": {
        "State": "UNREACHABLE"
    }
}
]
}

```

3. Verwenden Sie den `describe-service` Befehl, um sicherzustellen, dass der Status des `s3-snow` Dienstes lautet `DEGRADED`.

```
snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-device-1-address snow-device-2-address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example der Ausgabe des **describe-service** Befehls

```
{
  "ServiceId": "s3-snow",
  "Autostart": true,
  "Status": {
    "State": "DEGRADED"
  },
  "ServiceCapacities": [
    {
      "Name": "S3 Storage",
      "Unit": "Byte",
      "Used": 38768180432,
      "Available": 82961231819568
    }
  ],
  "Endpoints": [
    {
      "Protocol": "https",
      "Port": 443,
      "Host": "10.0.0.10",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
      },
      "Description": "s3-snow bucket API endpoint (for s3control SDK)",
      "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
      "Status": {
        "State": "ACTIVE"
      }
    }
  ],
}
```

```

    {
      "Protocol": "https",
      "Port": 443,
      "Host": "10.0.0.11",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
      },
      "Description": "Description" : "s3-snow object & bucket API endpoint
(for s3api SDK)",
      "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
      "Status": {
        "State": "ACTIVE"
      }
    },
    {
      "Protocol": "https",
      "Port": 443,
      "Host": "10.0.0.12",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
      },
      "Description": "Description" : "s3-snow bucket API endpoint (for
s3control SDK)",
      "DeviceId": "JID-beta-207012240003-24-02-05-17-17-27",
      "Status": {
        "State": "ACTIVE"
      }
    },
    {
      "Protocol": "https",
      "Port": 443,
      "Host": "10.0.0.13",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
      },
      "Description": "Description" : "s3-snow object & bucket API endpoint
(for s3api SDK)",
      "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
      "Status": {
        "State": "ACTIVE"
      }
    }
  ]
}

```

```
}  
]  
}
```

4. Verwenden Sie den `disassociate-device` Befehl, um den fehlerhaften Knoten vom Cluster zu trennen und ihn daraus zu entfernen.

```
snowballEdge disassociate-device --device-id device-id --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-unhealthy-device
```

Example Ausgabe des Befehls **disassociate-device**

Disassociating your Snowball Edge device from the cluster. Your Snowball Edge device will be disassociated from the cluster when it is in the "DISASSOCIATED" state. You can use the `describe-cluster` command to determine the state of your cluster.

5. Verwenden Sie den `describe-cluster` Befehl erneut, um sicherzustellen, dass der fehlerhafte Knoten vom Cluster getrennt wird.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-healthy-device
```

Example des **describe-cluster** Befehls zeigt an, dass der Knoten getrennt ist

```
{  
  "ClusterId": "CID12345678-1234-1234-1234-123456789012",  
  "Devices": [  
    {  
      "DeviceId": "JID12345678-1234-1234-1234-123456789012",  
      "UnlockStatus": {  
        "State": "UNLOCKED"  
      }  
    }  
  ]  
}
```

```

    },
    "ActiveNetworkInterface": {
      "IpAddress": "10.0.0.0"
    },
    "ClusterAssociation": {
      "ClusterId": "CID12345678-1234-1234-1234-123456789012",
      "State": "ASSOCIATED"
    },
    "NetworkReachability": {
      "State": "REACHABLE"
    },
    "Tags": []
  },
  {
    "DeviceId": "JID12345678-1234-1234-1234-123456789013",
    "UnlockStatus": {
      "State": "UNLOCKED"
    },
    "ActiveNetworkInterface": {
      "IpAddress": "10.0.0.1"
    },
    "ClusterAssociation": {
      "ClusterId": "CID12345678-1234-1234-1234-123456789012",
      "State": "ASSOCIATED"
    },
    "NetworkReachability": {
      "State": "REACHABLE"
    },
    "Tags": []
  },
  {
    "DeviceId": "JID12345678-1234-1234-1234-123456789014",
    "ClusterAssociation": {
      "ClusterId": "CID12345678-1234-1234-1234-123456789012",
      "State": "DISASSOCIATED"
    }
  }
]
}

```

6. Schalten Sie das defekte Gerät aus und setzen Sie es wieder auf. AWS Weitere Informationen finden Sie unter [Ausschalten des Snowball Edge-Geräts und Rückgabe des Snowball Edge-Geräts](#).

Wenn das Ersatzgerät eingetroffen ist, gehen Sie wie folgt vor, um es dem Cluster hinzuzufügen.

Um ein Ersatzgerät hinzuzufügen

1. Positionieren Sie das Ersatzgerät für den Cluster so, dass Sie Zugriff auf die Vorder-, Rück- und Oberseite aller Geräte haben.
2. Schalten Sie den Knoten ein und stellen Sie sicher, dass der Knoten mit demselben internen Netzwerk verbunden ist wie der Rest des Clusters. Weitere Informationen finden Sie unter [Verbindung mit Ihrem lokalen Netzwerk](#) herstellen.
3. Verwenden Sie den `unlock-cluster` Befehl und geben Sie die IP-Adresse des neuen Knotens an.

```
snowballEdge unlock-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-cluster-device --device-ip-addresses node-1-ip-address node-2-ip-address new-node-ip-address
```

Der Status des neuen Knotens bleibt so DEGRADED lange bestehen, bis Sie ihn im nächsten Schritt dem Cluster zuordnen.

4. Verwenden Sie den `associate-device` Befehl, um den Ersatzknoten dem Cluster zuzuordnen.

```
snowballEdge associate-device --device-ip-address new-node-ip-address
```

Example der **associate-device** Befehlsausgabe

```
Associating your Snowball Edge device with the cluster. Your Snowball Edge device will be associated with the cluster when it is in the ASSOCIATED state. You can use the describe-device command to determine the state of your devices.
```

5. Verwenden Sie den `describe-cluster` Befehl, um sicherzustellen, dass der neue Knoten dem Cluster zugeordnet ist.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://node-ip-address
```

Example der **describe-cluster** Befehlsausgabe

```
{
  "ClusterId": "CID12345678-1234-1234-1234-123456789012",
  "Devices": [
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789012",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.0"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    },
    {
      "DeviceId": "JID-CID12345678-1234-1234-1234-123456789013",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.1"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
```

```

        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    },
    {
      "DeviceId": "JID-CID12345678-1234-1234-1234-123456789015",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.2"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    }
  ]
}

```

6. Erstellen Sie auf dem neuen Knoten zwei virtuelle Netzwerkschnittstellen (VNIs). Weitere Informationen finden Sie unter [Starten des Amazon S3 S3-kompatiblen Speichers auf dem Snowball Edge-Service](#).
7. Verwenden Sie den stop-service Befehl, um den s3-Snow-Dienst zu beenden.

```

snowballEdge stop-service --service-id s3-snow --device-ip-addresses cluster-
device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint
https://snow-device-ip-address

```


Example der Befehlsausgabe **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.

8. Verwenden Sie den `start-service` Befehl, um den s3-Snow-Dienst zu starten, nachdem Sie dem Cluster den neuen Knoten hinzugefügt haben.

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses cluster-device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --virtual-network-interface-arns "device-1-vni-ip-address-a device-1-vni-ip-address-b device-2-vni-ip-address-a device-2-vni-ip-address-b device-3-vni-ip-address-a device-3-vni-ip-address-b" --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example der Befehlsausgabe **start-service**

Starting the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.

9. Verwenden Sie den `describe-service` Befehl, um sicherzustellen, dass der s3-Snow-Dienst gestartet wurde.

```
snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-device-1-address snow-device-2-address snow-device-3-address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example der Befehlsausgabe **describe-service**

```
{
  "ServiceId": "s3-snow",
  "Autostart": true,
  "Status": {
    "State": "ACTIVE"
  },
  "ServiceCapacities": [{
    "Name": "S3 Storage",
    "Unit": "Byte",
    "Used": 38768180432,
    "Available": 82961231819568
  }],
  "Endpoints": [{
    "Protocol": "https",
    "Port": 443,
    "Host": "10.0.0.10",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
    },
    "Description": "s3-snow bucket API endpoint (for s3control SDK)",
    "DeviceId": "JID12345678-1234-1234-1234-123456789012",
    "Status": {
      "State": "ACTIVE"
    }
  }, {
    "Protocol": "https",
    "Port": 443,
    "Host": "10.0.0.11",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
    },
    "Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
    "DeviceId": "JID12345678-1234-1234-1234-123456789013",
    "Status": {
      "State": "ACTIVE"
    }
  }, {
    "Protocol": "https",
```

```

        "Port": 443,
        "Host": "10.0.0.12",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow bucket API endpoint (for s3control SDK)",
        "DeviceId": "JID12345678-1234-1234-1234-123456789015",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.13",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.14",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow bucket API endpoint (for s3control SDK)",
        "DeviceId": "JID-beta-207012240003-24-02-05-17-17-28",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.15",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"

```

```
    },
    "Description": "s3-snow object & bucket API endpoint (for s3api SDK),
    "DeviceId": "JID-beta-207012320001-24-02-05-17-17-28",
    "Status": {
        "State": "ACTIVE"
    }
}
}]
}
```

Konfiguration von Amazon S3 S3-kompatiblen Speicher für Snowball Edge-Ereignisbenachrichtigungen

Amazon S3 S3-kompatibler Speicher auf Snowball Edge unterstützt Amazon S3 S3-Ereignisbenachrichtigungen für Objekt-API-Aufrufe, die auf dem Message Queuing Telemetry Transport (MQTT) -Protokoll basieren.

Sie können Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden, um Benachrichtigungen zu erhalten, wenn bestimmte Ereignisse in Ihrem S3-Bucket eintreten. Um Benachrichtigungen zu aktivieren, fügen Sie eine Benachrichtigungskonfiguration hinzu, die die Ereignisse identifiziert, die der Service veröffentlichen soll.

Amazon S3 S3-kompatibler Speicher auf Snowball Edge unterstützt die folgenden Benachrichtigungstypen:

- Neues Objekt erstellte Ereignisse
- Ereignisse zum Entfernen von Objekten
- Ereignismarkierungen von Objekten

Amazon S3 S3-Ereignisbenachrichtigungen konfigurieren

1. Bevor Sie beginnen, müssen Sie über eine MQTT-Infrastruktur in Ihrem Netzwerk verfügen.
2. Führen Sie in Ihrem Snowball Edge-Client den `snowballEdge configure` Befehl aus, um das Snowball Edge-Gerät einzurichten.

Wenn Sie dazu aufgefordert werden, geben Sie die folgenden Informationen ein:

- Der Pfad zu Ihrer Manifestdatei.
 - Der Entsperrcode des Geräts.
 - Der Endpunkt des Geräts (z. B. *https://10.0.0.1*).
3. Führen Sie den folgenden put-notification-configuration Befehl aus, um Benachrichtigungen an einen externen Broker zu senden.

```
snowballEdge put-notification-configuration --broker-endpoint ssl://mqtt-broker-ip-address:8883 --enabled true --service-id s3-snow --ca-certificate file:path-to-mqtt-broker-ca-cert
```

4. Führen Sie den folgenden get-notification-configuration Befehl aus, um zu überprüfen, ob alles korrekt eingerichtet ist:

```
snowballEdge get-notification-configuration --service-id s3-snow
```

Dadurch werden der Broker-Endpunkt und das aktivierte Feld zurückgegeben.

Nachdem Sie den gesamten Cluster so konfiguriert haben, dass er Benachrichtigungen an den MQTT-Broker im Netzwerk sendet, führt jeder Objekt-API-Aufruf zu einer Ereignisbenachrichtigung.

Note

Sie müssen das Thema `s3SnowEvents/Device ID`(oder *Cluster Id* falls es sich um einen Cluster handelt) /BucketName abonnieren. Sie können auch Platzhalter verwenden, zum Beispiel kann der Themenname oder sein. `# s3SnowEvents/#`

Im Folgenden finden Sie ein Beispiel für Amazon S3 S3-kompatiblen Speicher im Snowball Edge-Ereignisprotokoll:

```
{
  "eventDetails": {
    "additionalEventData": {
      "AuthenticationMethod": "AuthHeader",
      "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "SignatureVersion": "SigV4",
      "bytesTransferredIn": 1205,
```

```

        "bytesTransferredOut": 0,
        "x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg=="
    },
    "eventName": "PutObject",
    "eventTime": "2023-01-30T14:13:24.772Z",
    "requestAuthLatencyMillis": 40,
    "requestBandwidthKBs": 35,
    "requestID": "140CD93455CB62B4",
    "requestLatencyMillis": 77,
    "requestLockLatencyNanos": 1169953,
    "requestParameters": {
        "Content-Length": "1205",
        "Content-MD5": "GZdTU0hYHvHgQgmaw2gl4w==",
        "Host": "10.0.2.251",
        "bucketName": "bucket",
        "key": "file-key"
    },
    "requestTTFBLatencyMillis": 77,
    "responseElements": {
        "ETag": "\"19975350e8581ef1e042099ac36825e3\"",
        "Server": "AmazonS3",
        "x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg==",
        "x-amz-request-id": "140CD93455CB62B4"
    },
    "responseStatusCode": 200,
    "sourceIPAddress": "172.31.37.21",
    "userAgent": "aws-cli/1.27.23 Python/3.7.16 Linux/4.14.301-224.520.amzn2.x86_64
botocore/1.29.23",
    "userIdentity": {
        "identityType": "IAMUser",
        "principalId": "531520547609",
        "arn": "arn:aws:iam::531520547609:root",
        "userName": "root"
    }
}
}

```

Weitere Informationen zu Amazon S3 S3-Ereignisbenachrichtigungen finden Sie unter [Amazon S3 S3-Ereignisbenachrichtigungen](#).

Konfiguration lokaler SMTP-Benachrichtigungen auf Snowball Edge

Sie können lokale Benachrichtigungen für Ihre Snowball Edge-Geräte mit Simple Mail Transfer Protocol (SMTP) einrichten. Die lokalen Benachrichtigungen senden E-Mails an konfigurierte Server, wenn sich der Dienststatus (Aktiv, Heruntergestuft, Inaktiv) ändert oder wenn Sie die Schwellenwerte für die Kapazitätsauslastung von 80%, 90% oder 100% überschreiten.

Bevor Sie beginnen, stellen Sie sicher, dass:

- Sie haben Zugriff auf den neuesten Snowball Edge-Client.
- Ihr Gerät ist entsperrt und einsatzbereit.
- Ihr Gerät kann eine Verbindung zum Internet (wenn Sie Amazon Simple Email Service oder einen externen SMTP-Server verwenden) oder zu einem lokalen SMTP-Server herstellen.

Snowball Edge für lokale Benachrichtigungen konfigurieren

Richten Sie einen Snowball Edge ein, um E-Mail-Benachrichtigungen zu senden.

Um das Gerät für SMTP-Benachrichtigungen zu konfigurieren

1. Führen Sie den folgenden Befehl aus, um Ihrem Gerät eine SMTP-Konfiguration hinzuzufügen:

```
# If you don't specify a port, port 587 is the default.
SMTP_ENDPOINT=your-local-smtp-server-endpoint:port

# For multiple email recipients, separate with commas
RECIPIENTS_LIST=your-email-address

snowballEdge put-notification-configuration \
  --service-id local-monitoring \
  --enabled true \
  --type smtp \
  --broker-endpoint "$SMTP_ENDPOINT" \
  --sender example-sender@domain.com \
  --recipients "$RECIPIENTS_LIST"
```

Sie erhalten eine Test-E-Mail von `example-sender@domain.com`, wenn Sie erfolgreich waren.

2. Testen Sie die Konfiguration, indem Sie den folgenden `get-notification-configuration` Befehl ausführen:

```
snowballEdge get-notification-configuration \  
--service-id local-monitoring
```

Die Antwort enthält kein Passwort oder Zertifikat, auch wenn Sie sie angeben.

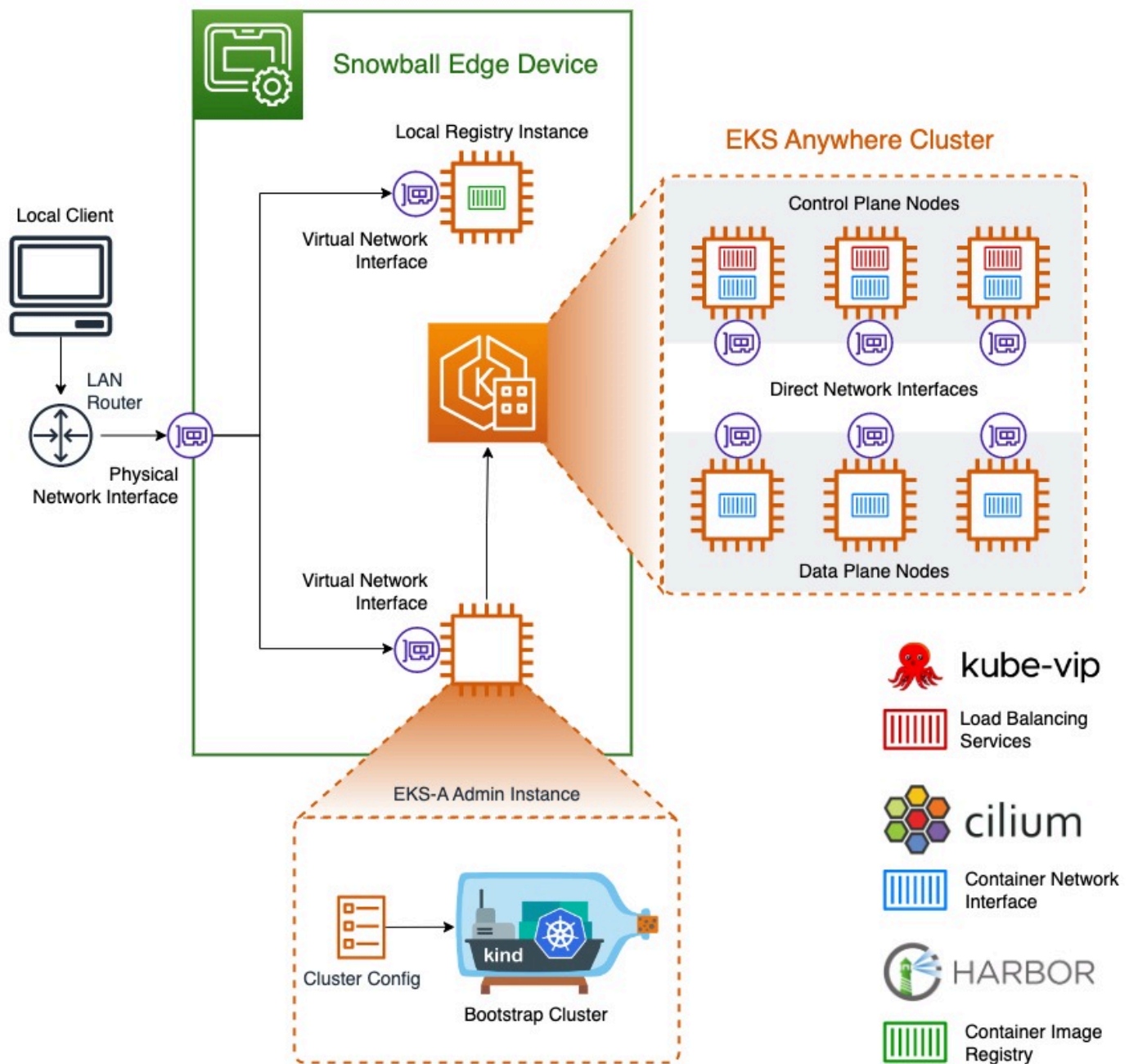
Verwenden von Amazon EKS Anywhere auf AWS Schnee

Amazon EKS Anywhere on AWS Snow unterstützt Sie bei der Erstellung und dem Betrieb von Kubernetes-Clustern auf Snowball Edge. Kubernetes ist Open-Source-Software, die zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen verwendet wird. Sie können Amazon EKS Anywhere auf einem Snowball Edge-Gerät mit oder ohne externe Netzwerkverbindung verwenden. Um Amazon EKS Anywhere auf einem Gerät ohne externe Netzwerkverbindung zu verwenden, stellen Sie eine Container-Registry bereit, die auf dem Snowball Edge-Gerät ausgeführt werden soll. Allgemeine Informationen zu Amazon EKS Anywhere finden Sie in der [Amazon EKS Anywhere Anywhere-Dokumentation](#).

Die Verwendung von Amazon EKS Anywhere on AWS Snow bietet Ihnen folgende Funktionen:

- Stellen Sie einen Kubernetes (K8s) -Cluster mit Amazon EKS Anywhere CLI (eksctl anywhere) auf rechenoptimierten Snowball Edge-Geräten bereit. Sie können Amazon EKS Anywhere auf einem einzelnen Snowball Edge-Gerät oder auf drei oder mehr Geräten bereitstellen, um eine hohe Verfügbarkeit zu gewährleisten.
- Support für Cilium Container Network Interface (CNI).
- Support für Ubuntu 20.04 als Node-Betriebssystem.

Dieses Diagramm zeigt einen Amazon EKS Anywhere Anywhere-Cluster, der auf einem Snowball Edge-Gerät bereitgestellt wird.



Wir empfehlen Ihnen, Ihren Kubernetes-Cluster mit der neuesten verfügbaren Kubernetes-Version zu erstellen, die von Amazon EKS Anywhere unterstützt wird. Weitere Informationen finden Sie unter [Amazon EKS-Anywhere Versioning](#). Wenn Ihre Anwendung eine bestimmte Version von Kubernetes erfordert, verwenden Sie eine beliebige Version von Kubernetes, die im Standard- oder erweiterten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten der Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust der Unterstützung für die Version von Kubernetes, die

Sie verwenden möchten, vermeiden. Weitere Informationen finden Sie im [Amazon EKS Kubernetes-Veröffentlichungskalender](#).

Weitere Informationen zu Amazon EKS Anywhere on AWS Snow finden Sie in der [Amazon EKS Anywhere Anywhere-Dokumentation](#).

Themen

- [Vor der Bestellung eines Snowball Edge-Geräts für Amazon EKS Anywhere on AWS Snow auszuführende Aktionen](#)
- [Bestellung eines Snowball Edge-Geräts zur Verwendung mit Amazon EKS Anywhere on AWS Snow](#)
- [Konfiguration und Ausführung von Amazon EKS Anywhere auf Snowball Edge-Geräten](#)
- [Konfiguration von Amazon EKS Anywhere on AWS Snow für den Betrieb ohne Internetverbindung](#)
- [Cluster auf Snowball Edge-Geräten erstellen und verwalten](#)

Vor der Bestellung eines Snowball Edge-Geräts für Amazon EKS Anywhere on AWS Snow auszuführende Aktionen

Derzeit ist Amazon EKS Anywhere mit computeroptimierten Snowball Edge-Geräten kompatibel. Bevor Sie ein Snowball Edge-Gerät bestellen, sollten Sie einige Dinge zur Vorbereitung tun.

- Erstellen Sie ein Betriebssystem-Image und stellen Sie es bereit, um virtuelle Maschinen auf dem Gerät zu erstellen.
- Ihr Netzwerk muss über eine statische IP-Adresse für den Endpunkt der K8s-Steuerebene verfügen und das Address Resolution Protocol (ARP) zulassen.
- Auf Ihrem Snowball Edge-Gerät müssen bestimmte Ports geöffnet sein. Weitere Informationen zu Ports finden Sie unter [Ports und Protokolle](#) in der Amazon EKS Anywhere Anywhere-Dokumentation.

Themen

- [Erstellen Sie ein Ubuntu EKS Distro AMI für den Snowball Edge](#)
- [Baue ein Harbor-AMI für den Snowball Edge](#)

Erstellen Sie ein Ubuntu EKS Distro AMI für den Snowball Edge

Informationen zum Erstellen des Ubuntu EKS Distro AMI finden Sie unter [Erstellen von Snow-Knotenimages](#).

Der Name des generierten AMI folgt dem Mustercapa-ami-ubuntu-20.04-version-timestamp. Beispiel, capa-ami-ubuntu-20.04-v1.24-1672424524.

Baue ein Harbor-AMI für den Snowball Edge

Richten Sie ein privates Harbor-REGISTRY-AMI ein, das auf dem Snowball Edge-Gerät enthalten sein soll, damit Sie Amazon EKS Anywhere auf dem Gerät ohne externe Netzwerkverbindung verwenden können. Wenn Sie Amazon EKS Anywhere nicht verwenden, während das Snowball Edge-Gerät vom externen Netzwerk getrennt ist, oder wenn Sie eine private Kubernetes-Registrierung in einem AMI haben, die Sie auf dem Gerät verwenden können, können Sie diesen Abschnitt überspringen.

Informationen zum Erstellen des lokalen Harbor-Registry AMI finden Sie unter [Erstellen eines Harbor-AMI](#).

Bestellung eines Snowball Edge-Geräts zur Verwendung mit Amazon EKS Anywhere on AWS Snow

Informationen zur Bestellung Ihres computeroptimierten Snowball Edge finden Sie [Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen](#) in dieser Anleitung und beachten Sie beim Bestellvorgang die folgenden Punkte:

- Wählen Sie in Schritt 1 den Auftragsstyp Nur lokale Datenverarbeitung und Speicher aus.
- Wählen Sie in Schritt 2 den Gerätetyp Snowball Edge Compute Optimized aus.
- Wählen Sie in Schritt 3 Amazon EKS Anywhere on AWS Snow und dann die benötigte Kubernetes-Version aus.

Note

Um die neueste Software bereitzustellen, konfigurieren wir das Gerät möglicherweise mit einer Version von ESK Anywhere, die neuer ist als die, die derzeit verfügbar ist. Weitere Informationen finden Sie unter [Versionierung](#) im Amazon EKS-Benutzerhandbuch.

Wir empfehlen Ihnen, Ihren Kubernetes-Cluster mit der neuesten verfügbaren Kubernetes-Version zu erstellen, die von Amazon EKS Anywhere unterstützt wird. Weitere Informationen finden Sie unter [Amazon EKS-Anywhere Versioning](#). Wenn Ihre Anwendung eine bestimmte Version von Kubernetes erfordert, verwenden Sie eine beliebige Version von Kubernetes, die im Standard- oder erweiterten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten der Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust der Unterstützung für die Version von Kubernetes, die Sie verwenden möchten, vermeiden. Weitere Informationen finden Sie im [Amazon EKS Kubernetes-Veröffentlichungskalender](#).

- Wählen AMIs Sie, ob das EKS-Distro-AMI (siehe [Erstellen Sie ein Ubuntu EKS Distro AMI für den Snowball Edge](#)) und optional das von Ihnen erstellte Harbor-AMI (siehe [Baue ein Harbor-AMI für den Snowball Edge](#)) auf Ihrem Gerät enthalten sein soll.
- Wenn Sie mehrere Snowball Edge-Geräte für Hochverfügbarkeit benötigen, wählen Sie unter Hochverfügbarkeit die Anzahl der benötigten Geräte aus.

Nachdem Sie Ihr Snowball Edge-Gerät oder Ihre Snowball Edge-Geräte erhalten haben, konfigurieren Sie Amazon EKS Anywhere entsprechend [Konfiguration und Ausführung von Amazon EKS Anywhere auf Snowball Edge-Geräten](#).

Konfiguration und Ausführung von Amazon EKS Anywhere auf Snowball Edge-Geräten

Gehen Sie wie folgt vor, um Amazon EKS Anywhere auf Ihren Snowball Edge-Geräten zu konfigurieren und zu starten. Um Amazon EKS Anywhere dann für den Betrieb auf getrennten Geräten zu konfigurieren, führen Sie zusätzliche Verfahren durch, bevor Sie diese Geräte vom externen Netzwerk trennen. Weitere Informationen finden Sie unter [Konfiguration von Amazon EKS Anywhere on AWS Snow für den Betrieb ohne Internetverbindung](#).

Themen

- [Ersteinrichtung für Amazon EKS Anywhere auf Snowball Edge](#)
- [Automatisches Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball Edge-Geräten](#)
- [Manuelles Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball Edge-Geräten](#)

Ersteinrichtung für Amazon EKS Anywhere auf Snowball Edge

Führen Sie die Ersteinrichtung auf jedem Snowball Edge-Gerät durch, indem Sie das Gerät mit Ihrem lokalen Netzwerk verbinden, den Snowball Edge-Client herunterladen, Anmeldeinformationen abrufen und das Gerät entsperren.

Führen Sie die Ersteinrichtung durch

1. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Den Snowball Edge-Client herunterladen und installieren](#).
2. Connect das Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#).
3. Holen Sie sich Anmeldeinformationen, um Ihr Gerät zu entsperren. Weitere Informationen finden Sie unter [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#).
4. Entsperren Sie das Gerät. Weitere Informationen finden Sie unter [Den Snowball Edge freischalten](#). Sie können auch ein Skripttool verwenden, anstatt Geräte manuell zu entsperren. Siehe [Geräte entsperren](#).

Automatisches Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball Edge-Geräten

Sie können Beispielskripttools verwenden, um die Umgebung einzurichten und eine Amazon EKS Anywhere Anywhere-Admin-Instance auszuführen, oder Sie können dies manuell tun. Informationen zur Verwendung der Skripttools finden Sie unter [Geräte entsperren und Umgebung für Amazon EKS Anywhere einrichten](#). Wenn Sie nach der Einrichtung der Umgebung und der Ausführung der Amazon EKS Anywhere-Admin-Instanz Amazon EKS Anywhere so konfigurieren müssen, dass es auf dem Snowball Edge-Gerät funktioniert, wenn keine Verbindung zum Netzwerk besteht, finden Sie weitere Informationen unter [Konfiguration von Amazon EKS Anywhere on AWS Snow für den Betrieb ohne Internetverbindung](#). Andernfalls lesen Sie unter [Cluster auf Snowball Edge-Geräten erstellen und verwalten](#) weiter.

Informationen zum manuellen Einrichten der Umgebung und zum Ausführen einer Amazon EKS Anywhere Anywhere-Admin-Instanz finden Sie unter [Manuelles Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball Edge-Geräten](#).

Manuelles Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball Edge-Geräten

Bevor Sie Amazon EKS Anywhere auf einem Snowball Edge-Gerät konfigurieren, richten Sie ein Profil für den Snowball Edge-Client ein. Weitere Informationen finden Sie unter [Konfiguration und Verwendung des Snowball Edge-Clients](#).

Themen

- [Einen lokalen Amazon EKS Anywhere IAM-Benutzer erstellen](#)
- [\(Optional\) Erstellen und importieren Sie einen Secure Shell-Schlüssel auf einem Snowball Edge](#)
- [Führen Sie eine Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge aus und übertragen Sie Anmelde- und Zertifikatsdateien darauf](#)

Einen lokalen Amazon EKS Anywhere IAM-Benutzer erstellen

Um bewährte Sicherheitsmethoden zu erhalten, erstellen Sie einen lokalen IAM-Benutzer für Amazon EKS Anywhere auf dem Snowball Edge-Gerät. Sie können dies manuell mithilfe der folgenden Verfahren tun.

Note

Tun Sie dies für jedes Snowball Edge-Gerät, das Sie verwenden.

Erstellen Sie einen lokalen Benutzer auf dem Snowball Edge

Verwenden Sie den `create-user` Befehl, um den Amazon EKS Anywhere IAM-Benutzer zu erstellen.

```
aws iam create-user --user-name user-name --endpoint http://snowball-ip:6078 --  
profile profile-name  
{  
  "User": {  
    "Path": "/",  
    "UserName": "eks-a-user",  
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",  
    "Arn": "arn:aws:iam::123456789012:user/eks-a-user",  
    "CreateDate": "2022-04-06T00:13:35.665000+00:00"
```

} }

Erstellen Sie eine Richtlinie für den lokalen Benutzer auf dem Snowball Edge

Erstellen Sie ein Richtliniendokument, verwenden Sie es, um eine IAM-Richtlinie zu erstellen, und hängen Sie diese Richtlinie an den lokalen Benutzer von Amazon EKS Anywhere an.

Um ein Richtliniendokument zu erstellen und es an den lokalen Benutzer von Amazon EKS Anywhere anzuhängen

1. Erstellen Sie ein Richtlinienokument und speichern Sie es auf Ihrem Computer. Kopieren Sie die unten stehende Richtlinie in das Dokument.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snowball-device:DescribeDevice",
        "snowball-device:CreateDirectNetworkInterface",
        "snowball-device>DeleteDirectNetworkInterface",
        "snowball-device:DescribeDirectNetworkInterfaces",
        "snowball-device:DescribeDeviceSoftware"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:TerminateInstances",
        "ec2:ImportKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeImages",

```



```

        "ec2:DeleteTags"
      ],
      "Resource": ["*"]
    }
  ]
}

```

2. Verwenden Sie den `create-policy` Befehl, um eine IAM-Richtlinie auf der Grundlage des Richtliniendokuments zu erstellen. Der Wert des `--policy-document` Parameters sollte den absoluten Pfad zur Richtliniendatei verwenden. Beispiel: `file:///home/user/policy-name.json`

```

aws iam create-policy --policy-name policy-name --policy-document file:///home/user/policy-name.json --endpoint http://snowball-ip:6078 --profile profile-name {
  "Policy": {
    "PolicyName": "policy-name",
    "PolicyId":
      "ANPACEMGEZDGNBVG3TQ0JQGEZAAAABP76TE5MKAAAABCCOTR2IJ43NBTJRZBU",
    "Arn": "arn:aws:iam::123456789012:policy/policy-name",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "CreateDate": "2022-04-06T04:46:56.907000+00:00",
    "UpdateDate": "2022-04-06T04:46:56.907000+00:00"
  }
}

```

3. Verwenden Sie den `attach-user-policy` Befehl, um die IAM-Richtlinie an den lokalen Benutzer von Amazon EKS Anywhere anzuhängen.

```

aws iam attach-user-policy --policy-arn policy-arn --user-name user-name --endpoint http://snowball-ip:6078 --profile profile-name

```

Erstellen Sie einen Zugriffsschlüssel und eine Anmeldeinformationsdatei auf dem Snowball Edge

Erstellen Sie einen Zugriffsschlüssel für den lokalen Amazon EKS Anywhere IAM-Benutzer. Erstellen Sie anschließend eine Anmeldeinformationsdatei und fügen Sie darin die Werte des AccessKeyId lokalen Benutzers ein. SecretAccessKey Die Anmeldeinformationsdatei wird später von der Amazon EKS Anywhere Anywhere-Admin-Instanz verwendet.

1. Verwenden Sie den `create-access-key` Befehl, um einen Zugriffsschlüssel für den lokalen Amazon EKS Anywhere Anywhere-Benutzer zu erstellen.

```
aws iam create-access-key --user-name user-name --endpoint http://snowball-ip:6078
--profile profile-name
{
  "AccessKey": {
    "UserName": "eks-a-user",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "Status": "Active",
    "SecretAccessKey": "RTT/wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
    "CreateDate": "2022-04-06T04:23:46.139000+00:00"
  }
}
```

2. Erstellen Sie eine Anmeldeinformationsdatei. Speichern Sie darin die SecretAccessKey Werte AccessKeyId und im folgenden Format.

```
[snowball-ip]
aws_access_key_id = ABCDEFGHIJKLMNOPQR2T
aws_secret_access_key = AfSD7sYz/TBZtzkReBl6PuuISzJ2WtNkeePw+nNzJ
region = snow
```

Note

Wenn Sie mit mehreren Snowball Edge-Geräten arbeiten, spielt die Reihenfolge der Anmeldeinformationen in der Datei keine Rolle, aber die Anmeldeinformationen für alle Geräte müssen sich in einer Datei befinden.

Erstellen Sie eine Zertifikatsdatei für die Admin-Instanz auf dem Snowball Edge

Die Amazon EKS Anywhere Anywhere-Admin-Instanz benötigt die Zertifikate der Snowball Edge-Geräte, um auf ihnen ausgeführt werden zu können. Erstellen Sie eine Zertifikatsdatei, die das Zertifikat für den Zugriff auf Snowball Edge-Geräte zur späteren Verwendung durch die Amazon EKS Anywhere Anywhere-Admin-Instanz enthält.

Um eine Zertifikatsdatei zu erstellen

1. Verwenden Sie den `list-certificates` Befehl, um Zertifikate für jedes Snowball Edge-Gerät abzurufen, das Sie verwenden möchten.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge list-certificates --endpoint
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-
code
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-device:::certificate/xxx",
    "SubjectAlternativeNames" : [ "ID:JID-xxx" ]
  } ]
}
```

2. Verwenden Sie den Wert von `CertificateArn` als Wert für den `--certificate-arn` Parameter des `get-certificate` Befehls.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge get-certificate --certificate-arn ARN
--endpoint https://snowball-ip --manifest-file path-to-manifest-file --unlock-
code unlock-code
```

3. Erstellen Sie eine Gerätezertifikatsdatei. Fügen Sie die Ausgabe von `get-certificate` in die Zertifikatsdatei ein. Im Folgenden finden Sie ein Beispiel für das Speichern der Ausgabe.

Note

Wenn Sie mit mehreren Snowball Edge-Geräten arbeiten, spielt die Reihenfolge der Anmeldeinformationen in der Datei keine Rolle, aber die Anmeldeinformationen für alle Geräte müssen sich in einer Datei befinden.

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydG1maWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydG1m
aWNhdGV1a3NhIHNUb3cgcGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZm1jYXRlZWtzYSBzbm93IHRlc3QgY2VydG1maWNhdGV1a3NhIHNUb3cgcGVz
dCBjZXJ0aWZpY2F0ZQMIIDXCcCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----
```

4. Wiederholen Sie [Einen lokalen Amazon EKS Anywhere IAM-Benutzer erstellen](#) den Vorgang, um auf allen Snowball Edge-Geräten einen lokalen IAM-Benutzer für Amazon EKS Anywhere zu erstellen.

(Optional) Erstellen und importieren Sie einen Secure Shell-Schlüssel auf einem Snowball Edge

Verwenden Sie dieses optionale Verfahren, um einen Secure Shell (SSH) -Schlüssel für den Zugriff auf alle Amazon EKS Anywhere Anywhere-Node-Instances zu erstellen und den öffentlichen Schlüssel auf alle Snowball Edge-Geräte zu importieren. Bewahren Sie diese Schlüsseldatei auf und sichern Sie sie.

Wenn Sie dieses Verfahren überspringen, erstellt und importiert Amazon EKS Anywhere bei Bedarf automatisch einen SSH-Schlüssel. Dieser Schlüssel wird auf der Admin-Instanz in `${PWD}/${CLUSTER_NAME}/eks-a-id_rsa` gespeichert.

Erstellen Sie einen SSH-Schlüssel und importieren Sie ihn in die Amazon EKS Anywhere Anywhere-Instance

1. Verwenden Sie den `ssh-keygen` Befehl, um einen SSH-Schlüssel zu generieren.

```
ssh-keygen -t rsa -C "key-name" -f path-to-key-file
```

2. Verwenden Sie den `import-key-pair` Befehl, um den Schlüssel von Ihrem Computer auf das Snowball Edge-Gerät zu importieren.

 Note

Der Wert des `key-name` Parameters muss identisch sein, wenn Sie den Schlüssel auf alle Geräte importieren.

```
aws ec2 import-key-pair --key-name key-name --public-key-material fileb:///path/to/  
key-file --endpoint http://snowball-ip:8008 --profile profile-name  
{  
  "KeyFingerprint": "5b:0c:fd:e1:a0:69:05:4c:aa:43:f3:3b:3e:04:7f:51",  
  "KeyName": "default",  
  "KeyPairId": "s.key-85edb5d820c92a6f8"  
}
```

Führen Sie eine Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge aus und übertragen Sie Anmelde- und Zertifikatsdateien darauf

Führen Sie eine Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge aus

Gehen Sie wie folgt vor, um eine Amazon EKS Anywhere Anywhere-Admin-Instance manuell auszuführen, ein Virtual Network Interface (VNI) für die Admin-Instance zu konfigurieren, den Status der Instance zu überprüfen, einen SSH-Schlüssel zu erstellen und damit eine Verbindung zur Admin-Instance herzustellen. Sie können ein Beispielskripttool verwenden, um die Erstellung einer Amazon EKS Anywhere Anywhere-Admin-Instance und die Übertragung von Anmelde- und Zertifikatsdateien auf diese Instance zu automatisieren. Weitere Informationen finden [Sie unter Amazon EKS Anywhere Anywhere-Admin-Instanz erstellen](#). Nachdem das Skripttool abgeschlossen ist, können Sie per SSH auf die Instance zugreifen und Cluster erstellen, indem Sie auf [Cluster auf Snowball Edge-Geräten erstellen und verwalten](#) verweisen. Wenn Sie die Amazon EKS Anywhere Anywhere-Instance manuell einrichten möchten, gehen Sie wie folgt vor.

 Note

Wenn Sie mehr als ein Snowball Edge-Gerät zur Bereitstellung des Clusters verwenden, können Sie eine Amazon EKS Anywhere Anywhere-Admin-Instance auf jedem der Snowball Edge-Geräte starten.

So führen Sie eine Amazon EKS Anywhere Anywhere-Admin-Instance aus

1. Verwenden Sie den `create-key-pair` Befehl, um einen SSH-Schlüssel für die Amazon EKS Anywhere Anywhere-Admin-Instance zu erstellen. Der Befehl speichert den Schlüssel unter. `$PWD/key-file-name`

```
aws ec2 create-key-pair --key-name key-name --query 'KeyMaterial' --output text --  
endpoint http://snowball ip:8008 > key-file-name --profile profile-name
```

2. Verwenden Sie den `describe-images` Befehl, um den Bildnamen zu finden, `eks-anywhere-admin` der mit F beginnt.

```
aws ec2 describe-images --endpoint http://snowball-ip:8008 --profile profile-name
```

3. Verwenden Sie den `run-instance` Befehl, um eine `eks-a` admin-Instance mit dem Amazon EKS Anywhere Anywhere-Admin-Image zu starten.

```
aws ec2 run-instances --image-id eks-a-admin-image-id --key-name key-name --  
instance-type sbe-c.xlarge --endpoint http://snowball-ip:8008 --profile profile-  
name
```

4. Verwenden Sie den `describe-instances` Befehl, um den Status der Amazon EKS Anywhere Anywhere-Instance zu überprüfen. Warten Sie, bis der Befehl anzeigt, dass der Status der Instance ist, `running` bevor Sie fortfahren.

```
aws ec2 describe-instances --instance-id instance-id --endpoint http://snowball-  
ip:8008 --profile profile-name
```

5. Notieren Sie sich in der Ausgabe des `describe-device` Befehls den Wert von `PhysicalNetworkInterfaceId` für die physische Netzwerkschnittstelle, die mit Ihrem Netzwerk verbunden ist. Sie werden dies verwenden, um ein VNI zu erstellen.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge describe-device --endpoint  
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-  
code
```

6. Erstellen Sie ein VNI für die Amazon EKS Anywhere Anywhere-Admin-Instanz. Verwenden Sie den Wert von `PhysicalNetworkInterfaceId` als Wert des `physical-network-interface-id` Parameters.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge create-virtual-network-interface  
--ip-address-assignment dhcp --physical-network-interface-id PNI --endpoint  
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-  
code
```

7. Verwenden Sie den Wert von `IpAddress` als Wert des `public-ip` Parameters des `associate-address` Befehls, um die öffentliche Adresse der Amazon EKS Anywhere Anywhere-Admin-Instance zuzuordnen.

```
aws ec2 associate-address --instance-id instance-id --public-ip VNI-IP --endpoint  
http://snowball-ip:8008 --profile profile-name
```

8. Stellen Sie per SSH Connect zur Amazon EKS Anywhere Anywhere-Admin-Instanz her.

```
ssh -i path-to-key ec2-user@VNI-IP
```

Zertifikat- und Anmeldeinformationsdateien an die Admin-Instanz auf dem Snowball Edge übertragen

Nachdem die Amazon EKS Anywhere Anywhere-Admin-Instance ausgeführt wurde, übertragen Sie die Anmeldeinformationen und Zertifikate Ihrer Snowball Edge-Geräte auf die Admin-Instance. Führen Sie den folgenden Befehl in demselben Verzeichnis aus, in dem Sie die Anmelde- und Zertifikatsdateien gespeichert haben, in [Erstellen Sie einen Zugriffsschlüssel und eine](#)

Anmeldeinformationsdatei auf dem Snowball Edge und Erstellen Sie eine Zertifikatsdatei für die Admin-Instanz auf dem Snowball Edge.

```
scp -i path-to-key path-to-credentials-file path-to-certificates-file ec2-user@eks-  
admin-instance-ip:~
```

Überprüfen Sie den Inhalt der Dateien auf der Amazon EKS Anywhere Anywhere-Admin-Instanz. Im Folgenden finden Sie Beispiele für die Anmelde- und Zertifikatsdateien.

```
[192.168.1.1]  
aws_access_key_id = EMGEZDGNBVGy3TQ0JQGEZB5ULEAAIWHWUJDDEXAMPLE  
aws_secret_access_key = AUHpqj00GZQHEYXDbN0neLN1fR0gEXAMPLE  
region = snow  
  
[192.168.1.2]  
aws_access_key_id = EMGEZDGNBVGy3TQ0JQGEZG507F3FJUCMYRMI4KPIEXAMPLE  
aws_secret_access_key = kY4C18+RJA wq/bu28Y8fUJepwqhDEXAMPLE  
region = snow
```

```
-----BEGIN CERTIFICATE-----  
ZWtzYSBzbm93IHRlc3QgY2VydGlmZWVhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm  
aWNhdGVla3NhIHhNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGN1  
cnRpZm1jYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmZWVhdGVla3NhIHhNub3cgdGVz  
dCBjZXJ0aWZpY2F0ZQMIIDXCcCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ  
...  
-----END CERTIFICATE-----  
  
-----BEGIN CERTIFICATE-----  
KJ0FP12PAYPEjxr81/PoCXfZeARBzn9WLUH5yz1ta+sYUJouzhzWuLJYA1xqcCPY  
mhV1kRsN4hVd1BNRnCCpRF766yjdJeibKVzXQxoXoZBjr0kuGwqRy3d3ndjK77h4  
OR5Fv9mjGf7CjcaSjk/4iwmZvRSaQacb0YG5GvEb4mfUAuVtuFoMeYfnAgMBAAGj  
azBpMAwGA1UdEwQFMAMBAf8wHQYDVR00BBYEFL/bRcnBRuSM5+FcyFa8HfIBomdF  
...  
-----END CERTIFICATE-----
```


Konfiguration von Amazon EKS Anywhere on AWS Snow für den Betrieb ohne Internetverbindung

Schließen Sie diese zusätzliche Konfiguration von Amazon EKS Anywhere auf dem Snowball Edge-Gerät ab, während es mit einem Netzwerk verbunden ist, um Amazon EKS Anywhere für die Ausführung in einer Umgebung ohne externe Netzwerkverbindung vorzubereiten.

Informationen zur Konfiguration von Amazon EKS Anywhere für die Nutzung ohne Verbindung mit Ihrer eigenen lokalen, privaten Kubernetes-Registry finden Sie unter [Registry Mirror-Konfiguration](#) in der EKS Anywhere-Dokumentation.

Wenn Sie ein privates Harbor-REGISTRY-AMI erstellt haben, gehen Sie wie in diesem Abschnitt beschrieben vor.

Themen

- [Konfigurieren Sie die Harbor-Registrierung auf einem Snowball Edge-Gerät](#)
- [Verwenden Sie die Harbor-Registrierung auf der Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge](#)

Konfigurieren Sie die Harbor-Registrierung auf einem Snowball Edge-Gerät

Siehe [Harbor auf einem Snowball Edge-Gerät konfigurieren](#).

Verwenden Sie die Harbor-Registrierung auf der Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge

Weitere Informationen finden Sie unter [Importieren von Amazon EKS Anywhere Anywhere-Container-Images in die lokale Harbor-Registrierung auf einem Snowball Edge-Gerät](#).

Cluster auf Snowball Edge-Geräten erstellen und verwalten

Bewährte Methoden für die Erstellung von Clustern auf einem Snowball Edge

Informationen zum Erstellen eines Amazon EKS Anywhere Anywhere-Clusters finden Sie unter [Create Snow clusters](#).

Beachten Sie bei der Erstellung von Amazon EKS Anywhere Anywhere-Clustern auf Snowball Edge-Geräten die folgenden bewährten Methoden:

- Bevor Sie einen Cluster in einem statischen IP-Adressbereich erstellen, stellen Sie sicher, dass es auf Ihrem Snowball Edge-Gerät keine anderen Cluster gibt, die denselben IP-Adressbereich verwenden.
- Bevor Sie einen Cluster mit DHCP-Adressierung auf Ihrem Snowball Edge-Gerät erstellen, stellen Sie sicher, dass sich alle statischen IP-Adressbereiche, die für Cluster verwendet werden, nicht im DHCP-Pool-Subnetz befinden.
- Wenn Sie mehr als einen Cluster erstellen, warten Sie, bis ein Cluster erfolgreich bereitgestellt wurde und läuft, bevor Sie einen anderen erstellen.

Aktualisieren von Clustern auf einem Snowball Edge

Um ein Amazon EKS Anywhere Admin AMI oder EKS Distro AMI zu aktualisieren, wenden Sie sich an AWS Support. Support stellt ein Snowball Edge-Update bereit, das das aktualisierte AMI enthält. Laden Sie anschließend das Snowball Edge-Update herunter und installieren Sie es. Siehe [Updates auf Snowball Edge-Geräte herunterladen](#) und [Updates auf Snowball Edge-Geräten installieren](#).

Nachdem Sie Ihr Amazon EKS Anywhere AMI aktualisiert haben, müssen Sie eine neue Amazon EKS Anywhere Anywhere-Admin-Instance starten. Siehe [Führen Sie eine Amazon EKS Anywhere Anywhere-Admin-Instanz auf einem Snowball Edge aus](#). Kopieren Sie dann die Schlüsseldateien, den Cluster-Ordner, die Anmeldeinformationen und Zertifikate von der vorherigen Admin-Instance auf die aktualisierte Instance. Diese befinden sich in einem Ordner, der nach dem Cluster benannt ist.

Bereinigen von Clusterressourcen auf einem Snowball Edge

Wenn Sie mehrere Cluster auf Ihren Snowball Edge-Geräten erstellen und diese nicht korrekt löschen, oder wenn im Cluster ein Problem auftritt und der Cluster nach der Wiederaufnahme Ersatzknoten erstellt, kommt es zu einem Ressourcenleck. Ein Beispielskripttool steht Ihnen zur Verfügung, das Sie ändern und verwenden können, um Ihre Amazon EKS Anywhere Anywhere-Admin-Instance und Ihre Snowball Edge-Geräte zu bereinigen. Weitere Informationen zu [Tools zur AWS Schneeräumung finden Sie in Amazon EKS Anywhere](#).

Lokales Verwenden von IAM auf einem Snowball Edge

AWS Identity and Access Management (IAM) hilft Ihnen, den Zugriff auf AWS Ressourcen, die auf Ihrem AWS Snowball Edge Gerät ausgeführt werden, sicher zu kontrollieren. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.

IAM wird lokal auf Ihrem Gerät unterstützt. Sie können den lokalen IAM-Dienst verwenden, um neue Benutzer zu erstellen und ihnen IAM-Richtlinien zuzuweisen. Sie können diese Richtlinien verwenden, um den für die Ausführung zugewiesener Aufgaben notwendigen Zugriff zu ermöglichen. Sie können einem Benutzer beispielsweise die Möglichkeit geben, Daten zu übertragen, seine Fähigkeit jedoch einschränken, neue EC2 Amazon-kompatible Instances zu erstellen.

Darüber hinaus können Sie mit AWS -Security-Token-Service (AWS STS) auf Ihrem Gerät lokale, sitzungsbasierte Anmeldeinformationen erstellen. Informationen zum IAM-Dienst finden Sie unter [Erste Schritte](#) im IAM-Benutzerhandbuch.

Die Root-Anmeldeinformationen Ihres Geräts können nicht deaktiviert werden, und Sie können in Ihrem Konto keine Richtlinien verwenden, um dem AWS-Konto Root-Benutzer ausdrücklich den Zugriff zu verweigern. Wir empfehlen Ihnen, Ihre Root-Benutzerzugriffsschlüssel zu sichern und IAM-Benutzeranmeldedaten für die tägliche Interaktion mit Ihrem Gerät zu erstellen.

Important

Die Dokumentation in diesem Abschnitt bezieht sich auf die lokale Verwendung von IAM auf einem AWS Snowball Edge Gerät. Informationen zur Verwendung von IAM in der finden Sie AWS Cloud unter. [Identity and Access Management in AWS Snowball Edge](#)

Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter [Portanforderungen für AWS Dienste auf einem Snowball Edge](#).

Themen

- [Verwenden der API-Operationen AWS CLI und auf einem Snowball Edge](#)
- [Liste der unterstützten AWS CLI IAM-Befehle auf einem Snowball Edge](#)
- [Beispiele für IAM-Richtlinien auf Snowball Edge](#)
- [TrustPolicy Beispiel auf einem Snowball Edge](#)

Verwenden der API-Operationen AWS CLI und auf einem Snowball Edge

Wenn Sie die API-Operationen AWS CLI oder verwenden, um IAM- AWS STS, Amazon S3- und EC2 Amazon-Befehle auf Snowball Edge auszugeben, müssen Sie das `region` als "snow" angeben. Sie können dies mithilfe `aws configure` oder innerhalb des Befehls selbst tun, wie in den folgenden Beispielen.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Oder

```
aws iam list-users --endpoint http://192.0.2.0:6078 --region snow --profile
snowballEdge
```

Note

Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel, die lokal verwendet werden, AWS Snowball Edge können nicht mit den Schlüsseln in der AWS Cloud ausgetauscht werden.

Liste der unterstützten AWS CLI IAM-Befehle auf einem Snowball Edge

Im Folgenden finden Sie eine Beschreibung der Teilmenge der AWS CLI Befehle und Optionen für IAM, die auf Snowball Edge-Geräten unterstützt werden. Wenn ein Befehl oder eine Option im Folgenden nicht aufgeführt ist, wird diese(r) nicht unterstützt. Nicht unterstützte Parameter für Befehle sind in der Beschreibung angegeben.

- [attach-role-policy](#)— Fügt die angegebene verwaltete Richtlinie der angegebenen IAM-Rolle hinzu.
- [attach-user-policy](#)— Ordnet dem angegebenen Benutzer die angegebene verwaltete Richtlinie zu.
- [create-access-key](#)— Erstellt einen neuen lokalen geheimen IAM-Zugriffsschlüssel und die entsprechende AWS Zugriffsschlüssel-ID für den angegebenen Benutzer.
- [create-policy](#) — Erstellt eine neue, von IAM verwaltete Richtlinie für Ihr Gerät.
- [create-role](#) — Erstellt eine neue lokale IAM-Rolle für Ihr Gerät. Die folgenden Parameter werden nicht unterstützt:
 - Tags
 - PermissionsBoundary
- [create-user](#) — Erstellt einen neuen lokalen IAM-Benutzer für Ihr Gerät. Die folgenden Parameter werden nicht unterstützt:
 - Tags
 - PermissionsBoundary
- [delete-access-key](#)— Löscht einen neuen lokalen geheimen IAM-Zugriffsschlüssel und die entsprechende AWS Zugriffsschlüssel-ID für den angegebenen Benutzer.
- [delete-policy](#) — Löscht die angegebene verwaltete Richtlinie.
- [delete-role](#) — Löscht die angegebene Rolle.
- [delete-user](#) — Löscht den angegebenen Benutzer.
- [detach-role-policy](#)— Entfernt die angegebene verwaltete Richtlinie aus der angegebenen Rolle.
- [detach-user-policy](#)— Entfernt die angegebene verwaltete Richtlinie vom angegebenen Benutzer.
- [get-policy](#) — Ruft Informationen über die angegebene verwaltete Richtlinie ab, einschließlich der Standardversion der Richtlinie und der Gesamtzahl der lokalen IAM-Benutzer, -Gruppen und -Rollen, an die die Richtlinie angehängt ist.
- [get-policy-version](#)— Ruft Informationen über die angegebene Version der angegebenen verwalteten Richtlinie ab, einschließlich des Richtliniendokuments.
- [get-role](#) — Ruft Informationen über die angegebene Rolle ab, einschließlich des Pfads, der GUID, des ARN und der Vertrauensrichtlinie der Rolle, die die Erlaubnis erteilt, die Rolle anzunehmen.
- [get-user](#) — Ruft Informationen über den angegebenen IAM-Benutzer ab, einschließlich des Erstellungsdatums, des Pfads, der eindeutigen ID und des ARN des Benutzers.
- [list-access-keys](#)— Gibt Informationen über den Zugriffsschlüssel zurück, der dem angegebenen IDs IAM-Benutzer zugeordnet ist.

- [list-attached-role-policies](#)— Listet alle verwalteten Richtlinien auf, die der angegebenen IAM-Rolle zugeordnet sind.
- [list-attached-user-policies](#)— Listet alle verwalteten Richtlinien auf, die dem angegebenen IAM-Benutzer zugeordnet sind.
- [list-entities-for-policy](#)— Listet alle lokalen IAM-Benutzer, -Gruppen und -Rollen auf, denen die angegebene verwaltete Richtlinie zugeordnet ist.
 - --EntityFilter: Es werden ausschließlich die Werte `role` und `user` unterstützt.
- [list-policies](#)— Listet alle verwalteten Richtlinien auf, die in Ihrer lokalen Umgebung verfügbar sind. AWS-Konto Der folgende Parameter wird nicht unterstützt:
 - --PolicyUsageFilter
- [list-roles](#)— Listet die lokalen IAM-Rollen auf, die das angegebene Pfadpräfix haben.
- [list-users](#)— Listet die IAM-Benutzer auf, die das angegebene Pfadpräfix haben.
- [update-access-key](#)— Ändert den Status des angegebenen Zugriffsschlüssels von Aktiv in Inaktiv oder umgekehrt.
- [update-assume-role-policy](#)— Aktualisiert die Richtlinie, die einer IAM-Entität die Erlaubnis erteilt, eine Rolle anzunehmen.
- [update-role](#)— Aktualisiert die Beschreibung oder die Einstellung für die maximale Sitzungsdauer einer Rolle.
- [update-user](#)— Aktualisiert den Namen und den Pfad and/or des angegebenen IAM-Benutzers.

Unterstützte IAM-API-Operationen auf Snowball Edge

Im Folgenden finden Sie die IAM-API-Operationen, die Sie mit einem Snowball Edge verwenden können, mit Links zu ihren Beschreibungen in der IAM-API-Referenz.

- [AttachRolePolicy](#)— Fügt die angegebene verwaltete Richtlinie der angegebenen IAM-Rolle hinzu.
- [AttachUserPolicy](#)— Ordnet dem angegebenen Benutzer die angegebene verwaltete Richtlinie zu.
- [CreateAccessKey](#)— Erstellt einen neuen lokalen geheimen IAM-Zugriffsschlüssel und die entsprechende AWS Zugriffsschlüssel-ID für den angegebenen Benutzer.
- [CreatePolicy](#)— Erstellt eine neue IAM-verwaltete Richtlinie für Ihr Gerät.
- [CreateRole](#)— Erstellt eine neue lokale IAM-Rolle für Ihr Gerät.
- [CreateUser](#)— Erzeugt einen neuen lokalen IAM-Benutzer für Ihr Gerät.

Die folgenden Parameter werden nicht unterstützt:

- Tags
- PermissionsBoundary
- [DeleteAccessKey](#)— Löscht den angegebenen Zugriffsschlüssel.
- [DeletePolicy](#)— Löscht die angegebene verwaltete Richtlinie.
- [DeleteRole](#)— Löscht die angegebene Rolle.
- [DeleteUser](#)— Löscht den angegebenen Benutzer.
- [DetachRolePolicy](#)— Entfernt die angegebene verwaltete Richtlinie aus der angegebenen Rolle.
- [DetachUserPolicy](#)— Entfernt die angegebene verwaltete Richtlinie vom angegebenen Benutzer.
- [GetPolicy](#)— Ruft Informationen über die angegebene verwaltete Richtlinie ab, einschließlich der Standardversion der Richtlinie und der Gesamtzahl der lokalen IAM-Benutzer, -Gruppen und -Rollen, denen die Richtlinie zugeordnet ist.
- [GetPolicyVersion](#)— Ruft Informationen über die angegebene Version der angegebenen verwalteten Richtlinie ab, einschließlich des Richtliniendokuments.
- [GetRole](#)— Ruft Informationen über die angegebene Rolle ab, einschließlich des Pfads, der GUID, des ARN und der Vertrauensrichtlinie der Rolle, die die Erlaubnis erteilt, die Rolle anzunehmen.
- [GetUser](#)— Ruft Informationen über den angegebenen IAM-Benutzer ab, einschließlich des Erstellungsdatums, des Pfads, der eindeutigen ID und des ARN des Benutzers.
- [ListAccessKeys](#)— Gibt Informationen über den Zugriffsschlüssel zurück, der dem angegebenen IAM-Benutzer IDs zugeordnet ist.
- [ListAttachedRolePolicies](#)— Listet alle verwalteten Richtlinien auf, die der angegebenen IAM-Rolle zugeordnet sind.
- [ListAttachedUserPolicies](#)— Listet alle verwalteten Richtlinien auf, die dem angegebenen IAM-Benutzer zugeordnet sind.
- [ListEntitiesForPolicy](#)— Ruft Informationen über den angegebenen IAM-Benutzer ab, einschließlich des Erstellungsdatums, des Pfads, der eindeutigen ID und des ARN des Benutzers.
 - --EntityFilter: Es werden ausschließlich die Werte `role` und `user` unterstützt.
- [ListPolicies](#)— Listet alle verwalteten Richtlinien auf, die in Ihrer Region verfügbar sind. AWS-Konto
Der folgende Parameter wird nicht unterstützt:
 - --PolicyUsageFilter
- [ListRoles](#)— Listet die lokalen IAM-Rollen auf, die das angegebene Pfadpräfix haben.
- [ListUsers](#)— Listet die IAM-Benutzer auf, die das angegebene Pfadpräfix haben.

- [UpdateAccessKey](#)— Ändert den Status des angegebenen Zugriffsschlüssels von Aktiv in Inaktiv oder umgekehrt.
- [UpdateAssumeRolePolicy](#)— Aktualisiert die Richtlinie, die einer IAM-Entität die Erlaubnis erteilt, eine Rolle anzunehmen.
- [UpdateRole](#)— Aktualisiert die Beschreibung oder die Einstellung für die maximale Sitzungsdauer einer Rolle.
- [UpdateUser](#)— Aktualisiert den Namen und and/or den Pfad des angegebenen IAM-Benutzers.

Unterstützte IAM-Richtlinienversion und Grammatik auf Snowball Edge

Im Folgenden finden Sie die lokale IAM-Unterstützungsversion 2012-10-17 der IAM-Richtlinie und einen Teilsatz der Richtliniengrammatik.

Richtlinientyp	Unterstützte Grammatik
Identitätsbasierte Richtlinien (Benutzer-/Rollenrichtlinie)	„Effect“, „Action“ und „Resource“  Note Lokales IAM „Condition“, „NotAction“, „NotResource“ und „Principal“ nicht.
Ressourcenbasierte Richtlinien (Rollenvertrauensrichtlinie)	„Effect“, „Action“ und „Principal“  Note Für Principal ist nur AWS-Konto ID oder Principal-ID zulässig.

Beispiele für IAM-Richtlinien auf Snowball Edge

Note

AWS Identity and Access Management (IAM) -Benutzer benötigen "snowballdevice:*" Berechtigungen, um die [AWS OpsHub for Snow Family Anwendung](#) zur Verwaltung von Snowball Edge zu verwenden.

Im Folgenden finden Sie Beispiele für Richtlinien, die einem Snowball Edge-Gerät Berechtigungen gewähren.

Zulassen des GetUser Aufrufs für einen Beispielbenutzer auf einem Snowball Edge über die IAM-API

Verwenden Sie die folgende Richtlinie, um den GetUser Aufruf eines Beispielbenutzers über die IAM-API zuzulassen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "iam:GetUser",
      "Resource": "arn:aws:iam::user/example-user"
    }
  ]
}
```

Vollzugriff auf die Amazon S3 S3-API auf einem Snowball Edge zulassen

Verwenden Sie die folgende Richtlinie, um vollen Zugriff auf die Amazon S3 S3-API zu gewähren.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Lese- und Schreibzugriff auf einen Amazon S3 S3-Bucket auf einem Snowball Edge zulassen

Mit der folgenden Richtlinie ermöglichen Sie den Lese- und Schreibzugriff auf einen bestimmten Bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::bucket-name"
    },
    {
      "Sid": "AllObjectActions",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::bucket-name/*"
    }
  ]
}
```

```
}
```

Zulassen des Auflisten-, Abruf- und Platzzugriffs auf einen Amazon S3 S3-Bucket auf einem Snowball Edge

Verwenden Sie die folgende Richtlinie, um List-, Get- und Put-Zugriff auf einen bestimmten S3-Bucket zuzulassen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Vollzugriff auf die EC2 Amazon-API auf einem Snowball Edge zulassen

Verwenden Sie die folgende Richtlinie, um vollen Zugriff auf Amazon zu gewähren EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
```

```

        "Resource": "*"
      }
    ]
  }

```

Zulassen des Zugriffs zum Starten und Beenden von EC2 Amazon-kompatiblen Instances auf einem Snowball Edge

Verwenden Sie die folgende Richtlinie, um den Zugriff zum Starten und Stoppen von EC2 Amazon-Instances zu gewähren.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*"
    }
  ]
}

```

Anrufe an einen Snowball Edge ablehnen, DescribeLaunchTemplates DescribeImages aber alle Anrufe zulassen

Mit der folgenden Richtlinie können Sie Aufrufe von DescribeLaunchTemplates ablehnen, jedoch alle Aufrufe von DescribeImages zulassen.

JSON

```

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

```

```

    "Statement": [
      {
        "Effect": "Deny",
        "Action": [
          "ec2:DescribeLaunchTemplates"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeImages"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

Richtlinie für API-Aufrufe auf einem Snowball Edge

Listet alle verwalteten Richtlinien auf, die auf Ihrem Snow-Gerät verfügbar sind, einschließlich Ihrer eigenen, vom Kunden definierten verwalteten Richtlinien. Weitere Einzelheiten finden Sie in der [Liste der Richtlinien](#).

```

aws iam list-policies --endpoint http://ip-address:6078 --region snow --profile
snowballEdge
{
  "Policies": [
    {
      "PolicyName": "Administrator",
      "Description": "Root user admin policy for Account 123456789012",
      "CreateDate": "2020-03-04T17:44:59.412Z",
      "AttachmentCount": 1,
      "IsAttachable": true,
      "PolicyId": "policy-id",
      "DefaultVersionId": "v1",
      "Path": "/",
      "Arn": "arn:aws:iam::123456789012:policy/Administrator",
      "UpdateDate": "2020-03-04T19:10:45.620Z"
    }
  ]
}

```

```
}
```

TrustPolicy Beispiel auf einem Snowball Edge

Eine Vertrauensrichtlinie gibt einen Satz temporärer Sicherheitsanmeldedaten zurück, mit denen Sie auf AWS Ressourcen zugreifen können, auf die Sie normalerweise keinen Zugriff haben. Diese temporären Anmeldeinformationen bestehen aus einer Zugriffsschlüssel-ID, einem geheimen Zugriffsschlüssel und einem Sicherheits-Token. In der Regel verwenden Sie für den kontoübergreifenden Zugriff `AssumeRole` in Ihrem Konto.

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie. Weitere Informationen zur Vertrauensrichtlinie finden Sie [AssumeRole](#) in der AWS -Security-Token-Service API-Referenz.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::AccountId:root" //You can use the Principal ID
instead of the account ID.
        ]
      },
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

Verwendung AWS -Security-Token-Service auf einem Snowball Edge

Mit AWS -Security-Token-Service (AWS STS) können Sie temporäre Anmeldeinformationen mit eingeschränkten Rechten für IAM-Benutzer anfordern.

Important

Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter [Portanforderungen für AWS Dienste auf einem Snowball Edge](#).

Themen

- [Verwenden der API-Operationen AWS CLI und auf einem Snowball Edge](#)
- [Unterstützte AWS STSAWS CLI Befehle auf einem Snowball Edge](#)
- [Unterstützte AWS STS API-Operationen auf einem Snowball Edge](#)

Verwenden der API-Operationen AWS CLI und auf einem Snowball Edge

Wenn Sie die API-Operationen AWS CLI oder verwenden, um IAM- AWS STS, Amazon S3- und EC2 Amazon-Befehle auf einem Snowball Edge-Gerät auszugeben, müssen Sie das `region` als "snow" angeben. Sie können dies mithilfe `AWS configure` oder innerhalb des Befehls selbst tun, wie in den folgenden Beispielen.

```
aws configure --profile snowballEdge
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Oder

```
aws iam list-users --endpoint http://192.0.2.0:6078 --region snow --profile  
snowballEdge
```

Note

Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel, die lokal verwendet werden, AWS Snowball Edge können nicht mit den Schlüsseln in der AWS Cloud ausgetauscht werden.

Unterstützte AWS STSAWS CLI Befehle auf einem Snowball Edge

Lokal wird ausschließlich der Befehl [assume-role](#) unterstützt.

Die folgenden Parameter werden für `assume-role` unterstützt:

- `role-arn`
- `role-session-name`
- `duration-seconds`

Beispielbefehl zum Übernehmen einer Rolle auf einem Snowball Edge

Zur Annahme einer Rolle verwenden Sie den folgenden Befehl.

```
aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/example-role" --  
role-session-name AWSCLI-Session --endpoint http://snow-device-IP-address:7078
```

Weitere Informationen zur Verwendung des `assume-role` Befehls finden Sie unter [Wie nehme ich eine IAM-Rolle an mit dem?](#) AWS CLI

Weitere Informationen zur Verwendung AWS STS finden Sie unter [Verwenden temporärer Sicherheitsanmeldeinformationen](#) im IAM-Benutzerhandbuch.

Unterstützte AWS STS API-Operationen auf einem Snowball Edge

Nur die [AssumeRole](#) API wird lokal unterstützt.

Die folgenden Parameter werden für AssumeRole unterstützt:

- RoleArn
- RoleSessionName
- DurationSeconds

Example eine Rolle zu übernehmen

```
https://sts.amazonaws.com/  
?Version=2011-06-15  
&Action=AssumeRole  
&RoleSessionName=session-example  
&RoleArn=arn:aws:iam::123456789012:role/demo  
&DurationSeconds=3600
```

Verwaltung von Public-Key-Zertifikaten auf Snowball Edge

Sie können über das HTTPS-Protokoll sicher mit AWS Diensten interagieren, die auf einem Snowball Edge-Gerät oder einem Cluster von Snowball Edge-Geräten ausgeführt werden, indem Sie ein Public-Key-Zertifikat bereitstellen. Sie können das HTTPS-Protokoll verwenden, um mit AWS Diensten wie IAM, Amazon EC2, S3-Adapter und Amazon S3 S3-kompatiblen Speicher auf Snowball Edge, Amazon EC2 Systems Manager und Snowball AWS STS Edge-Geräten zu interagieren. Bei einem Gerätecluster ist ein einzelnes Zertifikat erforderlich, das von jedem Gerät im Cluster generiert werden kann. Sobald ein Snowball Edge-Gerät das Zertifikat generiert hat und Sie das Gerät entsperren, können Sie Snowball Edge-Clientbefehle verwenden, um das Zertifikat aufzulisten, abzurufen und zu löschen.

Ein Snowball Edge-Gerät generiert ein Zertifikat, wenn die folgenden Ereignisse eintreten:

- Das Snowball Edge-Gerät oder -Cluster wird zum ersten Mal entsperrt.
- Das Snowball Edge-Gerät oder -Cluster wird nach dem Löschen des Zertifikats entsperrt (mit dem `delete-certificate` Befehl oder Zertifikat erneuern in AWS OpsHub).
- Das Snowball Edge-Gerät oder -Cluster wird nach Ablauf des Zertifikats neu gestartet und entsperrt.

Immer wenn ein neues Zertifikat generiert wird, ist das alte Zertifikat nicht mehr gültig. Ein Zertifikat ist ab dem Tag, an dem es generiert wurde, für einen Zeitraum von einem Jahr gültig.

Sie können es auch AWS OpsHub zur Verwaltung von Public-Key-Zertifikaten verwenden. Weitere Informationen finden Sie OpsHub in diesem Handbuch unter [Verwaltung von Public-Key-Zertifikaten mithilfe von Zertifikaten](#).

Themen

- [Das Zertifikat auf einem Snowball Edge auflisten](#)
- [Zertifikate von einem Snowball Edge abrufen](#)
- [Löschen von Zertifikaten auf einem Snowball Edge](#)

Das Zertifikat auf einem Snowball Edge auflisten

Verwenden Sie den `list-certificates` Befehl, um die Amazon-Ressourcennamen (ARNs) für das aktuelle Zertifikat zu sehen.

```
snowballEdge list-certificates
```

Example der **list-certificates** Ausgabe

```
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-
device::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7",
    "SubjectAlternativeNames" : [ "192.0.2.0" ]
  } ]
}
```

Zertifikate von einem Snowball Edge abrufen

Verwenden Sie den `get-certificate` Befehl, um den Inhalt des Zertifikats auf der Grundlage des bereitgestellten ARN anzuzeigen. Verwenden Sie den `list-certificates` Befehl, um den ARN des Zertifikats abzurufen, das als `certificate-arn` Parameter verwendet werden soll.

```
snowballEdge get-certificate --certificate-arn arn:aws:snowball-
device::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

Example der **get-certificate** Ausgabe

```
-----BEGIN CERTIFICATE-----
Certificate
-----END CERTIFICATE-----
```

Hinweise zur Konfiguration Ihres Zertifikats finden Sie unter [Konfiguration des AWS CLI für die Verwendung des S3-Adapters auf einem Snowball Edge als Endpunkt](#).

Löschen von Zertifikaten auf einem Snowball Edge

Verwenden Sie den `delete-certificate` Befehl, um das aktuelle Zertifikat zu löschen.

Verwenden Sie den `list-certificates` Befehl, um den ARN des Zertifikats abzurufen, das als `certificate-arn` Parameter verwendet werden soll. Um ein neues Zertifikat zu generieren, starten Sie Snowball Edge oder jeden Snowball Edge in einem Cluster neu. Sehen Sie sich den Befehl an [Das Snowball Edge-Gerät neu starten](#) oder verwenden Sie `ihnsnowballEdge reboot-device`.

```
snowballEdge delete-certificate --certificate-arn arn:aws:snowball-  
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

Example der `delete-certificate` Ausgabe

```
The certificate has been deleted from your Snow device. Please reboot your Snowball  
Edge or Snowball Edge cluster to generate a new certificate.
```

Portanforderungen für AWS Dienste auf einem Snowball Edge

Damit AWS Dienste auf einem AWS Snowball Edge Gerät ordnungsgemäß funktionieren, müssen Sie die Netzwerkports für den Dienst zulassen.

Im Folgenden finden Sie eine Liste der Netzwerkports, die für jeden AWS Dienst erforderlich sind.

Port	Protokoll	Kommentar
22 (HTTP)	TCP	Gerätezustandsprüfung und für EC2 SSH
443 (HTTPS)	TCP	HTTPS-Endpunkt der S3-API und der S3 Control API
2049 (HTTP)	TCP	NFS-Endpunkt
6078 (HTTP)	TCP	IAM-HTTP-Endpunkt
6089 (HTTPS)	TCP	IAM-HTTPS-Endpunkt
7078 (HTTP)	TCP	STS-HTTP-Endpunkt
7089 (HTTPS)	TCP	STS-HTTPS-Endpunkt
8080 (HTTP)	TCP	HTTP-Endpunkt des S3-Adapters
8008 (HTTP)	TCP	EC2 HTTP-Endpunkt
8243 (HTTPS)	TCP	EC2 HTTPS-Endpunkt
8443 (HTTPS)	TCP	HTTPS-Endpunkt des S3 Adapter
9091 (HTTP)	TCP	Endpunkt für die Geräteverwaltung

Port	Protokoll	Kommentar
9092	TCP	Eingehend für EKS Anywhere und CAPAS-Gerätecontroller
8242	TCP	Eingehend für EC2 HTTPS-Endpunkt für EKS Anywhere
6443	TCP	Eingehend für den Kubernetes-API-Endpunkt von EKS Anywhere
2379	TCP	Eingehend für den EKS Anywhere Etcd API-Endpunkt
2380	TCP	Eingehend für den EKS Anywhere Etcd API-Endpunkt

AWS Snowball Edge Device Management Zur Verwaltung von Snowball Edge verwenden

AWS Snowball Edge Device Management ermöglicht es Ihnen, Ihren Snowball Edge und lokale AWS Dienste remote zu verwalten. Alle Snowball Edge-Geräte unterstützen die Snowball Edge-Geräteverwaltung und sie wird auf neuen Geräten in den meisten Ländern installiert, in AWS-Regionen denen Snowball Edge verfügbar ist.

Mit Snowball Edge Device Management können Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine Aufgabe
- Überprüfen Sie den Status der Aufgabe
- Überprüfen Sie die Metadaten der Aufgabe
- Stornieren Sie eine Aufgabe
- Überprüfen Sie die Geräteinformationen
- Überprüfen Sie den EC2 Amazon-kompatiblen Instanzstatus
- Befehle und Syntax auflisten
- Listet Geräte auf, die per Fernzugriff verwaltet werden können
- Listet den Aufgabenstatus geräteübergreifend auf
- Verfügbare Ressourcen auflisten
- Aufgaben nach Status auflisten
- Geräte- oder Aufgaben-Tags auflisten
- Stichwörter anwenden
- Tags entfernen

Themen

- [Auswahl des Snowball Edge-Geräteverwaltungsstatus bei der Bestellung eines Snowball Edge](#)
- [Aktivieren der Snowball Edge-Geräteverwaltung auf einem Snowball Edge](#)
- [Hinzufügen von Berechtigungen für Snowball Edge Device Management zu einer IAM-Rolle auf einem Snowball Edge](#)
- [CLI-Befehle für die Snowball Edge-Geräteverwaltung](#)

Auswahl des Snowball Edge-Geräteverwaltungsstatus bei der Bestellung eines Snowball Edge

Wenn Sie einen Auftrag zur Bestellung eines Snow-Geräts erstellen, können Sie wählen, in welchem Status sich Snowball Edge Device Management bei Erhalt des Geräts befinden soll: installiert, aber nicht aktiviert oder installiert und aktiviert. Wenn es installiert, aber nicht aktiviert ist, müssen Sie den Snowball Edge-Client verwenden AWS OpsHub , um es zu aktivieren, bevor Sie es verwenden können. Wenn es installiert und aktiviert ist, können Sie Snowball Edge Device Management verwenden, nachdem Sie das Gerät erhalten und es mit Ihrem lokalen Netzwerk verbunden haben. Sie können den Snowball Edge-Geräteverwaltungsstatus wählen, wenn Sie einen Auftrag erstellen Managementkonsole für die AWS Snow-Familie, um ein Gerät über den Snowball Edge-Client AWS CLI, die oder die Snow Job Management API zu bestellen.

Um den Snowball Edge-Geräteverwaltungsstatus aus dem Managementkonsole für die AWS Snow-Familie

1. Um zu entscheiden, ob Snowball Edge-Geräteverwaltung installiert und aktiviert werden soll, wählen Sie Ihr Snow-Gerät remote mit AWS OpsHub oder Snowball-Client verwalten.
2. Wenn Sie festlegen möchten, dass Snowball Edge-Geräteverwaltung installiert, aber nicht aktiviert wird, wählen Sie Ihr Snow-Gerät nicht remote mit AWS OpsHub oder dem Snowball-Client verwalten aus.

Weitere Informationen finden Sie unter [Schritt 3: Wählen Sie Ihre Funktionen und Optionen](#) in diesem Handbuch.

So wählen Sie den Snowball Edge-Geräteverwaltungsstatus aus der AWS CLI Snowball Edge-Client- oder Snow-Job-Management-API aus:

- Verwenden Sie den `remote-management` Parameter, um den Snowball Edge-Geräteverwaltungsstatus anzugeben. Der `INSTALLED_ONLY` Wert des Parameters bedeutet, dass Snowball Edge Device Management installiert, aber nicht aktiviert ist. Der `INSTALLED_AUTOSTART` Wert des Parameters bedeutet, dass Snowball Edge Device Management installiert und aktiviert ist. Wenn Sie keinen Wert für diesen Parameter angeben, `INSTALLED_ONLY` ist dies der Standardwert.

Example der Syntax des **remote-management** Parameters des **create-job** Befehls

```
aws snowball create-job \
  --job-type IMPORT \
  --remote-management INSTALLED_AUTOSTART
  --device-configuration '{"SnowconeDeviceConfiguration": {"WirelessConnection":
{"IsWifiEnabled": false} } }' \
  --resources '{"S3Resources":[{"BucketArn":"arn:aws:s3:::bucket-name"}]}' \
  --description "Description here" \
  --address-id ADID000000000-0000-0000-0000-000000000000 \
  --kms-key-arn arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  --role-arn arn:aws:iam::000000000000:role/SnowconeImportGamma \
  --snowball-capacity-preference T8 \
  --shipping-option NEXT_DAY \
  --snowball-type SNC1_HDD \
  --region us-west-2 \
```

Weitere Informationen finden Sie unter [Job Management API Reference](#) in der AWS Snowball Edge API-Referenz.

Aktivieren der Snowball Edge-Geräteverwaltung auf einem Snowball Edge

Gehen Sie wie folgt vor, um die Snowball Edge-Geräteverwaltung mit dem Snowball Edge-Client zu aktivieren.

Bevor Sie dieses Verfahren verwenden, gehen Sie wie folgt vor:

- Laden Sie die neueste Version des Snowball Edge-Clients herunter und installieren Sie sie. Weitere Informationen finden Sie unter [Snowball-Client herunterladen und installieren](#).
- Laden Sie die Manifestdatei herunter und rufen Sie den Entsperrcode für das Snowball Edge-Gerät ab. Weitere Informationen finden Sie unter [Abrufen Ihrer Anmeldeinformationen und Tools](#).
- Connect das Snowball Edge-Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter für [die Verbindung mit Ihrem lokalen Netzwerk](#).
- Entsperren Sie das Snowball Edge-Gerät. Weitere Informationen finden Sie unter [Snowball Edge entsperren](#) Lokales .

```
snowballEdge set-features /  
  --remote-management-state INSTALLED_AUTOSTART /  
  --manifest-file JID1717d8cc-2dc9-4e68-aa46-63a3ad7927d2_manifest.bin /  
  --unlock-code 7c0e1-bab84-f7675-0a2b6-f8k33 /  
  --endpoint https://192.0.2.0:9091
```

Der Snowball Edge-Client gibt Folgendes zurück, wenn der Befehl erfolgreich ist.

```
{  
  "RemoteManagementState" : "INSTALLED_AUTOSTART"  
}
```

Hinzufügen von Berechtigungen für Snowball Edge Device Management zu einer IAM-Rolle auf einem Snowball Edge

Erstellen Sie auf dem Gerät, von dem AWS-Konto aus das Gerät bestellt wurde, eine AWS Identity and Access Management (IAM-) Rolle und fügen Sie der Rolle die folgende Richtlinie hinzu. Weisen Sie die Rolle dann dem IAM-Benutzer zu, der sich anmeldet, um Ihr Gerät mit Snowball Edge Device Management remote zu verwalten. Weitere Informationen finden Sie unter [Erstellen von IAM-Rollen](#) und [Erstellen eines IAM-Benutzers](#) in Ihrem AWS-Konto

Richtlinie

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "snow-device-management:ListDevices",  
        "snow-device-management:DescribeDevice",
```

```
        "snow-device-management:DescribeDeviceEc2Instances",
        "snow-device-management:ListDeviceResources",
        "snow-device-management:CreateTask",
        "snow-device-management:ListTasks",
        "snow-device-management:DescribeTask",
        "snow-device-management:CancelTask",
        "snow-device-management:DescribeExecution",
        "snow-device-management:ListExecutions",
        "snow-device-management:ListTagsForResource",
        "snow-device-management:TagResource",
        "snow-device-management:UntagResource"
    ],
    "Resource": "*"
}
]
```

CLI-Befehle für die Snowball Edge-Geräteverwaltung

In diesem Abschnitt AWS CLI werden die Befehle beschrieben, mit denen Sie Ihren Snowball Edge mit Snowball Edge Device Management remote verwalten können. Sie können einige Fernverwaltungsaufgaben auch mithilfe von ausführen. AWS OpsHub Weitere Informationen finden Sie unter [verwalten AWS Dienste auf Ihrem Gerät](#) verwalten.

Note

Stellen Sie vor der Verwaltung Ihres Geräts sicher, dass es eingeschaltet und mit Ihrem Netzwerk verbunden ist und eine Verbindung zu dem Gerät herstellen kann, auf AWS-Region dem es bereitgestellt wurde.

Themen

- [Eine Aufgabe zur Verwaltung eines Snowball Edge mit Snowball Edge Device Management erstellen](#)
- [Überprüfen des Status einer Aufgabe zur Verwaltung eines Snowball Edge](#)
- [Informationen zu einem Snowball Edge mithilfe von Snowball Edge Device Management überprüfen](#)

- [Status von EC2 Amazon-kompatiblen Instances auf Snowball Edge mit Snowball Edge Device Management überprüfen](#)
- [Aufgabenmetadaten auf Snowball Edge mit Snowball Edge Device Management anzeigen](#)
- [Abbrechen einer Aufgabe auf einem Snowball Edge mit Snowball Edge Device Management](#)
- [Befehle und Syntax der Snowball Edge-Geräteverwaltung auflisten](#)
- [Snowball Edge auflisten, die für die Fernverwaltung verfügbar sind](#)
- [Status von Snowball Edge-Geräteverwaltungsaufgaben in Snowball Edge auflisten](#)
- [Auflisten verfügbarer Ressourcen auf Snowball Edge mit Snowball Edge Device Management](#)
- [Tags für Snowball Edge- oder Snowball Edge-Gerätemanagement-Tags auflisten](#)
- [Snowball Edge-Geräteverwaltungsaufgaben nach Status auflisten](#)
- [Anwenden von Tags auf Snowball Edge-Geräteverwaltungsaufgaben oder Snowball Edge](#)
- [Snowball Edge-Gerätemanagement-Tags aus Aufgaben oder Snowball Edge entfernen](#)

Eine Aufgabe zur Verwaltung eines Snowball Edge mit Snowball Edge Device Management erstellen

Um ein oder mehrere Zielgeräte anzuweisen, eine Aufgabe auszuführen, wie z. B. das Entsperren oder Neustarten, verwenden Sie `create-task`. Sie geben Zielgeräte an, indem Sie eine Liste der verwalteten Geräte IDs mit dem `--targets` Parameter angeben und die Aufgaben angeben, die mit dem Parameter ausgeführt werden sollen. `--command` Auf einem Gerät kann jeweils nur ein einziger Befehl ausgeführt werden.

Unterstützte Befehle:

- `unlock`(keine Argumente)
- `reboot`(keine Argumente)

Verwenden Sie den folgenden Befehl, um eine Aufgabe zu erstellen, die von den Zielgeräten ausgeführt werden soll. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management create-task
```

```
--targets smd-fictbgr3rbcjeqa5  
--command reboot={}
```

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException  
ServiceQuotaExceededException
```

Ausgabe

```
{  
  "taskId": "st-ficthmqoc2pht111",  
  "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-  
cjkwhmqoc2pht111"  
}
```

Überprüfen des Status einer Aufgabe zur Verwaltung eines Snowball Edge

Verwenden Sie den `describe-execution` Befehl, um den Status einer Remote-Aufgabe zu überprüfen, die auf einem oder mehreren Zielgeräten ausgeführt wird.

Eine Aufgabe kann einen der folgenden Status haben:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

Verwenden Sie den folgenden Befehl, um den Status einer Aufgabe zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management describe-execution \  
--taskId st-ficthmqoc2phtlef \  
--managed-device-id smd-fictqic6gcldf111
```

Ausgabe

```
{  
  "executionId": "1",  
  "lastUpdatedAt": "2021-07-22T15:29:44.110000+00:00",  
  "managedDeviceId": "smd-fictqic6gcldf111",  
  "startedAt": "2021-07-22T15:28:53.947000+00:00",  
  "state": "SUCCEEDED",  
  "taskId": "st-ficthmqoc2pht111"  
}
```

Informationen zu einem Snowball Edge mithilfe von Snowball Edge Device Management überprüfen

Verwenden Sie den Befehl, um gerätespezifische Informationen wie Gerätetyp, Softwareversion, IP-Adressen und Sperrstatus zu überprüfen. `describe-device` Die Ausgabe umfasst außerdem Folgendes:

- `lastReachedOutAt`— Wann das Gerät das letzte Mal Kontakt mit dem aufgenommen hat AWS Cloud. Zeigt an, dass das Gerät online ist.
- `lastUpdatedAt`— Wann die Daten auf dem Gerät zuletzt aktualisiert wurden. Zeigt an, wann der Geräte-Cache aktualisiert wurde.

Verwenden Sie den folgenden Befehl, um die Geräteinformationen zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management describe-device \  
--managed-device-id smd-fictqic6gcldf111
```

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Status von EC2 Amazon-kompatiblen Instances auf Snowball Edge mit Snowball Edge Device Management überprüfen

Verwenden Sie den `describe-ec2-instances` Befehl, um den aktuellen Status der EC2 Amazon-Instance zu überprüfen. Die Ausgabe ähnelt der des `describe-device` Befehls, die Ergebnisse stammen jedoch aus dem Geräte-Cache im AWS Cloud und enthalten eine Teilmenge der verfügbaren Felder.

Verwenden Sie den folgenden Befehl, um den Status der Amazon EC2 -kompatiblen Instance zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management describe-device-ec2-instances \  
--managed-device-id smd-fictbgr3rbcje111 \  
--instance-ids s.i-84fa8a27d3e15e111
```

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError
```

ThrottlingException
AccessDeniedException

Ausgabe

```
{
  "instances": [
    {
      "instance": {
        "amiLaunchIndex": 0,
        "blockDeviceMappings": [
          {
            "deviceName": "/dev/sda",
            "ebs": {
              "attachTime": "2021-07-23T15:25:38.719000-07:00",
              "deleteOnTermination": true,
              "status": "ATTACHED",
              "volumeId": "s.vol-84fa8a27d3e15e111"
            }
          }
        ],
        "cpuOptions": {
          "coreCount": 1,
          "threadsPerCore": 1
        },
        "createdAt": "2021-07-23T15:23:22.858000-07:00",
        "imageId": "s.ami-03f976c3cadaa6111",
        "instanceId": "s.i-84fa8a27d3e15e111",
        "state": {
          "name": "RUNNING"
        },
        "instanceType": "snc1.micro",
        "privateIpAddress": "34.223.14.193",
        "publicIpAddress": "10.111.60.160",
        "rootDeviceName": "/dev/sda",
        "securityGroups": [
          {
            "groupId": "s.sg-890b6b4008bdb3111",
            "groupName": "default"
          }
        ]
      }
    ]
  },

```



```

        "updatedAt": "2021-07-23T15:29:42.163000-07:00"
      },
      "lastUpdatedAt": "2021-07-23T15:29:58.
071000-07:00"
    }
  ]
}

```

Aufgabenmetadaten auf Snowball Edge mit Snowball Edge Device Management anzeigen

Verwenden Sie den `describe-task` Befehl, um die Metadaten für eine bestimmte Aufgabe auf einem Gerät zu überprüfen. Die Metadaten für eine Aufgabe umfassen die folgenden Elemente:

- Die Zielgeräte
- Der Status der Aufgabe
- Wann die Aufgabe erstellt wurde
- Wann wurden die Daten auf dem Gerät zuletzt aktualisiert
- Wann wurde die Aufgabe abgeschlossen
- Die Beschreibung (falls vorhanden), die bei der Erstellung der Aufgabe angegeben wurde

Verwenden Sie den folgenden Befehl, um die Metadaten einer Aufgabe zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management describe-task \
--task-id st-ficthmqoc2pht111
```

Ausnahmen

```

ValidationException
ResourceNotFoundException
InternalServerError

```

```
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
  "completedAt": "2021-07-22T15:29:46.758000+00:00",
  "createdAt": "2021-07-22T15:28:42.613000+00:00",
  "lastUpdatedAt": "2021-07-22T15:29:46.758000+00:00",
  "state": "COMPLETED",
  "tags": {},
  "targets": [
    "smd-fictbgr3rbcje111"
  ],
  "taskId": "st-ficthmqoc2pht111",
  "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
ficthmqoc2pht111"
}
```

Abbrechen einer Aufgabe auf einem Snowball Edge mit Snowball Edge Device Management

Verwenden Sie den Befehl, um eine Stornierungsanfrage für eine bestimmte Aufgabe zu senden. `cancel-task` Sie können nur Aufgaben in dem `QUEUED` Status stornieren, die noch nicht ausgeführt wurden. Aufgaben, die bereits ausgeführt werden, können nicht storniert werden.

Note

Eine Aufgabe, die Sie abbrechen möchten, wird möglicherweise trotzdem ausgeführt, wenn sie aus der Warteschlange bearbeitet wird, bevor der `cancel-task` Befehl den Status der Aufgabe ändert.

Verwenden Sie den folgenden Befehl, um eine Aufgabe abzuberechnen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management cancel-task \  
--task-id st-ficthmqoc2pht111
```

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

```
{  
  "taskId": "st-ficthmqoc2pht111"  
}
```

Befehle und Syntax der Snowball Edge-Geräteverwaltung auflisten

Verwenden Sie den `help` Befehl, um eine Liste aller unterstützten Befehle für die Snowball Edge-Geräteverwaltungs-API zurückzugeben. Sie können den `help` Befehl auch verwenden, um detaillierte Informationen zu und die Syntax für einen bestimmten Befehl zurückzugeben.

Verwenden Sie den folgenden Befehl, um alle unterstützten Befehle aufzulisten.

Befehl

```
aws snow-device-management help
```

Verwenden Sie den folgenden Befehl, um detaillierte Informationen und die Syntax für einen Befehl zurückzugeben. *command* Ersetzen Sie ihn durch den Namen des Befehls, an dem Sie interessiert sind.

Befehl

```
aws snow-device-management command help
```

Snowball Edge auflisten, die für die Fernverwaltung verfügbar sind

Verwenden Sie den Befehl, um eine Liste aller Geräte in Ihrem Konto zurückzugeben, auf denen Snowball Edge-Geräteverwaltung aktiviert ist, AWS-Region wo der `list-devices` Befehl ausgeführt wird. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um Geräte aufzulisten, die per Fernzugriff verwaltet werden können. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management list-devices \  
--max-results 10
```

Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

```
{  
  "devices": [  
    {  
      "associatedWithJob": "ID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",  
      "managedDeviceId": "smd-fictbgr3rbcjeqa5",  
    }  
  ]  
}
```

```
        "managedDeviceArn": "arn:aws:snow-device-management:us-  
west-2:000000000000:managed-device/smd-fictbgr3rbcje111"  
        "tags": {}  
    }  
]  
}
```

Status von Snowball Edge-Geräteverwaltungsaufgaben in Snowball Edge auflisten

Verwenden Sie den `list-executions` Befehl, um den Status von Aufgaben für ein oder mehrere Zielgeräte zurückzugeben. Verwenden Sie den `--state` Parameter, um die Rückgabeliste so zu filtern, dass Aufgaben angezeigt werden, die sich derzeit in einem bestimmten Status befinden. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Eine Aufgabe kann einen der folgenden Status haben:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

Verwenden Sie den folgenden Befehl, um den Aufgabenstatus geräteübergreifend aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management list-executions \  
--taskId st-ficthmqoc2phtlef \  
--state SUCCEEDED \  
--max-results 10
```

Ausnahmen

```
ValidationException
InternalServerError
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
  "executions": [
    {
      "executionId": "1",
      "managedDeviceId": "smd-fictbgr3rbcje111",
      "state": "SUCCEEDED",
      "taskId": "st-ficthmqoc2pht111"
    }
  ]
}
```

Auflisten verfügbarer Ressourcen auf Snowball Edge mit Snowball Edge Device Management

Verwenden Sie den `list-device-resources` Befehl, um eine Liste der für ein Gerät verfügbaren AWS Ressourcen zurückzugeben. Verwenden Sie den `--type` Parameter, um die Liste nach einem bestimmten Ressourcentyp zu filtern. Derzeit sind EC2 Amazon-kompatible Instances der einzige unterstützte Ressourcentyp. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um die verfügbaren Ressourcen für ein Gerät aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management list-device-resources \
--managed-device-id smd-fictbgr3rbcje111 \
```

```
--type AWS::EC2::Instance  
--next-  
token YAQGPwAT9L3wVKaGYjt4yS34MiQLWvzcShe9oIeDJr05AT4rXSprqcqQhhBEYRfcerAp0YYbJmRT=  
--max-results 10
```

Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

```
{  
  "resources": [  
    {  
      "id": "s.i-84fa8a27d3e15e111",  
      "resourceType": "AWS::EC2::Instance"  
    }  
  ]  
}
```

Tags für Snowball Edge- oder Snowball Edge-Gerätemanagement-Tags auflisten

Verwenden Sie den `list-tags-for-resource` Befehl, um eine Liste von Tags für ein verwaltetes Gerät oder eine verwaltete Aufgabe zurückzugeben.

Verwenden Sie den folgenden Befehl, um die Tags für ein Gerät aufzulisten. Ersetzen Sie das Beispiel Amazon Resource Name (ARN) durch den ARN für Ihr Gerät.

Befehl

```
aws snow-device-management list-tags-for-resource
```

```
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/smd-fictbgr3rbcjeqa5
```

Ausnahmen

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Ausgabe

```
{
  "tags": {
    "Project": "PrototypeA"
  }
}
```

Snowball Edge-Geräteverwaltungsaufgaben nach Status auflisten

Verwenden Sie den `list-tasks` Befehl, um eine Liste der Aufgaben von den Geräten in der AWS Region zurückzugeben, in der der Befehl ausgeführt wird. Verwenden Sie den `--state` Parameter `IN_PROGRESS`, um die Ergebnisse nach `COMPLETED`, oder `CANCELED` Status zu filtern. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um Aufgaben nach Status aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management list-tasks \
--state IN_PROGRESS \
--next-token K8VAMqKiP2Cf4xGkmH8GMyZrg0F8FUb+d10KTP9+P4pUb+8PhW+6MiXh4= \
--max-results 10
```

Ausnahmen


```
ValidationException
InternalServerError
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
  "tasks": [
    {
      "state": "IN_PROGRESS",
      "tags": {},
      "taskId": "st-ficthmqoc2phtlef",
      "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
ficthmqoc2phtlef"
    }
  ]
}
```

Anwenden von Tags auf Snowball Edge-Geräteverwaltungsaufgaben oder Snowball Edge

Verwenden Sie den `tag-resource` Befehl, um ein Tag für ein Gerät oder für eine Aufgabe auf einem Gerät hinzuzufügen oder zu ersetzen. Der `--tags` Parameter akzeptiert eine durch Kommas getrennte Liste von `Key=Value` Paaren.

Verwenden Sie den folgenden Befehl, um Tags auf ein Gerät anzuwenden. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management tag-resource \
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/
smd-fictbgr3rbcjeqa5 \
--tags Project=PrototypeA
```

Ausnahmen

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Snowball Edge-Gerätemanagement-Tags aus Aufgaben oder Snowball Edge entfernen

Verwenden Sie den `untag-resources` Befehl, um ein Tag von einem Gerät oder von einer Aufgabe auf einem Gerät zu entfernen.

Verwenden Sie den folgenden Befehl, um Tags von einem Gerät zu entfernen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management untag-resources \
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/
smd-fictbgr3rbcjeqa5 \
--tag-keys Project
```

Ausnahmen

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Software auf Snowball Edge-Geräten aktualisieren

AWS wird Sie benachrichtigen, wenn neue Software für Ihren Snowball Edge verfügbar ist. Die Benachrichtigung erfolgt per E-Mail Health Dashboard und als CloudWatch Ereignis. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, mit dem das Snowball Edge-Gerät bestellt wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und laden Sie das Update so schnell wie möglich herunter und installieren Sie es, um eine Unterbrechung der Nutzung des Geräts zu vermeiden. Weitere Informationen zu Health Dashboard finden Sie im [AWS Health Benutzerhandbuch](#). Weitere Informationen zu CloudWatch Veranstaltungen finden Sie im [Amazon CloudWatch Events-Benutzerhandbuch](#).

Sie können Softwareupdates von Snowball Edge-Geräten in Ihren lokalen Umgebungen herunterladen AWS und auf diesen installieren. Diese Aktualisierungen erfolgen im Hintergrund. Sie können Ihre Geräte weiterhin wie gewohnt verwenden, während die neueste Software sicher von AWS Ihrem Gerät heruntergeladen wird. Um heruntergeladene Updates anzuwenden, müssen Sie jedoch die Workloads auf dem Gerät beenden und es neu starten.

Softwareupdates, die von AWS für Snowball Edge/Snowball Edge-Geräte (Appliances) bereitgestellt werden, sind Appliance-Software gemäß Abschnitt 9 der Servicebedingungen.

Die Softwareupdates werden ausschließlich zum Zweck der Installation der Softwareupdates auf dem jeweiligen Gerät im Namen von bereitgestellt. AWS Sie werden (oder versuchen), und Sie werden Dritten nicht erlauben oder dies auch nicht versuchen, (i) Kopien der Softwareupdates anzufertigen, die nicht für die Installation der Softwareupdates auf dem jeweiligen Gerät erforderlich sind, oder (ii) Funktionen oder Maßnahmen der Softwareupdates zu umgehen oder zu deaktivieren, einschließlich, aber nicht beschränkt auf die Verschlüsselung, die auf das Softwareupdate angewendet wird. Sobald die Softwareupdates auf dem jeweiligen Gerät installiert wurden, erklären Sie sich damit einverstanden, die Softwareupdates von allen Medien zu löschen, die bei der Installation der Softwareupdates auf dem Gerät verwendet wurden.

Warning

Wir empfehlen dringend, dass Sie alle Aktivitäten auf Ihrem Gerät unterbrechen, bevor Sie das Update installieren. Durch die Aktualisierung des Geräts und den Neustart werden die laufenden Instances gestoppt und alle Schreibvorgänge in lokale Amazon S3 S3-Buckets unterbrochen.

Themen

- [Voraussetzungen für die Aktualisierung von Software auf Snowball Edge-Geräten](#)
- [Updates auf Snowball Edge-Geräte herunterladen](#)
- [Updates auf Snowball Edge-Geräten installieren](#)
- [Aktualisierung des SSL-Zertifikats auf Snowball Edge-Geräten](#)
- [Aktualisieren Sie Ihr Amazon Linux 2 AMIs auf Snowball Edge](#)

Voraussetzungen für die Aktualisierung von Software auf Snowball Edge-Geräten

Bevor Sie Ihr Gerät aktualisieren können, müssen folgende Voraussetzungen umgesetzt werden:

- Sie haben den Auftrag erstellt, haben das Gerät zur Hand und haben es entsperrt. Weitere Informationen finden Sie unter [Erste Schritte mit Snowball Edge](#).
- Die Aktualisierung von Snowball Edge-Geräten erfolgt über den Snowball Edge-Client. Die neueste Version des Snowball Edge-Clients muss heruntergeladen und auf einem Computer in Ihrer lokalen Umgebung installiert werden, der über eine Netzwerkverbindung zu dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter [Verwenden des Snowball Edge-Clients](#).
- (Optional) Wir empfehlen, ein Profil für den Snowball Edge-Client zu konfigurieren. Weitere Informationen finden Sie unter [Konfiguration eines Profils für den Snowball Edge-Client](#).
- Für Amazon S3 S3-kompatiblen Speicher auf Snowball Edge auf geclusterten Snowball Edge-Geräten beenden Sie den S3-Snow-Dienst und deaktivieren Sie den Autostart für ihn. Siehe [Konfiguration von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge für den automatischen Start der Verwendung AWS OpsHub](#).

Note

Bei geclusterten Geräten müssen alle Befehle für jedes Gerät ausgeführt werden.

Nachdem Sie diese Aufgaben abgeschlossen haben, können Sie Updates für Snowball Edge-Geräte herunterladen und installieren.

Updates auf Snowball Edge-Geräte herunterladen

Es gibt zwei Möglichkeiten, ein Update für Snowball Edge herunterzuladen:

- Mit bestimmten Snowball Edge Client-Befehlen können Sie jederzeit manuelle Updates auslösen.
- Sie können programmgesteuert einen Zeitpunkt für die automatische Aktualisierung des Geräts bestimmen.

Das folgende Verfahren beschreibt den Vorgang zum manuellen Herunterladen von Aktualisierungen. Informationen zur automatischen Aktualisierung Ihres Snowball Edge-Geräts finden Sie unter `configure-auto-update-strategy` [Aktualisieren eines Snowball Edge-Geräts](#).

Note

Wenn Ihr Gerät keinen Internetzugang hat, können Sie mithilfe der API eine Aktualisierungsdatei herunterladen. [GetSoftwareUpdates](#) Zeigen Sie dann beim Aufrufen `download-updates` mithilfe des `uri` Parameters auf einen lokalen Dateispeicherort, wie im folgenden Beispiel.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Bei Windows-Betriebssystemen formatieren Sie den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file://C:/path/to/local-update
```

So suchen Sie nach Snowball Edge-Softwareupdates für eigenständige Geräte und laden sie herunter

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das Snowball Edge-Gerät mithilfe des `describe-device` Befehls entsperrt ist. Wenn das Gerät gesperrt ist, entsperren Sie es mit dem Befehl `unlock-device`. Weitere Informationen finden Sie unter [Snowball Edge entsperren](#).
2. Wenn das Gerät entsperrt ist, führen Sie den Befehl `snowballEdge check-for-updates` aus. Dieser Befehl gibt die neueste verfügbare Version der Snowball Edge-Software sowie die aktuell auf dem Gerät installierte Version zurück.

3. Wenn Ihre Gerätesoftware nicht mehr auf dem neuesten Stand ist, führen Sie den Befehl `snowballEdge download-updates` aus.

 Note

Wenn Ihr Gerät nicht mit dem Internet verbunden ist, laden Sie zunächst eine Aktualisierungsdatei über die [GetSoftwareUpdates](#)API herunter. Führen Sie dann den `snowballEdge download-updates` Befehl mit dem `uri` Parameter mit einem lokalen Pfad zu der Datei aus, die Sie heruntergeladen haben, wie im folgenden Beispiel gezeigt.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Formatieren Sie für Windows-Betriebssysteme den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file://C:/path/to/local-update
```

4. Sie können den Status dieses Downloads mit dem Befehl `snowballEdge describe-device-software` überprüfen. Während ein Update heruntergeladen wird, zeigen Sie den Status mit diesem Befehl an.

Example Ausgabe des **describe-device-software** Befehls

```
Install State: Downloading
```

So suchen Sie nach Snowball Edge-Softwareupdates für Gerätecluster und laden sie herunter

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass alle Snowball Edge-Geräte im Cluster mithilfe des `snowballEdge describe-device` Befehls entsperrt sind. Wenn die Geräte gesperrt sind, verwenden Sie den `snowballEdge unlock-cluster` Befehl, um sie zu entsperren. Weitere Informationen finden Sie unter [Snowball Edge entsperren](#).
2. Wenn alle Geräte im Cluster entsperrt sind, führen Sie für jedes Gerät im Cluster den Befehl aus. `check-for-updates` Dieser Befehl gibt die neueste verfügbare Version der Snowball Edge-Software sowie die aktuell auf dem Gerät installierte Version zurück.

```
snowballEdge check-for-updates --unlock-code 29-character-unlock-code --manifest-file path/to/manifest/file.bin --endpoint https://ip-address-of-snow-device
```

Note

Der Entsperrcode und die Manifestdatei sind für alle Geräte im Cluster identisch.

Example des **check-for-updates** Befehls

```
{  
  "InstalledVersion" : "118",  
  "LatestVersion" : "119"  
}
```

Wenn der Wert des LatestVersion Namens größer als der Wert des InstalledVersion Namens ist, ist ein Update verfügbar.

3. Verwenden Sie für jedes Gerät im Cluster den download-updates Befehl, um das Update herunterzuladen.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Note

Formatieren Sie für Windows-Betriebssysteme den Wert des uri Parameters wie folgt:

```
snowballEdge download-updates --uri file://C:/path/to/local-update
```

4. Verwenden Sie den describe-device-software Befehl, um den Status dieses Downloads für jedes Gerät im Cluster zu überprüfen.

```
snowballEdge describe-device-software --unlock-code 29-character-unlock-code --  
manifest-file path/to/manifest/file.bin --endpoint https://ip-address-of-snow-  
device
```

Example der Ausgabe des **describe-device-software** Befehls

```
{  
  "InstalledVersion" : "118",  
  "InstallingVersion" : "119",  
  "InstallState" : "DOWNLOADED",  
  "CertificateExpiry" : "Sat Mar 30 16:47:51 UTC 2024"  
}
```

Wenn der Wert des `InstallState` Namens lautet `DOWNLOADED`, wurde das Update heruntergeladen und kann installiert werden.

Updates auf Snowball Edge-Geräten installieren

Nachdem Sie Updates heruntergeladen haben, müssen Sie sie installieren und Ihr Gerät neu starten, damit die Updates wirksam werden. Das folgende Verfahren führt Sie durch die manuelle Installation von Updates.

Für Cluster von Snowball Edge-Geräten muss das Update auf jedes Gerät im Cluster heruntergeladen und installiert werden.

Note

Unterbrechen Sie alle Aktivitäten auf dem Gerät, bevor Sie Softwareupdates installieren. Durch die Installation von Updates werden laufende Instances gestoppt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen. Dies kann zu Datenverlusten führen

So installieren Sie Softwareupdates, die bereits auf den eigenständigen Snowball Edge-Computer heruntergeladen wurden

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das Snowball Edge-Gerät mithilfe des `describe-device` Befehls entsperrt ist. Wenn das Gerät gesperrt ist, entsperren Sie es mit dem Befehl `unlock-device`. Weitere Informationen finden Sie unter [Snowball Edge entsperren](#).
2. Führen Sie den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Dienste anzuzeigen. Der Befehl gibt den Dienst jedes Dienstes zurück, IDs der auf dem Gerät verfügbar ist.

```
snowballEdge list-services
```

Example der Ausgabe des **list-services** Befehls

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

3. Führen Sie für jede durch den `list-services` Befehl identifizierte Dienst-ID den `describe-service` Befehl aus, um den Status zu überprüfen. Verwenden Sie diese Informationen, um Dienste zu identifizieren, die beendet werden sollen.

```
snowballEdge describe-service --service-id service-id
```

Example der Ausgabe des **describe-service** Befehls

```
{
  "ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Storage" : {
```

```

"TotalSpaceBytes" : 99608745492480,
"FreeSpaceBytes" : 99608744468480
},
"Endpoints" : [ {
"Protocol" : "http",
"Port" : 8080,
"Host" : "192.0.2.0"
}, {
"Protocol" : "https",
"Port" : 8443,
"Host" : "192.0.2.0",
"CertificateAssociation" : {
"CertificateArn" : "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}

```

Diese Ausgabe zeigt, dass der s3 Dienst aktiv ist und mit dem stop-service Befehl beendet werden muss.

4. Verwenden Sie den stop-service Befehl, um jeden Dienst zu beenden, bei dem der Wert des State Namens ACTIVE in der Ausgabe des list-services Befehls enthalten ist. Wenn mehr als ein Dienst ausgeführt wird, beenden Sie jeden Dienst, bevor Sie fortfahren.

Note

Der Amazon S3 S3-Adapter EC2 AWS STS, Amazon und die IAM-Dienste können nicht gestoppt werden. Wenn Amazon S3 S3-kompatibler Speicher auf Snowball Edge läuft, beenden Sie ihn, bevor Sie Updates installieren. Amazon S3 S3-kompatibler Speicher auf Snowball Edge hat s3-snow als serviceId

```

snowballEdge stop-service --service-id service-id --device-ip-addresses snow-
device-1-ip-address snow-device-device-2-ip-address snow-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code 29-character-unlock-code --
endpoint https://snow-device-ip-address

```

Example der Ausgabe des Befehls **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.

5. Führen Sie den Befehl `snowballEdge install-updates` aus.
6. Sie können den Status dieser Installation mit dem Befehl `snowballEdge describe-device-software` überprüfen. Während ein Update installiert wird, zeigen Sie mit diesem Befehl den Status an.

Beispielausgabe

Install State: Installing //Possible values[NA, Installing, Requires Reboot]

Sie haben erfolgreich ein Softwareupdate für Ihr Snowball Edge-Gerät installiert. Wenn eine Aktualisierung aktualisiert wird, wird sie nicht automatisch auf das Gerät angewandt. Um die Installation der Aktualisierung abzuschließen, muss das Gerät neu gestartet werden.

Warning

Wenn Ihr Snowball Edge-Gerät neu gestartet wird, ohne die gesamte Aktivität auf dem Gerät zu stoppen, kann dies zu Datenverlust führen.

7. Wenn alle Dienste auf dem Gerät beendet wurden, starten Sie das Gerät neu, entsperren Sie das Gerät und starten Sie es erneut. Damit ist die Installation der heruntergeladenen Softwareupdates abgeschlossen. Weitere Informationen zum Entsperren des Geräts finden Sie unter Snowball Edge [entsperren Snowball Edge](#) .
8. Wenn das Gerät nach dem zweiten Neustart eingeschaltet wird, entsperren Sie das Gerät.
9. Führen Sie den Befehl `check-for-updates` aus. Dieser Befehl gibt die neueste verfügbare Version der Snowball Edge-Software sowie die aktuelle Version zurück, die auf dem Gerät installiert ist.

So installieren Sie Softwareupdates, die bereits auf einen Cluster von Snowball Edge-Geräten heruntergeladen wurden

1. Führen Sie für jedes Gerät im Cluster den `describe-device` Befehl aus, um festzustellen, ob die Geräte entsperrt sind. Wenn die Geräte gesperrt sind, verwenden Sie den `unlock-cluster` Befehl, um sie zu entsperren. Weitere Informationen finden Sie unter [Snowball Edge entsperren](#).
2. Führen Sie für jedes Gerät im Cluster den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Dienste anzuzeigen. Der Befehl gibt den Dienst jedes Dienstes zurück, IDs der auf dem Gerät verfügbar ist.

```
snowballEdge list-services
```

Example der Ausgabe des **list-services** Befehls

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

3. Führen Sie für jede durch den `list-services` Befehl identifizierte Dienst-ID den `describe-service` Befehl aus, um den Status zu überprüfen. Verwenden Sie diese Informationen, um Dienste zu identifizieren, die beendet werden sollen.

```
snowballEdge describe-service --service-id service-id
```

Example der Ausgabe des **describe-service** Befehls

```
{
  "ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Storage" : {
    "TotalSpaceBytes" : 99608745492480,

```

```

"FreeSpaceBytes" : 99608744468480
},
"Endpoints" : [ {
  "Protocol" : "http",
  "Port" : 8080,
  "Host" : "192.0.2.0"
}, {
  "Protocol" : "https",
  "Port" : 8443,
  "Host" : "192.0.2.0",
  "CertificateAssociation" : {
    "CertificateArn" : "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
  }
} ]
}

```

Diese Ausgabe zeigt, dass der s3 Dienst aktiv ist und mit dem stop-service Befehl beendet werden muss.

4. Verwenden Sie für jedes Gerät im Cluster den stop-service Befehl, um jeden Dienst zu beenden, bei dem der Wert des State Namens ACTIVE in der Ausgabe des list-services Befehls enthalten ist. Wenn mehr als ein Dienst ausgeführt wird, beenden Sie jeden Dienst, bevor Sie fortfahren.

Note

Der Amazon S3 S3-Adapter EC2 AWS STS, Amazon und die IAM-Dienste können nicht gestoppt werden. Wenn Amazon S3 S3-kompatibler Speicher auf Snowball Edge läuft, beenden Sie ihn, bevor Sie Updates installieren. Amazon S3 S3-kompatibler Speicher auf Snowball Edge hat s3-snow als serviceId

```

snowballEdge stop-service --service-id service-id --device-ip-addresses snow-
device-1-ip-address snow-device-device-2-ip-address snow-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code 29-character-unlock-code --
endpoint https://snow-device-ip-address

```

Example der Ausgabe des Befehls **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.

5. Führen Sie für jedes Gerät im Cluster den `install-updates` Befehl aus.

```
snowballEdge install-updates
```

6. Sie können den Status dieser Installation mit dem Befehl `describe-device-software` überprüfen.

```
snowballEdge describe-device-software
```

Example der Ausgabe des **describe-device-service** Befehls

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Wenn dies der `Install State` `Requires Reboot` ist, haben Sie das Softwareupdate für Ihr Snowball Edge-Gerät erfolgreich installiert. Wenn eine Aktualisierung aktualisiert wird, wird sie nicht automatisch auf das Gerät angewandt. Um die Installation der Aktualisierung abzuschließen, muss das Gerät neu gestartet werden.

Warning

Wenn Sie das Snowball Edge-Gerät neu starten, ohne alle Aktivitäten auf dem Gerät zu beenden, können Daten verloren gehen.

7. Starten Sie alle Geräte im Cluster neu, entsperren Sie den Cluster und starten Sie alle Geräte im Cluster erneut. Damit ist die Installation der heruntergeladenen Softwareupdates abgeschlossen. Weitere Informationen zum Neustarten der Geräte finden Sie unter Snowball Edge [neu starten](#).

Weitere Informationen zum Entsperren des Geräteclusters finden Sie unter [Snowball Edge entsperren](#).

8. Nachdem jedes Gerät im Cluster zweimal neu gestartet wurde, entsperren Sie den Cluster und überprüfen Sie dann mithilfe des `check-for-updates` Befehls, ob das Gerät aktualisiert wurde. Dieser Befehl gibt die neueste verfügbare Version der Snowball Edge-Software sowie die aktuelle Version zurück, die auf dem Gerät installiert ist. Wenn die aktuelle Version und die neueste verfügbare Version identisch sind, wurde das Gerät erfolgreich aktualisiert.

Sie haben den Snowball Edge oder den Gerätecluster jetzt erfolgreich aktualisiert und bestätigt, dass das Update auf die neueste Snowball Edge-Software durchgeführt wurde.

Aktualisierung des SSL-Zertifikats auf Snowball Edge-Geräten

Wenn Sie Ihren Snowball Edge länger als 360 Tage behalten möchten, müssen Sie das Secure Sockets Layer (SSL) -Zertifikat auf dem Gerät aktualisieren, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Wenn das Zertifikat abläuft, können Sie das Gerät nicht verwenden und müssen es an AWS zurückgeben.

AWS benachrichtigt Sie 30 Tage vor Ablauf des SSL-Zertifikats für Snowball Edge, das Sie besitzen. Die Benachrichtigung erfolgt per E-Mail Health Dashboard und als AWS CloudTrail Ereignis. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, mit dem das Snowball Edge-Gerät bestellt wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und fordern Sie so schnell wie möglich ein Update an, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Weitere Informationen zu Health Dashboard finden Sie im [AWS Health Benutzerhandbuch](#). Weitere Informationen zu CloudWatch Ereignissen finden Sie unter [Arbeiten mit dem CloudTrail Ereignisverlauf](#).

Die Aktualisierung des SSL-Zertifikats erfolgt über den Snowball Edge-Client. Die neueste Version des Snowball Edge-Clients muss heruntergeladen und auf einem Computer in Ihrer lokalen Umgebung installiert werden, der über eine Netzwerkverbindung zu dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter [Verwenden des Snowball Edge-Clients](#).

In diesem Thema wird erklärt, wie Sie feststellen, wann das Zertifikat abläuft, und wie Sie Ihr Gerät aktualisieren können.

1. Verwenden Sie den `snowballEdge describe-device-software` Befehl, um zu bestimmen, wann das Zertifikat abläuft. In der Ausgabe des Befehls `CertificateExpiry` beinhaltet der Wert von das Datum und die Uhrzeit, an dem das Zertifikat abläuft.

Example der **describe-device-software** Ausgabe

```
Installed version: 101
Installing version: 102
Install State: Downloading
CertificateExpiry : Thur Jan 01 00:00:00 UTC 1970
```

2. Kontaktieren Sie uns Support und fordern Sie eine Aktualisierung des SSL-Zertifikats an.
3. Support stellt eine Aktualisierungsdatei zur Verfügung. [Laden Sie die Aktualisierungsdatei herunter](#) und [installieren Sie](#) sie.
4. Verwenden Sie den neuen Entsperrcode und die neue Manifestdatei, wenn Sie [den Snowball Edge entsperren und ein Gerät](#) .

Aktualisieren Sie Ihr Amazon Linux 2 AMIs auf Snowball Edge

Als bewährte Methode zur Sicherheit sollten Sie Ihr Amazon Linux 2 AMIs up-to-date auf Snowball Edge verwenden. Suchen Sie regelmäßig nach Updates für [Amazon Linux 2 AMI \(HVM\), SSD Volume Type \(64-Bit x86\)](#). AWS Marketplace Wenn Sie feststellen, dass Ihr AMI aktualisiert werden muss, importieren Sie das neueste Amazon Linux 2-Image auf das Snow-Gerät. Weitere Informationen finden Sie unter [Importieren eines Images auf Ihr Gerät als EC2 Amazon-kompatibles AMI](#).

Sie können die neueste Amazon Linux 2-Image-ID auch mit dem `ssm get-parameters` Befehl in der abrufen AWS CLI.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Der Befehl gibt die neueste Image-ID des AMI zurück. Zum Beispiel:

ami-0ccb473bada910e74

Snowball Edge-Jobs verstehen

Ein Job in AWS Snowball Edge ist eine separate Arbeitseinheit, die definiert wird, wenn Sie ihn in der Konsole oder der Job-Management-API erstellen. Bei dem AWS Snowball Edge Gerät gibt es drei verschiedene Auftragsarten, die alle über lokale Speicher- und Rechenfunktionen verfügen. Diese Funktion verwendet die NFS-Schnittstelle oder die Amazon S3 S3-Schnittstelle zum Lesen und Schreiben von Daten. Es löst Lambda-Funktionen auf der Grundlage von Amazon S3 PUT-Objekt-API-Aktionen aus, die lokal auf dem AWS Snowball Edge Gerät ausgeführt werden.

- [Jobs zum Importieren von Daten in Amazon S3 mit einem Snowball Edge-Gerät](#)— Die Übertragung von 210 TB oder weniger Ihrer lokalen Daten wurde auf ein einzelnes Gerät kopiert und dann in Amazon S3 verschoben. Bei Importaufträgen bestehen zwischen Snowball-Geräten und Aufträgen eine one-to-one Beziehung. Jedem Auftrag wird genau ein Gerät zugeordnet. Wenn Sie mehr Daten importieren müssen, können Sie neue Importaufträge erstellen oder bestehende Aufträge klonen. Wenn Sie ein Gerät dieses Auftragsstyps zurücksenden, werden die darauf befindlichen Daten in Amazon S3 importiert.
- [Jobs zum Exportieren von Daten aus Amazon S3 mit einem Snowball Edge-Gerät](#)— Die Übertragung einer beliebigen Datenmenge (in Amazon S3), die auf eine beliebige Anzahl von Snowball Edge-Geräten kopiert und dann jeweils ein AWS Snowball Edge Gerät an Ihr lokales Datenziel verschoben wird. Exportaufträge werden bei der Erstellung in Teilaufträge getrennt. Jeder Auftragsteil ist nicht größer als 210 TB, und jedem Auftragsteil ist genau ein AWS Snowball Edge Gerät zugeordnet. Nach der Rückgabe eines Gerät für diese Auftragsart werden die Daten darauf gelöscht.
- [Informationen zur Verwendung von Snowball Edge-Geräten zur Bereitstellung lokaler Rechen- und Speicherfunktionen](#)— Diese Jobs betreffen ein AWS Snowball Edge Gerät oder mehrere Geräte, die in einem Cluster verwendet werden. Diese Jobs beginnen nicht wie bei einem Exportauftrag mit Daten in ihren Buckets, und sie können am Ende keine Daten wie bei einem Importauftrag in Amazon S3 importieren lassen. Nach der Rückgabe eines Gerät für diese Auftragsart werden die Daten darauf gelöscht. Bei dieser Auftragsart können Sie auch einen Cluster von Geräten erstellen. Ein Cluster bietet eine verbesserte Ausfallsicherheit und skalierbare Kapazität für den lokalen Speicher.

In Regionen, in denen Lambda nicht verfügbar ist, wird dieser Auftragsstyp nur als Lokaler Speicher bezeichnet.

Einzelheiten zu Snowball Edge-Jobs

Stellen Sie vor dem Erstellen eines Jobs sicher, dass die [Voraussetzungen](#) erfüllt sind. Jeder Auftrag wird über die Details definiert, die Sie bei seiner Erstellung angeben. In der folgenden Tabelle werden alle Details eines Auftrags beschrieben.

Konsolen-ID	API-Kennung	Beschreibung im Detail
Job name (Auftragsname)	Description	Ein Name für den Auftrag mit alphanumerischen Zeichen, Leerzeichen und beliebigen Unicode-Sonderzeichen.
Job type	JobType	Die Art des Auftrags – Import bzw. Export oder lokale Datenverarbeitung und Speicher.
Auftrags-ID	JobId	Eine eindeutige Bezeichnung mit 39 Zeichen zur Identifizierung des Auftrags. Die Auftrags-ID befindet sich unten auf dem Versandetikett im E Ink-Display und im Namen der Manifestdatei eines Auftrags.
Adresse	AddressId	Die Adresse, an die das Gerät gesendet wird. Im Falle der API ist dies die ID für den Adressdatentyp.
Created date	CreationDate	Das Datum, an dem Sie den Auftrag erstellt haben.
Shipping speed	ShippingOption	Versandoptionen sind regional unterschiedlich. Weitere Informationen finden Sie unter

Konsolen-ID	API-Kennung	Beschreibung im Detail
		Versandgeschwindigkeiten für Snowball Edge.
IAM role ARN (IAM-Rollen-ARN)	RoleARN	Dieser Amazon Resource Name (ARN) ist die AWS Identity and Access Management (IAM) -Rolle, die bei der Auftragserstellung mit Schreibberechtigungen für Ihre Amazon S3 S3-Bucket s erstellt wird. Der Erstellungsprozess erfolgt automatisch, und die IAM-Rolle, die Sie annehmen lassen AWS Snowball Edge , wird nur zum Kopieren Ihrer Daten zwischen Ihren S3-Buckets und dem Snowball verwendet. Weitere Informationen finden Sie unter Für die Verwendung der AWS Snowball Edge Konsole sind Berechtigungen erforderlich.

Konsolen-ID	API-Kennung	Beschreibung im Detail
AWS KMS Schlüssel	KmsKeyARN	In AWS Snowball Edge, AWS Key Management Service (AWS KMS) verschlüsselt die Schlüssel auf jedem Snowball. Wenn Sie Ihren Job erstellen, wählen oder erstellen Sie auch einen ARN für einen AWS KMS Verschlüsselungsschlüssel, den Sie besitzen. Weitere Informationen finden Sie unter AWS Key Management Service in AWS Snowball Edge .
Snowball capacity	SnowballCapacityPreference	Die Speicherkapazität des in diesem Job bestellten AWS Snowball Edge Geräts. Die verfügbare Größe hängt von Ihrer ab AWS-Region.
Storage Service	N/A	Der mit diesem Job verknüpfte AWS Speicherdienst, in diesem Fall Amazon S3.
Ressourcen	Resources	Die mit Ihrem Job verknüpften AWS Speicherservice-Ressourcen. In diesem Fall sind dies die Amazon S3 S3-Buckets, in die oder von denen Ihre Daten übertragen werden.

Konsolen-ID	API-Kennung	Beschreibung im Detail
Job type	JobType	Die Art des Auftrags – Import bzw. Export oder lokale Datenverarbeitung und Speicher.
Snowball type	SnowballType	Der Typ des Snowball Edge-Geräts, das für diesen Job bestellt wurde.
Cluster ID	ClusterId	Eine eindeutige Bezeichnung mit 39 Zeichen zur Identifizierung Ihres Clusters.

Status von Snowball Edge-Jobs

Jeder AWS Snowball Edge Geräteauftrag hat einen Status, der sich ändert und den aktuellen Status des Auftrags angibt. Der Auftragsstatus enthält keine Informationen zur Integrität, dem aktuellen Verarbeitungsstatus und dem auf den zugeordneten Geräten verbrauchten Speicher.

Um den Status eines Jobs zu sehen

1. Loggen Sie sich in die ein [Managementkonsole für die AWS Snow-Familie](#).
2. Wählen Sie im Job-Dashboard den Job aus.
3. Klicken Sie in der Konsole auf Ihren Jobnamen.
4. Der Bereich Auftragsstatus befindet sich ganz oben und gibt den Status des Jobs wieder.

AWS Snowball Edge Status des Geräteauftrags

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
Job created	New	Ihr Auftrag ist gerade erstellt worden. Nur in diesem Status können Sie einen Auftrag abbrechen (einen

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
		Exportauftrag auch teilweise).
Gerät wird vorbereitet	PreparingAppliance	AWS bereitet ein Gerät für Ihren Job vor.
Exporting	InProgress	AWS exportiert Ihre Daten von Amazon S3 auf ein Gerät.
Preparing shipment	PreparingShipment	AWS bereitet sich darauf vor, ein Gerät an Sie zu versenden . Die Informationen zur voraussichtlichen Sendungsverfolgung werden für Kunden im Status bereitgestellt.
In transit to you	InTransitToCustomer	Das Gerät wurde an die Adresse versendet, die Sie bei Erstellung des Auftrags angegeben haben.
Delivered to you	WithCustomer	Das Gerät ist an die Adresse ausgeliefert worden, die Sie bei Erstellung des Auftrags angegeben haben.

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
Auf dem Weg nach AWS	InTransitToAWS	Sie haben das Gerät zurückgeschickt an AWS.
Im Sortierzentrum	WithAWSSortingFacility	Das Gerät, das für diesen Auftrag notwendig ist, befindet sich in unserem internen Sortierzentrum. Jede weitere Verarbeitung von Importaufträgen in Amazon S3 wird in Kürze beginnen, normalerweise innerhalb von 2 Tagen.
Bei AWS	WithAWS	Ihre Sendung ist bei eingetroffen AWS. Wenn Sie Daten importieren, beginnt der Import in der Regel innerhalb eines Tages nach Ankunft der Sendung.
Importing	InProgress	AWS importiert Ihre Daten in Amazon Simple Storage Service (Amazon S3).

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
Completed	Complete	Ihr Auftrag bzw. ein Teil Ihres Auftrags wurde erfolgreich abgeschlossen.
Canceled	Cancelled	Ihr Auftrag wurde abgebrochen.

Status von Snowball Edge-Cluster-Jobs

Jeder Cluster besitzt einen Status, der sich entsprechend dem aktuellen allgemeinen Fortschritt des Clusters ändert. Jeder einzelne Knoten des Clusters hat seinen eigenen Auftragsstatus.

Der Status des Clusters umfasst keine Angaben zur Integrität, dem aktuellen Verarbeitungsstatus und dem Speicher, der für den Cluster oder seine Knoten verwendet wird.

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
Awaiting Quorum	AwaitingQuorum	Der Cluster wurde noch nicht erstellt, da nicht genügend Knoten vorhanden sind, um mit der Verarbeitung der Clusteranfrage zu beginnen. Damit ein Cluster erstellt werden kann, muss er mindestens fünf Knoten haben.
Ausstehend	Pending	Der Cluster wurde erstellt. Wir bereiten die Knoten für den Versand vor. Sie

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
		können den Status der einzelnen Knoten über deren jeweiligen Auftragsstatus nachverfolgen.
Delivered to you	InUse	Mindestens ein Knoten des Clusters befindet sich an der Adresse, die Sie bei der Auftragserstellung angegeben haben.
Completed	Complete	Alle Knoten des Clusters wurden zurückgegeben AWS.
Canceled	Cancelled	Die Anforderung zur Erstellung eines Clusters wurde storniert. Cluster-Anforderungen können nur abgebrochen werden, wenn sie den ausstehenden Status noch nicht erreicht haben.

Jobs zum Importieren von Daten in Amazon S3 mit einem Snowball Edge-Gerät

Bei einem Importauftrag werden Ihre Daten auf das AWS Snowball Edge Gerät mit dem integrierten Amazon S3 S3-Adapter oder dem NFS-Mountpoint kopiert. Ihre Importdatenquelle sollte sich vor Ort

befinden. Anders ausgedrückt, sollten die Speichergeräte mit den zu übertragenden Daten physisch an der Adresse vorliegen, die Sie bei der Auftragserstellung angegeben haben.

Wenn Sie Dateien importieren, wird jede Datei zu einem Objekt in Amazon S3 und jedes Verzeichnis wird zu einem Präfix. Wenn Sie Daten in einen vorhandenen Bucket importieren, werden vorhandene Objekte, die den gleichen Namen wie die gerade importierten Objekte haben, überschrieben. Die Import-Auftragsart bietet auch lokale Datenverarbeitungs- und Speicherfunktionalität. Diese Funktion verwendet die NFS-Schnittstelle oder den Amazon S3 S3-Adapter zum Lesen und Schreiben von Daten und löst Lambda-Funktionen aus, die auf den lokal auf dem Gerät ausgeführten Amazon S3 S3-PUT-Objekt-API-Aktionen basieren. AWS Snowball Edge

Wenn alle Ihre Daten in die angegebenen Amazon S3 S3-Buckets importiert wurden AWS Cloud AWS , wird das Gerät vollständig gelöscht. Die Löschung erfolgt gemäß NIST 800-88-Standard.

Nach Abschluss des Imports können Sie einen Auftragsbericht herunterladen. In diesem Bericht werden alle Objekte aufgeführt, die nicht erfolgreich importiert werden konnten. Weitere Informationen hierzu finden Sie in den Erfolgs- und Fehlerprotokollen.

Important

Löschen Sie Ihre lokalen Kopien der übertragenen Daten nicht, bis Sie die Ergebnisse des Auftragsabschlussberichts bestätigen und Ihre Importprotokolle überprüfen können.

Jobs zum Exportieren von Daten aus Amazon S3 mit einem Snowball Edge-Gerät

Note

Tags und Metadaten werden derzeit NICHT unterstützt, d. h. alle Tags und Metadaten würden beim Exportieren von Objekten aus S3-Buckets entfernt.

Ihre Datenquelle für einen Exportauftrag sind ein oder mehrere Amazon S3 S3-Buckets. Nachdem die Daten für einen Auftragsteil von Amazon S3 auf ein AWS Snowball Edge Gerät übertragen wurden, können Sie einen Auftragsbericht herunterladen. Dieser Bericht führt die Objekte auf, bei denen die Übertragung auf das Gerät fehlgeschlagen ist. Weitere Informationen hierzu finden Sie in den Erfolgs- und Fehlerprotokollen zu Ihrem Auftrag.

Sie können für jeden Exportauftrag eine beliebige Anzahl von Objekten exportieren und dabei so viele Geräte verwenden, wie für den Abschluss der Übertragung erforderlich sind. Die Teile jedes AWS Snowball Edge Geräts für den Auftrag eines Exportauftrags werden nacheinander geliefert. Die nachfolgenden Geräte werden an Sie versendet, nachdem der vorherige Teil des Auftrags den AWS Status In Bearbeitung erhalten hat.

Wenn Sie Objekte mithilfe des Amazon S3 S3-Adapters oder des NFS-Bereitstellungspunkts von einem Gerät in Ihr lokales Datenziel kopieren, werden diese Objekte als Dateien gespeichert. Beim Kopieren von Objekten an einen Speicherort, der bereits Dateien enthält, werden vorhandene Dateien gleichen Namens überschrieben. Die Export-Auftragsart umfasst außerdem lokale Datenverarbeitungs- und Speicherfunktionalität. Diese Funktion verwendet die NFS-Schnittstelle oder den Amazon S3 S3-Adapter zum Lesen und Schreiben von Daten und löst Lambda-Funktionen aus, die auf den lokal auf dem Gerät ausgeführten Amazon S3 S3-PUT-Objekt-API-Aktionen basieren.

AWS Snowball Edge

Wenn wir AWS ein zurückgesandtes Gerät erhalten, löschen wir es gemäß den NIST 800-88-Standards vollständig.

Important

Daten, die Sie auf ein Snow-Gerät exportieren möchten, müssen sich in Amazon S3 befinden. Alle Daten Amazon Glacier, die Sie auf das Snow-Gerät exportieren möchten, müssen aufgetaut oder in die Speicherklasse S3 verschoben werden, bevor sie exportiert werden können. Tun Sie dies, bevor Sie den Snow-Exportauftrag erstellen. Ändern, aktualisieren oder löschen Sie die exportierten Amazon S3 S3-Objekte erst, wenn Sie überprüfen können, ob alle Ihre Inhalte für den gesamten Job an Ihr lokales Datenziel kopiert wurden.

Wenn Sie einen Exportauftrag erstellen, können Sie einen gesamten Amazon S3 S3-Bucket oder einen bestimmten Bereich von Objektschlüsseln exportieren.

Verwenden von Amazon S3 S3-Objektschlüsseln beim Exportieren von Daten auf ein Snowball Edge-Gerät

Wenn Sie einen Exportauftrag in der [Managementkonsole für die AWS Snow-Familie](#) oder mit der Job-Management-API erstellen, können Sie einen gesamten Amazon S3 S3-Bucket oder einen bestimmten Bereich von Objektschlüsseln exportieren. Objektschlüsselnamen sind eindeutige

Bezeichner für ein Objekt in einem Bucket. Um einen Bereich zu exportieren, definieren Sie die Länge des Bereichs entweder durch die Angabe des Bereichsanfangs oder des Bereichsendes (beide Werte gehören zum Bereich) oder durch beide Angaben.

Bereiche sind gemäß UTF-8 binär sortiert. Binäre UTF-8-Daten werden folgendermaßen sortiert:

- Die Zahlen 0—9 stehen vor englischen Groß- und Kleinbuchstaben.
- Englische Großbuchstaben werden vor englischen Kleinbuchstaben eingeordnet.
- Englische Kleinbuchstaben werden nach englischen Großbuchstaben und Ziffern eingeordnet.
- Sonderzeichen werden zwischen den anderen Zeichensätzen eingeordnet.

[Weitere Informationen zu den Besonderheiten von UTF-8 finden Sie unter UTF-8 auf Wikipedia.](#)

Beispiele für die Verwendung von Amazon S3 S3-Objektschlüsseln beim Exportieren von Daten auf ein Snowball Edge-Gerät

Angenommen, Sie haben einen Bucket mit den folgenden Objekten und Präfixen, sortiert in binärer UTF-8-Binärreihenfolge:

- 01
- Aardvark
- Aardwolf
- Aasvogel/apple
- Aasvogel/arrow/object1
- Aasvogel/arrow/object2
- Aasvogel/banana
- Aasvogel/banker/object1
- Aasvogel/banker/object2
- Aasvogel/cherry
- Banana
- Car

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
(Keine)	(Keine)	Alle Objekte in Ihrem Bucket
(Keine)	Aasvogel	01 Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry
(Keine)	Aasvogel/banana	01 Aardvark Aardwolf Aasvogel/apple

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
		Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana
Aasvogel	(Keine)	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
Aardwolf	(Keine)	Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
Aar	(Keine)	Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
car	(Keine)	Es werden keine Objekte exportiert. Sie erhalten außerdem eine Fehlermeldung, wenn Sie versuchen, den Auftrag zu erstellen. Beachten Sie, dass car unterhalb von Car nach UTF-8-Binärwerten sortiert ist.
Aar	Aarr	Aardvark Aardwolf
AAS/Vogel/Pfeil	Aasvogel/Arrox	Aasvogel/arrow/object1 Aasvogel/arrow/object2

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
Aasvogel/apple	Aasvogel/banana	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana
Aasvogel/apple	Aasvogel/Bankier	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
Aasvogel/apple	Aasvogel/cherry	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry

Angenommen, Sie haben diese drei Buckets und möchten alle Objekte aus Folder2 kopieren.

- s3://bucket/folder1/
- s3://bucket/folder2/
- s3://bucket/folder3/

Der angegebene Bereich beginnt	Ende des angegebenen Bereichs	Objekte in dem Bereich, der exportiert werden soll
Ordner2/	Ordner2/	Alle Objekte im Bucket Folder2.

Bewährte Methoden für Jobs, die Daten von Amazon S3 auf ein Snowball Edge-Gerät exportieren

- Stellen Sie sicher, dass sich die Daten in Amazon S3 befinden, und stapeln Sie kleine Dateien, bevor Sie den Job bestellen
- Stellen Sie sicher, dass die Schlüsselbereiche in der Exportauftragsdefinition angegeben sind, wenn Sie Millionen von Objekten in Ihrem Bucket haben
- Aktualisieren Sie Objektschlüssel, um den Schrägstrich im Namen zu entfernen, da Objekte mit abschließenden Schrägstrichen im Namen (/oder\) nicht an Snowball Edge übertragen werden
- Für S3-Buckets beträgt die Objektlängenbeschränkung 255 Zeichen.
- Für S3-Buckets, für die Version aktiviert ist, wird nur die aktuelle Version von Objekten exportiert.
- Löschmarken werden nicht exportiert.

Informationen zur Verwendung von Snowball Edge-Geräten zur Bereitstellung lokaler Rechen- und Speicherfunktionen

Lokale Rechen- und Speicheraufträge ermöglichen es Ihnen, Amazon S3 S3-kompatiblen Speicher auf Snowball Edge lokal und ohne Internetverbindung zu verwenden. Sie können keine Daten von Amazon S3 auf das Gerät exportieren oder Daten in Amazon S3 importieren, wenn das Gerät zurückgegeben wird.

Themen

- [Informationen zu Aufträgen zum lokalen Speichern von Daten auf Snowball Edge-Geräten](#)
- [Informationen zu Aufträgen, die lokalen Speicher auf einem Cluster von Snowball Edge-Geräten bereitstellen](#)

Informationen zu Aufträgen zum lokalen Speichern von Daten auf Snowball Edge-Geräten

Sie können Objekte auf einem AWS Snowball Edge Gerät lesen und schreiben, indem Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge oder den S3-Adapter verwenden. Wenn Sie ein Gerät bestellen und den S3-Adapter verwenden möchten, wählen Sie auch aus, welche Amazon S3 S3-Buckets auf dem Gerät enthalten sein sollen, wenn Sie es erhalten. Wenn Sie Amazon S3 S3-kompatiblen Speicher auf Snowball Edge verwenden, sind keine Amazon S3 S3-Buckets auf dem Gerät enthalten, wenn Sie ihn erhalten.

Sie können Amazon S3 S3-Buckets auf den Snowball Edge-Geräten erstellen, um Objekte vor Ort für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Amazon S3-kompatibler Speicher auf Snowball Edge bietet eine neue Speicherklasse SNOW, die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Snowball Edge-Geräten zu speichern. Sie können für Snowball Edge-Buckets dieselben APIs Funktionen wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte zurückgegeben werden, werden alle Daten gelöscht AWS, die in einem Amazon S3 S3-kompatiblen Speicher auf Snowball Edge erstellt oder gespeichert wurden. Weitere Informationen finden Sie unter Jobs [nur für lokale Datenverarbeitung und Speicherung](#).

Weitere Informationen finden Sie in diesem Handbuch unter [Amazon S3 S3-kompatibler Speicher auf Snowball Edge](#).

Wenn Sie das Gerät nicht mehr verwenden, geben Sie es wieder an AWS, und das Gerät wird gelöscht. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Informationen zu Aufträgen, die lokalen Speicher auf einem Cluster von Snowball Edge-Geräten bereitstellen

Ein Cluster ist eine logische Gruppierung von Snowball Edge-Geräten in Gruppen von 3 bis 16 Geräten. Ein Cluster wird als einzelner Job erstellt, der im Vergleich zu anderen AWS Snowball Edge Jobangeboten eine höhere Haltbarkeit und Speichergröße bietet. Weitere Informationen zu Cluster-Aufträgen finden Sie in diesem Leitfaden unter [Clustering-Übersicht](#).

Bewährte Methoden für die Verwendung eines Snowball Edge-Geräts

Um den größtmöglichen Nutzen und die Zufriedenheit mit Ihrem AWS Snowball Edge Gerät zu erzielen, empfehlen wir Ihnen, diese bewährten Methoden zu befolgen.

Sicherheitsempfehlungen für Snowball Edge

Im Folgenden finden Sie Empfehlungen und bewährte Methoden zur Aufrechterhaltung der Sicherheit bei der Arbeit mit einem AWS Snowball Edge Gerät.

Allgemeine Sicherheit

- Wenn Sie etwas an dem AWS Snowball Edge Gerät bemerken, das verdächtig aussieht, verbinden Sie es nicht mit Ihrem internen Netzwerk. Setzen Sie [AWS Support](#) sich stattdessen mit uns in Verbindung und ein neues AWS Snowball Edge Gerät wird Ihnen zugeschickt.
- Wir empfehlen, dass Sie keine Kopie des Entsperrcodes am selben Ort auf der Workstation speichern wie das Manifest für diesen Job. Wenn Sie diese an verschiedenen Orten speichern, können Sie verhindern, dass Unbefugte Zugriff auf das AWS Snowball Edge Gerät erhalten. Beispielsweise können Sie eine Kopie des Manifests auf Ihrem lokalen Server speichern und den Code, der das Gerät entsperrt, per E-Mail an den Benutzer senden. Dieser Ansatz beschränkt den Zugriff auf das AWS Snowball Edge Gerät auf Personen, die Zugriff auf die auf dem Server gespeicherten Dateien und die E-Mail-Adresse des Benutzers haben.
- Die Anmeldeinformationen, die angezeigt werden, wenn Sie die Snowball Edge-Client-Befehle `list-access-keys` und `execute-get-secret-access-key`, sind ein Paar von Zugriffsschlüsseln, die für den Zugriff auf Ihr Gerät verwendet werden.

Diese Schlüssel sind ausschließlich dem Auftrag und den lokalen Ressourcen auf dem Gerät zugeordnet. Sie sind AWS-Konto weder Ihrem noch einem anderen AWS-Konto zugeordnet. Wenn Sie versuchen, mit diesen Schlüsseln auf Dienste und Ressourcen in der zuzugreifen AWS Cloud, schlagen sie fehl, da sie nur für die lokalen Ressourcen funktionieren, die mit Ihrem Job verknüpft sind.

- Wenn Sie der Meinung sind, dass Ihre Anmeldeinformationen verloren gegangen sind oder kompromittiert wurden, fordern Sie eine neue Manifestdatei und den Entsperrcode an, indem Sie den Schritten zur Aktualisierung des SSL-Zertifikats des Geräts folgen. Siehe [Aktualisierung des SSL-Zertifikats auf Snowball Edge-Geräten](#).

Informationen zur Verwendung von AWS Identity and Access Management (IAM-) Richtlinien zur Zugriffskontrolle finden Sie unter. [AWS-Verwaltete \(vordefinierte\) Richtlinien für AWS Snowball Edge](#)

Netzwerksicherheit

- Es wird empfohlen, jeweils nur eine Methode zum Lesen und Schreiben von Daten in einen lokalen Bucket auf einem AWS Snowball Edge Gerät zu verwenden.
- Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie das AWS Snowball Edge Gerät nicht vom Computer und ändern Sie nicht die Netzwerkeinstellungen, während Sie Daten übertragen.
- Dateien, in die auf dem Gerät geschrieben wird, sollten sich in einem statischen Zustand befinden. Dateien, die während des Schreibvorgangs geändert werden, können zu Lese-/Schreibkonflikten führen.
- Weitere Informationen zur Verbesserung der Leistung Ihres AWS Snowball Edge Geräts finden Sie unter. [Empfehlungen für die beste Datenübertragungsleistung zu oder von einem Snowball Edge](#)

Bewährte Methoden für die Verwaltung von Ressourcen auf einem Snowball Edge

Beachten Sie die folgenden bewährten Methoden für die Verwaltung von Aufträgen und Ressourcen auf Ihrem AWS Snowball Edge Gerät.

- Die 15 kostenlosen Tage für die Durchführung Ihrer lokalen Datenübertragung beginnen am Tag nach der Ankunft des AWS Snowball Edge Geräts in Ihrem Rechenzentrum. Dies gilt nur für Snowball Edge-Gerätetypen.
- Sie können einen Auftrag nur im Status Job created (Job wurde erstellt) abbrechen. Wenn ein Job einen anderen Status annimmt, können Sie ihn nicht stornieren. Dies gilt für Cluster.
- Löschen Sie bei Importaufträgen Ihre lokalen Kopien der übertragenen Daten erst, wenn der Import in Amazon S3 erfolgreich war. Stellen Sie als Teil des Vorgangs sicher, die Ergebnisse der Datenübertragung zu überprüfen.

Empfehlungen für die beste Datenübertragungsleistung zu oder von einem Snowball Edge

Note

Die Leistung der Datenübertragung hängt von der Netzwerkumgebung, den Betriebssystemen, der Kopiermethode, dem Protokoll, der Leseleistung der Quelldaten und den Datensatzmerkmalen wie der Dateigröße ab. Um die genauen Datenübertragungsraten und Datenübertragungszeiten zu ermitteln, empfehlen wir Ihnen, die Leistung anhand von proof-of-concept Tests in Ihrer Umgebung zu messen.

Im Folgenden finden Sie Empfehlungen und Informationen zur AWS Snowball Edge Geräteleistung. In diesem Abschnitt wird die Leistung allgemein beschrieben, da lokale Umgebungen unterschiedliche Vorgehensweisen haben — unterschiedliche Netzwerktechnologien, unterschiedliche Hardware, unterschiedliche Betriebssysteme, unterschiedliche Verfahren usw.

In der folgenden Tabelle wird beschrieben, wie sich die Übertragungsrate Ihres Netzwerks darauf auswirkt, wie lange es dauert, ein Snowball Edge-Gerät mit Daten zu füllen. Durch die Übertragung kleinerer Dateien wird Ihre Übertragungsgeschwindigkeit aufgrund des erhöhten Overheads reduziert. Wenn Sie viele kleine Dateien haben, empfehlen wir, diese in größere Archive zu komprimieren, bevor Sie sie auf ein Snowball Edge-Gerät übertragen.

Geschwindigkeit (MB/s)	82 TB Übertragungszeit
800	1.22 Tage
450	2.11 Tage
400	2.37 Tage
300	3.16 Tage
277	3.42 Tage
200	4.75 Tage
100	9.49 Tage

Geschwindigkeit (MB/s)	82 TB Übertragungszeit
60	15.53 Tage
30	31.06 Tage
10	85.42 Tage

Um aussagekräftige Hinweise zur Leistung zu geben, wird in den folgenden Abschnitten beschrieben, wie Sie bestimmen, wann das AWS Snowball Edge Gerät verwendet werden sollte und wie Sie den Service optimal nutzen können.

Die folgenden Methoden werden dringend empfohlen, da sie den größten Einfluss auf die Verbesserung der Leistung Ihrer Datenübertragung haben:

- Verzeichnisse sollten nicht mehr als 500.000 Dateien oder Verzeichnisse enthalten.
- Wir empfehlen, dass alle auf ein Snowball Edge-Gerät übertragenen Dateien nicht kleiner als 1 MB sind.
- Wenn Sie viele Dateien mit einer Größe von weniger als 1 MB haben, empfehlen wir, sie in größere Archive zu komprimieren, bevor Sie sie auf ein Snowball Edge-Gerät übertragen.

Verbesserung der Geschwindigkeit der Datenübertragung zu und von einem Snowball Edge

Eine der besten Möglichkeiten, die Leistung eines AWS Snowball Edge Geräts zu verbessern, besteht darin, die Übertragung von Daten zu und von einem Gerät zu beschleunigen. Im Allgemeinen können Sie die Übertragungsgeschwindigkeit von Ihrer Datenquelle zum Gerät auf folgende Weise verbessern. Die folgende Liste ist nach den größten und den kleinsten positiven Auswirkungen auf die Leistung geordnet:

1. Gleichzeitiges Ausführen mehrerer Schreibvorgänge — Führen Sie dazu jeden Befehl von mehreren Terminalfenstern auf einem Computer aus, der über eine Netzwerkverbindung zu einem einzelnen AWS Snowball Edge Gerät verfügt.
2. Kleine Dateien stapelweise übertragen — Jeder Kopiervorgang hat aufgrund der Verschlüsselung einen gewissen Overhead. Um den Vorgang zu beschleunigen, können Sie Dateien in einem einzigen Archiv stapeln. Wenn Sie Dateien stapeln, können sie automatisch extrahiert werden,

wenn sie in Amazon S3 importiert werden. Weitere Informationen finden Sie unter [Batching kleiner Dateien zur Verbesserung der Datenübertragungsleistung an Snowball Edge](#).

3. Führen Sie während der Übertragung keine anderen Operationen an Dateien durch — Das Umbenennen von Dateien während der Übertragung, das Ändern ihrer Metadaten oder das Schreiben von Daten in die Dateien während eines Kopiervorgangs wirkt sich negativ auf die Übertragungsleistung aus. Wir empfehlen, den Status der Dateien nicht zu verändern, während sie gesendet werden.
4. Reduzieren Sie die Nutzung des lokalen Netzwerks — Ihr AWS Snowball Edge Gerät kommuniziert über Ihr lokales Netzwerk. So können Sie die Datenübertragungsgeschwindigkeit verbessern, indem Sie den sonstigen lokalen Netzwerkverkehr zwischen dem AWS Snowball Edge Gerät, dem Switch, mit dem es verbunden ist, und dem Computer, der Ihre Datenquelle hostet, reduzieren.
5. Vermeiden Sie unnötige Hops — Wir empfehlen, dass Sie Ihr AWS Snowball Edge Gerät, Ihre Datenquelle und den Computer, auf dem die Terminalverbindung zwischen ihnen ausgeführt wird, so einrichten, dass sie die einzigen Computer sind, die über einen einzigen Switch kommunizieren. Dadurch können die Datenübertragungsgeschwindigkeiten verbessert werden.

Sicherheit für AWS Snowball Edge

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Snowball Edge, finden Sie unter [AWS Services in Umfang nach Compliance-Programmen](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, 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 Nutzung anwenden können AWS Snowball Edge. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Snowball Edge , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Snowball Edge Ressourcen unterstützen.

Themen

- [Datenschutz in AWS Snowball Edge Edge](#)
- [Identity and Access Management in AWS Snowball Edge](#)
- [Protokollierung und Überwachung in AWS Snowball Edge](#)
- [Konformitätsüberprüfung für AWS Snowball Edge](#)
- [Ausfallsicherheit](#)
- [Sicherheit der Infrastruktur in AWS Snowball Edge](#)

Datenschutz in AWS Snowball Edge

AWS Snowball Edge entspricht dem [Modell der AWS gemeinsamen Verantwortung](#), das Vorschriften und Richtlinien für den Datenschutz beinhaltet. AWS ist verantwortlich für den Schutz der globalen Infrastruktur, die alle AWS Dienste betreibt. AWS behält die Kontrolle über die auf dieser Infrastruktur gehosteten Daten, einschließlich der Sicherheitskonfigurationen für den Umgang mit Kundeneinhalten und personenbezogenen Daten. AWS Kunden und APN-Partner, die entweder als Datenverantwortliche oder als Datenverarbeiter agieren, sind für alle personenbezogenen Daten verantwortlich, die AWS Cloud sie eingeben.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) einrichten, sodass jeder Benutzer nur die Berechtigungen erhält, die für die Erfüllung seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden zu schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS Snowball Edge oder anderen AWS Diensten arbeiten, die die Konsole, die API oder verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in AWS Snowball Edge oder andere Services eingeben, werden möglicherweise in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag [AWS Shared Responsibility Model and GDPR](#) im AWS -Sicherheitsblog.

Themen

- [Schützen von Daten in der Cloud](#)
- [Schützen von Daten auf Ihrem Gerät](#)

Schützen von Daten in der Cloud

AWS Snowball Edge schützt Ihre Daten, wenn Sie Daten in Amazon S3 importieren oder exportieren, wenn Sie einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen und wenn Ihr Gerät aktualisiert wird. In den folgenden Abschnitten wird beschrieben, wie Sie Ihre Daten schützen können, wenn Sie Snowball Edge verwenden und online sind oder mit AWS der Cloud interagieren.

Themen

- [Verschlüsselung für AWS Snowball Edge](#)
- [AWS Key Management Service in AWS Snowball Edge](#)

Verschlüsselung für AWS Snowball Edge

Wenn Sie einen Snowball Edge verwenden, um Daten in S3 zu importieren, sind alle auf ein Gerät übertragenen Daten durch SSL-Verschlüsselung über das Netzwerk geschützt. Zum Schutz ruhender Daten verwendet AWS Snowball Edge serverseitige Verschlüsselung (SSE).

Serverseitige Verschlüsselung in AWS Snowball Edge

AWS Snowball Edge unterstützt serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3). Bei der serverseitigen Verschlüsselung geht es darum, Daten im Ruhezustand zu schützen, und SSE-S3 verfügt über eine starke Multifaktor-Verschlüsselung, um Ihre Daten im Ruhezustand in Amazon S3 zu schützen. Weitere Informationen zu SSE-S3 finden Sie unter [Schützen von Daten mithilfe serverseitiger Verschlüsselung mit Amazon S3-Managed Encryption Keys \(SSE-S3\) im Amazon Simple Storage Service-Benutzerhandbuch](#).

Bietet derzeit AWS Snowball Edge keine serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C) an. Amazon S3 S3-kompatibler Speicher auf Snowball Edge bietet SSE-C für lokale Rechen- und Speicherjobs. Sie möchten diesen SSE-Typ möglicherweise

jedoch zum Schutz von importierten Daten verwenden oder setzen ihn möglicherweise auch bereits für zu exportierende Daten ein. Beachten Sie in diesem Fall jedoch die folgenden Punkte:

- Importieren —

Wenn Sie SSE-C verwenden möchten, um die Objekte zu verschlüsseln, die Sie in Amazon S3 importiert haben, sollten Sie in Betracht ziehen, stattdessen die SSE-KMS- oder SSE-S3-Verschlüsselung zu verwenden, die als Teil der Bucket-Richtlinie dieses Buckets eingerichtet wurde. Wenn Sie jedoch SSE-C verwenden müssen, um die Objekte zu verschlüsseln, die Sie in Amazon S3 importiert haben, müssen Sie das Objekt in Ihren Bucket kopieren, um es mit SSE-C zu verschlüsseln. Ein Beispiel für einen CLI-Befehl, um dies zu erreichen, ist unten dargestellt:

```
aws s3 cp s3://amzn-s3-demo-bucket/object.txt s3://amzn-s3-demo-bucket/object.txt --sse-c --sse-c-key 1234567891SAMPLEKEY
```

or

```
aws s3 cp s3://amzn-s3-demo-bucket s3://amzn-s3-demo-bucket --sse-c --sse-c-key 1234567891SAMPLEKEY --recursive
```

- Export — Wenn Sie Objekte exportieren möchten, die mit SSE-C verschlüsselt sind, kopieren Sie diese Objekte zunächst in einen anderen Bucket, der entweder keine serverseitige Verschlüsselung hat oder für den SSE-KMS oder SSE-S3 in der Bucket-Richtlinie dieses Buckets angegeben sind.

Aktivierung von SSE-S3 für Daten, die von einem Snowball Edge in Amazon S3 importiert wurden

Verwenden Sie das folgende Verfahren in der Amazon S3-Managementkonsole, um SSE-S3 für Daten zu aktivieren, die in Amazon S3 importiert werden. Es ist keine Konfiguration im Managementkonsole für die AWS Snow-Familie oder auf dem Snowball-Gerät selbst erforderlich.

Um die SSE-S3-Verschlüsselung für die Daten zu aktivieren, die Sie in Amazon S3 importieren, legen Sie einfach die Bucket-Richtlinien für alle Buckets fest, in die Sie Daten importieren. Sie Aktualisieren die Richtlinien so, dass die Berechtigung zum Hochladen von Objekten (`s3:PutObject`) verweigert wird, wenn in der Upload-Anfrage kein `x-amz-server-side-encryption-Header` enthalten ist.

Um SSE-S3 für in Amazon S3 importierte Daten zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie in der Liste der Buckets den Bucket aus, in den Sie Daten importieren möchten.
3. Wählen Sie Permissions (Berechtigungen).
4. Wählen Sie Bucket Policy aus.
5. Geben Sie im Bucket policy editor (Bucket-Richtlinieneditor) die folgende Richtlinie ein. Ersetzen Sie alle Vorkommen von *YourBucket* in dieser Richtlinie durch den tatsächlichen Namen Ihres Buckets.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```



```
}  
]  
}
```

6. Wählen Sie Speichern.

Sie haben die Konfiguration Ihres Amazon S3 S3-Buckets abgeschlossen. Wenn Ihre Daten in diesen Bucket importiert werden, werden sie durch SSE-S3 geschützt. Wiederholen Sie diese Schritte je nach Bedarf für die anderen Buckets.

AWS Key Management Service in AWS Snowball Edge

AWS Key Management Service (AWS KMS) ist ein verwalteter Dienst, der es Ihnen leicht macht, die zur Verschlüsselung Ihrer Daten verwendeten Verschlüsselungsschlüssel zu erstellen und zu kontrollieren. AWS KMS verwendet Hardware-Sicherheitsmodule (HSMs), um die Sicherheit Ihrer Schlüssel zu gewährleisten. Insbesondere AWS Snowball Edge ist der Amazon-Ressourcenname (ARN) für den AWS KMS Schlüssel, den Sie für einen Job auswählen, einem KMS-Schlüssel zugeordnet. Dieser KMS-Schlüssel wird verwendet, um den Entsperrcode für Ihren Auftrag zu verschlüsseln. Der Entsperrcode wird zum Entschlüsseln der oberen Verschlüsselungsebene in Ihrer Manifest-Datei verwendet. Die in der Manifestdatei gespeicherten Verschlüsselungsschlüssel werden verwendet, um die Daten auf dem Gerät zu ver- und entschlüsseln.

In AWS KMS schützt die Verschlüsselungsschlüssel AWS Snowball Edge, die zum Schutz der Daten auf den einzelnen AWS Snowball Edge Geräten verwendet werden. Wenn Sie den Auftrag erstellen, wählen Sie auch einen vorhandenen KMS-Schlüssel. Die Angabe des ARN für einen AWS KMS Schlüssel gibt an AWS Snowball Edge, welcher AWS KMS keys zum Verschlüsseln der eindeutigen Schlüssel auf dem AWS Snowball Edge Gerät verwendet werden soll. Weitere Informationen zu den AWS Snowball Edge unterstützten Amazon S3 server-side-encryption S3-Optionen finden Sie unter [Serverseitige Verschlüsselung in AWS Snowball Edge](#).

Den verwalteten Kunden AWS KMS keys für Snowball Edge verwenden

Wenn Sie den verwalteten Kunden AWS KMS keys für Snowball Edge Edge verwenden möchten, der für Ihr Konto erstellt wurde, gehen Sie wie folgt vor.

Um den AWS KMS keys für Ihren Job auszuwählen

1. Wählen Sie auf der die Managementkonsole für die AWS Snow-Familie Option Job erstellen aus.
2. Wählen Sie Ihren Auftragsstyp aus und klicken Sie dann auf Next (Weiter).

3. Geben Sie Ihre Versanddetails an und klicken Sie dann auf Next (Weiter).
4. Geben Sie Ihre Auftragsdetails an und klicken Sie auf Next (Weiter).
5. Legen Sie Ihre Sicherheitsoptionen fest. Wählen Sie unter Verschlüsselung für KMS-Schlüssel entweder den Von AWS verwalteter Schlüssel oder einen benutzerdefinierten Schlüssel aus, der zuvor in erstellt wurde AWS KMS, oder wählen Sie Enter a key ARN, wenn Sie einen Schlüssel eingeben müssen, der einem separaten Konto gehört.

 Note

Die AWS KMS key ARN ist eine weltweit eindeutige Kennung für vom Kunden verwaltete Schlüssel.

6. Wählen Sie Weiter, um die Auswahl Ihres abzuschließen AWS KMS key.
7. Gewähren Sie dem IAM-Benutzer des Snow-Geräts Zugriff auf den KMS-Schlüssel.
 - a. Gehen Sie in der IAM-Konsole (<https://console.aws.amazon.com/iam/>) zu Encryption Keys und öffnen Sie den KMS-Schlüssel, mit dem Sie die Daten auf dem Gerät verschlüsseln möchten.
 - b. Wählen Sie unter Schlüsselbenutzer die Option Hinzufügen aus, suchen Sie nach dem IAM-Benutzer des Snow-Geräts und wählen Sie Anhängen aus.

Erstellen eines benutzerdefinierten KMS-Envelope-Verschlüsselungsschlüssels

Sie haben die Möglichkeit, Ihren eigenen benutzerdefinierten AWS KMS Envelope-Verschlüsselungsschlüssel mit AWS Snowball Edge zu verwenden. Wenn Sie Ihren eigenen Schlüssel erstellen, muss dieser in derselben Region wie Ihr Auftrag erstellt werden.

Informationen zum Erstellen eines eigenen AWS KMS Schlüssels für einen Job finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Schützen von Daten auf Ihrem Gerät

Sicherung Ihres AWS Snowball Edge

Im Folgenden finden Sie einige Sicherheitspunkte, die Sie bei der Verwendung berücksichtigen sollten AWS Snowball Edge, sowie einige allgemeine Informationen zu anderen Sicherheitsvorkehrungen, die wir treffen, wenn ein Gerät AWS zur Verarbeitung ankommt.

Wir empfehlen die folgenden Sicherheitsansätze:

- Nachdem Sie das Gerät erhalten haben, sollten Sie nach Beschädigungen und offensichtlichen Manipulationen suchen. Wenn Ihnen am Gerät irgendetwas Verdächtiges auffällt, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie sich stattdessen an den [AWS Support](#), um ein neues Gerät zu erhalten.
- Vermeiden Sie es möglichst, die Anmeldeinformationen für Ihren Auftrag offenzulegen. Jede Person mit Zugang zum Auftragsmanifest und zum Entsperrcode kann auf die Inhalte des Geräts für diesen Auftrag zugreifen.
- Lassen Sie das Gerät nicht auf einer Laderampe liegen. Auf einer Ladestation kann sie den Elementen ausgesetzt sein. Obwohl jedes AWS Snowball Edge Gerät robust ist, kann Wetter die robusteste Hardware beschädigen. Melden Sie gestohlene, vermisste oder defekte Geräte so schnell wie möglich. Je schneller ein Problem mit einer Appliance gemeldet wird, umso zügiger kann ein Ersatz versendet werden, um Ihren Auftrag abzuschließen.

 Note

Die AWS Snowball Edge Geräte sind Eigentum von. AWS Die Manipulation eines Geräts stellt einen Verstoß gegen die AWS Nutzungsbedingungen dar. Weitere Informationen finden Sie unter <http://aws.amazon.com/aup/>.

Wir führen die folgenden Sicherheitsschritte durch:

- Bei der Übertragung von Daten mit dem Amazon S3 S3-Adapter werden Objektmetadaten nicht dauerhaft gespeichert. Nur die Metadaten von `filename` und `filesize` bleiben unverändert. Alle anderen Metadaten werden entsprechend des folgenden Beispiels festgelegt: `-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]`
- Bei der Übertragung von Daten mit der NFS-Schnittstelle werden Objektmetadaten beibehalten.
- Wenn ein Gerät bei uns ankommt AWS, überprüfen wir es auf Anzeichen von Manipulation und stellen sicher, dass das Trusted Platform Module (TPM) keine Änderungen festgestellt hat. AWS Snowball Edge verwendet mehrere Sicherheitsebenen zum Schutz Ihrer Daten, darunter manipulationssichere Gehäuse, 256-Bit-Verschlüsselung und ein branchenübliches TPM, das sowohl Sicherheit als auch eine vollständige Aufbewahrungskette für Ihre Daten bietet.

- Sobald der Datenübertragungsauftrag verarbeitet und verifiziert wurde, wird eine AWS Softwarelöschung des Snowball-Geräts durchgeführt, die den Richtlinien des National Institute of Standards and Technology (NIST) zur Medienbereinigung entspricht.

Validieren von NFC-Tags

Snowball Edge Compute Optimized- und Snowball Edge Storage Optimized (für Datenübertragung) Geräte verfügen über integrierte NFC-Tags. Sie können diese Tags mit der AWS Snowball Edge Verifizierungs-App scannen, die auf Android verfügbar ist. Durch Scannen und Validieren dieser NFC-Tags können Sie überprüfen, dass Ihr Gerät nicht unbefugt geändert wurde, bevor Sie es verwenden.

Die Validierung von NFC-Tags umfasst die Verwendung des Snowball Edge-Clients zur Generierung eines gerätespezifischen QR-Codes, um zu überprüfen, ob die Tags, die Sie scannen, für das richtige Gerät sind.

Das folgende Verfahren beschreibt, wie Sie die NFC-Tags auf einem Snowball Edge-Gerät validieren. Stellen Sie vor Beginn sicher, dass Sie die folgenden ersten fünf Schritte der Übung "Erste Schritte" ausgeführt haben:

1. Erstellen Sie Ihren Snowball Edge-Job. Weitere Informationen finden Sie unter [Einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen](#)
2. Eingang des Geräts Weitere Informationen finden Sie unter [Erhalt des Snowball Edge](#).
3. Herstellen einer Verbindung mit dem lokalen Netzwerk Weitere Informationen finden Sie unter [Einen Snowball Edge mit Ihrem lokalen Netzwerk verbinden](#).
4. Abrufen von Anmeldeinformationen und Tools Weitere Informationen finden Sie unter [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#).
5. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Den Snowball Edge-Client herunterladen und installieren](#).

Um die NFC-Tags zu validieren

1. Führen Sie den `snowballEdge get-app-qr-code` Snowball Edge-Client-Befehl aus. Wenn Sie diesen Befehl für einen Knoten in einem Cluster ausführen, geben Sie die Seriennummer (`--device-sn`) an, um einen QR-Code für einen einzelnen Knoten zu erhalten. Wiederholen Sie diesen Schritt für jeden Knoten im Cluster. Weitere Informationen zur Verwendung dieses Befehls finden Sie unter [Einen QR-Code zur Validierung von Snowball Edge NFC-Tags erhalten](#).

Der QR-Code wird an einem Speicherort Ihrer Wahl als PNG-Datei gespeichert.

2. Navigieren Sie zu der von Ihnen gespeicherten PNG-Datei und öffnen Sie sie, sodass Sie den QR-Code mit der App scannen können.
3. Sie können diese Tags mit der AWS Snowball Edge Bestätigungs-App auf Android scannen.

 Note

Die AWS Snowball Edge Bestätigungs-App kann nicht heruntergeladen werden. Wenn Sie jedoch ein Gerät haben, auf dem die App bereits installiert ist, können Sie die App verwenden.

4. Starten Sie die App und befolgen Sie die Anweisungen auf dem Bildschirm.

Sie haben die NFC-Tags für Ihr Gerät jetzt erfolgreich gescannt und validiert.

Wenn beim Scannen Probleme auftreten, führen Sie die folgenden Schritte aus:

- Vergewissern Sie sich, dass Ihr Gerät über die für die Snowball Edge Compute Optimized Edge-Optionen verfügt.
- Wenn Sie die App auf einem anderen Gerät haben, versuchen Sie, dieses Gerät zu verwenden.
- Bringen Sie das Gerät in einen isolierten Bereich des Raums, fern von Störungen durch andere NFC-Tags, und versuchen Sie es erneut.
- Wenn die Probleme weiterhin bestehen, wenden Sie sich an [AWS Support](#).

Identity and Access Management in AWS Snowball Edge

Jeder AWS Snowball Edge Job muss authentifiziert werden. Dazu erstellen und verwalten Sie die IAM-Benutzer in Ihrem Konto. Mithilfe von IAM können Sie Benutzer und Berechtigungen in erstellen und verwalten. AWS

AWS Snowball Edge Benutzer müssen über bestimmte IAM-bezogene Berechtigungen verfügen, um auf die zugreifen zu können, um Jobs AWS Snowball Edge AWS-Managementkonsole zu erstellen. Ein IAM-Benutzer, der einen Import- oder Exportauftrag erstellt, muss auch Zugriff auf die richtigen Amazon Simple Storage Service (Amazon S3) -Ressourcen haben, z. B. die Amazon S3-Buckets, die für den Job verwendet werden sollen, AWS KMS Ressourcen, Amazon SNS SNS-Thema und EC2 Amazon-kompatibles AMI für Edge-Compute-Jobs.

 Important

Informationen zur lokalen Verwendung von IAM auf Ihrem Gerät finden Sie unter. [Lokales Verwenden von IAM auf einem Snowball Edge](#)

Themen

- [Zugriffskontrolle für Snowball Edge Console und Erstellen von Jobs](#)

Zugriffskontrolle für Snowball Edge Console und Erstellen von Jobs

Wie bei allen AWS Diensten AWS Snowball Edge erfordert der Zugriff auf Anmeldeinformationen, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen wie einen Amazon S3 S3-Bucket oder eine AWS Lambda Funktion verfügen. AWS Snowball Edge unterscheidet sich in zweierlei Hinsicht:

1. Jobs in haben AWS Snowball Edge keine Amazon-Ressourcennamen (ARNs).
2. Die Steuerung des physischen Zugangs und des Netzwerkzugriffs eines Geräts bei Ihnen vor Ort liegt in Ihrer Verantwortung.

[Identity and Access Management für AWS Snowball Edge](#) Einzelheiten dazu, wie Sie [AWS Identity and Access Management \(IAM\) verwenden und](#) wie Sie Ihre Ressourcen schützen können AWS Snowball Edge , indem Sie kontrollieren, wer darauf zugreifen kann, finden Sie in den Empfehlungen sowie in den AWS Cloud Empfehlungen zur lokalen Zugriffskontrolle.

Identity and Access Management für AWS Snowball Edge

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Snow Family IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)

- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Snow Family funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)
- [Problembehandlung bei AWS Snowball Edge Identität und Zugriff](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Snow Family

Dienstbenutzer — Wenn Sie den AWS Snow Family Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Snow Family Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter [Problembehandlung bei AWS Snowball Edge Identität und Zugriff](#) finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Snow Family haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Snow Family Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Snow Family. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Snow Family Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Snow Family, finden Sie unter [Wie AWS Snow Family funktioniert mit IAM](#).

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Snow Family verfassen können. Beispiele für AWS Snow Family identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS-Managementkonsole oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto](#) im AWS-Anmeldungsbenutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, stellt AWS ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter [AWS Signature Version 4 für API-Anforderungen](#) im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center -Benutzerhandbuch und [AWS Multi-Faktor-Authentifizierung \(MFA\) in IAM](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen

bereit. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb von Ihrem AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS-Managementkonsole, können Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Methoden für die Übernahme einer Rolle](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.
- **Serviceübergreifender Zugriff** — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle** – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, 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.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon ausgeführte Anwendungen EC2** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden](#).

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten

Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. 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.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS-Managementkonsole AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. 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.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter [Auswählen zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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 Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in

einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.

- **Ressourcenkontrollrichtlinien (RCPs)** — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) im AWS Organizations Benutzerhandbuch.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie AWS Snow Family funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS Snow Family, mit welchen IAM-Funktionen Sie arbeiten können. AWS Snow Family

IAM-Funktionen, die Sie mit verwenden können AWS Snow Family

IAM-Feature	AWS Snow Family Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS Snow Family und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für AWS Snow Family

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. 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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Snow Family

Beispiele für AWS Snow Family identitätsbasierte Richtlinien finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)

Ressourcenbasierte Richtlinien finden Sie in AWS Snow Family

Unterstützt ressourcenbasierte Richtlinien: Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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 Prinzipalen 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. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Snow Family

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. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Snow Family Aktionen finden Sie unter [Aktionen definiert von AWS Snow Family](#) in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Snow Family verwendet:

```
snowball
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
    "snowball:action1",  
    "snowball:action2"  
]
```

Beispiele für AWS Snow Family identitätsbasierte Richtlinien finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)

Politische Ressourcen für AWS Snow Family

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. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*" 
```

Eine Liste der AWS Snow Family Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter [Resources defined by AWS Snow Family](#) in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von AWS Snow Family definierte Aktionen](#).

Beispiele für AWS Snow Family identitätsbasierte Richtlinien finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)

Bedingungsschlüssel für Richtlinien für AWS Snow Family

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der AWS Snow Family Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS Snow Family](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS Snow Family](#).

Beispiele für AWS Snow Family identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge](#)

ACLs in AWS Snow Family

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Snow Family

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 AWS Snow Family

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS-Managementkonsole Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln von einer Benutzerrolle zu einer IAM-Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen weiterleiten für AWS Snow Family

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren

Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für AWS Snow Family

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

Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Snow Family Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Snow Family wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Snow Family

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst 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 in der Tabelle nach einem Service mit einem Yes in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Snowball Edge

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Snow Family -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 \(Konsole\)](#) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Snow Family, einschließlich des Formats von ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snow Family](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der AWS Snow Family -Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Snow Family Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu 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 [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) 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 für einen bestimmten Zweck 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 [Richtlinienvvalidierung mit IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert 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 [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der AWS Snow Family -Konsole

Um auf die AWS Snow Family Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Snow Family Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. 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 API 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 AWS Snow Family Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Snow Family *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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```



```
}
```

Problembehandlung bei AWS Snowball Edge Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Snow Family und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Snow Family](#)
- [Ich bin nicht berechtigt, iam durchzuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Snow Family Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Snow Family

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `snowball:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
snowball:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `snowball:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Snow Family übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte 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 AWS Snow Family 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 Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Snow Family Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Snow Family unterstützt werden, finden Sie unter [Wie AWS Snow Family funktioniert mit IAM](#)
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- 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.

Zugriffskontrolle im AWS Cloud

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen zu authentifizieren. AWS Ohne die erforderlichen Berechtigungen können Sie jedoch keine AWS Ressourcen erstellen oder darauf zugreifen. Beispielsweise müssen Sie über die erforderlichen Berechtigungen verfügen, um einen Auftrag zu erstellen, um ein Snowball Edge-Gerät zu bestellen.

In den folgenden Abschnitten wird die Verwaltung von cloudbasierten Berechtigungen für AWS Snowball Edge beschrieben. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Ressourcen im AWS Cloud](#)
- [Verwenden identitätsbasierter Richtlinien \(IAM-Richtlinien\) für AWS Snowball Edge](#)

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Ressourcen im AWS Cloud

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf eine Ressource werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuordnen, und einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

Note

Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter [Bewährte Methoden für IAM](#) im IAM-Benutzerhandbuch.

Themen

- [Ressourcen und Operationen](#)
- [Grundlegendes zum Eigentum an Ressourcen](#)

- [Verwaltung des Zugriffs auf Ressourcen in AWS Cloud](#)
- [Festlegen der Richtlinienelemente: Aktionen, Effekte und Prinzipale](#)
- [Angaben von Bedingungen in einer Richtlinie](#)

Ressourcen und Operationen

In ist AWS Snowball Edge die primäre Ressource ein Job. AWS Snowball Edge hat auch Geräte wie den Snowball und das AWS Snowball Edge Gerät, Sie können diese Geräte jedoch nur im Kontext eines vorhandenen Jobs verwenden. Amazon S3-Buckets und Lambda-Funktionen sind Ressourcen von Amazon S3 bzw. Lambda.

Wie bereits erwähnt, sind Jobs nicht mit Amazon Resource Names (ARNs) verknüpft. Den Ressourcen anderer Dienste, wie z. B. Amazon S3 S3-Buckets, ist jedoch unique (ARNs) zugeordnet, wie in der folgenden Tabelle dargestellt.

AWS Snowball Edge bietet eine Reihe von Vorgängen zum Erstellen und Verwalten von Aufträgen. Eine Liste der verfügbaren Operationen finden Sie in der [AWS Snowball Edge API-Referenz](#).

Grundlegendes zum Eigentum an Ressourcen

Der AWS-Konto besitzt die Ressourcen, die im Konto erstellt wurden, unabhängig davon, wer die Ressourcen erstellt hat. Insbesondere ist der Ressourcenbesitzer derjenige AWS-Konto der [Prinzipalität](#) (d. h. das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), die die Anfrage zur Ressourcenerstellung authentifiziert. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie Ihre Root-Kontoanmeldeinformationen verwenden, AWS-Konto um einen S3-Bucket zu erstellen, AWS-Konto sind Sie der Eigentümer der Ressource (in AWS Snowball Edge, die Ressource ist der Job).
- Wenn Sie in Ihrem einen IAM-Benutzer erstellen AWS-Konto und diesem Benutzer Berechtigungen zum Erstellen eines Auftrags zur Bestellung eines Snowball Edge-Geräts erteilen, kann der Benutzer einen Auftrag zur Bestellung eines Snowball Edge-Geräts erstellen. Ihre AWS-Konto, zu der der Benutzer gehört, besitzt jedoch die Jobressource.
- Wenn Sie eine IAM-Rolle in Ihrem AWS-Konto mit den Berechtigungen zum Erstellen eines Jobs erstellen, kann jeder, der die Rolle übernehmen kann, einen Job erstellen, um ein Snowball Edge-Gerät zu bestellen. Ihre AWS-Konto, zu der die Rolle gehört, besitzt die Jobressource.

Verwaltung des Zugriffs auf Ressourcen in AWS Cloud

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

Note

In diesem Abschnitt wird die Verwendung von IAM im Kontext von AWS Snowball Edge beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter [Was ist IAM?](#) im IAM-Benutzerhandbuch. Für Informationen über die Syntax und Beschreibungen von [AWS -IAM-Richtlinien](#) lesen Sie die IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die mit einer IAM-Identität verknüpft sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, und Richtlinien, die einer Ressource zugeordnet sind, werden als ressourcenbasierte Richtlinien bezeichnet. AWS Snowball Edge unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- [Ressourcenbasierte Richtlinien](#)

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon-S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Sie können beispielsweise eine Richtlinie an einen S3-Bucket anhängen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. AWS Snowball Edge unterstützt keine ressourcenbasierten Richtlinien.

Festlegen der Richtlinienelemente: Aktionen, Effekte und Prinzipale

Für jeden Job (siehe [Ressourcen und Operationen](#)) definiert der Service eine Reihe von API-Operationen (siehe [AWS Snowball Edge API-Referenz](#)), um den Job zu erstellen und zu verwalten. AWS Snowball Edge Definiert eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können, um Berechtigungen für diese API-Operationen zu erteilen. Beispielsweise werden für einen Auftrag die folgenden Aktionen definiert: `CreateJob`, `CancelJob` und `DescribeJob`. Zur Durchführung einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- **Ressource** – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Weitere Informationen finden Sie unter [Ressourcen und Operationen](#).

 Note

Dies wird für Amazon S3, Amazon EC2, AWS Lambda und viele andere Dienste unterstützt. AWS KMS

Snowball unterstützt nicht die Angabe eines Ressourcen-ARN im Resource Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Snowball zu ermöglichen, geben Sie dies "Resource": "*" in Ihrer Richtlinie an.

- **Aktion** – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Abhängig vom angegebenen Effect gestattet oder verweigert snowball:* den Benutzerberechtigungen z. B. die Durchführung von Operationen.

 Note

Dies wird für Amazon EC2, Amazon S3 und IAM unterstützt.

- **Auswirkung** – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.

 Note

Dies wird für Amazon EC2, Amazon S3 und IAM unterstützt.

- **Prinzipal** – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. Bei ressourcenbasierten Richtlinien geben Sie den Benutzer, das Konto, den Dienst oder die andere Entität an, für die Sie Berechtigungen erhalten möchten (gilt nur für ressourcenbasierte Richtlinien). AWS Snowball Edge unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der [AWS -IAM-Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

Eine Tabelle mit allen AWS Snowball Edge API-Aktionen finden Sie unter. [AWS Snowball Edge API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#)

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema [Bedingung](#) im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für AWS Snowball Edge gibt es keine speziellen Bedingungsschlüssel. Es gibt jedoch Bedingungsschlüssel für AWS alle Bereiche, die Sie je nach Bedarf verwenden können. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter [Verfügbare Schlüssel für Bedingungen](#) im IAM-Benutzerhandbuch.

Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Snowball Edge

Dieses Thema enthält Beispiele für identitätsbasierte Richtlinien, die zeigen, wie ein Kontoadministrator Berechtigungsrichtlinien an IAM-Identitäten (d. h. Benutzer, Gruppen und Rollen) anhängen kann. Diese Richtlinien gewähren somit Berechtigungen zur Ausführung von Vorgängen mit Ressourcen in der AWS Snowball Edge . AWS Cloud

Important

Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die Grundkonzepte und für Sie verfügbaren Optionen zum Verwalten des Zugriffs auf Ihre AWS Snowball Edge -Ressourcen erläutert werden. Weitere Informationen finden Sie unter [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Ressourcen im AWS Cloud](#).

Dieses Thema besteht aus folgenden Abschnitten:

- [Für die Verwendung der AWS Snowball Edge Konsole sind Berechtigungen erforderlich](#)
- [AWS-Verwaltete \(vordefinierte\) Richtlinien für AWS Snowball Edge](#)
- [Beispiele für vom Kunden verwaltete Richtlinien](#)

Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "snowball:*",
        "importexport:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Die Richtlinie enthält zwei Anweisungen:

- Die erste Anweisung erteilt Berechtigungen für drei Amazon S3 S3-Aktionen (s3:GetBucketLocations3:GetObject, unds3:ListBucket) für alle Amazon S3 S3-Buckets unter Verwendung des Amazon-Ressourcennamens (ARN) vonarn:aws:s3:::*. Der ARN gibt ein Platzhalterzeichen (*) an, sodass der Benutzer einen oder alle Amazon S3 S3-Buckets auswählen kann, aus denen Daten exportiert werden sollen.
- Die zweite Anweisung gewährt Berechtigungen für alle AWS Snowball Edge Aktionen. Da diese Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, sind in der Richtlinie sowie im Wert von Resource Platzhalterzeichen (*) angegeben.

Das Element `Principal` ist in der Richtlinie nicht angegeben, da in identitätsbasierten Richtlinien die Angabe des Prinzipals als Empfänger der Berechtigung nicht erforderlich ist. Wenn Sie einem Benutzer eine Richtlinie anfügen, ist der Benutzer automatisch der Prinzipal. Wird die Berechtigungsrichtlinie einer IAM-Rolle angefügt, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen.

Eine Tabelle mit allen API-Aktionen für die AWS Snowball Edge Auftragsverwaltung und den Ressourcen, für die sie gelten, finden Sie unter [AWS Snowball Edge API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

Für die Verwendung der AWS Snowball Edge Konsole sind Berechtigungen erforderlich

In der Referenztabelle für Berechtigungen sind die API-Operationen für die AWS Snowball Edge Auftragsverwaltung aufgeführt und die erforderlichen Berechtigungen für jeden Vorgang aufgeführt. Weitere Informationen zu API-Operationen zur Auftragsverwaltung finden Sie im Thema [AWS Snowball Edge API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

Um den verwenden zu können Managementkonsole für die AWS Snow-Familie, müssen Sie Berechtigungen für zusätzliche Aktionen erteilen, wie in der folgenden Berechtigungsrichtlinie beschrieben:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
```

```

        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
    ],
    "Resource": "arn:aws:lambda:*::function:*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:ListFunctions"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:RetireGrant",
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",

```

```

        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/snowball*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "importexport.amazonaws.com"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "sns:CreateTopic",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",

```

```

        "Action": [
            "greengrass:getServiceRoleForAccount"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "snowball:*"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",

```

```

        "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
    ],
    "Resource": "arn:aws:lambda::function:*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:ListFunctions"
    ],
    "Resource": "arn:aws:lambda::*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/snowball*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "importexport.amazonaws.com"
        }
    }
},
{

```

```

        "Effect": "Allow",
        "Action": [
            "ec2:DescribeImages",
            "ec2:ModifyImageAttribute"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "sns:CreateTopic",
            "sns:ListTopics",
            "sns:GetTopicAttributes",
            "sns:SetTopicAttributes",
            "sns:ListSubscriptionsByTopic",
            "sns:Subscribe"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "greengrass:getServiceRoleForAccount"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "snowball:*"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

Die AWS Snowball Edge Konsole benötigt diese zusätzlichen Berechtigungen aus den folgenden Gründen:

- **ec2**:— Diese ermöglichen es dem Benutzer, EC2 Amazon-kompatible Instances zu beschreiben und ihre Attribute für lokale Rechenzwecke zu ändern. Weitere Informationen finden Sie unter [Verwenden von EC2 Amazon-kompatiblen Compute-Instances auf Snowball Edge](#).
- **kms**:— Diese ermöglichen es dem Benutzer, den KMS-Schlüssel zu erstellen oder auszuwählen, mit dem Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie unter [AWS Key Management Service in AWS Snowball Edge](#).
- **iam**:— Diese ermöglichen es dem Benutzer, einen ARN für eine IAM-Rolle zu erstellen oder auszuwählen, AWS Snowball Edge der davon ausgeht, auf die AWS Ressourcen zuzugreifen, die mit der Auftragserstellung und -verarbeitung verbunden sind.
- **sns**:— Diese ermöglichen es dem Benutzer, die Amazon SNS SNS-Benachrichtigungen für die von ihm erstellten Jobs zu erstellen oder auszuwählen. Weitere Informationen finden Sie unter [Benachrichtigungen für Snowball Edge](#).

AWS-Verwaltete (vordefinierte) Richtlinien für AWS Snowball Edge

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet werden. AWS Die verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter [AWS - verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

Sie können die folgenden AWS verwalteten Richtlinien mit verwenden. AWS Snowball Edge

Erstellen einer IAM-Rollenrichtlinie für Snowball Edge Edge

Es muss eine IAM-Rollenrichtlinie mit Lese- und Schreibberechtigungen für Ihre Amazon S3 S3-Buckets erstellt werden. Die IAM-Rolle muss auch eine Vertrauensbeziehung mit Snowball Edge haben. Eine Vertrauensbeziehung bedeutet, dass AWS Sie die Daten in den Snowball und in Ihre Amazon S3 S3-Buckets schreiben können, je nachdem, ob Sie Daten importieren oder exportieren.

Wenn Sie einen Auftrag erstellen, um ein Snowball Edge-Gerät in der zu bestellen Managementkonsole für die AWS Snow-Familie, erfolgt die Erstellung der erforderlichen IAM-Rolle in Schritt 4 im Abschnitt Permission. Dieser Prozess erfolgt automatisch. Die IAM-Rolle, die Sie Snowball Edge übernehmen lassen, wird nur verwendet, um Ihre Daten in Ihren Bucket zu

schreiben, wenn der Snowball mit Ihren übertragenen Daten eintrifft. AWS Der Vorgang wird wie folgt ausgeführt.

Um die IAM-Rolle für Ihr i zu erstellen

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die AWS Snowball Edge Konsole unter <https://console.aws.amazon.com/importexport/>.
2. Wählen Sie Job erstellen aus.
3. Geben Sie im ersten Schritt die Details für Ihren Importauftrag in Amazon S3 ein und wählen Sie dann Weiter.
4. Im zweiten Schritt wählen Sie unter Permission (Berechtigung) die Option Create/Select IAM Role (IAM-Rolle erstellen/auswählen) aus.

Die IAM-Managementkonsole wird geöffnet und zeigt die IAM-Rolle an, mit der Objekte in Ihre angegebenen Amazon S3 S3-Buckets kopiert werden. AWS

5. Überprüfen Sie die Angaben auf dieser Seite und wählen Sie dann Allow (Zulassen) aus.

Sie kehren zu dem zurück Managementkonsole für die AWS Snow-Familie, wo der ARN der ausgewählten IAM-Rolle den Amazon-Ressourcennamen (ARN) für die IAM-Rolle enthält, die Sie gerade erstellt haben.

6. Wählen Sie Weiter, um die Erstellung Ihrer IAM-Rolle abzuschließen.

Das vorherige Verfahren erstellt eine IAM-Rolle mit Schreibberechtigungen für die Amazon S3 S3-Buckets, in die Sie Ihre Daten importieren möchten. Die erstellte IAM-Rolle weist eine der folgenden Strukturen auf, je nachdem, ob sie für einen Import- oder einen Exportauftrag gilt.

IAM-Rolle für einen Importauftrag

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
```



```

        "s3:ListBucketMultipartUploads"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketPolicy",
      "s3:PutObject",
      "s3:AbortMultipartUpload",
      "s3:ListMultipartUploadParts",
      "s3:PutObjectAcl",
      "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
}

```

Wenn Sie serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln (SSE-KMS) verwenden, um die Amazon S3 S3-Buckets zu verschlüsseln, die Ihrem Importauftrag zugeordnet sind, müssen Sie Ihrer IAM-Rolle auch die folgende Anweisung hinzufügen.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}

```

Wenn die Objektgrößen größer sind, verwendet der Amazon S3 S3-Client, der für den Importvorgang verwendet wird, den mehrteiligen Upload. Wenn Sie einen mehrteiligen Upload mit SSE-KMS initiieren, werden alle hochgeladenen Teile mit dem angegebenen Schlüssel verschlüsselt. AWS KMS Da die Teile verschlüsselt sind, müssen sie zuerst entschlüsselt werden, bevor sie zur Vervollständigung des mehrteiligen Uploads zusammengesetzt werden können. Sie benötigen also die Erlaubnis, den AWS KMS Schlüssel (kms:Decrypt) zu entschlüsseln, wenn Sie einen mehrteiligen Upload zu Amazon S3 mit SSE-KMS ausführen.

Im Folgenden finden Sie ein Beispiel für eine IAM-Rolle, die für einen Importauftrag benötigt wird, für den die Berechtigung `kms:Decrypt` erforderlich ist.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey", "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Im Folgenden finden Sie ein Beispiel für eine IAM-Rolle, die für einen Exportauftrag benötigt wird.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Wenn Sie serverseitige Verschlüsselung mit AWS KMS—managed keys verwenden, um die Amazon S3 S3-Buckets zu verschlüsseln, die Ihrem Exportauftrag zugeordnet sind, müssen Sie Ihrer IAM-Rolle auch die folgende Anweisung hinzufügen.

```
{
  "Effect": "Allow",
```

```
"Action": [
    "kms:Decrypt"
],
"Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Sie können Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für API-Operationen für die Auftragsverwaltung zu gewähren. AWS Snowball Edge Die benutzerdefinierten Richtlinien können Sie dann den IAM-Benutzern oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispielbenutzerrichtlinien, die Berechtigungen für verschiedene AWS Snowball Edge Job-Management-Aktionen gewähren. Diese Richtlinien funktionieren, wenn Sie AWS SDKs oder die verwenden AWS CLI. Bei Verwendung der Konsole müssen Sie zusätzliche konsolenspezifische Berechtigungen erteilen, die im Abschnitt [Für die Verwendung der AWS Snowball Edge Konsole sind Berechtigungen erforderlich](#) erläutert werden.

Note

Alle Beispiele verwenden die Region US-West-2 und enthalten ein fiktives Konto. IDs

Beispiele

- [Beispiel 1: Rollenrichtlinie, die es einem Benutzer ermöglicht, einen Job zu erstellen, um ein Snowball Edge-Gerät mit der API zu bestellen](#)
- [Beispiel 2: Rollenrichtlinie zum Erstellen von Importaufträgen](#)
- [Beispiel 3: Rollenrichtlinie zum Erstellen von Exportaufträgen](#)
- [Beispiel 4: Erwartete Rollenberechtigungen und Vertrauensrichtlinie](#)
- [AWS Snowball Edge API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#)

Beispiel 1: Rollenrichtlinie, die es einem Benutzer ermöglicht, einen Job zu erstellen, um ein Snowball Edge-Gerät mit der API zu bestellen

Die folgende Berechtigungsrichtlinie ist eine notwendige Komponente für alle Richtlinien, die Berechtigungen zur Auftrags- oder Clustererstellung über die Auftragsverwaltungs-API erteilen. Die Erklärung wird als Grundsatzerklärung zur Vertrauensbeziehung für die Snowball IAM-Rolle benötigt.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "importexport.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Beispiel 2: Rollenrichtlinie zum Erstellen von Importaufträgen

Sie verwenden die folgende Rollenvertrauensrichtlinie, um Importaufträge für Snowball Edge zu erstellen, die AWS Lambda AWS IoT Greengrass Power-By-Funktionen verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucketMultipartUploads"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketPolicy",
      "s3:GetBucketLocation",
      "s3:ListBucketMultipartUploads",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:AbortMultipartUpload",
      "s3:ListMultipartUploadParts",
      "s3:PutObjectAcl",
      "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "snowball:*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iot:AttachPrincipalPolicy",
      "iot:AttachThingPrincipal",
      "iot:CreateKeysAndCertificate",
      "iot:CreatePolicy",
      "iot:CreateThing",
      "iot:DescribeEndpoint",
      "iot:GetPolicy"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",

```

```

        "Action": [
            "lambda:GetFunction"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "greengrass:CreateCoreDefinition",
            "greengrass:CreateDeployment",
            "greengrass:CreateDeviceDefinition",
            "greengrass:CreateFunctionDefinition",
            "greengrass:CreateGroup",
            "greengrass:CreateGroupVersion",
            "greengrass:CreateLoggerDefinition",
            "greengrass:CreateSubscriptionDefinition",
            "greengrass:GetDeploymentStatus",
            "greengrass:UpdateGroupCertificateConfiguration",
            "greengrass:CreateGroupCertificateAuthority",
            "greengrass:GetGroupCertificateAuthority",
            "greengrass:ListGroupCertificateAuthorities",
            "greengrass:ListDeployments",
            "greengrass:GetGroup",
            "greengrass:GetGroupVersion",
            "greengrass:GetCoreDefinitionVersion"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

Beispiel 3: Rollenrichtlinie zum Erstellen von Exportaufträgen

Sie verwenden die folgende Rollenvertrauensrichtlinie, um Exportaufträge für Snowball Edge zu erstellen, die AWS Lambda AWS IoT Greengrass Power-By-Funktionen verwenden.

JSON

```

    {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "snowball:*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iot:AttachPrincipalPolicy",
      "iot:AttachThingPrincipal",
      "iot:CreateKeysAndCertificate",
      "iot:CreatePolicy",
      "iot:CreateThing",
      "iot:DescribeEndpoint",
      "iot:GetPolicy"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:GetFunction"

```

```

    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateDeployment",
        "greengrass:CreateDeviceDefinition",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:GetDeploymentStatus",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListDeployments",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Beispiel 4: Erwartete Rollenberechtigungen und Vertrauensrichtlinie

Die folgende Richtlinie für erwartete Rollenberechtigungen ist für die Verwendung einer vorhandenen Servicerolle erforderlich. Es ist eine einmalige Einrichtung.

JSON

```
{
```



```

"Version": "2012-10-17",
"Statement":
[
  {
    "Effect": "Allow",
    "Action": "sns:Publish",
    "Resource": ["[[snsArn]]"]
  },
  {
    "Effect": "Allow",
    "Action":
    [
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricData",
      "cloudwatch:PutMetricData"
    ],
    "Resource":
    [
      "*"
    ],
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/SnowFamily"
      }
    }
  }
]
}

```

Die folgende Richtlinie für das Vertrauen in Rollen ist für die Verwendung einer vorhandenen Servicerolle erforderlich. Es handelt sich um eine einmalige Einrichtung.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "importexport.amazonaws.com"
      }
    }
  ]
}

```

```
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

AWS Snowball Edge API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Wenn Sie die [Zugriffskontrolle im AWS Cloud](#) einrichten und eine Berechtigungsrichtlinie für eine IAM-Identität (identitätsbasierte Richtlinie) verfassen, können Sie die folgende Liste als Referenz verwenden. Die enthält jeden API-Vorgang für die AWS Snowball Edge Auftragsverwaltung und die entsprechenden Aktionen, für die Sie Berechtigungen zur Ausführung der Aktion erteilen können. Sie enthält auch für jeden API-Vorgang die AWS Ressource, für die Sie die Berechtigungen erteilen können. Die Aktionen geben Sie im Feld `Action` und den Wert für die Ressource im Feld `Resource` der Richtlinie an.

Sie können in Ihren AWS Snowball Edge Richtlinien AWS allgemeine Bedingungsschlüssel verwenden, um Bedingungen auszudrücken. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter [Verfügbare Schlüssel](#) im IAM-Benutzerhandbuch.

Note

Um eine Aktion anzugeben, verwenden Sie das Präfix `snowball:` gefolgt vom Namen der API-Operation (z. B. `snowball:CreateJob`).

Protokollierung und Überwachung in AWS Snowball Edge

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS Snowball Edge und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet verschiedene Tools zur Überwachung Ihrer AWS Snowball Edge Ressourcen und zur Reaktion auf potenzielle Vorfälle:

AWS CloudTrail Logs

CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in der AWS Snowball Edge Job Management API oder bei der Verwendung der AWS Konsole ausgeführt wurden. Anhand der von gesammelten Informationen können Sie die API-

Anfrage CloudTrail, die an den AWS Snowball Edge Service 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 [AWS Snowball Edge API-Aufrufe protokollieren mit AWS CloudTrail](#).

Konformitätsüberprüfung für AWS Snowball Edge

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt](#), finden Sie unter [Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Compliance und Governance im Bereich Sicherheit](#) – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- [Referenz für berechnete HIPAA-Services](#) – Listet berechnete HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- [AWS Security Hub CSPM](#)— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS - Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerelementreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch 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.

Sicherheit der Infrastruktur in AWS Snowball Edge

Als verwalteter Dienst AWS Snow Family ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Snow Family über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS -Security-Token-Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Validierung der mit Snowball Edge-Geräten übertragenen Daten

Im Folgenden finden Sie Informationen darüber, wie Datenübertragungen AWS Snowball Edge validiert werden und welche manuellen Schritte Sie ergreifen können, um die Datenintegrität während und nach einem Auftrag sicherzustellen.

Wenn Sie eine Datei aus einer lokalen Datenquelle mithilfe der Amazon S3 S3-Schnittstelle auf Snowball Edge kopieren, werden eine Reihe von Prüfsummen erstellt. Diese Prüfsummen werden verwendet, um die Daten während der Übertragung automatisch zu validieren.

Diese Prüfsummen werden grundsätzlich für jede Datei (oder für einzelne Teile großer Dateien) erstellt. Für Snowball Edge sind diese Prüfsummen sichtbar, wenn Sie den folgenden AWS CLI Befehl für einen Bucket auf dem Gerät ausführen. Die Prüfsummen werden verwendet, um die Integrität Ihrer Daten während der gesamten Übertragung zu überprüfen und sicherzustellen, dass Ihre Daten korrekt kopiert werden.

```
aws s3api list-objects --bucket bucket-name --endpoint http://ip:8080 --profile edge-profile
```

Wenn diese Prüfsummen nicht übereinstimmen, werden die zugehörigen Daten nicht in Amazon S3 importiert.

Lokaler Dateibestand und Snowball Edge-Datenübertragung

Erstellen Sie ein lokales Inventar von Dateien, die auf Snowball Edge kopiert wurden, wenn Sie den Amazon S3 S3-Adapter oder die CLI verwenden. Der Inhalt des lokalen Inventars kann verwendet werden, um ihn mit dem Inhalt des lokalen Speichers oder Servers zu vergleichen.

Zum Beispiel

```
aws s3 cp folder/ s3://bucket --recursive > inventory.txt
```

Häufige Ursachen für Datenvalidierungsfehler mit Snowball Edge

Wenn ein Validierungsfehler auftritt, werden die entsprechenden Daten (eine Datei oder ein Teil einer großen Datei) nicht in das Ziel geschrieben. Im Folgenden sind die häufigsten Ursachen für Validierungsfehler aufgeführt:

- Es wird versucht, symbolische Links zu kopieren.
- Es wird versucht, Dateien zu kopieren, die aktiv geändert werden. Der Versuch schlägt bei der Prüfsummenüberprüfung fehl und wird als fehlgeschlagene Übertragung markiert.
- Es wird versucht, Dateien mit einer Größe von mehr als 5 TB zu kopieren.
- Es wird versucht, Bauteilgrößen zu kopieren, die größer als 2 GiB sind.
- Es wird versucht, Dateien auf ein Snowball Edge-Gerät zu kopieren, das bereits die volle Datenspeicherkapazität erreicht hat.
- Es wird versucht, Dateien auf ein Snowball Edge-Gerät zu kopieren, das nicht den [Richtlinien zur Benennung von Objektschlüsseln](#) für Amazon S3 entspricht.

Wenn einer dieser Validierungsfehler auftritt, wird er protokolliert. Sie können Maßnahmen ergreifen, um manuell zu ermitteln, bei welchen Dateien die Überprüfung fehlgeschlagen ist und warum.

Weitere Informationen finden Sie unter [Manuelles Überprüfen von Daten von einem Snowball Edge-Gerät nach dem Import in Amazon S3](#).

Manuelles Überprüfen von Daten von einem Snowball Edge-Gerät nach dem Import in Amazon S3

Nach Abschluss eines Importauftrags haben Sie mehrere Möglichkeiten, die Daten in Amazon S3 manuell zu validieren, wie im Folgenden beschrieben.

Überprüfen des Abschlussberichts für den Auftrag und der zugehörigen Protokolle

Immer wenn Daten in Amazon S3 importiert oder aus Amazon S3 exportiert werden, erhalten Sie einen herunterladbaren PDF-Auftragsbericht. Bei Importaufträgen steht dieser Bericht am Ende des Importvorgangs zur Verfügung. Weitere Informationen finden Sie unter [Sie erhalten den Abschlussbericht und die Protokolle Ihres Datenübertragungsauftrags](#).

S3-Bestand

Wenn Sie in mehreren Aufträgen eine riesige Datenmenge in Amazon S3 übertragen haben, ist das Durchgehen der einzelnen Auftragsabschlussberichte möglicherweise keine effiziente Zeitnutzung. Stattdessen können Sie eine Bestandsaufnahme aller Objekte in einem oder mehreren Amazon S3 S3-Buckets abrufen. Das Amazon S3 S3-Inventar bietet eine Datei mit kommagetrennten Werten (CSV), in der Ihre Objekte und die entsprechenden Metadaten täglich oder wöchentlich angezeigt werden. Diese Datei deckt Objekte für einen Amazon S3 S3-Bucket oder ein gemeinsames Präfix ab (d. h. Objekte, deren Namen mit einer gemeinsamen Zeichenfolge beginnen).

Wenn Sie den Bestand der Amazon S3 S3-Buckets haben, in die Sie Daten importiert haben, können Sie ihn problemlos mit den Dateien vergleichen, die Sie an Ihrem Quelldatenspeicherort übertragen haben. Auf diese Weise können Sie schnell bestimmen, ob bzw. welche Dateien nicht übertragen wurden.

Verwenden Sie den Amazon S3 S3-Sync-Befehl

Wenn Ihre Workstation eine Verbindung zum Internet herstellen kann, können Sie eine endgültige Überprüfung all Ihrer übertragenen Dateien durchführen, indem Sie den AWS CLI Befehl ausführen `aws s3 sync`. Dieser Befehl synchronisiert Verzeichnisse und S3-Präfixe. Dieser Befehl kopiert neue und aktualisierte Dateien rekursiv aus dem Quellverzeichnis in das Ziel. Weitere Informationen finden Sie unter [Sync](#) in der AWS CLI Befehlsreferenz.

 Important

Wenn Sie Ihren lokalen Speicher als Ziel für diesen Befehl angeben, stellen Sie sicher, dass Sie eine Sicherungskopie der Dateien haben, mit denen Sie synchronisieren. Diese Dateien werden durch den Inhalt der angegebenen Amazon S3 S3-Quelle überschrieben.

Benachrichtigungen für Snowball Edge

So verwendet Snow Amazon SNS

Der Snow-Service ist so konzipiert, dass er die Vorteile der robusten Benachrichtigungen nutzt, die von Amazon Simple Notification Service (Amazon SNS) bereitgestellt werden. Bei der Erstellung eines Auftrags zur Bestellung eines Snow-Geräts können Sie E-Mail-Adressen angeben, um Benachrichtigungen über Ihre Jobstatusänderungen zu erhalten. Wenn Sie dies tun, wählen Sie ein vorhandenes SNS-Thema aus oder erstellen ein neues. Wenn das SNS-Thema verschlüsselt ist, müssen Sie die vom Kunden verwaltete KMS-Verschlüsselung für das Thema aktivieren und eine vom Kunden verwaltete KMS-Schlüsselrichtlinie einrichten. Siehe [Wählen Sie Einstellungen für Benachrichtigungen über den Snowball Edge-Job](#).

Nachdem Sie Ihren Job erstellt haben, erhält jede E-Mail-Adresse, die Sie für Amazon SNS SNS-Benachrichtigungen angegeben haben, eine E-Mail-Nachricht mit Benachrichtigungen, in der Sie um Bestätigung für das Themenabonnement gebeten werden. AWS Ein Benutzer des E-Mail-Kontos muss das Abonnement bestätigen, indem er Abonnement bestätigen wählt. Die Amazon SNS SNS-Benachrichtigungs-E-Mails sind auf jeden Jobstatus zugeschnitten und enthalten einen Link zu den [Managementkonsole für die AWS Snow-Familie](#).

Sie können Amazon SNS auch so konfigurieren, dass Textnachrichten für Benachrichtigungen über Statusänderungen von der Amazon SNS SNS-Konsole gesendet werden. Weitere Informationen finden Sie unter [Mobile Textnachrichten \(SMS\)](#) im Amazon Simple Notification Service Developer Guide.

Verschlüsselung von SNS-Themen für AWS Statusänderungen bei Snow Jobs

Aktivieren Sie die vom Kunden verwaltete KMS-Verschlüsselung für das SNS-Thema für Benachrichtigungen über Statusänderungen bei Snow Jobs. Mit AWS verwalteter Verschlüsselung verschlüsselte SNS-Themen können keine Änderungen am Status von Snow-Jobs empfangen, da die IAM-Rolle für den Schnee-Import keinen Zugriff auf den mit AWS-verwalteten KMS-Schlüssel zur Ausführung von Aktionen hat. Decrypt GenerateDataKey Darüber hinaus können die Richtlinien von AWS-verwalteten KMS-Schlüsseln nicht bearbeitet werden.

So aktivieren Sie die serverseitige Verschlüsselung für ein SNS-Thema mithilfe der Amazon SNS SNS-Managementkonsole

1. Melden Sie sich bei <https://console.aws.amazon.com/sns/v3/home> an AWS-Managementkonsole und öffnen Sie die Amazon SNS SNS-Konsole.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie auf der Seite „Themen“ das Thema aus, das für Benachrichtigungen zur Änderung des Jobstatus verwendet wird, und klicken Sie dann auf Bearbeiten.
4. Erweitern Sie den Abschnitt Encryption (Verschlüsselung) und gehen Sie wie folgt vor:
 - a. Wählen Sie Enable encryption (Verschlüsselung aktivieren) aus.
 - b. Geben Sie den AWS KMS-Schlüssel an. Siehe
 - c. Für jeden KMS-Typ werden die Beschreibung, das Konto und der KMS-ARN angezeigt.
5. Um einen benutzerdefinierten Schlüssel aus Ihrem AWS Konto zu verwenden, wählen Sie das Feld AWS KMS-Schlüssel und dann den benutzerdefinierten KMS-KMS aus der Liste aus. Anweisungen zum Erstellen eines benutzerdefinierten KMS finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Um einen benutzerdefinierten KMS-ARN von Ihrem AWS Konto oder einem anderen AWS Konto zu verwenden, geben Sie den KMS-Schlüssel-ARN in das Feld AWS KMS-Schlüssel ein.

6. Wählen Sie Änderungen speichern. Die serverseitige Verschlüsselung ist für Ihr Thema aktiviert und die Themenseite wird angezeigt.

Einrichtung einer vom Kunden verwalteten KMS-Schlüsselrichtlinie für AWS Snow

Nachdem Sie die Verschlüsselung für SNS-Themen aktiviert haben, die Benachrichtigungen über Änderungen des Snow-Auftragsstatus erhalten, aktualisieren Sie die KMS-Richtlinie für die SNS-Themenverschlüsselung und lassen Sie dem Snow-Serviceprinzipal Aktionen "importexport.amazonaws.com" zu. "kms:Decrypt" "kms:GenerateDataKey"

Um die Import-Export-Servicerolle in der KMS-Schlüsselrichtlinie zuzulassen

1. Melden Sie sich bei der AWS Key Management Service (AWS KMS) -Konsole an AWS-Managementkonsole und öffnen Sie sie 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. Ändern Sie in der oberen rechten Ecke der Konsole die Region AWS-Region der Konsole auf dieselbe Region, in der das Snow-Gerät bestellt wurde.
4. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
5. Wählen Sie in der Liste der KMS-Schlüssel den Alias oder die Schlüssel-ID des KMS-Schlüssels aus, der aktualisiert werden soll.
6. Wählen Sie die Registerkarte Schlüsselrichtlinie. In den wichtigsten Richtlinienanweisungen können Sie die Prinzipale sehen, denen durch die Schlüsselrichtlinie Zugriff auf den KMS-Schlüssel gewährt wurde, und Sie können sehen, welche Aktionen sie ausführen können.
7. Fügen Sie für den Snow Service Principal "importexport.amazonaws.com" die folgende Richtlinienerklärung "kms:Decrypt" und die folgenden "kms:GenerateDataKey*" Aktionen hinzu:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "service.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:service:region:customer-account-id:resource-type/customer-resource-id"
    }
  },
  "StringEquals": {
    "kms:EncryptionContext:aws:sns:topicArn": "arn:aws:sns:your_region:customer-account-id:your_sns_topic_name"
  }
}
```

8. Wählen Sie Änderungen speichern, um die Änderungen zu übernehmen und den Policy-Editor zu beenden.

Beispiele für Amazon SNS SNS-Benachrichtigungen für AWS Snow

Amazon SNS SNS-Benachrichtigungen erzeugen die folgenden E-Mail-Nachrichten, wenn sich Ihr Jobstatus ändert. Diese Nachrichten sind Beispiele für das Email-JSON SNS-Themenprotokoll.

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Job created

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) has been created. More
info - https://console.aws.amazon.
com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtN5IbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg=="
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

```
"SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

Appliance wird vorbereitet

SNS-Benachrichtigung (JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being prepared.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Exporting

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being Exported.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtN5IbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```


Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

In transit to you

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is in transit to
you. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Delivered to you

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) was delivered to
you. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtN5IbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Auf dem Weg nach AWS

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is in transit to
AWS. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Im Sortierzentrum

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is at AWS sorting
facility. More info - https://
console.aws.amazon.com/impor
texport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD0lzmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJLIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
```


Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

```
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Bei AWS

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is at AWS. More info
- https://console.aws.amazon.com/
importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Importing

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being imported.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtN5IbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Completed

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) complete.\nThanks
for using AWS Snowball Edge.\nCan you
take a quick survey on your experienc
e? Survey here: http://bit.ly/1pLQ
JMY. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkg
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd507lX1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7
Ta1MD0lzmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

```
22223333:ExampleTopic1:e103  
9402-24e7-40a3-a0d4-797da162b297"  
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Abgebrochen

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) was canceled. More
info - https://console.aws.amazon.
com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtN5IbZew3foxgx8GT
+1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```


Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

AWS Snowball Edge API-Aufrufe protokollieren mit AWS CloudTrail

Der AWS Snowball- oder Snowball Edge-Dienst ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für den AWS Snowball Edge-Dienst. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Snowball Edge Family-Konsole und Code-Aufrufe an die AWS Snowball Edge Family Job Management API. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Snowball Edge Family-API-Aufrufe. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der von CloudTrail gesammelten Informationen können Sie die mit der AWS Snowball Edge Family API gestellte Anfrage, die IP-Adresse der Anfrage, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Informationen ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

AWS Snowball Edge Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS Snowball Edge, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für AWS Snowball Edge, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert alle Ereignisse AWS-Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 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 in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)

- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle Aktionen zur Auftragsverwaltung sind in der [AWS Snowball Edge API-Referenz](#) dokumentiert und werden protokolliert, CloudTrail mit den folgenden Ausnahmen:

- Der [CreateAddress](#)Vorgang wird nicht protokolliert, um vertrauliche Kundeninformationen zu schützen.
- Alle schreibgeschützten API-Aufrufe (für API-Operationen, die mit dem Präfix von `Get`, `Describe` oder `List` beginnen) erfassen keine Antwortelemente.

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 Root- oder AWS Identity and Access Management (IAM-Benutzer-) Anmeldeinformationen 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 finden Sie im [CloudTrail UserIdentity-Element](#) im AWS CloudTrail Benutzerhandbuch.

Grundlegendes zu Protokolldateieinträgen für AWS Snowball Edge

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den [DescribeJob](#)Vorgang demonstriert.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {"attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2019-01-22T21:58:38Z"
        }},
        "invokedBy": "signin.amazonaws.com"
      },
      "eventTime": "2019-01-22T22:02:21Z",
      "eventSource": "snowball.amazonaws.com",
      "eventName": "DescribeJob",
      "awsRegion": "eu-west-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "signin.amazonaws.com",
      "requestParameters": {"jobId": "JIDa1b2c3d4-0123-abcd-1234-0123456789ab"},
      "responseElements": null,
      "requestID": "12345678-abcd-1234-abcd-ab0123456789",
      "eventID": "33c7ff7c-3efa-4d81-801e-7489fe6fff62",
      "eventType": "AwsApiCall",
      "recipientAccountId": "444455556666"
    }
  ]
}
```

AWS Snowball Edge Kontingente

Im Folgenden finden Sie Informationen zu Einschränkungen bei der Nutzung des AWS Snowball Edge Geräts.

Important

Wenn Sie Daten mit einem Snowball Edge in Amazon Simple Storage Service (Amazon S3) übertragen, denken Sie daran, dass die Größe einzelner Amazon S3-Objekte zwischen mindestens 0 Byte und maximal 5 Terabyte (TB) liegen kann.

Verfügbarkeit in der Region für AWS Snowball Edge

In der folgenden Tabelle sind die Regionen aufgeführt, in denen AWS Snowball Edge es verfügbar ist.

Region	Verfügbarkeit von Snowball Edge
US East (Ohio)	✓
USA Ost (Nord-Virginia)	✓
USA West (Nordkalifornien)	✓
USA West (Oregon)	✓
AWS GovCloud (US-Ost)	✓
AWS GovCloud (US-West)	✓
Kanada (Zentral)	✓
Asien-Pazifik (Jakarta)	✓
Asien-Pazifik (Mumbai)	✓
Asien-Pazifik (Osaka)	✓

Region	Verfügbarkeit von Snowball Edge
Asien-Pazifik (Seoul)	✓
Asien-Pazifik (Singapur)	✓
Asien-Pazifik (Sydney)	✓
Asien-Pazifik (Tokio)	✓
Europe (Frankfurt)	✓
Europa (Irland)	✓
Europa (London)	✓
Europa (Milan)	✓
Europe (Paris)	✓
Europa (Stockholm)	✓
Naher Osten (VAE)	✓
Südamerika (São Paulo)	✓

Informationen zu unterstützten AWS Regionen und Endpunkten finden Sie unter [AWS Snowball Edge-Endpunkte und](#) Kontingente in der Allgemeine AWS-Referenz

Einschränkungen für Jobs AWS Snowball Edge

Für die Erstellung von AWS Snowball Edge Gerätejobs gelten die folgenden Einschränkungen:

- Aus Sicherheitsgründen müssen Aufträge, bei denen ein AWS Snowball Edge Gerät verwendet wird, innerhalb von 360 Tagen nach der Vorbereitung abgeschlossen werden. Wenn Sie ein oder mehrere Geräte länger als 360 Tage behalten müssen, finden Sie weitere Informationen unter [Aktualisierung des SSL-Zertifikats auf Snowball Edge-Geräten](#). Andernfalls wird das Gerät nach 360 Tagen gesperrt, es kann nicht mehr darauf zugegriffen werden und muss zurückgegeben werden. Wenn das AWS Snowball Edge Gerät während eines Importauftrags gesperrt wird, können wir die vorhandenen Daten auf dem Gerät trotzdem nach Amazon S3 übertragen.

- AWS Snowball Edge unterstützt serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) und serverseitige Verschlüsselung mit AWS Key Management Service verwalteten Schlüsseln (SSE-KMS). Amazon S3 S3-kompatibler Speicher auf Snowball Edge unterstützt SSE-C für lokale Rechen- und Speicherjobs. Weitere Informationen finden Sie unter [Schutz von Daten durch serverseitige Verschlüsselung](#) im Amazon Simple Storage Service User Guide.
- Wenn Sie ein AWS Snowball Edge Gerät zum Importieren von Daten verwenden und mehr Daten übertragen müssen, als auf ein einzelnes Snowball Edge Edge-Gerät passen, erstellen Sie zusätzliche Jobs. Jeder Exportauftrag kann mehrere Snowball Edge Edge-Geräte verwenden.
- Das Standarddienstlimit für die Anzahl der Snowball Edge Edge-Geräte, die Sie gleichzeitig verwenden können, beträgt 1 pro Konto und pro AWS-Region. Wenn Sie Ihr Servicelimit erhöhen oder einen Cluster-Job erstellen möchten, wenden Sie sich an [AWS Support](#).
- Metadaten für Objekte, die auf ein Gerät übertragen wurden, werden nicht dauerhaft gespeichert. Nur die Metadaten von `filename` und `filesize` bleiben unverändert. Alle anderen Metadaten werden wie im folgenden Beispiel festgelegt:

```
-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]
```

Ratenbegrenzungen für AWS Snowball Edge

Der Rate Limiter wird verwendet, um die Rate der Anfragen in einer Servercluster-Umgebung zu steuern.

Verbindungslimit für Amazon Snow S3 Adapter

Das maximale Verbindungslimit für Snowball Edge auf Amazon S3 beträgt 1000. Alle Verbindungen über 1000 werden unterbrochen.

Einschränkungen bei der Übertragung von lokalen Daten mit einem Snowball Edge Edge-Gerät

Für die Übertragung von Daten zu oder von einem lokalen AWS Snowball Edge Gerät gelten die folgenden Einschränkungen:

- Dateien müssen beim Schreiben in statischem Zustand sein. Dateien, die während der Übertragung geändert werden, werden nicht in Amazon S3 importiert.

- Jumbo-Frames werden nicht unterstützt, d. h. Ethernet-Frames mit mehr als 1500 Byte Nutzlast.
- Beachten Sie bei der Auswahl der zu exportierenden Daten, dass Objekte mit abschließenden Schrägstrichen im Namen (oder) nicht übertragen werden. / \ Entfernen Sie bei solchen Objekten den abschließenden Schrägstrich im Namen, bevor Sie diese exportieren.
- Bei Verwendung der mehrteiligen Datenübertragung beträgt die maximale Bauteilgröße 2 GiB.

Kontingente für Recheninstanzen auf einem Snowball Edge-Gerät

Im Folgenden sind Speicherkontingente und Beschränkungen für gemeinsam genutzte Ressourcen für Rechenressourcen auf einem AWS Snowball Edge Gerät aufgeführt.

Ressourcenspeicherkontingente auf Snowball Edge berechnen

Der für Rechenressourcen verfügbare Speicher ist eine separate Ressource vom dedizierten Amazon S3 S3-Speicher auf einem Snowball Edge-Gerät. Es gelten die folgenden Speicherkontingente:

Ein für die Datenverarbeitung optimiertes Snowball Edge-Gerät kann bis zu 20 AMIs und 10 Volumes pro Instanz ausführen.

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	Unterstützte Gerätefunktion
sbe1.small	1	1	speicheroptimiert
sbe1.medium	1	2	speicheroptimiert
sbe1.large	2	4	speicheroptimiert
sbe1.xlarge	4	8	speicheroptimiert
sbe1.2xlarge	8	16	speicheroptimiert

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	Unterstützte Gerätekonfiguration
sbe1.4xlarge	16	32	speicheroptimiert
sbe1.6xlarge	24	32	speicheroptimiert
sbe-c.small	1	2	für Datenverarbeitung optimiert
sbe-c.medium	1	4	für Datenverarbeitung optimiert
sbe-c.large	2	8	für Datenverarbeitung optimiert
sbe-c.xlarge	4	16	für Datenverarbeitung optimiert
sbe-c.2xlarge	8	32	für Datenverarbeitung optimiert

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	Unterstützte Gerätekonfiguration
sbe-c.4xlarge	16	64	für Datenverarbeitung optimiert
sbe-c.8xlarge	32	128	für Datenverarbeitung optimiert
sbe-c.12xlarge	48	192	für Datenverarbeitung optimiert
sbe-c.16xlarge	64	256	für Datenverarbeitung optimiert
sbe-c.24xlarge	96	384	für Datenverarbeitung optimiert

Einschränkungen gemeinsam genutzter Rechenressourcen auf Snowball Edge

Alle Dienste auf einem Snowball Edge-Gerät verwenden einige der begrenzten Ressourcen auf dem Gerät. Ein Snowball Edge-Gerät, dessen verfügbare Rechenressourcen maximiert sind, kann keine neuen Rechenressourcen starten. Wenn Sie beispielsweise versuchen, die NFS-Schnittstelle zu starten und gleichzeitig eine sbe1.4xlarge Recheninstanz auf einem speicheroptimierten Gerät

auszuführen, wird der NFS-Schnittstellendienst nicht gestartet. Im Folgenden werden die verfügbaren Ressourcen auf den verschiedenen Geräteoptionen sowie die Ressourcenanforderungen für jeden Service beschrieben.

- Wenn keine Datenverarbeitungsservices den Status ACTIVE haben:
 - Bei einer speicheroptimierten Option stehen Ihnen 24 V CPUs und 32 GiB Arbeitsspeicher für Ihre Recheninstanzen zur Verfügung.
 - Bei einer berechnungsoptimierten Option stehen Ihnen 104 V CPUs und 208 GiB Arbeitsspeicher für Ihre Compute-Instances zur Verfügung.
- Während AWS IoT Greengrass und AWS Lambda betrieben von AWS IoT Greengrass sind ACTIVE:
 - Bei einer speicheroptimierten Option nutzen diese Services 4 vCPU-Prozessorkerne und 8 GiB Arbeitsspeicher.
 - Bei einer für die Datenverarbeitung optimierten Option nutzen diese Services 1 vCPU-Prozessorkern und 1 GiB Arbeitsspeicher.
 - Die NFS-Schnittstelle ist zwar vorhanden ACTIVE, verwendet aber 8 vCPU-Kerne und 16 GiB Arbeitsspeicher auf einem Snowball Edge-Gerät.
 - Während Amazon S3 S3-kompatibler Speicher auf Snowball Edge auf einem mit AMD EPYC Gen2 und NVME Snowball Edge Compute Optimized AKTIV ist, werden für einen einzelnen Knoten mit einer Mindestkonfiguration von 3 TB Amazon S3 S3-kompatiblen Speicher auf Snowball Edge 8 vCPU-Kerne und 16 GB Arbeitsspeicher verwendet. Für einen einzelnen Knoten mit mehr als 3 TB Amazon S3 S3-kompatiblen Speicher auf Snowball Edge werden 20 vCPU-Kerne und 40 GB Arbeitsspeicher verwendet. Für einen Cluster werden 20 vCPU-Kerne und 40 GB Arbeitsspeicher verwendet.

Sie können feststellen, ob sich ein Dienst ACTIVE auf einem Snowball Edge befindet, indem Sie den Befehl `snowballEdge describe-service` auf dem Snowball Edge-Client verwenden. Weitere Informationen finden Sie unter [Status von Diensten anzeigen, die auf Snowball Edge ausgeführt werden](#).

Einschränkungen beim Versand eines Snowball Edge Edge-Geräts

Für den Versand eines AWS Snowball Edge Geräts gelten die folgenden Einschränkungen:

- AWS versendet ein Snowball Edge Edge-Gerät nicht an ein Postfach.

- AWS versendet kein Snowball Edge Edge-Gerät zwischen Regionen außerhalb der USA, z. B. von der EU (Irland) in die EU (Frankfurt) oder in den asiatisch-pazifischen Raum (Sydney).
- Das Verschieben eines Snowball Edge Edge-Geräts an eine Adresse außerhalb des Landes, das bei der Erstellung des Jobs angegeben wurde, ist nicht zulässig und stellt einen Verstoß gegen die AWS Servicebedingungen dar.

Weitere Informationen zum Versand finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).

Einschränkungen bei der Verarbeitung eines zurückgegebenen Snowball Edge Edge für den Import

Um Ihre Daten importieren zu können AWS, muss das Gerät die folgenden Anforderungen erfüllen:

- Das AWS Snowball Edge Gerät darf nicht kompromittiert werden. Öffnen Sie das AWS Snowball Edge Gerät unter keinen Umständen, es sei denn, Sie müssen die drei Türen an der Vorder-, Rückseite und Oberseite öffnen oder den optionalen Luftfilter hinzufügen und austauschen.
- Das Gerät muss physisch unbeschädigt sein. Sie können Schäden verhindern, indem Sie die drei Türen am Snowball Edge Edge-Gerät schließen, bis die Riegel ein hörbares Klickgeräusch von sich geben.
- Das E Ink-Display auf dem Snowball Edge Edge-Gerät muss sichtbar sein. Es muss auch das Rücksendetikett enthalten, das automatisch generiert wurde, als Sie die Übertragung Ihrer Daten auf das AWS Snowball Edge Gerät abgeschlossen haben.

Note

Alle zurückgesandten Snowball Edge Edge-Geräte, die diese Anforderungen nicht erfüllen, werden gelöscht, ohne dass daran gearbeitet wurde.

Problembehandlung AWS Snowball Edge

Beachten Sie bei der Fehlerbehebung die folgenden allgemeinen Richtlinien.

- Objekte in Amazon S3 haben eine maximale Dateigröße von 5 TB.
- Objekte, die auf ein AWS Snowball Edge Gerät übertragen werden, haben eine maximale Schlüssellänge von 933 Byte. Bei Schlüsselnamen mit Zeichen, die mehr als 1 Byte umfassen, beträgt die maximale Schlüssellänge dennoch 933 Byte. Beim Ermitteln der Schlüssellänge berücksichtigen Sie den Datei- oder Objektnamen sowie den entsprechenden Pfad oder Präfixe. Dateien mit kurzen Dateinamen innerhalb eines stark verschachtelten Pfads können Schlüssel mit mehr als 933 Byte haben. Der Bucket-Name wird beim Ermitteln der Schlüssellänge für den Pfad nicht berücksichtigt. Im Folgenden sind einige Beispiele aufgeführt.

Name des Objekts	Bucket-Name	Pfad plus Bucket-Name	Schlüssellänge
sunflower-1.jpg	pictures	sunflower-1.jpg	15 Zeichen
receipts.csv	MyTaxInfo	/Users/Eric/Documents/2016/January/	47 Zeichen
bhv.1	\$7\$zWwwXKQj\$gLA0oZCj\$r8p	/.VfV/FqGC3QN\$7BXys3KHYePfuIOMNjY83dVxugPY1xVg/evpcQEJLT/rSwZc\$M1VVf/\$hwefVISRqwepB\$/BiiD/PP	135 Zeichen

Name des Objekts	Bucket-Name	Pfad plus Bucket-Name	Schlüssel länge
		F\$twRAjɾD /fIMp/0NY	

- Aus Sicherheitsgründen müssen Aufträge, bei denen ein AWS Snowball Edge Gerät verwendet wird, innerhalb von 360 Tagen nach der Vorbereitung abgeschlossen werden. Wenn Sie ein oder mehrere Geräte länger als 360 Tage behalten müssen, finden Sie weitere Informationen unter [Aktualisierung des SSL-Zertifikats auf Snowball Edge-Geräten](#). Andernfalls wird das Gerät nach 360 Tagen gesperrt, es kann nicht mehr darauf zugegriffen werden und muss zurückgegeben werden. Wenn das AWS Snowball Edge Gerät während eines Importauftrags gesperrt wird, können wir die vorhandenen Daten auf dem Gerät trotzdem nach Amazon S3 übertragen.
- Wenn Sie bei der Verwendung eines AWS Snowball Edge Geräts auf unerwartete Fehler stoßen, möchten wir davon erfahren. Kopieren Sie die entsprechenden Protokolle und fügen Sie sie zusammen mit einer kurzen Beschreibung der Probleme, auf die Sie gestoßen sind, einer Nachricht an bei AWS Support. Weitere Informationen über Protokolle finden Sie unter [Konfiguration und Verwendung des Snowball Edge-Clients](#).

Themen

- [So identifizieren Sie einen Snowball Edge](#)
- [Behebung von Startproblemen mit Snowball Edge](#)
- [Behebung von Verbindungsproblemen mit Snowball Edge](#)
- [Behebung von unlock-device Befehlsproblemen mit Snowball Edge](#)
- [Behebung von Problemen mit Anmeldeinformationen mit Snowball Edge](#)
- [Behebung von Datenübertragungsproblemen mit Snowball Edge](#)
- [Behebung von AWS CLI Problemen mit Snowball Edge](#)
- [Fehlerbehebung bei Compute-Instanzen auf Snowball Edge](#)

So identifizieren Sie einen Snowball Edge

Verwenden Sie den `describe-device` Befehl, um den Gerätetyp zu ermitteln, und suchen Sie dann DeviceType in der folgenden Tabelle nach dem zurückgegebenen Wert von, um die Konfiguration zu ermitteln.

```
snowballEdge describe-device
```

Example der **describe-device** Ausgabe

```
{
  "DeviceId" : "JID-206843500001-35-92-20-211-23-06-02-18-24",
  "UnlockStatus" : {
    "State" : "UNLOCKED"
  },
  ...
  "DeviceType" : "V3_5C"
}
```

DeviceTypeund Snowball Edge-Gerätekonfigurationen

DeviceType	Wert	Gerätekonfiguration
V3_5C		Snowball Edge rechneroptimiert mit AMD EPYC Gen2 und NVME
V3_5S		Snowball Edge, speicheroptimiert, 210 TB

Weitere Informationen zu Snowball Edge-Gerätekonfigurationen finden Sie unter [AWS Snowball Edge Informationen zur Gerätehardware](#).

Behebung von Startproblemen mit Snowball Edge

Die folgenden Informationen können Ihnen helfen, bestimmte Probleme zu beheben, die beim Starten Ihres Snowball Edge auftreten könnten.

- Warten Sie 10 Minuten, bis ein Gerät hochgefahren ist. Vermeiden Sie es, das Gerät während dieser Zeit zu bewegen oder zu benutzen.
- Stellen Sie sicher, dass beide Enden des Stromversorgungskabels fest angeschlossen sind.
- Ersetzen Sie das Stromversorgungskabel durch ein anderes Kabel, von dem Sie wissen, dass es einwandfrei ist.
- Connect das Stromversorgungskabel an eine andere Stromquelle an, von der Sie wissen, dass sie gut ist.

Behebung von Problemen mit dem LCD-Display eines Snowball Edge-Geräts während des Startvorgangs

Manchmal kann nach dem Einschalten eines Snowball Edge-Geräts ein Problem mit dem LCD-Display auftreten.

- Der LCD-Bildschirm ist schwarz und es wird kein Bild angezeigt, nachdem Sie das Snowball Edge-Gerät an die Stromversorgung angeschlossen und den Betriebsschalter über dem LCD-Bildschirm gedrückt haben.
- Der LCD-Bildschirm bewegt sich nicht über die Einstellung Ihres Snowball Edge hinaus. Dies kann einige Minuten dauern. Meldung und der Netzwerkkonfigurationsbildschirm wird nicht angezeigt.

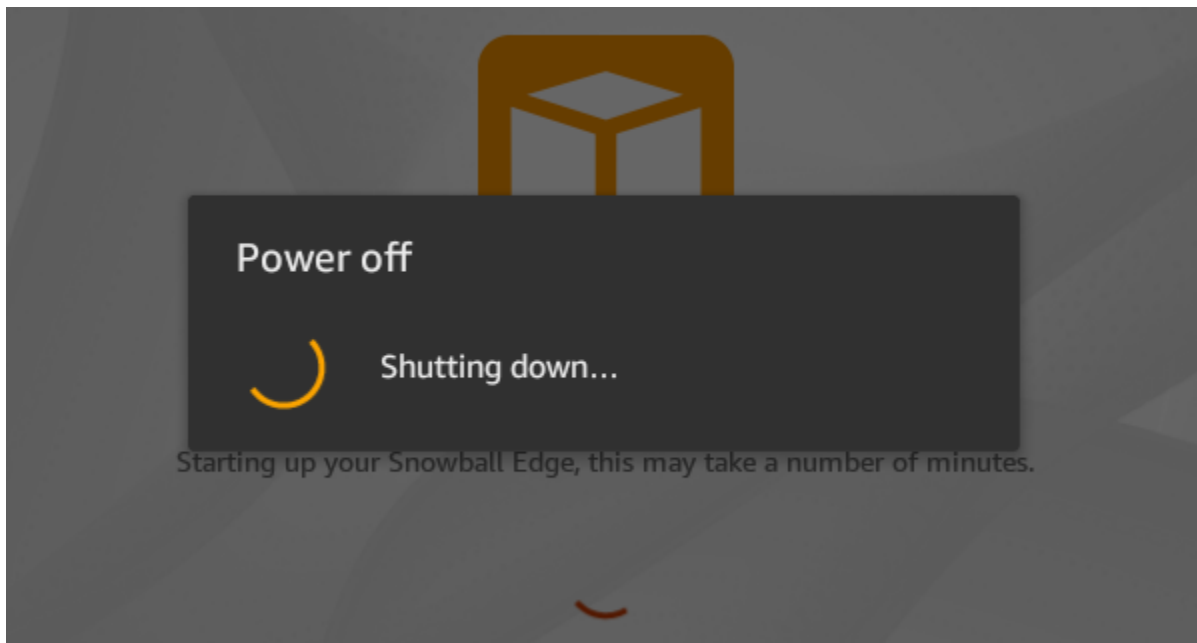


Aktion, die ausgeführt werden soll, wenn der LCD-Bildschirm nach dem Drücken des Betriebsschalters schwarz ist

1. Stellen Sie sicher, dass das Snowball Edge-Gerät an eine Stromquelle angeschlossen ist und die Stromquelle Strom liefert.
2. Lassen Sie das Gerät 1 bis 2 Stunden an die Stromquelle angeschlossen. Stellen Sie sicher, dass die Türen an der Vorder- und Rückseite des Geräts geöffnet sind.
3. Kehren Sie zum Gerät zurück und der LCD-Bildschirm ist betriebsbereit.

Aktion, die ergriffen werden muss, wenn Snowball Edge nicht zum Netzwerkkonfigurationsbildschirm wechselt

1. Lassen Sie den Bildschirm auf der Einstellung Ihres Snowball Edge stehen. Dies kann einige Minuten dauern. Nachricht für 10 Minuten.
2. Wählen Sie auf dem Bildschirm die Schaltfläche Anzeige neu starten. Es erscheint die Meldung Shutting down... und danach die Einstellung Ihres Snowball Edge. Dies kann einige Minuten dauern. Die Meldung wird angezeigt und das Gerät startet normal.



Wenn der LCD-Bildschirm nicht über die Einstellung Ihres Snowball Edge hinausgeht, kann dies einige Minuten dauern. Gehen Sie wie folgt vor, nachdem Sie die Taste „Display neu starten“ gedrückt haben.

Maßnahme

1. Drücken Sie über dem LCD-Bildschirm den Netzschalter, um das Gerät auszuschalten.
2. Trennen Sie alle Kabel vom Gerät.
3. Lassen Sie das Gerät 20 Minuten lang ausgeschaltet und vom Stromnetz getrennt.
4. Connect die Strom- und Netzkabel an.
5. Drücken Sie über dem LCD-Bildschirm den Netzschalter, um das Gerät einzuschalten.

Wenn das Problem weiterhin besteht, wenden Sie sich an uns, AWS Support um das Gerät zurückzugeben und ein neues Snowball Edge-Gerät zu erhalten.

Behebung von Problemen mit dem E-Ink-Display beim Systemstart

Manchmal wird nach dem Einschalten eines Snowball Edge-Geräts auf dem E Ink-Display oben auf dem Gerät möglicherweise die folgende Meldung angezeigt:

`The appliance has timed out`

Diese Meldung weist nicht auf ein Problem mit dem Gerät hin. Verwenden Sie es normal. Wenn Sie es ausschalten AWS, um es zurückzugeben, werden die Rücksendeinformationen wie erwartet angezeigt.

Behebung von Verbindungsproblemen mit Snowball Edge

Die folgenden Informationen können Ihnen helfen, bestimmte Probleme zu beheben, die möglicherweise bei der Verbindung mit Ihrem Snowball Edge auftreten:

- Router und Switches, die mit einer Geschwindigkeit von 100 Megabyte pro Sekunde arbeiten, funktionieren nicht mit einem Snowball Edge. Wir empfehlen die Verwendung eines Switches mit einer Datenrate von 1 GB pro Sekunde (oder schneller).
- Wenn Sie ungewöhnliche Verbindungsfehler mit dem Gerät haben, schalten Sie den Snowball Edge aus, ziehen Sie alle Kabel ab und lassen Sie ihn 10 Minuten lang stehen. Nach Ablauf von 10 Minuten starten Sie das Gerät neu und versuchen es erneut.
- Stellen Sie sicher, dass keine Antivirensoftware oder Firewalls die Netzwerkverbindung des Snowball Edge-Geräts blockieren.
- Beachten Sie, dass die NFS-Schnittstelle und die Amazon S3 S3-Schnittstelle unterschiedliche IP-Adressen haben.

Zur erweiterten Fehlerbehebung bei Verbindungsproblemen können Sie die folgenden Schritte durchführen:

- Wenn Sie nicht mit dem Snowball Edge kommunizieren können, pingen Sie die IP-Adresse des Geräts an. Wenn Ping no connect zurückgibt, überprüfen Sie die IP-Adresse des Geräts und Ihre lokale Netzwerkkonfiguration.
- Wenn die IP-Adresse korrekt ist und die LEDs auf der Rückseite des Geräts blinken, testen Sie das Gerät mit Telnet an den Anschlüssen 22, 9091 und 8080. Beim Testen von Port 22 wird festgestellt, ob Snowball Edge ordnungsgemäß funktioniert. Beim Testen von Port 9091 wird festgestellt, ob der zum Senden von Befehlen an das Gerät verwendet werden AWS CLI kann. Durch das Testen von Port 8080 wird sichergestellt, dass das Gerät nur mit dem S3-Adapter in die darauf befindlichen Amazon S3-Buckets schreiben kann. Wenn Sie eine Verbindung über Port 22, aber nicht über Port 8080 herstellen können, schalten Sie das Snowball Edge-Gerät aus und trennen Sie dann alle Kabel. Lassen Sie das Gerät für 10 Minuten stehen, schließen Sie es wieder an und starten Sie es erneut.

Behebung von **unlock-device** Befehlsproblemen mit Snowball Edge

Wenn der `unlock-device` Befehl zurückkehrt `connection refused`, haben Sie möglicherweise die Befehlssyntax falsch eingegeben, oder die Konfiguration Ihres Computers oder Netzwerks verhindert möglicherweise, dass der Befehl das Snow-Gerät erreicht. Ergreifen Sie die folgenden Maßnahmen, um das Problem zu lösen:

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.
 - a. Überprüfen Sie anhand des LCD-Bildschirms des Geräts, ob die im Befehl verwendete IP-Adresse korrekt ist.
 - b. Stellen Sie sicher, dass der Pfad zur im Befehl verwendeten Manifestdatei korrekt ist, einschließlich des Dateinamens.
 - c. Verwenden Sie die [AWS Snowball Edge Management Console](#), um zu überprüfen, ob der im Befehl verwendete Entsperrcode korrekt ist.
2. Stellen Sie sicher, dass sich der Computer, den Sie verwenden, im selben Netzwerk und Subnetz wie das Snow-Gerät befindet.
3. Stellen Sie sicher, dass der Computer, den Sie verwenden, und das Netzwerk so konfiguriert sind, dass der Zugriff auf das Snow-Gerät möglich ist. Ermitteln Sie anhand des `ping` Befehls für Ihr

Betriebssystem, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen der Antivirensoftware, der Firewall-Konfiguration, des virtuellen privaten Netzwerks (VPN) oder anderer Konfigurationen Ihres Computers und Netzwerks.

Behebung von Problemen mit Manifestdateien mit Snowball Edge

Jedem Auftrag ist eine bestimmte Manifestdatei zugeordnet. Wenn Sie mehrere Aufträge anlegen, sollten Sie festhalten, welches Manifest für welchen Auftrag gilt.

Wenn Sie eine Manifestdatei verlieren oder wenn eine Manifestdatei beschädigt ist, können Sie die Manifestdatei für einen bestimmten Job erneut herunterladen. Dazu verwenden Sie die Konsole oder eine der AWS APIs. AWS CLI

Wenn Sie ein Update auf dem Snowball Edge ausführen, muss eine neue Manifestdatei heruntergeladen und für den Job verwendet werden. Hinweise zum Herunterladen einer Manifestdatei finden Sie unter [Anmeldeinformationen für den Zugriff auf Snowball Edge abrufen](#).

Behebung von Problemen mit Anmeldeinformationen mit Snowball Edge

Verwenden Sie die folgenden Themen, um Probleme mit Anmeldeinformationen auf dem Snowball Edge-Gerät zu lösen.

AWS CLI Anmeldeinformationen für Snowball Edge konnten nicht gefunden werden

Wenn Sie mit dem AWS Snowball Edge Gerät über die Amazon S3 S3-Schnittstelle über die kommunizieren AWS CLI, wird möglicherweise die Fehlermeldung Unable to locate credentials angezeigt. Sie können Anmeldeinformationen konfigurieren, indem Sie „aws configure“ ausführen.

Maßnahme

Konfigurieren Sie die AWS Anmeldeinformationen, die AWS CLI verwendet werden, um Befehle für Sie auszuführen. Weitere Informationen finden Sie unter [Konfigurieren der AWS CLI](#) im AWS Command Line Interface -Leitfaden.

Fehlerbehebung bei der Snowball Edge-Fehlermeldung: Check Your Secret Access Key and Signing

Wenn Sie die Amazon S3 S3-Schnittstelle verwenden, um Daten auf einen Snowball Edge zu übertragen, wird möglicherweise die folgende Fehlermeldung angezeigt.

An error occurred (SignatureDoesNotMatch) when calling the CreateMultipartUpload operation: The request signature we calculated does not match the signature you provided.

Check your AWS secret access key and signing method. For more details go to:

[http://docs.aws.amazon.com/AmazonS3/latest/dev/](http://docs.aws.amazon.com/AmazonS3/latest/dev/RESTAuthentication.html#ConstructingTheAuthenticationHeader)

[RESTAuthentication.html#ConstructingTheAuthenticationHeader](http://docs.aws.amazon.com/AmazonS3/latest/dev/RESTAuthentication.html#ConstructingTheAuthenticationHeader)

Maßnahme

Holen Sie sich Ihre Anmeldeinformationen vom Snowball Edge-Client. Weitere Informationen finden Sie unter [Anmeldeinformationen für einen Snowball Edge abrufen](#).

Behebung von Datenübertragungsproblemen mit Snowball Edge

Wenn bei der Übertragung der Daten auf die oder von einer Snowball Edge-Appliance Leistungsprobleme auftreten, finden Sie unter [Empfehlungen für die beste Datenübertragungsleistung zu oder von einem Snowball Edge](#) Empfehlungen und Anleitungen zur Verbesserung der Übertragungsleistung. Die folgenden Punkte können Ihnen bei der Behebung von Problemen helfen, die bei der Datenübertragung zu oder von einem Snowball Edge-Gerät auftreten können.

- Sie können keine Daten in das Stammverzeichnis von Snowball Edge übertragen. Wenn Sie Probleme beim Übertragen von Daten in das Gerät haben, stellen Sie sicher, dass Sie Daten in ein Unterverzeichnis übertragen. Die Unterverzeichnisse der obersten Ebene haben die Namen der Amazon S3 S3-Buckets, die Sie in den Job aufgenommen haben. Speichern Sie Ihre Daten in diesen Unterverzeichnissen.
- Wenn Sie Linux verwenden und keine Dateien mit UTF-8-Zeichen auf ein AWS Snowball Edge Gerät hochladen können, liegt das möglicherweise daran, dass Ihr Linux-Server die UTF-8-Zeichenkodierung nicht erkennt. Sie können dieses Problem beheben, indem Sie das `locales`-Paket auf Ihrem Linux-Server installieren und es für die Verwendung eines der UTF-8-Gebietsschemata wie `en_US.UTF-8` konfigurieren. Sie können das `locales`-Paket konfigurieren, indem Sie die Umgebungsvariable `LC_ALL` exportieren. Beispiel: `export LC_ALL=en_US.UTF-8`

- Wenn Sie die Amazon S3 S3-Schnittstelle mit dem verwenden AWS CLI, können Sie mit Dateien oder Ordnern arbeiten, deren Namen Leerzeichen enthalten, z. B. my photo.jpg oder My Documents. Stellen Sie jedoch sicher, dass Sie die Leerzeichen korrekt angeben. Weitere Informationen finden Sie AWS CLI im AWS Command Line Interface Benutzerhandbuch unter [Angeben von Parameterwerten für](#).

Behebung von Problemen mit Importaufträgen mit Snowball Edge

Manchmal können Dateien nicht in Amazon S3 importiert werden. Wenn das folgende Problem auftritt, versuchen Sie die angegebenen Aktionen, um dieses Problem zu beheben. Wenn der Import einer Datei fehlschlägt, müssen Sie möglicherweise erneut versuchen, sie zu importieren. Wenn Sie es erneut importieren, ist möglicherweise ein neuer Job für Snowball Edge erforderlich.

Dateien konnten aufgrund ungültiger Zeichen in Objektnamen nicht in Amazon S3 importiert werden

Dieses Problem tritt auf, wenn ein Datei- oder Ordnername Zeichen enthält, die von Amazon S3 nicht unterstützt werden. Amazon S3 hat Regeln darüber, welche Zeichen in Objektnamen enthalten sein können. Weitere Informationen finden Sie unter [Erstellen von Objektschlüsselnamen](#) im Amazon S3 S3-Benutzerhandbuch.

Maßnahme

Wenn dieses Problem auftritt, wird die Liste der Dateien und Ordner angezeigt, die nicht in Ihren Auftragsabschlussbericht importiert werden konnten.

In einigen Fällen ist die Liste außerordentlich umfangreich oder die Dateien in der Liste sind zu groß für die Übertragung über das Internet. In diesen Fällen sollten Sie einen neuen Snowball-Importauftrag erstellen, die Datei- und Ordnernamen so ändern, dass sie den Amazon S3 S3-Regeln entsprechen, und die Dateien erneut übertragen.

Wenn die Dateien klein sind und es nicht viele davon gibt, können Sie sie über die AWS CLI oder die nach Amazon S3 kopieren AWS-Managementkonsole. Weitere Informationen finden Sie unter [Wie lade ich Dateien und Ordner in einen S3-Bucket hoch?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Behebung von Problemen mit Exportaufträgen mit Snowball Edge

Manchmal schlägt der Export von Dateien in Ihre Workstation fehl. Wenn das folgende Problem auftritt, versuchen Sie die angegebenen Aktionen, um dieses Problem zu beheben. Wenn der Export

einer Datei fehlschlägt, müssen Sie möglicherweise erneut versuchen, sie zu exportieren. Wenn Sie es erneut exportieren, ist möglicherweise ein neuer Job für Snowball Edge erforderlich.

Fehler beim Exportieren von Dateien auf einen Microsoft Windows Server

Der Export einer Datei auf einen Microsoft Windows Server schlägt möglicherweise fehl, wenn diese oder ein zugehöriger Ordner in einem Format benannt ist, das nicht von Windows unterstützt wird. Wenn der Datei- oder Ordnername beispielsweise einen Doppelpunkt (:) enthält, schlägt der Export fehl, da Windows dieses Zeichen in Datei- oder Ordnernamen nicht erlaubt.

Maßnahme

1. Erstellen Sie eine Liste der Namen, die den Fehler verursachen. Sie finden die Namen der Dateien und Ordner, die nicht exportiert werden konnten, in Ihren Protokollen. Weitere Informationen finden Sie unter [Protokolle von Snowball Edge anzeigen und herunterladen](#).
2. Ändern Sie die Namen der Objekte in Amazon S3, die das Problem verursachen, indem Sie die nicht unterstützten Zeichen entfernen oder ersetzen.
3. Wenn die Liste der Namen außerordentlich umfangreich ist oder wenn die Dateien in der Liste sind zu groß für die Übertragung über das Internet sind, erstellen Sie einen Exportauftrag speziell für diese Objekte.

Wenn die Dateien klein sind und es nicht viele davon gibt, kopieren Sie die umbenannten Objekte aus Amazon S3 über den AWS CLI oder den AWS-Managementkonsole. Weitere Informationen finden Sie unter [Wie lade ich ein Objekt aus einem S3-Bucket herunter?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Behebung von NFS-Schnittstellenproblemen mit Snowball Edge

Snowball Edge zeigt möglicherweise an, dass der Status der NFS-Schnittstelle lautet. DEACTIVATED Dies kann auftreten, wenn Snowball Edge ausgeschaltet wurde, ohne zuerst die NFS-Schnittstelle anzuhalten.

Maßnahme

Um das Problem zu beheben, beenden Sie den NFS-Dienst und starten Sie ihn neu. Gehen Sie dabei wie folgt vor.

1. Verwenden Sie den `describe-service` Befehl, um den Status des Dienstes zu ermitteln:

```
snowballEdge describe-service --service-id nfs
```

Der Befehl gibt Folgendes zurück.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "DEACTIVATED"
  }
}
```

2. Verwenden Sie den `stop-service` Befehl, um den NFS-Dienst zu beenden.

```
snowballEdge stop-service --service-id nfs
```

3. Verwenden Sie den `start-service` Befehl, um den NFS-Dienst zu starten. Weitere Informationen finden Sie unter [Verwaltung der NFS-Schnittstelle](#).

```
snowballEdge start-service --virtual-network-interface-arns vni-arn --service-id
nfs --service-configuration AllowedHosts=0.0.0.0/0
```

4. Verwenden Sie den `describe-service` Befehl, um sicherzustellen, dass der Dienst ausgeführt wird.

```
snowballEdge describe-service --service-id nfs
```

Wenn der Wert des `State` Namens lautet `ACTIVE`, ist der NFS-Schnittstellendienst aktiv.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  }
}
```



```

},
"Endpoints" : [ {
  "Protocol" : "nfs",
  "Port" : 2049,
  "Host" : "192.0.2.0"
} ],
"ServiceConfiguration" : {
  "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]
}
}

```

Behebung eines Fehlers „Zugriff verweigert“ bei der Übertragung von Daten über die S3-Schnittstelle

Wenn Sie die S3-Schnittstelle verwenden, um Daten zu oder von einem Snowball Edge-Gerät zu übertragen, tritt möglicherweise ein Fehler auf, der Zugriff verweigert wurde. Dieser Fehler kann auf IAM-Benutzer- oder Bucket-Richtlinien zurückzuführen sein.

Maßnahme

1. Überprüfen Sie die Richtlinie des S3-Buckets, den Sie verwenden, auf die folgenden Syntaxprobleme.
 - a. Wenn die Richtlinie nur das Hochladen von Daten zulässt, wenn KMS-Header übergeben werden, stellen Sie sicher, dass die Richtlinie einen Prinzipal-ARN anstelle einer Benutzer-ID angibt. Das folgende Beispiel zeigt die richtige Syntax.

```

{
  "Sid": "Statement3",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringNotLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
    },
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption": [

```

```

        "aws:kms",
        "AES256"
    ]
}
},
{
    "Sid": "Statement4",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringNotLike": {
            "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
        },
        "Null": {
            "s3:x-amz-server-side-encryption": "true"
        }
    }
}
}

```

- b. Wenn die Bucket-Richtlinie das Hochladen in den Bucket nur zulässt, wenn die richtigen Header übergeben werden, übergeben Uploads von Snowball Edge-Geräten standardmäßig keine Header. Ändern Sie die Richtlinie, um eine Ausnahme für den IAM-Benutzer zuzulassen, der zum Hochladen der Daten verwendet wurde. Im Folgenden finden Sie ein Beispiel für die korrekte Syntax dafür.

```

{
    "Sid": "Statement3",
    "Effect": "Deny",
    "Principal": "",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "AES256"
        },
        "StringNotLike": {
            "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
        }
    }
}

```

```

    }
  },
  {
    "Sid": "Statement4",
    "Effect": "Deny",
    "Principal": "",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      },
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
      }
    }
  }
}

```

- Überprüfen Sie die Richtlinie des KMS-Schlüssels, den Sie verwenden, auf die richtige Syntax im Principal-Element. Das folgende Beispiel zeigt die richtige Syntax.

```

{
  "Sid": "Statement2",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/service-role/JohnDoe"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}

```

Behebung eines verbotenen 403-Fehlers bei der Übertragung von Daten über die S3-Schnittstelle

Wenn Sie die S3-Schnittstelle verwenden, um Daten zu oder von einem Snowball Edge-Gerät zu übertragen, tritt möglicherweise der Fehler 403 Forbidden auf. Dieser Fehler kann auf IAM-Benutzer- oder Bucket-Richtlinien zurückzuführen sein. Überprüfen Sie die Richtlinie des S3-Buckets, den Sie verwenden, auf die folgenden Syntaxprobleme.

Maßnahme

1. Die Richtlinie bietet nicht die PrincipalArn. Verwenden Sie die folgende Richtlinie als Beispiel, um den PrincipalArn aws-Header zu verwenden und den ARN der IAM-Rolle ohne `:` bereitzustellen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyIncorrectEncryptionHeader",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::BucketName/*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
      },
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": [
          "aws:kms",
          "AES256"
        ]
      }
    }
  },
  {
    "Sid": "DenyUnEncryptedObjectUploads",
    "Effect": "Deny",
```

```

        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
        "Condition": {
            "StringNotLike": {
                "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
            },
            "Null": {
                "s3:x-amz-server-side-encryption": "true"
            }
        }
    },
    {
        "Sid": "DenyInsecureTransport",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::BucketName/*",
            "arn:aws:s3:::BucketName"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    },
    {
        "Sid": "AllowSnowballPutObjectAccess",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::1234567890:role/RoleName"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::BucketName/*"
    }
]
}s

```

2. Wenn die KMS-Richtlinie das falsche IAM-Rollenformat verwendet, kann ein 403-Fehler auftreten. Ändern Sie die Richtlinie, um eine Ausnahme für den IAM-Benutzer zuzulassen,

der zum Hochladen der Daten verwendet wurde. Im Folgenden finden Sie ein Beispiel für die korrekte Syntax dafür.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::1234567890:role/service-role/RoleName"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

3. Die IAM-Rolle muss möglicherweise die Bedingung für den Verschlüsselungsheader umgehen. Standardmäßig sind alle auf einem Snowball Edge-Gerät gespeicherten Objekte mit SSE-S3-Verschlüsselung verschlüsselt. Verwenden Sie die folgende Richtlinie, um eine Ausnahme für die IAM-Rolle bereitzustellen, um Objekte ohne Verschlüsselungsheader hochzuladen.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [{
    "Sid": "DenyIncorrectEncryptionHeader",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::BucketName/",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  ]
}
```

```

        "StringNotLike": {
            "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
        }
    },
    {
        "Sid": "DenyUnEncryptedObjectUploads",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::BucketName/*",
        "Condition": {
            "Null": {
                "s3:x-amz-server-side-encryption": "true"
            },
            "StringNotLike": {
                "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
            }
        }
    }
]
}

```

4. Die Fehlermeldung weist darauf hin, dass der Zugriff auf die PutObject Verwendung NotPrincipal mit IP-Bedingung verweigert wurde. Fügen Sie wie unten gezeigt eine Ausnahme für die Snowball Edge IAM-Rolle hinzu.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": [
          "IAMRole"

```

```

        ]
      },
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::BucketName/*",
        "arn:aws:s3:::BucketName"
      ],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "IPAddress"
          ]
        },
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
        }
      }
    }
  ]
}

```

Behebung von AWS CLI Problemen mit Snowball Edge

Mithilfe der folgenden Themen können Sie Probleme bei der Arbeit mit einem AWS Snowball Edge Gerät und dem beheben AWS CLI.

Fehlerbehebung bei der AWS CLI Fehlermeldung „Profile Cannot Be Null“ mit Snowball Edge

Wenn Sie mit dem arbeiten AWS CLI, wird möglicherweise eine Fehlermeldung angezeigt, die besagt, dass Profile nicht Null sein kann. Dieser Fehler kann auftreten, wenn AWS CLI das nicht installiert wurde oder kein AWS CLI Profil konfiguriert wurde.

Maßnahme

Stellen Sie sicher, dass Sie das heruntergeladen und AWS CLI auf Ihrer Workstation konfiguriert haben. Weitere Informationen finden [Sie im AWS Command Line Interface Benutzerhandbuch unter Installation oder Aktualisierung AWS CLI auf die neueste Version von](#).

Behebung eines Nullzeigerfehlers bei der Übertragung von Daten AWS CLI mit Snowball Edge

Wenn Sie den AWS CLI zum Übertragen von Daten verwenden, tritt möglicherweise ein Nullzeigerfehler auf. Dieser Fehler kann unter den folgenden Bedingungen auftreten:

- Wenn der angegebene Dateiname falsch geschrieben ist, z. B. `flower.png` oder `flower.npg` statt `flower.png`.
- Wenn der angegebene Pfad falsch ist, z. B. `C:\Documents\flower.png` statt `C:\Documents\flower.png`.
- Wenn die Datei beschädigt ist.

Maßnahme

Vergewissern Sie sich, dass der Dateiname und der Pfad korrekt sind und versuchen Sie es erneut. Wenn dieses Problem weiterhin auftritt, überprüfen Sie, ob die Datei beschädigt wurde. Brechen Sie die Übertragung ab oder versuchen Sie, die Datei zu reparieren.

Fehlerbehebung bei Compute-Instanzen auf Snowball Edge

Im Folgenden finden Sie Tipps zur Fehlerbehebung für Computerinstanzen auf Snowball Edge-Geräten.

Themen

- [Virtuelle Netzwerkschnittstelle hat die IP-Adresse 0.0.0.0](#)
- [Das Snowball Edge-Gerät reagiert nicht mehr, wenn eine große Recheninstanz gestartet wird](#)
- [Meine Instanz auf dem Snowball Edge hat ein Root-Volume](#)
- [Fehler in der ungeschützten privaten Schlüsseldatei](#)

Virtuelle Netzwerkschnittstelle hat die IP-Adresse 0.0.0.0

Dieses Problem kann auftreten, wenn die physische Netzwerkschnittstelle (NIC), die Sie Ihrer virtuellen Netzwerkschnittstelle (VNIC) zugeordnet haben, ebenfalls die IP-Adresse 0.0.0.0 hat. Dies kann passieren, wenn die NIC nicht mit einer IP-Adresse konfiguriert wurde (zum Beispiel, wenn Sie das Gerät gerade eingeschaltet haben). Oder wenn Sie die falsche Schnittstelle verwenden. Möglicherweise versuchen Sie, die IP-Adresse der SFP+-Schnittstelle abzurufen, aber es ist die RJ45 Schnittstelle, die mit Ihrem Netzwerk verbunden ist.

Maßnahme

Wenn dies der Fall ist, können Sie Folgendes tun:

- Erstellen Sie ein neues VNI, das einer Netzwerkkarte mit einer IP-Adresse zugeordnet ist. Weitere Informationen finden Sie unter [Netzwerkkonfigurationen für Recheninstanzen auf Snowball Edge](#).
- Aktualisieren Sie ein vorhandenes VNI. Weitere Informationen finden Sie unter [Aktualisierung einer virtuellen Netzwerkschnittstelle auf einem Snowball Edge](#).

Das Snowball Edge-Gerät reagiert nicht mehr, wenn eine große Recheninstanz gestartet wird

Es kann den Anschein haben, dass Ihr Snowball Edge aufgehört hat, eine Instance zu starten. Dies ist im Allgemeinen nicht der Fall. Es kann jedoch eine Stunde oder länger dauern, bis große Datenverarbeitungs-Instances gestartet werden.

Um den Status Ihrer Instances zu überprüfen, verwenden Sie den AWS CLI Befehl `aws ec2 describe-instances` run für den Amazon EC2 -kompatiblen HTTP- oder HTTPS-Endpunkt auf dem Snowball Edge.

Meine Instanz auf dem Snowball Edge hat ein Root-Volume

Instances besitzen standardmäßig ein Stamm-Volume. Alle sbe Instances haben ein einzelnes Root-Volume, aber auf einem Snowball Edge-Gerät können Sie je nach den Anforderungen Ihrer Anwendungen Blockspeicher hinzufügen oder entfernen. Weitere Informationen finden Sie unter [Blockspeicher mit EC2 Amazon-kompatiblen Instances auf Snowball Edge verwenden](#).

Fehler in der ungeschützten privaten Schlüsseldatei

Dieser Fehler kann auftreten, wenn Ihre `.h` Datei auf Ihrer Compute-Instanz nicht über ausreichende read/write Berechtigungen verfügt.

Maßnahme

Sie können dies beheben, indem Sie die Berechtigungen für die Datei mit der folgenden Vorgehensweise ändern:

1. Öffnen Sie ein Terminal und navigieren Sie zu dem Ort, an dem Sie Ihre `.pem` Datei gespeichert haben.
2. Geben Sie den folgenden Befehl ein.

```
chmod 400 filename.pem
```

Dokumentverlauf

- API-Version: 1.0
- Letzte Aktualisierung der Dokumentation: 14. März 2024

In der folgenden Tabelle werden wichtige Änderungen am AWS Snowball Edge Entwicklerhandbuch nach Juli 2018 beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Tape Gateway auf Snowball Edge-Geräten als veraltet	Die Tape Gateway-Funktionalität ist auf Snowball Edge-Geräten nicht mehr verfügbar.	14. März 2024
Die Dateischnittstelle ist veraltet	Die Dateischnittstelle ist nicht mehr für die Datenübertragung verfügbar.	1. März 2024
Amazon S3 S3-kompatibler Speicher auf Snowball Edge auf speicheroptimierten 210-TB-Geräten von Snowball Edge verfügbar	Amazon S3 S3-kompatibler Speicher auf Snowball Edge ist für S3-Speicher auf speicheroptimierten 210-TB-Geräten mit Snowball Edge verfügbar. Weitere Informationen finden Sie unter Verwenden von Amazon S3 S3-kompatiblen Speicher auf Snowball Edge .	26. Februar 2024
Fügen Sie AMIs bei der Bestellung von Geräten benutzerdefinierte Angaben hinzu	Benutzerdefinierte Amazon Machine Images können jetzt bei der Bestellung von Snowball Edge-Jobs vorgeladen werden. Weitere Informationen finden Sie unter	15. November 2023

[Hinzufügen eines AMI von AWS Marketplace.](#)

[Amazon S3 S3-kompatibler Speicher auf Snowball Edge allgemein verfügbar](#)

Amazon S3 S3-kompatibler Speicher auf Snowball Edge wird auf computeroptimierte n Snowball Edge-Geräten unterstützt. Weitere Informationen finden Sie unter [Amazon S3 S3-kompatibler Speicher auf Snowball Edge](#).

20. April 2023

[Neu unterstützt AWS-Region](#)

AWS Snowball Edge wird jetzt in der Region Naher Osten (VAE) unterstützt. Informationen zu Endpunkten für diese Region finden Sie unter [Snowball Edge Edge-Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Informationen zum Versand finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).

6. März 2023

[Neu unterstützt AWS-Region](#)

AWS Snowball Edge wird jetzt in der Region Asien-Pazifik (Jakarta) unterstützt. Informationen zu Endpunkten für diese Region finden Sie unter [Snowball Edge Edge-Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Informationen zum Versand finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).

7. September 2022

[Migration großer Datenmengen für Snowball Edge](#)

Snowball Edge unterstützt jetzt die Automatisierung eines Migrationsplans für große Datenmengen. Weitere Informationen finden Sie unter [Migration großer Datenmengen](#) (manuelle Schritte) und [Erstellen eines Migrationsplans für große Datenmengen](#), um bei Bedarf die Automatisierung einzuleiten.

27. April 2022

[Wir stellen vor AWS Snowball Edge Device Management](#)

Mit Snowball Edge Device Management können Sie Ihr Snowball Edge-Gerät und lokale AWS Dienste remote verwalten. Alle Snowball Edge-Geräte unterstützen die Snowball Edge-Geräteverwaltung und sie ist auf neuen Geräten in den meisten Ländern, in AWS-Regionen, denen Snowball Edge verfügbar ist, vorinstalliert. [Weitere Informationen finden Sie unter Geräte zur Verwaltung verwenden AWS Snowball Edge Device Management](#)

27. April 2022

[NFS-Konfiguration für Snowball Edge](#)

[NFS-Konfiguration für Snowball Edge](#) für speicheroptimierte Geräte hinzugefügt.

21. April 2022

Ratenbegrenzungen für Load Balancer	Snowball Edge unterstützt jetzt Ratenbegrenzungen für die Verteilung von Anfragen in einer Serverclusterumgebung.	19. April 2022
Support für Snowball Edge mit Tape Gateway	Sie können jetzt ein Snowball Edge-Gerät bestellen, das speziell für das Hosten des Tape Gateway-Dienstes konfiguriert ist. Diese Kombination von Technologien ermöglicht die sichere Offline-Migration von Banddaten.	30. November 2021
Support für die Network Time Protocol (NTP) -Serverkonfiguration	Snowball Edge-Geräte unterstützen jetzt die externe Network Time Protocol (NTP) -Serverkonfiguration.	16. November 2021
Support für NFS-Offline-Datenübertragung	Snowball Edge-Geräte unterstützen jetzt die Offline-Datenübertragung mit NFS. Weitere Informationen finden Sie unter Verwenden von NFS für die Offline-Datenübertragung .	4. August 2021

Neu unterstützt AWS-Region

Snowball Edge-Geräte sind jetzt in Afrika (Kapstadt) AWS-Region erhältlich. Weitere Informationen finden Sie unter [Snowball Edge Endpoints and Quotas in der](#). Allgemeine AWS-Referenz Informationen zum Versand finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).

23. November 2020

Support für den Import Ihres eigenen Bildes auf Ihr Gerät

Sie können jetzt einen Snapshot Ihres Images in Ihr Snowball Edge-Gerät importieren und es als EC2 Amazon-kompatibles Amazon Machine Image (AMI) registrieren. Weitere Informationen finden Sie unter [Importieren eines Images auf Ihr Gerät als Amazon EC2 AMI](#).

9. November 2020

Neu AWS-Region unterstützt

Snowball Edge-Geräte sind jetzt in Europa (Mailand) AWS-Region erhältlich. Weitere Informationen finden Sie unter [Snowball Edge Endpoints and Quotas in der](#). Allgemeine AWS-Referenz Informationen zum Versand finden Sie unter [Überlegungen zum Versand für Snowball Edge](#).

30. September 2020

[Umstrukturierung der Inhalte](#)

Es wurde ein Abschnitt „Erste Schritte“ erstellt, der dem Managementkonsole für die AWS Snow-Familie Arbeitsablauf entspricht, und andere Abschnitte wurden aus Gründen der Übersichtlichkeit aktualisiert. Weitere Informationen finden Sie unter [Erste Schritte mit einem AWS Snowball Edge](#).

17. September 2020

[Wir stellen vor AWS OpsHub](#)

Snowball Edge bietet jetzt ein benutzerfreundliches Tool AWS OpsHub, mit dem Sie Ihre Geräte und lokalen AWS Dienste verwalten können. Weitere Informationen finden Sie unter [Verwenden AWS OpsHub zur Verwaltung von Snowball-Geräten](#).

16. April 2020

[AWS Identity and Access Management \(IAM\) ist jetzt lokal auf dem Gerät verfügbar AWS Snowball Edge](#)

Sie können jetzt AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf AWS Ressourcen, die auf Ihrem AWS Snowball Edge Gerät ausgeführt werden, sicher zu kontrollieren. Weitere Informationen finden Sie unter [Lokale Verwendung von IAM](#).

16. April 2020

[Einführung einer neuen
Snowball Edge-Geräteoption
mit Speicheroptimierung \(für
Datenübertragung\)](#)

Snowball fügt jetzt ein neues speicheroptimiertes Gerät hinzu, das auf den aktuellen rechenoptimierten Geräten und GPU-Geräten basiert. Weitere Informationen finden Sie unter [Snowball Edge-Geräteoptionen](#).

23. März 2020

[Unterstützung für die Validierung von NFC-Tags](#)

In Snowball Edge Compute Optimized Geräte (mit oder ohne GPU) sind NFC-Tags integriert. Sie können diese Tags mit der AWS Snowball Edge Verifizierungs-App scannen, die auf Android verfügbar ist. Weitere Informationen finden Sie unter [Validieren von NFC-Tags](#).

13. Dezember 2018

[Sicherheitsgruppen sind
jetzt für Compute-Instances
verfügbar](#)

Sicherheitsgruppen in Snowball Edge-Geräten ähneln den Sicherheitsgruppen in der AWS Cloud, mit einigen subtilen Unterschieden. Weitere Informationen finden Sie unter [Sicherheitsgruppen auf Snowball Edge-Geräten](#).

26. November 2018

Wir stellen das lokale Update vor	Sie können jetzt die Software aktualisieren, mit der ein Snowball Edge-Gerät in Ihrer lokalen Umgebung ausgeführt wird. Beachten Sie, dass für lokale Aktualisierungen eine Internetverbindung benötigt wird. Weitere Informationen finden Sie unter Snowball Edge aktualisieren .	26. November 2018
Einführung neuer Geräteoptionen für Snowball Edge	Snowball Edge-Geräte gibt es in drei Optionen: speicheroptimiert, rechenoptimiert und mit GPU. Weitere Informationen finden Sie unter Snowball Edge-Geräteoptionen .	15. November 2018
Neu unterstützt AWS-Region	Snowball Edge-Geräte sind jetzt im asiatisch-pazifischen Raum (Mumbai) erhältlich. Beachten Sie, dass Compute-Instances und AWS Lambda Powered By AWS IoT Greengrass in dieser Region nicht unterstützt werden.	24. September 2018
Einführung der Unterstützung für EC2 Amazon-kompatible Recheninstanzen auf Snowball Edge-Geräten	AWS Snowball Edge unterstützt jetzt lokale Jobs mit EC2 Amazon-Compute-Instances , die auf Snowball Edge-Geräten ausgeführt werden.	17. Juli 2018
Der Inhalt zur Fehlerbehebung wurde verbessert	Die Kapitel "Fehlerbehebung" wurde aktualisiert und neu organisiert.	11. Juli 2018

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.