aws

Unable to locate subtitle

AWS Snowball Edge Entwicklerhandbuch

AWS Snowball Edge Entwicklerhandbuch: ***Unable to locate subtitle***

Table of Contents

Was ist AWS Snowball Edge?

AWS Snowball Edge ist eine Art von Snowball-Gerät mit integriertem Speicher und Rechenleistung für ausgewählte AWS Funktionen. Snowball Edge kann zusätzlich zur Übertragung von Daten zwischen Ihrer lokalen Umgebung und der lokale Verarbeitung und Edge-Computing-Workloads ausführen AWS Cloud.

Jedes Snowball Edge-Gerät kann Daten schneller als das Internet transportieren. Die Daten werden in den Appliances durch einen regionalen Kurierdienst transportiert. Die Appliances sind mit E-Ink-Versandetiketten ausgestattet.

Snowball-Edge-Geräte haben vier Optionen für Gerätekonfigurationen – speicheroptimiert, rechneroptimiert und rechneroptimiert mit GPU . Wenn sich dieses Handbuch auf Snowball Edge-Geräte bezieht, bezieht es sich auf alle Optionen des Geräts. Wenn bestimmte Informationen nur für eine oder mehrere optionale Konfigurationen von Geräten gelten (z. B. wie der Snowball Edge mit GPU über eine integrierte GPU verfügt), wird er speziell aufgerufen. Weitere Informationen finden Sie unter Optionen für Snowball Edge-Geräte.

Themen

AWS Snowball Edge-Funktionen

Snowball Edge-Geräte verfügen über die folgenden Funktionen:

- Große Mengen an Speicherkapazität oder Rechenfunktionalität für Geräte. Dies hängt von den Optionen ab, die Sie beim Erstellen Ihres Auftrags auswählen.
- Netzwerkadapter mit Übertragungsgeschwindigkeiten von bis zu 100 Gbit/Sekunde.

- 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 nutzen.
- Snowball-Edge-Geräte sind ihr eigenes Schutzfeld. Die integrierte E-Ink-Anzeige ändert sich und zeigt Ihr Versandetikett an, wenn das Gerät einsatzbereit ist.
- Snowball Edge-Geräte verfügen über ein integriertes Display, mit dem Sie Netzwerkverbindungen verwalten und Servicestatusinformationen abrufen können.
- Sie können Snowball Edge-Geräte für lokale Speicher- und Datenverarbeitungsaufträge clustern, um die 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 Amazon EC2-kompatible Endpunkte, was programmgesteuerte Anwendungsfälle ermöglicht.
- Snowball Edge-Geräte unterstützen die neuen Instance-`sbe-g`Typen `sbe-c`, und `sbe1`, mit denen Sie Rechen-Instances auf dem Gerät mithilfe von Amazon Machine Images (AMIs) ausführen können.
- Snowball Edge unterstützt die folgenden Datenübertragungsprotokolle für die Datenübertragung:
  - NFSv3
  - NFSv4
  - NFSv4.1
  - Amazon S3 über HTTP oder HTTPS (über API kompatibel mit AWS CLI-Version 1.16.14 und früher)

Voraussetzungen für die Verwendung von Snow Family-Geräten

Registrieren Sie sich für ein AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um eines zu erstellen.

So registrieren Sie sich für ein AWS-Konto

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

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

   Wenn Sie sich für ein registrieren AWS-Konto, Root-Benutzer des AWS-Kontos wird ein 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 eine Bestätigungs-E-Mail, nachdem der Registrierungsprozess abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

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

Schützen Ihrer Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console 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 Administratorbenutzers

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 Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Konfigurieren des Benutzerzugriffs mit dem Standard IAM-Identity-Center-Verzeichnis- im AWS IAM Identity Center -Benutzerhandbuch.

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 unter Anmelden beim - AWS Zugriffsportal im AWS-Anmeldung -Benutzerhandbuch.

Voraussetzungen für die Verwendung des Amazon S3-Adapters auf Snow-Family-Geräten für Import- und Exportaufträge

Sie verwenden den S3-Adapter auf Snow Family-Geräten, wenn Sie die Geräte verwenden, um Daten von On-Premises-Datenquellen in die Cloud oder von der Cloud in den On-Premises-Datenspeicher zu verschieben.

> **Note**
>
> Sie müssen den S3-Adapter auf Snow auswählen, wenn Sie Geräte bestellen. Siehe Schritt 2: Wählen Sie Ihre Datenverarbeitungs- und Speicheroptionen in diesem Handbuch.

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

Gehen Sie für Aufträge, 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. Alle 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 Ihrer großen Übertragung.

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 Exportbereichen.
- Ändern Sie für alle Dateien mit einem Doppelpunkt (`:`) im Dateinamen die Dateinamen in Amazon S3, bevor Sie den Exportauftrag erstellen, um diese Dateien abzurufen. Dateien mit einem Doppelpunkt im Dateinamen werden nicht zu Microsoft Windows Server exportiert.

Voraussetzungen für die Verwendung von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten

Sie verwenden Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten, wenn Sie Daten auf dem Gerät an Ihrem Edge-Standort speichern und die Daten für lokale Datenverarbeitungsvorgänge verwenden. Um Daten zu oder von zu migrieren AWS, richten Sie einen Export- oder Importauftrag ein und verwenden Sie den Amazon S3-Adapter.

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

- Sie stellen Amazon S3-Speicherkapazität bereit, wenn Sie das Gerät bestellen. Berücksichtigen Sie daher Ihren Speicherbedarf, bevor Sie ein Gerät bestellen.
- Sie können Amazon S3-Buckets auf dem Gerät erstellen, nachdem Sie es erhalten haben, anstatt ein Snow-Family-Gerät zu bestellen.
- Sie müssen die neueste Version des AWS CLI (v2.11.15 oder höher), des Snowball-Edge-Clients oder herunterladen AWS OpsHub und auf Ihrem Computer installieren, um Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten zu verwenden.

- Nachdem Sie Ihr Gerät empfangen haben, konfigurieren, starten und verwenden Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten gemäß Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten in diesem Handbuch.

Voraussetzungen für die Verwendung von Datenverarbeitungs-Instances auf Snow-Family-Geräten

Für Aufträge, die Datenverarbeitungs-AMIs verwenden, müssen Sie ein AMI in Ihrem AWS-Konto haben und es muss sich um einen unterstützten Image-Typ handeln. Derzeit basieren unterstützte AMIs auf folgenden Betriebssystemen:

- Amazon Linux 2
- CentOS 7 (x86_64) – mit Updates für HVM
- Ubuntu 16.04 LTS – Xenial (HVM)
- Ubuntu 20.04 LTS – Focal
- 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 Import/Export unterstützt und werden lokal in AMIs ausgeführt.

Sie können diese Bilder von abrufenAWS Marketplace.

Wenn Sie SSH verwenden, um eine Verbindung zu den Instances herzustellen, die auf einem Snowball Edge ausgeführt werden, können Sie Ihr eigenes Schlüsselpaar verwenden oder eines auf dem Snowball Edge erstellen. Informationen zur Verwendung von AWS OpsHub zum Erstellen eines Schlüsselpaars auf dem Gerät finden Sie unter Arbeiten mit Schlüsselpaaren. Informationen zur Verwendung der AWS CLI zum Erstellen eines Schlüsselpaars auf dem Gerät finden Sie unter `create-key-pair` in Liste der unterstützten AmazonEC2-compatible AWS CLI Befehle auf einem

Snowball-Edge. Weitere Informationen zu Schlüsselpaaren und Amazon Linux 2 finden Sie unter Amazon EC2-Schlüsselpaare und Linux-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Informationen zur Verwendung von Datenverarbeitungs-Instances auf einem Gerät finden Sie unter Verwenden von Amazon EC2-compatibleInstances.

Services im Zusammenhang mit AWS Snowball Edge

Sie können ein - AWS Snowball Edge Gerät mit den folgenden verwandten AWS Services verwenden:

- Amazon S3-Adapter – Verwenden Sie für die programmgesteuerte Datenübertragung in und aus AWS mithilfe der Amazon S3-API für Snowball Edge, die eine Teilmenge von Amazon S3-API-Operationen unterstützt. In dieser Rolle werden Daten von AWS in Ihrem Namen an das Snow-Gerät übertragen und das Gerät wird an Sie geliefert (für einen Exportauftrag) oder AWS sendet Ihnen ein leeres Snow-Gerät, und Sie übertragen Daten aus Ihren On-Premises-Quellen an das Gerät und senden sie zurück an AWS (für einen Importauftrag)“
- Amazon S3-kompatibler Speicher auf Snow Family-Geräten – Verwenden Sie , um die Datenanforderungen von Computing-Services wie Amazon EC2, Amazon EKS Anywhere in Snow und anderen zu erfüllen. Diese Funktion ist auf Snowball-Edge-Geräten verfügbar und bietet ein erweitertes Amazon S3-API-Set und Funktionen wie erhöhte Ausfallsicherheit mit flexibler Cluster-Einrichtung für 3 bis 16 Knoten, lokale Bucket-Verwaltung und lokale Benachrichtigungen.
- Amazon EC2 – Führen Sie Rechen-Instances auf einem Snowball Edge-Gerät mit dem Amazon EC2-kompatiblen Endpunkt aus, der eine Teilmenge der Amazon EC2-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 in Snow – Erstellen und betreiben Sie Kubernetes-Cluster auf Snow-Family-Geräten. Siehe Verwenden von Amazon EKS Anywhere in AWS Snow.
- AWS Lambda powered by AWS IoT Greengrass – Rufen Sie Lambda-Funktionen auf der Grundlage von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten auf, die auf einem - AWS Snowball Edge Gerät ausgeführt wurden. Weitere Informationen zur Verwendung von Lambda finden Sie unter Verwendung von AWS Lambda mit AWS Snowball Edge und im AWS Lambda -Entwicklerhandbuch.

- Amazon Elastic Block Store (Amazon EBS) – Stellen Sie Volumes für die Speicherung auf Blockebene für die Verwendung mit EC2-compatible 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 - AWS Ressourcen sicher zu steuern. Weitere Informationen finden Sie unter Was ist IAM?
- AWS Security Token Service (AWS STS) – Fordern Sie temporäre Anmeldeinformationen mit eingeschränkten Berechtigungen 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 in anzuzeigen und zu steuern AWS. Weitere Informationen finden Sie unter Was ist AWS Systems Manager?

Zugriff auf den Service

Sie können entweder die Managementkonsole für die AWS Snow-Familie oder die Job Management-API zum Erstellen und Verwalten von Aufträgen verwenden. Weitere Informationen zur Auftragsverwaltungs-API finden Sie in der Auftragsverwaltungs-API-Referenz für AWS Snowball.

Zugreifen auf ein AWS Snowball Edge -Gerät

Nachdem Ihr Snowball-Edge-Gerät vor Ort ist, können Sie es mit einer IP-Adresse über den Bol-Bildschirm konfigurieren und das Gerät mit dem Snowball-Edge-Client oder entsperren AWS OpsHub for Snow Family. Anschließend können Sie Datenübertragungs- oder Edge-Computing-Aufgaben ausführen. Weitere Informationen finden Sie unter Verwenden eines AWS Snowball Edge-Geräts.

Preise für Edge AWS Snowball

Informationen zu den Preisen und Gebühren für den Service und seine Geräte finden Sie unter -AWS Snowball Edge Preise.

Geräteüberwachung

AWS überwacht das Snow-Gerät und sammelt möglicherweise Metriken und Nutzungsinformationen, wenn das Snow-Gerät mit einem verbunden ist AWS-Region. Wenn das Snow-Gerät nicht mit dem verbunden ist AWS-Region, überwacht das Snow-Gerät AWS nicht.

Wenn ein irreparables Problem AWS erkennt und physische Geräte ersetzt werden müssen, AWS werden Sie von benachrichtigt. Anschließend können Sie einen Ersatzauftrag platzieren, den wir an Ihren Standort senden werden. Dafür fallen keine zusätzlichen Gebühren an, da die Überwachung von Snow-Geräten in der Servicegebühr für Snow-Geräte enthalten ist.

Verwenden Sie zum ersten Mal AWS Snowball ?

Wenn Sie den AWS Snow Family-Service zum ersten Mal verwenden, empfehlen wir Ihnen, nacheinander die folgenden Abschnitte zu lesen:

1. Weitere Informationen zu Gerätetypen und Optionen finden Sie unter AWS Snowball Edge-Geräteunterschiede.
2. Weitere Informationen zu den Arten von Aufträgen finden Sie unter Grundlegendes zu AWS Snowball-Edge-Aufträgen.
3. Eine end-to-end Übersicht über die Verwendung eines - AWS Snowball Edge Geräts finden Sie unter Funktionsweise von AWS Snowball Edge.
4. Wenn Sie bereit sind, sehen Sie sich Erste Schritte an.
5. Informationen zur Verwendung von Datenverarbeitungs-Instances auf einem Gerät finden Sie unter Verwenden von Amazon EC2-compatibleInstances.

AWS Snowball Edge-Geräteunterschiede

Dieses Handbuch enthält Dokumentation für Snowball Edge-Geräte. Sie können diese Geräte verwenden, um Terabyte an Daten in und aus Amazon S3 zu verschieben. Sie können sie über die Auftragsverwaltungs-API oder die AWS Snow Family-Konsole bestellen. Häufig gestellte Fragen und Preisinformationen finden Sie unter AWS Snowball.

Themen

- Optionen für Snowball Edge-Geräte
- AWS Snow Family Unterschiede im Anwendungsfall
- AWS Unterschiede im Snow Family Tool

Optionen für Snowball Edge-Geräte

Snowball Edge-Geräte haben die folgenden Optionen für Gerätekonfigurationen:

- Speicheroptimiert für Snowball Edge (für Datenübertragung) – Diese Snowball Edge-Geräteoption verfügt über 80 TB nutzbare Speicherkapazität.
- Snowball Edge speicheroptimiert 210 TB – Diese Snowball Edge-Geräteoption verfügt über 210 TB nutzbare Speicherkapazität.
- Speicheroptimiert für Snowball Edge (mit EC2-compatible Rechenfunktionalität) – Diese Snowball Edge-Geräteoption verfügt über bis zu 80 TB nutzbare Speicherkapazität, 40 vCPUs und 80 GB Arbeitsspeicher für Rechenfunktionen. Es verfügt auch über 1 TB zusätzlichen SSD-Speicherplatz für Block-Volumes, die an AmazonEC2-compatible AMIs angeschlossen sind.
- Snowball Edge-Datenverarbeitungsoptimiert – Dieses Snowball Edge-Gerät (mit AMD EPYC Gen2) verfügt über die meisten Rechenfunktionen, mit bis zu 104 vCPUs, 416 GB Arbeitsspeicher und 28 TB dedizierter NVMe-SSD für Datenverarbeitungs-Instances.

  Für die Datenverarbeitung von Snowball Edge optimiert (mit AMD EPYC Gen1) sind bis zu 52 vCPUs, 208 GB Arbeitsspeicher, 39,5 TB nutzbare Speicherkapazität und 7,68 TB dedizierte NVMe-SSD für Datenverarbeitungs-Instances verfügbar.
- Snowball-Edge-Datenverarbeitung optimiert mit GPU – Diese Snowball-Edge-Geräteoption ist identisch mit der für Datenverarbeitung optimierten Option (mit AMD EPYC Gen1) und enthält eine installierte Grafikverarbeitungseinheit (GPU). Die GPU entspricht der GPU, die im Amazon-EC2-kompatiblen P3-Instance-Typ verfügbar ist. EC2-compatible

> **Note**
>
> Wenn Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten auf diesen Geräten verwenden, variiert der nutzbare Speicher. Weitere Informationen finden Sie unter Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten auf Snow-Family-Geräten für die Speicherkapazität mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.

Weitere Informationen über die Datenverarbeitungsfunktionalität dieser drei Optionen finden Sie unter Verwenden von Amazon EC2-compatibleInstances. Unterschiede bei der Auftragserstellung und der Festplattenkapazität in Terabyte werden hier beschrieben.

> **Note**
>
> Wenn wir auf Snowball Edge-Geräte verweisen, umfasst dies alle optionalen Varianten des Geräts. Wenn Informationen für eine oder mehrere bestimmte optionale Konfigurationen gelten (z. B. wie die für die Datenverarbeitung von Snowball Edge optimierte mit der GPU-Option über einen integrierten GPU-Kabel verfügt), wird dies explizit erwähnt.

In der folgenden Tabelle werden die Unterschiede zwischen den verschiedenen Geräteoptionen zusammengefasst. Informationen zu Hardwarespezifikationen finden Sie unter AWS Snowball Edge-Gerätespezifikationen.

	Speicheroptimiert für Snowball Edge (für Datenübertragung)	Speicheroptimiert für Snowball Edge 210 TB	Speicheroptimiert für Snowball Edge (mit EC2-Rechenfunktionalität)	Snowball Edge-Datenverarbeitungsoptimiert mit AMD EPYC Gen2 und NVME	Snowball Edge-Datenverarbeitung optimiert mit AMD EPYC Gen1, HDD und optionaler GPU
CPU	AMD Naples, 32 Cores, 3,4 GHz	AMD Kere, 64 Kerne, 2 GHz	AMD Naples, 32 Cores, 3,4 GHz	AMD Kere, 64 Kerne, 2 GHz	AMD Naples, 32 Cores, 3,4 GHz
vCPUs	40	104	40	104	52
Verwendbarer Speicher	80 GB	416 GB	80 GB	416 GB	208 GB
Sicherheitskarte	Ja	Ja	Ja	Ja	Ja
GPU (optional)	Keine	Keine	Keine	None	NVidia V100
SSD	1 TB SATA	210 TB NVMe	1 TB SATA	28 TB NVMe	7,68 TB NVMe

	Speicheroptimiert für Snowball Edge (für Datenübertragung)	Speicheroptimiert für Snowball Edge 210 TB	Speicheroptimiert für Snowball Edge (mit EC2-Rechenfunktionalität)	Snowball Edge-Datenverarbeitungsoptimiert mit AMD EPYC Gen2 und NVME	Snowball Edge-Datenverarbeitungoptimiert mit AMD EPYC Gen1, HDD und optionaler GPU
Verwendbare Festplatte	80 TB	Nicht zutreffend	80 TB	Nicht zutreffend	39,5 TB verwendbar
Netzwerkschnittstellen	• 2x 10 Gbit – RJ45 (ein verwendbar) • 1x 25 Gbit – SFP28 • 1x 100 Gbit – QSFP28	• 2x 10 Gbit – RJ45 (ein verwendbar) • 1x 25 Gbit – SFP28 • 1x 100 Gbit – QSFP28	• 2x 10 Gbit – RJ45 (ein verwendbar) • 1x 25 Gbit – SFP28 • 1x 100 Gbit – QSFP28	• 2x 10 Gbit – RJ45 (ein verwendbar) • 1x 25 Gbit – SFP28 • 1x 100 Gbit – QSFP28	• 2x 10 Gbit – RJ45 (ein verwendbar) • 1x 25 Gbit – SFP28 • 1x 100 Gbit – QSFP28

	Speicheroptimiert für Snowball Edge (für Datenübertragung)	Speicheroptimiert für Snowball Edge 210 TB	Speicheroptimiert für Snowball Edge (mit EC2-Rechenfunktionalität)	Snowball Edge-Datenverarbeitungsoptimiert mit AMD EPYC Gen2 und NVME	Snowball Edge-Datenverarbeitungoptimiert mit AMD EPYC Gen1, HDD und optionaler GPU
Physische Sicherheitsfunktionen	• Versteckte Magnetschrauben • Eindringungsschalter • NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • GPS und Mobilfunk • Konforme Beschichtung	• Versteckte Magnetschrauben • Eindringungsschalter • NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • Konforme Beschichtung	• Versteckte Magnetschrauben • Eindringungsschalter • NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • GPS und Mobilfunk • Konforme Beschichtung	• Versteckte Magnetschrauben • Eindringungsschalter • NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • Konforme Beschichtung	• Versteckte Magnetschrauben • Eindringungsschalter • NFC-Tags • Antimanipulationseinsätze • Android-App zur Manipulationserkennung • Konforme Beschichtung

AWS Snow Family Unterschiede im Anwendungsfall

Die folgende Tabelle zeigt die Anwendungsfälle für die verschiedenen AWS Snow Family devices.

Anwendungsfall	Snowball-Edge	AWS Snowcone	
Importieren von Daten in Amazon S3	✓	✓	
Exportieren aus Amazon S3	✓		
Dauerhafter lokaler Speicher	✓		
Lokale Datenverarbeitung mit AWS Lambda	✓	✓	
Lokale Datenverarbeitungs-Instances	✓	✓	
Kabelloser Amazon S3-Speicher in einem Gerätecluster	✓		
Verwenden von mit AWS IoT Greengrass (IoT)	✓	✓	
Übertragen von Dateien über NFS mit einer GUI	✓	✓	
GPU-Workloads	✓		

Note

Für Workloads, die GPU-Unterstützung benötigen, ist die für die Datenverarbeitung optimierte Snowball Edge mit GPU-Option erforderlich.

Speicheroptimierte 210TB für Snowball Edge unterstützen die Datenübertragung über NFS, S3-Adapter und Amazon S3-kompatiblen Speicher auf Geräten der Snow Family.

AWS Unterschiede im Snow Family Tool

Im Folgenden werden die verschiedenen Tools beschrieben, die mit den Snow Family-Geräten verwendet werden, und wie sie verwendet werden.

Snowball-Edge-Tools

AWS OpsHub for Snow Family

- Geräte der Snow Family bieten jetzt ein benutzerfreundliches Tool namens AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen AWS Services verwalten können. Sie können AWS OpsHub auf einem Client-Computer verwenden, um Aufgaben wie das Entsperren und Konfigurieren einzelner oder gruppierter Geräte, das Übertragen von Dateien und das Starten und Verwalten von Instances auszuführen, die auf Snow-Family-Geräten ausgeführt werden. Weitere Informationen finden Sie unter Verwenden von AWS OpsHub for Snow Family zur Verwaltung von Snowball-Geräten.

Snowball Edge-Client mit Snowball Edge

- Laden Sie den Snowball Edge-Client von der Seite AWS Snowball Edge Ressourcen herunter und installieren Sie ihn auf Ihrem eigenen Computer.
- Verwenden Sie den Snowball Edge-Client, um den Snowball Edge oder den Cluster von Snowball Edge-Geräten zu entsperren. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients.
- Sie können den Snowball Edge-Client nicht verwenden, um Daten zu oder von Snow Family-Geräten zu übertragen.

Amazon S3-Adapter mit Snowball Edge

- Verwenden Sie den Amazon S3-Adapter für die Datenübertragung zu oder von AWS.
- Ist standardmäßig bereits auf dem Snowball Edge für Export- oder Importaufträge installiert. Muss nicht heruntergeladen oder installiert werden.

- Kann Daten an oder vom Snowball Edge übertragen. Weitere Informationen finden Sie unter Übertragen von Dateien mit dem Amazon S3-Adapter für die Datenmigration.
- Verschlüsselt Daten auf dem Snowball Edge, während die Daten auf das Gerät übertragen werden.

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten

- Verwenden Sie Amazon S3-kompatiblen Speicher auf Geräten der Snow Family für Edge-Datenverarbeitungs- und Speichervorgänge.
- Der Amazon S3-kompatible Speicher auf Snow-Family-Geräten wird auf einem Snowball-Edge-Gerät installiert, wenn er während der Auftragserstellung ausgewählt wird. Informationen zum Konfigurieren, Starten und Verwenden des Services finden Sie unter Amazon S3-kompatibler Speicher auf Snow-Family-Geräten in diesem Handbuch.

AWS IoT Greengrass -Konsole mit Snowball Edge

- Mit einem Snowball Edge können Sie die AWS IoT Greengrass Konsole verwenden, um Ihre AWS IoT Greengrass Gruppe und den Core zu aktualisieren, der auf dem Snowball Edge ausgeführt wird.

Für Snowball Edge bereitgestellte Elemente

Im Folgenden werden die Netzwerkadapter, verwendeten Kabel und Kabel beschrieben, die für das Snowball Edge-Gerät bereitgestellt werden.

Netzwerkschnittstelle	Snowball Edge-Unterstützung	Kabel, die mit dem Gerät bereitgestellt werden	
RJ45	✓	Nicht angegeben.	
SFP28	✓	Nicht angegeben.	
SFP28 (mit Trichter-Konnektor)	✓	Es werden keine Kabel bereitgestellt. Für Snowball-Edge-Geräte wird kein	

Netzwerkschnittstelle	Snowball Edge-Unterstützung	Kabel, die mit dem Gerät bereitgestellt werden	
		Trichter-Konnektor bereitgestellt.	
QSFP	✓	Es werden keine Kabel oder Kabel bereitgestellt.	

Weitere Informationen zu den Netzwerkschnittstellen, Kabeln und Konnektoren finden Sie unter Unterstützte Netzwerkhardware.

Funktionsweise von AWS Snowball Edge

AWS Snowball Edge-Geräte gehören und befinden sich an Ihrem On-Premises-Standort AWS, während sie verwendet werden.

Es gibt vier Auftragstypen, die Sie mit einem - AWS Snowball Edge Gerät verwenden können. Die Auftragstypen unterscheiden sich zwar in ihren Anwendungsfällen, doch verfügt jeder Auftragstyp über denselben Workflow zum Bestellen, Empfangen und Zurückgeben von Geräten. Unabhängig vom Auftragstyp folgt jeder Auftrag einer Datenlöschung des Standards des National Institute of Standards and Technology (NIST) 800-88, nachdem der Auftrag abgeschlossen ist.

Der gemeinsame Workflow

1. Erstellen des Auftrags – Jeder Auftrag wird in der Managementkonsole für die AWS Snow-Familie oder programmgesteuert über die Auftragsverwaltungs-API erstellt. Der Status eines Auftrags kann in der Konsole oder über die API verfolgt werden.
2. Ein Gerät ist für Ihren Auftrag vorbereitet – Wir bereiten ein AWS Snowball Edge Gerät für Ihren Auftrag vor und der Status Ihres Auftrags lautet jetzt Vorbereiten von Snowball.
3. Ein Gerät wird Ihnen vom Mobilfunkanbieter Ihrer Region zugestellt – Der Mobilfunkanbieter übernimmt von hier aus und der Status Ihres Auftrags lautet jetzt In Übertragung 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 von Snow-Family-Geräten.
4. Empfangen des Geräts – Einige Tage später übermittelt der Mobilfunkanbieter Ihrer Region das AWS Snowball Edge Gerät an die Adresse, die Sie beim Erstellen des Auftrags angegeben haben, und der Status Ihres Auftrags ändert sich in An Sie gesendet. Das Gerät wird nicht in einem Paket angeliefert, da das Gerät einen eigenen Transportbehälter umfasst.
5. Abrufen Ihrer Anmeldeinformationen und Herunterladen des Snowball Edge-Clients – Bereiten Sie sich auf die Übertragung von Daten vor, 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 On-Premises-Datenziel verwalten.

Sie können den Snowball Edge-Client von der AWS Snowball 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. Positionieren der Hardware – Verschieben Sie das Gerät in Ihr Rechenzentrum und öffnen Sie es gemäß den Anweisungen für den Fall. Schließen Sie das Gerät an eine Stromquelle an und verbinden Sie sie mit Ihrem lokalen Netzwerk.
7. Einschalten des Geräts – Schalten Sie als Nächstes das Gerät ein, indem Sie die Einschalttaste über der-Anzeige drücken. Nach einigen Minuten erscheint im Display die Meldung Ready (Bereit).
8. Abrufen der IP-Adresse für das Gerät – Auf der Bol-Anzeige befindet sich eine Registerkarte CONNECTION. Gehen Sie auf diese Registerkarte und rufen Sie die IP-Adresse für das AWS Snowball Edge Gerät ab.
9. Verwenden des Snowball Edge-Clients zum Entsperren des Geräts – Wenn Sie den Snowball Edge-Client zum Entsperren des AWS Snowball Edge Geräts verwenden, geben Sie die IP-Adresse des Geräts, den Pfad zu Ihrem Manifest und den Entsperrcode ein. Der Snowball Edge-Client entschlüsselt das Manifest und verwendet es, um Ihren Zugriff auf das Gerät zu authentifizieren.
10. Verwenden des Geräts – Das Gerät ist betriebsbereit. Sie können damit Daten mit dem Amazon S3-Adapter oder dem Network File System (NFS)-Mountingpunkt oder für die lokale Datenverarbeitung und Speicherung mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten übertragen.
11. Vorbereiten des Geräts auf seinen Rücklauf – Nachdem Sie mit dem Gerät an Ihrem On-Premises-Standort fertig sind, drücken Sie die Einschalttaste über der Bol-Anzeige. 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.

12 Der Mobilfunkanbieter Ihrer Region gibt das Gerät an zurück AWS – Wenn der Mobilfunkanbieter über das AWS Snowball Edge Gerät verfügt, wird der Status des Auftrags auf „Übertragung an“ AWS gesetzt.

> **Note**
>
> Es gibt zusätzliche Schritte für Export- und Cluster-Aufträge. Weitere Informationen finden Sie unter Funktionsweise von Exportaufträgen und Funktionsweise eines gruppierten lokalen Datenverarbeitungs- und Speicherauftrags.

Themen

Funktionsweise von Importaufträgen

Jeder Importauftrag verwendet eine einzelne Snowball-Appliance. Nachdem Sie einen Auftrag erstellt haben, um ein Snow Family-Gerät in der Managementkonsole für die AWS Snow-Familie oder der Auftragsverwaltungs-API zu bestellen, senden wir Ihnen einen Snowball zu. Wenn es innerhalb weniger Tage eintrifft, 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 Übertragung von Daten fertig sind, senden Sie den Snowball zurück an und AWS wir importieren Ihre Daten in Amazon S3.

Funktionsweise von Exportaufträgen

Jeder Exportauftrag kann eine beliebige Anzahl von AWS Snowball Edge-Geräten verwenden. Wenn die Auflistung mehr Daten enthält, als auf ein einzelnes Gerät passen kann, 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 Vorbereiten von Snowball.

> **Note**
>
> Der Auflistungsvorgang, der zum Teilen Ihres Auftrags verwendet wird, ist eine Funktion von Amazon S3, und Ihnen wird dieser genauso in Rechnung gestellt wie jeder Amazon S3-Vorgang.

Kurz darauf beginnen wir mit dem Exportieren Ihrer Daten in ein Gerät. Die zum Exportieren Ihrer Daten erforderliche Zeit hängt von der Art Ihres Datensatzes ab. Beispielsweise dauert der Export vieler kleiner Dateien (weniger als 10 MB) erheblich länger. Wenn der Export abgeschlossen ist, AWS wird das Gerät von der Fluggesellschaft Ihrer Region abgeholt. Wenn es eintrifft, verbinden Sie das AWS AWS Snowball Edge Gerät mit Ihrem Netzwerk und übertragen die Daten vom Gerät in den Speicher in Ihrem Netzwerk.

Wenn Sie mit der Übertragung von Daten fertig sind, senden Sie das Gerät zurück an AWS. Wenn wir das Gerät für Ihren Exportauftrag erhalten, 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 Schlüsselliste

  Bevor wir die Objekte im S3-Bucket exportieren, scannen wir den Bucket. Wenn der Bucket nach dem Scan geändert wird, kann es beim Auftrag zu Verzögerungen kommen, da wir nach fehlenden oder geänderten Objekten suchen.
- Für S3 Glacier Flexible Retrieval

  Es ist wichtig zu beachten, dass Objekte in der Speicherklasse S3 Glacier nicht exportieren AWS Snowball kann. Diese Objekte müssen wiederhergestellt werden, bevor die Objekte im Bucket erfolgreich exportieren AWS Snowball kann.

Funktionsweise von lokalen Datenverarbeitungs- und Speicheraufträgen

Sie können die lokale Rechen- und Speicherfunktionalität eines - AWS Snowball Edge Geräts verwenden, indem Sie AWS EC2-compatible Rechen-Instances oder Kubernetes-Container in Amazon EKS Anywhere in Snow ausführen. Für Rechenfunktionen wird die Datenspeicherung durch Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten bereitgestellt.

Sie können Amazon S3-Buckets auf den Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte an zurückgegeben werden AWS, werden alle Daten, die im Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten erstellt oder gespeichert werden, gelöscht. Weitere Informationen finden Sie unter Lokale Datenverarbeitungs- und reine Speicheraufträge.

Weitere Informationen finden Sie unter Rein lokale Datenverarbeitungs- und Speicheraufträge.

Funktionsweise eines gruppierten lokalen Datenverarbeitungs- und Speicherauftrags

Ein Cluster-Auftrag ist eine spezielle Art von Auftrag nur für die lokale Speicherung und Datenverarbeitung. Sie ist für Workloads gedacht, die eine höhere Datenbeständigkeit und Speicherkapazität erfordern. Weitere Informationen finden Sie unter Lokale Cluster-Option.

> **Note**
>
> Wie eigenständige lokale Speicher- und Datenverarbeitungsaufträge 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-Auftrags importieren.

Cluster verfügen über 3 bis 16 AWS Snowball Edge-Geräte, die als Knoten bezeichnet werden. 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 Entsperrungsbefehl zu entsperren, wobei Sie die IP-Adresse eines der Knoten verwenden. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients.

Sie können Daten in einen entsperrten Cluster schreiben, indem Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten 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 Cluster-Knoten erhalten, führen wir eine vollständige Löschung des Snowball durch. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Snowball-Edge-Videos und -Blogs

- Migrieren gemischter Dateigrößen mit auf snow-transfer-tool 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.
- Aktivieren Sie umfangreiche Datenbankmigrationen mit DMS und AWS Snowball
- Bewährte Methoden für die Datenmigration mit AWS Snowball Edge
- AWS Snowball Ressourcen
- Amazon S3-kompatibler Speicher auf AWS Snowball Edge-Computing-optimierten Geräten jetzt allgemein verfügbar
- Erste Schritte mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten auf AWS Snowball-Edge-Geräten

AWS Snowball Edge-Gerätespezifikationen

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

Themen

Spezifikationen für Snowball Edge Storage Optimized (für Datenübertragung)

Die folgende Tabelle enthält Hardwarespezifikationen für Snowball Edge Storage Optimized-Geräte.

Item	Spezifikationen für Snowball Edge Storage Optimized (für Datenübertragung)
Speicherspezifikationen	
HDD-Speicherkapazität	80 TB verwendbar
Spezifikationen für die Stromversorgung	
Stromversorgung	In AWS-Regionen den USA: Bol 5–15p 100–220 . In allen AWS Regionen ist ein Stromkabel enthalten
Stromverbrauch	304 Watt für einen durchschnittlichen Anwendungsfall, obwohl die Stromversorgung auf 1200 Watt ausgelegt ist.
Spannung	100 – 240 V AC

Item	Spezifikationen für Snowball Edge Storage Optimized (für Datenübertragung)
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit – RJ45 (ein verwendbar) 1x 25 Gbit – SFP28 1x 100 Gbit – QSFP28
Kabel	Jedes AWS Snowball Edge Gerät liefert länderspezifische Stromkabel. Es werden keine weiteren Kabel oder optischen Stecker mitgeliefert. Weitere Informationen finden Sie unter Unterstützte Netzwerkhardware.
Thermische Anforderungen	AWS Snowball Edge-Geräte sind für den Betrieb im Büro konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät 68 Dezibel, die in der Regel lauter sind als ein Vakuumbereinigungsgerät oder eine Arzt-Raum-Audio.
Dimensionen und Gewichtungsspezifikationen	
Gewicht	22,54 Kilogramm
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Umgebungsspezifikationen	
Vibration	Nicht-betriebliche Verwendung entspricht Bol D4169 Truck Level I 0.73 GRMS

Item	Spezifikationen für Snowball Edge Storage Optimized (für Datenübertragung)
Schock	Betriebliche Verwendung entspricht 70G (MIL-S-901) Nicht-betriebliche Verwendung entspricht 50G (ISTA-3A)
Höhe	Betriebliche Nutzung entspricht 0–3 000 Metern (0–10 000 Fuß) Nicht-betriebliche Verwendung entspricht 0–12 000 Metern
Temperaturbereich	0–45°C (betrieblich)

Snowball Edge Storage Optimized 210 TB Spezifikationen

Die folgende Tabelle enthält Hardwarespezifikationen für Snowball Edge Storage Optimized 210 TB-Geräte.

Item	Snowball Edge Storage Optimized 210 TB Spezifikationen
Datenverarbeitungs- und Speicherspezifikationen	
CPU	104 vCPUs
RAM	416 GB
Speicherspezifikationen	
NVME-Speicherkapazität	210 TB verwendbar (für Objekt- und NFS-Datenübertragung)

Item	Snowball Edge Storage Optimized 210 TB Spezifikationen
SSD-Speicherkapazität	None
Spezifikationen für die Stromversorgung	
Stromversorgung	In AWS-Regionen den USA: Bol 5–15p 100–220 . In allen AWS Regionen ist ein Stromkabel enthalten
Stromverbrauch	304 Kers für einen durchschnittlichen Anwendungsfall, obwohl das Netzteil für 1200 Kers ausgelegt ist
Spannung	100 – 240 V AC
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit – RJ45 (ein verwendbar) 1x 25 Gbit – SFP28 1x 100 Gbit – QSFP28
Kabel	Jedes AWS Snowball Edge Gerät liefert länderspezifische Stromkabel. Es werden keine weiteren Kabel oder optischen Stecker mitgeliefert. Weitere Informationen finden Sie unter Unterstützte Netzwerkhardware.
Thermische Anforderungen	AWS Snowball Edge -Geräte sind für den Betrieb im Büro konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät 68 Dezibel, die in der Regel lauter sind als ein Vakuumbereinigungsgerät oder eine Arzt-Raum-Audio.
Dimensionen und Gewichtungsspezifikationen	
Gewicht	22,54 Kilogramm

Item	Snowball Edge Storage Optimized 210 TB Spezifikationen
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Umgebungsspezifikationen	
Vibration	Nicht-betriebliche Verwendung entspricht Bol D4169 Truck Level I 0.73 GRMS
Schock	Betriebliche Verwendung entspricht 70G (MIL-S-901) Nicht-betriebliche Verwendung entspricht 50G (ISTA-3A)
Höhe	Betriebliche Nutzung entspricht 0–3 000 Metern (0–10 000 Fuß) Nicht-betriebliche Verwendung entspricht 0–12 000 Metern
Temperaturbereich	0–30°C (betrieblich)

Snowball Edge Storage Optimized (mit EC2)-Spezifikationen

Die folgende Tabelle enthält Hardwarespezifikationen für Snowball Edge Storage Optimized (mit EC2)-Geräte.

Item	Snowball Edge Storage Optimized (mit EC2)-Spezifikationen
Datenverarbeitungs- und Speicherspezifikationen	
CPU	40 vCPUs
RAM	80 GiB

Item	Snowball Edge Storage Optimized (mit EC2)-Spezifikationen
Speicherspezifikationen	
HDD-Speicherkapazität	80 TB verwendbar (für Objekt- und Blockspeicher)
SSD-Speicherkapazität	1 TB verwendbarer SATA-SSD-Speicher (für Blockspeicher)
Spezifikationen für die Stromversorgung	
Stromversorgung	In AWS-Regionen den USA: Bol 5–15p 100–220 . In allen AWS Regionen ist ein Stromkabel enthalten
Stromverbrauch	304 Kers für einen durchschnittlichen Anwendungsfall, obwohl das Netzteil für 1200 Kers ausgelegt ist
Spannung	100 – 240 V AC
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit – RJ45 (ein verwendbar) 1x 25 Gbit – SFP28 1x 100 Gbit – QSFP28
Kabel	Jedes AWS Snowball Edge Gerät liefert länderspezifische Stromkabel. Es werden keine weiteren Kabel oder optischen Stecker mitgeliefert. Weitere Informationen finden Sie unter Unterstützte Netzwerkhardware.
Thermische Anforderungen	AWS Snowball Edge -Geräte sind für den Betrieb im Büro konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät 68 Dezibel, die in der Regel lauter sind als ein Vakuumbereinigungsgerät oder eine Arzt-Raum-Audio.

Item	Snowball Edge Storage Optimized (mit EC2)-Spezifikationen
Dimensionen und Gewichtungsspezifikationen	
Gewicht	22,54 Kilogramm
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Umgebungsspezifikationen	
Vibration	Nicht-betriebliche Verwendung entspricht Bol D4169 Truck Level I 0.73 GRMS
Schock	Betriebliche Verwendung entspricht 70G (MIL-S-901) Nicht-betriebliche Verwendung entspricht 50G (ISTA-3A)
Höhe	Betriebliche Nutzung entspricht 0–3 000 Metern (0–10 000 Fuß) Nicht-betriebliche Verwendung entspricht 0–12 000 Metern
Temperaturbereich	0–45°C (betrieblich)

Spezifikationen für für Computing-optimierte Snowball Edge-Geräte

Item	Spezifikationen für Snowball Edge Compute Optimized
Datenverarbeitungs- und Speicherspezifikationen	
CPU	Bis zu 104 vCPUs (verfügbar in Konfigurationen von 52 oder 104 vCPUs)

Item	Spezifikationen für Snowball Edge Compute Optimized
RAM	512 GB RAM (bis zu 416 GB RAM – vom Kunden verwendbar)
GPU	nVidia V100 (verfügbar in Compute Optimized with GPU configuration – nur mit 52 vCPU angeboten)
Speicherspezifikationen	
SSD-Speicherkapazität	28 TB NVMe SSD oder 42 TB HDD (39,5 TB verwendbar)
Spezifikationen für die Stromversorgung	
Stromversorgung	In AWS-Regionen den USA: Bol 5–15p 100–220 . In allen AWS Regionen ist ein Stromkabel enthalten
Stromverbrauch	304 Kers für einen durchschnittlichen Anwendungsfall, obwohl das Netzteil für 1200 Kers ausgelegt ist
Spannung	100 – 240 V AC
Häufigkeit	47/63 Hz
Daten- und Netzwerkverbindungen	2x 10 Gbit – RJ45 (ein verwendbar) 1x 25 Gbit – SFP28 1x 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 Unterstützte Netzwerkhardware.

Item	Spezifikationen für Snowball Edge Compute Optimized
Thermische Anforderungen	AWS Snowball Edge -Geräte sind für den Betrieb im Büro konzipiert und eignen sich ideal für den Betrieb von Rechenzentren.
Dezibel	Im Durchschnitt erzeugt ein AWS Snowball Edge Gerät 68 Dezibel, die in der Regel langsamer sind als ein Bereinigungsgerät oder Musik im Arztraum.
Dimensionen und Gewichtungsspezifikationen	
Gewicht	22,54 Kilogramm
Höhe	39,40 Zentimeter
Width	26,50 Zentimeter
Länge	71,80 Zentimeter
Umgebungsspezifikationen	
Vibration	Nicht-betriebliche Verwendung entspricht Bol D4169 Truck Level I 0.73 GRMS
Schock	Betriebliche Verwendung entspricht 70G (MIL-S-901) Nicht-betriebliche Verwendung entspricht 50G (ISTA-3A)
Höhe	Betriebliche Nutzung entspricht 0–3 000 Metern (0–10 000 Fuß) Nicht-betriebliche Verwendung entspricht 0–12 000 Metern
Temperaturbereich	0–45°C (betrieblich)

Unterstützte Netzwerkhardware

Um das AWS Snowball Edge Gerät verwenden zu können, benötigen Sie Ihre eigenen Netzwerkkabel. Für RJ45-Kabel gibt es keine besonderen Empfehlungen. Es wurde überprüft, ob SFP+- und QSFP+-Kabel und -Module von Kerlanox und Finisar mit dem Gerät kompatibel sind.

Nachdem Sie die Rückwand des AWS Snowball Edge Geräts geöffnet haben, sehen Sie die Netzwerkports ähnlich den Ports, die im folgenden Screenshot gezeigt werden.

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

SFP

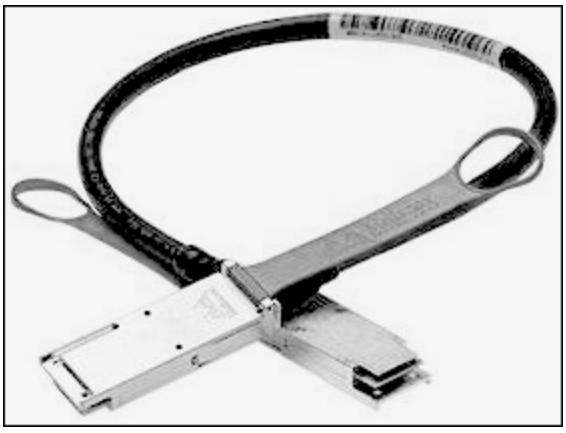
Dieser Anschluss bietet eine 10G/25G SFP28-Schnittstelle, die mit SFP28 und SFP+-Transceiver-Modulen und DAC-Kabeln (Direct-Attach Copper) kompatibel ist. Sie müssen Ihre eigenen Transceiver- oder DAC-Kabel bereitstellen.

- 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 eine beliebige SFP28+-Option verwenden. 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-Transceiver (Monomodefaser)
- 40Gbase-SR4-Transceiver (Multimodefaser)
- QSFP+ DAC

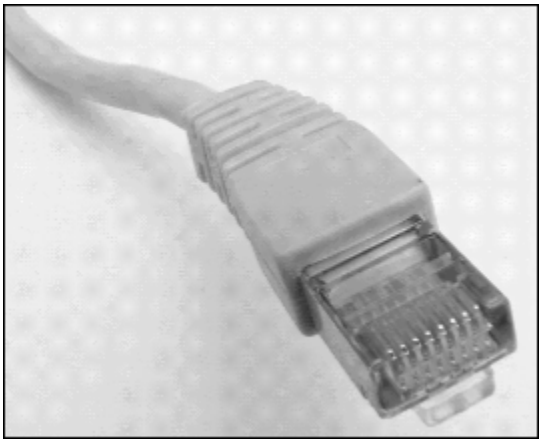


RJ45

Dieser Port unterstützt einen 1Gbase TX/10Gbase-TX-Betrieb. Es ist über ein UTP-Kabel mit einem RJ45-Anschluss verbunden. Snowball Edge-Geräte haben zwei RJ45-Ports. Wählen Sie einen Port aus, der verwendet werden soll.

1G-Betrieb wird durch eine gelb blinkende Lampe angezeigt. Die 1G-Operation wird für umfangreiche Datenübertragungen auf das Snowball Edge-Gerät nicht empfohlen, da sie die Zeit für die Datenübertragung erheblich erhöht.

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.



Langfristige Preise für Snowball-Edge-Geräte

Wenn Sie ein Snowball Edge-Gerät bestellen, können Sie die Preisoption wählen, die am besten zu Ihrem Anwendungsfall passt. Die Preise sind auf zwei Arten verfügbar: On-Demand für jeden Tag, an dem Sie das Gerät haben, oder für jeden Tag, an dem Sie über ein Gerät verfügen, langfristige Preise in monatlichen, ein- oder dreijährigen Laufzeiten, je nach Gerätetyp. Sie können Ihre langfristige Preisoption für ein- oder dreijährige Laufzeit automatisch verlängern, sodass eine neue Telefoniezeit beginnt, wenn der vorherige Zeitraum endet, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Die monatliche langfristige Preisoption wird automatisch verlängert, während sich das Gerät in Ihrem Besitz befindet. Weitere Informationen zum Bestellen eines Geräts finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts in diesem Leitfaden.

Neben der budgetären Bequemlichkeit können Sie mit den langfristigen Preisen Snowball Edge-Geräte während des Preiszeitraums austauschen, wenn sich Ihre betrieblichen Anforderungen ändern. Sie können beispielsweise anfordern, dass Geräte austauschen, sodass das neue Gerät ein neues AMI oder neue Daten von Amazon S3 enthält, oder ein ausgefallenes Gerät ersetzen. Siehe Geräte während des langfristigen Preiszeitraums austauschen.

> **Note**
>
> Wenn Sie beantragen, ein Snowball Edge-Gerät unter einem Commit-Preisplan für ein Jahr oder drei Jahre aus einem anderen Grund als Hardware oder einem Softwareproblem zu tauschen oder zu ersetzen, das dem AWS Snow-Service zugeordnet ist, wird Ihnen eine Gebühr für das Wechseln von Geräten in Rechnung gestellt. Diese Gebühr für das Kehren von Geräten wird als monatliche Gebühr (für Snowball Edge Compute Optimized) oder On-Demand-Auftragsgebühr für Ihre Konfiguration festgelegt.

Weitere Informationen zu langfristigen Preisen finden Sie unter Optimieren der Kosten mit langfristigen Preisoptionen für AWS Snowball. Die AWS Snowball Preise für Ihr finden Sie unter AWS-Region-AWS SnowballPreise.

Geräte während des langfristigen Preiszeitraums austauschen

Das Auslagern 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 Ersatz-Snowball-Edge-Gerät. Das Ersatzgerät muss für denselben Auftragstyp sein und dieselben Rechen- und Speicheroptionen haben wie das Gerät, das Sie haben. Weitere Informationen finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts in diesem Leitfaden.
2. Geben Sie sofort das Gerät zurück, das Sie haben. Siehe Ausschalten des Snowball Edge und Zurückgeben des Snowball Edge-Geräts. AWS verwaltet die Logistik für den Geräteaustausch, und für diesen Austausch wird eine Gebühr für den Geräteverkehr erhoben.

Einrichten Ihres AWS Zugriffs für AWS Snowball Edge

> **Note**
>
> Im Asien-Pazifik (Mumbai) wird der AWS-Region Service von Amazon in Internet Services Private Limited (AISPL) bereitgestellt. Informationen zur Registrierung für Amazon Web Services in der Asien-Pazifik (Mumbai) AWS-Region finden Sie unter Registrierung für AISPL.

Bei der Registrierung für Amazon Web Services (AWS) AWS-Konto wird Ihr automatisch für alle Services in registriert AWS, einschließlich AWS Snow Family. Berechnet werden Ihnen aber nur die Services, die Sie nutzen. Weitere Informationen zu Preisen und Gebühren finden Sie unter AWS Snowball Edge Preise. AWS Snowball Die Nutzung von Edge ist nicht kostenlos. Weitere Informationen zu AWS den Services, die kostenlos sind, finden Sie unter AWS Kostenloses Nutzungskontingent für .

Notieren Sie sich Ihre - AWS-Konto Nummer, da Sie sie benötigen, um einen Auftrag zum Bestellen eines Snowball Edge zu erstellen.

Services in AWS, wie Edge AWS Snowball , erfordern, dass Sie Anmeldeinformationen angeben, wenn Sie auf sie zugreifen, damit der Service bestimmen kann, ob Sie über die Berechtigung zum Zugriff auf seine Ressourcen verfügen. AWS rät davon ab, die Root-Anmeldeinformationen Ihres für Anfragen AWS-Konto zu verwenden. Erstellen Sie stattdessen einen AWS Identity and Access Management (IAM)-Benutzer und gewähren Sie diesem vollständigen Zugriff. Wir bezeichnen diese Benutzer als IAM-Benutzer mit Anmeldeinformationen auf Administratorebene.

Sie können die Anmeldeinformationen des Administratorbenutzers anstelle der Root-Anmeldeinformationen Ihres -Kontos verwenden, um mit zu interagieren AWS und Aufgaben auszuführen, z. B. um einen Amazon S3-Bucket zu erstellen, Benutzer zu erstellen und ihnen Berechtigungen zu erteilen. Weitere Informationen finden Sie unter Vergleichen von Root-Benutzer-Anmeldeinformationen des - AWS Kontos und IAM-Benutzer-Anmeldeinformationen in der AWS Allgemeinen -Referenz und unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Registrieren Sie sich für ein AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um eines zu erstellen.

So registrieren Sie sich für ein AWS-Konto

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

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

   Wenn Sie sich für ein registrieren AWS-Konto, Root-Benutzer des AWS-Kontos wird ein 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 eine Bestätigungs-E-Mail, nachdem der Registrierungsprozess abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

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

Sichern Ihrer Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console 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 Administratorbenutzers

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 Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Konfigurieren des Benutzerzugriffs mit dem Standard IAM-Identity-Center-Verzeichnis- im AWS IAM Identity Center -Benutzerhandbuch.

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 unter Anmelden beim - AWS Zugriffsportal im AWS-Anmeldung -Benutzerhandbuch.

Vor der Bestellung eines Snowball Edge-Geräts

AWS Snowball Edge ist ein regionsspezifischer Service. Bevor Sie Ihren Auftrag planen, stellen Sie daher sicher, dass der Service in Ihrem verfügbar ist AWS-Region. Stellen Sie sicher, dass sich Ihr Standort und Ihr Amazon S3-Bucket innerhalb desselben AWS-Region oder desselben Landes befinden, da dies sich auf Ihre Fähigkeit auswirkt, das Gerät zu bestellen.

Um Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten mit für Datenverarbeitung optimierten Geräten für lokale Edge-Datenverarbeitungs- und Speicheraufträge zu verwenden, müssen Sie S3-Kapazität auf dem Gerät oder den Geräten bereitstellen, wenn Sie bestellen. Amazon S3-kompatibler Speicher auf Snow-Family-Geräten 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 Bestellprozesses 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 Auftrag zu verschlüsseln. Weitere Informationen zum Erstellen von IAM-Rollen und KMS-Schlüsseln finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts.

Themen

Fragen zur lokalen Umgebung

Wenn Sie Ihren Datensatz und die Einrichtung der lokalen Umgebung verstehen, können Sie Ihre Datenübertragung abschließen. Beachten Sie Folgendes, bevor Sie Ihre Bestellung aufgeben.

Welche Daten werden übertragen?

> Die Übertragung einer großen Anzahl kleiner Dateien funktioniert mit AWS Snowball Edge nicht gut. Dies liegt daran, dass Snowball Edge jedes einzelne Objekt verschlüsselt. Kleine

Dateien enthalten Dateien mit einer Größe von weniger als 1 MB. Wir empfehlen Ihnen, sie zu komprimieren, bevor Sie sie auf das AWS Snowball Edge-Gerät übertragen. 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, einen statischen Datensatz zu haben (d. h., es greifen während der Übertragung keine Benutzer oder Systeme auf die Daten zu). Andernfalls kann die Dateiübertragung aufgrund einer Nichtübereinstimmung der Prüfsumme fehlschlagen. Die Dateien werden nicht übertragen und als markiert`Failed`.

Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie ein AWS Snowball Edge-Gerät nicht und ändern Sie nicht dessen Netzwerkeinstellungen während der Übertragung von Daten. Dateien müssen beim Schreiben auf das Gerät in statischem Zustand sein. Dateien, die geändert werden, während sie auf das Gerät geschrieben werden, können zu Lese-/Schreibkonflikten führen.

Unterstützt das Netzwerk die AWS Snowball Datenübertragung?

Snowball Edge unterstützt die RJ45-, SFP+- oder QSFP+-Netzwerkadapter. Stellen Sie sicher, dass es sich bei Ihrem Schalter um einen Gigabit-Schalter handelt. Je nach Switch-Marke kann dies 10/100/1000 sein. Snowball Edge-Geräte unterstützen keinen Megabit- oder 10/100-Schalter.

Arbeiten mit Dateinamen, die Sonderzeichen enthalten

Es ist wichtig zu beachten, dass Sie möglicherweise auf Fehler stoßen, wenn die Namen Ihrer Objekte Sonderzeichen enthalten. Obwohl Amazon S3 Sonderzeichen zulässt, empfehlen wir 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 beim Kopieren einzelner Objekte oder beim Ausführen eines rekursiven Befehls vorsichtig sein. In Befehlen umgeben Sie die Namen von Objekten, die Leerzeichen in den Namen enthalten, mit Anführungszeichen. Im Folgenden finden Sie Beispiele für solche Dateien.

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

> **Note**
>
> Die einzigen übertragenen Objektmetadaten sind der Objektname und die Größe.

Verwenden von Amazon EC2 auf Snow Family-Geräten

Dieser Abschnitt bietet einen Überblick über die Verwendung von Amazon EC2-compatible Rechen-Instances auf einem AWS Snowball Edge-Gerät. Sie enthält konzeptionelle Informationen, Verfahren und Beispiele.

> **Note**
>
> Diese Amazon EC2-Funktionen in AWS Snowball werden in den Regionen Asien-Pazifik (Mumbai) und Europa (Paris) nicht unterstützt AWS-Regionen.

Sie können Amazon EC2-compatible Rechen-Instances ausführen, die auf einem AWS Snowball Edge gehostet werden`sbe1`, mit den Instance-`sbe-g`Typen `sbe-c`, und :

- Der `sbe1` Instance-Typ funktioniert auf Geräten mit der Option Snowball Edge Storage Optimized.
- Der `sbe-c` Instance-Typ funktioniert auf Geräten mit der Option Snowball Edge Compute Optimized.
- Sowohl die Instances`sbe-c`s`be-g`-Typen als auch funktionieren auf Geräten mit der Option Snowball Edge Compute Optimized with GPU.

Alle Datenverarbeitungs-Instance-Typen, die auf Snowball Edge-Geräteoptionen unterstützt werden, sind für AWS Snowball Edge-Geräte eindeutig. Wie ihre cloudbasierten Pendants benötigen diese Instances Amazon-Systemabbilder (Amazon Machine Images, AMIs) zum Starten. Sie wählen das AMI für eine Instance aus, bevor Sie Ihren Snowball-Edge-Auftrag erstellen.

Um eine Rechen-Instance auf einem Snowball Edge zu verwenden, erstellen Sie einen Auftrag, um ein Snow Family-Gerät zu bestellen und Ihre AMIs anzugeben. Sie können dies über die - AWS Snowball Managementkonsole, die AWS Command Line Interface (AWS CLI) oder eines der - AWS SDKs tun. Um Ihre Instances verwenden zu können, müssen Sie in der Regel einige Voraussetzungen für die Verwaltung erfüllen, bevor Sie Ihren Auftrag erstellen.

Wenn Ihr Gerät eingetroffen ist, können Sie mit der Verwaltung Ihrer AMIs und Instances beginnen. Sie können Ihre Datenverarbeitungs-Instances auf einem Snowball Edge über einen Amazon EC2-Endpunkt verwalten. Diese Art von Endpunkt unterstützt viele der Amazon EC2-CLI-Befehle und - Aktionen für die - AWS SDKs. Sie können die AWS Management Console auf dem Snowball Edge nicht verwenden, um Ihre AMIs und Rechen-Instances zu verwalten.

Wenn Sie mit Ihrem Gerät fertig sind, geben Sie es an zurück AWS. 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 ein vollständiges Löschen des Geräts durch, wenn es an zurückgegeben wird AWS. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

> **Important**
>
> Daten in Datenverarbeitungs-Instances, die auf einem Snowball Edge ausgeführt werden, werden nicht in importiert AWS.

Unterschied zwischen Amazon EC2- und AmazonEC2-compatible Instances auf Snow-Family-Geräten

AWS ECEC2-compatible der Snow Family ermöglichen es Kunden, AmazonEC2-compatible Instances mithilfe einer Teilmenge von EC2-APIs und einer Teilmenge von AMIs zu verwenden und zu verwalten.

Preise für Compute Instances auf Snowball Edge

Die Verwendung von Datenverarbeitungs-Instances verursacht zusätzliche Kosten. Weitere Informationen finden Sie unter AWS Snowball Edge -Preisgestaltung.

Voraussetzungen

Bevor Sie Ihren Auftrag erstellen, sollten Sie die folgenden Informationen beachten:

- Bevor Sie Ihrer Auftragsanforderung AMIs hinzufügen, stellen Sie sicher, dass Sie ein AMI erstellt haben, das in Ihrem unterstützt wird AWS-Konto. Derzeit basieren unterstützte AMIs auf den Images CentOS 7 (x86_64) – mit Updates für HVM und Ubuntu 16.04 LTS – Xenial (HVM). Sie können diese Bilder von der AWS Marketplace Website abrufen.
- Alle AMIs müssen auf Amazon Elastic Block Store (Amazon EBS) mit einem einzigen Volume basieren.
- Wenn Sie eine Verbindung zu einer Datenverarbeitungs-Instance herstellen, die auf einem Snowball Edge ausgeführt wird, müssen Sie Secure Shell (SSH) verwenden. Hierzu müssen Sie zunächst das Schlüsselpaar hinzufügen. Weitere Informationen finden Sie unter Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden.

Erstellen eines Linux-AMI aus einer Instance

Sie können ein AMI mithilfe der AWS Management Console oder der Befehlszeile erstellen. Beginnen Sie mit einem vorhandenen AMI, starten Sie eine Instance, passen Sie sie an, erstellen Sie daraus ein neues AMI und starten Sie schließlich eine Instance Ihres neuen AMI.

So erstellen Sie mit der Konsole ein AMI aus einer Instance

1. Wählen Sie ein geeignetes EBS-gestütztes AMI als Ausgangspunkt für Ihr neues AMI aus und konfigurieren Sie es vor dem Start nach Bedarf. Weitere Informationen finden Sie unter Starten einer Instance mit dem Launch Instance Wizard im Amazon EC2-Benutzerhandbuch für Linux-Instances.
2. Wählen Sie Starten, um eine Instance des ausgewählten EBS-gestützten AMI zu starten. Akzeptieren Sie beim Durchlaufen des Assistenten die Standardwerte. Weitere Informationen finden Sie unter Starten einer Instance mit dem Launch Instance Wizard.
3. Stellen Sie eine Verbindung mit der Instance her, während sie ausgeführt wird. Sie können die folgenden Aktionen auf Ihrer Instance ausführen, um sie an Ihre Bedürfnisse anzupassen:
   - Installieren Sie Software und Anwendungen.
   - Daten kopieren.
   - Reduzieren Sie die Startzeit, indem Sie temporäre Dateien löschen, Ihre Festplatte defragmentieren und keinen freien Speicherplatz mehr benötigen.
   - Fügen Sie zusätzliche Amazon EBS-Volumes an.
4. (Optional) Erstellen Sie Snapshots von allen Volumes, die an Ihre Instance angefügt sind. Weitere Informationen zum Erstellen von Snapshots finden Sie unter Erstellen von Amazon-EBS-Snapshots im Amazon EC2-Benutzerhandbuch für Linux-Instances.
5. Wählen Sie im Navigationsbereich Instances und anschließend Ihre Instance aus. Wählen Sie Aktionen, wählen Sie Image und dann Image erstellen aus.

   > **Tip**
   >
   > Wenn diese Option nicht verfügbar ist, ist Ihre Instance keine Amazon-EBS-gestützte Instance.

6. Geben Sie im Dialogfeld Image erstellen die folgenden Informationen an und wählen Sie dann Image erstellen aus.

- Image name – Ein eindeutiger Name für das Image.
- Bildbeschreibung – Eine optionale Beschreibung des Bildes mit bis zu 255 Zeichen.
- Kein Neustart – Diese Option ist standardmäßig nicht ausgewählt. Amazon EC2 fährt die Instance herunter, erstellt Snapshots von allen angefügten Volumes, erstellt und registriert das AMI und startet dann die Instance neu. Wählen Sie No reboot (Kein Neustart) aus, wenn Sie vermeiden möchten, dass Ihre Instance heruntergefahren wird.

  > ⚠ Warning
  >
  > Wenn Sie No reboot (Kein Neustart) auswählen, können wir die Integrität des Dateisystems für das erstellte Abbild nicht garantieren.

- Instance-Volumes – Mit den Feldern in diesem Abschnitt können Sie das Stamm-Volume ändern und weitere Amazon EBS- und Instance-Speicher-Volumes hinzufügen. Sie erhalten weitere Informationen zu den einzelnen Feldern, indem Sie jeweils auf das i-Symbol neben den Feldern klicken; dadurch wird die QuickInfo zum jeweiligen Feld angezeigt. Einige wichtige Punkte sind im Folgenden aufgeführt:
  - Um die Größe des Root-Volumes zu ändern, suchen Sie in der Spalte Volume-Typ nach Root. Geben Sie für Größe (GiB) den erforderlichen Wert ein.
  - Wenn Sie Bei Beendigung löschen auswählen, wird das Amazon-EBS-Volume gelöscht, wenn Sie die aus diesem AMI erstellte Instance beenden. Wenn Sie Löschen bei Beendigung deaktivieren, wird beim Beenden der Instance das Amazon-EBS-Volume nicht gelöscht. Weitere Informationen finden Sie unter Beibehalten von Amazon-EBS-Volumes beim Beenden einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
  - Um ein Amazon-EBS-Volume hinzuzufügen, wählen Sie Neues Volume hinzufügen (was eine neue Zeile hinzufügt). Wählen Sie unter Volume Type (Volumetyp) die Option EBS und füllen Sie die Felder in der Zeile aus. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden diese zusätzlichen Volumes automatisch der Instance zugeordnet. Leere Volumes müssen formatiert und „gemountet“ werden. Volumes, die auf einem Snapshot basieren, müssen „gemountet“ werden.
  - Informationen zum Hinzufügen eines Instance-Speicher-Volumes finden Sie unter Hinzufügen von Instance-Speicher-Volumes zu einem AMI im Amazon EC2-Benutzerhandbuch für Linux-Instances. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden zusätzliche Volumes automatisch initialisiert und gemountet. Diese Volumes

enthalten keine Daten von den Instance-Speicher-Volumes der laufenden Instance, auf der Sie Ihr AMI basieren.

7. Sie können den Status Ihres AMI während der Erstellung anzeigen, indem Sie im Navigationsbereich die Option AMIs auswählen. Anfänglich ist der Status ausstehend, sollte sich aber nach einigen Minuten in verfügbar ändern.

   (Optional) Wählen Sie die Option Snapshots aus, um den Snapshot anzuzeigen, der für das neue AMI erstellt wurde. Wenn Sie eine Instance über dieses AMI starten, verwenden wir diesen Snapshot, um den dazugehörigen Root-Gerät-Volume zu erstellen.

8. Starten Sie eine Instance über Ihr neues AMI. Weitere Informationen finden Sie unter Starten einer Instance mit dem Launch Instance Wizard im Amazon EC2-Benutzerhandbuch für Linux-Instances.

9. Die neue ausgeführte Instance enthält alle Anpassungen, die Sie in den letzten Schritten vorgenommen haben.

So erstellen Sie ein AMI aus einer Instance mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen finden Sie unter Zugriff auf Amazon EC2 im Amazon EC2-Benutzerhandbuch für Linux-Instances.

- create-image (AWS CLI)
- New-EC2Image (AWS Tools für Windows PowerShell)

Erstellen eines Linux-AMI aus einem Snapshot

Wenn Sie einen Snapshot des Root-Gerät-Volumes einer Instance haben, können Sie aus diesem Snapshot mithilfe der AWS Management Console oder der Befehlszeile ein AMI erstellen.

So erstellen Sie mit der Konsole ein AMI aus einem Snapshot

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Elastic Block Store die Option Snapshots.
3. Wählen Sie den Snapshot, Aktionen und dann Image erstellen aus.

4. Füllen Sie im Dialogfeld Image aus EBS-Snapshot erstellen die Felder aus, um Ihr AMI zu erstellen. Wählen Sie die Option Erstellen aus. Wenn Sie eine übergeordnete Instance neu erstellen, wählen Sie dieselben Optionen wie für die übergeordnete Instance aus.

   - Architektur – Wählen Sie i386 für 32-Bit oder x86_64 für 64-Bit.
   - Name des Root-Geräts – Geben Sie den entsprechenden Namen für das Root-Volume ein. Weitere Informationen finden Sie unter Gerätebenennung bei Linux-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.
   - Virtualisierungstyp – Wählen Sie aus, ob Instances, die über dieses AMI gestartet werden, Paravirtual (PV)- oder Hardware Virtual Machine (HVM)-Virtualisierung verwenden. Weitere Informationen finden Sie unter Linux AMI-Virtualisierungstypen.
   - (Nur PV-Virtualisierungstyp) Kernel-ID und RAM-Datenträger-ID – Wählen Sie die AKI und ARI aus den Listen aus. Wenn Sie die Standard-AKI oder keine AKI auswählen, müssen Sie jedes Mal, wenn Sie eine Instance mit diesem AMI starten, eine AKI angeben. Darüber hinaus besteht die Möglichkeit, dass Ihre Instance die Zustandsprüfungen nicht besteht, wenn die Standard-AKI nicht mit der Instance kompatibel ist.
   - (Optional) Blockgerät-Zuweisungen – Fügen Sie Volumes hinzu oder erweitern Sie die Standardgröße des Root-Volumes für das AMI. Weitere Informationen zur Größenanpassung des Dateisystems auf Ihrer Instance für ein größeres Volume finden Sie unter Erweitern eines Linux-Dateisystems nach der Größenanpassung eines Volumes im Amazon EC2-Benutzerhandbuch für Linux-Instances.

So erstellen Sie ein AMI aus einem Snapshot mithilfe der Befehlszeile

Um ein AMI aus einem Snapshot zu erstellen, können Sie einen der folgenden Befehle verwenden. Weitere Informationen zu diesen Befehlszeilenschnittstellen finden Sie unter Zugriff auf Amazon EC2 im Amazon EC2-Benutzerhandbuch für Linux-Instances.

- register-image (AWS CLI)
- Register-EC2Image (AWS Tools for Windows PowerShell)

Verwenden von Amazon S3 auf Snowball Edge

Im Rahmen des Bestellvorgangs werden Sie aufgefordert, eine AWS Identity and Access Management (IAM)-Rolle und einen AWS Key Management Service (AWS KMS)-Schlüssel zu erstellen. Der KMS-Schlüssel wird zum Verschlüsseln der Daten im Ruhezustand auf dem Snowball-

Edge-Gerät verwendet. Weitere Informationen zum Erstellen von IAM-Rollen und KMS-Schlüsseln finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts.

> **Important**
>
> Wenn die importierten Daten im S3-Bucket mit serverseitiger Verschlüsselung mit Schlüsseln verschlüsselt werden müssen, die in AWS KMS (SSE-KMS) gespeichert sind, finden Sie weitere Informationen unter Amazon S3-Verschlüsselung mit AWS KMS.
> Wenn die importierten Daten im S3-Bucket mit serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) verschlüsselt werden müssen, finden Sie weitere Informationen unter Amazon S3-Verschlüsselung mit serverseitiger Verschlüsselung.

So funktioniert der Import

Jeder Importauftrag verwendet ein einzelnes Snowball Edge-Gerät. Nachdem Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellt haben, senden wir Ihnen ein Snowball Edge-Gerät. Wenn es eintrifft, verbinden Sie das Snowball Edge-Gerät mit Ihrem Netzwerk und übertragen die Daten, die Sie in Amazon S3 importieren möchten, auf diesen Snowball Edge. Wenn Sie mit der Übertragung von Daten fertig sind, senden Sie den Snowball Edge zurück an AWS. Anschließend importieren wir Ihre Daten in Amazon S3.

> **Important**
>
> Snowball Edge kann nicht in Buckets schreiben, wenn Sie die S3-Objektsperre aktiviert haben. Wir können auch nicht in Ihren Bucket schreiben, wenn IAM-Richtlinien für den Bucket das Schreiben in den Bucket verhindern.

So funktioniert der Export

Jeder Exportauftrag kann eine beliebige Anzahl von AWS Snowball Edge-Geräten verwenden. Nachdem Sie einen Auftrag erstellt haben, beginnt ein Auflistungsvorgang in Amazon S3. Dieses Auflisten von Operationen teilt Ihren Auftrag in mehrere Teile auf. Jedem Teilauftrag wird genau einem Gerät zugeordnet. Nachdem Ihre Teilaufträge erstellt wurden, wechselt der erste Teilauftrag in den Status Preparing Snowball (Snowball wird vorbereitet).

> **Note**
>
> Der Auflistungsvorgang zum Teilen Ihres Auftrags ist eine Funktion von Amazon S3, und Ihnen wird der gleiche wie der Amazon S3-Vorgang in Rechnung gestellt.

Anschließend beginnen wir mit dem Exportieren Ihrer Daten auf ein Gerät. Der Datenexport dauert in der Regel einen Werktag. Der Vorgang kann unter Umständen jedoch auch länger dauern. Wenn der Export abgeschlossen ist, AWS stellt das Gerät bereit, damit Ihr regionaler Transporteur es abholen kann.

Wenn das Gerät an Ihrem Standort eintrifft, verbinden Sie es mit Ihrem Netzwerk und übertragen die Daten, die Sie in Amazon S3 importieren möchten, auf das Gerät. Wenn Sie mit der Übertragung der Daten fertig sind, senden Sie das Gerät zurück an AWS. Wenn wir das zurückgegebene Gerät erhalten, 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. Wenn weitere Teilaufträge vorhanden sind, wird nun der nächste Teilauftrag für den Versand vorbereitet.

> **Important**
>
> Snowball Edge kann keine Dateien exportieren, die sich in der Speicherklasse S3 Glacier befinden. Diese Objekte müssen wiederhergestellt werden, bevor wir die Dateien exportieren können. Wenn wir auf Dateien in der S3-Glacier-Speicherklasse stoßen, wenden wir uns an Sie, um Sie darüber zu informieren. Dies kann jedoch zu Verzögerungen bei Ihrem Exportauftrag führen.

Verwenden von Amazon S3-kompatiblem Speicher auf Geräten der Snow Family für Edge-Computing- und Speicheraufträge

Amazon S3-kompatibler Speicher auf Geräten der Snow Family bietet sicheren Objektspeicher mit erhöhter Ausfallsicherheit, Skalierung und erweiterter Amazon S3-API-Feature-Set für die Telefonie-, mobilen Edge- und getrennten Umgebungen. Amazon S3-kompatibler Speicher auf Snow-Family-Geräten ermöglicht es Kunden, Daten zu speichern und hochverfügbare Anwendungen auf Snow-Family-Geräten für Edge-Computing-Anwendungsfälle auszuführen.

Sie können Amazon S3-Buckets auf den Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte an zurückgegeben werden AWS, werden alle Daten, die im Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten erstellt oder gespeichert werden, gelöscht. Weitere Informationen finden Sie unter Lokale Datenverarbeitungs- und reine Speicheraufträge.

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten kann in eigenständiger Konfiguration oder Cluster-Konfiguration bereitgestellt werden. In einer eigenständigen Konfiguration können Sie nutzbare S3-Kapazität auf dem Gerät bereitstellen und der Saldo ist als Blockspeicher verfügbar. Bei der Clustereinrichtung wird die gesamte Datenfestplattenkapazität für den S3-Speicher genutzt. Abhängig von der Größe des Clusters ist der S3-Service so konzipiert, dass die Fehlertoleranz von 1 oder 2 Geräten aufrechterhalten wird. Weitere Informationen zur Cluster-Fehlertoleranz finden Sie unter Clustering-Übersicht.

Informationen zum Einrichten und Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten finden Sie unter Amazon S3-kompatibler Speicher auf Snow-Family-Geräten in diesem Handbuch.

Amazon S3-Verschlüsselung mit AWS KMS

Sie können die standardmäßigen AWS von oder vom Kunden verwalteten Verschlüsselungsschlüssel verwenden, um Ihre Daten beim Importieren oder Exportieren von Daten zu schützen.

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

So aktivieren Sie die AWS verwaltete Verschlüsselung mit AWS KMS

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Amazon 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 dann den KMS-Schlüssel aus, den Sie verwenden möchten. Dieser Schlüssel wird verwendet, um Objekte zu verschlüsseln, die in den Bucket geschrieben werden.
6. Wählen Sie Speichern.

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

Im Folgenden finden Sie Beispiele für eine solche Anweisung.

Zum Importieren von Daten

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

Example Beispiel für eine Snowball-Import-IAM-Rolle

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

Example Snowball-Export-IAM-Rolle

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

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

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

Zum Importieren von Daten

So aktivieren Sie die vom Kunden verwaltete Verschlüsselung mit AWS KMS

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Key Management Service (AWS KMS)-Konsole unter https://console.aws.amazon.com/kms.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im linken Navigationsbereich Kundenverwaltete Schlüssel und dann den KMS-Schlüssel aus, der den Buckets zugeordnet ist, die Sie verwenden möchten.
4. Erweitern Sie die Schlüsselrichtlinie, falls sie noch nicht erweitert ist.
5. Wählen Sie im Abschnitt Schlüsselbenutzer die Option Hinzufügen und suchen Sie nach der IAM-Rolle. Wählen Sie die IAM-Rolle und dann Hinzufügen aus.
6. Alternativ können Sie Zur Richtlinienansicht wechseln wählen, um das Schlüsselrichtliniendokument anzuzeigen und der Schlüsselrichtlinie eine Anweisung 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 es auch erforderlich, die IAM-Rolle zu aktualisieren, die dem Snowball-Auftrag zugeordnet ist. Standardmäßig ist die Rolle `snowball-import-s3-only-role`.

Example der Snowball-Import-IAM-Rolle

```
{
  "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 von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Snowball.

Der verwendete KMS-Schlüssel sieht wie folgt aus:

`“Resource”:“arn:aws:kms:`*`region`*`:`*`AccoundID`*`:key/*”`

Zum Exportieren 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 es auch erforderlich, die IAM-Rolle zu aktualisieren, die dem Snowball-Auftrag zugeordnet ist. Standardmäßig sieht die Rolle wie folgt aus:

`snowball-export-s3-only-role`

Example der Snowball-Export-IAM-Rolle

```
{
  "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 es auch erforderlich, die IAM-Rolle zu aktualisieren, die dem Snowball-Auftrag zugeordnet ist. Standardmäßig ist die Rolle `snowball-export-s3-only-role`.

Amazon S3-Verschlüsselung mit serverseitiger Verschlüsselung

AWS Snowball unterstützt die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3). Bei der serverseitigen Verschlüsselung geht es um den Schutz von Daten im Ruhezustand, und SSE-S3 verfügt über eine starke Multifaktor-Verschlüsselung

zum Schutz Ihrer Daten im Ruhezustand in Amazon S3. Weitere Informationen zu SSE-S3 finden Sie unter Schutz von Daten mit serverseitiger Verschlüsselung mit von Amazon S3-Managed Verschlüsselungsschlüsseln (SSE-S3) im Benutzerhandbuch für Amazon Simple Storage Service.

> **Note**
>
> Derzeit unterstützt keine serverseitige AWS Snowball 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 SSE-C verwenden möchten, um die Objekte zu verschlüsseln, die Sie in S3 importiert haben, 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 ieren– Wenn Sie mit SSE-C verschlüsselte Objekte exportieren möchten, kopieren Sie diese Objekte zunächst in einen anderen Bucket, der entweder keine serverseitige Verschlüsselung hat oder in der Bucket-Richtlinie dieses Buckets SSE-KMS oder SSE-S3 angegeben ist.

Snowball-Edge-Cluster

Für den AWS Snowball Service ist ein Cluster ein Kollektiv von Snowball Edge-Geräten, die als einzelne logische Einheit für lokale Speicher- und Rechenzwecke verwendet werden.

Ein Cluster ist eine logische Gruppierung von AWS Snowball Edge-Geräten in Gruppen von 3 bis 16 Geräten. Ein Cluster wird mit einem einzigen Auftrag erstellt. Ein Cluster bietet eine höhere Haltbarkeit und Speicherkapazität. Dieser Abschnitt enthält Informationen zu Snowball Edge-Clustern mit Amazon S3-kompatiblem Speicher auf Snow Family-Geräten.

Überlegungen zu Clusteraufträgen für AWS Snowball Edge

Beachten Sie die folgenden Überlegungen, wenn Sie planen, einen Cluster von Snowball-Edge-Geräten zu verwenden:

- Wir empfehlen die Verwendung einer redundanten Stromversorgung, um potenzielle Leistungs- und Stabilitätsprobleme für Ihren Cluster zu minimieren.

- Wie eigenständige lokale Speicher- und Datenverarbeitungsaufträge 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-Auftrags importieren.
- Um Daten aus Amazon S3 in einen Cluster zu übertragen, erstellen Sie einen separaten Exportauftrag und kopieren Sie die Daten von den Geräten des Exportauftrags in den Cluster.
- Sie können die Konsole, die oder das AWS SDK verwenden AWS CLI, um einen Cluster-Auftrag zu erstellen.
- Cluster-Knoten haben Knoten-IDs. Eine Knoten-ID entspricht der Auftrags-ID für ein Gerät, das Sie von der Konsole, der , AWS CLI den AWS SDKs oder dem Snowball Edge-Client abrufen können. Sie können die Knoten-IDs verwenden, um alte Knoten von Clustern zu entfernen. Mit dem Befehl `snowballEdge describe-device` erhalten Sie eine Liste der Knoten-IDs auf einem entsperrten Gerät, mit dem Befehl `describe-cluster` für einen entsperrten Cluster.
- Die Lebensdauer eines Clusters wird durch das Sicherheitszertifikat begrenzt, das für die Cluster-Geräte bei der Bereitstellung des Clusters gewährt wird.
- Wenn ein zurückgegebenes Gerät AWS empfängt, 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.

Überlegungen zum Versand von Snow-Family-Geräten

Wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen, geben Sie eine Lieferadresse an und wählen die Versandgeschwindigkeit aus. Beachten Sie, dass die Versandgeschwindigkeit nicht angibt, wie schnell Sie erwarten können, dass Sie das Gerät an dem Tag erhalten, an dem Sie den Auftrag erstellt haben. Vielmehr wird die Zeit angegeben, zu der das Gerät zwischen AWS und Ihrer Lieferadresse unterwegs ist. Bevor das Gerät ausgeliefert wird, AWS verarbeitet das Gerät für den Auftrag. Die Zeit, die für die Verarbeitung Ihres Auftrags erforderlich ist, hängt von Faktoren wie Auftragstyp und -größe ab. Außerdem holen Spediteure ausgehende Snow-Family-Geräte in der Regel nur einmal täglich ab und die Spediteure holen an Wochenenden keine ausgehenden Geräte ab. Daher kann die Bearbeitungszeit vor dem Versand auch länger dauern als einen Tag. Während Ihr Gerät auf den Versand AWS vorbereitet und das Gerät nach der Rückgabe erhält, können Sie den Status Ihres Auftrags über die überwachenManagementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter Job Statuses.

> **Note**
>
> Die von Ihnen gewählte Versandgeschwindigkeit gilt, wenn das Gerät an Sie AWS sendet und wenn Sie das Gerät an zurückgebenAWS.
> Snowball Edge-Geräte können nur verwendet werden, um Daten innerhalb der AWS Region zu importieren oder zu exportieren, in der die Geräte bestellt sind.

Weitere Informationen zur Auswahl der Versandgeschwindigkeit und zur Eingabe Ihrer Lieferadresse beim Erstellen eines Auftrags zur Bestellung eines Snow Family-Geräts finden Sie unter Schritt 4: Auswählen von Sicherheits-, Versand- und Benachrichtigungseinstellungen. Weitere Informationen zum Zurückgeben eines Snow Family-Geräts an finden Sie AWSunter Zurückgeben des Snowball Edge-Geräts.

Weitere Informationen zu Versandgebühren finden Sie unter -AWS Snowball EdgePreise.

Einschränkungen des regionsbasierten Versands

Bevor Sie einen Auftrag zum Bestellen eines Snow-Family-Geräts erstellen, sollten Sie sich von derselben AWS-Region wie Ihre Amazon S3-Daten bei der Konsole anmelden. sendet AWS keine Snow-Family-Geräte zwischen Ländern innerhalb derselben AWS-Region, z. B. von Asien-Pazifik (India) nach Asien-Pazifik (Australien).

Eine Ausnahme beim Versand zwischen Ländern sind die Mitgliedslander der EU (Europe Union). Für Datenübertragungen in den Europa-AWSRegionen senden wir Geräte nur in die aufgeführten EU-Mitgliedslander:

Estland, Estland, Finnland, Frankreich, Deutschland, Ungarn, Italien, Irland, Lettland, Litauen, Luxemburg, Malta, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien und Italien.

Geräte der Snow Family können nur in dieselbe AWS Region zurückgegeben werden, in der die Geräte bestellt wurden.

Sendungen, die sich in demselben Land befinden, sind zulässig. Beispiele:

- Für Datenübertragungen in der Region Großbritannien liefern wir Geräte innerhalb Großbritanniens aus.
- Für Datenübertragungen in Asien-Pazifik (Mumbai) liefern wir Geräte innerhalb von Indien.

> **Note**
>
> AWS sendet keine Snow Family-Geräte an Postfächer.

Erste Schritte

Mit einem - AWS Snowball Edge Gerät können Sie auf die Speicher- und Rechenleistung des AWS Cloud lokal und kostengünstig an Orten zugreifen, an denen eine Internetverbindung möglicherweise keine Option ist. Sie können auch Hunderte von Terabyte oder Petabyte an Daten zwischen Ihren On-Premises-Rechenzentren und Amazon Simple Storage Service (Amazon S3) übertragen.

Im Folgenden finden Sie allgemeine Anweisungen zum Erstellen und Abschließen Ihres ersten AWS Snowball Edge Geräteauftrags 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 Funktionsweise von AWS Snowball Edge.

Bei den Übungen für die ersten Schritte wird davon ausgegangen, dass Sie die verwenden, Managementkonsole für die AWS Snow-Familie um Ihren Auftrag zu erstellen, die AWS OpsHub for Snow Family zum Entsperren und Verwalten des AWS Snowball Edge Geräts und die Amazon S3-Schnittstelle zum Lesen und Schreiben von Daten. Wenn Sie Aufträge stattdessen programmgesteuert erstellen möchten, um mehr Optionen zu nutzen, können Sie dazu die Auftragsverwaltungs-API einsetzen. Weitere Informationen finden Sie unter AWS Snowball -API-Referenz.

Bevor Sie beginnen können, müssen Sie einen AWS-Konto und einen Administratorbenutzer in AWS Identity and Access Management (IAM) erstellen. Weitere Informationen finden Sie unter Einrichten Ihres AWS Zugriffs für AWS Snowball Edge.

Themen

- Zurückgeben des Snowball Edge-Geräts
- Versand von Artikeln der Snow Family
- Überwachen des Importstatus
- Abrufen Ihres Auftragsabschlussberichts und der Protokolle auf der Konsole

Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts

Um ein Snow Family-Gerät zu bestellen, erstellen Sie einen Auftrag, um ein Snow Family-Gerät in der zu bestellen Managementkonsole für die AWS Snow-Familie. Ein Auftrag ist ein Begriff, der AWS verwendet, um den Lebenszyklus der Verwendung eines Snow-Family-Geräts durch einen Kunden zu beschreiben. Ein Auftrag beginnt mit der Bestellung eines Geräts, wird fortgesetzt, wenn das Gerät AWS vorbereitet und an Sie sendet und Sie es verwenden, und wird abgeschlossen, nachdem das Gerät AWS empfangen und verarbeitet hat, nachdem Sie es zurückgegeben haben. Aufträge werden nach Typ kategorisiert: Export, Import sowie lokale Rechenleistung und Speicher. Weitere Informationen finden Sie unter Grundlegendes zu AWS Snowball-Edge-Aufträgen.

Nachdem Sie den Auftrag erstellt haben, um ein Gerät zu bestellen, können Sie die verwenden, Managementkonsole für die AWS Snow-Familie um den Auftragsstatus anzuzeigen und den Fortschritt des von Ihnen bestellten Geräts zu überwachen, während das Gerät auf den Versand an Sie AWS vorbereitet und nachdem es zurückgegeben wurde. Weitere Informationen finden Sie unter Auftragsstatus. Nachdem das Gerät von zurückgegeben und verarbeitet wurde AWS, können Sie über auf einen Auftragsabschlussbericht und Protokolle zugreifen Managementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter Abrufen Ihres Auftragsabschlussberichts und der Protokolle in der -Konsole.

Sie können Aufträge auch mithilfe der Auftragsverwaltungs-API erstellen und verwalten. Weitere Informationen finden Sie in der AWS Snowball -API-Referenz.

Themen

- Schritt 1: Auswählen eines Auftragstyps
- Schritt 2: Auswählen Ihrer Datenverarbeitungs- und Speicheroptionen
- Schritt 3: Auswählen Ihrer Funktionen und Optionen
- Schritt 4: Auswählen von Sicherheits-, Versand- und Benachrichtigungseinstellungen
- Schritt 5: Überprüfen der Auftragsübersicht und Erstellen Ihres Auftrags
- Herunterladen AWS OpsHub

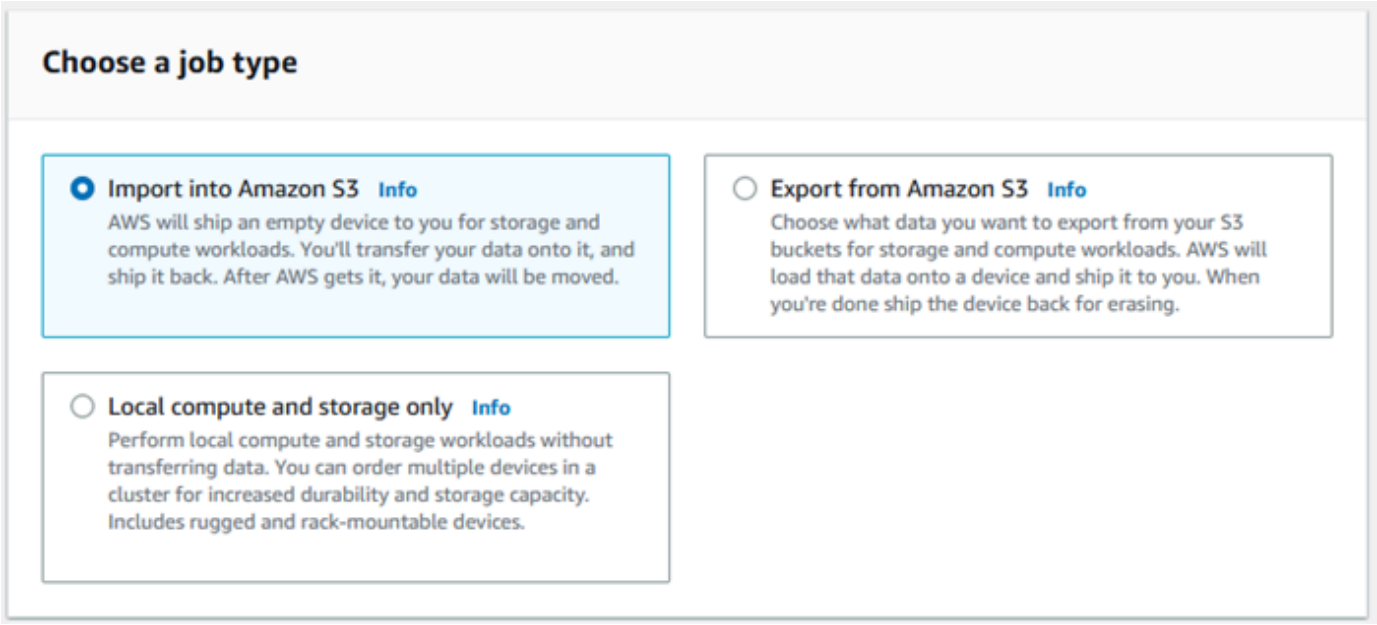
Schritt 1: Auswählen eines Auftragstyps

Der erste Schritt beim Erstellen eines Auftrags besteht darin, den benötigten Auftragstyp zu bestimmen und mit der Planung mit der zu beginnen Managementkonsole für die AWS Snow-Familie.

So wählen Sie Ihren Auftragstyp aus

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Managementkonsole für die AWS Snow-Familie. Wenn Sie zum ersten Mal einen Auftrag in dieser erstellen AWS-Region, wird die Seite AWS Snow Family angezeigt. Andernfalls wird die Liste der vorhandenen Aufträge angezeigt.
2. Wenn dies Ihr erster Auftrag ist, wählen Sie Ein AWS Snow Family-Gerät bestellen aus. Wenn Sie erwarten, dass mehrere Aufträge mehr als 500 TB Daten migrieren, wählen Sie Erstellen Sie Ihren großen Datenmigrationsplan mit mehr als 500 TB aus. Wählen Sie andernfalls in der linken Navigationsleiste Auftrag erstellen aus. Wählen Sie Nächster Schritt, um die Seite Planen Ihres Auftrags zu öffnen.
3. Geben Sie im Abschnitt Auftragsname einen Namen für Ihren Auftrag im Feld Auftragsname ein.
4. Wählen Sie je nach Bedarf einen der folgenden Auftragstypen aus:

   - In Amazon S3 importieren – Wählen Sie diese Option, damit Ihnen ein leeres Snowball Edge-Gerät AWS zugestellt wird. Sie verbinden das Gerät mit Ihrem lokalen Netzwerk und führen den Snowball Edge-Client aus. Sie kopieren Daten mithilfe der NFS-Freigabe oder des S3-Adapters auf das Gerät, senden sie zurück an AWS und Ihre Daten werden in hochgeladen AWS.
   - Aus Amazon S3 exportieren – Wählen Sie diese Option, um Daten aus Ihrem Amazon S3-Bucket auf Ihr Gerät zu exportieren. AWS lädt Ihre Daten auf das Gerät und sendet 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 und AWS Ihre Daten werden vom Gerät gelöscht.
   - Nur lokale Datenverarbeitung und Speicher – Führen Sie Datenverarbeitungs- und Speicher-Workloads auf dem Gerät durch, ohne Daten zu übertragen.



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

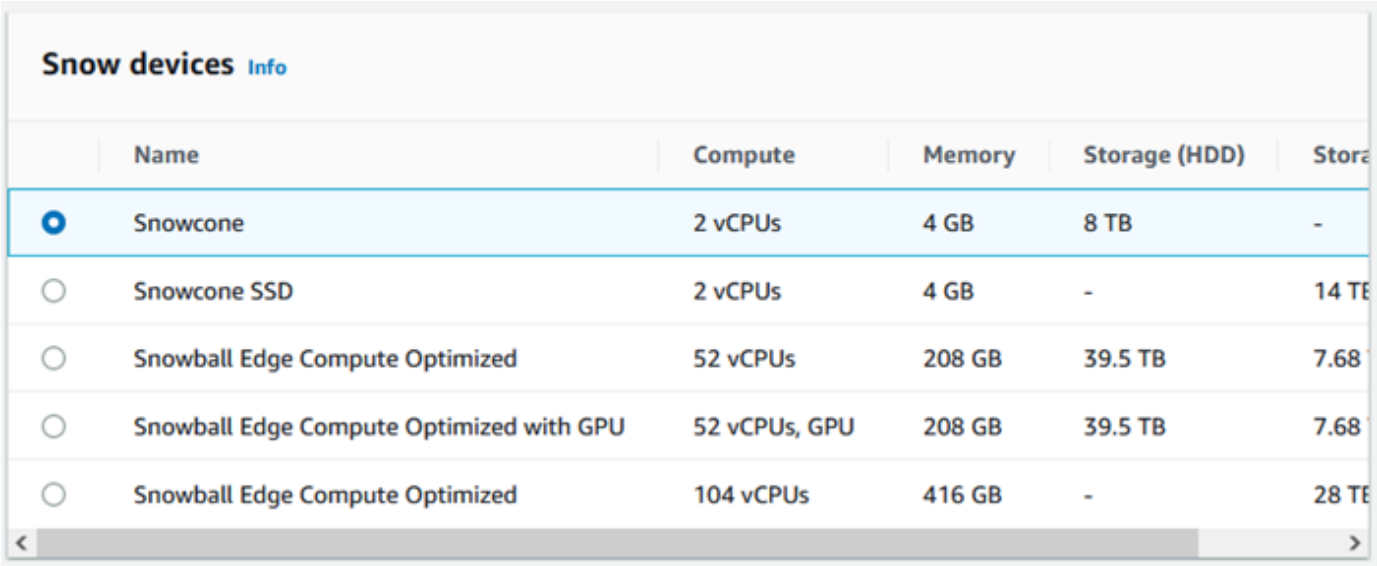
Schritt 2: Auswählen Ihrer Datenverarbeitungs- und Speicheroptionen

Wählen Sie die Hardwarespezifikationen für Ihr Snow Family-Gerät aus, welche Ihrer Amazon EC2-compatible Instances darauf aufgenommen werden sollen, wie Daten gespeichert werden und Preise.

So wählen Sie die Rechen- und Speicheroptionen Ihres Geräts aus

1. Wählen Sie im Abschnitt Snow-Geräte das zu bestellende Snow Family-Gerät aus.

> **Note**
>
> Einige Snow Family-Geräte sind möglicherweise nicht verfügbar, abhängig von der , bei der AWS-Region Sie bestellen, und dem von Ihnen ausgewählten Auftragstyp.



2. Wählen Sie im Abschnitt Preisoption auswählen im Menü Preisoption auswählen den Preistyp aus, der auf diesen Auftrag angewendet werden soll. Wenn Sie die Vorabpreise für 1 oder 3 Jahre festlegen, wählen Sie unter Automatische Verlängerung die Option Ein, um die Preise automatisch zu verlängern, wenn der aktuelle Zeitraum endet, oder Aus, um die Preise nicht automatisch zu verlängern, wenn der aktuelle Zeitraum endet. Weitere Informationen zu den langfristigen Preisoptionen für Snowball-Edge-Geräte finden Sie unter Langfristige Preise für Snowball-Edge-Geräte in diesem Leitfaden. Die Gerätepreise für Ihr finden Sie unter AWS-Region-AWS Snowball Preise.
3. Treffen Sie im Abschnitt Speichertyp auswählen eine Auswahl je nach Bedarf:

   - S3-Adapter: Verwenden Sie den S3-Adapter, um Daten mithilfe von Amazon S3-REST-API-Aktionen programmgesteuert zu und von Snow-Family-Geräten zu übertragen.
   - Amazon S3-kompatibler Speicher: Verwenden Sie Amazon 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 Network File System (NFS)-basierte Datenübertragung, um Dateien von Ihrem Computer in Amazon S3-Buckets auf Snow-Family-Geräten zu ziehen und abzulegen.

> **Warning**
>
> Die NFS-basierte Datenübertragung unterstützt den S3-Adapter nicht. Wenn Sie mit der NFS-basierten Datenübertragung fortfahren, müssen Sie die NFS-Freigabe mounten, um Objekte zu übertragen. Die Verwendung der AWS CLI zum Übertragen von Objekten schlägt fehl.
> Weitere Informationen finden Sie unter Verwenden von NFS für Offline-Datenübertragungen im AWS Snowball Edge-Entwicklerhandbuch.

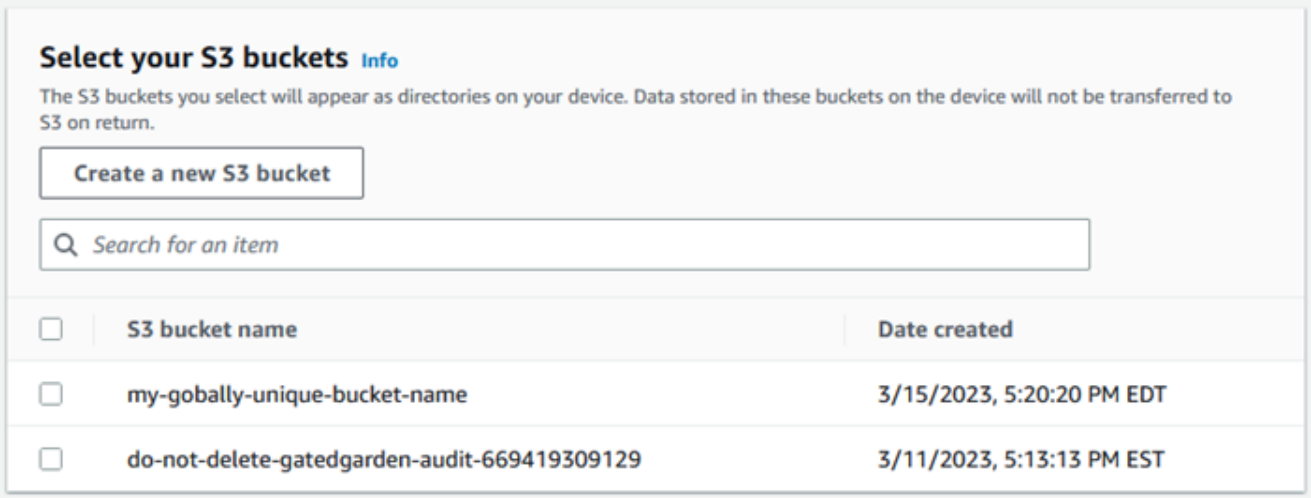
> **Note**
>
> Die verfügbaren Speichertypoptionen hängen vom ausgewählten Auftragstyp und dem ausgewählten Snow-Gerät ab.

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 S3-Buckets auswählen einen oder mehrere der folgenden Schritte aus, um einen oder mehrere S3-Buckets auszuwählen:

     1. Wählen Sie den S3-Bucket aus, den Sie in der Liste S3-Bucket-Name verwenden möchten.
     2. Geben Sie im Feld Nach einem Element suchen einen Bucket-Namen 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 die Option Neuen S3-Bucket erstellen aus, um einen neuen S3-Bucket zu erstellen. Der neue Bucket-Name wird in der Liste Bucket-Name angezeigt. Wählen Sie diese aus.

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

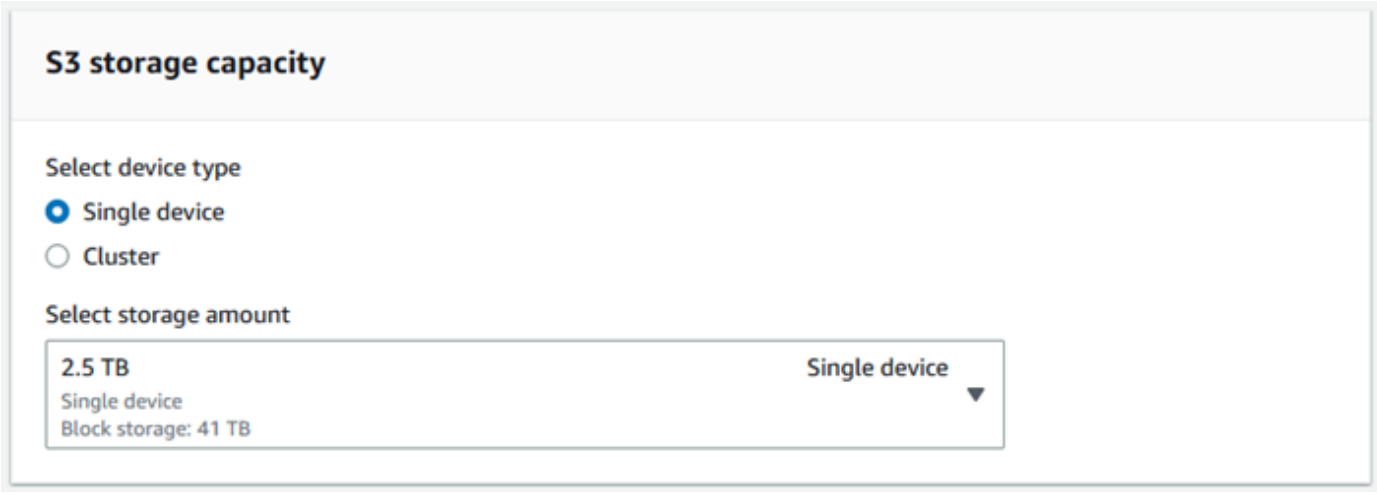


5. Wenn Sie Amazon S3-kompatiblen Speicher als Speichertyp ausgewählt haben, gehen Sie im Abschnitt S3-Speicherkapazität wie folgt vor:

   a. Wählen Sie aus, ob Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten auf einem einzigen 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-kompatiblen Speicher auf Snow-Family-Geräten verwendet werden soll.

> **Note**
>
> Wenn Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwenden, können Sie Amazon S3-Buckets verwalten und erstellen, nachdem Sie das Gerät erhalten haben, sodass Sie sie bei der Bestellung nicht auswählen müssen. Weitere Informationen finden Sie unter Amazon S3-kompatibler Speicher auf Snow-Family-Geräten in diesem Handbuch.



6. Wenn Sie die NFS-basierte Datenübertragung als Speichertyp ausgewählt haben, führen Sie im Abschnitt S3-Buckets auswählen einen oder mehrere der folgenden Schritte aus, um einen oder mehrere S3-Buckets auszuwählen:

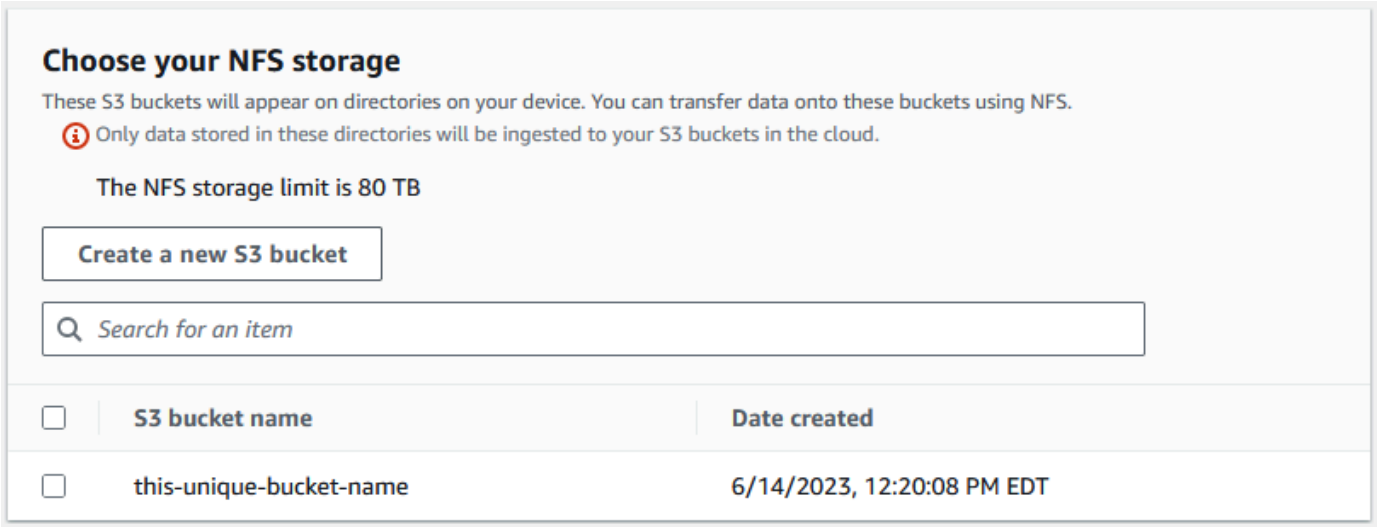
   a. Wählen Sie den S3-Bucket aus, den Sie in der Liste S3-Bucket-Name verwenden möchten.

   b. Geben Sie im Feld Nach einem Element suchen einen Bucket-Namen 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 die Option Neuen S3-Bucket erstellen aus, um einen neuen S3-Bucket zu erstellen. Der neue Bucket-Name wird in der Liste Bucket-Name angezeigt. Wählen Sie diese aus.

   d. Nachdem Sie S3-Buckets für die Verwendung mit der NFS-Datenübertragung ausgewählt haben, wählen Sie auch einen S3-Bucket aus, der als Blockspeicher für AMIs verwendet werden soll. Sehen Sie sich die Schritte zur Auswahl eines -S3Buckets an.

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



7. Wählen Sie im Abschnitt Datenverarbeitung mit EC2-compatible Instances – optional die Option Amazon EC2-compatible AMIs aus Ihrem Konto aus, um sie auf das Gerät aufzunehmen. Oder geben Sie in das Suchfeld den Namen eines AMI ganz oder teilweise ein, um die Liste der verfügbaren AMIs nach Ihrem Eintrag zu filtern, und wählen Sie dann das AMI aus.

   Weitere Informationen finden Sie unter Hinzufügen eines AMI beim Bestellen Ihres Geräts in diesem Leitfaden.

   Für diese Funktion fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter AWS Snowball Edge -Preisgestaltung.
8. Klicken Sie auf die Schaltfläche Next.

Schritt 3: Auswählen Ihrer Funktionen und Optionen

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

So wählen Sie Ihre Funktionen und Optionen aus

1. Um im Abschnitt Amazon EKS Anywhere in AWS Snow Amazon EKS Anywhere in AWS Snow einzuschließen, wählen Sie Amazon EKS Anywhere in Snow einbinden 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 jede Version von Kubernetes, die im Standard- oder verlängerten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten von Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust des Supports für die Kubernetes-Version vermeiden, die Sie verwenden möchten. Weitere Informationen finden Sie unter Amazon-EKS-Kubernetes-Release-Kalender.

   a. Wählen Sie im Abschnitt Ihr eigenes AMI erstellen die AMIs aus, die Sie für Amazon EKS Anywhere erstellt haben. Siehe Abzuschließende Aktionen, bevor Sie ein Snowball-Edge-Gerät für Amazon EKS Anywhere in AWS Snow bestellen.

   b. Um Amazon EKS Anywhere-Cluster über mehrere Snowball-Edge-Geräte hinweg zu betreiben, wählen Sie im Abschnitt Hochverfügbarkeit die Anzahl der Geräte aus, die Sie in Ihre Bestellung aufnehmen möchten.

2. Um im Abschnitt AWS IoT Greengrass auf Snow ein validiertes AMI für IoT-Workloads einzuschließen, wählen Sie AWS IoT Greengrass Validiertes AMI auf meinem Snow-Gerät installieren aus.
3. Um die Remote-Verwaltung Ihres Snow Family-Geräts durch AWS OpsHub oder Snowball Edge Client zu aktivieren, wählen Sie Ihr Snow-Gerät remote mit AWS OpsHub oder Snowball-Client verwalten aus.
4. Wählen Sie die Schaltfläche Weiter aus.

Schritt 4: Auswählen von Sicherheits-, Versand- und Benachrichtigungseinstellungen

Themen

- Auswählen von Sicherheitseinstellungen

- Wählen Sie Ihre Versandeinstellungen
- Wählen Sie Ihre Benachrichtigungseinstellungen

Auswählen von Sicherheitseinstellungen

Wenn Sie die Sicherheit festlegen, werden die Berechtigungen und Verschlüsselungseinstellungen für Ihren AWS Snow-Family-Geräteauftrag hinzugefügt, um Ihre Daten während der Übertragung zu schützen.

So legen Sie die Sicherheit für Ihren Auftrag fest

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) aus. 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 Schlüssel-ARN eingeben, geben Sie den Amazon-Ressourcennamen (ARN) im Feld Schlüssel-ARN 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:
   - Wählen Sie Snow-Konsole, um eine serviceverknüpfte Rolle zu erstellen und zu verwenden, um in Ihrem Namen auf - AWS Ressourcen zuzugreifen. , um AWS Snow Family Berechtigungen zur Verwendung von Amazon S3 und Amazon Simple Notification Service (Amazon SNS) in Ihrem Namen zu erteilen. Die Rolle gewährt dem Snow-Service AWS Security Token Service (AWS STS)- AssumeRole Vertrauen
   - Wählen Sie Vorhandene Servicerolle hinzufügen, um zu verwenden, um den gewünschten Rollen-ARN anzugeben, oder Sie können die Standardrolle verwenden.
3. Wählen Sie Weiter aus.

Wählen Sie Ihre Versandeinstellungen

Der Empfang und die Rückgabe eines Snow Family-Geräts beinhaltet den hin und her Versand des Geräts. Daher ist es wichtig, dass Sie genaue Versandinformationen angeben.

So geben Sie Versanddetails an

1. Wählen Sie im Abschnitt Versandadresse eine vorhandene Adresse aus oder fügen Sie eine neue Adresse hinzu.

   - Wenn Sie Aktuelle Adresse verwenden wählen, werden die Adressen in der Datei angezeigt. Wählen Sie sorgfältig die gewünschte Adresse aus der Liste aus.
   - Wenn Sie Neue Adresse hinzufügen wählen, geben Sie die angeforderten Adressinformationen ein. Managementkonsole für die AWS Snow-Familie speichert Ihre neuen Versandinformationen.

   > **Note**
   >
   > Das Land, das Sie in der Adresse angeben, muss mit dem Zielland für das Gerät übereinstimmen und für dieses Land gültig sein.

2. Wählen Sie im Abschnitt Versandgeschwindigkeit eine Versandgeschwindigkeit für den Auftrag aus. Diese Geschwindigkeit zeigt, wie schnell das Gerät zwischen Zielen geliefert wird und nicht widerspiegelt, wie schnell es nach dem heutigen Datum eintrifft. Die Versandgeschwindigkeiten, die Sie wählen können, sind:

   - Eintägiger Versand (ein Werktag)
   - Zweitägiger Versand (2 Werktage)
   - Weitere Informationen finden Sie unter Versandunternehmen.

Wählen Sie Ihre Benachrichtigungseinstellungen

Benachrichtigungen aktualisieren Sie über den neuesten Status Ihrer AWS Snow-Family-Geräteaufträge. Sie erstellen ein SNS-Thema und erhalten E-Mails von Amazon Simple Notification Service (Amazon SNS), wenn sich Ihr Auftragsstatus ändert.

Richten Sie Benachrichtigungen wie folgt ein

- Führen Sie im Abschnitt Benachrichtigungen festlegen einen der folgenden Schritte aus:
  - Wenn Sie ein vorhandenes SNS-Thema verwenden möchten, wählen Sie Ein vorhandenes SNS-Thema verwenden und wählen Sie das Thema Amazon-Ressourcenname (ARN) aus der Liste aus.

- Wenn Sie ein neues SNS-Thema erstellen möchten, wählen Sie Neues SNS-Thema erstellen aus. Geben Sie einen Namen für Ihr Thema und eine E-Mail-Adresse ein.

Die Benachrichtigungen werden in etwa einem der folgenden Status Ihres Auftrags angezeigt:

- Job created
- Vorbereitung des Geräts
- Preparing shipment
- In transit to you
- Delivered to you
- Während der Übertragung zu AWS
- Im Sortierzentrum
- At AWS
- Importing
- Completed
- Canceled

Weitere Informationen zu Benachrichtigungen über Auftragsstatusänderungen und verschlüsselten SNS-Themen finden Sie unter Benachrichtigungen für Snow Family-Geräte in diesem Handbuch.

Wählen Sie das Next aus.

Schritt 5: Überprüfen der Auftragsübersicht und Erstellen Ihres Auftrags

Nachdem Sie alle erforderlichen Informationen für Ihren AWS Snow Family-Geräteauftrag angegeben haben, überprüfen Sie den Auftrag und erstellen Sie ihn. Nachdem Sie den Auftrag erstellt haben, AWS beginnt mit der Vorbereitung des Snow Family-Geräts für die Sendung an Sie.

Aufträge unterliegen den Exportkontrollgesetzen in bestimmten Ländern und erfordern möglicherweise eine Exportlizenz. Es gelten auch US-Export- und Reexportgesetz. Die Abweichung von den Gesetzen und Vorschriften des Landes und der USA ist verboten.

1. Überprüfen Sie auf der Seite Auftragsübersicht alle Abschnitte, bevor Sie den Auftrag 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 Auftrag erstellen aus.

> **Note**
>
> Nachdem Sie einen Auftrag erstellt haben, um ein Snow Family-Gerät zu bestellen, können Sie es stornieren, während es sich im Status Auftrag erstellt befindet, ohne dass Gebühren anfallen. Weitere Informationen finden Sie unter Stornieren eines Auftrags über die Managementkonsole für die AWS Snow-Familie.

Nachdem Ihr Auftrag erstellt wurde, können Sie den Status des Auftrags im Abschnitt Auftragsstatus sehen. Ausführliche Informationen zu Auftragsstatus finden Sie unter Auftragsstatus .

Herunterladen AWS OpsHub

Die Geräte der AWS Snow Family bieten ein benutzerfreundliches Tool AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen verwalten können AWS-Services.

Wenn auf Ihrem Client-Computer AWS OpsHub installiert ist, können Sie Aufgaben wie die folgenden ausführen:

- Entsperren und Konfigurieren einzelner oder geclusterter Geräte
- Übertragen von Dateien
- Starten und Verwalten von Instances, die auf Snow Family-Geräten ausgeführt werden.

Weitere Informationen finden Sie unter Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten.

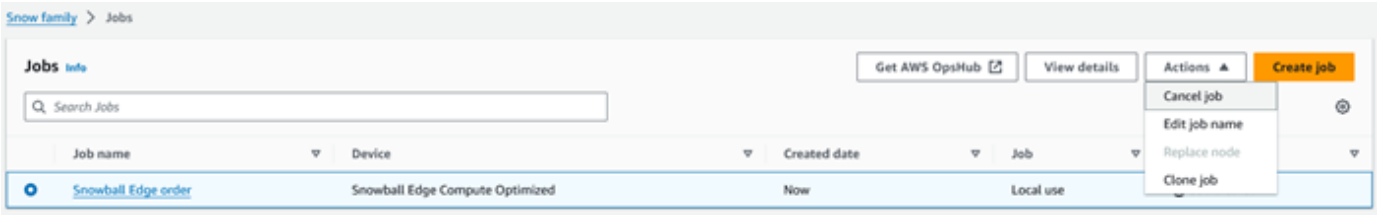
So laden Sie herunter und installieren es AWS OpsHub for Snow Family

1. Klicken Sie in den AWS Snowball Ressourcen auf AWS OpsHub. Wählen Sie im AWS OpsHub Abschnitt mit den Download-Links den entsprechenden Download-Link aus, den Sie AWS OpsHub für Ihr Betriebssystem installieren möchten.
2. Wählen Sie im AWS OpsHub Abschnitt Herunterladen für Ihr Betriebssystem und folgen Sie den Installationsschritten. Wählen Sie danach Next aus.

Stornieren eines Auftrags über die Managementkonsole für die AWS Snow-Familie

Nachdem Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellt haben, können Sie den Auftrag über die abbrechenManagementkonsole für die AWS Snow-Familie. Wenn Sie den Auftrag abbrechen, erhalten Sie das von Ihnen bestellte Gerät nicht. Sie können den Auftrag nur abbrechen, während der Auftragsstatus Auftrags erstellt lautet. Nachdem der Auftrag diesen Status überschritten hat, können Sie den Auftrag nicht abbrechen. Weitere Informationen finden Sie unter Auftragsstatus.

1. Melden Sie sich bei den Managementkonsole für die AWS Snow-Familie an.
2. Wählen Sie den Auftrag aus, der abgebrochen werden soll.
3. Wählen Sie Aktionen. Wählen Sie im daraufhin angezeigten Menü Auftrag abbrechen aus.



4. Das Fenster Auftrag abbrechen wird angezeigt. Um das Abbrechen des Auftrags zu bestätigen, geben Sie ein **`job name`** und wählen Sie Auftrag abbrechen aus. In der Liste der Aufträge wird Cancelled in der Spalte Status angezeigt.

Empfangen des Snowball Edge

Wenn Sie das AWS Snowball Edge Gerät erhalten, stellen Sie möglicherweise fest, dass es nicht in einem Feld enthalten ist. 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 AWS Support und informieren Sie sie über das Problem, damit Ihnen ein neues Gerät zugestellt werden kann.

> **Important**
>
> Das AWS Snowball Edge Gerät ist die Eigenschaft von AWS. Die Überschreitung eines - AWS Snowball Edge Geräts stellt einen Verstoß gegen die Richtlinie AWS für zulässige Nutzung dar. Weitere Informationen finden Sie unter AWS Akzeptable Nutzungsrichtlinie.

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: Herstellen einer Verbindung mit Ihrem lokalen Netzwerk

Herstellen einer Verbindung mit Ihrem lokalen Netzwerk

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 verfügt über drei Drucker: eine Front, eine Back und eine Top-.

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 Front- und Back-Kabel, während Sie das Snowball-Edge-Gerät verwenden. Die offenen Kabel ermöglichen das Abkühlen des Geräts. Das Schließen der Kabel während der Verwendung des Geräts kann dazu führen, dass das Gerät heruntergefahren wird, um eine Kabelablösung zu verhindern.

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 Netzwerkkabel aus – RJ45, SFP+ oder QSFP+ – 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 die Einschalttaste über der 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 Beheben von Problemen beim Hochfahren.

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

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

   Es wird ein Bildschirm angezeigt, auf dem Sie die aktuellen Netzwerkeinstellungen für das AWS Snowball Edge Gerät sehen. Die IP-Adresse unter dem Dropdown-Feld wird automatisch aktualisiert, um die vom AWS Snowball Edge Gerät angeforderte DHCP-Adresse widerzuspiegeln.

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 und ändern Sie nicht seine Verbindungseinstellungen, während es verwendet wird.

Weiter: Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät

Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät

Jeder Auftrag verfügt über einen Satz von Anmeldeinformationen, die Sie von der Managementkonsole für die AWS Snow-Familie oder der Auftragsverwaltungs-API abrufen müssen, um Ihren Zugriff auf das Snow Family-Gerät 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 Auftrags in der anzeigen Managementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter Job Statuses.

So rufen Sie Ihre Anmeldeinformationen mit der Konsole ab

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Managementkonsole für die AWS Snow-Familie.
2. Suchen Sie in der -Konsole in der Tabelle nach dem spezifischen Auftrag, für den das Auftragsmanifest heruntergeladen werden soll, und wählen Sie dann diesen Auftrag aus.

3. Erweitern Sie diesen Bereich Auftragsstatus und wählen Sie Auftragsdetails 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 angeben müssen, um das Gerät zu entsperren.
   - Wählen Sie im Dialogfeld Manifest herunterladen aus und folgen Sie den Anweisungen, um die Auftragsmanifestdatei auf Ihren Computer herunterzuladen. Der Name Ihrer Manifestdatei enthält Ihre Job ID (Auftrags-ID).

> **Note**
>
> Es wird empfohlen, keine Kopie des Entsperrcodes am selben Speicherort auf dem Computer wie das Manifest für diesen Auftrag zu speichern. Weitere Informationen finden Sie unter Bewährte Methoden für die Verwendung des Snowball Edge-Geräts.

Nachdem Sie nun über Ihre -Anmeldeinformationen verfügen, besteht der nächste Schritt darin, den Snowball-Edge-Client herunterzuladen, der zum Entsperren des AWS Snowball Edge Geräts verwendet wird.

Weiter: Herunterladen und Installieren des Snowball Edge-Clients

Herunterladen und Installieren des Snowball Edge-Clients

Der Snowball Edge-Client ist das Tool, mit dem Sie das AWS Snowball Edge Gerät entsperren. Wir empfehlen Ihnen, die AWS OpsHub for Snow Family Anwendung zu verwenden. Anweisungen finden Sie unter Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten.

Sie können den Snowball Edge-Client von der AWS Snowball Ressourcenseite auf eine leistungsstarke Workstation herunterladen und installieren, die Sie besitzen.

Weiter: Entsperren des Snow Family-Geräts

Entsperren des Snow Family-Geräts

In diesem Abschnitt wird das Entsperren des Snow Family-Geräts mithilfe der Snowball Edge CLI beschrieben. Informationen zum Entsperren des Geräts mit AWS OpsHub, einem Tool für die

grafische Benutzeroberfläche (GUI) für Snow-Family-Geräte, finden Sie unter Entsperren eines Geräts

Bevor Sie ein Gerät der Snow Family verwenden, um Daten zu übertragen oder Edge-Computing-Aufgaben auszuführen, müssen Sie das Gerät entsperren. Beim Entsperren des Geräts authentifizieren Sie Ihre Fähigkeit, darauf zuzugreifen, 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 zu oder von diesem verschieben, Amazon-ECEC2-compatible einrichten und verwenden und vieles mehr.

Vor dem Entsperren eines Geräts muss das Gerät an Strom und Netzwerk angeschlossen, aktiviert und eine IP-Adresse zugewiesen werden. Siehe Herstellen einer Verbindung mit Ihrem lokalen Netzwerk Sie benötigen die folgenden Informationen über das Snow Family-Gerät:

- Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients.
- Rufen Sie die Anmeldeinformationen von der ab Managementkonsole für die AWS Snow-Familie. Für ein oder mehrere eigenständige Geräte die Entsperrcodes und die Manifestdatei für jedes Snow Family-Gerät. 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 Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät.
- Schalten Sie jedes Gerät ein und verbinden Sie es mit Ihrem Netzwerk. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem lokalen Netzwerk.

So entsperren Sie ein eigenständiges Gerät mit dem Snowball Edge-Client

1. Suchen Sie die IP-Adresse für das AWS Snowball Edge Gerät auf der Bol-Anzeige des AWS Snowball Edge Geräts auf der Registerkarte Verbindungen. Notieren Sie die IP-Adresse.
2. Verwenden Sie den `unlock-device` Befehl , um Ihren Zugriff auf das Snow Family-Gerät mit der IP-Adresse des Snow Family-Geräts 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 zeigt an, dass es erfolgreich entsperrt wurde, mit der folgenden Meldung.

```
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 zurückgibt`connection refused`, finden Sie weitere Informationen unter Fehlerbehebung beim Entsperren eines Snow Family-Geräts.

Example des **`unlock-device`** Befehls

In diesem Beispiel lautet die IP-Adresse für das Gerät `192.0.2.0`, der Manifestdateiname ist `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin`und der 29-stellige Entsperrcode ist `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-Adresse jedes der Geräte im Cluster auf der Bol-Anzeige 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 Cluster von AWS Snowball Edge Gerätegeräten mit 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 zeigt an, dass er erfolgreich entsperrt wurde, mit der folgenden Meldung.

```
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 zurückgibt`connection refused`, finden Sie weitere Informationen unter Fehlerbehebung beim Entsperren eines Snow Family-Geräts.

Example des **`unlock-cluster`** Befehls

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

Fehlerbehebung beim Entsperren eines Snow Family-Geräts

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

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.

   a. Verwenden Sie den Bildschirm Bol auf dem Gerät, um zu überprüfen, 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 Managementkonsole für die AWS Snow-Familie, 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 erlaubt wird. Verwenden Sie den `ping` Befehl für Ihr Betriebssystem, um festzustellen, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen von Antivirensoftware, Firewall-Konfiguration, Virtual Private Network (VPN) oder anderen Konfigurationen Ihres Computers und Netzwerks.

Jetzt können Sie das Snow Family-Gerät verwenden.

Weiter: Einrichten von lokalen Benutzern

Einrichten von lokalen Benutzern

Im Folgenden finden Sie 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 Abrufen von Anmeldeinformationen.
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 zum Konfigurieren der AWS CLI finden Sie unter Konfigurieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.
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 --profile ProfileID --region
 snow --user-name UserName
```

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 Serviceverwaltungsaufgaben 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**
>
> Dieses Szenario erfordert IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden. Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

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

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

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.

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

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

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

Weitere Informationen zur lokalen Verwendung von IAM finden Sie unter Lokales Verwenden von IAM.

Weiter: Verwenden eines AWS Snowball Edge-Geräts

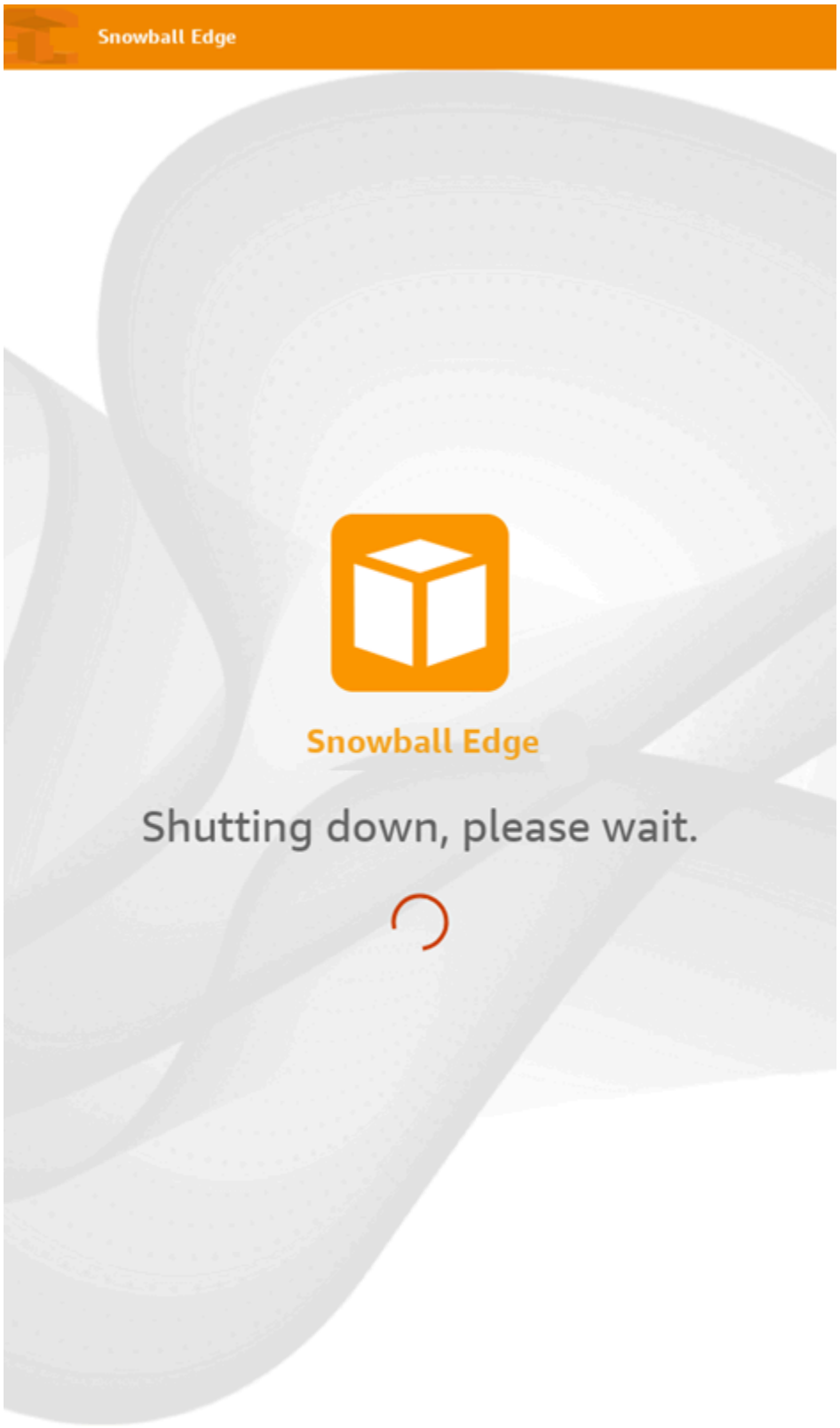
Neustarten des Snow Family-Geräts

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

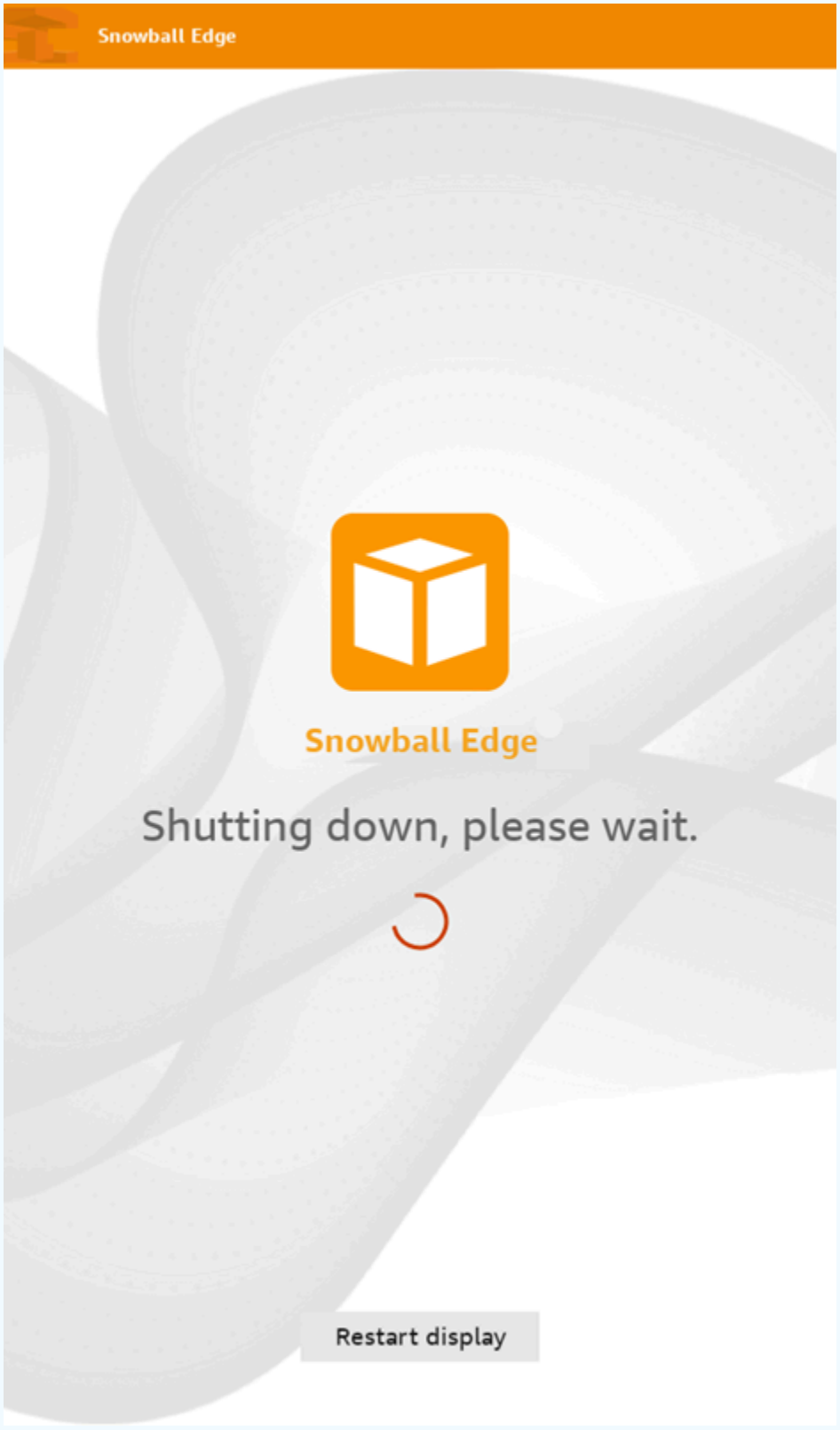
So starten Sie das Gerät mit der Einschalttaste neu:

1. Wenn die gesamte Kommunikation mit dem Gerät beendet ist, schalten Sie sie aus, indem Sie die Netztaste über dem drücken. Das Herunterfahren des Geräts dauert ca. 20 Sekunden.

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



> **Note**
>
> Wenn auf dem Bildschirm des Bildschirms das Herunterfahren angezeigt wird, wenn das Gerät nicht tatsächlich heruntergefahren wird, drücken Sie die Schaltfläche Anzeige neu starten auf dem Bildschirm, um den Bildschirm wieder in den normalen Betrieb zu versetzen.


Snowball Edge
Snowball Edge
Shutting down, please wait.
Restart display

2. Drücken Sie die Einschalttaste. 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 Entsperren des Snow Family-Geräts.

So starten Sie das Gerät mit dem Snowball Edge-Client neu:

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.

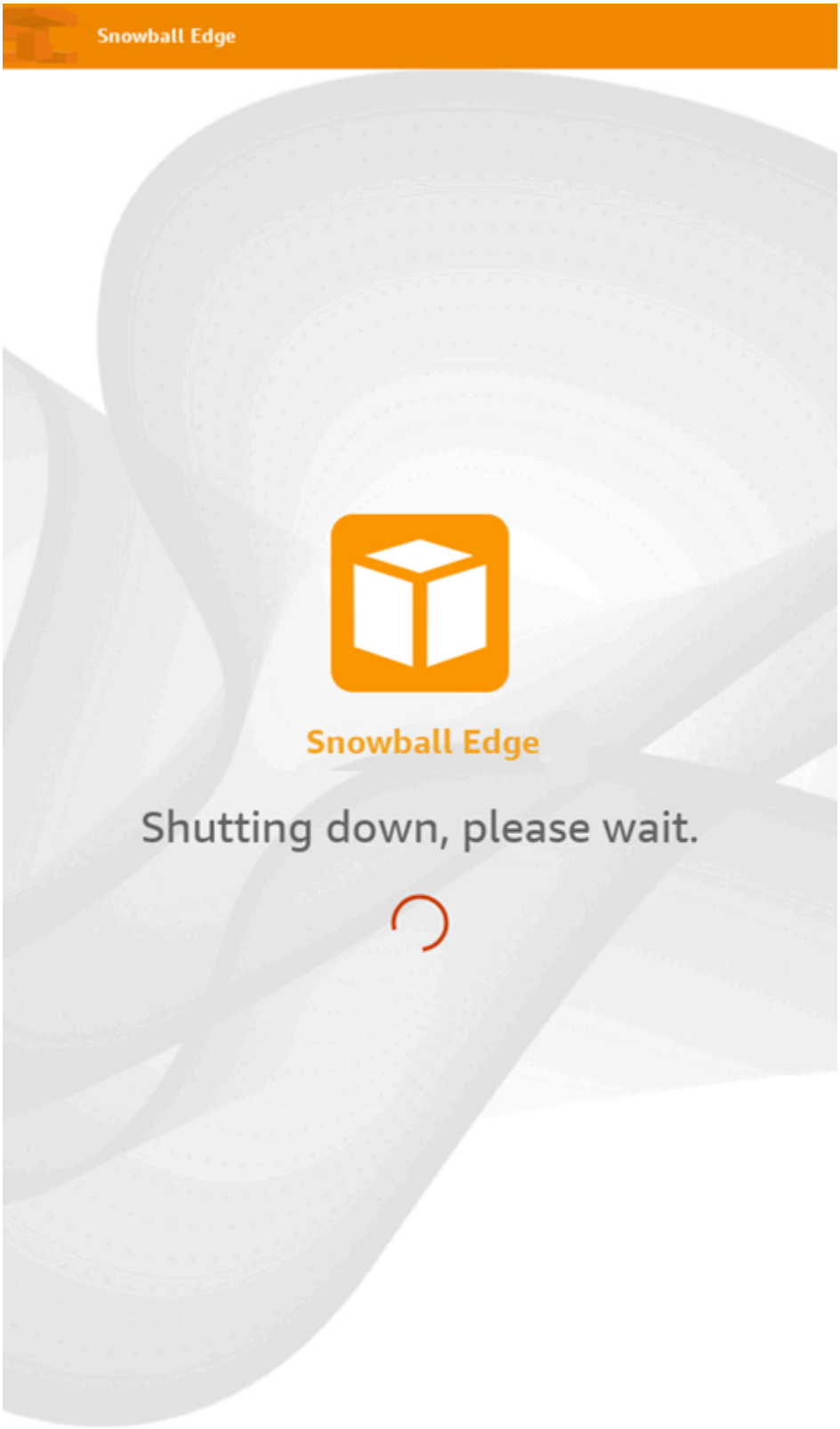
   ```
   snowballEdge reboot-device
   ```

2. Entsperren Sie das Gerät. Siehe Entsperren des Snow Family-Geräts.

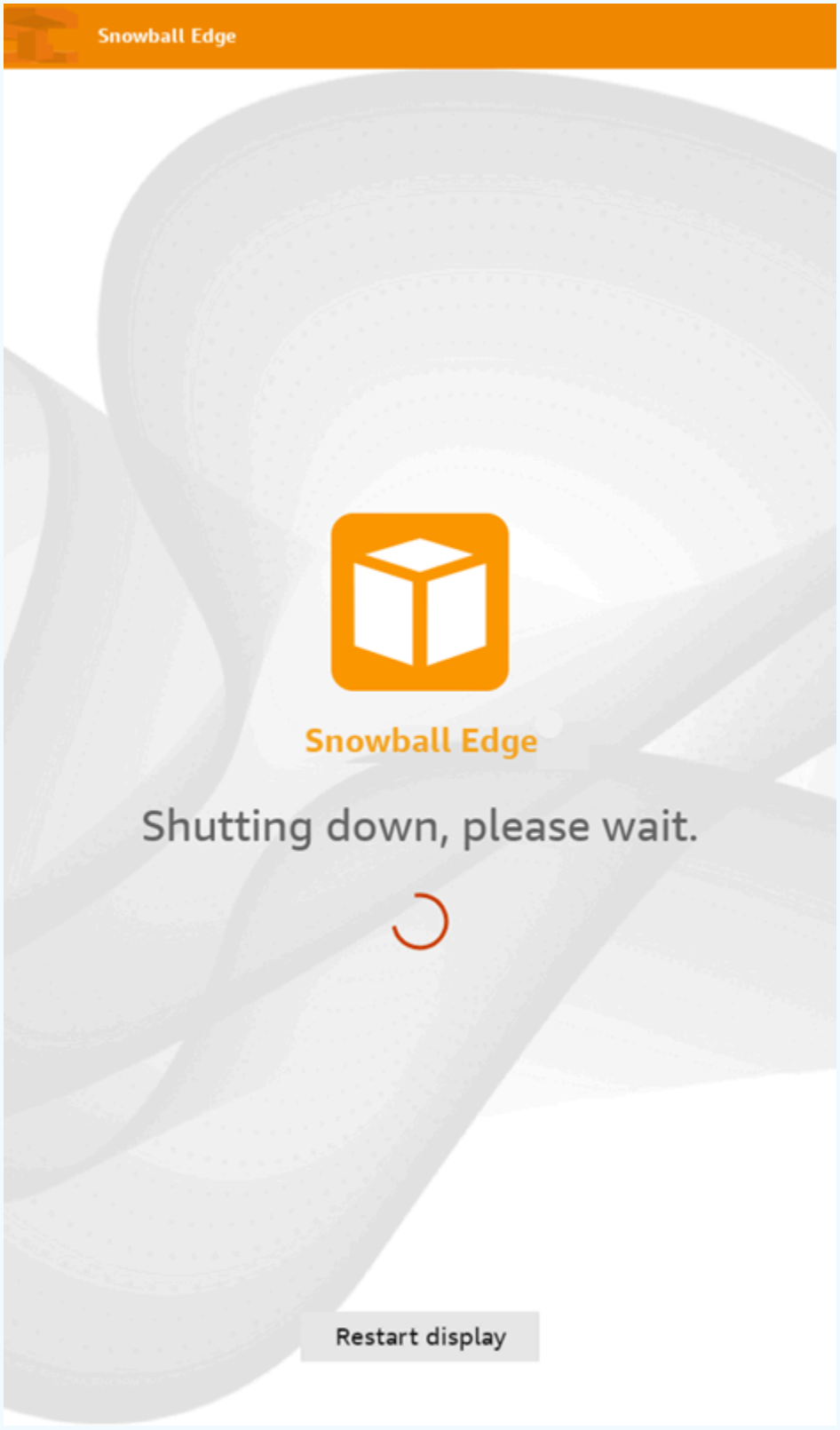
Ausschalten des Snowball Edge

Wenn Sie die Übertragung von Daten auf das AWS Snowball Edge Gerät abgeschlossen haben, bereiten Sie sie für den Rückweg zu 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 Verwalten der NFS-Schnittstelle.

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


Snowball Edge
Snowball Edge
Shutting down, please wait.

> **Note**
>
> Wenn auf dem Bildschirm Bol die Meldung zum Herunterfahren angezeigt wird, wenn das Gerät nicht tatsächlich heruntergefahren wird, drücken Sie die Schaltfläche Display neu starten auf dem Bildschirm, um den Bildschirm wieder in den normalen Betrieb zu versetzen.


Snowball Edge
Snowball Edge
Shutting down, please wait.
Restart display

Nachdem das Gerät heruntergefahren wurde, werden die Versandinformationen auf der E-Ink-Anzeige angezeigt.

Weiter: Zurückgeben des Snowball Edge-Geräts

Zurückgeben des Snowball Edge-Geräts

Die vorab angezeigten Versandinformationen auf der E-Ink-Anzeige enthalten die Adresse, an die das AWS Snowball Edge Gerät zurückgegeben werden soll. Informationen darüber, mit welchem Mobilfunkanbieter das Gerät zurückgegeben werden soll, finden Sie unter Spediteure.

> **Note**
>
> Sobald Sie das Snow-Gerät für den Import in Amazon S3 zurückgegeben haben, AWS beginnt mit der Aufnahme der Daten, nachdem sichergestellt wurde, dass das Gerät nicht manipuliert wurde und dass das Gerät fehlerfrei ist. Falls Sie nicht möchten, dass die Daten auf dem Gerät in Ihren S3-Ziel-Bucket aufgenommen werden, können Sie den Snow-Auftrag abbrechen. Wenn Sie den Auftrag abbrechen, überspringen wir die Datenübertragung und löschen das Gerät sicher nach den festgelegten Prozessen. Aufgrund unserer strengen Kette von Aufbewahrungs- und Betriebsverfahren können wir kein Gerät mit Ihren Daten in unseren Einrichtungen aufbewahren.

Das Gerät wird an eine AWS Sortiereinrichtung geliefert und an das AWS Rechenzentrum weitergeleitet. Der Mobilfunkanbieter stellt automatisch eine Nachverfolgungsnummer für Ihren Auftrag an den bereit Managementkonsole für die AWS Snow-Familie. Sie können auf die Nachverfolgungsnummer und einen Link zur Nachverfolgungswebsite des Mobilfunkanbieters zugreifen, indem Sie die Statusdetails des Auftrags in der Konsole anzeigen oder Aufrufe an die Auftragsverwaltungs-API tätigen.

Sie können die Statusänderungen Ihres Auftrags über die verfolgen, Managementkonsole für die AWS Snow-Familie während das Gerät AWS verarbeitet. Sie können Amazon SNS-Benachrichtigungen verwenden, wenn Sie diese Option bei der Auftragserstellung ausgewählt haben, oder Sie können Aufrufe an die Auftragsverwaltungs-API tätigen. Weitere Informationen zu dieser API finden Sie in der APIAWS Snowball -Referenz zu .

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

Vorbereiten eines AWS Snowball Edge-Geräts für den Versand

Im Folgenden wird erläutert, wie Sie ein AWS Snowball Edge Gerät vorbereiten und an zurücksenden AWS.

So bereiten Sie ein AWS Snowball Edge Gerät für den Versand vor

1. Trennen Sie das Stromkabel und hängen Sie es im Kabelknoten oben auf dem AWS Snowball Edge Gerät ab.
2. Schließen Sie die Kabel auf der Rück-, oberen und oberen Seite des AWS Snowball Edge Geräts. Drücken Sie ein, bis Sie hören und sie klicken.

Sie müssen das AWS Snowball Edge Gerät nicht in einen Container packen, da es sich bei dem Gerät selbst um einen eigenen physisch hängenden Versandcontainer handelt. Die Anzeige E Ink oben auf dem AWS Snowball Edge Gerät zeigt die Rücksendeinformationen an, wenn das Gerät ausgeschaltet ist.

Auftragstypbezogene Überlegung

> **Important**
>
> Wenn Sie Daten importieren, löschen Sie Ihre lokalen Kopien der übertragenen Daten erst, wenn der Import in Amazon S3 am Ende des Prozesses erfolgreich war, und Sie können die Ergebnisse der Datenübertragung überprüfen.

Versand von Artikeln der Snow Family

Das AWS Snowball Edge Gerät wird von einem - AWS Rechenzentrum aus versendet und an dieses geliefert. Die vorab angezeigten Versandinformationen auf dem Bildschirm E Ink auf dem Gerät enthalten die Adresse, an die das AWS Snowball Edge Gerät zurückgegeben werden soll. Die Versandgeschwindigkeit für die Rückgabe entspricht der ursprünglichen Versandgeschwindigkeit, als Sie das Gerät erhalten haben. Sie können Statusänderungen mithilfe der verfolgen Managementkonsole für die AWS Snow-Familie und den Fortschritt des Pakets über den Mobilfunkanbieter Ihrer Region verfolgen.

Weitere Informationen zum Zurückgeben Ihres AWS Snowball Edge Geräts finden Sie unter Spediteure.

> **Important**
>
> Sofern nicht anders von angewiesen AWS, hängen Sie niemals ein separates Versandetikett an das AWS Snowball Edge Gerät an. Verwenden Sie immer die Versandinformationen, die auf der Anzeige E Ink des AWS Snowball Edge Geräts angezeigt werden.

Spediteure

Wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen, geben Sie die Adresse an, an die das AWS Snowball Edge Gerät gesendet werden soll. Der Transporteur, der Ihre Region unterstützt, übernimmt den Versand von Geräten von AWS an Sie und von Ihnen zurück an AWS. Sie können die Informationen zum ausgehenden Versand sehen, wenn Ihr Auftrag den Status Vorbereiten der Sendung erreicht.

Für jedes ausgelieferte AWS Snowball Edge Gerät gibt es eine Nachverfolgungsnummer. Sie finden die Nachverfolgungsnummer und einen Link zur Nachverfolgungswebsite über das Managementkonsole für die AWS Snow-Familie Auftrags-Dashboard oder die Auftragsverwaltungs-API.

Diese Mobilfunkanbieter werden für AWS Snowball Edge-Geräte unterstützt:

- Für Indien ist Blue Dart der Mobilfunkanbieter.
- Für Korea, Japan, Australien und Indonesien ist Kuehne + der Mobilfunkanbieter.
- Für China und Hong Kong ist S.F. Express der Mobilfunkanbieter.
- In allen anderen Regionen erfolgt der Versand per UPS.

Themen

- AWS Snowball Transporte in Singapur, Japan und Indonesien
- AWS Snowball Empfang und Rückgabe in Bol, Vereinigte Arabische Emirate
- Versandgeschwindigkeiten

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

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

- Planen Sie direkt eine Annahme mit microSD oder bringen Sie das AWS Snowball Edge Gerät in eine Einrichtung für das Drop-off von microSD-Paketen, um es an zu senden AWS.
- Das Telefonie-Versandetikett auf der E-Ink-Anzeige enthält die Rückgabeadresse für das AWS Snowball Edge Gerät.
- Das AWS Snowball Edge Gerät wird an eine AWS Sortiereinrichtung geliefert und an ein AWS Rechenzentrum weitergeleitet. Bol stellt Ihnen eine Nachverfolgungsnummer zur Verfügung.

> **Important**
>
> Sofern nicht anders von angewiesen AWS, hängen Sie niemals ein separates Versandetikett an das AWS Snowball Edge Gerät an. Verwenden Sie immer die Versandinformationen, die auf der E-Ink-Anzeige des Geräts angezeigt werden.

Bol sendet Snowball Edge-Geräte in die folgenden EU-Mitgliedslander: Österreich, Italien, Bulgarien, Italien, Polen, Zypern, Tschechien, Estland, Finnland, Frankreich, Deutschland, Spanien, Ungarn, Italien, Irland, Lettland, Litauen, Luxemburgembourg, Malta, Polen, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien und Italien.

> **Note**
>
> Bestellungen zwischen dem Vereinigten Königreich und den Ländern der EU gelten jetzt als international und erfordern die Genehmigung durch einen speziellen internationalen Prozess. Wenn Sie Ihr Gerät zwischen dem Vereinigten Königreich und der EU versenden müssen, senden Sie uns eine E-Mail an `<snowball-shipping@amazon.com>`, um eine

kommerzielle Rechnung anzufordern, bevor Sie eine Annahme oder einen Drop-off bei Bol arrangieren.

Die microSD-Services für die Snow-Produktfamilie sind nur innerhalb eines Landes regional.

AWS Snowball -Abholungen in Großbritannien

Beachten Sie in Großbritannien die folgenden Informationen, damit Bol einen Snowball Edge aufnehmen kann:

- Sie arrangieren, dass microSD das AWS Snowball Edge Gerät abholt, indem Sie direkt eine Annahme mit microSD planen, oder bringen das AWS Snowball Edge Gerät in eine microSD-Paket-Drop-off-Einrichtung, um an gesendet zu werden AWS.
- Das Telefonie-Versandetikett auf der E-Ink-Anzeige enthält die richtige Adresse für die Rückgabe des AWS Snowball Edge Geräts.
- Das AWS Snowball Edge Gerät wird an eine AWS Sortiereinrichtung geliefert und an das AWS Rechenzentrum weitergeleitet. UPS übermittelt Ihnen automatisch eine Sendungsverfolgungsnummer zu Ihrem Auftrag.

Important

Sofern von nicht anders angegeben AWS, hängen Sie niemals ein separates Versandetikett an das AWS Snowball Edge Gerät an. Verwenden Sie immer die Versandinformationen, die auf der E-Ink-Anzeige des Geräts angezeigt werden.

Die -Services für die Snow-Produktfamilie sind nur innerhalb eines Landes regional.

Note

Seit Januar 2021 ist Großbritannien nicht mehr Teil der EU. Bei Bestellungen zwischen Großbritannien und anderen EU- Ländern handelt es sich um internationale Bestellungen. Dabei handelt es sich um einen nicht allgemeinen Verfügbarkeitsprozess, der nur durch einen speziellen internationalen Prozess genehmigt wurde. Wenn ein Kunde eine Genehmigung erhalten hat und ein Gerät aus einem EU-Land zurück an LHR oder aus Großbritannien zurück an ein EU-Land zurückgibt, muss er zunächst eine Rückgabe

an <snowball-shipping@amazon.com> beantragen, damit eine Handelsrechnung ausgestellt werden kann, bevor er die Annahme/Abgabe mit Bol anfordert.

AWS Snowball -Abholungen in Brasilien

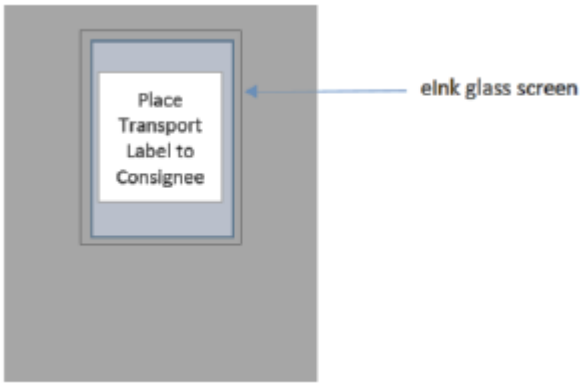
Im Folgenden finden Sie einige Richtlinien für Bol, um ein Snowball-Edge-Gerät in Brasilien zu übernehmen:

- Wenn Sie bereit sind, ein Snowball-Edge-Gerät zurückzugeben, rufen Sie 0800-770-9035 auf, um eine Annahme mit Bol zu planen.
- Snowball Edge ist in Brasilien verfügbar, das 26 Bundesstaaten und das 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. Vergewissern Sie sich bei Ihrer Steuerabteilung, welches der folgenden Dokumente in Ihrem Bundesstaat erforderlich ist, gemäß Ihrer Registrierung von Imposto sobreão deadorias e Servios (ICMS):
  - Innerhalb von São Paulo – In der Regel sind eine Nicht-ICMS-Deklaration und eine Rechnung für die elektronische Steuer (NF-e) erforderlich.
  - Außerhalb von São Paulo – In der Regel ist Folgendes erforderlich:
    - Eine Erklärung zur Befreiung von der Warenumlaufsteuer
    - Eine Nota Fiscal
    - Elektronische Steuerrechnung (NF-e)

> **Note**
>
> Für die Deklaration eines Nicht-ICMS-Steuerzahlers empfehlen wir, vier Kopien der Deklaration zu generieren: eine Kopie für Ihre Datensätze und die anderen drei für den Transport.

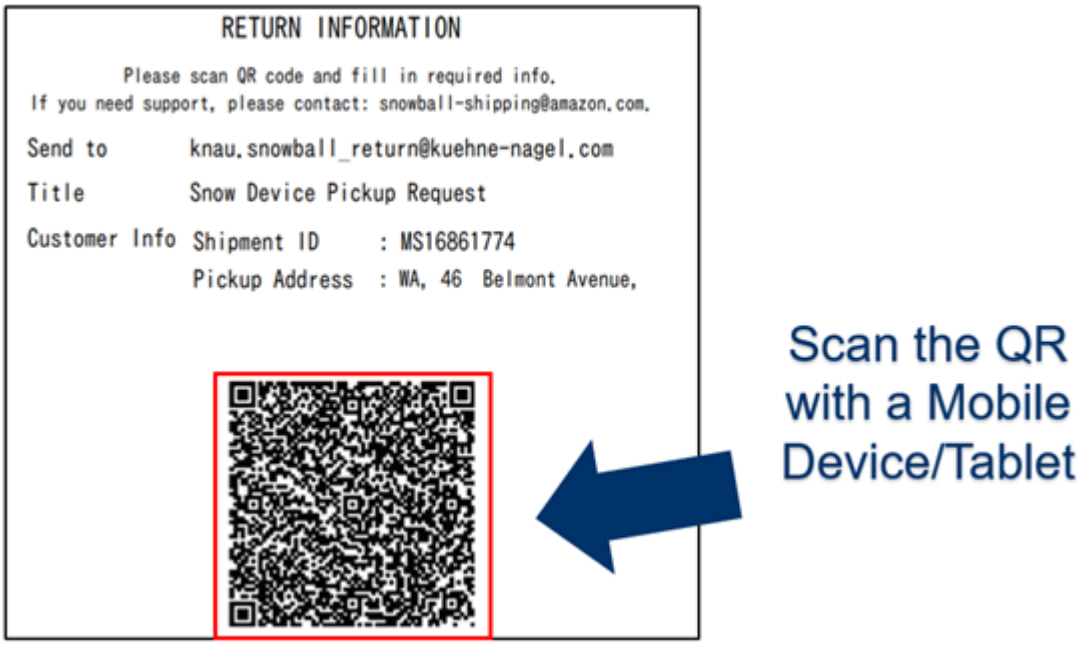
AWS Snowball -Abholungen in Australien

Wenn Sie in Australien ein AWS Snowball Edge Gerät zurück nach senden AWS, platzieren Sie das Rückgabetransportetikett (in der Maske mit diesen Anweisungen zu finden) über das E-Ink-Label auf dem Snow-Gerät.



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

Um die Rückgabe des Snow Family-Geräts anzuordnen, scannen Sie den QR-Code auf den Rückgabeanweisungen mit Ihrem Mobilgerät. Auf Ihrem Gerät wird ein Hyperlink zu einer E-Mail-Nachricht angezeigt. Die Nachricht enthält Informationen wie E-Mail-Adresse, Betreff und Kontrollnummer oder Konsignationsnummer. Geben Sie das Datum, den Namen und die Kontaktdaten der Annahme ein oder geben Sie eine neue Annahmeadresse an, falls Änderungen vorgenommen werden.



AWS Snowball -Abholungen in Indien

In Indien übernimmt Blue Dart das Snowball-Gerät. Wenn Sie bereit sind, Ihr Snowball-Gerät zurückzugeben, schalten Sie es aus und bereiten Sie es für den Rücksende 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:

- Auftrags-ID – Die Auftrags-ID, die dem Snowball zugeordnet ist, den Sie an zurückgeben möchten AWS.
- AWS-Konto ID – Die ID für das AWS Konto, das den Auftrag erstellt hat.
- Früheste Annahmezeit (Ihre Ortszeit) – Die früheste Uhrzeit, zu der der Snowball abgeholt werden soll.
- Letzte Aufnahmezeit (Ihre Ortszeit) – Die letzte Uhrzeit, zu der der Snowball abgeholt werden soll.
- Spezielle Anweisungen (optional) – Alle speziellen Anweisungen für die Aufnahme des Snowballs, einschließlich Kontaktdaten für die Koordination der Aufnahme.

Das Snowball-Team ordnet die Aufnahme mit Blue Dart an und sendet Ihnen eine Bestätigungs-E-Mail. Blue Dart stellt Ihnen ein Papier-Versandetikett zur Verfügung und holt das Snowball-Gerät ab.

> **Important**
>
> Wenn Sie einen Snowball in Indien verwenden, denken Sie daran, alle relevanten Steuerdokumente bei Ihrem Bundesstaat einzureichen.

AWS Snowball Edge-Abholungen 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:

- Auftrags-ID – Die Auftrags-ID, die dem Snowball zugeordnet ist, den Sie an zurückgeben möchten AWS.
- Aufnahmeadresse – Die Adresse, an der das Gerät abgeholt wird.
- Aufnahmedatum – Der früheste Tag, an dem das Gerät abgeholt werden soll.
- Kontaktdatenpunkt – Der Name, die E-Mail-Adresse und die lokale Telefonnummer, die Kuehne + verwenden kann, um sich bei Bedarf mit Ihnen in Verbindung zu setzen.

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.

AWS Snowball Edge-Abholungen in Hong Kong

In Hong Kong übernimmt S.F. Express Ihre -Abholungen. Wenn Sie bereit sind, Ihr Gerät zurückzugeben, senden Sie eine E-Mail mit der Snowball-Abholanfrage in der Betreffzeile an snowball-shipping-ap-east-1@amazon.com, damit wir die Aufnahme für Sie planen können. Geben Sie im Text der E-Mail folgende Informationen an:

- Auftrags-ID
- AWS-Konto ID
- Name des Ansprechpartners
- Telefonnummer des Ansprechpartners
- E-Mail-Adresse des Ansprechpartners

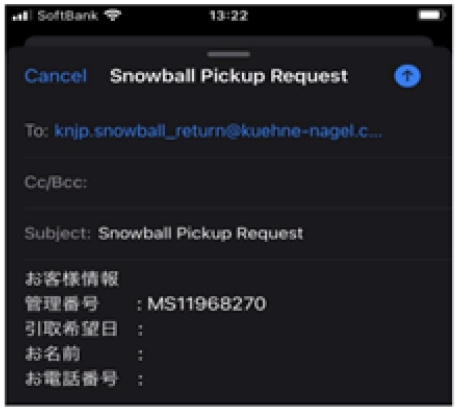
- Der Tag, an dem die Geräte abgeholt werden sollen
- Früheste Abholzeit
- Späteste Abholzeit
- Abholadresse

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

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

AWS Snowball Transporte in Singapur, Japan und Indonesien

Wenn Sie in Singapur, Japan und Indonesien bereit sind, Ihr Gerät zurückzugeben, scannen Sie mit Ihrem Mobiltelefon den QR-Code, der auf dem E-Ink-Rückgabeetikett angezeigt wird. Dadurch gelangen Sie direkt zu einer E-Mail-Vorlage. Bitte geben Sie Datum/Uhrzeit der Annahme und Kontaktdaten ein.



> **Note**
>
> Wenn sich Ihre Annahmeadresse von der Adresse unterscheidet, an die das Gerät geliefert wurde, fügen Sie bitte die neue Adresse im E-Mail-Text hinzu, damit der Mobilfunkanbieter informiert werden kann.

> **Note**
>
> In Japan erhebt das Versandunternehmen eine Versandgebühr von 120,00 USD. Die Beschreibung der Gebühr zeigt Snowball an, aber die Gebühr gilt für den Versand aller Snow Family-Geräte.

AWS Snowball Empfang und Rückgabe in Bol, Vereinigte Arabische Emirate

Im Folgenden finden Sie einige Richtlinien, die Sie befolgen müssen, wenn Sie ein AWS Snowball Edge Gerät in Bol empfangen oder zurückgeben.

Empfangen eines Snowball Edge-Geräts

Wenn Sie ein Snowball Edge-Gerät in einer kostenlosen Zone erhalten und von darüber informiert werden, dass das Paket für die Zustellung bereit ist, beantragen Sie den Torpass für Ihre kostenlose Zone, erhalten Sie ihn und geben Sie ihn frei.

Wenn Sie sich in einer Freizone oder im Festland befinden, signieren Sie den Zustellungsnachweis (POD), wenn Sie das Gerät erhalten.

Zurückgeben eines Snowball Edge-Geräts

Wenn Sie ein Snowball-Edge-Gerät zurückgeben, ordnen Sie zu, dass Bol das Gerät aufnimmt, indem Sie direkt auf 600 544 743 oder über die microSD-Website eine Aufnahme mit microSD planen. Stellen Sie sicher, dass die Rücksendeinformationen auf der E-Ink-Anzeige angezeigt werden, bevor das Gerät abgeholt wird. Siehe Zurückgeben des Snowball Edge-Geräts. Wenn Sie in einer kostenlosen Zone darüber informiert werden, dass ein Bol-Treiber für die Aufnahme des Geräts zugewiesen ist, beantragen, erhalten und teilen Sie den Torpass für Ihre kostenlose Zone.

Die Telefonie-Versandinformationen auf der E-Ink-Anzeige enthalten die richtige Adresse, um das Snowball-Edge-Gerät zurückzugeben.

Das Snowball Edge-Gerät wird an eine AWS Sortiereinrichtung geliefert und an das AWS Rechenzentrum weitergeleitet. microSD stellt automatisch eine Nachverfolgungsnummer für Ihren Auftrag bereit.

> **Important**
>
> Sofern von nicht anders angegeben AWS, fügen Sie dem Snowball Edge-Gerät niemals ein separates Versandetikett an. Verwenden Sie immer das Versandetikett, das auf der E-Ink-Anzeige des Geräts angezeigt wird.

Die -Services für die Snow-Produktfamilie gelten nur innerhalb eines Landes.

Versandgeschwindigkeiten

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

- Australien, Japan, Singapur, Indonesien, S.Korea – Wenn Sie innerhalb dieser Länder versenden, haben Sie Zugriff auf die Standard-Versandgeschwindigkeit von 1–3 Tagen.
- Brasilien – Wenn Sie innerhalb Brasiliens versenden, haben Sie Zugriff auf den Express- Saver-Versand von Bol microSD, der innerhalb von zwei Werktagen während der Geschäftszeiten geliefert wird. Die Transportdauer kann durch Verspätungen an den zwischenstaatlichen Grenzen verlängert werden.
- Europa (EU) – Wenn Sie in eines der Länder innerhalb der EU versenden, haben Sie Zugriff auf Express-Versand. In der Regel werden AWS Snowball Edge Geräte, die Express geliefert werden, in 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.
- Hong Kong – Wenn Sie innerhalb von Hong Kong versenden, haben Sie Zugriff auf Express-Versand.
- Indien – Beim Versand innerhalb Indiens werden Snowball Edge-Geräte innerhalb von AWS 7 Tagen nach Erhalt aller zugehörigen Steuerdokumente versendet.
- Bol, Vereinigte Arabische Emirate – Sie haben Zugriff auf den Versand von Courier Express Saver.
- Großbritannien (UK) – Wenn Sie innerhalb Großbritanniens versenden, haben Sie Zugriff auf Express-Versand. In der Regel werden ausgelieferte Snowball Edge-Geräte in etwa einem Tag

geliefert. Darüber hinaus haben Sie Zugriff auf den Standard-Versand, der normalerweise weniger als eine Woche dauert.

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

Überwachen des Importstatus

Um den Status Ihres Importauftrags in der Konsole zu überwachen, melden Sie sich bei der in der AWS-Region an, Managementkonsole für die AWS Snow-Familie in der der Auftrag 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 Auftrag ausgewählt haben, werden detaillierte Informationen für diesen Auftrag in der Tabelle angezeigt, einschließlich einer Leiste, die den Echtzeitstatus Ihres Auftrags anzeigt.

> **Note**
>
> Wenn wir aufgrund eines Problems mit den von Ihnen konfigurierten Zugriffsberechtigungen keine Daten vom Snow-Gerät in unsere Rechenzentren importieren können, versuchen wir, Sie zu benachrichtigen, und Sie haben 30 Tage ab dem Datum, an dem wir die Benachrichtigung zur Behebung des Problems bereitstellen, Zeit. Wenn das Problem nicht behoben ist, brechen wir möglicherweise Ihren AWS Snow Family Auftrag ab und löschen Daten vom Gerät.

Nachdem Ihr Gerät bei angekommen ist AWS, ändert sich Ihr Auftragsstatus von Bei der Übertragung zu AWS AWS. Im Durchschnitt dauert es einen Tag, bis Ihr Datenimport in Amazon S3 beginnt. Der Status Ihres Auftrags wechselt dann zu Importing (Wird importiert). Es dauert ungefähr die gleiche Zeit AWS , bis Ihre Daten vom Snow-Family-Gerät importiert hat, wie Sie sie auf das Snow-Family-Gerät verschieben. Nachdem Ihre Daten importiert wurden, ändert sich der Auftragsstatus in Abgeschlossen.

Jetzt AWS Snowball ist Ihr erster Datenimportauftrag in Amazon S3 mit 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 Abrufen Ihres Auftragsabschlussberichts und der Protokolle auf der Konsole.

Weiter: Abrufen Ihres Auftragsabschlussberichts und der Protokolle auf der Konsole

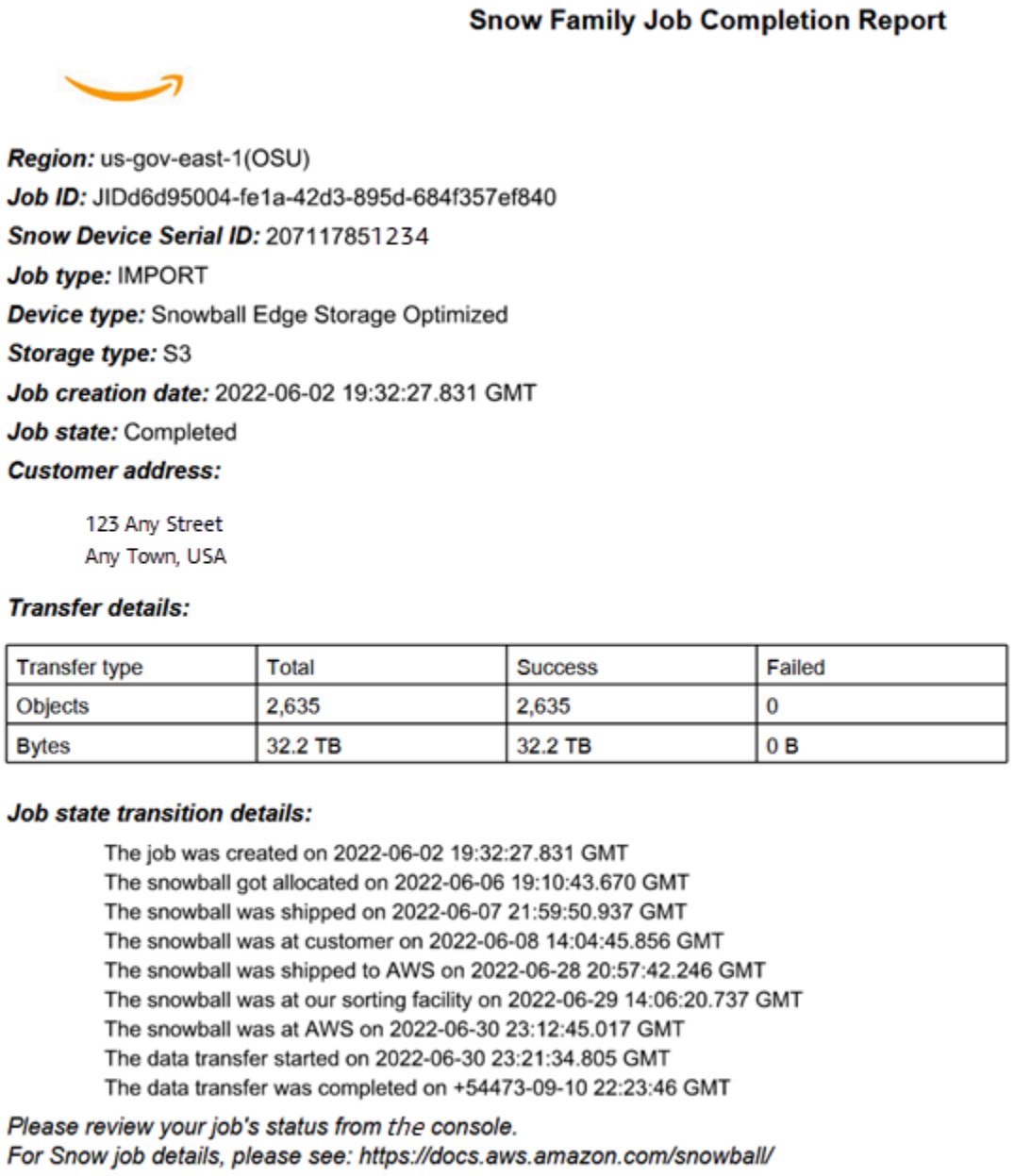
Abrufen Ihres Auftragsabschlussberichts und der Protokolle auf der Konsole

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. Für Exportaufträge wird Ihr Auftragsbericht normalerweise für Sie verfügbar, während das AWS Snowball Edge Gerät für Ihren Auftragsteil an Sie geliefert wird. Für den Auftragstyp Local Use sind keine Auftragsabschlussberichte verfügbar.

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

Einen tieferen Einblick in den Status Ihrer übertragen 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 der an AWS Management Console und öffnen Sie die Managementkonsole für die AWS Snow-Familie.
2. Wählen Sie Ihren Auftrag oder Auftragsteil 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.

Weiter: Verwenden eines AWS Snowball Edge-Geräts

Migration großer Daten mit AWS Snow Family devices

Die Migration großer Daten von On-Premises-Standorten erfordert eine sorgfältige Planung, Orchestrierung und Ausführung, um sicherzustellen, dass Ihre Daten erfolgreich zu migriert werden AWS.

Wir empfehlen Ihnen, vor Beginn Ihrer Migration eine Datenmigrationsstrategie einzurichten, um das Potenzial für verpasste Fristen, die Überschreitung von Budgets und Migrationsfehlern zu vermeiden. Die AWS -Snow-Services helfen Ihnen, Ihre großen Datenmigrationsprojekte über die Funktion Snow Family Large Data Migration Manager (LDMM) in der zu platzieren, zu bestellen und zu verfolgen Managementkonsole für die AWS Snow-Familie.

Die Themen Planen Ihrer großen Übertragung und Einen großen Transfer reduzieren beschreiben einen manuellen Datenmigrationsprozess. Sie können die manuellen Schritte mithilfe des LDMM-Migrationsplans der Snow Family optimieren.

Themen

Planen Ihrer großen Übertragung

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

Themen

Schritt 1: Verstehen, was Sie in die Cloud verschieben

Bevor Sie Ihren ersten Auftrag mit der erstellen Managementkonsole für die AWS Snow-Familie, stellen Sie sicher, dass Sie das Datenvolumen bewerten, das Sie übertragen müssen, wo es derzeit gespeichert ist und an das Ziel, an das Sie es übertragen möchten. Bei Datenübertragungen, die ein Petabyte groß oder größer sind, erleichtert diese administrative Verwaltung das Eintreffen Ihrer Snow-Family-Geräte viel.

Wenn Sie Daten AWS Cloud zum ersten Mal in migrieren, empfehlen wir Ihnen, ein Cloud-Migrationsmodell zu entwerfen. Die Cloud-Migration findet nicht über Nacht statt. 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 Ihrer Zielübertragungsrate

Es ist wichtig zu schätzen, wie schnell Sie Daten an die Snow Family-Geräte übertragen können, die mit jedem Ihrer Server verbunden sind. Diese geschätzte Geschwindigkeit in MB/Sek. bestimmt, wie schnell Sie die Daten mithilfe Ihrer lokalen Netzwerkinfrastruktur von Ihrer Datenquelle an Snowball-Edge-Geräte übertragen können.

> **Note**
>
> Für große Datenübertragungen empfehlen wir die Verwendung der Amazon 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 eine kleine Teilmenge Ihrer Daten auf das Snowball Edge-Gerät oder übertragen Sie eine 10-GB-Beispieldatei und beobachten Sie den Durchsatz.

Beachten Sie bei der Festlegung Ihrer Zielübertragungsgeschwindigkeit, dass Sie den Durchsatz verbessern können, indem Sie Ihre Umgebung, einschließlich der Netzwerkkonfiguration, optimieren, indem Sie die Netzwerkgeschwindigkeit, die Größe der übertragenen Dateien und die Geschwindigkeit ändern, mit der Daten von Ihren lokalen Servern gelesen werden können. Der Amazon S3-Adapter kopiert Daten so schnell wie möglich auf Snow-Family-Geräte.

Schritt 3: Ermitteln, wie viele Snow Family-Geräte Sie benötigen

Anhand der Gesamtmenge der Daten, die Sie in die Cloud verschieben möchten, der geschätzten Übertragungsgeschwindigkeit und der Anzahl der Tage, die Sie zulassen möchten, um die Daten in zu verschieben AWS, bestimmen Sie, wie viele Snow Family-Geräte Sie für Ihre groß angelegte Datenmigration benötigen. Je nach Gerätetyp verfügen Snowball Edge-Geräte über etwa 39,5 TB, 80 TB oder 210 TB nutzbaren Speicherplatz. Wenn Sie beispielsweise 300 TB an Daten AWS über 10 Tage verschieben möchten und eine Übertragungsgeschwindigkeit von 250 MB/s haben, benötigen Sie 4 Snowball Edge-Geräte. Wenn weniger als 40 TB an Daten übertragen werden müssen, werden AWS Snowcone Geräte (mit 14TB nutzbarem Speicherplatz) empfohlen.

> **Note**
>
> Das AWS Snow Family devices LDMM bietet einen Assistenten zur Schätzung der Anzahl der AWS Snow Family devices , die gleichzeitig unterstützt werden können. Weitere Informationen finden Sie unter Erstellen eines großen Datenmigrationsplans.

Schritt 4: Erstellen Ihrer Aufträge

Nachdem Sie wissen, wie viele Snow Family-Geräte Sie benötigen, müssen Sie für jedes Gerät einen Importauftrag erstellen. Die Erstellung mehrerer Aufträge wird durch das Snow Family LDMM vereinfacht. Weitere Informationen finden Sie unter Ablegen Ihrer nächsten Auftragsbestellung.

> **Note**
>
> Sie können Ihre nächste Auftragsbestellung aufgeben und sie automatisch direkt aus dem empfohlenen Zeitplan für die Auftragsbestellung zu Ihrem Plan hinzufügen. Weitere Informationen finden Sie unter Empfohlener Zeitplan für die Auftragsbestellung.

Schritt 5: Trennen Ihrer Daten in Übertragungssegmente

Als bewährte Methode für große Datenübertragungen mit mehreren Aufträgen empfehlen wir Ihnen, Ihre Daten logisch in eine Reihe kleinerer, verwaltbarer Datensätze aufzuteilen. 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 kombinierten Partitionen auf die Snow Family-

Geräte für den Auftrag passen. Sie können Ihre Übertragung beispielsweise auf eine der folgenden Arten in Partitionen aufteilen:

- Sie können 10 Partitionen mit jeweils 8 TB für einen Snowball Edge erstellen.
- Bei großen Dateien kann jede Datei eine einzelne Partition bis zur Größenbeschränkung von 5 TB für Objekte in Amazon S3 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 Arten von Dateien zu bestimmen.

> **Note**
>
> Metadatenoperationen werden für jede Datei ausgeführt, die übertragen wird. Dieser Aufwand ist derselbe, unabhängig von der Dateigröße. Daher erzielen Sie eine schnellere Leistung, indem Sie kleine Dateien in ein größeres Paket komprimieren, Ihre Dateien zusammenfassen oder größere einzelne Dateien übertragen.

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

Wenn Sie mit der Planung Ihrer Datenübertragung im Petabytebereich fertig sind, empfehlen wir Ihnen, einige Segmente von Ihrem Server auf das Snow Family-Gerät zu übertragen, um Ihre Geschwindigkeit und die Gesamtübertragungszeit zu verkürzen.

Einen großen Transfer reduzieren

Sie können die Übertragungsleistung verringern, indem Sie einen repräsentativen Satz Ihrer Datenpartitionen übertragen. Wählen Sie mehrere Partitionen aus, die Sie definiert haben, und übertragen Sie sie auf ein Snow Family-Gerät. Notieren Sie sich die Übertragungsgeschwindigkeit und die Gesamtübertragungszeit für jeden Vorgang. Wenn die Ergebnisse der Telefonie niedriger als die Zielübertragungsrate sind, können Sie möglicherweise mehrere Teile Ihrer Datenübertragung gleichzeitig kopieren. Wiederholen Sie in diesem Fall die Trichterung mit den zusätzlichen Partitionen Ihres Datensatzes.

Fahren Sie während der Stabilisierung mit dem Hinzufügen paralleler Kopiervorgänge fort, bis Sie in der Summe der Übertragungsgeschwindigkeit aller Instances, die derzeit Daten übertragen, einen Rückgang feststellen. Beenden Sie die letzte aktive Instance und notieren Sie sich Ihre neue Zielübertragungsrate.

Sie können Daten schneller auf Snow-Family-Geräte übertragen, indem Sie Daten mit einem der folgenden Szenarien parallel übertragen:

- Verwenden mehrerer Sitzungen des S3-Adapters auf einer Workstation auf einem einzigen Snow-Family-Gerät.
- Verwenden mehrerer Sitzungen des S3-Adapters auf mehreren Workstations auf einem einzigen Snow-Family-Gerät.
- Verwenden mehrerer Sitzungen der S3-Schnittstelle (mit einer oder mehreren Workstations), die auf mehrere Snow-Family-Geräte ausgerichtet sind.

Wenn Sie diese Schritte ausführen, sollten Sie wissen, wie schnell Sie Daten auf ein Snow Family-Gerät übertragen können.

Erstellen eines großen Datenmigrationsplans

Mit der Funktion AWS Snow Family für große Datenmigrationspläne können Sie große Datenmigrationen von 500 TB zu mehreren Petabyte mithilfe mehrerer Snow-Family-Serviceprodukte planen, verfolgen, überwachen und verwalten.

Verwenden Sie die Funktion für große Datenmigrationspläne, um Informationen über Ziele der Datenmigration zu sammeln, z. B. die Größe der zu verschiebenden Daten AWS und die Anzahl der Snow Family-Geräte, die für die gleichzeitige Migration der Daten erforderlich sind. 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 verfügbar, die größer als 500 TB sind.

Themen

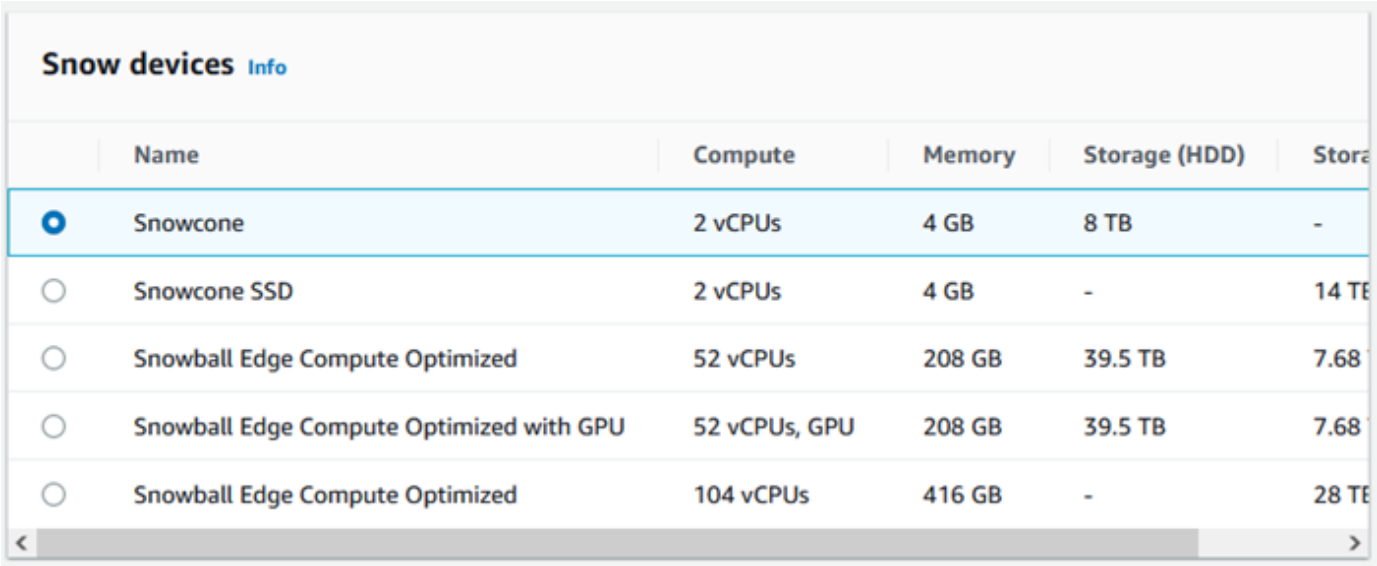
- Schritt 2: Auswählen Ihrer Versand-, Sicherheits- und Benachrichtigungseinstellungen
- Schritt 3: Überprüfen und Erstellen Ihres Plans

Schritt 1: Auswählen Ihrer Migrationsdetails

> **Note**
>
> Für Datenmigrationen mit mehr als 500 TB ist ein großer Datenmigrationsplan verfügbar. Erstellen Sie Aufträge einzeln auf Snow Family-Geräten für Ihre Datenübertragungsprojekte mit weniger als 500 TB. Weitere Informationen finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts in diesem Handbuch.

1. Melden Sie sich an der Managementkonsole für die AWS Snow-Familie an. Wenn Sie die Managementkonsole für die AWS Snow-Familie in dieser zum ersten Mal verwenden AWS-Region, wird die AWS Snow Family Seite angezeigt. Andernfalls wird die Liste der vorhandenen Aufträge angezeigt.
2. Wenn dies Ihr erster Datenmigrationsplan ist, wählen Sie auf der Hauptseite die Option Erstellen Ihres Plans für die Migration großer Daten aus. Wählen Sie andernfalls Großer Datenmigrationsplan aus. Wählen Sie Datenmigrationsplan erstellen, um den Assistenten zur Planerstellung zu öffnen.
3. Geben Sie unter Benennen Ihres Datenmigrationsplans einen Namen für den Datenmigrationsplan an. Der Planname kann bis zu 64 Zeichen lang sein. Gültige Zeichen sind A-Z, a-z, 0-9 und . - (Bindestrich). Ein Planname darf nicht mit beginnen**`aws:`**.
4. Geben Sie für Gesamtdaten, die zu migriert werden sollen AWS, die Datenmenge ein, die Sie zu migrieren möchten AWS.
5. Wählen Sie unter Snow-Geräte ein Snow-Family-Gerät aus.

   > **Note**
   >
   > Unterstützte Geräteoptionen können je nach Geräteverfügbarkeit in bestimmten variieren AWS-Regionen.



6. Geben Sie für Gleichzeitige Geräte die Anzahl der Snow Family-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 zur Verwendung des Assistenten für gleichzeitige Geräteschätzer zu erhalten.
7. Wählen Sie Weiter aus.

Verwenden des Assistenten zur Schätzung gleichzeitiger Geräte

Der Assistent für gleichzeitige Geräteschätzer hilft Ihnen, die Anzahl der gleichzeitigen Geräte zu bestimmen, die Sie bei Migrationen großer Daten verwenden können.

Voraussetzungen:

- Sie haben einen Machbarkeitsnachweis durchgeführt, um Ihre Datenübertragungsmethode und die gemessene Leistung mit einem Snow Family-Gerät in Ihrer Umgebung zu testen.
- Sie kennen das Netzwerk und die Verbindung zum Backend-Speicher.

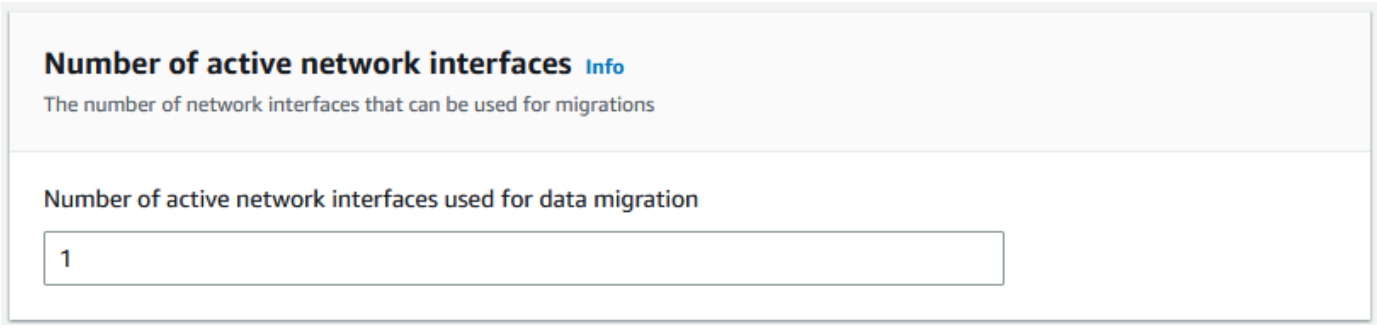
Schritt 1: Geben Sie Datenquelleninformationen ein

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

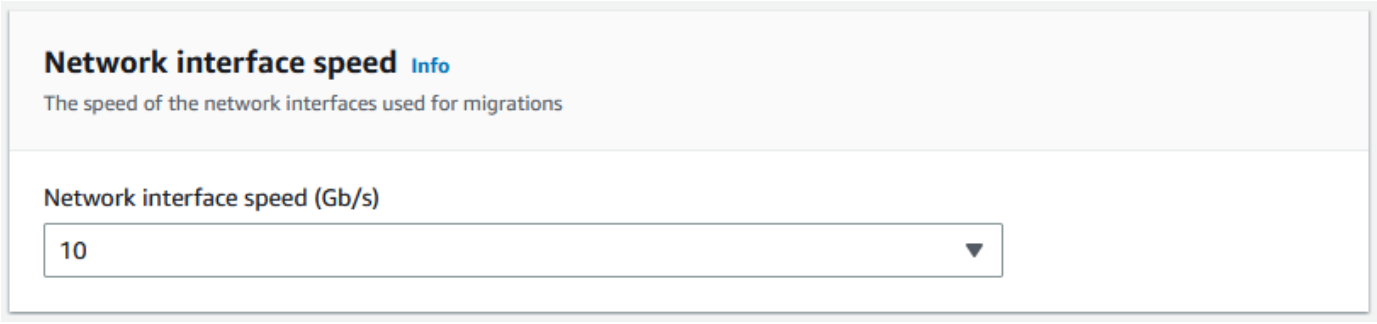
1. Geben Sie unter Zu migrierende Gesamtdaten die Datenmenge ein, die Sie migrieren möchten.

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

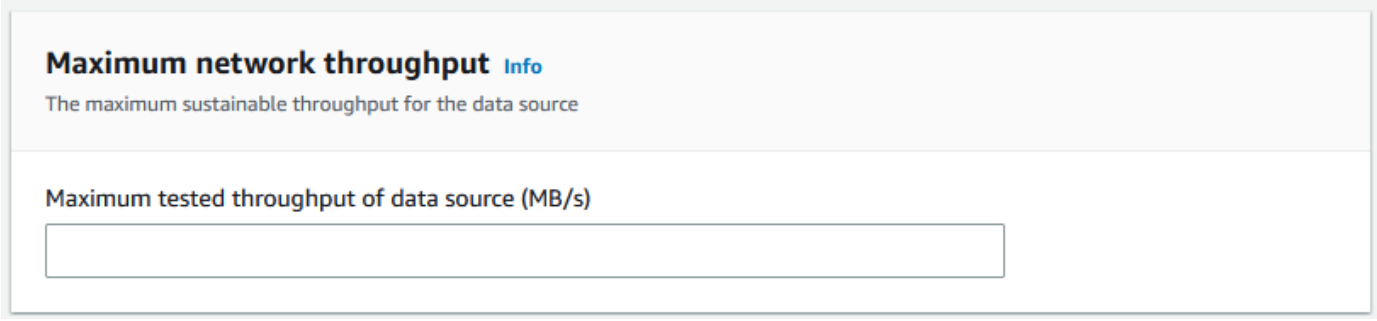
2. Geben Sie unter Anzahl der aktiven Netzwerkschnittstellen die Anzahl der aktiven Netzwerkschnittstellen ein, die Sie für die Datenmigration aus der Speicherquelle zur Verfügung haben.



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



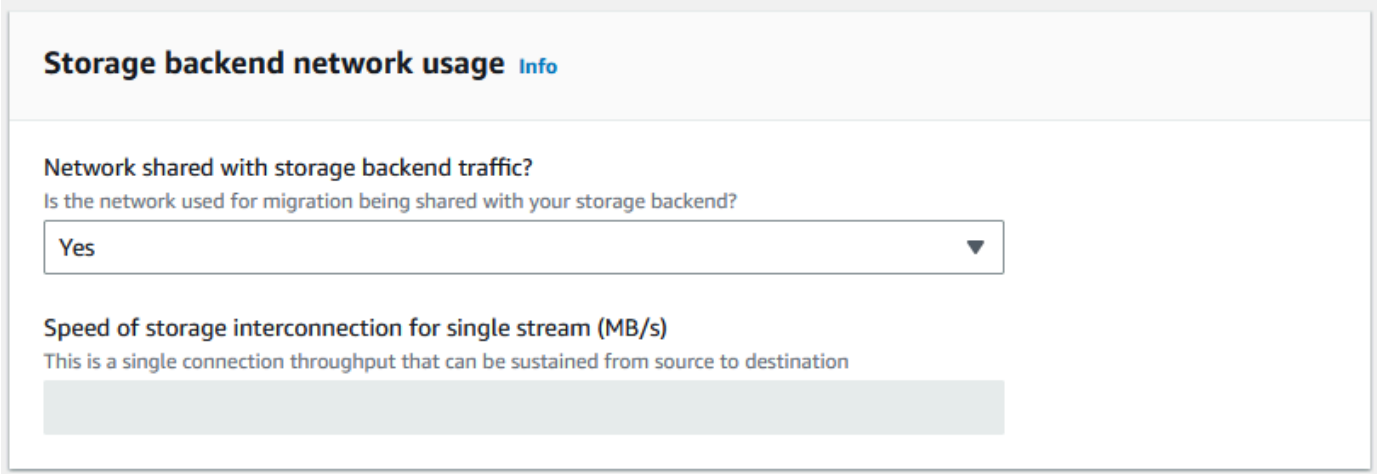
4. Geben Sie für Maximaler Netzwerkdurchsatz den maximal getesteten Netzwerkdurchsatz zu Ihrer Speicherquelle ein, den Sie während des Machbarkeitsnachweises ermittelt haben. Der Durchsatz wird in MB/S angegeben.



5. Geben Sie für Speicher-Backend-Netzwerknutzung an, ob die Speicherquelle ein Netzwerk mit dem Backend-Speicher teilt.

- Wählen Sie Ja, wenn das Netzwerk nicht freigegeben ist. Sie müssen nicht die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream eingeben.
- Wählen Sie Nein, wenn das Netzwerk freigegeben ist. Geben Sie die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream in MB/s ein.

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



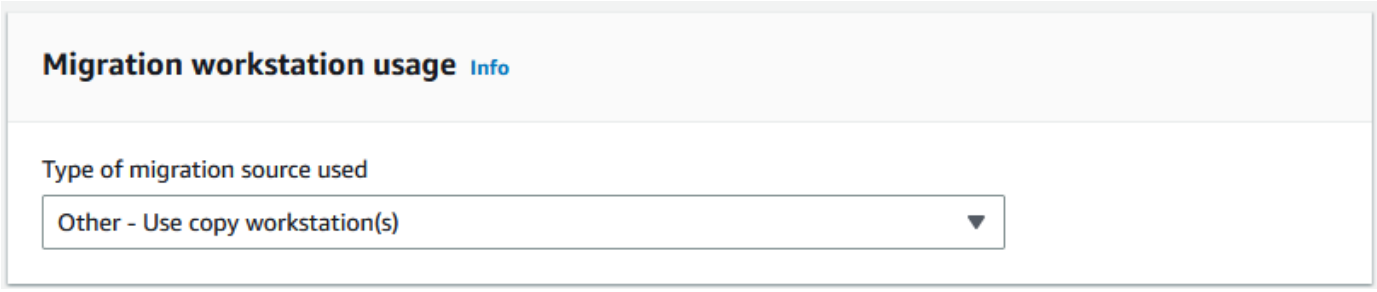
6. Wählen Sie Weiter aus.

Schritt 2: Eingabe-Migrations-Workstation-Parameter

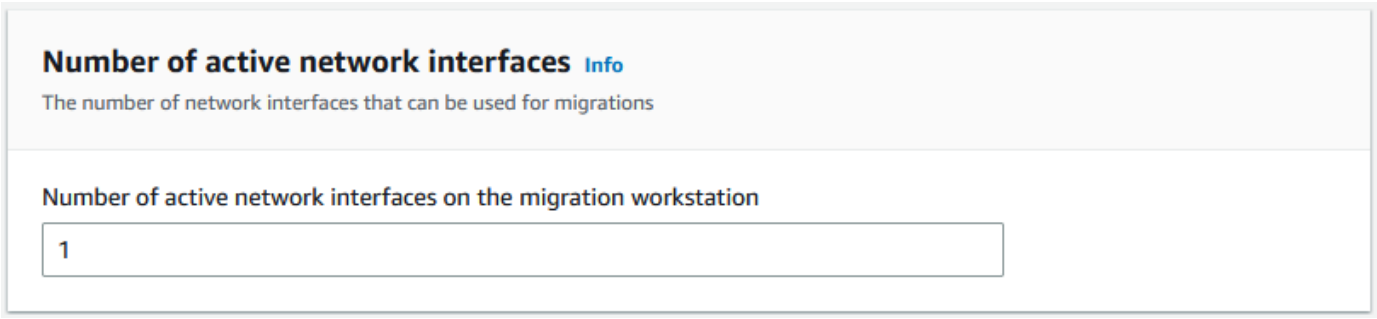
Sie können yourSnow Family direkt mit Ihrer Speicherquelle verbinden (z. B. ein Microsoft-Windows-Server). Sie können stattdessen yourSnow Family-Geräte mit einer oder mehreren Workstations verbinden, um Daten aus der Speicherquelle zu kopieren.

1. Geben Sie für Migration Workstation-Nutzung Ihre Workstation-Nutzungsauswahl an.

   - Wählen Sie Keine – Verwenden Sie die Datenquelle direkt, um Daten direkt aus einer Datenquelle zu übertragen, ohne eine Workstation zu verwenden, und wählen Sie dann Weiter aus.
   - Wählen Sie Andere – Kopieren Sie Workstation(s), um eine oder mehrere Workstations für die Übertragung von Daten zu verwenden.



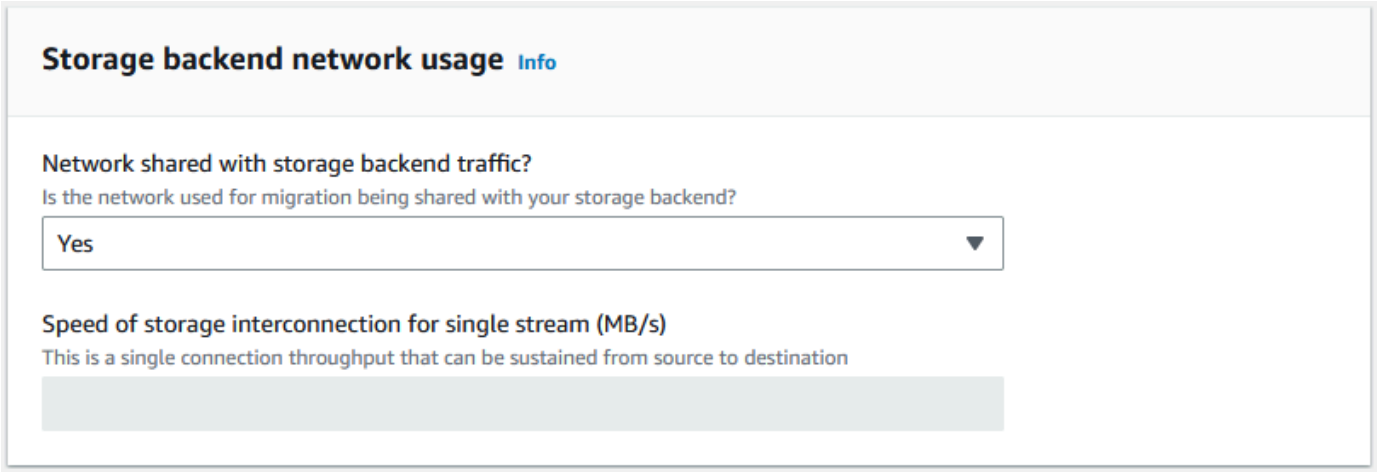
2. Geben Sie unter Anzahl der aktiven Netzwerkschnittstellen die Anzahl der Ports ein, die für die Datenmigration verwendet werden sollen.



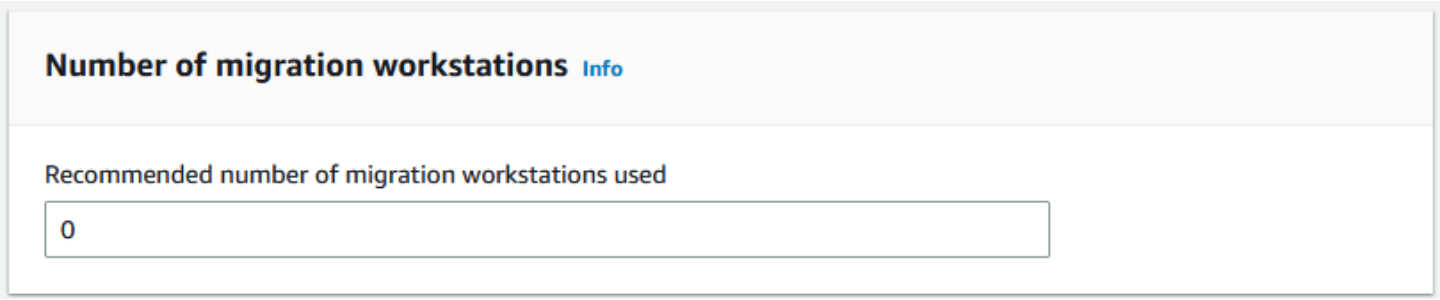
3. Wählen Sie für Netzwerkschnittstellengeschwindigkeit die Geschwindigkeit der Netzwerkschnittstellen in GB/s aus.

4. Geben Sie unter Speicher-Backend-Netzwerknutzung an, ob das Netzwerk, in dem sich die Workstations befinden, für Backend-Speicher freigegeben ist.

   - Wählen Sie Ja, wenn es freigegeben ist.
   - Wählen Sie Nein, wenn es nicht freigegeben ist. Geben Sie die Geschwindigkeit der Speicherverbindung für einen einzelnen Stream in MB/s ein.

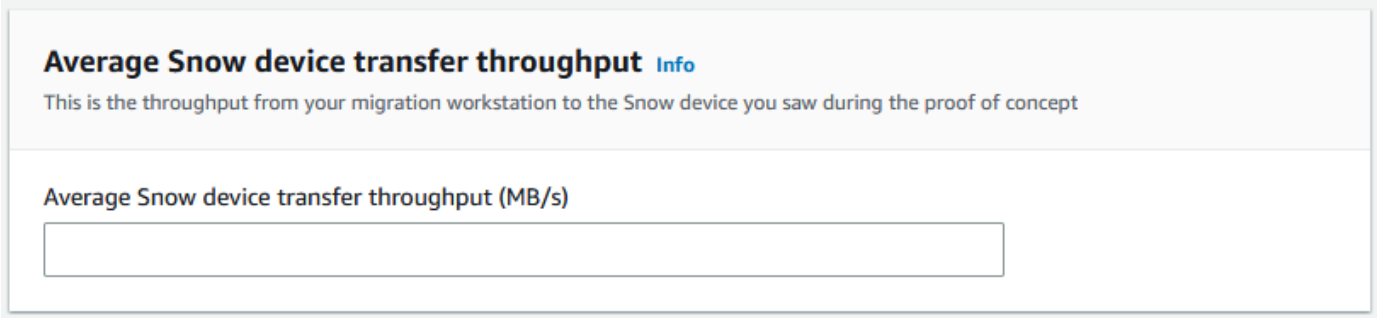


Basierend auf Ihren Eingaben zeigt der Assistent eine Empfehlung unter Anzahl der Migrationsarbeitsplätze an. Sie können die Zahl manuell ändern, wenn Sie die Empfehlung nicht einhalten. Diese Nummer wird im Plan zur Migration großer Daten in Gleichzeitige Geräte angezeigt.



Schritt 3: Eingabe des durchschnittlichen Übertragungsdurchsatzes von Snow-Family-Geräten

1. Geben Sie im Feld Durchschnittlicher Übertragungsdurchsatz für Snow-Geräte den Übertragungsdurchsatz in MB/s ein, den Sie während Ihres Machbarkeitsnachweises gesehen haben.



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

2. Wählen Sie Diese Nummer verwenden, um fortzufahren und zur Auswahl Ihrer Migrationsdetails zurückzukehren. Wählen Sie Weiter und fahren Sie mit dem nächsten Schritt () fortSchritt 2: Auswählen Ihrer Versand-, Sicherheits- und Benachrichtigungseinstellungen.

> **Note**
>
> Sie können bis zu 5 gleichzeitige Snow-Geräte verwenden.

Schritt 2: Auswählen Ihrer Versand-, Sicherheits- und Benachrichtigungseinstellungen

1. Wählen Sie im Abschnitt Versandadresse eine vorhandene Adresse aus oder erstellen Sie eine neue.

   - > **Note**
     >
     > Das Land in der Adresse muss mit dem Zielland für das Gerät übereinstimmen und für dieses Land gültig sein.

2. Führen Sie unter Servicezugriffstyp auswählen einen der folgenden Schritte aus:

   - Erlauben Sie Snow Family, eine neue serviceverknüpfte Rolle für Sie mit allen erforderlichen Berechtigungen zu erstellen, um CloudWatch Metriken und Amazon SNS-Benachrichtigungen für Ihre Snow-Family-Aufträge zu veröffentlichen.
   - Fügen Sie eine vorhandene 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 Benachrichtigungen über Datenmigrationspläne senden wählen, keine Benachrichtigungen von diesem Plan erhalten, aber trotzdem Auftragsbenachrichtigungen.

4. Für Festlegen von Benachrichtigungen,
   - Wählen Sie Vorhandenes SNS-Thema verwenden
   - oder Erstellen eines neuen SNS-Themas.

Schritt 3: Überprüfen und Erstellen Ihres Plans

1. Überprüfen Sie Ihre Informationen unter Plandetails und Versand-, Sicherheits- und Benachrichtigungseinstellungen und bearbeiten Sie sie bei Bedarf.
2. Wählen Sie Datenmigrationsplan erstellen, um den Plan zu erstellen.

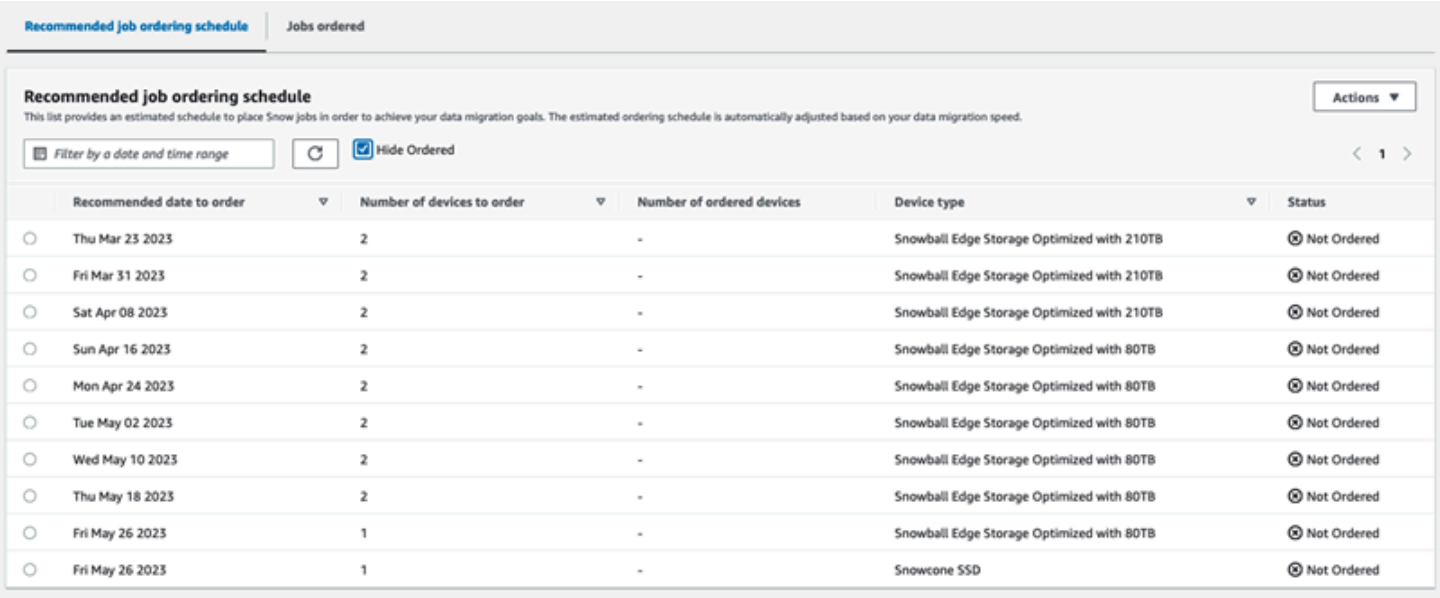
Verwenden des großen Datenmigrationsplans

Nachdem Sie Ihren großen Datenmigrationsplan erstellt haben, können Sie den resultierenden Zeitplan und das Dashboard verwenden, um Sie durch den Rest des Migrationsprozesses zu führen.

Empfohlener Zeitplan für die Auftragsbestellung

Nachdem Sie einen AWS Snow Family devices großen Migrationsplan erstellt haben, können Sie den empfohlenen Zeitplan für die Auftragsbestellung verwenden, um neue Aufträge zu erstellen.

> **Note**
>
> Manuelle Aktualisierungen, die Sie an der Datengröße oder Anzahl gleichzeitiger Geräte vornehmen, führen dazu, dass sich der Zeitplan anpasst. 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, wird der Zeitplan automatisch angepasst.



Ablegen Ihrer nächsten Auftragsbestellung

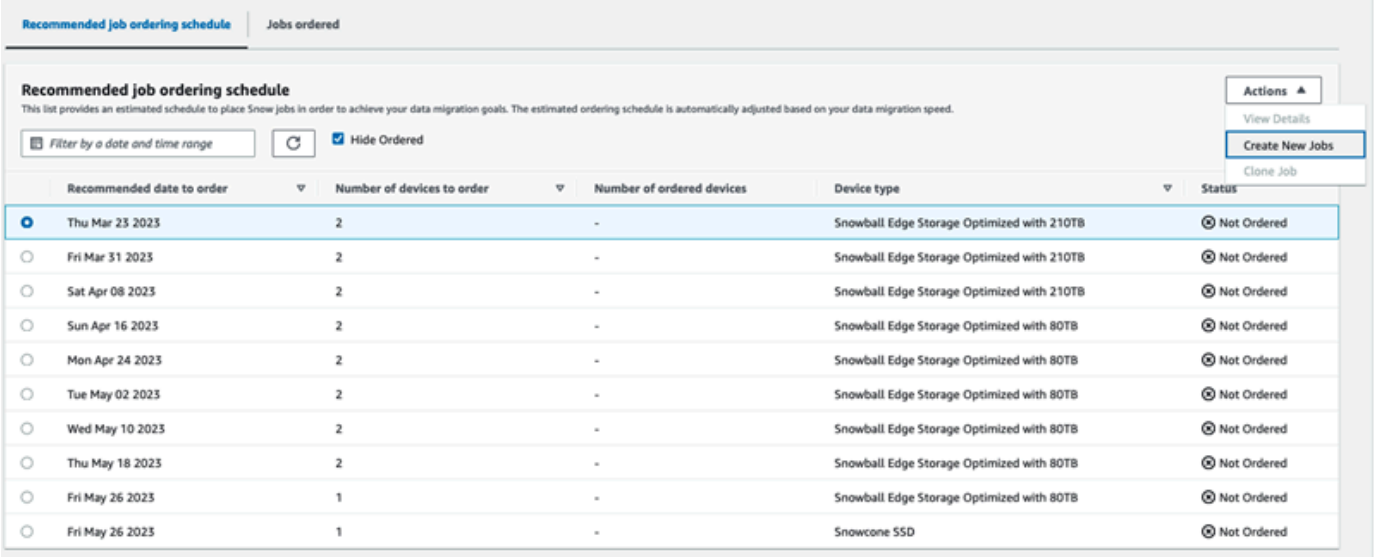
Um Ihnen die nächste Bestellung zu geben, haben Sie die Möglichkeit, entweder einen zuvor bestellten Auftrag zu klonen oder einen vorausgefüllten Auftrag zu erstellen, anstatt einen Auftrag manuell zu erstellen und ihn dann Ihrem Plan hinzuzufügen.

So klonen Sie einen Auftrag:

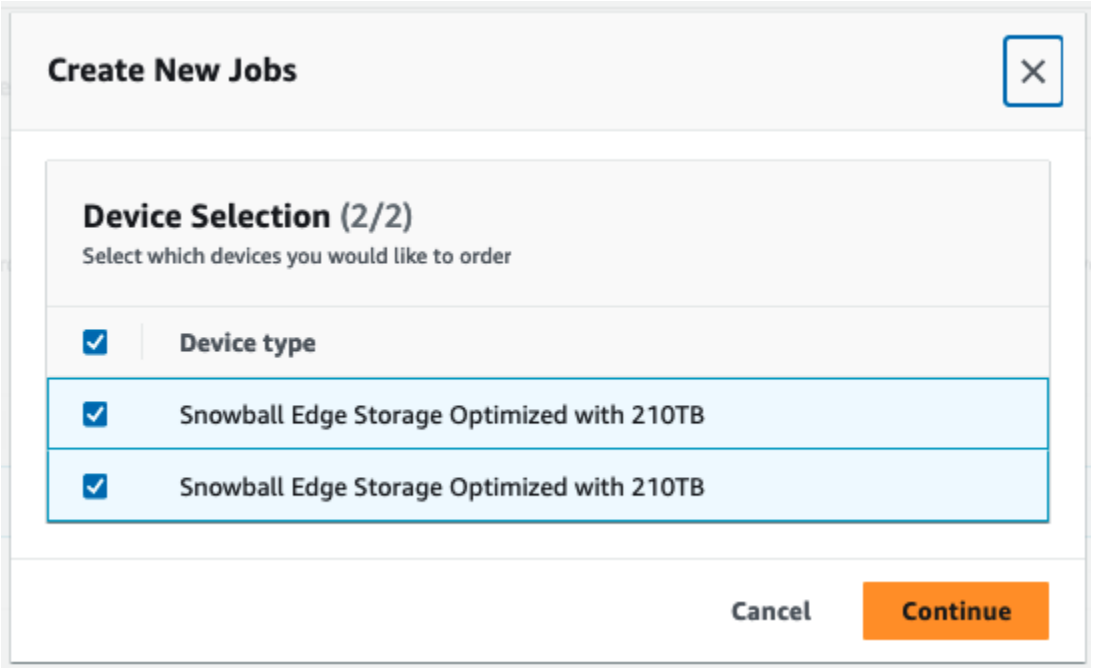
1. Wählen Sie die nächste Reihenfolge (die erste Empfehlung mit dem Status Nicht bestellt) aus dem Zeitplan Empfohlene Auftragsbestellung und wählen Sie dann im Menü Aktionen die Option Auftrag klonen aus. Das Fenster Auftrag klonen wird angezeigt.
2. Wählen Sie im Fenster Auftrag klonen im Abschnitt Aufträge sortiert den zu klonenden Auftrag aus.
3. Wählen Sie im Abschnitt Details zu neuen Aufträgen die Geräte aus, die Sie bestellen möchten. Für jedes ausgewählte Gerät wird der Auftragsname automatisch basierend auf dem ausgewählten Auftrag ausgefüllt. Sie können den Auftragsnamen überschreiben.
4. Wählen Sie Bestätigen, um die Auftragsbestellung für die ausgewählten Geräte zu platzieren. Das System klont den Auftrag für jedes Gerät.

So erstellen Sie neue Aufträge:

1. Wählen Sie die nächste Reihenfolge (die erste Empfehlung mit dem Status Nicht sortiert) aus dem Zeitplan Empfohlene Auftragsbestellung und dann Neue Aufträge erstellen aus dem Menü Aktionen aus. Das Fenster Neue Aufträge erstellen wird angezeigt.



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



3. Die Seite Neu erstellen wird angezeigt. Die meisten Parameter, z. B. Auftragstyp, Lieferadresse und Gerätetyp, werden auf der Grundlage des Plans festgelegt. Das System erstellt den Auftrag für jedes Gerät.

Sie können sehen, ob der Auftrag oder die Aufträge erfolgreich erstellt wurden oder nicht. Erfolgreich erstellte Aufträge werden dem Plan automatisch hinzugefügt.

Liste der geordneten Aufträge

Jeder Plan zeigt eine Liste der Auftragsreihenfolgen an. Dies ist zunächst leer. Wenn Sie mit der Bestellung von Aufträgen beginnen, können Sie Ihrem Plan Aufträge hinzufügen, indem Sie im Menü Aktionen die Option Auftrag hinzufügen auswählen. Aufträge, die Sie hier hinzufügen, werden auf dem Überwachungs-Dashboard verfolgt.

In ähnlicher Weise können Sie den Auftrag aus der Liste Auftragsreihenfolge entfernen, indem Sie im Menü Aktionen die Option Auftrag entfernen auswählen.

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

Überwachen des Dashboards

Nachdem Sie Ihrem Plan Aufträge hinzugefügt haben, können Sie Metriken auf dem Dashboard sehen, wenn die Aufträge AWS zur Aufnahme an zurückkehren. Diese Metriken können Ihnen helfen, Ihren Fortschritt zu verfolgen:

- Daten, die zu migriert wurden AWS – Die Menge der Daten, die AWS bisher zu migriert wurden.
- Durchschnitt pro Auftrag migrierte Daten – Die durchschnittliche Datenmenge pro Auftrag in Terabyte.
- Gesamtzahl der Snow-Aufträge – Die Anzahl der sortierten Snowball-Edge-Aufträge im Vergleich zu den verbleibenden Aufträgen, die bestellt werden sollen.
- Durchschnittliche Dauer für einen Migrationsauftrag – Die durchschnittliche Dauer eines Auftrags in Tagen.
- Snow-Auftragsstatus – Die Anzahl der Aufträge in jedem Status.

Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten

Die Snow Family-Geräte bieten jetzt ein benutzerfreundliches Tool AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen AWS Services verwalten können. Sie verwenden 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 Instances auszuführen, die auf Snow Family-Geräten ausgeführt werden. Sie können verwenden AWS OpsHub , um sowohl die Gerätetypen Storage Optimized als auch Compute Optimized Snow zu verwalten. Die AWS OpsHub Anwendung ist ohne zusätzliche Kosten für Sie verfügbar.

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

AWS OpsHub bietet eine einheitliche Ansicht der AWS Services, die auf Snow Family-Geräten ausgeführt werden, und automatisiert Betriebsaufgaben über AWS Systems Manager. Mit können AWS OpsHub Benutzer mit unterschiedlichem technischem Fachwissen eine große Anzahl von Snow Family-Geräten verwalten. Mit wenigen Klicks können Sie Geräte entsperren, Dateien übertragen, Amazon-ECEC2-compatible 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 es lokal verwalten und unterstützte - AWS Services verwenden. AWS OpsHub bietet ein Dashboard, das wichtige Metriken wie Speicherkapazität und aktive Instances auf Ihrem Gerät zusammenfasst. Es bietet auch eine Auswahl von AWS Services, die auf den Snow Family-Geräten unterstützt werden. Innerhalb weniger Minuten können Sie mit der Übertragung von Dateien zum Gerät beginnen.

Themen

- Automatisierung von Verwaltungsaufgaben
- Festlegen der NTP-Zeitserver für Ihr Gerät

AWS OpsHub Für Snow Family-Geräte herunterladen

So laden Sie herunter AWS OpsHub

1. Navigieren Sie zur AWS Website für Snowball-Ressourcen .

2. Wählen Sie im AWS OpsHub Abschnitt Herunterladen für Ihr Betriebssystem und folgen Sie den Installationsschritten.

Entsperren eines Geräts

Wenn Ihr Gerät an Ihrem Standort eintrifft, besteht der erste Schritt darin, es zu verbinden und zu entsperren. AWS OpsHub Mit können Sie sich mit den folgenden Methoden anmelden, entsperren und verwalten:

- Lokal – Um sich lokal bei einem Gerät anzumelden, müssen Sie das Gerät einschalten und es mit Ihrem lokalen Netzwerk verbinden. Geben Sie dann einen Entsperrcode und eine Manifestdatei an.
- Remote – 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 zu herstellen kann. Geben Sie dann die AWS Identity and Access Management (IAM)-Anmeldeinformationen (Zugriffsschlüssel und geheimer Schlüssel) für das an AWS-Konto , das mit Ihrem Gerät verknüpft ist.

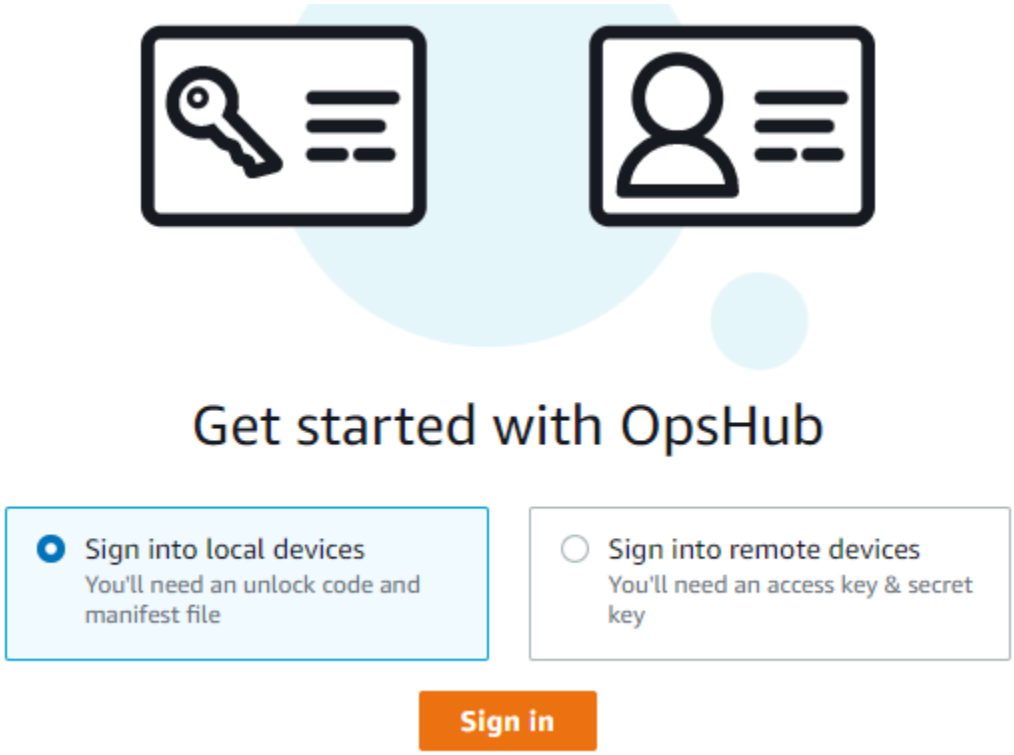
Informationen zum Aktivieren der Remote-Verwaltung und zum Erstellen eines zugehörigen Kontos finden Sie unter Aktivieren der Snow Device Management.

Themen

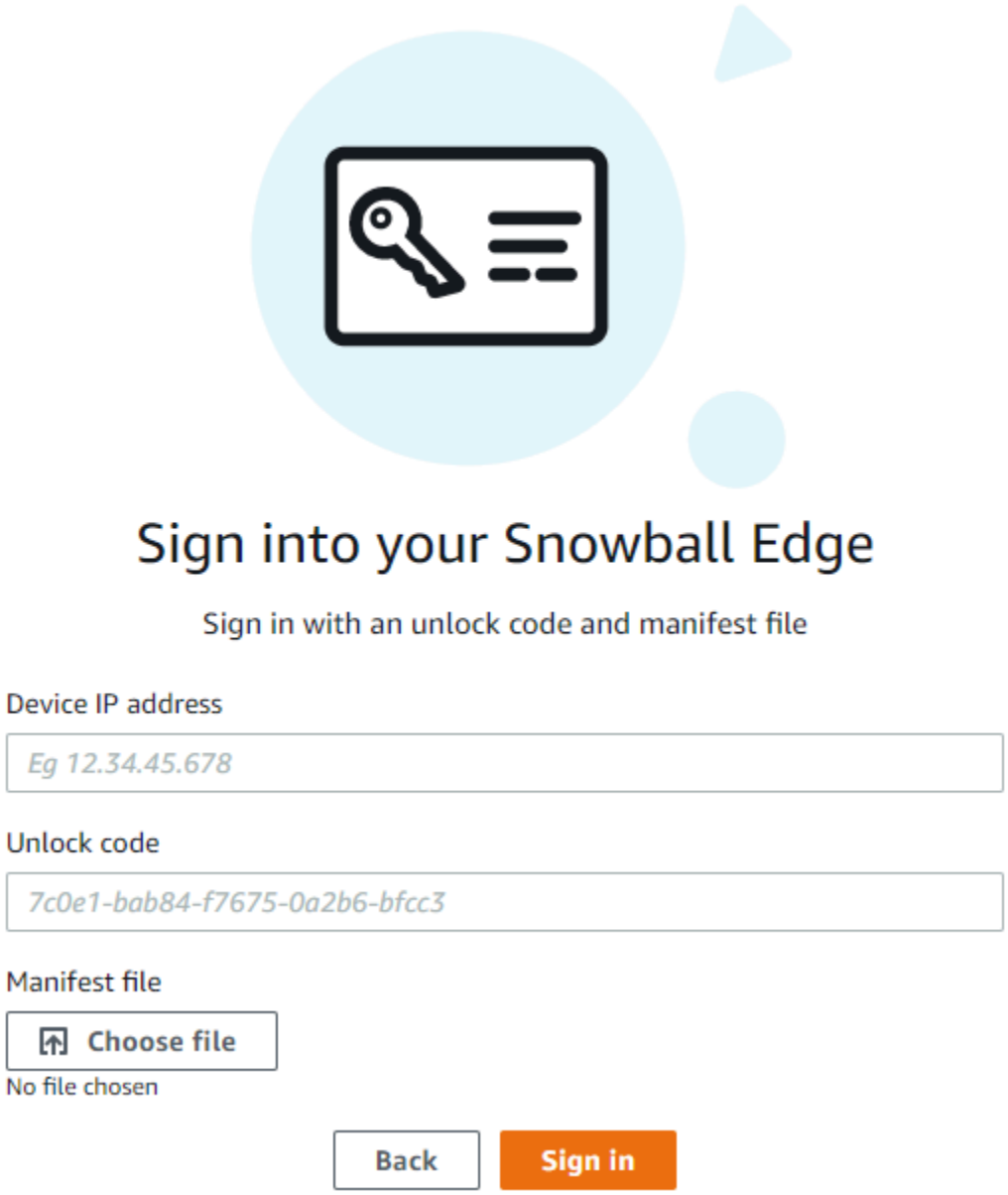
Lokales Entsperren eines Geräts

So stellen Sie eine lokale Verbindung her und entsperren Ihr Gerät

1. Öffnen Sie die Maus auf Ihrem Gerät, suchen Sie das Stromkabel und verbinden Sie es mit einer Stromquelle.
2. Verbinden Sie das Gerät mit Ihrem Netzwerk über ein Netzwerkkabel (in der Regel ein Ethernet RJ45-Kabel), öffnen Sie dann die Frontleiste und schalten Sie das Gerät ein.
3. Öffnen Sie die AWS OpsHub Anwendung. Wenn Sie zum ersten Mal verwenden, werden Sie aufgefordert, eine Sprache auszuwählen. Wählen Sie anschließend Weiter.
4. Wählen Sie auf der Seite Erste Schritte mit OpsHub die Option Bei lokalen Geräten anmelden und dann Anmelden aus.



5. Wählen Sie auf der Seite Bei lokalen Geräten anmelden Ihren Snow-Family-Gerätetyp 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.



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 Verwalten von Profilen.
8. Wählen Sie auf der Registerkarte Lokale Geräte ein Gerät aus, um dessen Details anzuzeigen, z. B. die Netzwerkschnittstellen und AWS Services, die auf dem Gerät ausgeführt werden. Sie können auch Details für Cluster auf dieser Registerkarte anzeigen oder Ihre Geräte genauso verwalten wie mit (AWS Command Line Interface AWS CLI). Weitere Informationen finden Sie unter Verwalten von AWS Services auf Ihrem Gerät.

Für Geräte, auf denen AWS Snow Device Management installiert ist, können Sie Remote-Verwaltung aktivieren auswählen, um die Funktion zu aktivieren. Weitere Informationen finden Sie unter Verwendung von AWS Snow Device Management für die Verwaltung von Geräten.

Entsperren eines Geräts aus der Ferne

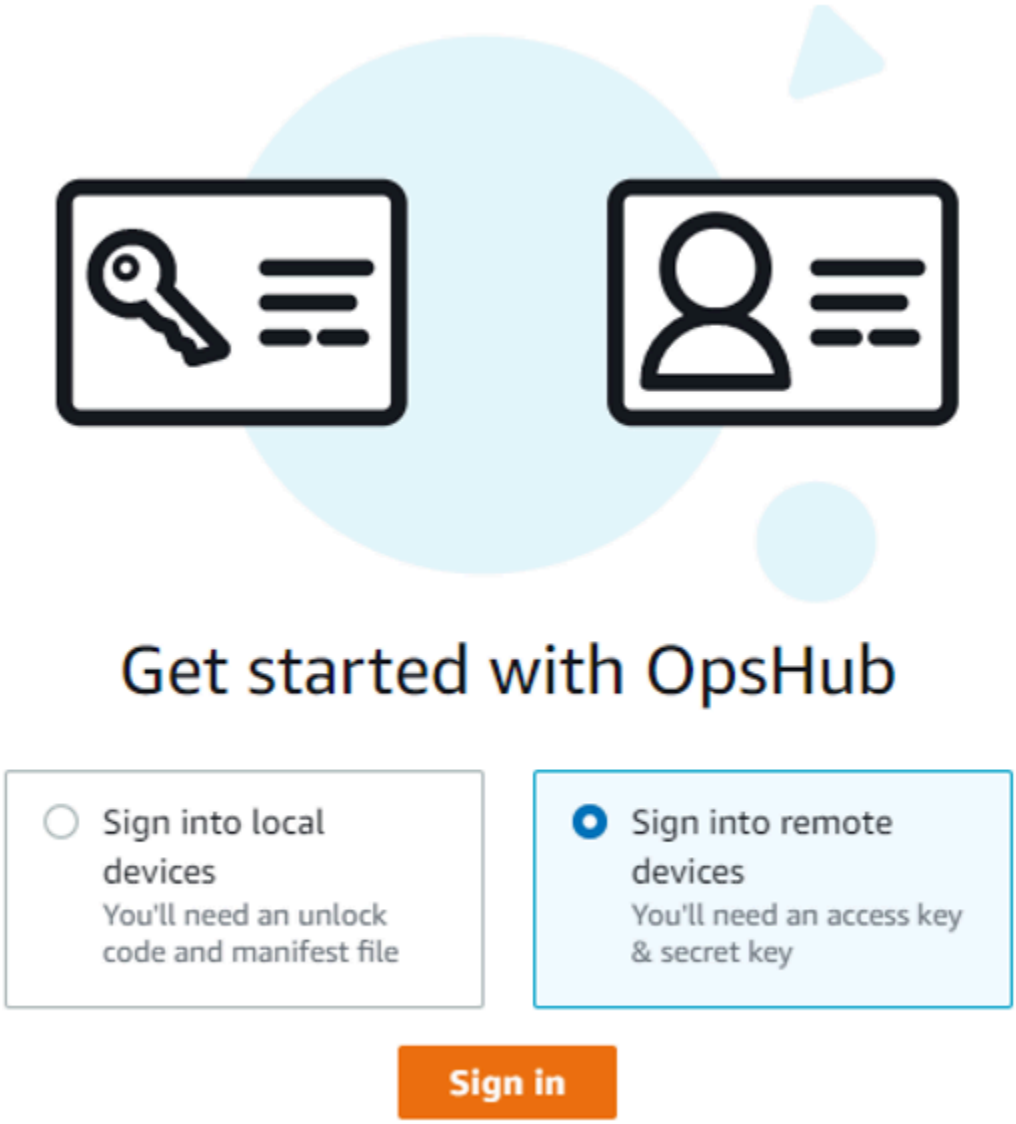
So entsperren Sie ein Snow Family-Gerät nicht

So verbinden und entsperren Sie Ihr Gerät remote

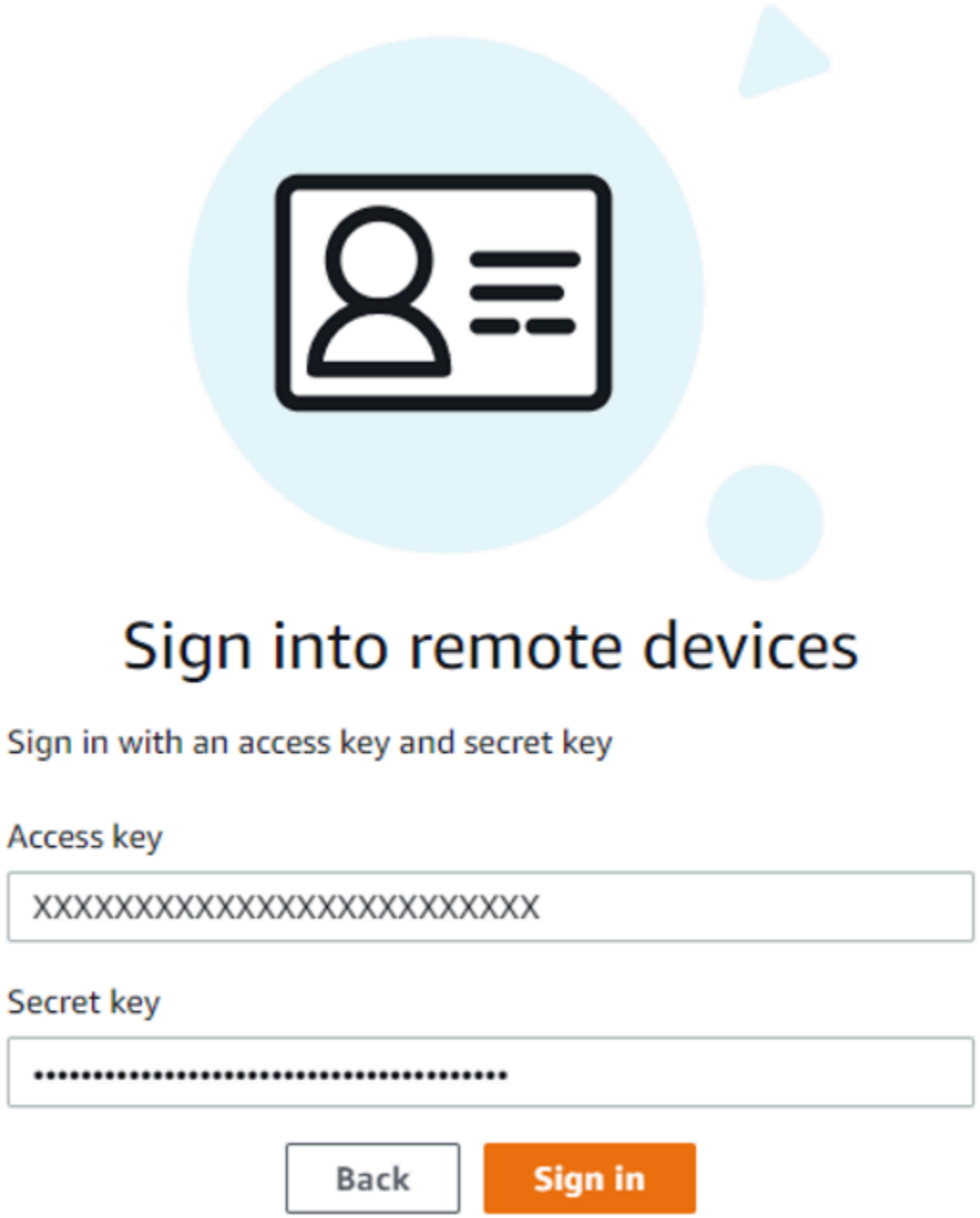
1. Öffnen Sie die Maus auf Ihrem Gerät, suchen Sie das Stromkabel und verbinden Sie es mit einer Stromquelle.
2. Verbinden Sie das Gerät über ein Ethernet-Kabel (in der Regel ein RJ45-Kabel) mit Ihrem Netzwerk, öffnen Sie dann die Frontleiste und schalten Sie das Gerät ein.

   > **Note**
   >
   > Um remote entsperrt zu werden, muss Ihr Gerät eine Verbindung zu herstellen können*device-order-region*`.amazonaws.com`.

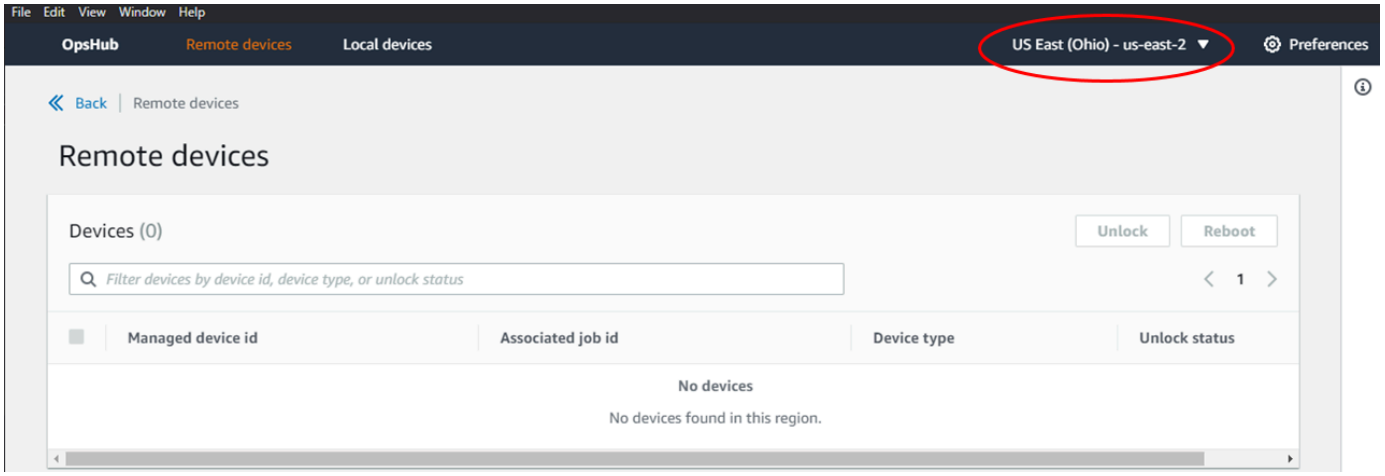
3. Öffnen Sie die AWS OpsHub Anwendung. Wenn Sie zum ersten Mal verwenden, werden Sie aufgefordert, eine Sprache auszuwählen. Wählen Sie anschließend Weiter.
4. Wählen Sie auf der Seite Erste Schritte mit OpsHub die Option Bei Remote-Geräten anmelden und dann Anmelden aus.



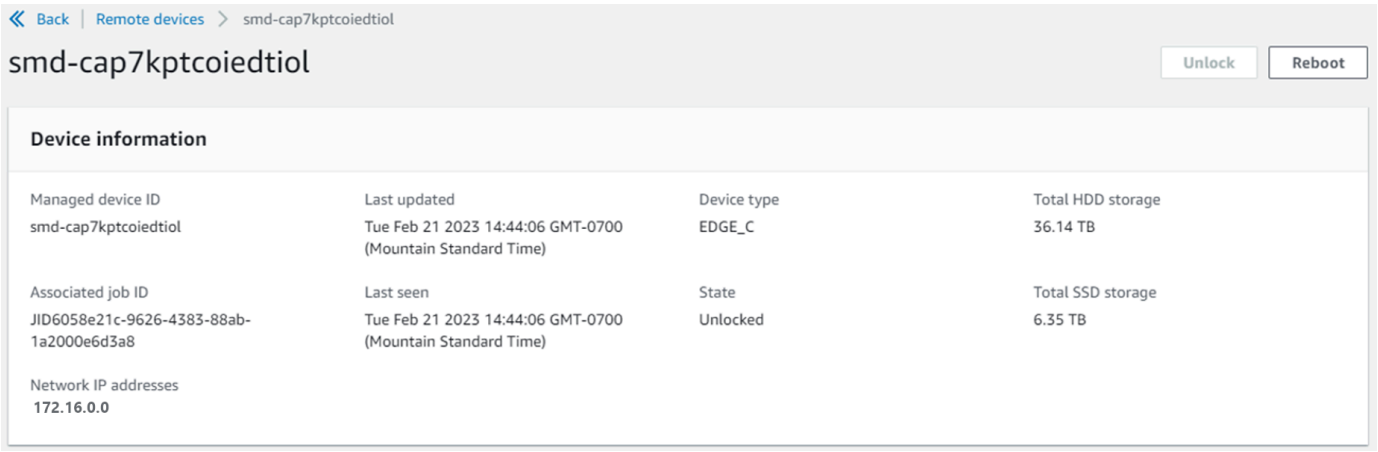
5. Geben Sie auf der Seite Bei Remote-Geräten anmelden die AWS Identity and Access Management (IAM)-Anmeldeinformationen (Zugriffsschlüssel und geheimer Schlüssel) für das ein AWS-Konto , das mit Ihrem Gerät verknüpft ist, und wählen Sie dann Anmelden aus.



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



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



Auf der Detailseite des Remote-Geräts können Sie Ihre Geräte auch neu starten und genauso verwalten wie mit AWS Command Line Interface (AWS CLI). Um Remote-Geräte in verschiedenen anzuzeigen AWS-Regionen, wählen Sie die aktuelle Region auf der Navigationsleiste und dann die Region aus, die Sie anzeigen möchten. Weitere Informationen finden Sie unter Verwalten von AWS Services auf Ihrem Gerät.

Überprüfen der PGP-Signatur von AWS OpsHub (optional)

Das AWS OpsHub Anwendungsinstallationsprogrammpaket 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 geändert werden, schlägt die Verifizierung 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-Betriebssysteminstallationsprogramm unter AWS Snowcone Ressourcen oder Snowball Edge-Ressourcen herunterladen.

So überprüfen Sie das AWS OpsHub Installationspaket auf für das Linux-Betriebssystem

1. Kopieren Sie den folgenden öffentlichen Schlüssel, speichern Sie ihn in einer Datei und benennen Sie die Datei. Beispiel: `opshub-public-key.pgp`

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBF/hGf8BEAC9HCDV8uljDX02Jxspi6kmPu4xqf4ZZLQsSqJcHU61oL/c
/zAN+mUqJT9aJ1rr0QFGVD1bMogecUPflTWlDkEEpG8ZbX5P8vR+EElO/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmIO7j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZXcI/+u+99YLaugJIP6ZYIeDfpxnghqyVtaappBFTAyfG67Y
N/5mea1VqJzd8liFpIFQnl+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvfTb47bbv9Z28Vl284
4lw2w1Bl007FoO2v/Y0ukrN3VHCpmJQS1IiqZbYRa0DVK6UR5QNvUlj5fwWs
4qW9UDPhT/HDuaMrMFCejEn/7wvRUrGVtzCT9F56Al/dwRSxBejQQEb1AC8j
uuyi7gJaPdyNntROEFTD7iO2L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTpOry/
Wvw0iKZFbo4AkiI0aLyBCk9HBXhUKa9x06gOnhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90wlRBUAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZIenrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQS4NAwARAQABzTlBV1MgT3BzSHVi
IGZvciBTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFAl/hGf8GCwkHCAMCBBUICgIEFgIBAAIZAQIbAwIeAQAh
CRAhgc9adPNF8RYhBDcvpelIaY930bOvqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIawOSXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmxWWbg
cxg1g0GXNXCM4lAd68CmbAOLoLTaWSQX30ZbswzhbtX2ADAlopV8RLBik7fm
bS9FyuubDRhfYRQq0fpjUGXFiEgwg6aMFxsrGLlv4QD7t+6ftFIe/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+FOVMmPeEN5JRazEeUrl
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDWOq/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty25lo8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4EDl19Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEZa/2upDJ1m+4OHK4p
8DrEzP/3jTahT8q5ofFWSRDL17d3lTSU+JBmPE3mz311FNXgiO8w+taY320z
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
O7vxMO5xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFZvzT/tDi5FiEEi+O9
V+UAYN9Gnw36EVm/NP+0OLnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvgOtUBxqmCOjr+8AKH0OtiBWSuO
lsS8JU5rindEsKUrKTwcG2wyZFoe1zlE8xPkLRSRN5ZbbgKsTz16l1HgCCId
Do+WJdDkWGWxmtDvzjM32EI/PVBd108ga9aPwXdhLwOdKAjZ4JrJXLUQJjRI
```

```
IVDSyMObEHOUM6a/+mWNZazNfo0LsGWqGVa6Xn5WJWlwR1S78vPNfO3BQYuO
YRjaVQR+kPtB9aSAZNi5sWfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7Xl03o/VjblneZOhJK6kAKU172tnPJTJ31JbOxX73wsMWDYZRZVcK
9X9+GFrpwhKHWKKPjpMOt/FRxNepvqRl72TkgBPqGH2TMOFdB1f/uQprvqge
PBbS0JrmBIH9/anIqgtMdtcNQB/0erLdCDqI5afOuD1OLcLwdJwG9/bSrfwT
TVEE3WbXmJ8pZgMzlHUiZE6V2DSadV/YItk50IOjjrOVHOHvlFMwGCEAIFzf
9P/pNi8hpEmlRphRiOVVcdQ30bH0M0gPHu5V9flIhyCL1zU3LjYTHkq0yJD5
YDA1xO1MYq3DcSM513OVBbLmuVS2GpcsTCYqlgQA6h/zzMwz+/7OwU0EX+EZ
/wEQAOAY8ULmcJIQWIr14V0jylpJeD3qwj7wd+QsBzJ+mOpOB/3ZFAhQiNOl
9yCDlHeiZeAmWYX9OIXrNiIdcHy+WTAp4G+NaMpqE52qhbDjz+IbvLpl1yDH
bYEHPjnTHXEy2lbvKAJOKkw/2RcQOi4dodGnq5icyYj+9gcuHvnVwbrQ96Ia
0D7c+b5T+bzFqk90nIcztrMRuhDLJnJpi7OjpvQwfq/TkkZA+mzupxfSkq/Y
N9qXNEToT/VI2gn/LS0X4Ar1l2KxBjzNEsQkwGSiWSYtMA5J+Tj5ED0uZ/qe
omNblAlD4bm7Na8NAoLxCtAiDq/f3To9Xb18lHsndOmfLCb/BVgP4edQKTIi
C/OZHy9QJlfmN0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXMOd3I
e6NUvU7pW0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQqYZe0
jXD3IJ7T+X2XA8M/BmypwMW0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcPxzehwsSVq1lzaL2ureJBLOKkBgYxUJYXpbS01ax1TsFG
09ldANOs9Ej8CND37GsNnuygjOgWXbX6MNgbvPs3H3zi/AbMunQ1VBlw07JX
zdM1hBQZh6w+NeiEsK1T6wHi7IhxABEBAAHCwXYEGAEIAAkFAl/hGf8CGwwA
IQkQIYHPWnTzRfEWIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PVbF
ywKvwi3GLOlpY7BXn8lQaHyunMGuavmO8OfaRROynkH0ZqLHCp6bIajFOfvF
b7c0Jamzx8Hg+SIdl6yRpRY+fA4RQ6PNnnmT93ZgWW3EbjPyJGlm0/rt03SR
+0yn4/ldlg2KfBX4pqMoPCMKUdWxGrmDETXsGihwZ0gmCZqXe8lK122PYkSN
JQQ+LlfjKvCaxfPKEjXYTbIbfyyhCR6NzAOVZxCrzSz2xDrYWp/V002Klxda
0ix6r2aEHf+xYEUhOaBt8OHY5nXTuRReCVU789MUVtCMqD2u6amdo4BR0kWA
QNg4yavKwV+LVtyYh2Iju9VSyv4xL1Q4xKHvcAUrSH73bHG7b7jkUJckD0f4
twhjJk/Lfwe6RdnVo2WoeTvE93w+NAq2FXmvbiG7eltl0XfQecvQU3QNbRvH
U8B96W0w8UXJdvTKg4f0NbjSw7iJ3x5naixQ+rA8hLV8xOgn2LX6wvxT/SEu
mn20KX+fPtJELK7v/NheFLX1jsKLXYo4jHrkfIXNsNUhg/x2E71kAjbeT3s+
t9kCtxt2iXDDZvpIbmGO4QkvLFvoROaSmN6+8fupe3e+e2yN0e6xGTuE60gX
I2+X1p1g9IduDYTpoI2OXleHyyMqGEeIb4gOiiSloTp5oi3EuAYRGflXuqAT
VA19bKnpkBsJ0A==
=tD2T
-----END PGP PUBLIC KEY BLOCK-----
```

2. Importieren Sie den öffentlichen Schlüssel in Ihren Schlüsselbund und notieren Sie den zurückgegebenen Schlüsselwert.

   GPG

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

Beispielausgabe

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

3. Überprüfen Sie den Fingerprint Stellen Sie sicher, dass Sie durch *key-value* den Wert aus dem vorherigen Schritt ersetzen. Wir empfehlen, GPG zur Überprüfung des Fingerabdrucks zu verwenden.

```
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 Snow Family <aws-opshub-signer@amazon.com>
sub   rsa4096 2020-12-21 [E]
```

Der Fingerabdruck sollte wie folgt aussehen:

```
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 AWS Support.

4. Überprüfen Sie das Installationspaket und laden Sie die SIGNATURE-Datei entsprechend der Architektur und dem Betriebssystem Ihrer Instance herunter, falls noch nicht geschehen.
5. Überprüfen Sie die Installer-Paketsignatur. Ersetzen Sie *signature-filename* und unbedingt durch *OpsHub-download-filename* die Werte, die Sie beim Herunterladen der SIGNATURE-Datei und AWS OpsHub -Anwendung angegeben haben.

GPG

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

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

GPG

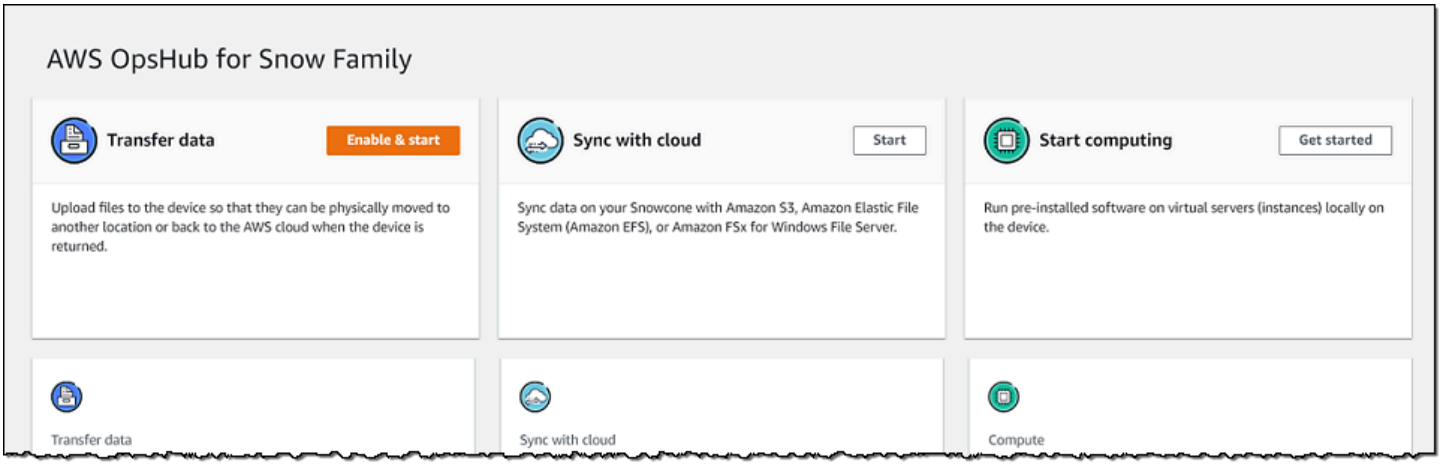
```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snow Family <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication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

Wenn die Ausgabe bei Verwendung von GPG den Satz enthält, überprüfen SieBAD `signature`, ob Sie das Verfahren korrekt ausgeführt haben. Wenn Sie diese Antwort weiterhin erhalten, wenden Sie sich an AWS Support und installieren Sie den Kundendienstmitarbeiter nicht. Die Warnmeldung über die Vertrauensstellung 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.

Verwalten von AWS Services auf Ihrem Gerät

Mit können AWS OpsHub Sie - AWS Services auf Ihren Snow Family-Geräten verwenden und verwalten. Derzeit AWS OpsHub unterstützt die folgenden Ressourcen:

- Amazon Elastic Compute Cloud (Amazon EC2)-Instances – Verwenden Sie Amazon EC2-compatible Instances, um Software auszuführen, die auf einem virtuellen Server installiert ist, ohne sie zur Verarbeitung an den AWS Cloud zu senden.
- Network File System (NFS) – Verwenden Sie Dateifreigaben, um Daten auf Ihr Gerät zu verschieben. Sie können das Gerät an senden AWS , um Ihre Daten an die zu übertragen AWS Cloud, oder verwenden, DataSync um an andere - AWS Cloud Standorte zu übertragen.
- Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Bietet sicheren Objektspeicher mit erhöhter Ausfallsicherheit, Skalierung und einem erweiterten Amazon S3-API-Feature-Set für Telefonie-, mobile Edge- und getrennte Umgebungen. Mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten können Sie Daten speichern und hochverfügbare Anwendungen auf Snow-Family-Geräten für Edge-Computing ausführen.



Themen

- Lokales Verwenden von Amazon EC2-compatible Rechen-Instances
- Verwalten eines Amazon EC2-Clusters
- Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten
- Verwalten des Amazon S3-Adapterspeichers
- Verwalten der NFS-Schnittstelle

Lokales Verwenden von Amazon EC2-compatible Rechen-Instances

Sie können verwenden AWS OpsHub , um vorinstallierte Software auf virtuellen Servern (Instances) lokal auf Ihrem Gerät auszuführen und auch Amazon-ECAmazon EC2 auf Ihrem Gerät zu verwalten.

Themen

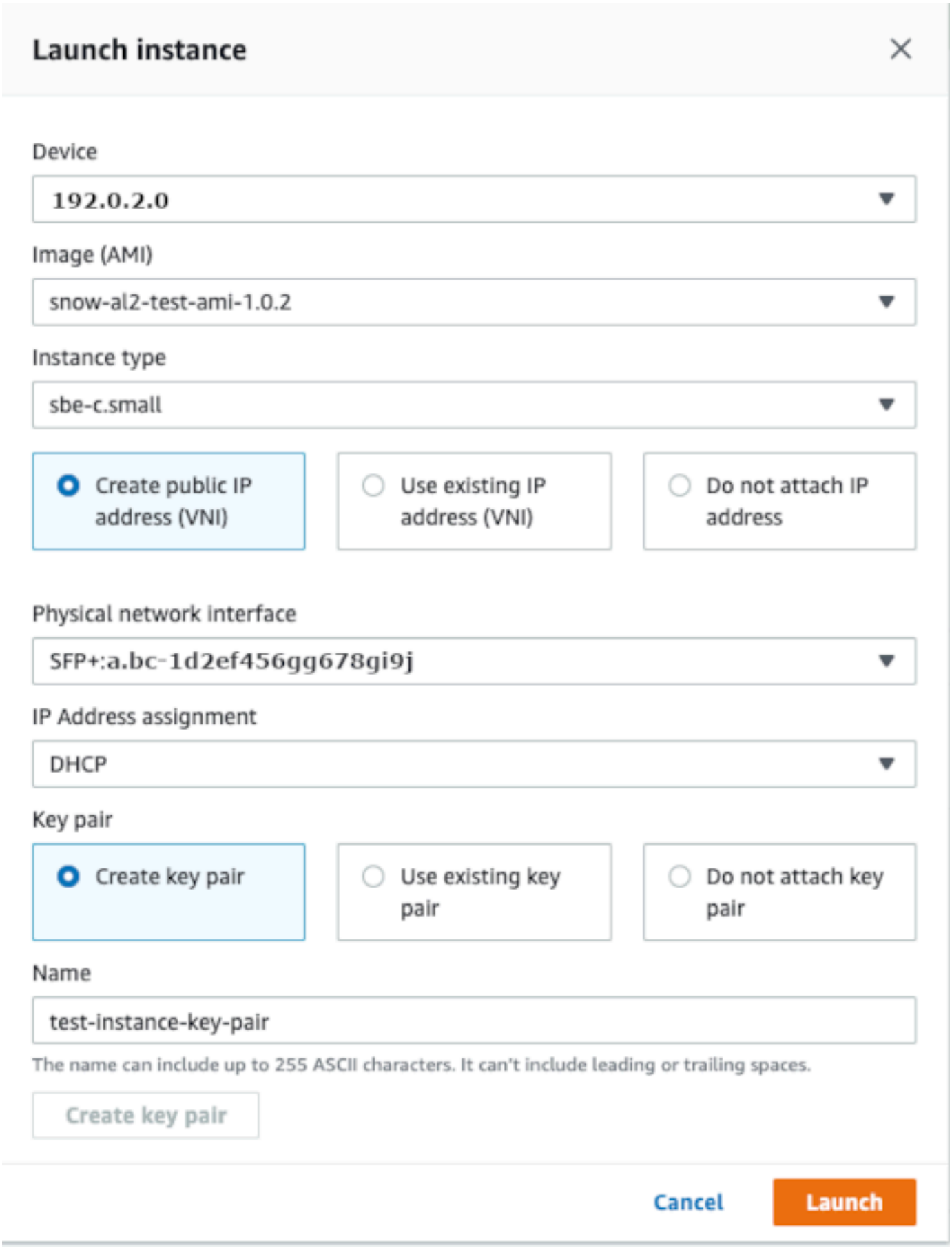
- Starten einer Amazon EC2-compatible Instance
- Anhalten einer Amazon EC2-compatible Instance
- Starten einer Amazon EC2-compatible Instance
- Arbeiten mit Schlüsselpaaren
- Beenden einer Amazon EC2-compatible Instance
- Lokale Verwendung von Speicher-Volumes
- Importieren eines Images in Ihr Gerät als Amazon EC2-compatible AMI
- Löschen eines Snapshots
- Aufheben der Registrierung eines AMI

Starten einer Amazon EC2-compatible Instance

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

So starten Sie eine Amazon EC2-compatible 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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wenn auf Ihrem Gerät Amazon EC2-compatible Instances ausgeführt werden, werden diese in der Spalte Instance-Name 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 für Gerät das Snow-Gerät aus, das Sie die AmazonEC2-compatible 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
Key pair
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 über eine physische Netzwerkschnittstelle zu erstellen. Wählen Sie eine physische Netzwerkschnittstelle und eine IP-Adresszuweisung aus.
   - Vorhandene IP-Adresse (VNI) verwenden – Wählen Sie diese Option, um eine vorhandene IP-Adresse zu verwenden, und verwenden Sie dann vorhandene virtuelle Netzwerkschnittstellen. Wählen Sie eine physische und eine virtuelle Netzwerkschnittstelle aus.
   - IP-Adresse nicht anfügen – Wählen Sie diese Option, wenn Sie keine IP-Adresse anfügen möchten.
9. Wählen Sie aus, wie Sie ein Schlüsselpaar an die Instance anfügen möchten. Ihnen stehen folgende Optionen zur Verfügung:

   Schlüsselpaar erstellen – Wählen Sie diese Option, um ein neues Schlüsselpaar zu erstellen und die neue Instance mit diesem Schlüsselpaar zu starten.

   Vorhandenes Schlüsselpaar verwenden – Wählen Sie diese Option, um ein vorhandenes Schlüsselpaar zum Starten der Instance zu verwenden.

   IP-Adresse nicht anfügen – Wählen Sie diese Option, wenn Sie kein Schlüsselpaar anfügen möchten. Sie müssen bestätigen, dass Sie keine Verbindung zu dieser Instance herstellen können, es sei denn, Sie kennen bereits das Passwort, das in dieses AMI integriert ist.

   Weitere Informationen finden Sie unter Arbeiten mit Schlüsselpaaren.
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.

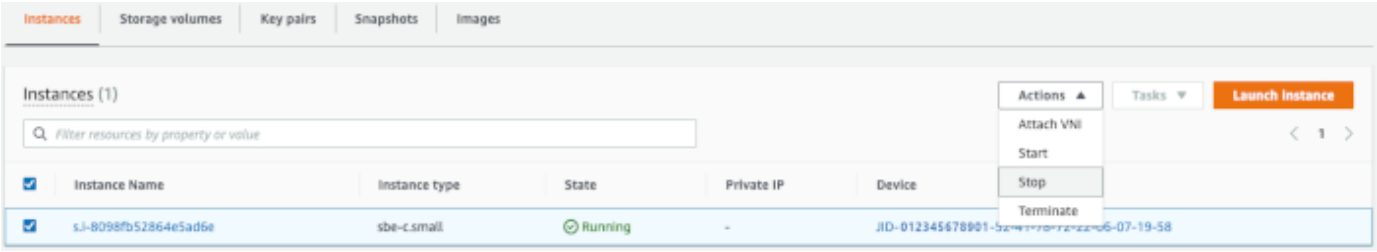
Anhalten einer Amazon EC2-compatible Instance

Führen Sie die folgenden Schritte aus, um eine AmazonEC2-compatible Instance AWS OpsHub mit anzuhalten.

So halten Sie eine Amazon EC2-compatible Instance an

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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen.

   Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wenn auf Ihrem Gerät Amazon EC2-compatible Instances ausgeführt werden, werden diese in der Spalte Instance-Name unter Instances angezeigt.
4. Wählen Sie die Instance aus, die Sie anhalten möchten, wählen Sie das Menü Aktionen und dann Anhalten aus. Der State (Status) wird in Stopping (Wird angehalten) und anschließend nach Abschluss in Stopped (Angehalten) geändert.



Starten einer Amazon EC2-compatible Instance

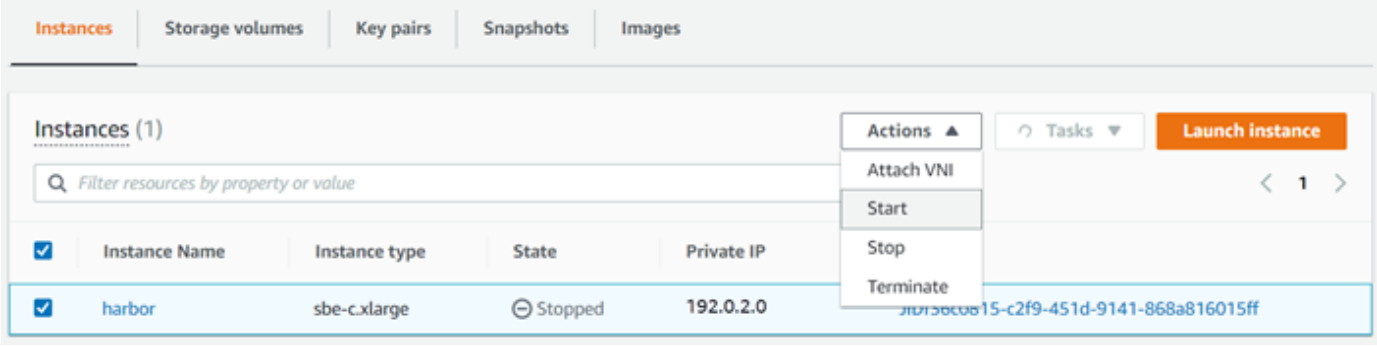
Gehen Sie wie folgt vor, um eine Amazon EC2-compatible Instance mit zu starten AWS OpsHub.

So starten Sie eine Amazon EC2-compatible 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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen.

   Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Suchen Sie in der Spalte Instance name (Instance-Name) unter Instances (Instanzen) die Instance, die Sie starten möchten.

4. 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

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

So erstellen, importieren oder verwalten Sie Schlüsselpaare

1. Öffnen Sie Datenverarbeitung im AWS OpsHub Dashboard.
2. Wählen Sie im Navigationsbereich die Seite Datenverarbeitung (EC2) und dann die Registerkarte Schlüsselpaare aus. Sie werden zur Amazon EC2-Konsole weitergeleitet, in der Sie Ihre Schlüsselpaare erstellen, importieren oder verwalten können.
3. Anweisungen zum Erstellen und Importieren von Schlüsselpaaren finden Sie unter Amazon EC2-Schlüsselpaare und Linux-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Beenden einer Amazon EC2-compatible Instance

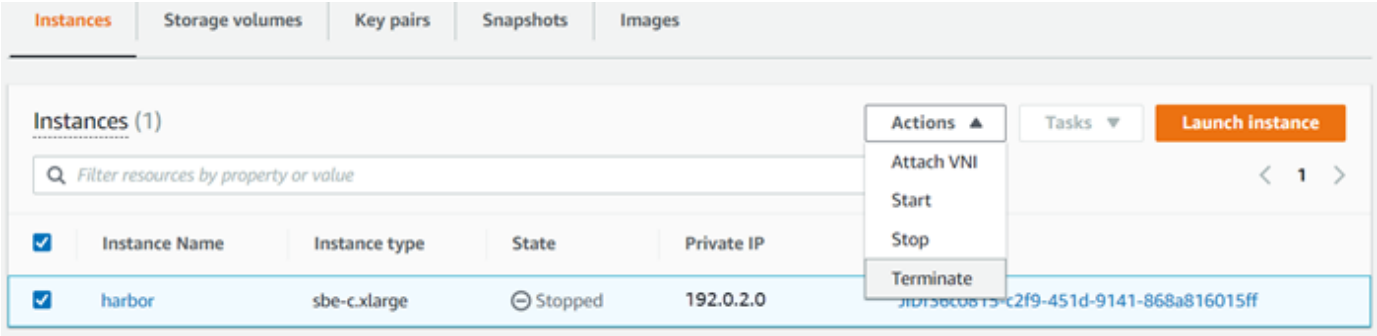
Nachdem Sie eine Amazon EC2-compatible Instance beendet haben, können Sie die Instance nicht neu starten.

So beenden Sie eine Amazon EC2-compatible Instance

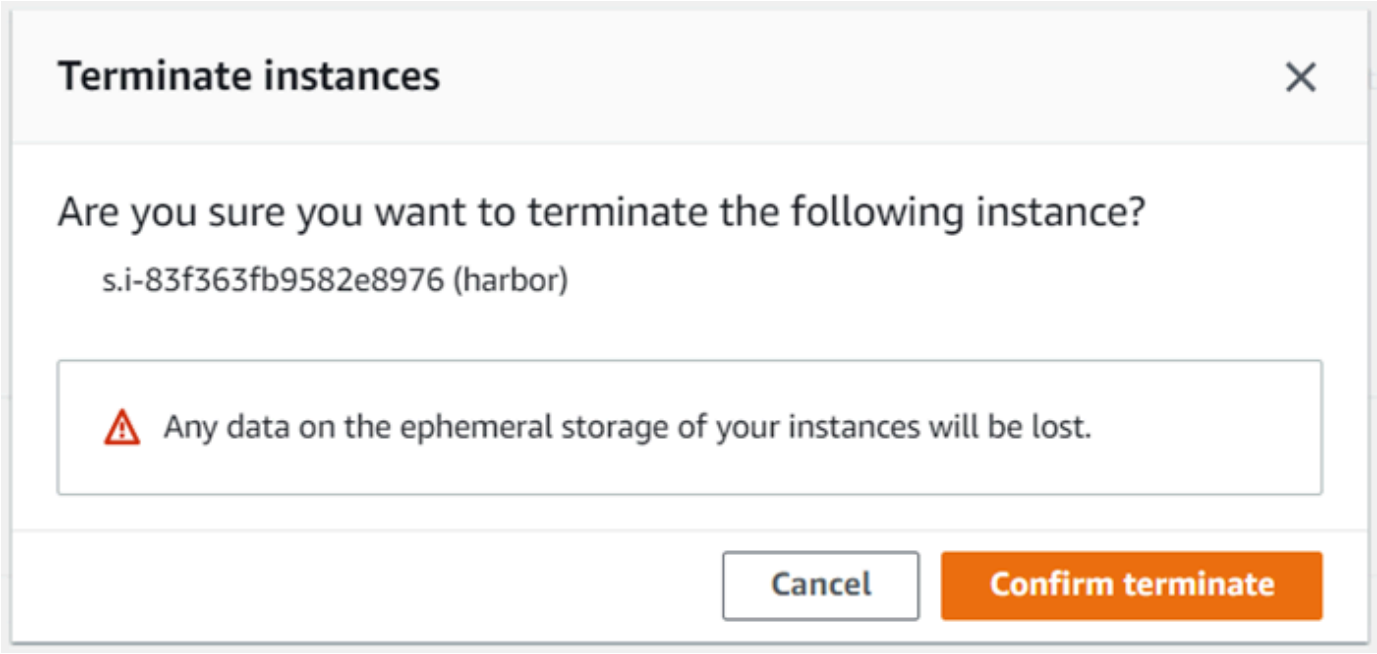
1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und

anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) 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 Instance und dann das Menü Aktionen aus. Wählen Sie im Menü Aktionen die Option Beenden aus.



5. Wählen Sie im Fenster Instances beenden die Option Beenden aus.



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

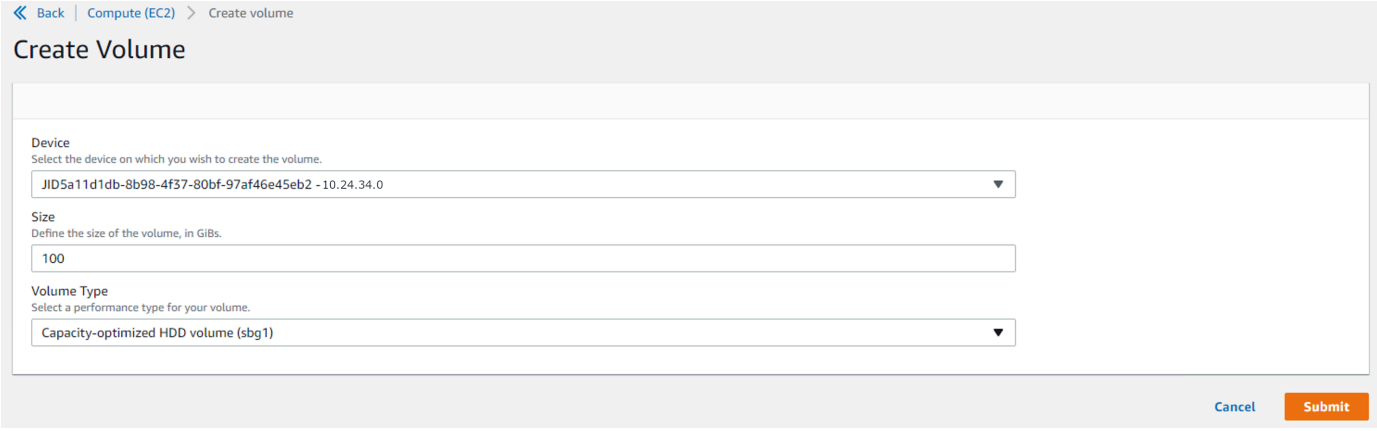
Der State (Status) wird in Terminating (Wird beendet) und anschließend nach Abschluss in Terminated (Beendet) geändert.

Lokale Verwendung von Speicher-Volumes

Amazon EC2-compatible Instances verwenden Amazon EBS-Volumes für die Speicherung. In diesem Verfahren erstellen Sie ein Speicher-Volume und fügen es mit an Ihre Instance an 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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) 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.

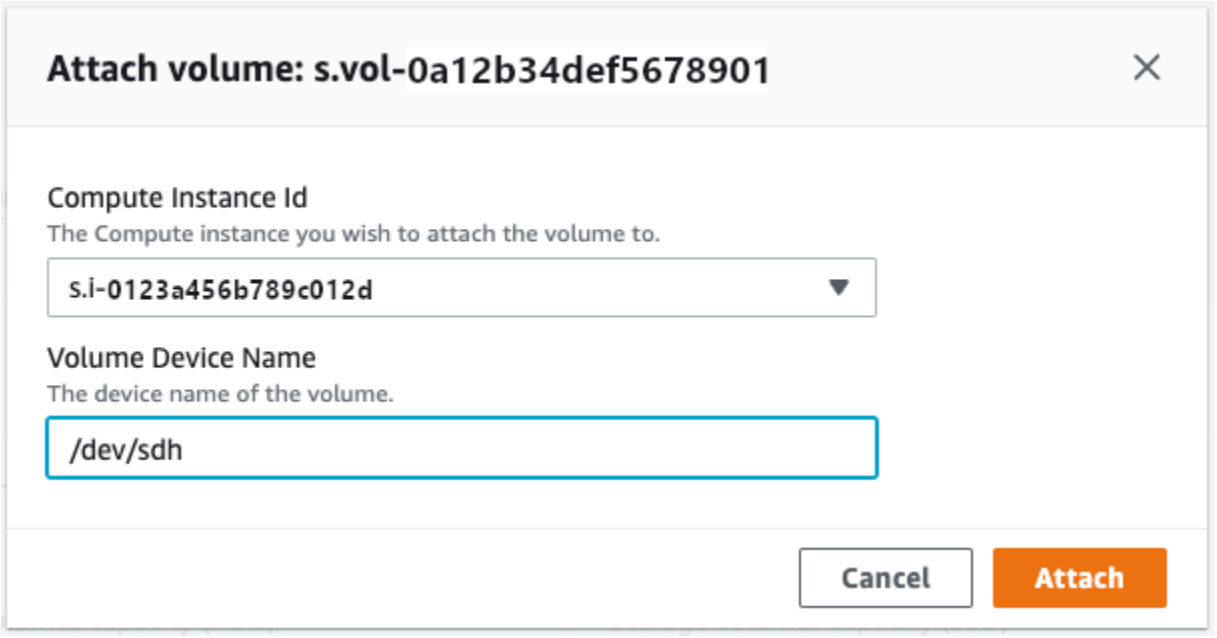


5. Wählen Sie das Gerät aus, auf dem Sie das Volume erstellen möchten, geben Sie die Größe (in GiBs) ein, die Sie erstellen möchten, und wählen Sie den Volume-Typ aus.

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.



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-Gerätename) 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.

Importieren eines Images in Ihr Gerät als Amazon EC2-compatible AMI

Sie können einen Snapshot Ihres Bildes in Ihr Snowball Edge-Gerät importieren und als Amazon EC2-compatible Amazon Machine Image (AMI) registrieren. Ein Snapshot ist im Grunde eine Kopie Ihres Speicher-Volumes, mit der Sie ein AMI oder ein anderes Speicher-Volume erstellen können.

Auf diese Weise können Sie Ihr eigenes Image aus einer externen Quelle auf Ihr Gerät bringen und es als Amazon EC2-compatible Instance starten.

Gehen Sie wie folgt vor, um den Import Ihres Images abzuschließen.

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

> **Note**
>
> Beachten Sie die folgenden Einschränkungen beim Hochladen von Snapshots auf Snow Family-Geräte.
>
> - Snow Family-Geräte unterstützen derzeit nur den Import von Snapshots im RAW-Image-Format.
> - Geräte der Snow Family unterstützen derzeit nur den Import von Snapshots mit Größen von 1 GB bis 1 TB.

Schritt 1: Hochladen eines Snapshots in einen S3-Bucket auf Ihrem Gerät

Sie müssen Ihren Snapshot auf Amazon S3 auf Ihr Gerät 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 Image gespeichert werden soll.

So laden Sie einen Snapshot in Amazon S3 hoch

- Informationen zum Erstellen eines S3-Buckets finden Sie unter Erstellen von Amazon S3 Storage.

  Informationen zum Hochladen eines Snapshots in einen S3-Bucket finden Sie unter Hochladen von Dateien in Amazon S3 Storage.

Schritt 2: Importieren des Snapshots aus einem S3-Bucket

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

So importieren Sie den Snapshot auf Ihr Gerät

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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie die Registerkarte Snapshots, um alle Snapshots anzuzeigen, 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 Snapshot-ID oder Status des Snapshots filtern, um bestimmte Snapshots zu finden. Sie können eine Snapshot-ID auswählen, um Details zu diesem Snapshot anzuzeigen.
4. Wählen Sie den Snapshot aus, den Sie importieren möchten, und klicken Sie auf Snapshot importieren, um die Seite Snapshot importieren zu öffnen.
5. Wählen Sie für Gerät die IP-Adresse des Snow Family-Geräts aus, in das Sie importieren möchten.
6. Geben Sie für Importbeschreibung und Snapshot-Beschreibung jeweils eine Beschreibung ein.
7. Wählen Sie in der Liste Rolle eine Rolle aus, die für den Import verwendet werden soll. Snow Family-Geräte verwenden VM Import/Export, um Snapshots zu importieren. AWS übernimmt diese Rolle und verwendet sie, um den Snapshot in Ihrem Namen zu importieren. Wenn Sie keine Rolle auf Ihrem konfiguriert haben AWS Snowball Edge, öffnen Sie die AWS Identity and Access Management (IAM in AWS OpsHub , in der Sie eine lokale IAM-Rolle erstellen können. Die Rolle benötigt auch eine Richtlinie, die über die erforderlichen VM Import/Export-Berechtigungen zum Durchführen des Imports verfügt. Sie müssen diese Richtlinie an die Rolle anfügen. Weitere Informationen dazu finden Sie unter Lokale Verwendung von IAM.

   Im Folgenden finden Sie ein Beispiel für die -Richtlinie.

```
{
   "Version":"2012-10-17",
```

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

Melden Sie sich bei der an AWS Management Console 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.

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

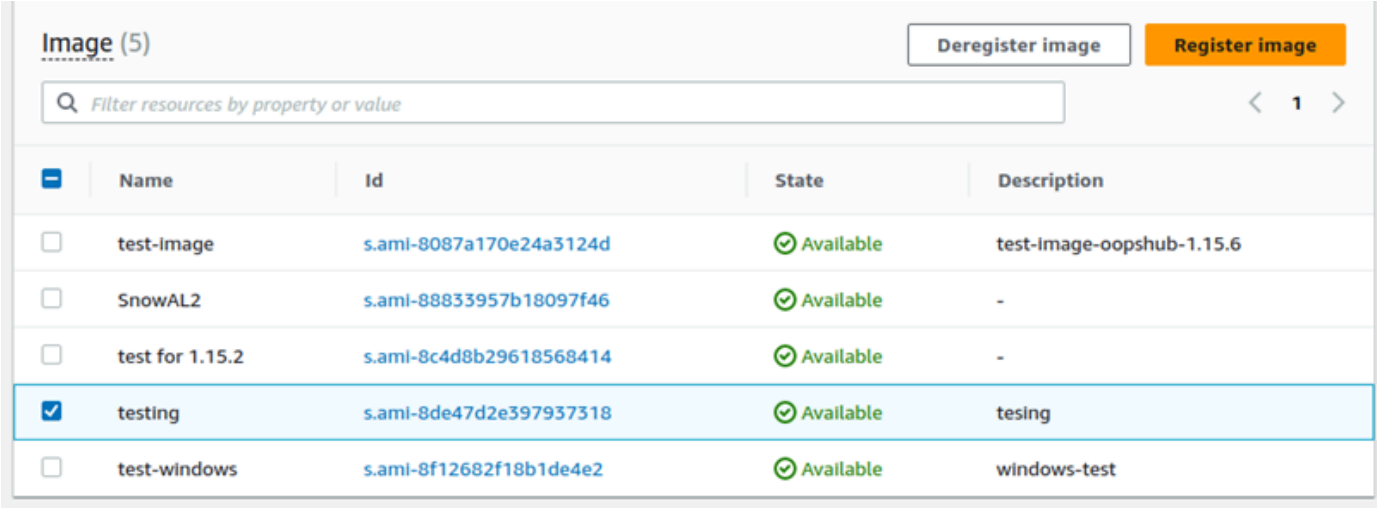
8. Wählen Sie S3 durchsuchen und wählen Sie den S3-Bucket aus, der den Snapshot enthält, den Sie importieren möchten. Wählen Sie den Snapshot und dann Absenden aus. Der Snapshot beginnt mit dem Herunterladen auf Ihr Gerät. Sie können die Snapshot-ID auswählen, um die Details anzuzeigen. Sie können den Importvorgang von dieser Seite aus abbrechen.

Schritt 3: Registrieren des Snapshots als AmazonEC2-compatible AMI

Das Erstellen eines AmazonEC2-compatible AMI aus einem als Snapshot importierten Image wird als Registrierung bezeichnet. Images, die auf Ihr Gerät importiert werden, müssen registriert werden, bevor sie als Amazon EC2-compatible Instances gestartet werden können.

So registrieren Sie ein als Snapshot importiertes Image

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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie die Registerkarte Images. Sie können die Bilder nach Namen, ID oder Status filtern, um ein bestimmtes Bild zu finden.
4. Wählen Sie das Image aus, das Sie registrieren möchten, und wählen Sie Image registrieren aus.



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

   Im Abschnitt Blockgerät können Sie die Größe des Volumes und den Volume-Typ ändern.
7. Wenn Sie möchten, dass das Volume gelöscht wird, wenn die Instance beendet wird, wählen Sie Bei Beendigung löschen aus.
8. Wenn Sie weitere Volumes hinzufügen möchten, wählen Sie Neues Volume hinzufügen aus.

9. Wenn Sie fertig sind, wählen Sie Senden aus.

Schritt 4: Starten des AmazonEC2-compatible AMI

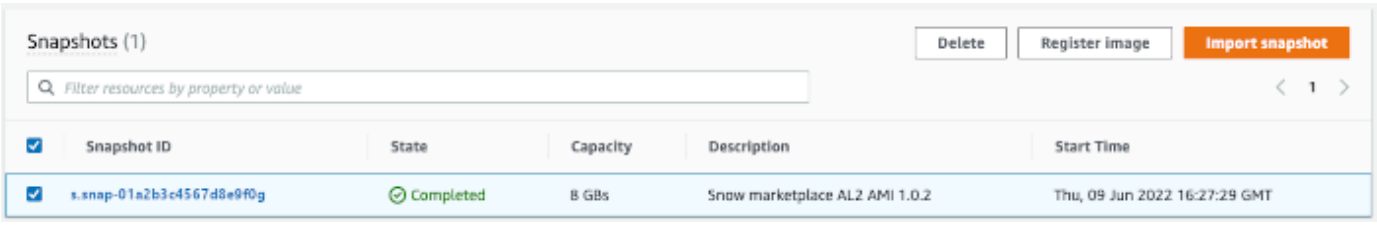
- Weitere Informationen finden Sie unter Starten einer AmazonEC2-compatible Instance.

Löschen eines Snapshots

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 zu löschende Snapshot von einem Image verwendet wird, kann er nicht gelöscht werden. Nachdem der Import abgeschlossen ist, können Sie auch die .raw-Datei löschen, die Sie auf Amazon S3 auf Ihrem Gerät hochgeladen haben.

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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wählen Sie die Registerkarte Snapshot, um alle importierten Snapshots anzuzeigen. 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 wählen Sie Löschen aus. Sie können mehrere Snapshots auswählen.

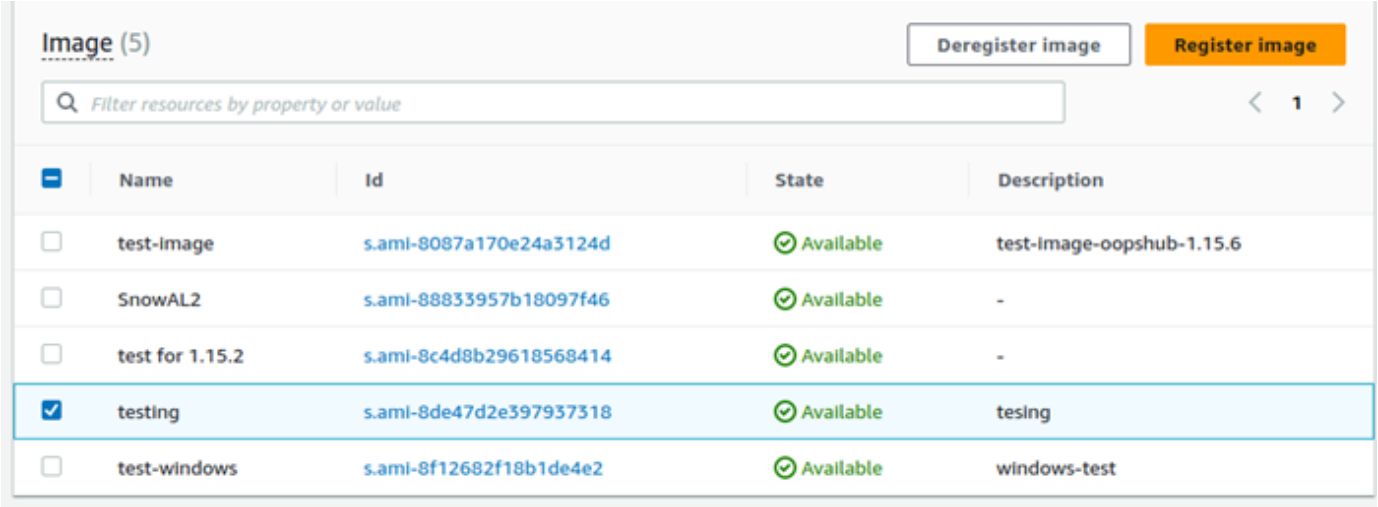


5. Wählen Sie im Bestätigungsfeld Snapshot löschen die Option Snapshot löschen aus. Wenn Ihr Löschvorgang erfolgreich ist, wird der Snapshot aus der Liste auf der Registerkarte Snapshots entfernt.

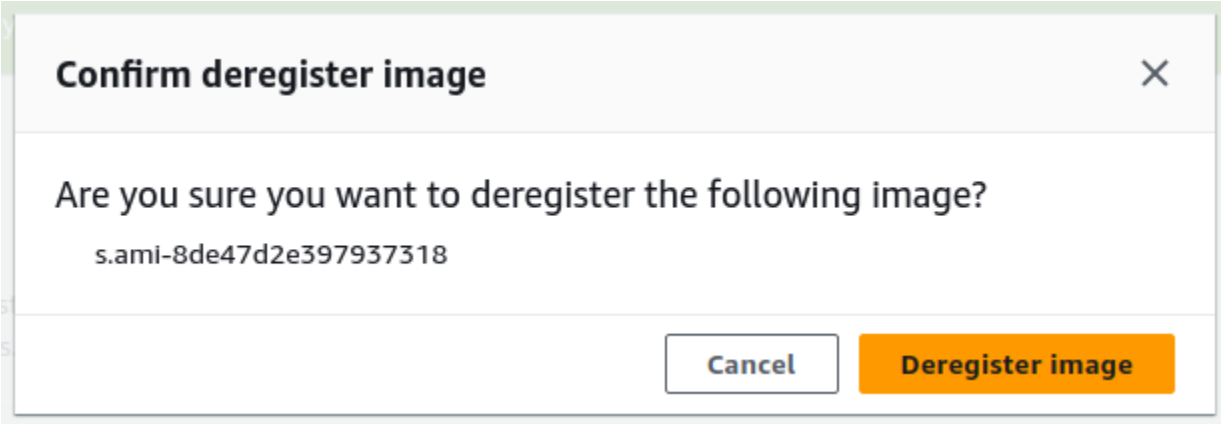
Aufheben der Registrierung eines AMI

So heben Sie die Registrierung eines AMI auf

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. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) 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 Namen, ID oder Status filtern, um ein bestimmtes Bild zu finden.
4. Wählen Sie das Abbild aus, dessen Registrierung Sie aufheben möchten, und wählen Sie Abmelden aus.



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



Verwalten eines Amazon EC2-Clusters

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

So erstellen Sie einen Amazon EC2-Cluster

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 Geräts.
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 256-Bit-Verschlüsselung, um sowohl Sicherheit als auch vollständige Daten chain-of-custody zu gewährleisten.

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

   Sie können jetzt mit der Verwendung von - AWS Services und der Verwaltung Ihres Clusters beginnen. Sie verwalten die Instances im Cluster genau wie einzelne Instances. Anleitungen Anweisungen finden Sie unter Verwalten von AWS Services auf Ihrem Gerät oder Verwaltung Ihrer Geräte.

Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten

Der Amazon S3-kompatible Speicher auf Snow-Family-Geräten ist standardmäßig nicht aktiv. Um den Service auf einem Gerät oder Cluster zu starten, müssen Sie zwei virtuelle Netzwerkschnittstellen (VNICs) auf jedem Gerät erstellen, um sie an die `s3api` Endpunkte `s3control` und anzufügen.

Themen

Voraussetzungen

Bevor Sie Ihr Gerät oder Ihren Cluster mit einrichten können AWS OpsHub for Snow Family, 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 herunter und installieren Sie sieAWS OpsHub. Stellen Sie eine Verbindung zum Gerät oder Cluster her, um es mit einer Manifestdatei zu entsperren. Weitere Informationen finden Sie unter Entsperren eines Geräts.

Verwenden der einfachen Einrichtungsoption

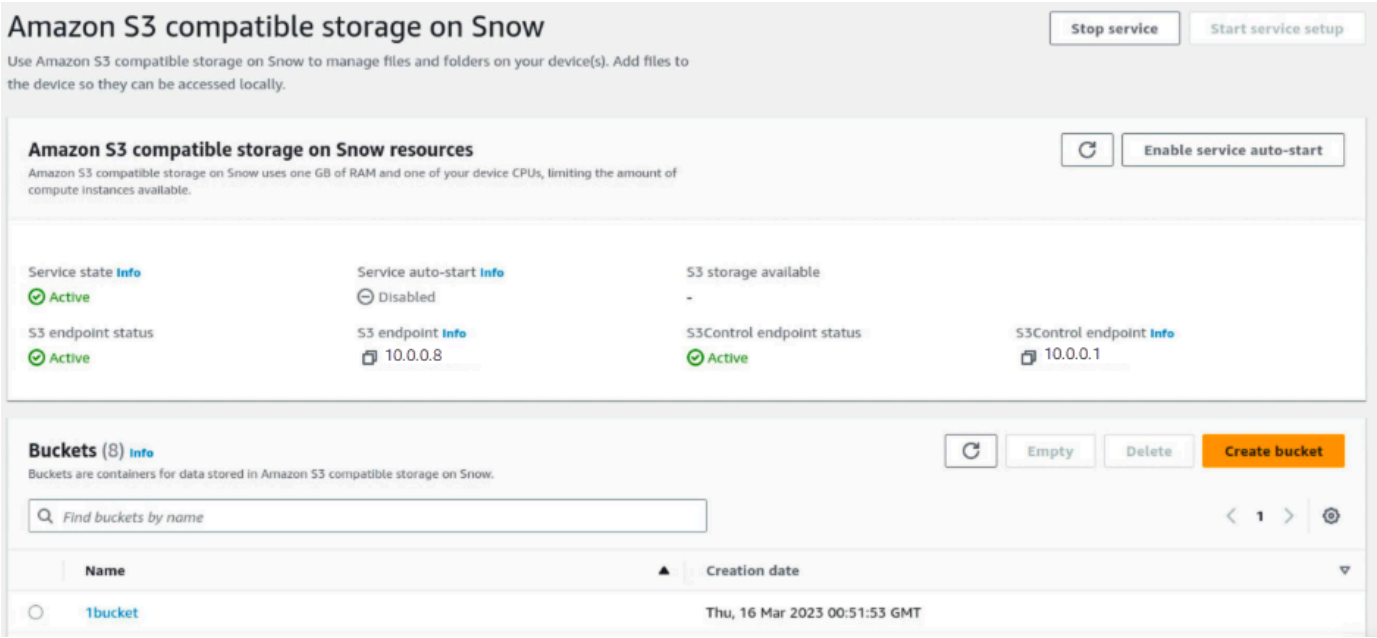
Verwenden Sie die einfache Einrichtungsoption, wenn Ihr Netzwerk DHCP verwendet. Mit dieser Option werden die VNICs automatisch auf jedem Gerät erstellt, wenn Sie den Service starten.

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

   Dadurch gelangen Sie zur Startseite für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten.
2. Wählen Sie für Service-Einrichtungstyp starten die Option Einfach aus.
3. Wählen Sie Service starten aus.

> **Note**
>
> Dies dauert einige Minuten und hängt von der Anzahl der von Ihnen verwendeten Geräte ab.

Nach dem Start des Services ist der Servicestatus aktiv und es gibt Endpunkte.



Verwenden der erweiterten Einrichtungsoption

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

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

   Dadurch gelangen Sie zur Startseite für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten.
2. Wählen Sie für Service-Einrichtungstyp starten die Option Erweitert aus.
3. Wählen Sie die Geräte aus, für die Sie VNICs erstellen müssen.

   Für Cluster benötigen Sie ein Mindestquorum von Geräten, um den Amazon S3-kompatiblen Speicher auf dem Snow-Family-Geräteservice zu starten. Das Quorum ist zwei für einen Cluster mit drei Knoten.

   > **Note**
   >
   > Für den ersten Start des Services in einer Cluster-Einrichtung müssen Sie alle Geräte im Cluster konfiguriert und verfügbar haben, damit der Service gestartet werden kann. Für nachfolgende Starts können Sie eine Teilmenge der Geräte verwenden, wenn Sie das Quorum erfüllen, aber der Service startet in einem degradierten Zustand.
4. Wählen Sie für jedes Gerät eine vorhandene VNIC oder wählen Sie VNI erstellen 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 aus.
6. Nachdem Sie Ihr VNICS erstellt haben, wählen Sie Service starten aus.

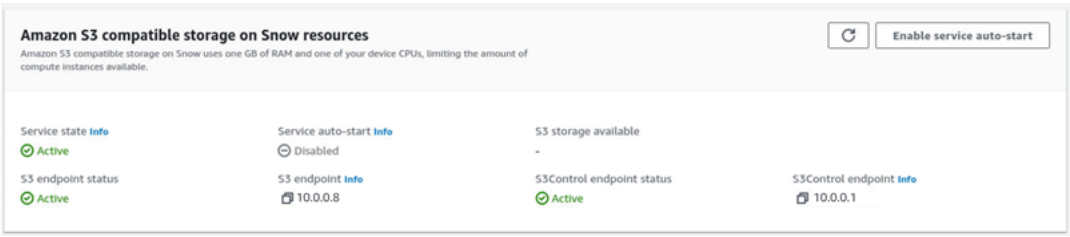
   > **Note**
   >
   > Dies dauert einige Minuten und hängt von der Anzahl der von Ihnen verwendeten Geräte ab.

Nach dem Start des Services ist der Servicestatus aktiv und es gibt Endpunkte.

Konfigurieren des Amazon S3-kompatiblen Speichers auf Snow-Family-Geräten für den automatischen Start

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

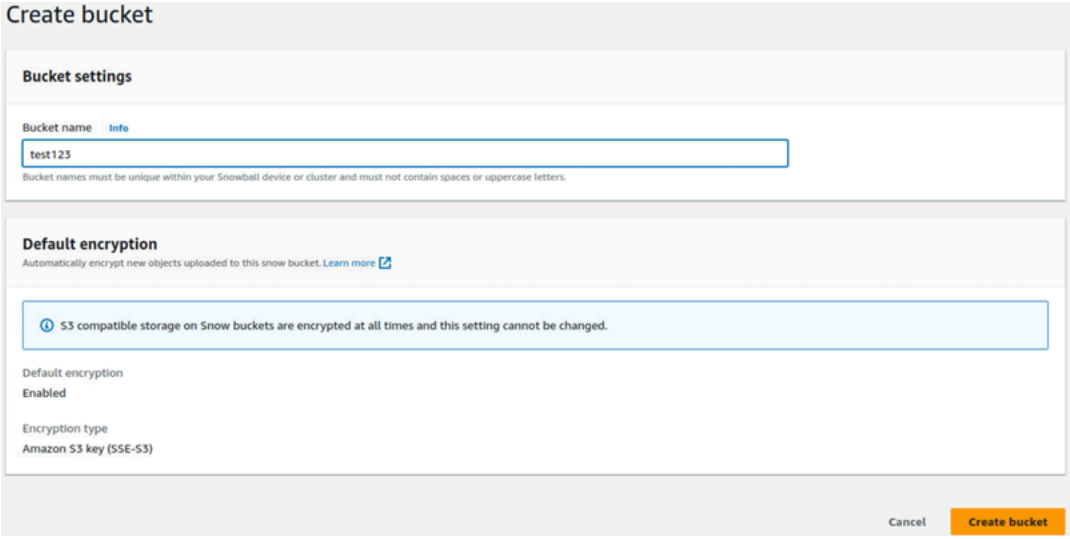
   Dadurch gelangen Sie zur Startseite des Amazon S3-kompatiblen Speichers auf Snow-Family-Geräten.
2. Wählen Sie im Amazon S3-kompatiblen Speicher auf Snow-Ressourcen die Option Service-Autostart aktivieren aus. Das System konfiguriert den Service so, dass er in Zukunft automatisch gestartet wird.



Erstellen eines Buckets im Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten

Verwenden Sie die - AWS OpsHub Schnittstelle, um einen Amazon S3-Bucket auf Ihrem Snow-Family-Gerät zu erstellen.

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



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

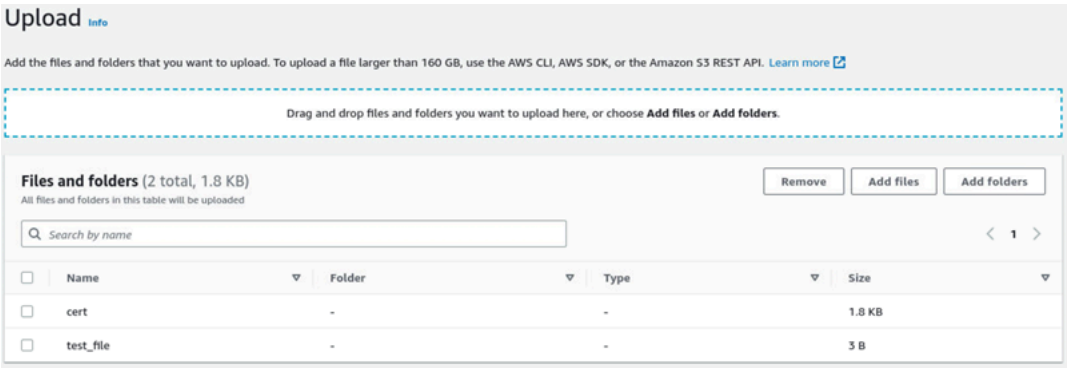
> **Note**
>
> Bucket-Namen müssen innerhalb Ihres Snowball-Geräts oder -Clusters eindeutig sein und dürfen keine Leerzeichen oder Großbuchstaben enthalten.

5. Wählen Sie Bucket erstellen aus. Das System erstellt den Bucket und er wird in Buckets auf der Seite Amazon S3-kompatibler Speicher in Snow angezeigt.

Hochladen von Dateien und Ordnern in Amazon S3-kompatiblen Speicher auf Geräte-Buckets der Snow Family

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

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



4. Laden Sie Dateien oder Ordner hoch, indem Sie sie aus einem Betriebssystem-Dateimanager 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 aus, die hochgeladen werden sollen. 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 von Dateien und Ordnern aus dem Amazon S3-kompatiblen Speicher auf Geräte-Buckets der Snow Family

Verwenden Sie die - AWS OpsHub Schnittstelle, um Dateien und Ordner aus Buckets auf dem Snow Family-Gerät zu entfernen und dauerhaft zu löschen.

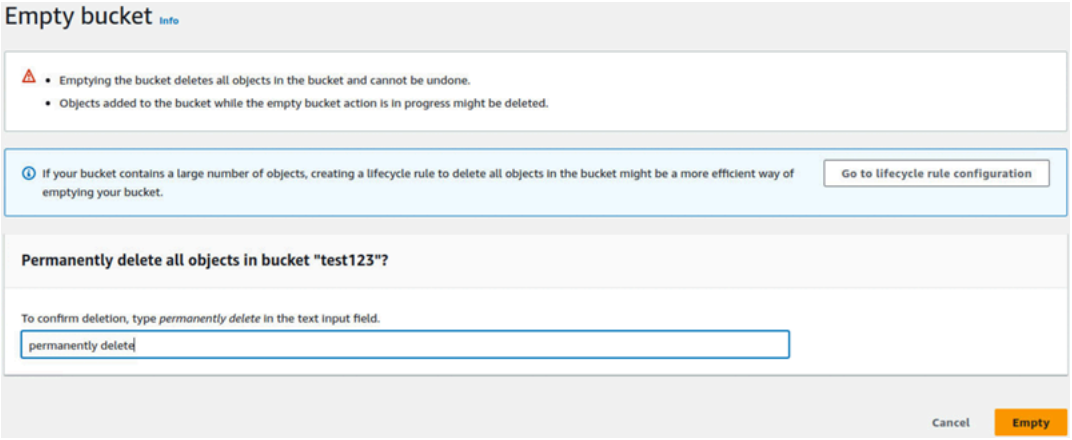
1. Öffnen Sie AWS OpsHub.
2. Wählen Sie unter Speicher verwalten in Buckets den Namen eines Buckets aus, aus dem Dateien und Ordner gelöscht werden sollen. Die Seite für diesen Bucket wird angezeigt.
3. Aktivieren Sie unter Dateien und Ordner die Kontrollkästchen der Dateien und Ordner, die dauerhaft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

Löschen von Buckets aus Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten

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 für leere Buckets. Informationen zum Entfernen von Dateien und Ordnern finden Sie unter Entfernen von Dateien und Ordnern aus dem Amazon S3-kompatiblen Speicher auf Geräte-Buckets der Snow Family.

So verwenden Sie das Tool zum Leeren von Buckets

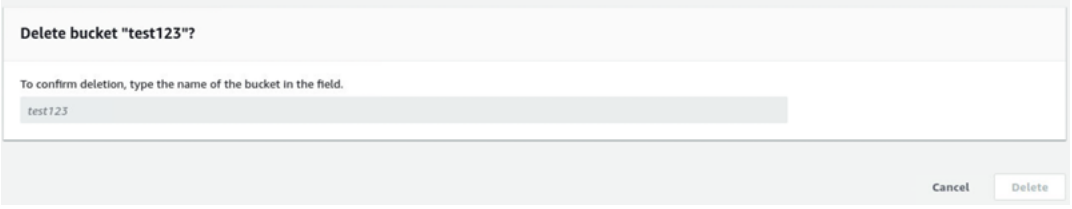
1. Öffnen Sie AWS OpsHub.
2. Wählen Sie unter Speicher verwalten in Buckets das Optionsfeld des zu leerenden Buckets aus.
3. Wählen Sie Leer aus. Die Seite Leerer Bucket wird angezeigt.



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

So löschen Sie einen leeren Bucket

1. Wählen Sie unter Speicher verwalten in Buckets das Optionsfeld des zu löschenden Buckets aus.
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.

Verwalten des Amazon S3-Adapterspeichers

Sie können verwenden AWS OpsHub , um Amazon Simple Storage Service (Amazon S3)-Speicher auf Ihren Snow Family-Geräten zu erstellen und zu verwalten, indem Sie den S3-Adapter für Import- und Exportaufträge verwenden.

Themen

Zugriff auf Amazon S3 Storage

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 in importieren, AWS Cloud wenn das Gerät zurückgegeben wird.

Geräte der Snow Family verwenden Amazon S3-Buckets, um Dateien auf Ihrem Gerät zu speichern und zu verwalten.

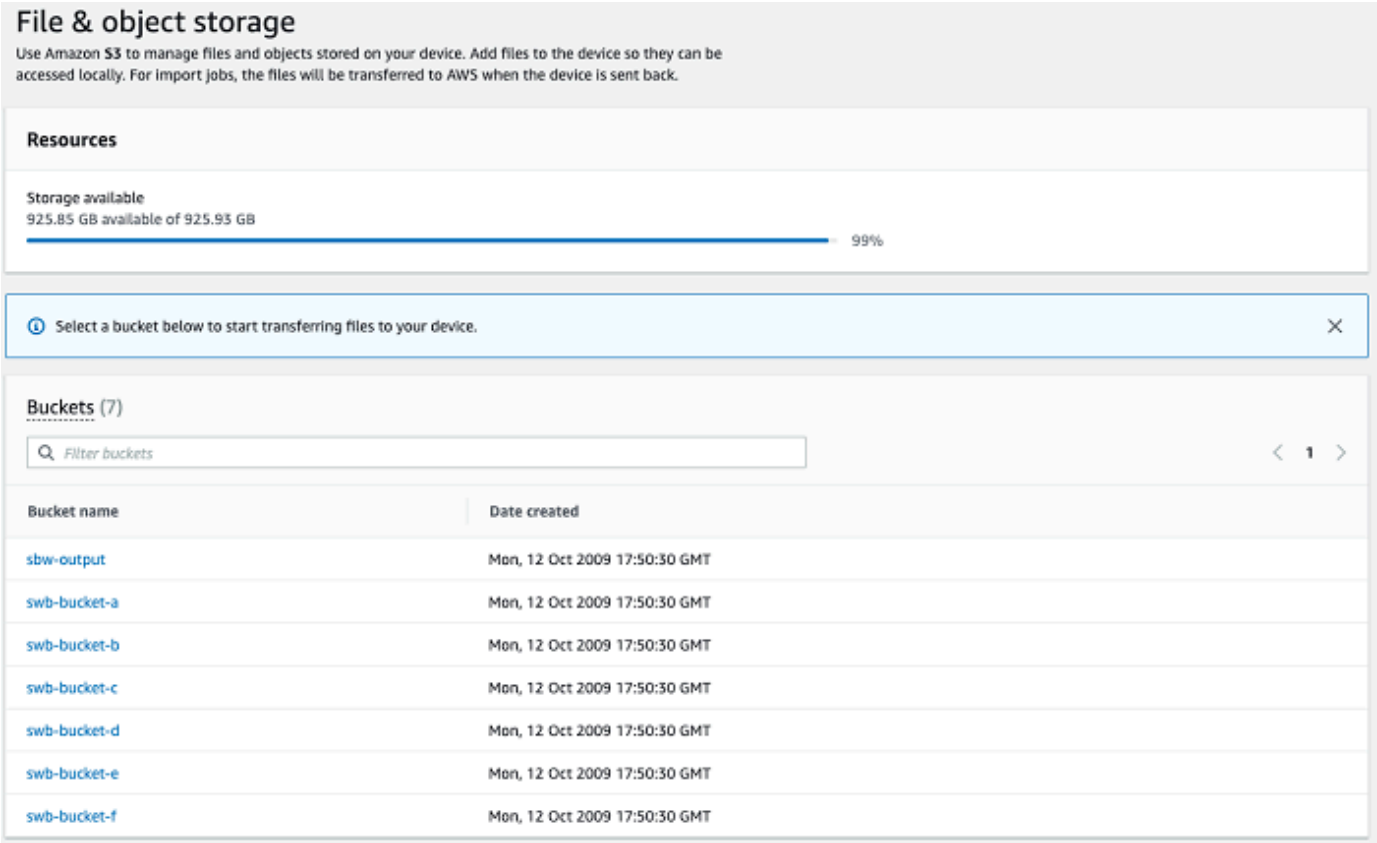
So greifen Sie auf einen S3-Bucket zu

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-Übertragungsmechanismus bestellt wurde, werden diese im Abschnitt Buckets der Seite Datei- und Objektspeicher angezeigt. Auf der Seite Datei- und Objektspeicher können Sie Details zu jedem Bucket anzeigen.

   > **Note**
   >
   > Wenn das Gerät mit dem NFS-Übertragungsmechanismus bestellt wurde, wird der Bucket-Name nach der Konfiguration und Aktivierung des NFS-Service unter dem

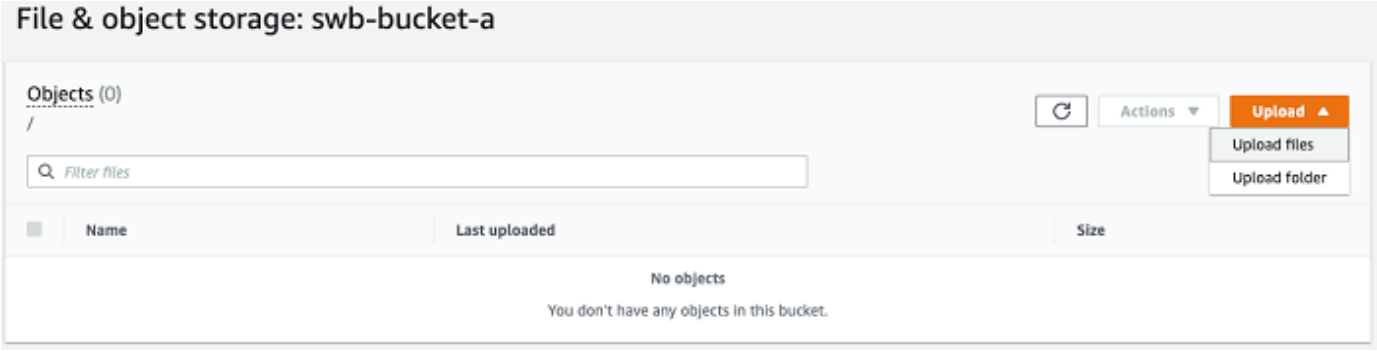
Abschnitt Mountingpunkte angezeigt. Weitere Informationen zur Verwendung der Dateischnittstelle finden Sie unter Verwalten der NFS-Schnittstelle.



Hochladen von Dateien in den Amazon S3-Speicher

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-Buckets auf Ihrem Gerät haben, werden diese im Abschnitt Buckets auf der Seite Dateispeicher 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 die Dateien per Drag-and-Drop im Bucket und dann OK aus.

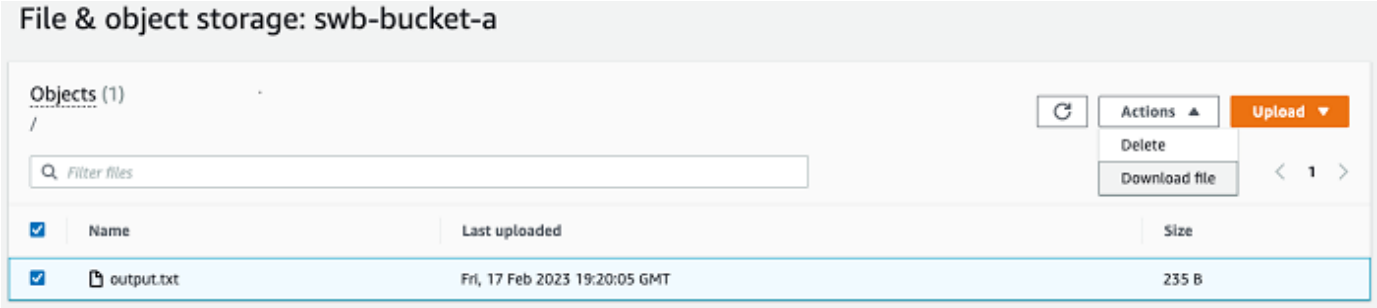


> **Note**
>
> Um größere Dateien hochzuladen, können Sie das Feature für mehrteilige Uploads in Amazon S3 mithilfe der verwenden AWS CLI. Weitere Informationen zum Konfigurieren von S3-CLI-Einstellungen finden Sie unter CLI-S3-Konfiguration. Weitere Informationen zum mehrteiligen Upload finden Sie unter Übersicht über den mehrteiligen Upload im Benutzerhandbuch für Amazon Simple Storage Service.
> Das Hochladen eines Ordners von einem lokalen Computer auf Snowball Edge mit der AWS OpsHub wird unterstützt. Wenn die Ordnergröße sehr groß ist, dauert es einige Zeit, OpsHub bis die Datei-/Ordnerauswahl gelesen hat. Während die Dateien und Ordner OpsHub liest, wird kein Fortschritts-Tracker angezeigt. Es zeigt jedoch an, dass ein Fortschritts-Tracker angezeigt wird, sobald der Upload-Prozess beginnt.

Herunterladen von Dateien aus dem Amazon S3-Speicher

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-Speicher

Wenn Sie eine Datei nicht mehr benötigen, können Sie sie aus Ihrem Amazon 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-Buckets auf Ihrem Gerät haben, werden diese im Abschnitt Buckets auf der Seite Dateispeicher 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.

Verwalten der NFS-Schnittstelle

Verwenden Sie die Network File System (NFS)-Schnittstelle, um Dateien auf das Snow Family-Gerät hochzuladen, als wäre das Gerät lokaler Speicher auf Ihrem Betriebssystem. Dies ermöglicht einen benutzerfreundlicheren Ansatz für die Übertragung von Daten, da Sie Funktionen Ihres Betriebssystems verwenden können, z. B. das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche. Jeder S3-Bucket auf dem Gerät ist als NFS-Schnittstellenendpunkt verfügbar und kann zum Kopieren von Daten gemountet werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

Sie können die NFS-Schnittstelle verwenden, wenn das Snowball Edge-Gerät so konfiguriert wurde, dass es beim Erstellen des Auftrags zur Bestellung des Geräts enthalten war. Wenn das Gerät nicht für die Aufnahme der NFS-Schnittstelle konfiguriert ist, verwenden Sie den S3-Adapter oder Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten, um Daten zu übertragen. Weitere Informationen zum S3-Adapter finden Sie unter Verwalten des Amazon S3-Adapterspeichers. Weitere Informationen zum Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten finden Sie unter Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.

Beim Start verwendet die NFS-Schnittstelle 1 GB Arbeitsspeicher und 1 CPU. Dies kann die Anzahl der anderen Services, die auf dem Snow Family-Gerät ausgeführt werden, oder die Anzahl der EC2-compatible Instances, die ausgeführt werden können, einschränken.

Über die NFS-Schnittstelle übertragene Daten werden während der Übertragung nicht verschlüsselt. Bei der Konfiguration der NFS-Schnittstelle können Sie CIDR-Blöcke bereitstellen und das Snow Family-Gerät schränkt den Zugriff auf die NFS-Schnittstelle von Client-Computern mit Adressen in diesen Blöcken ein.

Dateien auf dem Gerät werden an Amazon S3 übertragen, wenn es an zurückgegeben wird AWS. Weitere Informationen finden Sie unter Importieren von Aufträgen in Amazon S3

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.

- Dateinamen sind Objektschlüssel in Ihrem lokalen S3-Bucket auf dem Snow Family-Gerät. Der Schlüsselname ist eine Folge von Unicode-Zeichen, deren UTF-8-Kodierung maximal 1 024 Byte lang ist. Wir empfehlen, nach Möglichkeit NFSv4.1 zu verwenden und Dateinamen mit Unicode UTF-8 zu codieren, um einen erfolgreichen Datenimport zu gewährleisten. Dateinamen, die nicht mit UTF-8 kodiert sind, werden möglicherweise nicht in S3 oder mit einem anderen Dateinamen in S3 hochgeladen, je nachdem, welche NFS-Kodierung Sie verwenden.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Snow Family-Geräte unterstützen keine Dateipfade, die größer als 1024 Zeichen sind. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateiimport.
- Weitere Informationen finden Sie unter Objektschlüssel im Benutzerhandbuch für Amazon Simple Storage Service.
- Bei NFS-basierten Übertragungen werden Ihren Objekten standardmäßige Metadaten im POSIX-Stil hinzugefügt, wenn sie von Snow Family-Geräten in Amazon S3 importiert werden. Darüber

hinaus werden Metadaten „x-amz-meta-user-agent aws-datasync“ angezeigt, da wir derzeit als Teil des internen Importmechanismus für den Geräteimport in Amazon S3 für Snow Family mit der Option NFS verwenden AWS DataSync .

- Sie können bis zu 40M Dateien mit einem einzigen Snowball Edge-Gerät übertragen. Wenn Sie mehr als 40M Dateien in einem einzigen Auftrag übertragen müssen, bündeln Sie die Dateien, um die Dateinummern pro Übertragung zu reduzieren. Einzelne Dateien können von jeder Größe mit einer maximalen Dateigröße von 5 TB für Snowball Edge-Geräte mit der erweiterten NFS-Schnittstelle oder der S3-Schnittstelle sein.

Sie können die NFS-Schnittstelle auch mit dem Snowball Edge-Client konfigurieren und verwalten, einem Befehlszeilenschnittstellen-Tool (Command Line Interface, CLI). Weitere Informationen finden Sie unter Verwalten der NFS-Schnittstelle.

Themen

Starten des NFS-Service auf einem Windows-Betriebssystem

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

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.

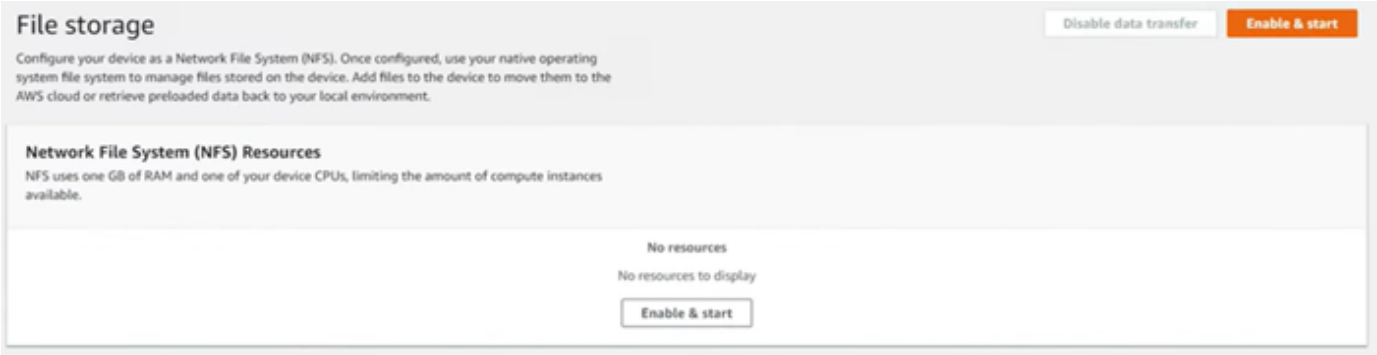
> **Note**
>
> Um Windows-Funktionen einzuschalten, müssen Sie möglicherweise einen Administratorbenutzernamen und ein Passwort für Ihren Computer angeben.

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

Automatisches Konfigurieren der NFS-Schnittstelle

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt, daher müssen Sie sie starten, um die Datenübertragung auf dem Gerät zu aktivieren. Mit wenigen Klicks kann Ihr Snow Family-Gerät 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.

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



2. Wenn der NFS-Service gestartet wird, wird die IP-Adresse der NFS-Schnittstelle auf dem Dashboard angezeigt und im Abschnitt Daten übertragen wird angezeigt, dass der Service aktiv ist.
3. Wählen Sie Im Explorer öffnen (bei Verwendung eines Windows- oder Linux-Betriebssystems), um die Dateifreigabe im Dateibrowser Ihres Betriebssystems zu öffnen und mit der Übertragung von Dateien auf das Snow Family-Gerät zu beginnen. Sie können Dateien von Ihrem Client-Computer in die Dateifreigabe kopieren und einfügen oder per Drag-and-Drop ablegen. Im Windows-Betriebssystem sieht Ihre Dateifreigabe wie folgt aus`buckets(\\12.123.45.679)(Z:)`.

> **Note**
>
> In Linux-Betriebssystemen erfordert das Mounten von NFS-Endpunkten Root-Berechtigungen.

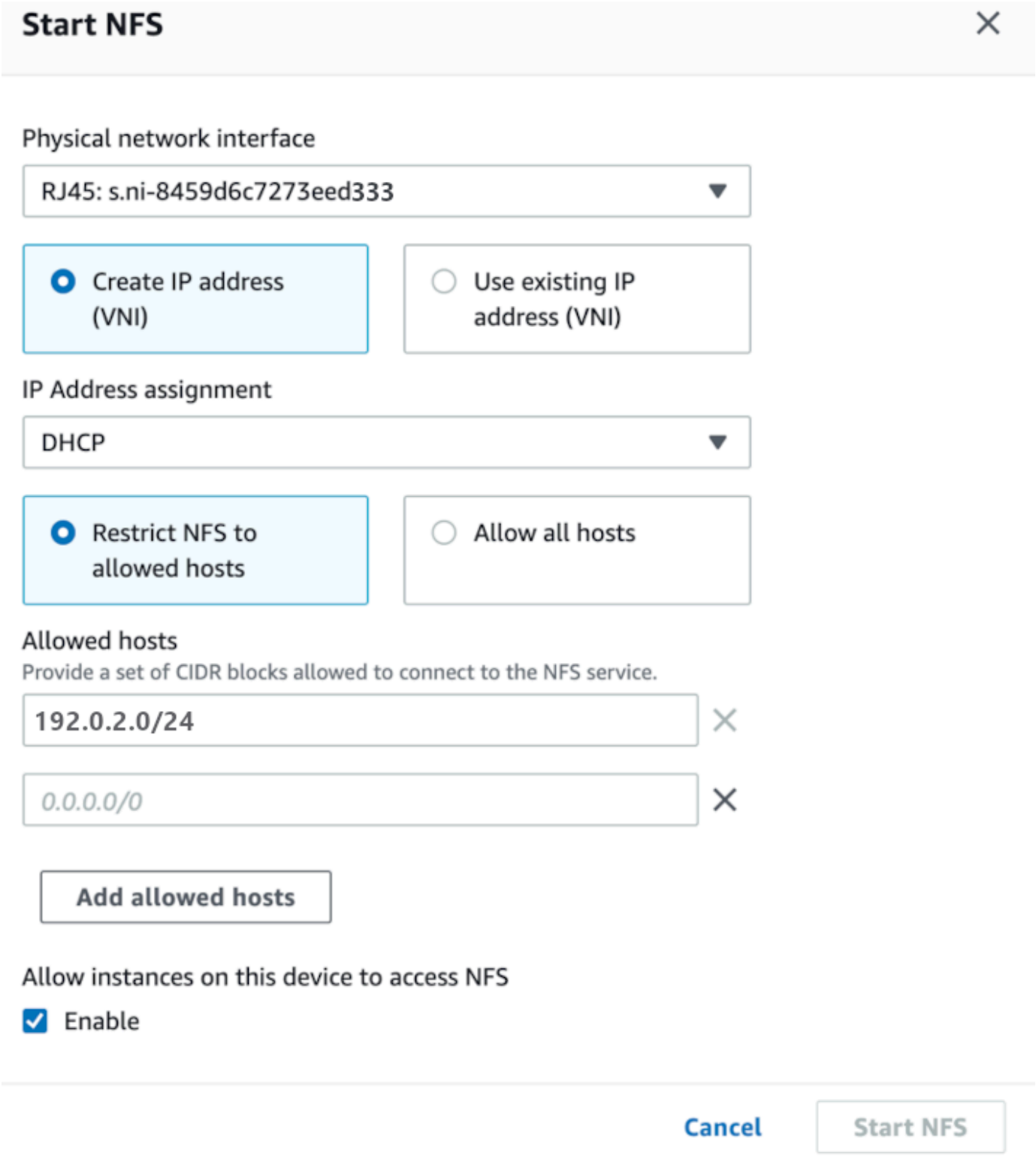
Manuelles Konfigurieren der NFS-Schnittstelle

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt, daher müssen Sie sie starten, um die Datenübertragung auf dem Gerät zu aktivieren. Sie können die NFS-Schnittstelle manuell konfigurieren, indem Sie die IP-Adresse einer Virtual Network Interface (VNI) angeben, die auf dem Snow Family-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 Snow Family-Gerät ein. Weitere Informationen finden Sie unter Netzwerkkonfiguration für Datenverarbeitungs-Instances.

Sie können das Snow Family-Gerät auch die NFS-Schnittstelle automatisch konfigurieren lassen. Weitere Informationen finden Sie unter Automatisches Konfigurieren der NFS-Schnittstelle.

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 Physische Netzwerkschnittstelle wird ausgefüllt.



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

4. Wenn Sie IP-Adresse erstellen (VNI) auswählen, wählen Sie DHCP oder Statische IP im Listenfeld IP-Adresszuweisung aus.

   > **Important**
   >
   > Wenn Sie ein DHCP-Netzwerk verwenden, ist es möglich, dass die IP-Adresse der NFS-Schnittstelle vom DCHP-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 übernehmen. In diesem Fall hat der neue Client Zugriff auf die Freigabe. Um dies zu verhindern, verwenden Sie DHCP-Reservierungen oder statische IP-Adressen.

   Wenn Sie Vorhandene IP-Adresse verwenden auswählen, 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 Geräten im Netzwerk den Zugriff auf die NFS-Schnittstelle auf dem Snow Family-Gerät erlauben.

   - Um den Zugriff auf die NFS-Schnittstelle auf dem Snow Family-Gerät einzuschränken, wählen Sie NFS auf zulässige Hosts beschränken aus. Geben Sie unter 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 einen Satz von Blöcken zu entfernen, wählen Sie X neben dem Feld, das die Blöcke enthält. Wählen Sie Zulässige Hosts hinzufügen aus.

     > **Note**
     >
     > Wenn Sie NFS auf zulässige Hosts beschränken wählen und keine zulässigen CIDR-Blöcke bereitstellen, lehnt das Snow Family-Gerät alle Anforderungen zum Mounten der NFS-Schnittstelle ab.

   - Um jedem Gerät im Netzwerk den Zugriff auf die NFS-Schnittstelle zu erlauben, wählen Sie Alle Hosts zulassen aus.

6. Um EC2-compatible Instances, die auf dem Snow Family-Gerät ausgeführt werden, den Zugriff auf den NFS-Adapter zu ermöglichen, wählen Sie Aktivieren aus.

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

   > **Important**
   >
   > Schalten Sie das Snow Family-Gerät nicht aus, während die NFS-Schnittstelle gestartet wird.

   Im Abschnitt Network File System (NFS) Resources wird der Status der NFS-Schnittstelle als Aktiv angezeigt. Sie benötigen die aufgelistete IP-Adresse, um die Schnittstelle als lokalen Speicher auf Client-Computern zu mounten.

Verwalten von NFS-Endpunkten auf dem Snow Family-Gerät

Jeder S3-Bucket auf dem Snow Family-Gerät wird als Endpunkt dargestellt und unter Mount-Pfade 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, heben Sie zuerst das Mounting des aktuellen Endpunkts auf.

So mounten Sie einen Endpunkt

1. Führen Sie im Abschnitt Mount-Pfade einen der folgenden Schritte aus, um einen Endpunkt auszuwählen:

   - Geben Sie im Feld Endpunkte filtern einen Bucket-Namen ganz oder teilweise ein, um die Liste der verfügbaren Endpunkte in Ihrem Eintrag zu filtern, und wählen Sie dann den Endpunkt aus.
   - Wählen Sie in der Liste Mount-Pfade den zu mountenden Endpunkt aus.

2. Wählen Sie NFS-Endpunkt mounten aus. Das Snow Family-Gerät mountet den Endpunkt zur Verwendung.

So heben Sie das Mounting eines Endpunkts auf

1. Wählen Sie im Abschnitt Mountingpfade den Endpunkt aus, dessen Mounting aufgehoben werden soll.

2. Wählen Sie Unmount-Endpunkt aus. Das Snow Family-Gerät löst das Mounting des Endpunkts auf und es ist nicht mehr zur Verwendung verfügbar.

> **Note**
>
> Bevor Sie das Mounting eines Endpunkts aufheben, stellen Sie sicher, dass keine Daten von oder auf ihn kopiert werden.

Mounten von NFS-Endpunkten auf Client-Computern

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

1. Wählen Sie unter Mount-Pfade das Kopiersymbol des zu mountenden Endpunkts aus. Fügen Sie es beim Mounten des Endpunkts in Ihr Betriebssystem ein.
2. Im Folgenden sind die Standard-Mounting-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
   ```

Anhalten der NFS-Schnittstelle

Halten Sie die NFS-Schnittstelle auf dem Snow Family-Gerät an, wenn Sie mit der Übertragung von Dateien zu oder von diesem 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). In der Regel dauert es bis zu 2 Minuten, bis die NFS-Endpunkte aus dem Dashboard verschwinden.

Verwaltung Ihrer Geräte

Sie verwenden die AWS OpsHub , um Ihre Snow Family-Geräte zu verwalten. Auf der Seite Gerätedetails können Sie dieselben Aufgaben ausführen wie mit der AWS CLI, einschließlich des Änderns des Alias Ihres Geräts, des Neustarts des Geräts und der Überprüfung auf Updates.

Themen

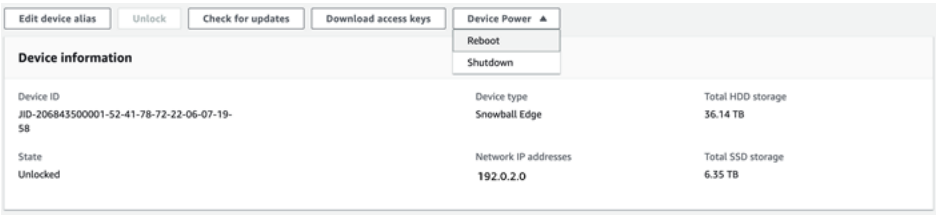
Neustarten Ihres Geräts

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

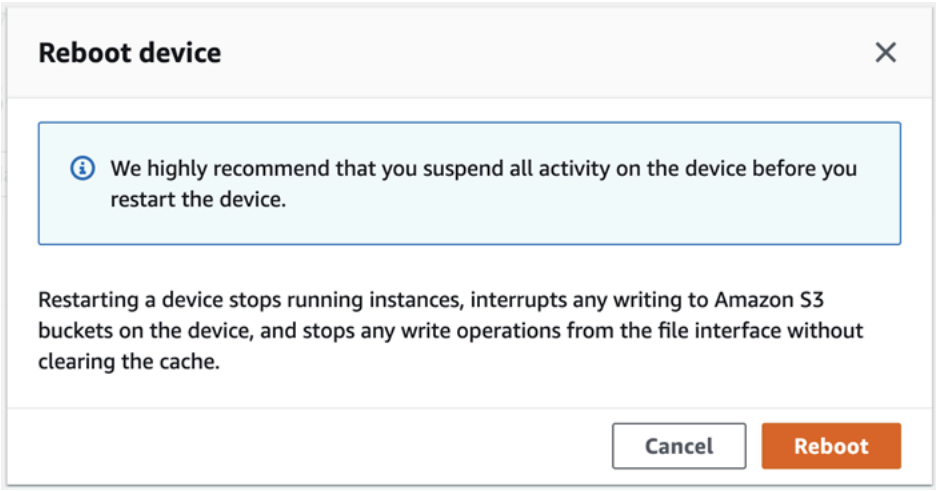
> **Important**
>
> Es wird nachdrücklich empfohlen, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät neu starten. Beim Neustart eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen.

So starten Sie ein Gerät neu

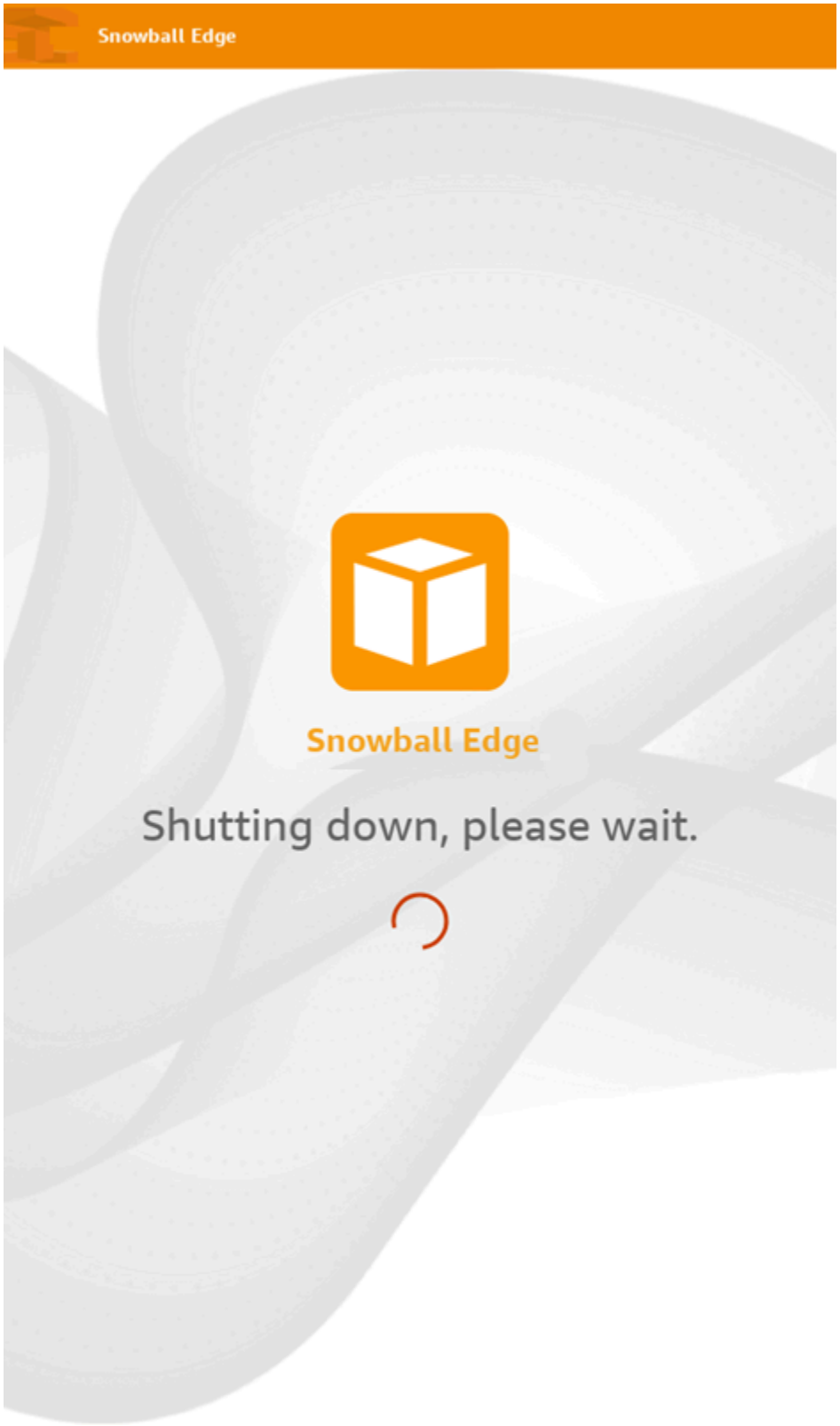
1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . Wählen Sie anschließend das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie das Menü Geräteleistung und dann Neustart aus. Ein Dialogfeld wird angezeigt.



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



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


Snowball Edge
Snowball Edge
Shutting down, please wait.

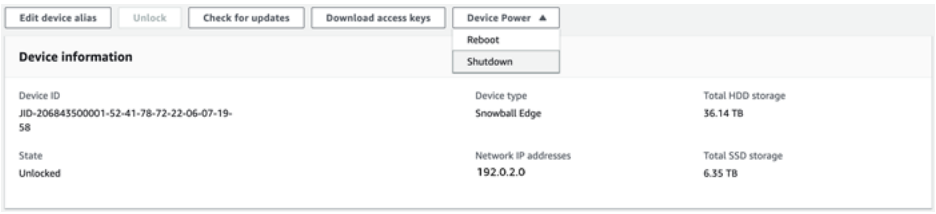
Herunterfahren Ihres Geräts

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

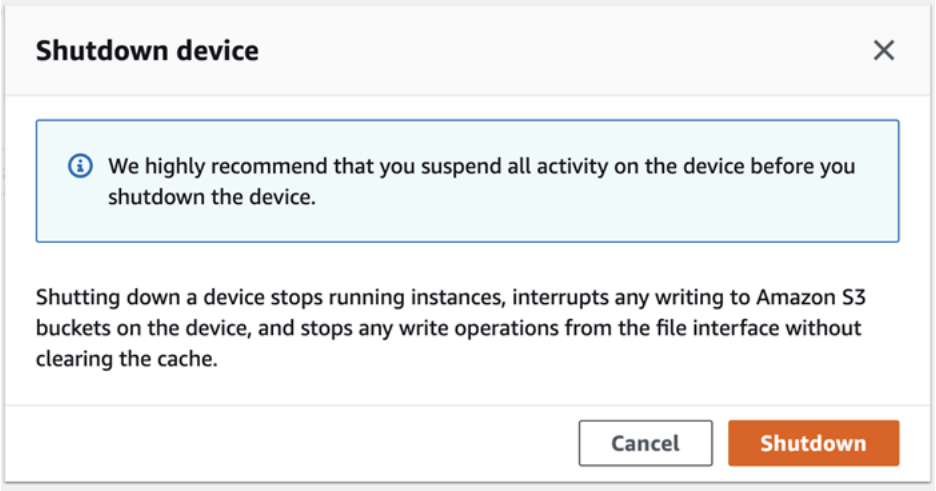
> **Important**
>
> Wir empfehlen dringend, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät herunterfahren. Beim Herunterfahren eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen.

So fahren Sie ein Gerät herunter

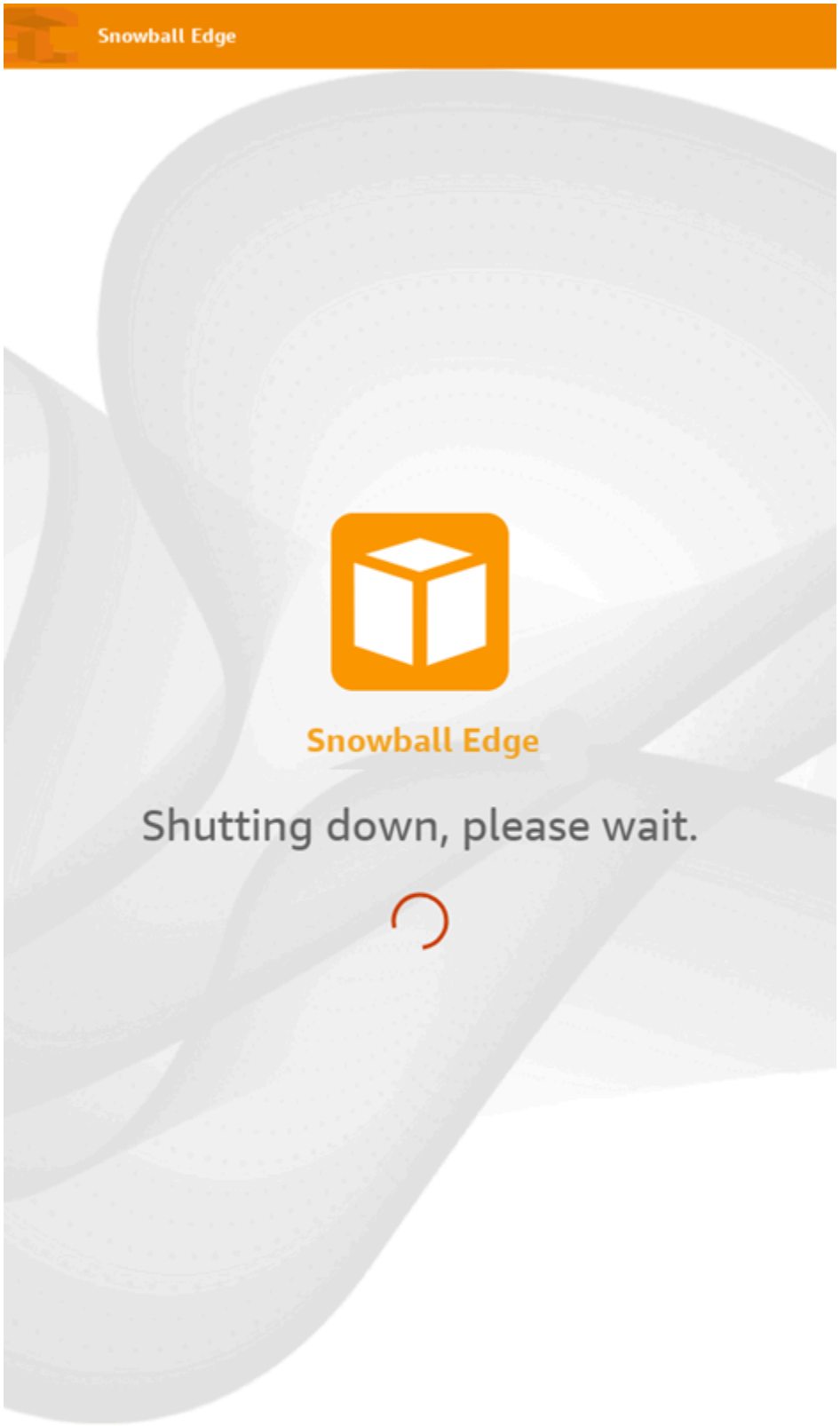
1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . Wählen Sie anschließend das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie das Menü Device Power und dann Shutdown aus. Ein Dialogfeld wird angezeigt.



3. Wählen Sie im Dialogfeld Shutdown aus. Ihr Gerät wird heruntergefahren.



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

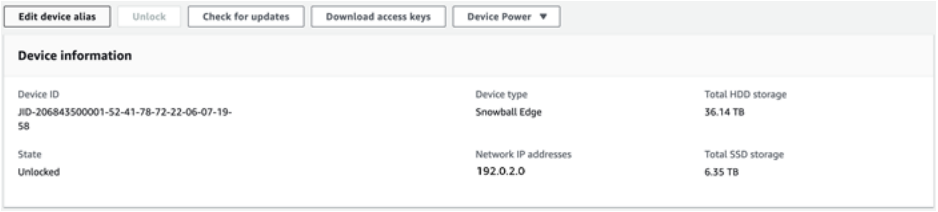

Snowball Edge
Snowball Edge
Shutting down, please wait.

Bearbeitung des Gerätealias

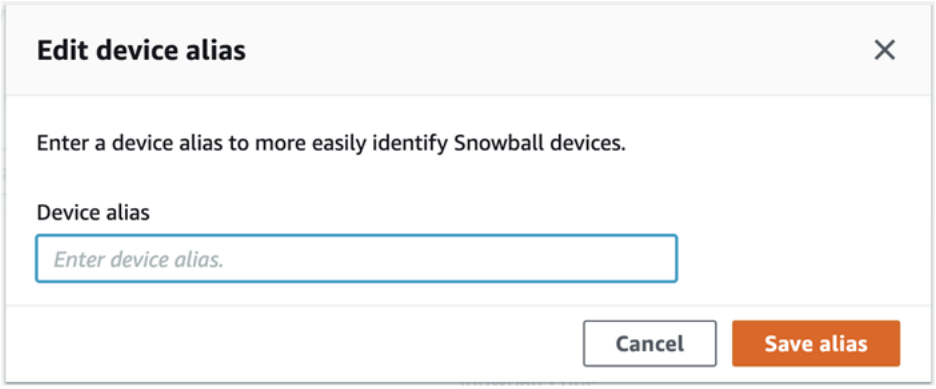
Gehen Sie wie folgt vor, um Ihren Gerätealias mit zu bearbeiten AWS OpsHub.

So bearbeiten Sie den Alias Ihres Geräts

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . 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.



Verwalten von Zertifikaten für öffentliche Schlüssel mit OpsHub

Sie können über das HTTPS-Protokoll sicher mit AWS Services interagieren, die auf einem Snowball-Edge-Gerät oder einem Cluster von Snowball-Edge-Geräten ausgeführt werden, indem Sie ein öffentliches Schlüsselzertifikat bereitstellen. Sie können das HTTPS-Protokoll verwenden, um mit -AWS Services wie IAM, Amazon EC2, S3-Adapter, Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten, Amazon EC2 Systems Manager und AWS STS auf Snowball-Edge-Geräten zu interagieren. Im Falle eines Geräte-Clusters ist ein einzelnes Zertifikat erforderlich und kann von jedem Gerät im Cluster generiert werden. Sobald ein Snowball Edge-Gerät das Zertifikat generiert und Sie das Gerät entsperren, können Sie Snowball Edge-Client-Befehle 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 der Cluster wird zum ersten Mal entsperrt.
- Das Snowball Edge-Gerät oder der Cluster wird nach dem Löschen des Zertifikats entsperrt (mit dem `delete-certificate` Befehl oder Zertifikat erneuern in AWS OpsHub).
- Das Snowball Edge-Gerät oder der Cluster wird nach Ablauf des Zertifikats neu gestartet und entsperrt.

Jedes Mal, wenn ein neues Zertifikat generiert wird, ist das alte Zertifikat nicht mehr gültig. Ein Zertifikat ist für einen Zeitraum von einem Jahr ab dem Tag gültig, an dem es generiert wurde.

Sie können den Snowball Edge-Client auch verwenden, um Zertifikate für öffentliche Schlüssel zu verwalten. Weitere Informationen finden Sie unter Verwalten von Zertifikaten für öffentliche Schlüssel.

Themen

Herunterladen des öffentlichen Schlüsselzertifikats mit OpsHub

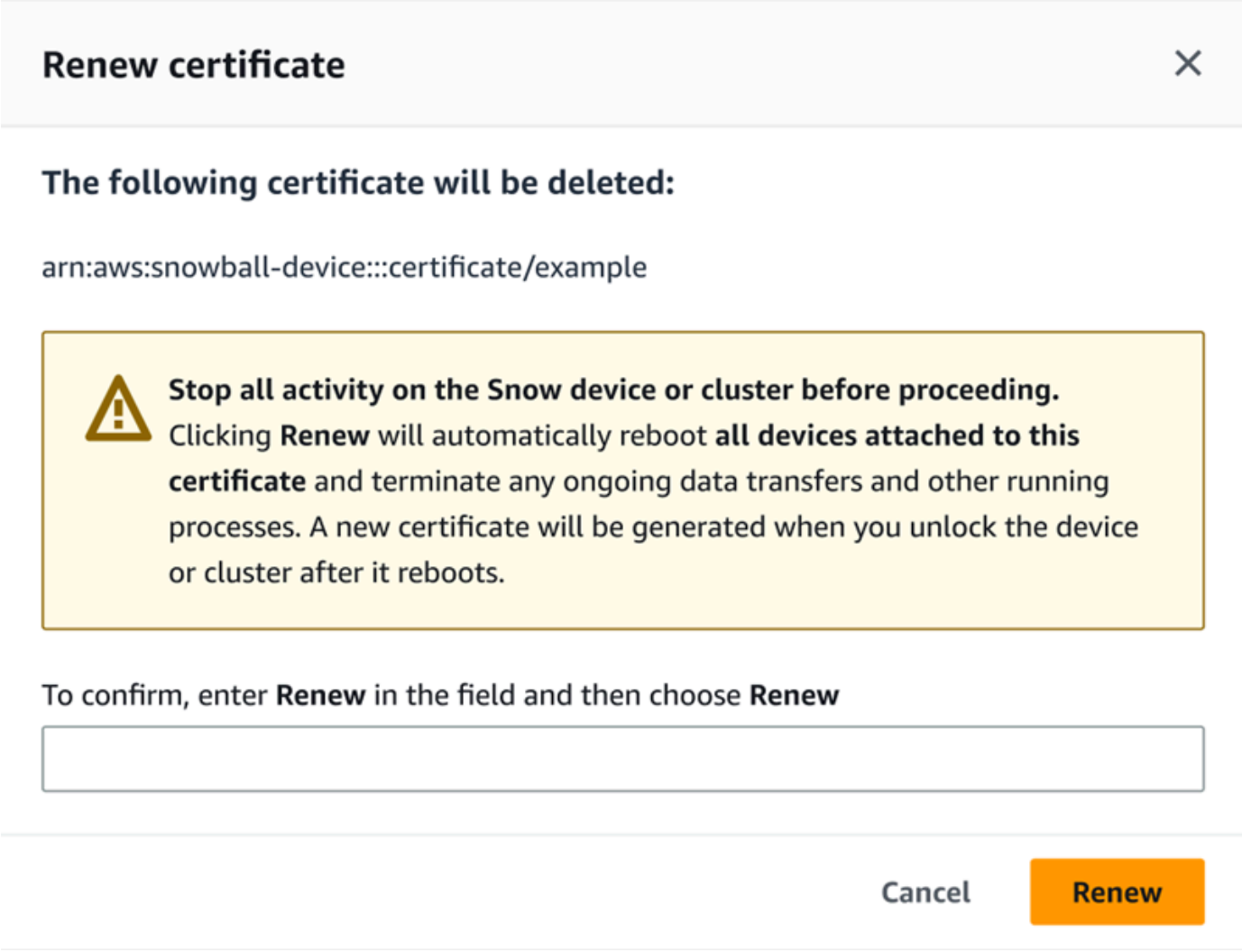
Sie können das aktive öffentliche Schlüsselzertifikat auf Ihren Computer herunterladen.

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . 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 aus.
3. Es wird ein Fenster angezeigt, in dem Sie die herunterzuladende Zertifikatsdatei benennen und den Speicherort auf Ihrem Computer auswählen können, an den sie heruntergeladen werden soll. Wählen Sie Speichern.

Erneuern des öffentlichen Schlüsselzertifikats mit OpsHub

Bevor Sie das öffentliche Schlüsselzertifikat erneuern, beenden Sie alle Datenübertragungen zum oder vom Snow Family-Gerät und beenden Sie alle EC2-compatible , die ausgeführt werden. Weitere Informationen finden Sie unter Anhalten einer AmazonEC2-compatible Instance in diesem Handbuch.

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . 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 Zertifikat erneuern aus.
3. Geben Sie im Fenster Zertifikat verlängern **`Renew`** in das Feld ein und wählen Sie Erneuern aus. Das Snow Family-Gerät löscht das vorhandene öffentliche Schlüsselzertifikat und startet das Gerät oder den Cluster neu.



Abrufen von Updates für Ihr Gerät und die AWS OpsHub Anwendung

Sie können nach Updates für Ihr Gerät suchen und diese installieren. Sie können auch so konfigurieren AWS OpsHub , dass die Anwendung automatisch auf die neueste Version aktualisiert wird.

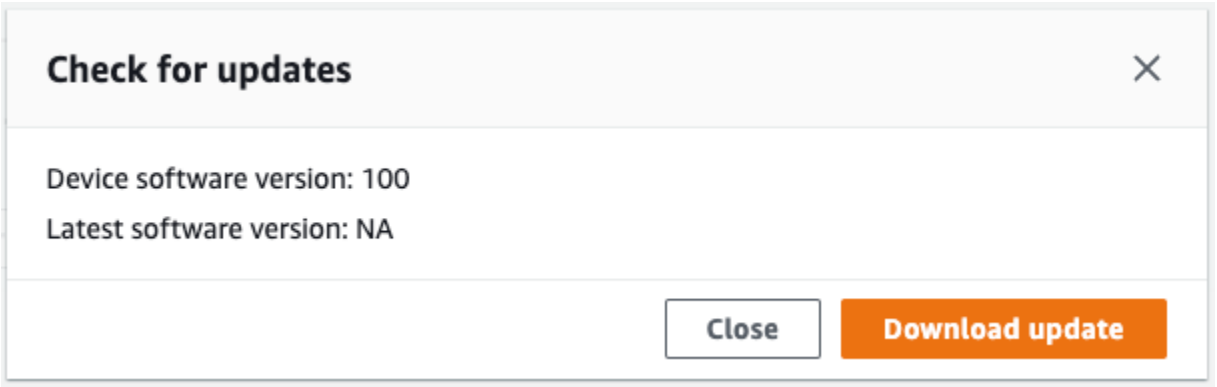
Aktualisieren Ihres Geräts

Gehen Sie wie folgt vor, um Ihr Snow-Gerät AWS OpsHub mit zu aktualisieren.

So aktualisieren Sie Ihr Gerät

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . 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.



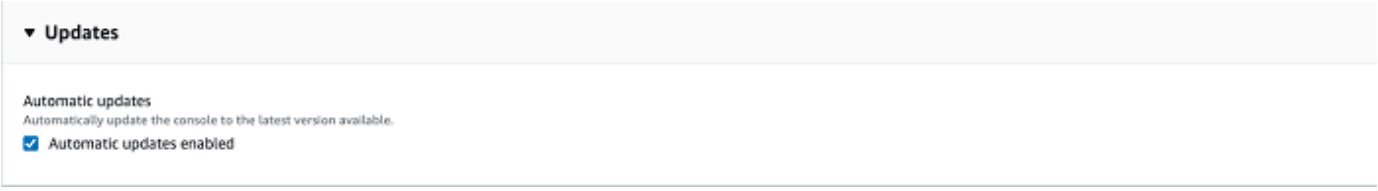
3. Wenn ein Update vorliegt, wählen Sie Update herunterladen aus. Wählen Sie andernfalls Close aus.

Aktualisieren Ihrer AWS OpsHub Anwendung

AWS OpsHub aktualisiert die Anwendung automatisch auf die neueste Version. Gehen Sie wie folgt vor, um zu überprüfen, ob die automatische Aktualisierung aktiviert ist.

So überprüfen Sie, ob automatische Updates für aktiviert sind AWS OpsHub

1. Wählen Sie im AWS OpsHub Dashboard Einstellungen aus.
2. Öffnen Sie die Registerkarte Updates.
3. Überprüfen Sie, ob Automatische Updates aktiviert ausgewählt ist. Die automatische Aktualisierung ist standardmäßig aktiviert.



Wenn Automatische Updates nicht aktiviert ist, erhalten Sie nicht die neueste Version der AWS OpsHub Anwendung.

Verwalten von Profilen

Sie können ein Profil für die persistente Speicherung Ihrer Anmeldeinformationen auf Ihrem lokalen Dateisystem erstellen. Mit haben Sie die Möglichkeit AWS OpsHub, jedes Mal ein neues Profil zu erstellen, wenn Sie das Gerät mit der Geräte-IP-Adresse, dem Entsperrcode und der Manifestdatei entsperren.

Sie können den Snowball Edge Client auch verwenden, um jederzeit ein Profil zu erstellen. Weitere Informationen finden Sie unter Konfigurieren eines Profils für den Snowball Edge Client.

Um Profile zu bearbeiten oder zu löschen, bearbeiten Sie die Profildatei in einem Texteditor.

Example **`snowball-edge.config`**-Beispieldatei

Dieses Beispiel zeigt eine Profildatei mit drei Profilen – `SnowDevice1profileSnowDevice2profile`, 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":[]
    }
}
```

So erstellen Sie ein Profil

1. Entsperren Sie Ihr Gerät lokal und melden Sie sich gemäß den Anweisungen unter anEntsperren eines Geräts.
2. Benennen Sie das Profil und wählen Sie Save profile name (Profilname speichern) aus.

So bearbeiten Sie ein Profil

1. Öffnen Sie in einem Texteditor `snowball-edge.config` von `home directory\.aws \snowball\config`.
2. Bearbeiten Sie die Datei nach Bedarf. Um beispielsweise die IP-Adresse eines Geräts im Profil zu ändern, 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`.
2. Löschen Sie die Zeile, die den Profilnamen, die geschweiften Klammern`{}`, die dem Profilnamen folgen, und den Inhalt innerhalb dieser Klammern enthält.
3. Speichern und schließen Sie die Datei.

Automatisierung von Verwaltungsaufgaben

Sie können verwenden AWS OpsHub , um Betriebsaufgaben zu automatisieren, die Sie häufig auf Ihren Snow Family-Geräten ausführen. Sie können eine Aufgabe für wiederkehrende Aktionen erstellen, die Sie möglicherweise auf -Ressourcen ausführen möchten, z. B. den Neustart virtueller Server, das Anhalten von AmazonEC2-compatible Instances usw. Sie stellen ein Automatisierungsdokument bereit, das sicher operative Aufgaben ausführt und den Vorgang auf AWS Ressourcen in großen Mengen 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-Service gestartet werden. Informationen zum Starten eines Services auf Ihrem Snowball Edge finden Sie unter Starten eines Services auf Ihrem Snowball Edge.

Themen

Erstellung und Start einer Aufgabe

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 beispielsweise **`/AWS::EC2::Instance`** angeben, dass die Aufgaben auf einer Amazon EC2-compatible Instance oder auf allen Ressourcentypen ausgeführt werden **`/`** sollen.
5. Wählen Sie im Abschnitt Inhalt die Option YAML oder JSON aus 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.
6. Wählen Sie Erstellen. 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

Im folgenden Beispiel wird eine Amazon EC2-compatible 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

            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}"
    }
  } ]
}
```

Anzeige von Details für eine Aufgabe

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

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.

Festlegen der NTP-Zeitserver für Ihr Gerät

Gehen Sie wie folgt vor, um anzuzeigen und zu aktualisieren, mit welchen Zeitservern Ihr Gerät die Zeit synchronisieren muss.

So überprüfen Sie Zeitquellen

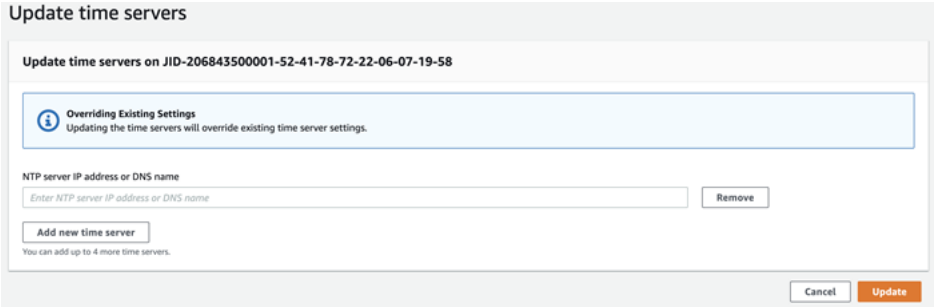
1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. In der Tabelle „Zeitquellen“ wird eine Liste der Zeitquellen angezeigt, mit denen Ihr Gerät Zeit synchronisiert.

   Die Tabelle „Zeitquellen“ hat 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 Status:
     - AKTUELL: Die Zeitquelle wird derzeit zum Synchronisieren der Zeit verwendet
     - COMBINED : Die Zeitquelle wird mit der aktuellen Quelle kombiniert
     - AUSGESCHLAGEN: Die Zeitquelle wird durch den Kombinationsalgorithmus ausgeschlossen
     - LOST: Die Verbindung mit der Zeitquelle wurde unterbrochen
     - NICHT VERFÜGBARKEIT: Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder als falseticker angesehen hat oder zu viel Variabilität aufweist
   - Typ : Network Time Protocol (NTP)-Quellen können ein Server oder ein Peer sein. Ein Server kann vom Benutzer mit dem update-time-server Befehl eingerichtet werden, während ein Peer nur mit anderen Snowball Edge-Geräten im Cluster eingerichtet werden kann und automatisch eingerichtet wird, wenn der Cluster zugeordnet ist.
   - Bolum : Die Stratum der Quelle. Bolum 1 gibt eine Quelle mit einer lokal angefügten Referenzuhr an. Eine Quelle, die mit einerum-1-Quelle synchronisiert ist, wird aufum 2 festgelegt. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert wird, wird aufum 3 usw. festgelegt.

So aktualisieren Sie die Zeitserver

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . 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 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 an, mit denen Ihr Gerät die Zeit synchronisieren soll, und wählen Sie Aktualisieren aus.



Unterstützte NTP-Gerätetypen und Softwareversionen

NTP ist auf Speicher- und Datenverarbeitungsgerätetypen der Version 2 nicht verfügbar. Speicher- und Datenverarbeitungsgerätetypen der Snowball Edge Version 3 mit Softwareversion 77 oder höher unterstützen jedoch NTP. Um zu überprüfen, ob NTP aktiviert ist, verwenden Sie den Snowball Edge CLI-Befehl `describe-time-sources`.

Verwenden eines AWS Snowball Edge-Geräts

Im Folgenden finden Sie eine Übersicht über das AWS Snowball Edge Gerät. Snowball Edge ist ein physisches Gerät, das durch AWS Key Management Service (AWS KMS) geschützt ist und das Sie für die lokale Speicherung und Datenverarbeitung oder für die Übertragung von Daten zwischen Ihren On-Premises-Servern und Amazon Simple Storage Service (Amazon S3) verwenden.

Informationen zum Entsperren eines - AWS Snowball Edge Geräts finden Sie unter Verwenden des Snowball Edge Clients.

Nachdem Sie das Gerät erhalten haben, sollten Sie nach Beschädigungen und offensichtlichen Manipulationen suchen.

> **Warning**
>
> Wenn Ihnen am Gerät irgendetwas Verdächtiges auffällt, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie sich stattdessen an AWS Support, und eine neue wird Ihnen zugestellt.

Die folgende Abbildung zeigt, wie das AWS Snowball Edge Gerät aussieht.

Das Gerät verfügt über drei Kabel – eine Front, eine Back und eine Top-, die alle durch -Latten geöffnet werden können. Hinter der Tür an der Oberseite befindet sich das Stromkabel des Geräts. Die anderen beiden Trichter können geöffnet und innerhalb des Geräts verschoben werden, sodass sie nicht im Weg sind, während Sie sie verwenden. Durch Öffnen der Türen erhalten Sie Zugang zum E-Ink-LCD-Display, das in die Vorderseite des Geräts eingelassen ist, sowie auf die Strom- und Netzwerkanschlüsse auf der Rückseite.

Nachdem Ihr Gerät eintrifft und eingeschaltet ist, können Sie es verwenden.

Themen

- Verwendung von AWS Lambda mit AWS Snowball Edge
- Verwenden von Amazon EC2-compatibleInstances
- Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten
- Verwenden von Amazon EKS Anywhere in AWS Snow
- Lokales Verwenden von IAM
- Verwenden von AWS Security Token Service
- Verwaltung von Public-Key-Zertifikaten
- Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports

Verwenden des Snowball Edge Clients

Im Folgenden finden Sie Informationen zum Abrufen und Verwenden des Snowball Edge-Clients mit Ihrem AWS Snowball Edge Gerät. Der Snowball Edge-Client ist eine eigenständige Terminalanwendung, die Sie auf Ihrem lokalen Server ausführen, um das Gerät zu entsperren und Anmeldeinformationen, Protokolle und Statusinformationen abzurufen. Sie können den Client auch für administrative Aufgaben für ein Cluster verwenden. Während Sie den Snowball Edge-Client verwenden, erhalten Sie zusätzliche Supportinformationen, indem Sie den `snowballEdge help` Befehl ausführen.

Wenn Sie Daten auf das AWS Snowball Edge Gerät lesen und schreiben, verwenden Sie den Amazon S3-Adapter oder die Dateischnittstelle.

Herunterladen und Installieren des Snowball Edge Clients

Sie können den Snowball Edge-Client von AWS Snowball Edge Ressourcen herunterladen und installieren. Auf dieser Seite finden Sie das Installationspaket für Ihr Betriebssystem. Folgen Sie den Anweisungen, um den Snowball Edge-Client zu installieren. Das Ausführen des Snowball Edge-Clients von einem Terminal auf Ihrer Workstation erfordert möglicherweise die Verwendung eines bestimmten Pfads, abhängig von Ihrem Betriebssystem:

- Microsoft Windows – Wenn der Client installiert wurde, können Sie ihn ohne zusätzliche Vorbereitung von jedem Verzeichnis aus ausführen.
- Linux – Der Snowball Edge-Client muss über das `~/snowball-client-linux-`*`build_number`*`/bin/` Verzeichnis ausgeführt werden. Der Snowball Edge-Client wird nur auf 64-Bit-Linux-Distributionen unterstützt.

- macOS – Das `install.sh`Skript kopiert Ordner aus der Snowball Edge-Client-.tar-Datei in das `/usr/local/bin/snowball` Verzeichnis . Wenn Sie dieses Skript ausführen, können Sie den Snowball Edge-Client von jedem Verzeichnis aus ausführen, wenn ein Pfad in Ihrem `/usr/local/bin` ist`bash_profile`. Sie können Ihren Pfad mit dem `echo $PATH` Befehl überprüfen.

Befehle für den Snowball Edge Client

Im Folgenden finden Sie Informationen zu den Snowball Edge-Clientbefehlen, einschließlich Beispielen für die Verwendung und Beispielausgaben.

Themen

- Löschen einer Direct Network Interface
- Überprüfen des Feature-Status
- Einstellen von Zeitservern
- Überprüfen von Zeitquellen

Konfigurieren eines Profils für den Snowball Edge Client

Jedes Mal, wenn Sie einen Befehl für den Snowball Edge-Client ausführen, geben Sie Ihre Manifestdatei, Ihren Entsperrcode und eine IP-Adresse an. Sie können die ersten beiden davon über die Managementkonsole für die AWS Snow-Familie oder die Auftragsverwaltungs-API abrufen. Weitere Informationen zum Abrufen der Manifestdatei und des Entsperrcodes finden Sie unter Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät.

Sie können den `snowballEdge configure`-Befehl verwenden, um den Pfad zur Manifestdatei, den 29-stelligen Entsperrcode und den Endpunkt als Profil zu speichern. Nach der Konfiguration können Sie andere Snowball Edge-Clientbefehle verwenden, ohne diese Werte für einen bestimmten Auftrag manuell eingeben zu müssen. Nachdem Sie den Snowball Edge-Client konfiguriert haben, werden die Informationen in einem Klartext-JSON-Format in gespeichert*`home directory`*`/.aws/snowball/config/snowball-edge.config`.

Der Endpunkt ist die IP-Adresse, zu der `https://` hinzugefügt wird. Sie finden die IP-Adresse für das AWS Snowball Edge Gerät auf der AWS Snowball Edge Device-Anzeige. Wenn das AWS Snowball Edge Gerät zum ersten Mal mit Ihrem Netzwerk verbunden ist, erhält es automatisch eine DHCP-IP-Adresse, sofern ein DHCP-Server verfügbar ist. Wenn Sie eine andere IP-Adresse verwenden möchten, können Sie diese auf dem LCD-Display ändern. Weitere Informationen finden Sie unter Verwenden eines AWS Snowball Edge-Geräts.

> **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.

Usage

Diesen Befehl können Sie auf zwei Arten verwenden: inline oder bei Aufforderung. In diesem Anwendungsbeispiel wird die Aufforderungsmethode gezeigt.

```
snowballEdge configure
```

Example Output

```
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
```

Sie können mehrere Profile einrichten, wenn Sie mehrere Aufträge gleichzeitig verwalten oder einen Cluster von verschiedenen Endpunkten aus verwalten möchten. Weitere Informationen zu mehreren AWS CLI Profilen finden Sie unter Benannte Profile im AWS Command Line Interface - Benutzerhandbuch.

Anfordern Ihres QR-Codes für die NFC-Validierung

Sie können diesen Befehl verwenden, um einen gerätespezifischen QR-Code für die Verwendung mit der AWS Snowball Edge-Verifizierungsapp zu generieren. Weitere Informationen zur Bol-Validierung finden Sie unter Validieren von NFC-Tags.

Usage

```
snowballEdge get-app-qr-code --output-file ~/downloads/snowball-qr-code.png
```

Example Output

```
QR code is saved to ~/downloads/snowball-qr-code.png
```

Snowball Edge-Clientversion

Verwenden Sie den `version` Befehl , um die Version des Snowball Edge Command Line Interface (CLI)-Clients anzuzeigen.

Verwendung

```
    snowballEdge version
```

Beispielausgabe

```
    Snowball Edge client version: 1.2.0  Build 661
```

Entsperren von Snowball-Edge-Geräten

Um ein eigenständiges AWS Snowball Edge Gerät zu entsperren, führen Sie den `snowballEdge unlock-device` Befehl aus. Zum Entsperren eines Clusters verwenden Sie den `snowballEdge unlock-cluster`-Befehl. Diese Befehle authentifizieren Ihren Zugriff auf das AWS Snowball Edge Gerät.

> **Note**
>
> Um die mit Ihrem Auftrag verknüpften Geräte zu entsperren, müssen sich die Geräte vor Ort befinden, an die Stromversorgung und das Netzwerk angeschlossen und aktiviert sein. Darüber hinaus muss die Bol-Anzeige auf der Front des AWS Snowball Edge Geräts darauf hinweisen, dass das Gerät einsatzbereit ist.

Usage

```
snowballEdge unlock-device --endpoint https://192.0.2.0 --manifest-file Path/to/
manifest/file --unlock-code 01234-abcde-ABCDE-01234
```

Example Eingabe für ein einzelnes Gerät Entsperren

```
snowballEdge unlock-device --endpoint https://192.0.2.0 --manifest-file /usr/home/
manifest.bin --unlock-code 01234-abcde-ABCDE-01234
```

Example Ausgabe für ein einzelnes Gerät entsperren

```
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.
```

Cluster-Nutzung

Wenn Sie einen Cluster entsperren, geben Sie den Endpunkt für einen der Knoten und alle IP-Adressen der anderen Geräte in Ihrem Cluster an.

```
snowballEdge unlock-cluster --endpoint https://192.0.2.0 --manifest-file Path/to/
manifest/file --unlock-code 01234-abcde-ABCDE-01234 --device-ip-addresses 192.0.2.0
 192.0.2.1 192.0.2.2 192.0.2.3 192.0.2.4
```

Example Ausgabe für Cluster entsperren

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

Aktualisieren eines Snowball Edge

Verwenden Sie die folgenden Befehle, um Updates für Ihr Snowball Edge-Gerät herunterzuladen und zu installieren. Prozeduren, die diese Befehle verwenden, finden Sie unter Aktualisieren von Software auf Snowball-Edge-Geräten.

`snowballEdge check-for-updates` – Gibt Versionsinformationen über die in der Cloud verfügbare Snowball Edge-Software und die aktuelle auf dem Gerät installierte Version zurück.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge check-for-updates
```

Example Output

```
Latest version: 102
Installed version: 101
```

`snowballEdge describe-device-software` – Gibt die aktuelle Softwareversion und das Ablaufdatum des SSL-Zertifikats des Geräts zurück. Wenn ein Softwareupdate heruntergeladen oder installiert wird, wird außerdem der Status angezeigt. Nachstehend werden mögliche Ausgaben aufgelistet:

- NA – Derzeit werden keine Softwareupdates ausgeführt.
- `Downloading` – Neue Software wird heruntergeladen.
- `Installing` – Neue Software wird installiert.

- `Requires Reboot` – Neue Software wurde installiert und das Gerät muss neu gestartet werden.

> **Warning**
>
> Wir empfehlen dringend, dass Sie alle Aktivitäten auf dem Gerät anhalten, bevor Sie das Gerät neu starten. Beim Neustart eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen. Alle diese Prozesse können zu Datenverlust führen.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge describe-device-software
```

Example Output

```
Installed version: 101
Installing version: 102
Install State: Downloading
CertificateExpiry: Thur Jan 01 00:00:00 UTC 1970
```

`snowballEdge download-updates` – Beginnt mit dem Herunterladen der neuesten Softwareupdates für Ihren Snowball Edge.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge download-updates
```

Example Output

```
Download started. Run describe-device-software API for additional information.
```

`snowballEdge install-updates` – Startet die Installation der neuesten Softwareupdates für Ihren Snowball Edge, die bereits heruntergeladen wurden.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge install-updates
```

Example Output

```
Installation started.
```

`snowballEdge reboot-device` – Startet das Gerät neu.

> **Warning**
>
> Wir empfehlen dringend, dass Sie alle Aktivitäten auf dem Gerät anhalten, bevor Sie das Gerät neu starten. Beim Neustart eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen. Alle diese Prozesse können zu Datenverlust führen.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge reboot-device
```

Example Output

```
Rebooting device now.
```

`snowballEdge configure-auto-update-strategies` – Konfiguriert eine automatische Aktualisierungsstrategie.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge configure-auto-update-strategy --auto-check autoCheck [--auto-check-
frequency
autoCheckFreq] --auto-download autoDownload
[--auto-download-frequency autoDownloadFreq]
--auto-install autoInstall
[--auto-install-frequency autoInstallFreq]
--auto-reboot autoReboot [--endpoint
endpoint]
```

Example Output

```
Successfully configured auto update strategy. Run describe-auto-update-strategies for
 additional information.
```

`snowballEdge describe-auto-update-strategies` – Gibt jede aktuell konfigurierte automatische Aktualisierungsstrategie zurück.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge describe-auto-update-strategies
```

Example Output

```
auto-update-strategy {[
auto-check:true,
auto-check-frequency: "0 0 * * FRI", // CRON Expression String, Every Friday at
 midnight
auto-download:true,
auto-download-frequency: "0 0 * * SAT", // CRON Expression String, Every Saturday at
midnight
auto-install:true,
auto-install-frequency: "0 13 * * Sun", // CRON Expression String, Every Saturday at
midnight
auto-reboot: false;
]}
```

Abrufen von Anmeldeinformationen

Mit den `snowballEdge get-secret-access-key` Befehlen `snowballEdge list-access-keys` und können Sie die Anmeldeinformationen des Administratorbenutzers Ihres AWS-Konto auf Snowball Edge abrufen. Sie können diese Anmeldeinformationen verwenden, um AWS Identity and Access Management (IAM-Benutzer) und -Rollen zu erstellen und Ihre Anforderungen zu authentifizieren, wenn Sie die AWS CLI oder mit einem - AWS SDK verwenden. Diese Anmeldeinformationen sind nur einem einzelnen Auftrag für Snowball Edge zugeordnet, und Sie können sie nur auf dem Gerät oder Cluster von Geräten verwenden. Das Gerät oder die Geräte haben keine IAM-Berechtigungen in der AWS Cloud.

> **Note**
>
> Wenn Sie die AWS CLI mit dem Snowball Edge verwenden, müssen Sie diese Anmeldeinformationen beim Konfigurieren der CLI verwenden. Informationen zum Konfigurieren von Anmeldeinformationen für die AWS CLI finden Sie unter Konfigurieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-access-keys
```

Example Output

```
{
  "AccessKeyIds" : [ "AKIAIOSFODNN7EXAMPLE" ]
}
```

Nutzung (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
```

Starten eines Services auf Ihrem Snowball-Edge

Snowball Edge-Geräte unterstützen neben Amazon S3 mehrere -Services. Dazu gehören Rechen-Instances, die Dateischnittstelle und AWS IoT Greengrass. Amazon S3 und Amazon EC2 sind standardmäßig immer aktiviert und können nicht mit dem Snowball Edge-Client gestoppt oder neu gestartet werden. Die Dateischnittstelle und AWS IoT Greengrass können jedoch mit dem `snowballEdge start-service` Befehl gestartet werden. Um die Service-ID für den jeweiligen Service zu erhalten, können Sie den Befehl `snowballEdge 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.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge start-service --service-id service_id --virtual-network-interface-
arns virtual-network-interface-arn
```

Example Output

```
Starting the AWS service on your Snowball Edge. You can determine the status of the AWS
 service using the describe-service command.
```

Stoppen eines Services auf Ihrem Snowball-Edge

Um einen Service zu beenden, der auf Ihrem Snowball Edge ausgeführt wird, können Sie den `snowballEdge stop-service` Befehl verwenden.

Der Amazon S3-Adapter AWS STS, Amazon EC2 und die IAM-Services können nicht gestoppt werden.

> **Warning**
>
> Datenverlust kann auftreten, wenn die Dateischnittstelle angehalten wird, bevor die verbleibenden gepufferten Daten auf das Gerät geschrieben werden. Weitere Informationen zur Verwendung der Dateischnittstelle finden Sie unter Verwalten der NFS-Schnittstelle.

> **Note**
>
> Durch das Anhalten des Amazon S3-kompatiblen Speichers auf dem Snow-Family-Geräteservice wird der Zugriff auf die Daten deaktiviert, die in Ihren S3-Buckets auf dem Gerät oder Cluster gespeichert sind. Der Zugriff wird wiederhergestellt, wenn der Amazon S3-kompatible Speicher auf Snow-Family-Geräten erneut gestartet wird. Für Geräte, die mit Amazon S3-kompatiblem Speicher auf Geräten der Snow Family aktiviert sind, wird empfohlen, den Service zu starten, nachdem das Snowball-Edge-Gerät hochgefahren wurde. Siehe Einrichten von Snowball Edge in diesem Handbuch.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge stop-service --service-id service_id
```

Example Output

```
Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS
 service using the describe-service command.
```

Starten von NFS und Einschränken des Zugriffs

> **Important**
>
> Starten Sie den NFS-Service nicht, wenn Sie Amazon Elastic Block Store (Amazon EBS) verwenden möchten. Wenn NFS zum ersten Mal gestartet wird, wird der gesamte Speicher NFS zugewiesen. Es ist nicht möglich, den NFS-Speicher neu in Amazon EBS zu platzieren, auch wenn der NFS-Service gestoppt ist.

> **Note**
>
> Sie können CIDR-Blöcke für IP-Bereiche bereitstellen, die die vom Gerät verfügbar gemachten NFS-Freigaben mounten dürfen. Beispiel: `10.0.0.0/16` Wenn Sie keine zulässigen CIDR-Blöcke angeben, werden alle Mount-Anforderungen abgelehnt.
> Beachten Sie, dass Daten, die über NFS übertragen werden, während der Übertragung nicht verschlüsselt werden.
> Neben den zulässigen Hosts durch CIDR-Blöcke bietet Snowcone keinen Authentifizierungs- oder Autorisierungsmechanismus für die NFS-Freigaben.

Starten Sie NFS mit dem `snowballEdge start-service` Befehl . Um die Service-ID für den NFS-Service abzurufen, können Sie den `snowballEdge list-services` Befehl 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. Sie können den Zugriff auf Ihre Dateifreigaben und Daten in Ihren Amazon S3-Buckets einschränken und sehen, welche Einschränkungen derzeit gelten. Dazu weisen Sie CIDR-Blöcke für zulässige Hosts zu, die auf Ihre Dateifreigabe und S3-Buckets zugreifen können, wenn Sie den NFS-Service starten.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge start-service --service-id nfs --virtual-network-interface-arns
 arn:aws:snowball-device:::interface/s.ni-12345fgh45678j --service-configuration
 AllowedHosts=ip address-1/32,ip address-2/24
```

Example Beispielausgabe

```
Starting the service on your Snowball Edge. You can determine the status of the service
 using the describe-service command.
```

Beschränken des Zugriffs auf NFS-Anteile, wenn NFS ausgeführt wird

Sie können den Zugriff auf Ihre Dateifreigaben und Daten in Ihren Amazon S3-Buckets einschränken, nachdem Sie NFS gestartet haben. Sie können sehen, welche Einschränkungen derzeit gelten, und jedem Bucket unterschiedliche Zugriffsbeschränkungen zuweisen. Dazu weisen Sie CIDR-Blöcke für Hosts zu, die auf Ihre Dateifreigabe und S3-Buckets zugreifen können, wenn Sie den NFS-Service starten. Nachfolgend finden Sie ein Beispielbefehl.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge start-service \
    --service-id nfs \
    --virtual-network-interface-arns virtual-network-interface-arn --service-
configuration AllowedHosts=ip-address-1/32,ip-address-1/24
```

Verwenden Sie den `describe-service` Befehl , um die aktuellen Einschränkungen anzuzeigen.

```
 snowballEdge describe-service --service-id nfs
```

AWS Snowball Edge Protokolle

Wenn Sie Daten zwischen Ihrem On-Premises-Rechenzentrum und einem Snowball Edge übertragen, werden Protokolle automatisch 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.

  Nutzung (konfigurierter Snowball-Edge-Client)

  ```
  snowballEdge list-logs
  ```

Example Output

```
{
  "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 auf Ihren Server unter einem bestimmten Pfad herunter. -`CUSTOMER`Protokolle werden im -`.zip`Format gespeichert und Sie können diese Art von Protokoll extrahieren, um ihren Inhalt anzuzeigen. -`SUPPORT`Protokolle sind verschlüsselt und können nur von AWS Support Technikern gelesen werden. Sie haben die Möglichkeit, einen Namen und einen Pfad für das Protokoll anzugeben.

  Nutzung (konfigurierter Snowball Edge-Client)

  ```
  snowballEdge get-log --log-arn arn:aws:snowball-device:::log/fileinterface-
  JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709
  ```

  Example Output

  ```
  Logs are being saved to download/path/snowball-edge-logs-1515EXAMPLE88.bin
  ```

- `get-support-logs` – Lädt eine Kopie aller `SUPPORT` Arten von Protokollen von Snowball Edge auf Ihren Service unter einem bestimmten Pfad herunter.

  Nutzung (konfigurierter Snowball Edge-Client)

  Snowball Edge-Client

```
snowballEdge get-support-logs
```

Example Output

```
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.

Abrufen des Gerätestatus

Sie können den Status und den allgemeinen Zustand Ihrer Snowball Edge-Geräte mit den folgenden Snowball Edge-Clientbefehlen ermitteln:

- `describe-device`

  Nutzung (konfigurierter Snowball Edge-Client)

  ```
  snowballEdge describe-device
  ```

  Example Output

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

- `describe-cluster`

  Nutzung (konfigurierter Snowball Edge-Client)

  ```
  snowballEdge describe-cluster
  ```

  Example Output

  ```
  {
    "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5",
    "Devices" : [ {
      "DeviceId" : "JIDEXAMPLE2-bc53-4618-a538-917EXAMPLE94",
      "UnlockStatus" : {
        "State" : "UNLOCKED"
      },
      "ActiveNetworkInterface" : {
        "IpAddress" : "192.0.2.0"
      },
      "ClusterAssociation" : {
        "State" : "ASSOCIATED",
  ```

```
      "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5"
    },
    "NetworkReachability" : {
      "State" : "REACHABLE"
    }
  }, {
    "DeviceId" : "JIDEXAMPLE2-bc53-4618-a538-917EXAMPLE94",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.0.2.1"
    },
    "ClusterAssociation" : {
      "State" : "ASSOCIATED",
      "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5"
    },
    "NetworkReachability" : {
      "State" : "REACHABLE"
    }
  }, {
    "DeviceId" : "JIDEXAMPLE2-bc53-4618-a538-917EXAMPLE94",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.0.2.2"
    },
    "ClusterAssociation" : {
      "State" : "ASSOCIATED",
      "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5"
    },
    "NetworkReachability" : {
      "State" : "REACHABLE"
    }
  }, {
    "DeviceId" : "JIDEXAMPLE2-bc53-4618-a538-917EXAMPLE94",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.0.2.3"
    },
    "ClusterAssociation" : {
```

```
      "State" : "ASSOCIATED",
      "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5"
    },
    "NetworkReachability" : {
      "State" : "REACHABLE"
    }
  }, {
    "DeviceId" : "JIDEXAMPLE2-bc53-4618-a538-917EXAMPLE94",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.0.2.4"
    },
    "ClusterAssociation" : {
      "State" : "ASSOCIATED",
      "ClusterId" : "CIDEXAMPLE7-5402-4c19-9feb-7c9EXAMPLEd5"
    },
    "NetworkReachability" : {
      "State" : "REACHABLE"
    }
  } ]
}
```

Abrufen des Servicestatus

Sie können den Status und den allgemeinen Zustand der Services, die auf Snowball-Edge-Geräten ausgeführt werden, mit dem `describe-service` Befehl ermitteln. Sie können zunächst den `list-services`-Befehl ausführen, um zu sehen, welche Services ausgeführt werden.

- `list-services`

  Nutzung (konfigurierter Snowball Edge-Client)

  ```
  snowballEdge list-services
  ```

  Example Output

  ```
  {
    "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-kompatiblen Speicher auf Snow-Family-Geräten weist dieser Status darauf hin, dass eine oder mehrere Festplatten oder Geräte im Cluster ausgefallen sind. Der Amazon S3-kompatible Speicher auf Snow-Family-Geräten läuft ohne Unterbrechung, aber Sie sollten das betroffene Gerät wiederherstellen oder ersetzen, bevor das Cluster-Quorum verloren geht, um das Risiko eines Datenverlusts zu minimieren. Siehe Clustering-Übersicht in diesem Handbuch.
  - `INACTIVE` – Der Service wird nicht ausgeführt und steht nicht zur Verfügung.

  Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge describe-service --service-id service-id
```

  Example Output

```
{
"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-kompatibler Speicher auf Snow-Family-Geräten – Serviceausgabe

Der `describe-service` Befehl stellt die folgende Ausgabe für den **`s3-snow`** Wert des `service-id` Parameters bereit.

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

Entfernen eines Knotens aus einem Cluster

Der `disassociate-device` Befehl entfernt einen Knoten aus einem Snowball Edge-Cluster. Wenn Sie einen fehlerhaften Knoten ersetzen möchten, verwenden Sie diesen Befehl. Weitere Informationen zu -Clustern finden Sie unter Übersicht über das Custering in diesem Handbuch.

> **Important**
>
> Verwenden Sie den Befehl `disassociate-device` nur, um einen fehlerhaften Knoten zu entfernen. Dieser Befehl gibt möglicherweise einen Fehler zurück, wenn Sie versuchen, einen betriebsbereiten Knoten zu entfernen.

Verwenden Sie diesen Befehl nicht, um einen Knoten zu entfernen, der versehentlich ausgeschaltet wurde oder nicht mehr mit dem Netzwerk verbunden ist und deshalb für den Rest des Clusters vorübergehend nicht zur Verfügung steht. Knoten, die mit diesem Befehl entfernt wurden, können keinem Cluster hinzugefügt werden und müssen an zurückgegeben werden AWS.

Wenn ein Knoten versehentlich ausgeschaltet oder vom Netzwerk getrennt wurde, schließen Sie den Knoten wieder an die Stromversorgung und das Netzwerk an und verwenden Sie den `associate-device` Befehl . Sie können den `disassociate-device`-Befehl nicht verwenden, um einen Knoten zu trennen, der eingeschaltet und betriebsbereit ist.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge disassociate-device --device-id Job ID for the Device
```

Example Output

```
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.
```

Hinzufügen eines Knoten zu einem Cluster

Der `associate-device` Befehl fügt einem Cluster von Snowball Edge-Geräten einen Knoten hinzu. Wenn Sie einen Knoten ausschalten, wird er wieder entsperrt und gesperrt. Um ihn wieder zu entsperren, verwenden Sie den folgenden Befehl. Verwenden Sie diesen Befehl, um einen nicht verfügbaren Knoten durch einen neuen Knoten zu ersetzen, den Sie als Ersatz bestellt haben. Weitere Informationen zu Clustern finden Sie unter Clustering-Übersicht in diesem Handbuch.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge associate-device --device-ip-address IP Address
```

Example Output

```
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-cluster command to determine the state of your cluster.
```

Erstellen von Tags für Ihr Gerät

Fügt die angegebenen Tags auf Ihrem Gerät hinzu oder überschreibt sie. Sie können maximal 50 Tags erstellen. Jedes Tag besteht aus einem Schlüssel-Wert-Paar. Der -Wert ist optional.

> **Note**
>
> Setzen Sie keine sensiblen Daten in Ihre Tags ein.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge create-tags --tag Key=Name,Value=user-test --tag Key=Stage,Value=beta
```

Weitere Informationen erhalten Sie, indem Sie den `describe-tags`-Befehl ausführen.

Example Output

```
Tag(s) [Key=Name,Value=test, Key=Stage,Value=beta] created.
```

Löschen von Tags von Ihrem Gerät

Der `delete-tags` Befehl löscht die angegebenen Tags von Ihrem Snowball Edge-Gerät.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge delete-tags --tag Key=Stage,Value=beta
    Tag(s) [Key=Stage,Value=beta] deleted.
```

Weitere Informationen erhalten Sie, indem Sie den `describe-tags`-Befehl ausführen.

> **Note**
>
> Wenn Sie mehrere Tags gleichzeitig löschen möchten, können Sie mehrere Schlüssel-Wert-Paare angeben, wie etwa die folgenden:
> `delete-tags --tag Key=Name,Value=test --tag Key=Stage,Value=Beta`
> Wenn Sie einen Tag-Schlüssel ohne Tag-Wert angeben, wird jedes Tag mit diesem Schlüssel unabhängig von seinem Wert gelöscht. Wenn Sie einen Tag-Schlüssel mit einer leeren

Zeichenfolge als Tag-Wert angeben, werden nur Tags gelöscht, die eine leere Zeichenfolge als Wert aufweisen.

Beschreiben von Tags auf Ihrem Gerät

Der `describe-tags` Befehl beschreibt die Tags auf Ihrem Snowball Edge-Gerät.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge describe-tags
```

Weitere Informationen erhalten Sie, indem Sie den `describe-tags`-Befehl ausführen.

Example Output

```
{
  "Tags" : [ {
    "Key" : "Name",
    "Value" : "user-test"
  }, {
    "Key" : "Stage",
    "Value" : "beta"
  } ]
}
```

Erstellen einer direkten Netzwerkschnittstelle

- `create-direct-network-interface` – Erstellt eine Direct Network Interface (DNI). Erstellt eine direkte Netzwerkschnittstelle zur Verwendung mit Amazon EC2-compatible Rechen-Instances auf Ihrem Gerät. Sie finden die auf Ihrem Gerät verfügbaren direkten Netzwerkschnittstellen mithilfe des `describe-direct-network-interfaces` Befehls .

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge create-direct-network-interface [--endpoint endpoint] [--instance-
id instanceId] [--mac macAddress]
                                [--manifest-file manifestFile] [--physical-network-
interface-id physicalNetworkInterfaceId]
```

```
                                [--profile profile] [--unlock-code unlockCode] [--
vlan vlanId]
```

Abrufen von Informationen zu einer Direct Network Interface

- `describe-direct-network-interface` – Ruft die direkten Netzwerkschnittstellen auf Ihrem Gerät ab. Eine direkte Netzwerkschnittstelle kann verwendet werden, um Netzwerke für Amazon EC2-compatible Rechen-Instances und -Services auf Ihrem Gerät zu konfigurieren. Sie können eine neue direkte Netzwerkschnittstelle erstellen, indem Sie den `create-direct-network-interface` Befehl verwenden.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge describe-direct-network-interfaces [--endpoint endpoint] [--manifest-
file manifestFile] [--profile profile] [--unlock-code unlockCode]
```

Aktualisieren einer Direct Network Interface

- `update-direct-network-interface` – Aktualisiert eine direkte Netzwerkschnittstelle. Verwenden Sie diesen Befehl, um eine direkte Netzwerkschnittstelle zu aktualisieren, die mit AmazonEC2-compatible Rechen-Instances auf dem Gerät verwendet wird. Sie können die direkten Netzwerkschnittstellen finden, die auf Ihrem Gerät verfügbar sind, indem Sie den Befehl `describe-direct-network`-interfaces verwenden. Wenn Sie eine Netzwerkschnittstelle ändern, die an eine Amazon EC2-compatible Instance angehängt ist, wird die Schnittstelle zuerst getrennt.

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge update-direct-network-interface [--direct-network-interface-
arn directNetworkInterfaceArn] [--endpoint endpoint]
                                [--mac macAddress]
                                [--manifest-file manifestFile] [--profile profile] [--
unlock-code unlockCode]
                                [--vlan vlanId] [--attach-instance-id instanceId | --
detach]
```

Löschen einer Direct Network Interface

- `delete-direct-network-interface` – Löscht eine direkte Netzwerkschnittstelle, die nicht mehr verwendet wird. Um eine direkte Netzwerkschnittstelle zu löschen, die Ihrer Amazon EC2-compatible Rechen-Instance zugeordnet ist, müssen Sie zuerst die Zuordnung der direkten Netzwerkschnittstelle zu Ihrer Instance aufheben.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge delete-direct-network-interface [--direct-network-interface-
arn directNetworkInterfaceArn] [--endpoint endpoint]
                                [--manifest-file manifestFile] [--profile profile] [--
unlock-code unlockCode]
```

Überprüfen des Feature-Status

Verwenden Sie den `describe-features` Befehl , um den Status der auf Ihrem Gerät verfügbaren Funktionen aufzulisten.

`RemoteManagementState` gibt den Status von Snow Device Management an und gibt einen der folgenden Status zurück:

- `INSTALLED_ONLY` – Die Funktion ist installiert, aber nicht aktiviert.
- `INSTALLED_AUTOSTART` – Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu seinem herzustellen, AWS-Region wenn es eingeschaltet ist.
- `NOT_INSTALLED` – Das Gerät unterstützt das Feature nicht oder war bereits vor dem Start im Feld .

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge describe-features \
  --manifest-file manifest.bin path \
  --unlock-code unlock-code \
  --endpoint https://device-local-ip:9091
```

Beispielausgabe

```
{
  "RemoteManagementState" : String
}
```

Einstellen von Zeitservern

Sie können einen externen Network Time Protocol (NTP)-Server einrichten. Sie können die NTP-CLI-Befehle verwenden, wenn sich das Gerät sowohl im gesperrten als auch im entsperrten Zustand befindet. Der Manifest- und Entsperrcode sind erforderlich. Sie können diese entweder mit dem `snowballEdge configure` Befehl oder mit den `--unlock-code` Optionen `--manifest-file` und festlegen. Beachten Sie, dass Sie die `snowballEdge` CLI sowohl auf AWS Snowcone Edge als auch auf verwenden können AWS Snowcone.

Es liegt in Ihrer Verantwortung, einen sicheren NTP-Zeitserver bereitzustellen. Um festzulegen, mit welchen NTP-Zeitservern das Gerät eine Verbindung herstellt, verwenden Sie den `update-time-servers` CLI-Befehl .

> **Note**
>
> Der `update-time-servers` Befehl überschreibt die vorherigen Einstellungen des NTP-Zeitservers.

Unterstützte NTP-Gerätetypen und Softwareversionen

NTP ist auf Speicher- und Datenverarbeitungsgerätetypen der Version 2 nicht verfügbar. Speicher- und Datenverarbeitungsgerätetypen der Snowball Edge Version 3 mit Softwareversion 77 oder höher unterstützen jedoch NTP. Um zu überprüfen, ob NTP aktiviert ist, verwenden Sie den Snowball Edge CLI-Befehl `describe-time-sources`.

Usage

```
snowballEdge update-time-servers time.google.com
```

Example Beispielausgabe

```
Updating time servers now.
```

Überprüfen von Zeitquellen

Verwenden Sie den `describe-time-sources` Snowball Edge CLI-Befehl , um zu sehen, mit welchen NTP-Zeitquellen das Gerät derzeit verbunden ist.

Usage

```
snowballEdge describe-time-sources
```

Example Beispielausgabe

```
{
  "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 Zeitquellenstatus zurück. Jeder Quellstatus 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 Status:
  - `CURRENT` – Die Zeitquelle wird derzeit zum Synchronisieren der Zeit verwendet.
  - `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 falseticker angesehen wurde oder zu viel Variabilität aufweist.
- `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-Geräte im Cluster sein und werden automatisch eingerichtet, wenn der Cluster zugeordnet ist.
- `Stratum` – Dieses Feld zeigt die Stratum der Quelle an. Bolum 1 gibt eine Quelle mit einer lokal angefügten Referenzuhr an. Eine Quelle, die mit einer Stratum-1-Quelle synchronisiert wird, befindet sich in Stratum 2. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert wird, 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 festgelegt werden, während ein Peer nur andere Snowball Edge-Geräte im Cluster sein könnte. In der Beispielausgabe `describe-time-sources` wird auf einem Snowball Edge aufgerufen, der sich in einem Cluster von 5 befindet. Die Ausgabe enthält 4 Peers und 1 Server. Die Peers haben ein -Stratum von 10, während der Server ein -Stratum von 1 hat. Daher wird der Server als aktuelle Zeitquelle ausgewählt.

Übertragen von Dateien mit dem Amazon S3-Adapter für die Datenmigration

Im Folgenden finden Sie eine Übersicht über den Amazon S3-Adapter, mit dem Sie Daten mithilfe von Amazon S3-S3-REST-API-Aktionen programmgesteuert in und aus S3-Buckets übertragen können, die sich bereits auf dem AWS Snowball Edge Gerät befinden. Diese Amazon S3-REST-

API-Unterstützung ist auf eine Teilmenge von Aktionen beschränkt. Sie können diese Teilmenge von Aktionen mit einem der AWS -SDKs verwenden, um Daten programmgesteuert zu übertragen. Sie können auch die Teilmenge der unterstützten AWS Command Line Interface (AWS CLI)-Befehle für Amazon S3 verwenden, um Daten programmgesteuert zu übertragen.

Wenn Ihre Lösung AWS SDK for Java Version 1.11.0 oder neuer verwendet, müssen Sie folgende `S3ClientOptions` verwenden:

- `disableChunkedEncoding()` – Zeigt an, dass die aufgeteilte Kodierung von der Schnittstelle nicht unterstützt wird.
- `setPathStyleAccess(true)` – Konfiguriert die Schnittstelle für die Verwendung des Zugriffs im Pfadformat für alle Anforderungen.

Weitere Informationen finden Sie unter Klasse S3ClientOptions.Builder im Amazon AppStream SDK for Java .

> **Important**
>
> Wir empfehlen, jeweils nur eine Methode zum Lesen und Schreiben von Daten in einen lokalen Bucket auf einem -AWS Snowball EdgeGerät zu verwenden. Die gleichzeitige Verwendung der Dateischnittstelle und des Amazon S3-Adapters auf demselben Bucket kann zu Lese-/Schreibkonflikten führen.
> AWS Snowball Edge-Kontingente beschreibt die Limits.
> Damit AWS Services auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Services zulassen. Details hierzu finden Sie unter Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports.

Themen

- Herunterladen und Installieren der AWS CLI Version 1.16.14 zur Verwendung mit dem Amazon S3-Adapter
- Verwenden der - AWS CLI und -API-Operationen auf Snowball-Edge-Geräten
- Abrufen und Verwenden lokaler Amazon S3-Anmeldeinformationen
- Nicht unterstützte Amazon S3-Funktionen für den Amazon S3-Adapter
- Batching kleiner Dateien
- Unterstützte AWS CLI Befehle

- Unterstützte REST-API-Aktionen

Herunterladen und Installieren der AWS CLI Version 1.16.14 zur Verwendung mit dem Amazon S3-Adapter

Derzeit unterstützen Snowball Edge-Geräte nur Version 1.16.14 und früher von AWS CLI für die Verwendung mit dem Amazon S3-Adapter. Neuere Versionen von AWS CLI sind nicht mit dem Amazon S3-Adapter kompatibel, da sie nicht die gesamte Funktionalität des S3-Adapters unterstützen.

> **Note**
>
> Wenn Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwenden, können Sie die neueste Version von verwendenAWS CLI. Informationen zum Herunterladen und Verwenden der neuesten Version finden Sie im AWS Command Line Interface - Benutzerhandbuch.

Installieren der 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 der AWS CLI unter Windows-Betriebssystemen

Laden Sie die Installationsdatei für Ihr Betriebssystem herunter und führen Sie sie aus:

- 32-Bit
- 64-Bit

Verwenden der - AWS CLI und -API-Operationen auf Snowball-Edge-Geräten

Wenn Sie die - AWS CLI oder -API-Operationen verwenden, um IAM-, Amazon S3- und Amazon EC2-Befehle auf Snowball Edge auszugeben, müssen Sie die Region als „“ angebensnow. Sie können dies mit `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 --profile snowballEdge --endpoint http://192.0.2.0:8080 --region snow
```

Autorisierung mit der Amazon S3-API-Schnittstelle für AWS Snowball

Wenn Sie den Amazon S3-Adapter verwenden, wird jede Interaktion standardmäßig mit dem AWS Algorithmus Signature Version 4 signiert. Diese Autorisierung wird nur verwendet, um die Daten zu überprüfen, die von ihrer 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-Anmeldeinformationen zum Signieren Ihrer Anforderungen an das AWS Snowball Edge Gerät abzurufen, führen Sie die `snowballEdge get-secret-access-keys` Snowball-Edge-Clientbefehle `snowballEdge list-access-keys` und aus. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients. Diese lokalen Amazon S3-Anmeldeinformationen enthalten 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 verwendet, um die Daten zu überprüfen, die von der Quelle zur Schnittstelle übertragen werden. Daher berücksichtigt diese Signierung niemals die Verschlüsselungsschlüssel, die zur Verschlüsselung Ihrer Daten auf dem Snowball verwendet werden.

Abrufen und Verwenden lokaler Amazon S3-Anmeldeinformationen

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-Anmeldeinformationen zum Signieren Ihrer Anforderungen an das Edge-Gerät des Snowball-Edge-Clients abrufen, indem Sie die Informationen des `snowballEdge list-access-keys` und des `snowballEdge get-secret-access-key` Snowball-Edge-Clients ausführen, siehe Abrufen von Anmeldeinformationen. Diese lokalen Amazon S3-Anmeldeinformationen enthalten ein Schlüsselpaar: eine Zugriffsschlüssel-ID und einen geheimen Schlüssel. Diese Anmeldeinformationen sind nur für die Geräte gültig, die Ihrer Aufgabe zugeordnet sind. Sie können nicht in der verwendet werden, AWS Cloud da sie kein IAM-Pendant haben.

Sie können diese Anmeldeinformationen der 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 der AWS -SDKs und von der gemeinsam genutztAWS 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
```

Angeben des S3-Adapters als AWS CLI Endpunkt

Wenn Sie die verwenden, AWS CLI um einen Befehl an das AWS Snowball Edge Gerät auszugeben, geben Sie an, dass der Endpunkt der Amazon S3-Adapter ist. Sie können den HTTPS-Endpunkt oder einen ungesicherten HTTP-Endpunkt, wie hier gezeigt, verwenden.

Gesicherter HTTPS-Endpunkt

```
aws s3 ls --profile snowballEdge --endpoint https://192.0.2.0:8443 --ca-bundle path/to/certificate
```

Ungesicherter HTTP-Endpunkt

```
aws s3 ls --profile snowballEdge --endpoint http://192.0.2.0:8080
```

Wenn Sie den HTTPS-Endpunkt von verwenden`8443`, werden Ihre Daten sicher von Ihrem Server an den 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 der Pfad zu Ihrem Zertifikat wie unten beschrieben hinzugefügt wird.

So verknüpfen Sie Ihr Zertifikat mit dem Schnittstellenendpunkt

1. Verbinden Sie den Snowball Edge mit dem Strom 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 von einem Terminal in Ihrem Netzwerk sicher, dass Sie den Snowball Edge 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.
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 --profile snowballEdge --endpoint https://192.0.2.0:8443
```

Nicht unterstützte Amazon S3-Funktionen für den Amazon S3-Adapter

Mit dem Amazon S3-Adapter können Sie Daten mithilfe von Amazon S3-S3-API-Aktionen programmgesteuert zu und von einem Snowball-Edge übertragen. Bei Verwendung des Amazon

S3-Adapters werden jedoch nicht alle Amazon-SAmazon S3-Übertragungsfunktionen und -API-Aktionen für die Verwendung mit einem Snowball-Edge-Gerät unterstützt. Die folgenden Funktionen und Aktionen werden beispielsweise nicht für die Verwendung mit Snowball Edge unterstützt:

- TransferManager – Dieses Dienstprogramm überträgt Dateien mit dem SDK for Java aus einer lokalen Umgebung an Amazon S3. Erwägen Sie stattdessen, die unterstützten API-Aktionen oder -AWS CLIBefehle 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 Verwendung der Aktion GET Bucket (List Objects) Version 1 oder des AWS CLI Befehls ls.
- ListBuckets – Die ListBuckets mit dem Objektendpunkt wird nicht unterstützt. Der folgende Befehl funktioniert nicht mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten:

```
aws s3 ls --endpoint https://192.0.2.0 --profile profile
```

Batching kleiner Dateien

Bei jeder Kopieroperation entsteht ein zusätzlicher verschlüsselungsbedingter Overhead. Um das Übertragen kleiner Dateien auf Ihr AWS Snowball Edge Gerät zu beschleunigen, können Sie sie in einem einzigen Archiv zusammenfassen. Wenn Sie Dateien zusammenstapeln, können sie automatisch extrahiert werden, wenn sie in Amazon S3 importiert werden, wenn sie in einem der unterstützten Archivformate gestapelt 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. Mehr als 100.000 Dateien in einem Batch können sich darauf auswirken, wie schnell diese Dateien in Amazon S3 importiert werden, nachdem Sie das Gerät zurückgegeben haben. 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 mit dem AWS CLI `cp` Befehl mit der `--metadata snowball-auto-extract=true` Option auf ein Snowball Edge-Gerät. Durch die Angabe von wird automatisch der Inhalt der archivierten Dateien `snowball-auto-extract=true` extrahiert, wenn die Daten in Amazon S3 importiert werden, solange die Größe der Stapeldatei nicht größer als 100 GB ist.

> **Note**
>
> Alle 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. Batchen Sie Ihre Dateien in der Befehlszeile, wie in den folgenden Beispielen gezeigt.

   - Für Linux können Sie die Dateien in derselben Befehlszeile zusammenfassen, die für die Übertragung Ihrer Dateien auf das Gerät verwendet wurde.

     ```
     tar -cf - /Logs/April | aws s3 cp - s3://mybucket/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 zum Speichern der Archive, bevor Sie sie auf die Snowball-Appliance übertragen.

   - Verwenden Sie für Windows den folgenden Beispielbefehl, um die Dateien im Batch zu speichern, wenn sich alle Dateien in demselben Verzeichnis befinden, in dem der Befehl ausgeführt wird:

     ```
     7z a -tzip -so "test" | aws s3 cp - s3://mybucket/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, aus dem der Befehl ausgeführt wird, zu stapeln:

```
7z a -tzip -so "test" "c:\temp" | aws s3 cp - s3://mybucket/batch01.zip --
metadata snowball-auto-extract=true --endpoint http://10.x.x.x:8080
```

> **Note**
>
> Für Microsoft Windows 2016 ist tar nicht verfügbar, aber Sie können es von der Website Tar for Windows herunterladen.
> Sie können 7 ZIP von der 7ZIP-Website herunterladen.

4. Wiederholen Sie diesen Vorgang, bis Sie alle kleinen Dateien archiviert haben, die Sie mit einem Snowball Edge an Amazon S3 übertragen möchten.
5. Übertragen Sie die archivierten Dateien in den Snowball. Wenn Sie möchten, dass die Daten automatisch extrahiert werden, und Sie eines der unterstützten Archivformate verwendet haben, die zuvor in Schritt 1 erwähnt wurden, verwenden Sie den AWS CLI `cp` Befehl mit der `--metadata snowball-auto-extract=true` Option .

> **Note**
>
> Wenn Dateien vorhanden sind, die nicht archiviert sind, verwenden Sie diesen Befehl nicht.

Beim Erstellen der Archivdateien behält die Extraktion die aktuelle Datenstruktur bei. 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 demselben Verzeichnis extrahiert, in dem sie gespeichert ist, und die Ordnerstrukturen werden entsprechend erstellt. Beachten Sie, dass es beim Kopieren von Archivdateien wichtig ist, das Flag festzulegen`--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 die Dateien `a.txt`, `b.txt` und enthältc`.txt`. Wenn diese Archivdatei im Stammverzeichnis von / mybucket/ platziert wurde, würden die Daten nach der Extraktion wie folgt aussehen:

```
/mybucket/Logs/April/a.txt
/mybucket/Logs/April/b.txt
```

```
/mybucket/Logs/April/c.txt
```

Wenn die Archivdatei in /mybucket/Test/ platziert wurde, würde die Extraktion wie folgt aussehen:

```
/mybucket/Test/Logs/April/a.txt
/mybucket/Test/Logs/April/b.txt
/mybucket/Test/Logs/April/c.txt
```

Unterstützte AWS CLI Befehle

Im Folgenden finden Sie Informationen dazu, wie Sie den Amazon S3-Adapter oder Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten als Endpunkt für entsprechende AWS Command Line Interface (AWS CLI)-Befehle angeben. Sie finden auch 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-kompatiblem Speicher auf Snow-Family-Geräten unterstützt werden.

> **Note**
>
> Informationen zum Installieren und Einrichten der AWS CLI, einschließlich der Angabe, für welche Regionen Sie AWS CLI Aufrufe tätigen möchten, finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Derzeit unterstützen Snowball Edge-Geräte AWS CLI bei Verwendung des Amazon S3-Adapters nur Version 1.16.14 und früher von . Siehe Snowball Edge-Clientversion. Wenn Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwenden, können Sie die neueste Version des verwendenAWS 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 Amazon S3

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 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 werden würden, werden ohne Ausführung angezeigt.
  - `--quiet` (Boolean) – Vom angegebenen Befehl ausgeführte Operationen werden nicht angezeigt.
  - `--include` (Zeichenfolge) – Schließen Sie keine Dateien oder Objekte im Befehl aus, die dem angegebenen Muster entsprechen. Weitere Informationen finden Sie unter Verwendung von Exclude- und Include-Filtern in der AWS CLI -Befehlsreferenz.
  - `--exclude` (Zeichenfolge) – Schließen Sie alle Dateien oder Objekte aus dem Befehl aus, der dem angegebenen Muster entspricht.
  - `--follow-symlinks | --no-follow-symlinks` (Boolean) – Symbolische Links (Symlinks) werden nur befolgt, wenn sie vom lokalen Dateisystem zu Amazon S3 hochgeladen werden. Amazon S3 unterstützt keine symbolischen Links, sodass der Inhalt des Linkziels unter dem Namen des Links hochgeladen wird. 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 unter dem 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` (Zuweisung) – Eine Zuordnung von Metadaten, die 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`metadata-directive`-Speicherorten ist das Argument standardmäßig , `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 unter dem 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 werden würden, werden ohne Ausführung angezeigt.
  - `--include` (Zeichenfolge) – Schließen Sie keine Dateien oder Objekte im Befehl aus, die dem angegebenen Muster entsprechen. Weitere Informationen finden Sie unter Verwendung von Filter ausschließen und einschließen in der -BefehlsreferenzAWS CLI.
  - `--exclude` (Zeichenfolge) – Schließen Sie alle Dateien oder Objekte aus dem Befehl aus, der dem angegebenen Muster entspricht.
  - `--recursive` (Boolean) – Der Befehl wird für alle Dateien oder Objekte unter dem 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) – Vom 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 Verzeichnisse nur im Ziel, wenn sie eine oder mehrere Dateien enthalten.

> **Important**
>
> Das Synchronisieren von einem Verzeichnis zu einem anderen Verzeichnis auf demselben Snowball Edge wird nicht unterstützt.
> Das Synchronisieren von einem AWS Snowball-Gerät mit einem anderen AWS Snowball-Gerät wird nicht unterstützt.
> Sie können diese Option nur verwenden, um den Inhalt zwischen Ihrem On-Premises-Datenspeicher und einem Snowball Edge zu synchronisieren.

- `--dryrun` (Boolean) – Die Operationen, die mit dem angegebenen Befehl ausgeführt werden würden, werden ohne Ausführung angezeigt.
- `--quiet` (Boolean) – Vom angegebenen Befehl ausgeführte Operationen werden nicht angezeigt.
- `--include` (Zeichenfolge) – Schließen Sie keine Dateien oder Objekte im Befehl aus, die dem angegebenen Muster entsprechen. Weitere Informationen finden Sie unter Verwendung von Filter ausschließen und einschließen in der -BefehlsreferenzAWS CLI.
- `--exclude` (Zeichenfolge) – Schließen Sie alle Dateien oder Objekte aus dem Befehl aus, der dem angegebenen Muster entspricht.
- `--follow-symlinks` oder `--no-follow-symlinks` (Boolean) – Symbolische Links (Symlinks) werden nur befolgt, wenn sie vom lokalen Dateisystem zu Amazon S3 hochgeladen werden. Amazon S3 unterstützt keine symbolischen Links, sodass der Inhalt des Linkziels unter dem Namen des Links hochgeladen wird. 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 eine Listenoperation zurückgegeben werden sollen. Der Standardwert lautet 1000 (das zulässige Maximum). Ein niedrigerer Wert kann bei einem Timeout einer Operation hilfreich sein.
- `--metadata` (Zuweisung) – Eine Zuordnung von Metadaten, die 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`metadata-directive`-Speicherorten ist das Argument standardmäßig , `REPLACE` sofern nicht anders angegeben.

> **Important**
>
> Das Synchronisieren von einem Verzeichnis zu einem anderen Verzeichnis auf demselben Snowball Edge wird nicht unterstützt.
> Das Synchronisieren von einem AWS Snowball-Gerät mit einem anderen AWS Snowball-Gerät wird nicht unterstützt.
> Sie können diese Option nur verwenden, um den Inhalt zwischen Ihrem On-Premises-Datenspeicher und einem Snowball Edge zu synchronisieren.

- `--size-only` (Boolean) – Mit dieser Option ist die Größe jedes Schlüssels das einzige Kriterium, das verwendet wird, um zu entscheiden, ob von der Quelle zum Ziel synchronisiert werden soll.
- `--exact-timestamps` (Boolean) – Bei der Synchronisierung von Amazon S3 mit dem lokalen Speicher werden Elemente derselben Größe nur ignoriert, wenn die Zeitstempel genau übereinstimmen. Das Standardverhalten besteht darin, Elemente gleicher Größe zu ignorieren, es sei denn, die lokale Version ist neuer als die Amazon S3-Version.
- `--delete` (Boolean) – Dateien, die im Ziel, aber nicht in der Quelle vorhanden sind, 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 korrekt angeben. Weitere Informationen finden Sie unter Angeben von Parameterwerten für die AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

Unterstützte REST-API-Aktionen

Im Folgenden finden Sie REST-API-Aktionen, die Sie mit einem -AWS Snowball EdgeGerät und Amazon S3 verwenden können.

Themen

- Unterstützte REST-API-Aktionen für Snowball Edge-Geräte
- Unterstützte REST-API-Aktionen für den Amazon S3-Adapter

Unterstützte REST-API-Aktionen für Snowball Edge-Geräte

HEAD-Snowball-Edge

Beschreibung

Derzeit gibt es nur einen Snowball Edge REST-API-Vorgang, mit dem Sie Statusinformationen für ein bestimmtes Gerät zurückgeben können. Dieser Vorgang gibt den Status eines Snowball Edge zurück. Dieser Status enthält Informationen, die von AWS Support für Fehlerbehebungszwecke verwendet werden können.

Sie können diesen Vorgang nicht mit den AWS -SDKs oder der verwendenAWS CLI. Wir empfehlen, dass Sie `curl` oder einen HTTP-Client verwenden. Die Anforderung muss für diese Operation nicht signiert sein.

Anforderung

Im folgenden Beispiel lautet die IP-Adresse für den Snowball Edge *`192.0.2.0`*. Ersetzen Sie diesen Wert durch die IP-Adresse Ihres tatsächlichen Geräts.

```
curl -X HEAD http://192.0.2.0:8080
```

Antwort

```
<Status xsi:schemaLocation="http://s3.amazonaws.com/doc/2006-03-01/" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <snowballIp>127.0.0.1</snowballIp>
    <snowballPort>8080</snowballPort>
    <snowballId>device-id</snowballId>
    <totalSpaceInBytes>499055067136</totalSpaceInBytes>
    <freeSpaceInBytes>108367699968</freeSpaceInBytes>
    <jobId>job-id</jobId>
    <snowballServerVersion>1.0.1</snowballServerVersion>
    <snowballServerBuild>DevBuild</snowballServerBuild>
    <snowballClientVersion>Version 1.0</snowballClientVersion>
    <snowballRoundTripLatencyInMillis>33</snowballRoundTripLatencyInMillis>
</Status>
```

Unterstützte REST-API-Aktionen für den Amazon S3-Adapter

Im Folgenden finden Sie die Liste der Amazon S3-REST-API-Aktionen, die für die Verwendung des Amazon 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-API-Aktion und dem AWS Snowball Edge Geräte-Pendant ab. Alle Antworten, die von einem -AWS Snowball EdgeGerät zurückgegeben werden, `Server` deklarieren als `AWSSnowball`, wie im folgenden Beispiel.

```
HTTP/1.1 201 OK
x-amz-id-2: JuKZqmXuiwFeDQxhD7M8KtsKobSzWA1QEjLbTMTagkKdBX2z7Il/jGhDeJ3j6s80
x-amz-request-id: 32FE2CEB32F5EE25
Date: Fri, 08 2016 21:34:56 GMT
Server: AWSSnowball
```

Amazon S3-REST-API-Aufrufe erfordern eine SigV4-Signatur. Wenn Sie die AWS CLI oder ein AWS SDK verwenden, um diese API-Aufrufe durchzuführen, wird die SigV4-Signatur für Sie erledigt. Andernfalls müssen Sie Ihre eigene SigV4 Signatur-Lösung implementieren. Weitere Informationen finden Sie unter Authentifizieren von Anforderungen (AWS Signature Version 4) im Benutzerhandbuch für Amazon Simple Storage Service.

- GET Bucket (List Objects) Version 1 – Unterstützt. In dieser Implementierung der GET-Operation wird jedoch Folgendes nicht unterstützt:
  - Paginierung
  - Marker
  - Trennzeichen
  - Wenn die Liste zurückgegeben wird, wird die Liste nicht sortiert

  Es wird nur Version 1 unterstützt. GET Bucket (List Objects) Version 2 wird nicht unterstützt.
- GET-Service
- HEAD-Bucket
- HEAD Object
- GET Object – ist ein DOWNLOAD eines Objekts aus dem S3-Bucket des Snow-Geräts.
- PUT Object – Wenn ein Objekt mit auf ein AWS Snowball Edge Gerät hochgeladen wirdPUT `Object`, wird ein ETag generiert.

  Das ETag ist ein Hash-Wert des Objekts. Das ETag gibt nur Änderungen am Inhalt eines Objekts wieder, nicht an seinen Metadaten. Das ETag kann ein MD5 Digest der Objektdaten sein, muss aber nicht. Weitere Informationen zu ETags finden Sie unter Häufige Antwort-Header in der API-Referenz zu Amazon Simple Storage Service.

- DELETE Object
- Initiieren eines mehrteiligen Uploads – Bei dieser Implementierung löscht das Initiieren einer mehrteiligen Upload-Anforderung für ein Objekt, das bereits auf dem AWS Snowball Edge Gerät vorhanden ist, dieses Objekt zuerst. Anschließend wird es in Teilen auf das AWS Snowball Edge Gerät kopiert.
- List Multipart Uploads
- Upload Part
- Abschließen eines mehrteiligen Uploads
- Abort Multipart Upload

> **Note**
>
> Alle Amazon S3-Adapter-REST-API-Aktionen, die hier nicht aufgeführt sind, werden nicht unterstützt. Die Verwendung aller nicht unterstützten REST-API-Aktionen mit Ihrem Snowball Edge gibt eine Fehlermeldung zurück, die besagt, dass die Aktion nicht unterstützt wird.

Verwalten der NFS-Schnittstelle

Verwenden Sie die Network File System (NFS)-Schnittstelle, um Dateien auf das Snow Family-Gerät hochzuladen, als wäre das Gerät lokaler Speicher auf Ihrem Betriebssystem. Dies ermöglicht einen benutzerfreundlicheren Ansatz für die Übertragung von Daten, da Sie Funktionen Ihres Betriebssystems verwenden können, z. B. das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche. Jeder S3-Bucket auf dem Gerät ist als NFS-Schnittstellenendpunkt verfügbar und kann zum Kopieren von Daten gemountet werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

Sie können die NFS-Schnittstelle verwenden, wenn das Snowball Edge-Gerät so konfiguriert wurde, dass es beim Erstellen des Auftrags zur Bestellung des Geräts enthalten war. Wenn das Gerät nicht für die Aufnahme der NFS-Schnittstelle konfiguriert ist, verwenden Sie den S3-Adapter oder Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten, um Daten zu übertragen. Weitere Informationen zum S3-Adapter finden Sie unter Verwalten des Amazon S3-Adapterspeichers. Weitere Informationen zum Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten finden Sie unter Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.

Beim Start verwendet die NFS-Schnittstelle 1 GB Arbeitsspeicher und 1 CPU. Dies kann die Anzahl der anderen Services, die auf dem Snow Family-Gerät ausgeführt werden, oder die Anzahl der EC2-compatible Instances, die ausgeführt werden können, einschränken.

Über die NFS-Schnittstelle übertragene Daten werden während der Übertragung nicht verschlüsselt. Bei der Konfiguration der NFS-Schnittstelle können Sie CIDR-Blöcke bereitstellen, und das Snow Family-Gerät schränkt den Zugriff auf die NFS-Schnittstelle von Client-Computern mit Adressen in diesen Blöcken ein.

Dateien auf dem Gerät werden an Amazon S3 übertragen, wenn es an zurückgegeben wirdAWS. Weitere Informationen finden Sie unter Importieren von Aufträgen in Amazon S3

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.

- Dateinamen sind Objektschlüssel in Ihrem lokalen S3-Bucket auf dem Snow Family-Gerät. Der Schlüsselname ist eine Folge von Unicode-Zeichen, deren UTF-8-Kodierung maximal 1 024 Byte lang ist. Wir empfehlen, nach Möglichkeit NFSv4.1 zu verwenden und Dateinamen mit Unicode UTF-8 zu codieren, um einen erfolgreichen Datenimport zu gewährleisten. Dateinamen, die nicht mit UTF-8 kodiert sind, werden möglicherweise nicht in S3 oder mit einem anderen Dateinamen in S3 hochgeladen, je nachdem, welche NFS-Kodierung Sie verwenden.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Snow Family-Geräte unterstützen keine Dateipfade, die größer als 1024 Zeichen sind. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateiimport.
- Weitere Informationen finden Sie unter Objektschlüssel im Benutzerhandbuch für Amazon Simple Storage Service.
- Bei NFS-basierten Übertragungen werden Ihren Objekten standardmäßige Metadaten im POSIX-Stil hinzugefügt, wenn sie von Snow Family-Geräten in Amazon S3 importiert werden. Darüber hinaus werden Metadaten „x-amz-meta-user-agent aws-datasync“ angezeigt, da wir derzeit AWS DataSync als Teil des internen Importmechanismus für den Geräteimport in Amazon S3 für Snow Family mit der Option NFS verwenden.
- Sie können bis zu 40M Dateien mit einem einzigen Snowball Edge-Gerät übertragen. Wenn Sie mehr als 40M Dateien in einem einzigen Auftrag übertragen müssen, stapeln Sie die Dateien bitte zusammen, um die Dateinummern pro Übertragung zu reduzieren. Einzelne Dateien können von jeder Größe mit einer maximalen Dateigröße von 5 TB für Snowball Edge-Geräte mit der erweiterten NFS-Schnittstelle oder der S3-Schnittstelle sein.

Sie können die NFS-Schnittstelle auch mit , einem GUI-ToolAWS OpsHub, konfigurieren und verwalten. Weitere Informationen finden Sie unter Verwalten der NFS-Schnittstelle

NFS-Konfiguration für Snow Family-Geräte

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt, daher müssen Sie sie starten, um die Datenübertragung auf das Gerät zu aktivieren. Sie können die NFS-Schnittstelle konfigurieren, indem Sie die IP-Adresse einer Virtual Network Interface (VNI) angeben, die auf dem Snow Family-Gerät 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 Snow Family-Gerät ein. Weitere Informationen finden Sie unter Netzwerkkonfiguration für Datenverarbeitungs-Instances.

Konfigurieren von Snow Family-Geräten für die NFS-Schnittstelle

- 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-Service `ACTIVE` oder zurück`INACTIVE`.

  ```
  {
    "ServiceId" : "nfs",
    "Status" : {
    "State" : "ACTIVE"
    }
  }
  ```

  Wenn der Wert des `State` Namens lautet`ACTIVE`, ist der NFS-Schnittstellenservice aktiv und Sie können das NFS-Volume des Snow-Family-Geräts mounten. Weitere Informationen finden Sie unter

  Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie den Endpunkt als lokalen Speicher auf 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
```

. Wenn der Wert ist`INACTIVE`, müssen Sie den Service starten.

Starten des NFS-Service auf dem Snow Family-Gerät

Starten Sie bei Bedarf eine virtuelle Netzwerkschnittstelle (VNI) und starten Sie dann den NFS-Service auf dem Snow Family-Gerät. Geben Sie bei Bedarf beim Starten des NFS-Service 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 dem Snow Family-Gerät verfügbaren VNIs anzuzeigen.

```
snowballEdge describe-virtual-network-interfaces
```

Wenn eine oder mehrere VNIs auf dem Snow Family-Gerät aktiv 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 der VNI, die mit der NFS-Schnittstelle verwendet werden soll.

2. Wenn keine VNIs verfügbar sind, verwenden Sie den `create-virtual-network-interface` Befehl , um eine 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-Service zu starten und ihn der 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 Servicestatus zu überprüfen. Es wird ausgeführt, wenn der Wert des `State` Namens ist`ACTIVE`.

```
snowballEdge describe-service --service-id nfs
```

Der Befehl gibt den Servicestatus sowie die IP-Adresse und Portnummer des NFS-Endpunkts und der CIDR-Bereiche zurück, die auf den Endpunkt zugreifen dürfen.

```
{
 "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 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
```

Anhalten der NFS-Schnittstelle

Wenn Sie mit der Übertragung von Dateien über die NFS-Schnittstelle fertig sind und bevor Sie das Snow Family-Gerät ausschalten, verwenden Sie den `stop-service` Befehl , um den NFS-Service zu beenden.

```
snowballEdge stop-service --service-id nfs
```

BenutzenAWS IoT Greengrassum vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen

AWS IoT Greengrassist ein Open-Source-Edge-Runtime- und Cloud-Service für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können. Sie können Folgendes verwendenAWS IoT Greengrassum Software zu entwickeln, die es Ihren Geräten ermöglicht, lokal auf die von ihnen generierten Daten zu reagieren, Vorhersagen auf der Grundlage von Modellen für maschinelles Lernen durchzuführen und Gerätedaten zu filtern und zu aggregieren. Für detaillierte Informationen überAWS IoT Greengrass, siehe Was istAWS IoT Greengrass?in derAWS IoT Greengrass Version 2Leitfaden für Entwickler.

Durch die Verwendung vonAWS IoT GreengrassAuf Ihrem Snow Family-Gerät ermöglichen Sie es dem Gerät, Daten näher am Ort ihrer Entstehung zu sammeln und zu analysieren, selbstständig

auf lokale Ereignisse zu reagieren und sicher mit anderen Geräten im lokalen Netzwerk zu kommunizieren.

Richten Sie Ihre Amazon EC2-kompatible Instance ein

> **Note**
>
> Um zu installierenAWS IoT Greengrass Version 2Stellen Sie auf einem Snow Family-Gerät sicher, dass Ihr Gerät mit dem Internet verbunden ist. Nach der Installation ist kein Internet erforderlich, damit ein Snow Family-Gerät verwendet werden kannAWS IoT Greengrass.

Um eine EC2-kompatible Instanz einzurichten fürAWS IoT Greengrass V2

1. Starten Sie denAWS IoT Greengrassvalidiertes AMI mit einer öffentlichen IP-Adresse und einem SSH-Schlüssel:

   a. Unter Verwendung desAWS CLI:Instanzen ausführen.

   b. VerwendenAWS OpsHub:Starten einer Amazon EC2-kompatiblen Instance.

   > **Note**
   >
   > Notieren Sie sich die öffentliche IP-Adresse und den Namen des SSH-Schlüssels, die der Instanz zugeordnet sind.

2. Stellen Sie mithilfe von SSH eine Verbindung zur EC2-kompatiblen Instance her. Führen Sie dazu den folgenden Befehl auf dem Computer aus, der mit Ihrem Gerät verbunden ist. Ersetzen*SSH-Schlüssel*mit dem Schlüssel, mit dem Sie die EC2-kompatible Instance gestartet haben. Ersetzen*public-ip-address*durch die öffentliche IP-Adresse der EC2-kompatiblen Instance.

   ```
   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 SSH-Befehl, oder Sie haben SSH, können aber keine Verbindung zu Ihrer EC2-kompatiblen Instance herstellen. Um eine Verbindung

zu Ihrer EC2-kompatiblen Instance herzustellen, können Sie PuTTY installieren und konfigurieren. Dabei handelt es sich um einen kostenlosen Open-Source-SSH-Client. Sie müssen den SSH-Schlüssel konvertieren von `.pem`formatieren Sie in das PuTTY-Format und stellen Sie eine Verbindung zu Ihrer EC2-Instance her. Für Anweisungen zur Konvertierung von `.pem`in das PuTTY-Format finden Sie unterKonvertieren Sie Ihren privaten Schlüssel mit PuTTYgenim Amazon EC2-Benutzerhandbuch für Linux-Instances.

Installieren von AWS IoT Greengrass

Als Nächstes richten Sie Ihre EC2-kompatible Instance alsAWS IoT GreengrassKerngerät, das Sie für die lokale Entwicklung verwenden können.

So installieren Sie AWS IoT Greengrass

1. Verwenden Sie den folgenden Befehl, um die erforderliche Software für zu installierenAWS IoT Greengrass. Dieser Befehl installiert denAWS 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 Erlaubnis, das auszuführenAWS IoT GreengrassSoftware und ändern Sie die Root-Rechte von`root ALL=(ALL) ALL`zu`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 das herunterzuladenAWS IoT GreengrassKernsoftware.

   ```
   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 bereitzustellenAWS IoT GreengrassKernsoftware. 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 des IAM-Benutzers imAWSRegion, nicht das Snow Family-Gerät.

5. Verwenden Sie den folgenden Befehl, um das zu installierenAWS IoT GreengrassKernsoftware. Der Befehl erstelltAWSRessourcen, 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`: DasAWSRegion, in der Ressourcen gesucht oder erstellt werden sollen.
   - `MyGreengrassCore`: Der Name desAWS IoTDing für deinAWS IoT GreengrassKerngerät.
   - `MyGreengrassCoreGroup`: Der Name desAWS IoTDinggruppe für deineAWS IoT GreengrassKerngerät.

```
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 unterInstallieren Sie dasAWS IoT GreengrassKernsoftware.

Wenn du fertig bist, wirst du eine habenAWS IoT GreengrassCore läuft auf Ihrem Snow Family-Gerät für Ihren lokalen Gebrauch.

Verwendung von AWS Lambda mit AWS Snowball Edge

AWS Lambdabetrieben vonAWS IoT Greengrassist 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 MQTT-Nachrichten (Message Queuing Telemetry Transport) aufzurufen, Python-Code in Lambda-Funktionen auszuführen und sie für öffentliche Aufrufe zu verwendenAWSService-Endpunkte in der Cloud. Um Lambda-Funktionen mit Snowball Edge-Geräten verwenden zu können, müssen Sie Ihre Snowball Edge-Jobs in einem erstellenAWS-Regionunterstützt vonAWS IoT Greengrass. Für eine Liste gültigerAWS-Regionen, sieheAWS IoT Greengrassin derAllgemeine 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

Bevor Sie beginnen

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

AWS IoT Greengrassist Software, die erweitertAWS CloudFunktionen für lokale Geräte.AWS IoT Greengrassermöglicht es lokalen Geräten, Daten näher an der Informationsquelle zu sammeln und zu analysieren und gleichzeitig in lokalen Netzwerken sicher miteinander zu kommunizieren. Genauer gesagt, Entwickler, die verwendenAWS IoT Greengrasskönnen serverlosen Code (Lambda-Funktionen) in derAWS Cloud. Sie können diesen Code dann einfach für Geräte zur lokalen Ausführung von Anwendungen bereitstellen.

Das FolgendeAWS IoT GreengrassBei der Verwendung von Konzepten ist es wichtig, sie zu verstehenAWS IoT Greengrassmit einem Snowball Edge:

- AWS IoT GreengrassAnforderungen— Für eine vollständige Liste vonAWS IoT GreengrassAnforderungen finden Sie unterAnforderungenin derAWS IoT Greengrass Version 2Leitfaden für Entwickler.
- AWS IoT GreengrassKern— Laden Sie das herunterAWS IoT GreengrassKernsoftware und installieren Sie sie auf einer EC2-Instanz, die auf dem Gerät läuft. SieheVerwendenAWS IoT Greengrassauf Amazon EC2-Instancesin diesem Handbuch.

  Um Lambda-Funktionen auf einem Snowball Edge-Gerät verwenden zu können, müssen Sie zuerst Folgendes installierenAWS IoT GreengrassKernsoftware auf einer Amazon EC2-Instance auf dem Gerät. Die Lambda-Funktionen, die Sie auf dem Snowball Edge-Gerät verwenden möchten, müssen mit demselben Konto erstellt werden, das Sie für die Installation verwenden werdenAWS IoT Greengrassauf dem Snowball Edge-Gerät. Für Informationen zur InstallationAWS IoT Greengrassauf Ihrem Snowball Edge-Gerät finden Sie unterBenutzenAWS IoT Greengrassum vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen.
- AWS IoT GreengrassGruppe— Ein Snowball Edge-Gerät ist Teil einesAWS IoT GreengrassGruppe als Kerngerät der Gruppe. Weitere Informationen zu Gruppen finden Sie unterAWSGreengrass IoT-Gruppenin derAWS IoT GreengrassLeitfaden für Entwickler.
- MQTT—AWS IoT Greengrassverwendet das einfache MQTT-Protokoll nach Industriestandard, um innerhalb einer Gruppe zu kommunizieren. Jedes Gerät oder jede Software, die mit MQTT kompatibel ist, in IhremAWS IoT GreengrassEine Gruppe kann MQTT-Nachrichten aufrufen. Diese

Nachrichten können Lambda-Funktionen aufrufen, wenn Sie die zugehörige MQTT-Nachricht entsprechend definieren.

Voraussetzungen für AWS Lambda

AWS Lambda ist ein Datenverarbeitungsservice, 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, hochgeladen und auf Lambda veröffentlicht und auf einem Snowball Edge verwendet. Weitere Informationen finden Sie unterLambda-Funktionenin derAWS LambdaLeitfaden für Entwickler.
- Lambda-Konsole— Die Konsole, in der Sie Ihre Lambda-Funktionen in Python-Sprache zur Verwendung auf einem Snowball Edge hochladen, aktualisieren und veröffentlichen. Für weitere Informationen überLambda-Konsole, sieheLambda-Konsolein derAWS LambdaLeitfaden für Entwickler.
- Python— Die High-Level-Programmiersprache, die für Ihre Lambda-Funktionen verwendet wird, unterstützt vonAWS IoT Greengrassauf einem Snowball Edge.AWS IoT Greengrassunterstützt 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 einem auszuführenAWS IoT GreengrassGruppe, importieren Sie die Funktion als Komponente. Vollständige Informationen zum Importieren einer Funktion als Komponente finden Sie unterAWS IoT GreengrassKonsole finden Sie unterImportieren Sie eine Lambda-Funktion als Komponente (Konsole)in derAWS IoT Greengrass Version 2Leitfaden für Entwickler.

1. In derAWSIoT-Konsole, auf derGreengrass-KomponentenSeite, wählenKomponente erstellen.
2. InQuelle der Komponente, wählenLambda-Funktion importieren. InLambda-Funktion, wählen Sie den Namen Ihrer Funktion. InVersion der Lambda-Funktion, wählen Sie die Version Ihrer Funktion.
3. Um der Funktion Nachrichten zu abonnieren, auf die sie reagieren kann, wählen SieEventquelle hinzufügenund wählen Sie das Ereignis aus. InTimeout (Sekunden), geben Sie einen Timeout-Zeitraum in Sekunden an.
4. InFestgesteckt, wählen Sie aus, ob Sie Ihre Funktion fixieren möchten oder nicht.

5. WählleKomponente erstellen
6. Wählen Sie Bereitstellen aus.
7. InEinsatz, wählenZu vorhandener Bereitstellung hinzufügenund wählen Sie dann Ihre Greengrass-Gruppe aus. Wählen Sie Weiter aus.
8. InÖffentliche Komponenten, wählen Sie diese Komponenten aus:
   - AWS.GreenGrass.cli
   - aws.greengrass.LambdaLauncher
   - aws.greengrass.LambdaManager
   - aws.greengrass.LambdaRuntimes
   - AWS.Greengrass.Nucleus
9. Wählen Sie Bereitstellen aus.

Verwenden von Amazon EC2-compatibleInstances

Dieser Abschnitt bietet einen Überblick über die Verwendung von AmazonEC2-compatible Rechen-Instances auf einem -AWS Snowball EdgeGerät, einschließlich konzeptioneller Informationen, Verfahren und Beispiele.

Themen

Übersicht

Sie können Amazon EC2-compatible Rechen-Instances ausführen, die auf einem Snowball Edge gehostet werden`sbe1`, mit den Instance-`sbe-g`Typen `sbe-c`, und . Der `sbe1` Instance-Typ funktioniert auf Geräten mit der Option Snowball Edge Storage Optimized. Der `sbe-c` Instance-Typ funktioniert auf Geräten mit der Option Snowball Edge Compute Optimized. Sowohl die `sbe-c` `sbe-g` Instance-Typen als auch funktionieren auf Geräten mit der Option Snowball Edge Compute Optimized with GPU. Eine Liste mit unterstützten Instance-Typen finden Sie unter Kontingente für Datenverarbeitungs-Instances auf einem Snowball-Edge-Gerät.

Alle drei Datenverarbeitungs-Instance-Typen, die für die Verwendung auf Snowball Edge-Geräten unterstützt werden, sind für Snowball Edge-Geräte eindeutig. Wie ihre cloudbasierten Pendants benötigen diese Instances Amazon-Systemabbilder (Amazon Machine Images, AMIs) zum Starten. Sie wählen das AMI als Basis-Image für eine Instance in der Cloud aus, bevor Sie Ihren Snowball-Edge-Auftrag erstellen.

Um eine Rechen-Instance auf einem Snowball Edge zu verwenden, erstellen Sie einen Auftrag, um ein Snow Family-Gerät zu bestellen und Ihre AMIs anzugeben. Sie können dies über die Managementkonsole für die AWS Snow-Familie, die AWS CLIoder eines der -AWSSDKs tun. SDKs In der Regel gibt es einige organisatorische Voraussetzungen, die Sie vor dem Erstellen Ihres Auftrags umsetzen müssen, um Ihre Instances nutzen zu können.

Wenn Ihr Gerät eingetroffen ist, können Sie mit der Verwaltung Ihrer AMIs und Instances beginnen. Sie können Ihre Datenverarbeitungs-Instances auf einem Snowball Edge über einen Amazon

EC2-compatible Endpunkt verwalten. Diese Art von Endpunkt unterstützt viele der Amazon EC2-compatible CLI-Befehle und -Aktionen für die AWS SDKs . Sie können die AWS Management Console auf dem Snowball Edge nicht verwenden, um Ihre AMIs und Datenverarbeitungs-Instances zu verwalten.

Wenn Sie mit der Arbeit an Ihrem Gerät fertig sind, senden Sie es an AWS. 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 ein vollständiges Löschen des Geräts durch, wenn es an zurückgegeben wirdAWS. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

> **Important**
>
> - Die Verwendung verschlüsselter AMIs auf Snowball-Edge-Geräten wird nicht unterstützt.
> - Daten in Datenverarbeitungs-Instances, die auf einem Snowball Edge ausgeführt werden, werden nicht in importiertAWS.

Unterschied zwischen Amazon EC2- und AmazonEC2-compatible Instances auf Snow-Family-Geräten

AWS ECEC2-compatible der Snow Family ermöglichen es Kunden, Amazon EC2-compatible Instances mithilfe einer Teilmenge von EC2-APIs und einer Teilmenge von AMIs zu verwenden und zu verwalten.

Preise für Compute Instances auf Snowball Edge

Die Verwendung von Datenverarbeitungs-Instances verursacht zusätzliche Kosten. Weitere Informationen finden Sie unter AWS Snowball Edge-Preisgestaltung.

Verwenden eines Amazon EC2-compatible AMI auf Snow Family-Geräten

Um ein Amazon Machine Image (AMI) auf Ihrem AWS Snow Family-Gerät zu verwenden, müssen Sie es zuerst dem Gerät hinzufügen. Sie können ein AMI wie folgt hinzufügen:

- Laden Sie das AMI hoch, wenn Sie das Gerät bestellen.
- Fügen Sie das AMI hinzu, wenn Ihr Gerät an Ihrem Standort eintrifft.

Amazon EC2-Computing-Instances, die mit Ihren Snow Family-Geräten geliefert werden, werden basierend auf den Amazon EC2-AMIs gestartet, die Sie Ihrem Gerät hinzufügen. Amazon EC2-compatible AMIs unterstützen sowohl Linux- als auch Microsoft Windows-Betriebssysteme.

Linux

Die folgenden Linux-Betriebssysteme werden unterstützt:

- Amazon Linux 2 für Snow Family

  > **Note**
  >
  > Die neueste Version dieses AMI wird zu dem Zeitpunkt bereitgestellt, an dem Ihr Snow Family-Gerät bereit ist, von zu versenden AWS. Informationen zum Ermitteln der Version dieses AMI auf dem Gerät, wenn Sie es erhalten, finden Sie unter Bestimmen der Version des Amazon Linux 2 AMI für Snow Family.

- CentOS 7 (x86_64) – mit Updates für 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 Import/Export unterstützt und werden lokal in AMIs ausgeführt.

- Ubuntu 20.04 LTS – Focal
- Ubuntu 22.04 LTS – Jammy

Behalten Sie als bewährte Methode für die Sicherheit Ihre Amazon Linux 2-AMIs up-to-date auf Snow Family-Geräten bei, sobald neue Amazon Linux 2-AMIs veröffentlicht werden. Siehe Aktualisieren Ihrer Amazon Linux 2-AMIs auf Snow Family-Geräten.

Windows

Die folgenden Windows-Betriebssysteme werden unterstützt:

- Windows Server 2012 R2
- Windows Server 2016

- Windows Server 2019

Sie können Ihrem Gerät Windows-AMIs hinzufügen, indem Sie Ihr Windows Virtual Machine (VM)-Image AWS mithilfe von VM Import/Export in importieren. Oder Sie können das Image direkt nach der Bereitstellung des Geräts auf Ihrem Standort in Ihr Gerät importieren. Weitere Informationen finden Sie unter Hinzufügen eines Microsoft Windows-AMI.

> **Note**
>
> Windows-AMIs, die von stammen, AWS können Ihrem Gerät nicht hinzugefügt werden. Lokal importierte AMIs müssen sich im BIOS-Startmodus befinden, da UEFI nicht unterstützt wird.

Snow Family unterstützt das BYOL-Modell (Bring Your Own License). Weitere Informationen finden Sie unter Hinzufügen eines Microsoft Windows-AMI.

> **Note**
>
> AWS ECEC2-compatible der Snow Family ermöglichen es Kunden, Amazon EC2-compatible Instances mithilfe einer Teilmenge von EC2-APIs und einer Teilmenge von AMIs zu verwenden und zu verwalten.

Themen

Hinzufügen eines AMI bei der Bestellung Ihres Geräts

Wenn Sie Ihr Gerät bestellen, können Sie dem Gerät AMIs hinzufügen, indem Sie sie im Abschnitt Datenverarbeitung mit EC2-Instances – optional im auswählen Managementkonsole für die AWS

Snow-Familie. Die Option Datenverarbeitung mit EC2-Instances – optional listet alle AMIs auf, die auf Ihr Gerät geladen werden können. Die AMIs lassen sich in die folgenden Kategorien einteilen:

- AMIs aus AWS Marketplace – Dies sind AMIs, die aus der Liste der unterstützten AMIs erstellt wurden. Informationen zum Erstellen eines AMI aus den unterstützten AMIs von AWS Marketplace finden Sie unter Hinzufügen eines AMI von AWS Marketplace.
- AMIs, die mit VM Import/Export hochgeladen wurden – Wenn Sie Ihr Gerät bestellen, werden die AMIs, die mit VM Import/Export hochgeladen wurden, in der Konsole aufgeführt. Weitere Informationen finden Sie unter Importieren einer VM als Image mithilfe von VM Import/Export im VM Import/Export-Benutzerhandbuch. Informationen zu unterstützten Virtualisierungsumgebungen finden Sie unter VM Import/Export-Anforderungen.

Hinzufügen eines AMI von AWS Marketplace

Sie können AWS Marketplace Ihrem Snow Family-Gerät viele AMIs von hinzufügen, indem Sie die AWS Marketplace Instance starten, daraus ein AMI erstellen und das AMI in derselben Region konfigurieren, in der Sie das Snow-Gerät bestellen. Anschließend können Sie das AMI auf dem Gerät einschließen, wenn Sie einen Auftrag zur Bestellung des Geräts erstellen. Stellen Sie bei der Auswahl eines AMI im Marketplace sicher, dass es über einen unterstützten Produktcode und eine Plattform verfügt.

Themen

- Überprüfen von Produktcodes und Plattformdetails von AWS Marketplace AMIs
- Bestimmen der Version des Amazon Linux 2 AMI für Snow Family
- Konfigurieren des AMI für das Snow Family-Gerät

Überprüfen von Produktcodes und Plattformdetails von AWS Marketplace AMIs

Bevor Sie mit dem Prozess zum Hinzufügen eines AMI von AWS Marketplace zu Ihrem Snow Family-Gerät beginnen, stellen Sie sicher, dass der Produktcode und die Plattformdetails des AMI in Ihrem unterstützt werden AWS-Region.

1. Öffnen Sie die Amazon EC2-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 erstellen Sie den Auftrag, um das Snow Family-Gerät zu bestellen. Sie können eine beliebige Region auswählen, die Ihnen zur Verfügung steht, unabhängig von Ihrem Standort.

3. Wählen Sie im Navigationsbereich die Option AMIs.
4. Verwenden Sie die Filter- und Suchoptionen, um die Liste der angezeigten AMIs so einzugrenzen, dass nur die AMIs angezeigt werden, die Ihren Kriterien entsprechen. Wählen Sie beispielsweise AMIs, die von der bereitgestellt werden AWS Marketplace, Öffentliche Images aus. Verwenden Sie dann die Suchoptionen, um die Liste der angezeigten AMIs weiter einzugrenzen:

   - (Neue Konsole) Wählen Sie die Suchleiste und dann im Menü Besitzeralias , dann den Operator = und dann 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 von AWS Marketplace enthalten aws-marketplace in der Spalte Quelle.

5. Wählen Sie in der Spalte AMI-ID die AMI-ID des AMI aus.
6. Stellen Sie in der Image-Zusammenfassung des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der folgenden Tabelle.

   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	avyfzznywektkgl5qv5f57ska
Ubuntu 20.04 LTS	a8jynf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkjt189a13aqe

7. Stellen Sie dann auch 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 für Oracle bring-your-own-license
- Windows bring-your-own-license

Bestimmen der Version des Amazon Linux 2 AMI für Snow Family

Gehen Sie wie folgt vor, um die Version des Amazon Linux 2 AMI für Snow Family auf dem Snow Family-Gerät zu ermitteln. Installieren Sie die neueste Version von , AWS CLI bevor Sie fortfahren. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von im AWS CLI AWS Command Line Interface -Benutzerhandbuch.

- Verwenden Sie den `describe-images` AWS CLI Befehl , um die Beschreibung des AMI anzuzeigen. Die Version ist in der Beschreibung enthalten. Stellen Sie das öffentliche Schlüsselzertifikat 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 **`describe-images`** Befehls

```
{
    "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 Snow Family **`2.0.20240131.0`**. Sie finden sie im Wert des `Description` Namens.

Konfigurieren des AMI für das Snow Family-Gerät

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Starten Sie eine neue Instance eines unterstützten AMI in AWS Marketplace.

> **Note**
>
> Stellen Sie beim Starten Ihrer Instance sicher, dass die der Instance zugewiesene Speichergröße für Ihren Anwendungsfall geeignet ist. In der Amazon EC2-Konsole tun Sie dies im Schritt Speicher hinzufügen.

3. Installieren und konfigurieren Sie die Anwendungen, die Sie auf dem Snowball Edge ausführen möchten, und stellen Sie sicher, dass sie wie erwartet funktionieren.

> **Important**
>
> - Es werden nur Einzel-Volume-AMIs unterstützt.
> - Das EBS-Volume in Ihrem AMI sollte 10 TB oder weniger betragen. Wir empfehlen Ihnen, die EBS-Volume-Größe bereitzustellen, die für die Daten im AMI erforderlich ist. Dies trägt dazu bei, die Zeit zu verkürzen, die benötigt wird, um Ihr AMI zu exportieren und in Ihr Gerät zu laden. Sie können die Größe ändern oder Ihrer Instance nach der Bereitstellung Ihres Geräts weitere Volumes hinzufügen.
> - Der EBS-Snapshot in Ihrem AMI darf nicht verschlüsselt sein.

4. Erstellen Sie eine Kopie der PEM- oder PPK-Datei, die Sie beim Erstellen dieser Instance für das SSH-Schlüsselpaar verwendet 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 sie benötigen, wenn Sie SSH verwenden, um eine Verbindung mit der EC2-compatible Instance auf Ihrem Gerät herzustellen.

   > **Important**
   >
   > Wenn Sie dieses Verfahren nicht befolgen, können Sie keine Verbindung zu Ihren Instances mit SSH herstellen, wenn Sie Ihr Snowball-Edge-Gerät erhalten.

5. Speichern Sie die Instance als AMI. Weitere Informationen finden Sie im Amazon EC2-Benutzerhandbuch für Linux-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.
6. Wiederholen Sie die Schritte 1 bis 4 für jede der Instances, mit der Sie über SSH eine Verbindung herstellen möchten. Stellen Sie sicher, dass Sie Kopien der einzelnen SSH-Schlüsselpaare erstellen und die AMIs verfolgen, denen sie zugeordnet sind.
7. Wenn Sie Ihr Gerät bestellen, können diese AMIs Ihrem Gerät hinzugefügt werden.

Lokales Hinzufügen eines AMI

Wenn das Gerät an Ihrem Standort eintrifft, können Sie ihm neue AMIs hinzufügen. Anweisungen finden Sie unter Importieren eines Images einer virtuellen Maschine auf ein Snow Family-Gerät. Beachten Sie, dass, obwohl alle VMs unterstützt werden, nur unterstützte AMIs auf volle Funktionalität getestet wurden.

> **Note**
>
> Wenn Sie VM Import/Export verwenden, um Ihrem Gerät AMIs hinzuzufügen oder nach der Bereitstellung Ihres Geräts eine VM zu importieren, können Sie VMs hinzufügen, die ein beliebiges Betriebssystem verwenden. Allerdings wurden nur unterstützte Betriebssysteme auf Snow-Family-Geräten getestet und validiert. Sie sind dafür verantwortlich, die Geschäftsbedingungen aller Betriebssysteme oder Software einzuhalten, die sich im virtuellen Image befinden, das Sie auf Ihr Gerät importieren.
>
> > **Important**
> >
> > Damit AWS Services auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Services zulassen. Details hierzu finden Sie unter Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports.

Hinzufügen eines Microsoft Windows-AMI

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 in importieren oder direkt nach der Bereitstellung auf Ihrem Standort 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 mit seiner On-Premises-Lizenz besitzen, auf übertragen wird AWS. AWS stellt sowohl gemeinsame als auch dedizierte Bereitstellungsoptionen für die BYOL-Option bereit.

Sie können Ihr Windows-VM-Image zu Ihrem Gerät hinzufügen, indem Sie es AWS mithilfe von VM Import/Export in importieren oder direkt nach der Bereitstellung auf Ihrer Website in Ihr Gerät importieren. Sie können keine Windows-AMIs hinzufügen, die aus stammen AWS. Daher müssen Sie Ihr eigenes Windows VM-Image erstellen und importieren und Ihre eigene Lizenz mitbringen, wenn Sie das AMI auf Ihrem Snow Family-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 zum Importieren auf Ihr Gerät

Um ein Windows-VM-Image zu erstellen, benötigen Sie eine Virtualisierungsumgebung, z. B. VirtualBox, die für die Windows- und macOS-Betriebssysteme unterstützt wird. Wenn Sie eine VM für Snow-Geräte erstellen, empfehlen wir, mindestens zwei Kerne mit mindestens 4 GB RAM zuzuweisen. Wenn die VM betriebsbereit ist, müssen Sie Ihr Betriebssystem installieren (Windows Server 2012, 2016 oder 2019). Um die erforderlichen Treiber für das Snow Family-Gerät zu installieren, folgen Sie den Anweisungen in diesem Abschnitt.

Damit ein Windows-AMI auf einem Snow-Gerät ausgeführt werden kann, müssen Sie die VioStor Treiber VirtIO , FLR, NetVCM , Vioinput, Viorng, Vioscsi, Vioserial und hinzufügen. Sie können einen Microsoft Software Installer (virtio-win-guest-tools-installer) für die Installation dieser Treiber auf Windows-Images aus dem Repository auf herunterladen GitHub. virtio-win-pkg-scripts

> **Note**
>
> Wenn Sie Ihr VM-Image direkt auf Ihr bereitgestelltes Snow-Gerät importieren möchten, muss die VM-Image-Datei im RAW-Format vorliegen.

So erstellen Sie ein Windows-Image

1. Wählen Sie auf Ihrem Microsoft-Windows-Computer Start und geben Sie ein, **`devmgmt.msc`** um Device Manager zu öffnen.
2. Wählen Sie im Hauptmenü Aktionen und dann Legacy-Hardware hinzufügen aus.
3. Wählen Sie im Assistenten Weiter aus.
4. Wählen Sie Installieren der Hardware, die ich manuell aus einer Liste auswähle (erweitert), und wählen Sie Weiter aus.
5. Wählen Sie Alle Geräte anzeigen und dann Weiter aus.
6. Wählen Sie Festplatte haben, öffnen Sie die Dateien des Copy-Herstellers aus der Liste und navigieren Sie zur ISO-Datei.
7. Navigieren Sie in der ISO-Datei zum `Driver\W2K8R2\amd64` Verzeichnis und suchen Sie dann die `.INF` Datei.
8. Wählen Sie die .INF-Datei, wählen Sie Öffnen und dann OK aus.
9. Wenn Sie den Treibernamen sehen, wählen Sie Weiter und dann zweimal Weiter aus. Klicken Sie auf Finish (Fertig stellen).

Dadurch wird ein Gerät mit dem neuen Treiber installiert. Die eigentliche Hardware ist nicht vorhanden, daher wird ein gelbes Ausrufezeichen angezeigt, das auf ein Problem auf dem Gerät hinweist. Sie müssen dieses Problem beheben.

So beheben Sie das Hardwareproblem

1. Öffnen Sie das Kontextmenü (rechte Maustaste) für das Gerät mit dem Ausrufezeichen.
2. Wählen Sie Deinstallieren, löschen Sie die Treibersoftware für dieses Gerät und wählen Sie OK aus.

   Der Treiber ist installiert und Sie können das AMI auf Ihrem Gerät starten.

Importieren eines VM-Images auf Ihr Gerät

Nachdem Sie Ihr VM-Image vorbereitet haben, können Sie eine der Optionen verwenden, um das Image auf Ihr Gerät zu importieren.

- In der Cloud mit VM Import/Export – Wenn Sie Ihr VM-Image in importieren AWS und es als AMI registrieren, können Sie es Ihrem Gerät hinzufügen, wenn Sie eine Bestellung über die tätigen Managementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter Importieren einer VM als Image mithilfe von VM Import/Export im VM Import/Export-Benutzerhandbuch.
- Lokal auf Ihrem Gerät, das an Ihrem Standort bereitgestellt wird – Sie können Ihr VM-Image direkt in Ihr Gerät importieren, indem Sie AWS OpsHub for Snow Family oder die AWS Command Line Interface (AWS CLI) verwenden.

  Informationen zur Verwendung von finden Sie AWS OpsHub unter Lokale Verwendung von AmazonEC2-compatible Rechen-Instances.

  Informationen zur Verwendung der finden Sie AWS CLI unter Importieren eines Images einer virtuellen Maschine auf ein Snow Family-Gerät.

Exportieren des neuesten Amazon Linux 2-AMI

Um Ihre 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 dann dieses VM-Image 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 Amazon EC2-Benutzerhandbuch für Linux-Instances. Verwenden Sie die neueste Image-ID des Amazon Linux 2-AMI als Wert des `-image-id`Parameters des `-ec2 export-image`Befehls.

3. Importieren Sie das VM-Image mithilfe der AWS CLI oder in das Snow-Gerät AWS OpsHub.

   - Informationen zur Verwendung von AWS CLI finden Sie unter Importieren eines Images einer virtuellen Maschine auf ein Snow Family-Gerät.
   - Informationen zur Verwendung von AWS OpsHub finden Sie unter Importieren eines Images in Ihr Gerät als Amazon EC2-compatible AMI .

Importieren eines Images einer virtuellen Maschine auf ein Snow Family-Gerät

Sie können die AWS CLI und den VM Import/Export-Service verwenden, um ein Image der virtuellen Maschine (VM) als Amazon Machine Image (AMI) auf das Snow Family-Gerät zu importieren. Nachdem Sie ein VM-Image importiert haben, registrieren Sie das Image als AMI und starten Sie es als Amazon EC2-compatible Instance.

Sie können dem Gerät AMIs von Amazon EC2 hinzufügen, wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen. Gehen Sie wie folgt vor, nachdem Sie das Snow Family-Gerät erhalten haben. Weitere Informationen finden Sie unter Schritt 2: Auswählen Ihrer Datenverarbeitungs- und Speicheroptionen.

Sie können auch verwendenAWS OpsHub, um die VM-Image-Datei hochzuladen. Weitere Informationen finden Sie unter Importieren eines Images in Ihr Gerät als AmazonEC2-compatible AMI in diesem Handbuch.

Themen

Schritt 1: Vorbereiten des VM-Images und Hochladen auf das Snow Family-Gerät

Bereiten Sie das VM-Image vor, indem Sie ein VM-Image aus einem Amazon EC2-AMI oder einer Instance in der AWS Cloud mit VM Import/Export exportieren oder das VM-Image lokal mit einer Virtualisierungsplattform Ihrer Wahl generieren.

Informationen zum Exportieren einer Amazon EC2-Instance als VM-Image mit VM Import/Export finden Sie unter Exportieren einer Instance als VM mit VM Import/Export im Benutzerhandbuch für VM Import/Export. Informationen zum Exportieren eines Amazon EC2-AMI als VM-Image mit VM Import/Export finden Sie unter Exportieren einer VM direkt von einem Amazon Machine Image (AMI) im VM-Import/Export-Benutzerhandbuch.

Wenn Sie ein VM-Image aus Ihrer lokalen Umgebung generieren, stellen Sie sicher, dass das Image für die Verwendung als AMI auf dem Snow Family-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 Netzwerkzeitprotokoll (Network Time Protocol, NTP) konfiguriert ist.
- Fügen Sie bei Bedarf öffentliche SSH-Schlüssel ein. Erstellen Sie lokale Kopien der Schlüsselpaare. Weitere Informationen finden Sie unter Verwenden von SSH zum Herstellen einer Verbindung mit Ihren Compute-Instances auf einem Snowball-Edge.
- Installieren und konfigurieren Sie alle Software, die Sie auf dem Snow Family-Gerät verwenden werden.

> **Note**
>
> Beachten Sie die folgenden Einschränkungen, wenn Sie einen Datenträger-Snapshot für ein Snow Family-Gerät vorbereiten.
>
> - Snow Family-Geräte unterstützen derzeit nur den Import von Snapshots im RAW-Image-Format.
> - Geräte der Snow Family unterstützen derzeit nur den Import von Snapshots mit Größen von 1 GB bis 1 TB.

Hochladen eines VM-Images in einen Amazon S3-Bucket auf das Snow-Family-Gerät

Nachdem Sie ein VM-Image vorbereitet haben, laden Sie es in einen S3-Bucket auf dem Snow Family-Gerät oder -Cluster hoch. Sie können den S3-Adapter oder Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwenden, um den Snapshot hochzuladen.

So laden Sie das Image der virtuellen Maschine mit dem S3-Adapter hoch

- 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.

So laden Sie das VM-Image mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräte hoch

- 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 --profile your-profile --endpoint-url s3api-endpoint-ip
  ```

Weitere Informationen finden Sie unter Arbeiten mit S3-Objekten auf einem Snowball-Edge-Gerät.

Schritt 2: Einrichten der erforderlichen Berechtigungen

Damit der Import erfolgreich ist, müssen Sie Berechtigungen für VM Import/Export auf dem Snow Family-Gerät, Amazon EC2 und dem Benutzer einrichten.

> **Note**
>
> Die Servicerollen und Richtlinien, die diese Berechtigungen bereitstellen, befinden sich auf dem Snow Family-Gerät.

Erforderliche Berechtigungen für VM Import/Export

Bevor Sie den Importvorgang starten können, müssen Sie eine IAM-Rolle mit einer Vertrauensrichtlinie erstellen, die VM Import/Export auf dem Snow Family-Gerät erlaubt, die Rolle zu übernehmen. Der Rolle werden zusätzliche Berechtigungen erteilt, damit VM Import/Export auf dem Gerät auf das Image zugreifen kann, das im S3-Bucket auf dem Gerät gespeichert ist.

Erstellen einer JSON-Datei für Vertrauensrichtlinien

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie, die an die Rolle angehängt werden muss, damit VM Import/Export auf den Snapshot zugreifen kann, der aus dem S3-Bucket importiert werden muss.

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

Erstellen einer Rolle mit der JSON-Datei der Vertrauensrichtlinie

Der Rollenname kann vmimport sein. Sie können sie 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 --profile profile-name --endpoint http://snowball-ip:6078 --region
 snow
```

Im Folgenden finden Sie eine Beispielausgabe des `create-role` Befehls .

```
{
   "Role":{
      "AssumeRolePolicyDocument":{
         "Version":"2012-10-17",
         "Statement":[
            {
               "Action":"sts:AssumeRole",
               "Effect":"Allow",
               "Principal":{
                  "Service":"vmie.amazonaws.com"
               }
            }
         ]
      },
      "MaxSessionDuration":3600,
      "RoleId":"AROACEMGEZDGNBVGY3TQOJQGEZAAAABQBB6NSGNAAAABPSVLTREPY3FPAFOLKJ3",
      "CreateDate":"2022-04-19T22:17:19.823Z",
      "RoleName":"vmimport",
      "Path":"/",
      "Arn":"arn:aws:iam::123456789012:role/vmimport"
   }
}
```

Erstellen einer Richtlinie für die Rolle

Die folgende Beispielrichtlinie verfügt über die mindestens erforderlichen Berechtigungen für den Zugriff auf Amazon S3. Ändern Sie den Namen des Amazon S3-Buckets in den Bucket, der Ihre Bilder enthält. Ändern Sie bei einem eigenständigen Snowball Edge-Gerät *snow-id* in Ihre Auftrags-ID. Ändern Sie für einen Gerätecluster *snow-id* in die Cluster-ID. Sie können auch Präfixe verwenden, um den Speicherort weiter einzugrenzen, von dem VM Import/Export Snapshots importieren kann. Erstellen Sie eine Richtlinien-JSON-Datei wie diese.

```
{
   "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 --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Im Folgenden finden Sie ein Ausgabebeispiel aus dem Befehl create-policy.

```
{
   "Policy":{
      "PolicyName":"vmimport-resource-policy",
      "PolicyId":"ANPACEMGEZDGNBVGY3TQOJQGEZAAAABOOEE3IIHAAAABWZJPI2VW4UUTFEDBC2R",
      "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"
   }
}
```

Anfügen der Richtlinie an die Rolle

Fügen Sie der vorherigen Rolle eine Richtlinie an und erteilen Sie Berechtigungen für den Zugriff auf die erforderlichen Ressourcen. Dadurch kann der lokale VM Import/Export-Service 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 --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Erforderliche Berechtigungen für den Aufrufer

Zusätzlich zu der Rolle, die der Snowball Edge VM Import/Export übernehmen soll, müssen Sie auch sicherstellen, dass der Benutzer über die Berechtigungen verfügt, die es ihm ermöglichen, die Rolle an VMIE zu übergeben. Wenn Sie den Standardstammbenutzer zum Durchführen des Imports verwenden, verfügt der Stammbenutzer bereits über alle erforderlichen Berechtigungen, sodass Sie diesen Schritt überspringen und mit Schritt 3 fortfahren können.

Fügen Sie dem Benutzer, der den Import durchführt, die folgenden beiden IAM-Berechtigungen hinzu.

- `pass-role`
- `get-role`

Erstellen einer Richtlinie für die Rolle

Im Folgenden finden Sie eine Beispielrichtlinie, die es einem Benutzer ermöglicht, die `pass-role` Aktionen `get-role` und für die IAM-Rolle auszuführen.

```
{
   "Version":"2012-10-17",
   "Statement":[
        {
            "Effect":"Allow",
            "Action": "iam:GetRole",
            "Resource":"*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
```

```
            "Resource": "*",
            "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 --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Im Folgenden finden Sie ein Ausgabebeispiel aus dem Befehl create-policy.

```
{
   "Policy":{
      "PolicyName":"caller-policy",
      "PolicyId":"ANPACEMGEZDGNBVGY3TQOJQGEZAAAABOOOTUOE3AAAAAAPPBEUM7Q7ARPUE53C6R",
      "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, fügen Sie die Richtlinie den IAM-Benutzern an, die die Amazon EC2-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 --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Erforderliche Berechtigungen zum Aufrufen von Amazon EC2-APIs auf Ihrem Gerät

Um einen Snapshot zu importieren, muss der IAM-Benutzer über die `-ec2:ImportSnapshot`Berechtigungen verfügen. Wenn die Einschränkung des Zugriffs auf den

Benutzer nicht erforderlich ist, können Sie die `ec2:*` Berechtigungen verwenden, um vollen Amazon EC2-Zugriff zu gewähren. Im Folgenden sind die Berechtigungen aufgeführt, die für Amazon EC2 auf Ihrem Gerät erteilt oder eingeschränkt werden können. Erstellen Sie eine Richtliniendatei mit dem angezeigten Inhalt:

```
{
   "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 --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Im Folgenden finden Sie ein Ausgabebeispiel aus dem Befehl create-policy.

```
{
    "Policy":
        {
            "PolicyName": "ec2-import.json",
            "PolicyId":
 "ANPACEMGEZDGNBVGY3TQOJQGEZAAAABQBGPDQC5AAAAATYN62UNBFYTF5WVCSCZS",
            "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, fügen Sie die Richtlinie den IAM-Benutzern an, die die Amazon EC2-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 --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Schritt 3: Importieren des VM-Images als Snapshot auf dem Gerät

Der nächste Schritt besteht darin, das VM-Image als Snapshot auf dem 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}" --profile profile-name --endpoint http://snowball-ip:8008 --
region snow
```

Weitere Informationen finden Sie unter import-snapshot in der -AWS CLIBefehlsreferenz.

Dieser Befehl unterstützt die folgenden Schalter nicht.

- [--client-data`value`]
- [--client-token`value`]
- [--dry-run]
- [--no-dry-run]
- [--verschlüsselt]
- [--no-encrypted]
- [--kms-key-id `value`]
- [--tag-Spezifikationen`value`]

Example Ausgabe des **`import-snapshot`** Befehls

```
{
   "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**
>
> Geräte der Snow Family lassen derzeit nur jeweils einen aktiven Importauftrag pro Gerät zu. 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 Snow Family-Gerät nicht neu, während der Import läuft. Wenn Sie das Gerät neu starten, schlägt der Import fehl und der Fortschritt wird gelöscht, sobald das Gerät zugänglich wird. Verwenden Sie den folgenden Befehl, um den Status Ihrer Snapshot-Importaufgabe zu überprüfen:
>
> ```
> aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --endpoint http://snowball-ip:8008 --region snow
> ```

Schritt 4: Registrieren des Snapshots als AMI

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 seine Snapshots verfügbar sind.

Weitere Informationen finden Sie unter register-image in der -AWS CLIBefehlsreferenz.

Example des **`register-image`** Befehls

```
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 \
--profile profile-name \
--endpoint http://snowball-ip:8008 \
--region snow
```

Im Folgenden finden Sie ein Beispiel für JSON für die Blockgerät-Zuweisung. Weitere Informationen finden Sie unter dem block-device-mapping Parameter register-image in der -AWS CLIBefehlsreferenz.

```
[
    {
        "DeviceName": "/dev/sda",
        "Ebs":
            {
                "Encrypted": false,
                "DeleteOnTermination": true,
                "SnapshotId": "snapshot-id",
                "VolumeSize": 30
            }
    }
]
```

Example des **`register-image`** Befehls

```
{
    "ImageId": "s.ami-8de47d2e397937318"
```

```
 }
```

Schritt 5: Starten einer Instance über das AMI

Informationen zum Starten einer Instance finden Sie unter run-instances in der -AWS CLIBefehlsreferenz.

Der Wert des `image-id` Parameters ist der Wert des `ImageId` Namens als Ausgabe des `register-image` Befehls.

```
aws ec2 run-instances --image-id image-id --instance-type instance-type --
profile profile-name --endpoint http://snowball-ip:8008 --region snow
```

```
{
   "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 auch verwendenAWS OpsHub, um die Instance zu starten. Weitere Informationen finden Sie unter Starten einer AmazonEC2-compatible Instance in diesem Handbuch.

Zusätzliche AMI-Aktionen

Sie können zusätzliche AWS CLI Befehle verwenden, um den Snapshot-Importstatus zu überwachen, Details zu importierten Snapshots abzurufen, den Import eines Snapshots abzubrechen und Snapshots nach dem Import zu löschen oder abzumelden.

Überwachen des Snapshot-Importstatus

Um den aktuellen Status des Importfortschritts anzuzeigen, können Sie den Amazon EC2-`describe-import-snapshot-tasks`Befehl ausführen. Dieser Befehl unterstützt die Paginierung und Filterung auf dem `task-state`.

Example des **`describe-import-snapshot-tasks`** Befehls

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

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 die Ausgabe für Aufgaben an, die innerhalb der letzten 7 Tage erfolgreich abgeschlossen oder als gelöscht markiert wurden. Filtern unterstützt nur `Name=task-state`, `Values=active | deleting | deleted | completed`

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Abbrechen einer Importaufgabe

Um eine Importaufgabe abzubrechen, 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 --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

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 abgebrochen werden.

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Beschreiben von Snapshots

Nachdem ein Snapshot importiert wurde, können Sie ihn mit diesem Befehl beschreiben. Um die Snapshots zu filtern, können Sie `snapshot-ids` mit der Snapshot-ID aus der vorherigen Antwort der Importaufgabe übergeben. Dieser Befehl unterstützt die Paginierung und den Filter für `volume-id`status, und `start-time`.

Example des **`describe-snapshots`** Befehls

```
aws ec2 describe-snapshots --snapshot-ids snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

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 Snow Family-Gerät

Um Snapshots zu entfernen, die Sie besitzen und die Sie nicht mehr benötigen, können Sie den `delete-snapshot` Befehl verwenden.

Example des **`delete-snapshot`** Befehls

```
aws ec2 delete-snapshot --snapshot-id snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

> **Note**
>
> Snowball Edge unterstützt nicht das Löschen von Snapshots, die sich im Status PENDING befinden oder als Root-Gerät für ein AMI vorgesehen sind.

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Aufheben der Registrierung eines AMI

Um die Registrierung von AMIs aufzuheben, die Sie nicht mehr benötigen, können Sie den `deregister-image` Befehl ausführen. Das Aufheben der Registrierung eines AMI, das sich im Status Ausstehend befindet, wird derzeit nicht unterstützt.

Example des **`deregister-image`** Befehls

```
aws ec2 deregister-image --image-id image-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

Dieser Befehl unterstützt die folgenden Parameter nicht.

- [--dry-run]
- [--no-dry-run]

Verwenden der AWS CLI und API-Operationen auf Snowball Edge

Wenn Sie die AWS Command Line Interface (AWS CLI)- oder -API-Operationen verwenden, um IAM-, Amazon S3- und Amazon EC2-Befehle auf Snowball Edge auszugeben, müssen Sie `region` als „“ angebensnow. Sie können dies mit `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 --profile ProfileName --endpoint http://192.0.2.0:8080 --region snow
```

Kontingente für Datenverarbeitungs-Instances auf einem Snowball-Edge-Gerät

Im Folgenden finden Sie Speicherkontingente und gemeinsame Ressourcenbeschränkungen für Rechenressourcen auf einem -AWS Snowball EdgeGerät.

Speicherkontingente

Der für Rechenressourcen verfügbare Speicher ist eine separate Ressource vom dedizierten Amazon S3-Speicher auf einem Snowball-Edge-Gerät. Es gelten die folgenden Speicherkontingente:

- Speicherkontingente für die Option Snowball Edge Storage Optimized – Der insgesamt verfügbare Speicher für Amazon S3 liegt zwischen 60 TB und 80 TB, je nachdem, ob Sie Rechen-Instances auf dem Gerät verwenden. Wenn Sie Datenverarbeitungs-Instances verwenden, beträgt der gesamte verfügbare dedizierte Speicher für `sbe1` Datenverarbeitungs-Instances für die Option Snowball Edge Storage Optimized 1.000 GB.
- Speicherkontingente für die Snowball Edge Compute Optimized und mit GPU-Optionen – Der insgesamt verfügbare dedizierte Speicher für - `sbe-c` und -`sbe-g`Instances beträgt 7,68 TB. Der verbleibende insgesamt verfügbare Speicherplatz ist 42 TB.

In den folgenden Tabellen werden die verfügbaren Rechenressourcen für Snowball Edge-Geräte beschrieben.

Funktion	Einschränkung
Anzahl der AMIs auf einer einzelnen Snowball Edge Storage Optimized-Option	10
Anzahl der AMIs auf einer einzigen für Snowball Edge Compute optimierten Option	20
Anzahl der AMIs auf einem einzelnen Snowball Edge Compute Optimized with GPU-Option	20
Anzahl der Volumes pro Instance	10
Gleichzeitig ausgeführte (oder gestoppte) Instances	Variiert je nach verfügbaren Ressourcen

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	GPUs	Unterstützte Geräteoption
`sbe1.small`	1	1	0	speicheroptimiert
`sbe1.medium`	1	2	0	speicheroptimiert
`sbe1.large`	2	4	0	speicheroptimiert
`sbe1.xlarge`	4	8	0	speicheroptimiert
`sbe1.2xlarge`	8	16	0	speicheroptimiert
`sbe1.4xlarge`	16	32	0	speicheroptimiert
`sbe1.6xlarge`	24	32	0	speicheroptimiert
`sbe-c.small`	1	2	0	für Datenverarbeitung optimiert

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	GPUs	Unterstützte Geräteoption
sbe-c.medium	1	4	0	für Datenverarbeitung optimiert
sbe-c.large	2	8	0	für Datenverarbeitung optimiert
sbe-c.xlarge	4	16	0	für Datenverarbeitung optimiert
sbe-c.2xlarge	8	32	0	für Datenverarbeitung optimiert
sbe-c.4xlarge	16	64	0	für Datenverarbeitung optimiert
sbe-c.8xlarge	32	128	0	für Datenverarbeitung optimiert
sbe-c.12xlarge	48	192	0	für Datenverarbeitung optimiert
sbe-c.16xlarge	64	256	0	für Datenverarbeitung optimiert
sbe-c.24xlarge	96	384	0	für Datenverarbeitung optimiert
sbe-g.small	1	2	1	mit GPU
sbe-g.medium	1	4	1	mit GPU
sbe-g.large	2	8	1	mit GPU
sbe-g.xlarge	4	16	1	mit GPU
sbe-g.2xlarge	8	32	1	mit GPU

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	GPUs	Unterstützte Geräteoption
`sbe-g.4xlarge`	16	64	1	mit GPU
`sbe-g.8xlarge`	32	128	1	mit GPU
`sbe-g.12xlarge`	48	192	1	mit GPU

Einschränkungen für geteilte Datenverarbeitungsressourcen

Alle Services auf einem Snowball Edge-Gerät verwenden einige der endlichen Ressourcen auf dem Gerät. Ein Snowball-Edge-Gerät mit seinen maximal verfügbaren Rechenressourcen kann keine neuen Rechenressourcen starten. Wenn Sie beispielsweise versuchen, die NFS-Schnittstelle zu starten und gleichzeitig eine `sbe1.4xlarge` Rechen-Instance auf einem speicheroptimierten Gerät auszuführen, startet der NFS-Schnittstellenservice nicht. Im Folgenden werden die verfügbaren Ressourcen auf den verschiedenen Geräteoptionen sowie die Ressourcenanforderungen für jeden Service beschrieben.

- Wenn keine Datenverarbeitungsservices den Status `ACTIVE` haben:
  - Auf einer speicheroptimierten Option sind 24 vCPUs und 32 GiB Arbeitsspeicher für Ihre Datenverarbeitungs-Instances verfügbar.
  - Auf einer für die Datenverarbeitung optimierten Option sind 52 vCPUs und 208 GiB Arbeitsspeicher für Ihre Datenverarbeitungs-Instances verfügbar. Dies trifft auch bei vorhandener GPU-Option zu.
- Während AWS IoT Greengrass und AWS Lambda powered by 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. Dies trifft auch auf die GPU-Option zu.
  - Während die NFS-Schnittstelle ist`ACTIVE`, verwendet sie 8 vCPU-Kerne und 16 GiB Arbeitsspeicher auf einem Snowball-Edge-Gerät.
  - Während Amazon S3-kompatibler Speicher auf Snow-Family-Geräten AKTIV ist:

- Auf einem Snowball Edge, der mit AMD EPYC Gen2 und NVME optimiert ist, verwendet er für einen einzelnen Knoten mit der Mindestkonfiguration von 3 TB Amazon S3-kompatiblem Speicher auf Geräten der Snow Family 8 vCPU-Kerne und 16 GB Speicher. Für einen einzelnen Knoten mit mehr als 3 TB Amazon S3-kompatiblem Speicher auf Geräten der Snow Family verwendet er 20 vCPU-Kerne und 40 GB Speicher. Für einen Cluster verwendet er 20 vCPU-Kerne und 40 GB Arbeitsspeicher.
- Auf einem Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD und optionaler GPU verwendet er für einen einzelnen Knoten 8 vCPU-Kerne und 16 GB Arbeitsspeicher. Für einen Cluster verwendet er 20 vCPU-Kerne und 40 GB Arbeitsspeicher.

Sie können feststellen, ob sich ein Service `ACTIVE` auf einem Snowball Edge befindet, indem Sie den Befehl `snowballEdge describe-service` auf dem Snowball Edge-Client verwenden. Weitere Informationen finden Sie unter Abrufen des Servicestatus.

Erstellen eines Datenverarbeitungsauftrags

In diesem Abschnitt erstellen Sie Ihren ersten AmazonEC2-compatibleInstance-Auftrag für ein AWS Snowball-Edge-Gerät.

> **Important**
>
> Beachten Sie die folgenden Punkte, bevor Sie Ihren Auftrag anlegen:
>
> - Stellen Sie sicher, dass die Ihrem AMI zugeordneten vCPU-, Arbeitsspeicher- und Datenspeicherungswerte mit dem Typ der zu erstellenden Instance übereinstimmen.
> - Wenn Sie Secure Shell (SSH) verwenden, um eine Verbindung mit der Instance herzustellen, nachdem Sie die Instance auf Ihrem Snowball Edge gestartet haben, müssen Sie zuerst das folgende Verfahren ausführen. Sie können die AMIs auf Ihrem Snowball Edge nicht mehr aktualisieren. Diesen Schritt müssen Sie vor dem Anlegen des Auftrags durchführen.

Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden

Um Secure Shell (SSH) zum Herstellen einer Verbindung mit Ihren Datenverarbeitungs-Instances auf Snowball-Edge-Geräten zu verwenden, müssen Sie das folgende Verfahren ausführen. Hiermit wird

der SSH-Schlüssel dem AMI vor dem Erstellen Ihres Auftrags hinzugefügt. Wir empfehlen außerdem, dass Sie diese Vorgehensweise nutzen, um Ihre Anwendungen in der Instance einzurichten, die Sie als AMI für Ihren Auftrag nutzen möchten.

> **Important**
>
> Wenn Sie dieses Verfahren nicht befolgen, können Sie keine Verbindung zu Ihren Instances mit SSH herstellen, wenn Sie Ihr Snowball Edge-Gerät erhalten.

So fügen Sie einen SSH-Schlüssel einem AMI hinzu

1. Starten Sie eine neue Instance in der AWS Cloud , die auf dem CentOS 7 (x86_64) basiert – mit Updates für HVM, Ubuntu 16.04 LTS – Xenial (HVM) und Amazon Linux 2 AMI-Image oder Windows.

   Stellen Sie beim Starten Ihrer Instance sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihre spätere Verwendung auf dem Snowball Edge geeignet ist. In der Amazon EC2-Konsole tun Sie dies in Schritt 4: Hinzufügen von Speicher . Eine Liste der unterstützten Größen für Rechen-Instance-Speicher-Volumes auf einem Snowball Edge finden Sie unter Kontingente für Datenverarbeitungs-Instances auf einem Snowball-Edge-Gerät.
2. Installieren und konfigurieren Sie die Anwendungen, die Sie auf dem Snowball Edge ausführen möchten, und testen Sie, ob sie wie erwartet funktionieren.
3. Erstellen Sie eine Kopie der PEM/PPK-Datei, die Sie für das SSH-Schlüsselpaar zur Erstellung dieser Instance verwendet haben. Speichern Sie diese Datei auf dem Server, den Sie für die Kommunikation mit dem Snowball Edge verwenden möchten. Diese Datei wird benötigt, um eine SSH-Verbindung zur gestarteten Instance auf Ihrem Gerät herzustellen. Notieren Sie sich also den Pfad zu dieser Datei.
4. Speichern Sie die Instance als AMI. Weitere Informationen finden Sie unter Erstellen eines Amazon-EBS-gestützten Linux-AMI im Amazon EC2-Benutzerhandbuch für Linux-Instances.
5. Wiederholen Sie dieses Verfahren für jede der Instances, mit der Sie über SSH eine Verbindung herstellen möchten. Erstellen Sie unbedingt eine Kopie der verschiedenen SSH-Schlüsselpaare und notieren Sie sich die dazugehörigen AMIs.

Erstellen des Auftrags in der Konsole

Ihr nächster Schritt besteht darin, einen Auftrag zum Bestellen eines Snow Family-Geräts zu erstellen. Ihr Auftrag kann ein beliebiger Auftragstyp sein, einschließlich eines Clusters. Befolgen Sie mithilfe der Managementkonsole für die AWS Snow-Familiedie Anweisungen unter Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts. Wenn Sie die Seite Schritt 3: Geben Sie Auftragsdetails im Assistenten zur Auftragserstellung aufrufen, führen Sie die folgenden zusätzlichen Schritte aus.

1. Wählen Sie Datenverarbeitung mit EC2 aktivieren aus.
2. Wählen Sie Ein AMI hinzufügen aus.
3. Wählen Sie im sich öffnenden Dialogfeld ein AMI und dann Speichern aus.
4. Fügen Sie Ihrem Auftrag insgesamt bis zu 20 AMIs hinzu, je nach Gerätetyp.
5. Legen Sie Ihren Auftrag wie gewohnt an.

Erstellen Ihres -Auftrags in der AWS CLI

Außerdem können Sie einen Auftrag mithilfe der AWS CLI erstellen. Öffnen Sie dazu ein Terminal und führen Sie den folgenden Befehl aus, wobei Sie den roten Text durch Ihre tatsächlichen Werte ersetzen.

```
aws snowball create-job --job-type IMPORT --resources '{"S3Resources":
[{"BucketArn":"arn:aws:s3:::bucket-name"}],"Ec2AmiResources":
[{"AmiId":"ami-12345678"}]}' --description Example --address-
id ADIEXAMPLE60-1234-1234-5678-41fEXAMPLE57  --kms-key-arn arn:aws:kms:us-
west-2:012345678901:key/eEXAMPLE-1234-1234-5678-5b4EXAMPLE8e --role-
arn arn:aws:iam::012345678901:role/snowball-local-s3-lambda-us-west-2-role --snowball-
capacity-preference T100 --shipping-option SECOND_DAY --snowball-type EDGE
```

Nachdem es eintrifft und Sie Ihr Gerät entsperren, verwenden Sie den Snowball Edge-Client, um Ihre lokalen Anmeldeinformationen zu erhalten. Weitere Informationen finden Sie unter Abrufen von Anmeldeinformationen.

Netzwerkkonfiguration für Datenverarbeitungs-Instances

Nachdem Sie Ihre Datenverarbeitungs-Instances auf einem Snow Family-Gerät gestartet haben, müssen Sie ihm eine IP-Adresse bereitstellen, indem Sie eine Netzwerkschnittstelle erstellen. Snow

Family-Geräte unterstützen zwei Arten von Netzwerkschnittstellen, eine virtuelle Netzwerkschnittstelle und eine direkte Netzwerkschnittstelle.

Virtuelle Netzwerkschnittstelle (VNI)

Eine virtuelle Netzwerkschnittstelle ist die Standardnetzwerkschnittstelle für die Verbindung mit einer EC2-compatible Instance auf Ihrem Snow Family-Gerät. Sie müssen für jede Ihrer EC2-compatible Instances eine VNI erstellen, unabhängig davon, ob Sie auch eine direkte Netzwerkschnittstelle verwenden oder nicht. Der Datenverkehr, der durch eine VNI geleitet wird, ist durch die Sicherheitsgruppen geschützt, die Sie eingerichtet haben. Sie können VNIs nur dem physischen Netzwerkport zuordnen, den Sie zur Steuerung Ihres Snow-Family-Geräts verwenden.

> **Note**
>
> VNI verwendet dieselbe physische Schnittstelle (RJ45, SFP+ oder QSFP), die für die Verwaltung des Snow Family-Geräts verwendet wird. Das Erstellen einer VNI auf einer anderen physischen Schnittstelle als der, die für die Geräteverwaltung verwendet wird, kann zu unerwarteten Ergebnissen führen.

Direct Network Interface (DNI)

Eine Direct Network Interface (DNI) ist ein erweitertes Netzwerkfeature, das Anwendungsfälle wie Multicast-Streams, transitives Routing und Load Balancing ermöglicht. Indem Sie Instances Netzwerkzugriff auf Layer 2 ohne Zwischenübersetzung oder -filterung gewähren, können Sie eine größere Flexibilität bei der Netzwerkkonfiguration Ihres Snow Family-Geräts und eine verbesserte Netzwerkleistung erzielen. DNIs unterstützen VLAN-Tags und die Anpassung der MAC-Adresse. Der Datenverkehr auf DNIs ist nicht durch Sicherheitsgruppen geschützt.

Auf Snowball-Edge-Geräten können DNIs den RJ45-, SFP- oder QSFP-Ports zugeordnet werden. Jeder physische Port unterstützt maximal 63 DNIs. DNIs müssen nicht demselben physischen Netzwerkport zugeordnet werden, den Sie zur Verwaltung des Snow Family-Geräts verwenden.

> **Note**
>
> Für Snowball Edge-Speicher optimierte Geräte (mit EC2-Rechenfunktionalität) unterstützen keine DNIs.

Themen

Voraussetzungen

Bevor Sie eine VNI oder eine DNI konfigurieren, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben.

1. Stellen Sie sicher, dass Ihr Gerät mit Strom versorgt ist 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 Snow Family-Gerät verwenden.
3. Konfigurieren Sie Ihren Snowball Edge-Client. Weitere Informationen finden Sie unter Konfigurieren eines Profils für den Snowball-Edge-Client.
4. Entsperren Sie das Gerät. Wir empfehlen, AWS OpsHub for Snow Family zum Entsperren Ihres Geräts zu verwenden. Anweisungen finden Sie unter Entsperren eines Geräts.

   Wenn Sie den CLI-Befehl verwenden möchten, führen Sie den folgenden Befehl aus und geben Sie die Informationen ein, die im Dialogfeld angezeigt werden.

   ```
   snowballEdge configure
   ```

   ```
   Snowball Edge Manifest Path: manifest.bin

   Unlock Code: unlock code

   Default Endpoint: https://device ip
   ```

5. Führen Sie den folgenden Befehl aus.

   ```
   snowballEdge unlock-device
   ```

   Das Update der Geräteanzeige zeigt an, dass es entsperrt ist.

6. Starten Sie eine EC2-compatible Instance auf dem Gerät. Sie verknüpfen die VNI mit dieser Instance.

7. Führen Sie den Befehl `snowballEdge describe-device` aus, um die Liste der IDs der physischen Netzwerkschnittstellen abzurufen.
8. Identifizieren Sie die ID der physischen Netzwerkschnittstelle, die Sie verwenden möchten. Notieren Sie diese.

Einrichten einer Virtual Network Interface (VNI)

Nachdem Sie die ID für Ihre physische Netzwerkschnittstelle identifiziert haben, können Sie eine virtuelle Netzwerkschnittstelle (VNI) einrichten. Gehen Sie wie folgt vor, um eine VNI einzurichten. Stellen Sie sicher, dass Sie die erforderlichen Aufgaben ausführen, bevor Sie eine VNI erstellen.

Erstellen einer VNI und Zuordnen einer IP-Adresse

1. Führen Sie den Befehl `snowballEdge create-virtual-network-interface` aus. 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

           //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
   ```

   Der Befehl gibt eine JSON-Struktur zurück, die die IP-Adresse enthält. Notieren Sie sich diese IP-Adresse für den `ec2 associate-address` AWS CLI Befehl später im Prozess.

   Wenn Sie diese IP-Adresse benötigen, können Sie sie mit dem `snowballEdge describe-virtual-network-interfaces` Snowball Edge-Client-Befehl oder dem `-aws ec2 describe-addresses`AWS CLIBefehl abrufen.
2. Um Ihre neu erstellte IP-Adresse Ihrer Instance zuzuordnen, verwenden Sie den folgenden Befehl 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://Snow Family device physical IP address:8008
```

Einrichten einer Direct Network Interface (DNI)

> **Note**
>
> Das Feature für direkte Netzwerkschnittstellen ist am oder nach dem 12. Januar 2021 verfügbar und ist in allen verfügbar, in AWS-Regionen denen Snow Family-Geräte verfügbar sind.

Voraussetzungen

Bevor Sie eine Direct Network Interface (DNI) einrichten, müssen Sie die Aufgaben im Abschnitt Voraussetzungen ausführen.

1. Führen Sie die erforderlichen Aufgaben aus, bevor Sie die DNI einrichten. Anweisungen finden Sie unter Voraussetzungen.
2. Darüber hinaus müssen Sie eine Instance auf Ihrem Gerät starten, eine VNI erstellen und sie der Instance zuordnen. Anweisungen finden Sie unter Einrichten einer Virtual Network Interface (VNI).

> **Note**
>
> Wenn Sie Ihrem vorhandenen Gerät direkte Netzwerke hinzugefügt haben, indem Sie ein in-the-field Software-Update durchgeführt haben, müssen Sie das Gerät zweimal neu starten, um die Funktion vollständig zu aktivieren.

Erstellen einer DNI und Zuordnen einer IP-Adresse

1. Erstellen Sie eine direkte Netzwerkschnittstelle und fügen Sie sie an die Amazon EC2-compatible Instance an, indem Sie den folgenden Befehl ausführen. Sie benötigen die MAC-Adresse des Geräts für den nächsten Schritt.

```
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 Anforderung gesendet werden soll. Der Endpunkt für Ihre Geräte ist eine URL, die das `https` Schema gefolgt von einer IP-Adresse verwendet. 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-compatible Instance-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. Sie können die physischen Netzwerkschnittstellen ermitteln, die auf Ihrem Snowball Edge verfügbar sind, indem Sie den `describe-device` Befehl verwenden.

`--vlan <vlanId>` Legen Sie das zugewiesene VLAN für die Schnittstelle fest (optional). Wenn angegeben, wird der gesamte von der Schnittstelle gesendete Datenverkehr mit der angegebenen VLAN-ID markiert. Eingehender Datenverkehr wird nach der angegebenen VLAN-ID gefiltert und alle VLAN-Tags werden entfernt, bevor sie an die Instance übergeben werden.

2. Wenn Sie Ihre DNI in Schritt 1 nicht mit einer Instance verknüpft haben, können Sie sie verknüpfen, indem Sie den Aktualisieren einer Direct Network Interface Befehl ausführen.
3. Nachdem Sie eine DNI erstellt und mit Ihrer EC2-compatible Instance verknüpft haben, müssen Sie zwei Konfigurationsänderungen in Ihrer Amazon EC2-compatible Instance vornehmen.

   - Stellen Sie zunächst sicher, dass Pakete, die für die VNI bestimmt sind, die der EC2-compatible Instance zugeordnet ist, über eth0 gesendet werden.
   - Die zweite Änderung konfiguriert Ihre direkte Netzwerkschnittstelle so, dass beim Start entweder DCHP oder statische IP verwendet wird.

   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=$(LANG=C ip -o link | awk -F ': ' -vIGNORECASE=1 '!/link\/
ieee802\.11/ && /'"$DNI_MAC"'/ { print $2 }')
ip link set $CURRENT_DEVICE_NAME name $DNI

# Make all changes live.
systemctl restart network
```

Herstellen einer Verbindung mit Datenverarbeitungs-Instances auf einem Snow Family-Gerät über SSH

Um Secure Shell (SSH) zu verwenden, um eine Verbindung zu Datenverarbeitungs-Instances auf einem Snow Family-Gerät herzustellen, haben Sie die folgenden Möglichkeiten, einen SSH-Schlüssel bereitzustellen oder zu erstellen.

- Sie können den SSH-Schlüssel für das Amazon Machine Image (AMI) angeben, wenn Sie einen Auftrag zum Bestellen eines Geräts erstellen. Weitere Informationen finden Sie unter Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden.
- Sie können den SSH-Schlüssel für das AMI angeben, wenn Sie ein Image für eine virtuelle Maschine erstellen, das auf ein Snow Family-Gerät importiert werden soll. Weitere Informationen finden Sie unter Importieren eines Images einer virtuellen Maschine auf ein Snow Family-Gerät.
- Sie können ein Schlüsselpaar auf dem Snow Family-Gerät erstellen und eine Instance mit diesem lokal generierten öffentlichen Schlüssel starten. Weitere Informationen finden Sie unter Erstellen eines Schlüsselpaars mit Amazon EC2 im Amazon EC2-Benutzerhandbuch für Linux-Instances.

So stellen Sie über SSH eine Verbindung zu einer Instance her

1. Stellen Sie sicher, dass Ihr Gerät eingeschaltet, mit dem Netzwerk verbunden und entsperrt ist. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem lokalen Netzwerk.
2. Stellen Sie sicher, dass Sie die Netzwerkeinstellungen für Ihre Datenverarbeitungs-Instances konfiguriert haben. Weitere Informationen finden Sie unter Netzwerkkonfiguration für Datenverarbeitungs-Instances.
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 Netzwerkkonfiguration für Datenverarbeitungs-Instances einrichten.

   ```
   ssh -i path/to/PEM/key/file instance-user-name@192.0.2.0
   ```

   Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance mit SSH im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Übertragen von Daten von EC2-compatible Compute Instances in S3-Buckets am selben Snowball-Edge

Sie können Daten zwischen Datenverarbeitungs-Instances und Amazon S3-Buckets auf demselben Snowball-Edge-Gerät übertragen. Dazu verwenden Sie die unterstützten AWS CLI Befehle und die entsprechenden Endpunkte. Angenommen, Sie möchten Daten aus einem Verzeichnis in meiner `sbe1.xlarge` Instance in den Amazon S3-Bucket `myBucket` auf demselben Gerät verschieben. Angenommen, Sie verwenden den Amazon S3-kompatiblen Speicher auf dem Endpunkt für Snow-Family-Geräte `https://S3-object-API-endpoint:443`. Sie führen die folgenden Schritte aus.

> **Note**
>
> Diese Vorgehensweise funktioniert nur, wenn Sie die Anweisungen unter Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden befolgt haben.

So übertragen Sie Daten zwischen einer Datenverarbeitungs-Instance und einem Bucket auf demselben Snowball-Edge

1. Verwenden Sie SSH, um eine Verbindung zu Ihrer Datenverarbeitungs-Instance herzustellen.
2. Laden Sie das AWS CLI herunter und installieren Sie es. 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 AWS CLI auf Ihrer Computing-Instance so, dass sie mit dem Amazon S3-Endpunkt auf dem Snowball Edge funktioniert. Weitere Informationen finden Sie unter Abrufen und Verwenden lokaler Amazon S3-Anmeldeinformationen.
4. Verwenden Sie den unterstützten Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten, um Daten zu übertragen. Beispielsweise:

```
aws s3 cp ~/june2018/results s3://myBucket/june2018/results --recursive --endpoint
 https://S3-object-API-endpoint:443
```

Snowball Edge Client-Befehle für Compute Instances

Der Snowball Edge-Client ist eine eigenständige Terminalanwendung, die Sie auf Ihrem lokalen Server ausführen können. Sie können damit einige administrative Aufgaben auf Ihrem Snowball Edge-Gerät oder Cluster von Geräten ausführen. Weitere Informationen zur Verwendung des Snowball Edge-Clients, einschließlich des Startens und Stoppens von Services, finden Sie unter Verwenden des Snowball Edge Clients.

Im Folgenden finden Sie Informationen zu den Snowball Edge-Clientbefehlen, die für Rechen-Instances spezifisch sind, einschließlich Beispiele für die Verwendung.

Eine Liste der Amazon EC2-compatible Befehle, die Sie auf Ihrem AWS Snowball Edge Gerät verwenden können, finden Sie unter Unterstützte AmazonEC2-compatible AWS CLI Befehle auf einem Snowball-Edge.

Erstellen einer Startkonfiguration zum automatischen Starten von Amazon EC2-compatible Instances

Um Amazon EC2-compatible Rechen-Instances automatisch auf Ihrem AWS Snowball Edge Gerät 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]
```

Aktualisieren einer Startkonfiguration zum Autostart von EC2-compatible Instances

Verwenden Sie den `snowballEdge update-autostart-configuration` Befehl , um eine vorhandene 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 Startkonfiguration zum Autostart von EC2-compatible Instances

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
```

Auflisten von Startkonfigurationen zum Autostart von EC2-compatible Instances

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

Um eine Rechen-Instance auf Ihrem Snowball Edge auszuführen oder die NFS-Schnittstelle auf Ihrem Snowball Edge zu starten, erstellen Sie zunächst eine virtuelle Netzwerkschnittstelle (VNIC). Jeder Snowball Edge verfügt über drei Netzwerkschnittstellen (NICs), die physischen Netzwerkschnittstellencontroller für das Gerät. Es handelt sich dabei um die RJ45-, SFP- und QSFP-Ports auf der Rückseite des Geräts.

Alle VNICs basieren auf einer physischen Schnittstelle. Sie können mit jeder NIC beliebig viele VNICs verbinden. 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 konfiguriertem 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 von 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"
  }
}
```

Beschreibung Ihrer virtuellen Netzwerkschnittstellen

Um die zuvor auf Ihrem Gerät erstellten VNICs zu beschreiben, verwenden Sie den Befehl `snowballEdge describe-virtual-network-interfaces`. Im Folgenden wird gezeigt, wie Sie ihn verwenden.

Verwendung

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfiguriertem 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 von 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"
  },{
    "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"
  }
]
```

Aktualisieren einer virtuellen Netzwerkschnittstelle

Nach der Erstellung einer virtuellen Netzwerkschnittstelle (Virtual Network Interface, VNIC) können Sie ihre Konfiguration mit dem Befehl `snowballEdge update-virtual-network-interface`

aktualisieren. Nach der Bereitstellung des Amazon-Ressourcennamens (ARN) für eine bestimmte VNIC geben Sie nur für die Elemente Werte ein, die Sie aktualisieren.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfiguriertem 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

Um eine virtuelle Netzwerkschnittstelle zu löschen, können Sie den Befehl `snowballEdge delete-virtual-network-interface` verwenden.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfiguriertem 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 Amazon EC2-compatible Endpunkts

Im Folgenden finden Sie eine Übersicht über den Amazon EC2-compatible Endpunkt. Mit diesem Endpunkt können Sie Ihre Amazon Machine Images (AMIs) und Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten.

Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt

Wenn Sie die verwenden, AWS CLI um einen Befehl an das AWS Snowball Edge Gerät auszugeben, können Sie angeben, dass der Endpunkt der Amazon EC2-compatible Endpunkt ist. 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 vom 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 Amazon EC2-compatible Endpunkt

1. Verbinden Sie 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 von einem Terminal in Ihrem Netzwerk sicher, dass Sie den Snowball Edge 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.
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 AmazonEC2-compatible AWS CLI Befehle auf einem Snowball-Edge

Sie können Ihre Datenverarbeitungs-Instances auf einem Snow Family-Gerät über einen Amazon EC2-compatible Endpunkt verwalten. Diese Art von Endpunkt unterstützt viele der Amazon EC2-CLI-Befehle und -Aktionen der -AWSSDKs. SDKs Weitere Informationen zum Installieren und Einrichten der AWS CLI, einschließlich der Angabe, für welche AWS-Regionen Sie AWS CLI Aufrufe tätigen möchten, finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Liste der unterstützten AmazonEC2-compatible 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 – Fügt ein Amazon EBS-Volume an eine angehaltene oder ausgeführte Instance auf Ihrem Gerät an und stellt es der Instance mit dem angegebenen Gerätenamen bereit.
  - --device `value` – Der Gerätename.
  - --instance-id – Die ID einer Amazon EC2-compatibleInstance.
  - --volume-id `value` – Die ID des EBS-Volumes.
- authorize-security-group-egress – Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln für die Verwendung mit einem Snowball-Edge-Gerät hinzu. Insbesondere diese Aktion erlaubt Instances, Datenverkehr an eine oder mehrere IPv4-CIDR-Zieladressbereiche zu senden. Weitere Informationen finden Sie unter Sicherheitsgruppen in Snowball Edge-Geräten.
  - --group-id `value` – Die ID der Sicherheitsgruppe
  - [--ip-permissions `value`] – 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-name `value`] – Der Name der Sicherheitsgruppe.
  - [--group-id `value`] – Die ID der Sicherheitsgruppe
  - [--ip-permissions `value`] – 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.
  - [--port `value`] – Für TCP oder UDP der Bereich der zuzulassenden Ports. 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.
  - [--cidr `value`] – 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-description `string`] – Eine Beschreibung für die erste Version der Startvorlage.
- --endpoint `snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.

- 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-version `string`] – 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-description `string`] – Eine Beschreibung für die erste Version der Startvorlage.
- --endpoint `snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.

- create-tags – Fügt ein oder mehrere Tags für die angegebene Ressource hinzu oder überschreibt sie. 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 einer Instance auf Ihrem Gerät zugeordnet werden kann.
  - [-Größe `value`] – Die Größe des Volumes in GiBs, das zwischen 1 GiB und 1 TB (1000) liegen kann GiBs.
  - [--snapshot-id `value`] – Der Snapshot, aus dem das Volume erstellt werden soll.
  - [--volume-type `value`] – Der Volume-Typ. Wenn kein Wert angegeben wird, lautet der Standardwert `sbg1`. Die folgenden Werte sind möglich:
    - `sbg1` für magnetische Volumes
    - `sbp1` für SSD-Volumes
  - [--tag-specification `value`] – Eine Liste von Tags, die während 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 Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.
- 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 (list) `"string" "string"` – Die Versionsnummern einer oder mehrerer zu löschender Startvorlagenversionen.
  - --endpoint `snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.
- 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, Datenverarbeitungs-Instance, Startvorlage oder Sicherheitsgruppe).
- delete-volume – Löscht das angegebene Amazon EBS-Volume. Das Volume muss den `available`-Status aufweisen (nicht an eine Instance angefügt).
  - --volume-id `value` – Die ID des Volumes.
- describe-addresses – Beschreibt eine oder mehrere Ihrer virtuellen IP-Adressen, die derselben Anzahl von Instances auf Ihrem Gerät zugeordnet `sbe` sind.
  - --public-ips – Eine oder mehrere der virtuellen IP-Adressen, die Ihren Instances zugeordnet sind.
- describe-images – Beschreibt eines oder mehrere der Images (AMIs), die Ihnen zur Verfügung stehen. Images, die Ihnen zur Verfügung stehen, werden dem Snowball Edge-Gerät während 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 IDs einer oder mehrerer `sbe`-Instances, die auf dem Gerät gestoppt wurden.
  - --page-size – Die Größe jeder Seite, die im Aufruf enthalten sein 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, das angibt, 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 aller Ihrer Instances. Standardmäßig werden nur ausgeführte Instances beschrieben, es sei denn, Sie geben ausdrücklich an, den Status aller Instances zurückzugeben. Der Instance-Status umfasst die folgenden Komponenten:
  - Statusprüfungen – Snow-Gerät führt Statusprüfungen an ausgeführten Amazon EC2-compatible Instances durch, um Hardware- und Softwareprobleme zu identifizieren.
  - Instance-Status – Sie können Ihre Instances ab dem Zeitpunkt, an dem Sie sie starten, bis zu ihrer Beendigung verwalten.

  Mit diesem Befehl werden die folgenden Filter unterstützt.

  - `[--filters]` (Liste)

    Die Filter.

    - `instance-state-code` – Der Code für den Instance-Status als 16-Bit-Ganzzahl ohne Vorzeichen. Das hohe Byte wird für interne Service-Berichte verwendet und sollte ignoriert werden. Das niedrige Byte wird basierend auf dem repräsentierten Status festgelegt. Die gültigen Werte sind 0 (anstehend), 16 (ausgeführt), 32 (Herunterfahren), 48 (beendet), 64 (beendet) und 80 (beendet).
    - `instance-state-name` – Der Status der Instance (`pending` | `running` | | `shutting-down` | `terminated` `stopping` | | `stopped`).

  - `instance-status.reachability` – Filtert nach dem Instance-Status, bei dem der Name `reachability` (`passed` | `failed` | | `initializing` | `insufficient-data`) lautet.
  - `instance-status.status` – Der Status der Instance (ok | `impaired` | `initializing` | `insufficient-data` | | `not-applicable`).
  - `system-status.reachability` – Filtert den Systemstatus, bei dem der Name erreichbar ist (`passed` | `failed` | `initializing` | | `insufficient-data`).
  - `system-status.status` – Der Systemstatus der Instance (ok | `impaired` | | `initializing` `insufficient-data` | | `not-applicable`).
- JSON-Syntax:

```
[
  {
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
]
```

- `[--instance-ids]` (Liste)

  Die Instance-IDs .

  Standard: Beschreibt alle Ihre Instances.
- `[--dry-run|--no-dry-run]` (boolean)

  Prüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anforderung tatsächlich zu stellen, und gibt eine Fehlerantwort aus. Wenn Sie über die erforderlichen Berechtigungen verfügen, lautet die Fehlerantwort `DryRun0peration`.

  Andernfalls ist es `Unauthorized0peration`.
- `[--include-all-instances | --no-include-all-instances]` (boolean)

  Bei `true`schließt den Zustand für alle Instances ein. Wenn `false`, enthält der Zustand nur für ausgeführte Instances.

  Standard: `false`
- `[--page-size]` (Ganzzahl) – Die Größe jeder Seite, die in den Aufruf aufgenommen 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]` (Ganzzahl) – 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]` (Zeichenfolge) – 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 Ergebnisdatensatz abzurufen.

  Geben Sie in der Anfrage entweder die Startvorlagen-IDs oder die Startvorlagennamen an.

  - --launch-template-ids (Liste) `"string" "string"` – Eine Liste von IDs der Startvorlagen.
  - --launch-template-names (Liste) `"string" "string"` – Eine Liste von Namen für die Startvorlagen.
  - --page-size – Die Größe jeder Seite, die in den Aufruf aufgenommen 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, das angibt, 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 Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.

- describe-launch-template-versions – Beschreibt eine oder mehrere Versionen einer angegebenen 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 Ergebnisdatensatz abzurufen.

  Geben Sie in der Anfrage entweder die Startvorlagen-IDs oder die Startvorlagennamen an.

  - --launch-template-id `string` – Die ID der Startvorlage.
  - --launch-template-name `string` – Ein Name für die Startvorlage.
  - [--versions (list) `"string" "string"`] – Die Versionsnummern einer oder mehrerer zu löschender Startvorlagenversionen.
  - [--min-version `string`] – Die Versionsnummer, nach der Startvorlagenversionen beschrieben werden sollen.
  - [--max-version `string`] – Die Versionsnummer, bis zu der Startvorlagenversionen beschrieben werden sollen.
  - --page-size – Die Größe jeder Seite, die in den Aufruf aufgenommen 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, das angibt, 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 Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.
- 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 Ergebnisdatensatz abzurufen.

  - [--group-name `value`] – Der Name der Sicherheitsgruppe.
  - [--group-id `value`] – Die ID der Sicherheitsgruppe.
  - [-page-size `value`] – Die Größe jeder Seite, die im AWS Serviceaufruf abgerufen werden soll. Diese Größe 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 des AWS Services und zum Abrufen weniger Elemente in jedem Aufruf. Dieser Ansatz kann dazu beitragen, ein Timeout der AWS Service-Aufrufe zu verhindern. Anwendungsbeispiele finden Sie unter Paginierung im AWS Command Line Interface -Benutzerhandbuch.
  - [--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. Verwenden Sie das -`NextToken`Antwortelement nicht direkt außerhalb der AWS CLI. Anwendungsbeispiele finden Sie unter Paginierung im AWS Command Line Interface -Benutzerhandbuch.
  - [--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. Anwendungsbeispiele finden Sie unter Paginierung im AWS Command Line Interface -Benutzerhandbuch.
- 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 `value`] – Eine oder mehrere Volume-IDs .
- detach-volume – Trennt ein Amazon-EBS-Volume von einer angehaltenen oder ausgeführten Instance.
  - [--device `value`] – Der Gerätename.
  - [--instance-id] – Die ID einer Amazon EC2Ziel-Instance.
  - --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 Instance 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 Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.
- 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 Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt.
- 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-id `value`] – Die ID der Sicherheitsgruppe
  - [--ip-permissions `value`] – Ein oder mehrere Sätze von IP-Berechtigungen.
- revoke-security-group-ingress – Widerruft eine oder mehrere Eingangsregeln für eine Sicherheitsgruppe. Wenn Sie `revoke-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
  - [--group-name `value`] – Der Name der Sicherheitsgruppe.
  - [--group-id `value`] – Die ID der Sicherheitsgruppe.
  - [--ip-permissions `value`] – 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.
  - [--port `value`] – Für TCP oder UDP der Bereich der zuzulassenden Ports. 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.
  - [--cidr `value`] – Der CIDR-IP-Bereich.
- run-instances – Startet eine Reihe von Rechen-Instances mithilfe einer Snowball-AMI-ID für ein AMI.

  > **Note**
  >
  > Je nach Größe und Typ der Instance kann es bis zu einer halben Stunde dauern, bis eine Rechen-Instance auf einem Snowball-Edge gestartet wird.

  - [-- –block-device-mappings `(list)`] Die Blockgerät-Zuweisungseinträge. 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": "sbp1"|"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 Aufrufen von erhalten können`describe-images`. Um eine Instance zu starten, wird ein AMI benötigt.
- -- InstanceInitiatedShutdownBehavior – Wenn Sie ein Herunterfahren Ihrer Instance einleiten (mit einem Befehl wie Herunterfahren oder Ausschalten), wird die Instance standardmäßig angehalten. 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 von der Instance initiierten Herunterfahrverhaltens im Amazon EC2-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 mit erstellenCreateSecurityGroup. Wenn kein Wert angegeben wird, wird die ID für die Standard-Sicherheitsgruppe den erstellten Instances zugewiesen.

- --tag-specifications – Die Tags, die während des Starts auf die Ressourcen angewendet werden sollen. Instances können nur beim Start markiert werden. Die angegebenen Tags werden auf alle Instances angewendet, die beim Start erstell werden. Um eine Ressource mit einem Tag zu versehen, nachdem sie erstellt wurde, verwenden Sie `create-tags`.
- --user-data – Die Benutzerdaten, die der Instance zur Verfügung gestellt werden sollen. Wenn Sie die AWS CLI verwenden, wird für Sie die Base64-Kodierung durchgeführt und Sie können den Text aus einer Datei laden. Andernfalls müssen Sie einen base64-kodierten Text bereitstellen.
- --key-name (Zeichenfolge) – Der Name des Schlüsselpaars. Sie können ein Schlüsselpaar mit `CreateKeyPair` oder erstellen`ImportKeyPair`.

  > **Warning**
  >
  > Wenn Sie kein Schlüsselpaar angeben, können Sie keine Verbindung mit der Instance herstellen, es sei denn, Sie wählen ein AMI aus, das so konfiguriert ist, dass Benutzern eine andere Anmeldemethode erlaubt wird.

- start-instances – Startet eine `sbe` Instance, die Sie zuvor angehalten haben. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.
  - --instance-ids – Die IDs einer oder mehrerer `sbe`-Instances, die auf dem Gerät gestoppt wurden.
- stop-instances – Stoppt eine ausgeführte `sbe` Instance. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.
  - --Instance-IDs: Die IDs einer oder mehrerer `sbe`-Instances, die auf dem Gerät gestoppt werden sollen.
- terminate-instances – Fügt eine oder mehrere Instances herunter. Dieser Vorgang ist idempotent. Wenn Sie eine Instance mehr als einmal beenden, ist jeder Aufruf erfolgreich. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Die Daten werden jedoch gelöscht, wenn die Instance beendet wird.

  > **Note**
  >
  > Wenn Sie einen Befehl wie `shutdown` oder `poweroff` zum Starten des Herunterfahrens über Ihre Instance verwenden, wird die Instance standardmäßig angehalten. Sie können jedoch das `InstanceInitiatedShutdownBehavior` Attribut verwenden, um dieses

Verhalten so zu ändern, dass diese Befehle Ihre Instance beenden. Weitere Informationen finden Sie unter Ändern des von der Instance initiierten Herunterfahrverhaltens im Amazon EC2-Benutzerhandbuch für Linux-Instances.

- --instance-ids – Die IDs einer oder mehrerer `sbe` Instances, die auf dem Gerät beendet werden sollen. Alle für diese Instances gespeicherten Daten gehen verloren.

- create-key-pair – Erstellt 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 privater PKCS#1-Schlüssel zurückgegeben. Wenn bereits ein Schlüssel mit dem angegebenen Namen vorhanden ist, gibt Amazon EC2 einen Fehler zurück.
  - --key-name (Zeichenfolge) – Ein eindeutiger Name für das Schlüsselpaar.

    Einschränkungen: Bis zu 255 ASCII-Zeichen.
  - [--tag-specifications] (Liste) – Die Tags, die auf das neue Schlüsselpaar angewendet werden sollen.

```
{
    "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
      ...
    ]
  }
  ...
```

- import-key-pair –
  - --key-name (Zeichenfolge) – Ein eindeutiger Name für das Schlüsselpaar.

    Einschränkungen: Bis zu 255 ASCII-Zeichen.
  - --public-key-material (blob) – Der öffentliche Schlüssel. Für API-Aufrufe muss der Text base64-kodiert sein. Bei Befehlszeilen-Tools wird die Base64-Codierung für Sie durchgeführt.
  - [--tag-specifications] (Liste) – Die Tags, die auf das neue Schlüsselpaar 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 Schlüsselpaars.
  - key-name – Der Name des Schlüsselpaars.
  - 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 ist, unabhängig vom Tag-Wert.
  - [--tag-specifications] (Liste) – Die Tags, die auf das neue Schlüsselpaar angewendet werden sollen.
  - tag :key – Die Schlüssel-Wert-Kombination eines Tags, das der Ressource zugewiesen ist. 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] (Liste) – Die Schlüsselpaarnamen.

  Standard: Beschreibt alle Ihre Schlüsselpaare.

- [--key-pair-ids] (Liste) – Die IDs der Schlüsselpaare.
- delete-key-pair –
  - [--key-name] (Zeichenfolge) – Der Name des Schlüsselpaars.

- [--key-pair-id] (Zeichenfolge) – Die ID des Schlüsselpaars.

Unterstützte Amazon EC2-compatible API-Operationen

Im Folgenden finden Sie AmazonEC2-compatible API-Operationen, die Sie mit einem Snowball Edge verwenden können, mit Links zu ihren Beschreibungen in der Amazon EC2-API-Referenz. Amazon EC2-compatible API-Aufrufe erfordern Signature Version 4 (SigV4)-Signatur. Wenn Sie die AWS CLI oder ein AWS -SDK verwenden, um diese API-Aufrufe durchzuführen, wird die SigV4-Signatur für Sie erledigt. Andernfalls müssen Sie Ihre eigene SigV4 Signatur-Lösung implementieren. Weitere Informationen finden Sie unter Abrufen und Verwenden lokaler Amazon S3-Anmeldeinformationen.

- 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 für die Verwendung mit einem Snowball Edge-Gerät hinzu. Insbesondere diese Aktion erlaubt Instances, Datenverkehr an eine oder mehrere IPv4-CIDR-Zieladressbereiche zu senden.
- AuthorizeSecurityGroupIngress – Fügt einer Sicherheitsgruppe eine oder mehrere Eingangsregeln hinzu. Beim Aufruf AuthorizeSecurityGroupIngressvon müssen Sie einen Wert für `GroupName` oder angeben`GroupId`.
- 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 Ergebnisdatensatz abzurufen.

- DescribeTags – Mit diesem Befehl werden die folgenden Filter unterstützt:
  - `resource-id`
  - `resource-type` – Nur AMI oder Rechen-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 Aufruf RevokeSecurityGroupIngressvon müssen Sie einen Wert für `group-name` oder angeben`group-id`.
- RunInstances –

  > **Note**
  >
  > Je nach Größe und Typ der Instance kann es bis zu einer halben Stunde dauern, bis eine Rechen-Instance auf einem Snowball Edge gestartet wird.

- StartInstances
- StopInstances – Ressourcen, die einer angehaltenen Instance zugeordnet sind, bleiben bestehen. Sie können die Instance beenden, um diese Ressourcen freizugeben. Alle zugehörigen Daten werden jedoch gelöscht.

- TerminateInstances

Automatisches Starten von Amazon EC2-compatible Instances mit Startvorlagen

Sie können Ihre AmazonEC2-compatible Instances automatisch auf Ihrem AWS Snowball Edge Gerät mithilfe von Startvorlagen und Snowball-Edge-Client-Startkonfigurationsbefehlen starten.

Eine Startvorlage enthält die Konfigurationsinformationen, die zum Erstellen einer Amazon EC2-compatible 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-compatible Instance auf Ihrem Snowball Edge starten.

Wenn Sie Autostart-Konfigurationen auf Ihrem Snowball Edge verwenden, konfigurieren Sie die Parameter, mit denen Ihre AmazonEC2-compatible Instance beginnen soll. Nachdem Ihr Snowball Edge konfiguriert wurde und Sie ihn neu starten und entsperren, verwendet er 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 Instance-Starts (nach geplanten oder ungeplanten Neustarts) erfolgen automatisch, nachdem Ihr Gerät entsperrt wurde.

Eine Startvorlage kann die Amazon Machine Image (AMI)-ID, den Instance-Typ, die Benutzerdaten, Sicherheitsgruppen und Tags für eine Amazon EC2-compatible Instance angeben, wenn Sie diese Instance starten. Eine Liste mit unterstützten Instance-Typen finden Sie unter Kontingente für Datenverarbeitungs-Instances auf einem Snowball-Edge-Gerät.

Gehen Sie wie folgt vor, um EC2-compatible Instances automatisch auf Ihrem Snowball Edge zu starten:

1. Wenn Sie Ihr AWS Snowball Edge Gerät bestellen, erstellen Sie einen Auftrag, um ein Snow Family-Gerät mit Datenverarbeitungs-Instances zu bestellen. Weitere Informationen finden Sie unter Erstellen eines Datenverarbeitungsauftrags.

2. Nachdem Sie Ihren Snowball Edge empfangen haben, entsperren Sie ihn.
3. Verwenden Sie den EC2-compatible API-Befehl `aws ec2 create-launch-template` , um eine Startvorlage zu erstellen.
4. Verwenden Sie den Snowball Edge-Client-Befehl`snowballEdge create-autostart-configuration`, um Ihre EC2-compatible Instance-Startvorlage an Ihre Netzwerkkonfiguration zu binden. Weitere Informationen finden Sie unter Erstellen einer Startkonfiguration zum automatischen Starten von Amazon EC2-compatible Instances.
5. Starten Sie Ihr Gerät neu und entsperren Sie es dann. Ihre EC2-compatible Instances werden automatisch mit den Attributen gestartet, die in Ihrer Startvorlage und Ihrem Snowball-Edge-Clientbefehl angegeben sind`create-autostart-configuration`.

Um den Status Ihrer laufenden Instances anzuzeigen, verwenden Sie den EC2-compatible API-Befehl `describe-autostart-configurations`.

> **Note**
>
> Es gibt keine Konsolen- oder Auftragsverwaltungs-API für die AWS Snowball Unterstützung von Startvorlagen. Sie verwenden EC2-compatible und Snowball Edge-Client-CLI-Befehle, um EC2-compatible Instances automatisch auf Ihrem AWS Snowball Edge Gerät zu starten.

Verwenden von Instance Metadata Service für Snow mit Amazon EC2-compatible Instances

IMDS for Snow stellt Instance Metadata Service (IMDS) für AmazonEC2-compatible Instances in Snow bereit. Instance-Metadaten sind Kategorien von Informationen zu Instances. Sie enthält Kategorien wie Hostname , Ereignisse und Sicherheitsgruppen . Mit IMDS für Snow können Sie Instance-Metadaten verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Starten Ihrer Amazon-ECEC2-compatible angegeben haben. Sie können beispielsweise IMDS für Snow verwenden, um Parameter für die Konfiguration Ihrer Instance anzugeben oder diese Parameter in ein einfaches Skript aufzunehmen. Sie können generische AMIs erstellen und mit Hilfe von Benutzerdaten die beim Start ausgelieferten Konfigurationsdateien ändern.

Weitere Informationen zu Instance-Metadaten und Benutzerdaten sowie SnowEC2-compatible Instances finden Sie unter Unterstützte Instance-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**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des Instance-Metadatenservices verwendet: 169.254.169.254. Das Abrufen von Instance-Metadaten mit der Link-lokalen IPv6-Adresse wird nicht unterstützt.

Themen

IMDS-Versionen

Sie können mit IMDS Version 2 oder IMDS Version 1 von einer laufenden Instance aus auf Instance-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 IMDSv1, IMDSv2 oder beides verwenden. Dies hängt auch vom Typ des AMI ab, das in der EC2-compatible Instance ausgeführt wird. Einige AMIs, z. B. solche, auf denen Ubuntu 20.04 ausgeführt wird, erfordern IMDSv2. Der Instance-Metadaten-Service unterscheidet zwischen IMDSv1- und IMDSv2-Anforderungen basierend auf dem Vorhandensein von - `PUT` oder -`GET`Headern. IMDSv2 verwendet beide Header. IMDSv1 verwendet nur den -`GET`Header.

AWS empfiehlt die Verwendung von IMDSv2 anstelle von IMDSv1, da IMDSv2 eine höhere Sicherheit bietet. Weitere Informationen finden Sie unter Erweitern Sie den EC2-Instance-Metadata-Service, um Abwehr von offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen an EC2-Instance-Metadata-Service.

IMDSv2

IMDSv2 verwendet sitzungsorientierte Anfragen. Bei sitzungsorientierten Anforderungen erstellen Sie ein 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 zukünftige Anfragen erstellen.

Im folgenden Beispiel werden ein Linux-Shell-Skript und IMDSv2 verwendet, um die Metadatenelemente der Instance der obersten Ebene abzurufen. Dieses Beispiel:

1. Erstellt mithilfe der PUT Anforderung ein Sitzungstoken von sechs Stunden (21 600 Sekunden).
2. Speichert den Sitzungstoken-Header in einer Variablen mit dem Namen `TOKEN`.
3. Fordert die Metadatenelemente der obersten Ebene mit dem Token an.

Sie können zwei Befehle separat ausführen oder kombinieren.

Separate Befehle

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 mit dem folgenden Befehl 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/
```

Kombinierte Befehle

Sie können das Token speichern und die Befehle kombinieren. Das folgende Beispiel kombiniert die beiden oben genannten Befehle und speichert den Sitzungstoken-Header in einer Variablen namens `TOKEN`.

> **Note**
>
> Wenn beim Erstellen des Tokens ein Fehler auftritt, wird eine Fehlermeldung in der Variablen anstelle eines gültigen Tokens gespeichert und der Befehl funktioniert nicht.

Example kombinierte Befehle

```
    [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 der , die im vorherigen Beispiel `$TOKEN` erstellt wurde.

Example Wiederverwenden eines Tokens

```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
```

Wenn Sie IMDSv2 verwenden, um Instance-Metadaten anzufordern, muss die Anforderung den folgenden Regeln entsprechen:

1. Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance-Metadaten-Service zu starten. Die PUT-Anfrage gibt ein Token zurück, das in nachfolgenden GET-Anfragen an den Instance-Metadaten-Service enthalten sein muss. Das Token wird für den Zugriff auf Metadaten mit IMDSv2 benötigt.
2. Nehmen Sie das Token in alle GET-Anfragen an den Instance-Metadaten-Service auf.
   a. Das Token ist ein Instance-spezifischer Schlüssel. Das Token ist auf anderen EC2-compatible Instances nicht gültig und wird abgelehnt, wenn Sie versuchen, es außerhalb der Instance 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.

In PUT-Instance-Metadatenanfragen sind HTTP GET- und HEAD-Methoden zulässig. -Anfragen werden abgelehnt, wenn sie einen X-Forwarded-For-Header enthalten.

Standardmäßig hat die Antwort auf -PUTAnfragen ein Antwort-Hop-Limit (Time to Live) von 1 auf IP-Protokollebene. IMDS für Snow kann das Hop-Limit für PUT Antworten nicht ändern.

IMDSv1

IMDSv1 verwendet das Anfrage-Antwort-Modell. Um Instance-Metadaten anzufordern, senden Sie eine GET Anforderung an den Instance-Metadaten-Service.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Abrufen von Instance-Metadaten

Ihre Instance-Metadaten sind von Ihrer laufenden Instance aus verfügbar, sodass Sie keine Amazon EC2-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.

Um alle Kategorien von Instance-Metadaten innerhalb einer laufenden Instance anzuzeigen, verwenden Sie den folgenden IPv4-URI:

```
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.

Antworten und Fehlermeldungen

Alle Instance-Metadaten werden als Text zurückgegeben (HTTP-Inhaltstyp `text/plain`).

Eine Anforderung für eine bestimmte Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode 404 – Not Found zurück, wenn die Ressource nicht verfügbar ist.

Eine Anforderung für eine allgemeine Metadatenressource (wenn der URI mit einem / Zeichen endet) gibt eine Liste der verfügbaren Ressourcen oder einen HTTP-Fehlercode 404 - Not Found zurück, wenn es keine solche Ressource gibt. Die Listenelemente befinden sich in separaten Zeilen, die durch Zeilenvorschübe (ASCII-Zeichencode 10) beendet werden.

Für Anforderungen, die mit IMDSv1 gestellt werden, können die folgenden HTTP-Fehlercodes zurückgegeben werden:

- 400 – Fehlende oder ungültige Parameter – Die `PUT` Anforderung ist ungültig.
- 401 – Nicht autorisiert – Die `GET` Anforderung verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.

- 403 – Verboten – Die Anforderung ist nicht zulässig oder der Instance-Metadatenservice ist deaktiviert.

Beispiele für das Abrufen von Instance-Metadaten mit IMDSv1 und IMDSv2

Die folgenden Beispiele enthalten Befehle, die Sie für eine Linux-Instance verwenden können.

Example Abrufen der verfügbaren Versionen der Instance-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://192.0.2.0/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v
 http://192.0.2.0/
   % 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 192.0.2.0...
   * TCP_NODELAY set
   * Connected to 192.0.2.0 (192.0.2.0) port 80 (#0)
   > GET / HTTP/1.1
   > Host: 192.0.2.0
   > 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://192.0.2.0/
    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 Abrufen der Top-Level-Metadatenelemente

In diesem Beispiel werden die Metadatenelemente der obersten Ebene abgerufen. Informationen zu Metadaten der obersten Ebene finden Sie unter Unterstützte Instance-Metadaten und Benutzerdaten in diesem Handbuch.

IMDSv2

```
    [ec2-user ~]$ TOKEN=`curl -X PUT "http://192.0.2.0/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v
 http://192.0.2.0/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://192.0.2.0/latest/meta-data/
    ami-id
    hostname
    instance-id
    instance-type
    local-hostname
    local-ipv4
    mac
    network/
    reservation-id
    security-groups
```

Example Abrufen von Werten von Top-Level-Metadaten

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 vorhergehenden Beispielbefehl erstellt wurde (vorausgesetzt, es ist nicht abgelaufen).

`ami-id` IMDSv2

```
    curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/latest/meta-data/
ami-id ami-0abcdef1234567890
```

`ami-id` IMDSv1

```
    curl http://192.0.2.0/latest/meta-data/ami-id ami-0abcdef1234567890
```

`reservation-id` IMDSv2

```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/
latest/meta-data/reservation-id r-0efghijk987654321
```

`reservation-id` IMDSv1

```
    [ec2-user ~]$ curl http://192.0.2.0/latest/meta-data/reservation-id \
    r-0efghijk987654321
```

`local-hostname` IMDSv2

```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/
latest/meta-data/local-hostname ip-00-000-00-00
```

`local-hostname` IMDSv1

```
    [ec2-user ~]$ curl http://192.0.2.0/latest/meta-data/local-hostname ip-00-000-00-00
```

Verwenden von Block Storage mit Ihren Amazon EC2-compatible Instances

Mit Blockspeicher auf Snowball Edge können Sie Blockspeicher je nach den Anforderungen Ihrer Anwendungen hinzufügen oder entfernen. Volumes, die an eine Amazon EC2-compatible Instance angefügt sind, werden als Speicher-Volumes bereitgestellt, die unabhängig von der Lebensdauer der Instance bestehen bleiben. Sie können den Blockspeicher mit der vertrauten Amazon EBS-API verwalten.

Bestimmte Amazon-EBS-Befehle werden mithilfe des EC2-compatible 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 AmazonEC2-compatible AWS CLI Befehle auf einem Snowball-Edge.

> **Important**
>
> Stellen Sie sicher, dass Sie das Mounting aller Dateisysteme auf dem Gerät in Ihrem Betriebssystem aufheben, bevor Sie das Volume trennen. Andernfalls kann es zu Datenverlusten kommen.

Im Folgenden finden Sie Amazon-EBS-Volume-Kontingente und Unterschiede zwischen Amazon-EBS-Volumes auf Ihrem Gerät und Amazon-EBS-Volumes in der Cloud:

- Amazon EBS-Volumes sind nur für EC2-compatible Instances verfügbar, die auf dem Gerät ausgeführt werden, auf dem die Volumes gehostet werden.
- Volume-Typen sind entweder auf kapazitätsoptimierte HDDs (`sbg1`) oder auf leistungsoptimierte SSDs () beschränkt`sbp1`. Der Standard-Volume-Typ ist `sbg1`.
- Snowball Edge teilt HDD-Speicher zwischen Amazon S3-Objekten und Amazon EBS. Wenn Sie HDD-basierten Blockspeicher auf verwendenAWS Snowball Edge, reduziert dies die Speichermenge, die für Amazon S3-Objekte verfügbar ist. Ebenso reduzieren Amazon S3-Objekte die Speichermenge, die für Amazon-EBS-Blockspeicher auf HDD-Volumes verfügbar ist.
- Amazon EC2-compatible 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.
- Es können bis zu 10 Amazon EBS-Volumes an eine einzelne EC2-compatible Instance angefügt werden.
- Es gibt keine formelle Begrenzung für die Anzahl der Amazon-EBS-Volumes, die Sie auf Ihrem AWS Snowball Edge Gerät haben können. Die Gesamtkapazität des Amazon-EBS-Volumes wird jedoch durch den verfügbaren Speicherplatz auf Ihrem Gerät begrenzt.

Sicherheitsgruppen in Snowball Edge-Geräten

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 Amazon-EC2-Sicherheitsgruppen für Linux-Instances im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Sicherheitsgruppen in Snowball Edge-Geräten ähneln Sicherheitsgruppen in der -AWSCloud. Virtual Private Clouds (VPCs) werden auf Snowball-Edge-Geräten nicht unterstützt.

Im Folgenden finden Sie die anderen Unterschiede zwischen Snowball-Edge-Sicherheitsgruppen und EC2-VPC-Sicherheitsgruppen:

- Jeder Snowball Edge 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 die AWS CLI-Aktionen und API-Aufrufe aufgelisteten Parameter werden unterstützt. Dabei handelt es sich in der Regel um einen Teilsatz der in EC2-VPC-Instances unterstützten Parameter.

Weitere Informationen zu unterstützten AWS CLI Aktionen finden Sie unter Liste der unterstützten AmazonEC2-compatible AWS CLI Befehle auf einem Snowball-Edge. Weitere Informationen zu unterstützten API-Operationen finden Sie unter Unterstützte Amazon EC2-compatible API-Operationen.

Unterstützte Instance-Metadaten und Benutzerdaten

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Snowball Edge unterstützt eine Teilmenge von Instance-Metadatenkategorien für Ihre Datenverarbeitungs-Instances. Weitere Informationen dazu finden Sie unter Instance-Metadaten und Benutzerdaten im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Die folgenden Kategorien werden unterstützt. Bei Verwendung anderer Kategorien wird eine `404` Fehlermeldung zurückgegeben.

Unterstützte Instance-Metadatenkategorien auf einem Snowball Edge

Daten	Beschreibung
`ami-id`	Die für den Start der Instance verwendete AMI-ID
`hostname`	Der private IPv4-DNS-Hostname der Instance.

Daten	Beschreibung
`instance-id`	Die ID dieser Instance
`instance-type`	Der Typ der Instance.
`local-hostname`	Der private IPv4-DNS-Hostname der Instance.
`local-ipv4`	Die private IPv4-Adresse der Instance.
`mac`	Die Media Access Control-Adresse (MAC) der Instance.
`network/interfaces/macs/` *`mac`*`/local-hostname`	Der lokale Hostname der Schnittstelle
`network/interfaces/macs/` *`mac`*`/local-ipv4s`	Die privaten IPv4-Adressen, die mit der Netzwerkschnittstelle verknüpft sind
`network/interfaces/macs/` *`mac`*`/mac`	Die MAC-Adresse der Instance
`network/interfaces/macs/` *`mac`*`/public-ipv4s`	Die Elastic IP-Adressen, die mit der Schnittst elle 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-Scripts zum Übermitteln von Anweisung en an eine Instance beim Start.

Unterstützte dynamische Instance-Datenkategorien auf einem Snowball Edge

Daten	Beschreibung
instance-identity/document	JSON-Daten mit Instance-Attributen. Nur `instanceId` , `imageId`, `privateIp` und

Daten	Beschreibung
	`instanceType` verfügen über Werte, und die anderen zurückgegebenen Attribute sind auf Null gesetzt. Weitere Informationen finden Sie unter Instance-Identitätsdokumente im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Benutzerdaten in Snowball Compute Instances

Benutzerdaten werden für die Verwendung mit Shell-Skripten für Rechen-Instances auf einem Snowball-Edge unterstützt. Durch die Nutzung von Shell-Scripts können Sie einer Instance beim Start Anweisungen übermitteln. Sie können Benutzerdaten über den AWS CLI-Befehl `modify-instance-attribute` oder die `ModifyInstanceAttribute` API-Aktion ändern.

So ändern Sie Benutzerdaten

1. Stoppen Sie Ihre Datenverarbeitungs-Instance über den AWS CLI-Befehl `stop-instances`.
2. Verwenden Sie den AWS CLI-Befehl `modify-instance-attribute` um das `userData`-Attribut zu ändern.
3. Starten Sie Ihre Datenverarbeitungs-Instance über den AWS CLI-Befehl `start-instances` neu.

Es werden nur Shell-Skripts mit Datenverarbeitungs-Instances unterstützt. Es gibt keine Unterstützung für `cloud-init` Paketdirektiven auf Datenverarbeitungs-Instances, die auf einem Snowball Edge ausgeführt werden. Weitere Informationen zum Arbeiten mit AWS CLI Befehlen finden Sie in der AWS CLI -Befehlsreferenz.

Anhalten von EC2-compatible Instances

Um ein versehentliches Löschen der Amazon EC2-compatible Instances zu vermeiden, die Sie auf Ihrem Gerät erstellen, fahren Sie Ihre Instances nicht vom Betriebssystem herunter. 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-compatible Instances auszusetzen, die Sie beibehalten möchten.

Fehlerbehebung bei Datenverarbeitungs-Instances auf Snowball-Edge-Geräten

Im Folgenden finden Sie Tipps zur Fehlerbehebung für Snowball-Edge-Aufträge mit Datenverarbeitungs-Instances.

Themen

Die 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. Zum Beispiel, wenn Sie versuchen, die IP-Adresse der SFP+-Schnittstelle zu ermitteln, aber die RJ45-Schnittstelle mit Ihrem Netzwerk verbunden ist.

Maßnahme

Wenn dies der Fall ist, können Sie Folgendes tun:

- Erstellen Sie eine neue VNIC, die mit einer NIC verbunden ist, die eine IP-Adresse hat. Weitere Informationen finden Sie unter Netzwerkkonfiguration für Datenverarbeitungs-Instances.
- Aktualisieren Sie eine bestehende VNIC. Weitere Informationen finden Sie unter Aktualisieren einer virtuellen Netzwerkschnittstelle.

Snowball Edge hängt beim Starten einer großen Datenverarbeitungs-Instance

Es kann so aussehen, als ob Ihr Snowball Edge das Starten einer Instance beendet hat. 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 , der für den HTTP- oder HTTPS-Amazon EC2-compatible Endpunkt auf dem Snowball Edge `aws ec2 describe-instances` ausgeführt wird.

Meine Instance hat ein Stamm-Volumen

Instances besitzen standardmäßig ein Stamm-Volume. Alle `sbe` Instances verfügen über ein einziges Root-Volume, aber mit Snowball Edge können Sie Blockspeicher je nach den Anforderungen Ihrer Anwendungen hinzufügen oder entfernen. Weitere Informationen finden Sie unter Verwenden von Block Storage mit Ihren Amazon EC2-compatible Instances.

"Ungeschützte private Schlüsseldatei"-Fehler

Dieser Fehler kann auftreten, wenn die .pem-Datei auf Ihrer Datenverarbeitungs-Instance nicht über ausreichende Lese-/Schreibrechte verfügt.

Maßnahme

Sie können dies beheben, indem Sie die Berechtigungen für die Datei mit der folgenden Vorgehensweise ändern:

1. Öffnen Sie ein Terminalfenster 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
```

Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten bietet sicheren Objektspeicher mit erhöhter Ausfallsicherheit, Skalierung und einem erweiterten Amazon S3-API-Featuresatz für Telefonie-, mobile Edge- und getrennte Umgebungen. Mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten können Sie Daten speichern und hochverfügbare Anwendungen auf Snow-Family-Geräten für Edge-Computing ausführen.

Sie können Amazon S3-Buckets auf den Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale

Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte an zurückgegeben werden AWS, werden alle Daten, die im Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten erstellt oder gespeichert werden, gelöscht. Weitere Informationen finden Sie unter Lokale Datenverarbeitungs- und reine Speicheraufträge.

Sie können Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten in eigenständiger Konfiguration oder in Cluster-Konfiguration bereitstellen. In einer eigenständigen Konfiguration können Sie S3-Kapazität auf dem Gerät bereitstellen und der Saldo ist als Blockspeicher verfügbar. In der Clusterkonfiguration wird die gesamte Datenfestplattenkapazität für den S3-Speicher verwendet. Ein Cluster kann aus mindestens 3 Geräten bis maximal 16 Geräten bestehen. Abhängig von der Größe des Clusters ist der S3-Service so konzipiert, dass er die Fehlertoleranz von 1 oder 2 Geräten aufrechterhält.

Mit können AWS DataSync Sie Objekte zwischen Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten auf einem Snowball-Edge-Gerät und AWS Speicherservices übertragen. Weitere Informationen finden Sie unter Konfigurieren von Übertragungen mit S3-kompatiblem Speicher auf Snowball Edge im AWS DataSync -Benutzerhandbuch.

Im Folgenden finden Sie den Amazon S3-kompatiblen Speicher auf der Speicherkapazität von Snow Family-Geräten und die Blockspeicherkapazität für ein eigenständiges Gerät, das Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwendet. Informationen zur Fehlertoleranz und Speicherkapazität von Clustern finden Sie unter this table.

Snowball Edge Compute Optimized and Compute Optimized with GPU

Speicherkapazität von Amazon S3-kompatiblem Speicher auf Geräten der Snow Family und Blockspeicher von für Snowball Edge Compute optimierten Geräten (mit AMD EPYC Gen1, HDD und optionaler GPU)

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
2.5	41

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
5.5	37
8.5	33
11	29
14	25
17	21
19,5	17
22,5	13
25.5	9
28,5	5
31	1

Snowball Edge Compute Optimized with NVMe storage

Speicherkapazität von Amazon S3-kompatiblem Speicher auf Geräten der Snow Family und Blockspeicher von für Snowball Edge Compute optimierten Geräten (mit AMD EPYC Gen2 und NVMe optimiert)

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
3	17.5
5.5	14.5
10.5	8.5
12	6,5
13	5.5

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
16.5	1.5

Snowball Edge storage optimized 210 TB

Speicherkapazität von Amazon S3-kompatiblem Speicher auf Geräten der Snow Family und Blockspeicher von für Snowball Edge-Speicher optimierten Geräten mit 210 TB

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten – Speicherkapazität (in TB)	Blockspeicherkapazität (in TB)
20	206
40	182
60	158
80	134
100	110
120	86
140	62
160	38
180	14
190	2

Amazon S3-kompatibler Speicher auf Spezifikationen für Snow-Family-Geräte:

- Die maximale Anzahl von Geräte-Buckets der Snow Family beträgt 100 pro Gerät oder Cluster.
- Das Bucket-Eigentümerkonto des S3-on-Snow-Family-Geräts besitzt alle Objekte im Bucket.
- Nur das Bucket-Eigentümerkonto des S3-on-Snow-Family-Geräts kann Operationen für den Bucket ausführen.

- Objektgrößenbeschränkungen entsprechen denen in Amazon S3.
- Alle auf S3 auf Snow Family-Geräten 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 vorhanden ist, um ein Objekt auf Ihrem Snow Family-Gerät zu speichern, gibt die API eine Ausnahme wegen unzureichender Kapazität (ICE) zurück.

Themen

Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten bestellen

Das Bestellen eines Geräts für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten ist dem Bestellvorgang eines Snowball-Edge sehr ähnlich. Informationen zur Bestellung finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts in diesem Handbuch. Beachten Sie dabei die folgenden Elemente:

- Wählen Sie für Auftragstyp auswählen die Option Nur lokale Rechenleistung und Speicher aus.
- Wählen Sie unter Snow-Geräte die Option Snowball Edge Compute Optimized aus.
- Wählen Sie unter Speichertyp auswählen die Option Amazon S3-kompatibler Speicher auf Snow-Family-Geräten aus.

- Wählen Sie für ein eigenständiges Gerät unter Speicherkapazität die Option Einzelnes Gerät und dann die gewünschte Speichermenge aus.
- Wählen Sie für einen Cluster unter Speicherkapazität die Option Cluster und dann Ihre gewünschte Speicherkapazität und Fehlertoleranz aus.

Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten

Installieren und konfigurieren Sie Softwaretools von AWS in Ihrer lokalen Umgebung, um mit dem Snowball Edge-Gerät oder dem Gerätecluster und Amazon S3-kompatiblem Speicher auf Snow Family-Geräten zu interagieren. Verwenden Sie dann diese Tools, um das Snowball Edge-Gerät oder den Cluster einzurichten und Amazon S3-kompatiblen Speicher auf Snow Family-Geräten zu starten.

Voraussetzungen

Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten müssen Sie den Snowball Edge Client und die in Ihrer lokalen Umgebung AWS CLI installiert haben. Sie können auch AWS SDK for .NET und AWS Tools for Windows verwenden PowerShell , um mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten zu arbeiten. AWS empfiehlt die Verwendung der folgenden Versionen dieser Tools:

- Snowball Edge Client – Verwenden Sie die neueste Version. Weitere Informationen finden Sie unter Herunterladen und Installieren des Snowball Edge Clients in diesem Handbuch.
- AWS CLI – Version 2.11.15 oder höher. Weitere Informationen finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI im AWS Command Line Interface - Benutzerhandbuch.
- AWS SDK for .NET – AWSSDK.S3Control 3.7.304.8 oder höher. Weitere Informationen finden Sie unter AWS SDK for .NET.
- AWS Tools für Windows PowerShell – Version 4.1.476 oder höher. Weitere Informationen finden Sie im AWS Tools for Windows PowerShell -Benutzerhandbuch.

Einrichten Ihrer lokalen Umgebung

In diesem Abschnitt wird beschrieben, wie Sie den Snowball Edge Client und Ihre lokale Umgebung für die Verwendung mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten einrichten und konfigurieren.

Einrichten Ihrer Umgebung

1. Laden Sie die neueste Version des Snowball Edge Clients herunter und installieren Sie sie. Weitere Informationen finden Sie unter Herunterladen und Installieren des Snowball Edge Clients in diesem Handbuch.
2. Führen Sie die folgenden Befehle aus, um Ihre Ordner zu konfigurieren.

```
chmod u+x new_cli/bin/snowballEdge
chmod u+x new_cli/jre/bin/java
```

3. Fügen Sie `new_cli/bin` zu Ihrem hinzu`$PATH`.
4. Führen Sie den Befehl `snowballEdge configure` aus. Sie erhalten eine Antwort ähnlich der folgenden:

```
Configuration will be stored at /home/user/.aws/snowball/config/snowball-
edge.config
```

5. Geben Sie die folgenden Informationen ein:

   - Der Manifestpfad.
   - Ein Entsperrcode.
   - Der Standardendpunkt. Verwenden Sie für eigenständige Snowball Edge-Geräte die IP-Adresse des Geräts. Geben Sie für einen Gerätecluster die IP-Adresse für jedes Gerät im Cluster an. Um zu testen, ob die Standardendpunkte vom Client aus verfügbar sind, verwenden Sie einen Befehl ähnlich dem folgenden. Verwenden Sie für die Portnummer 9091 (Aktivierungsport), 22 (SSH) und 8080 (HTTP-Endpunkt für s3).

```
telnet snowball_ip port_number
```

6. Wenn Sie verwenden AWS SDK for .NET, legen Sie den `clientConfig.AuthenticationRegion` Parameterwert wie folgt fest:

```
clientConfig.AuthenticationRegion = "snow"
```

Einrichten Ihres Snowball Edge-Geräts

Richten Sie Ihr Snowball Edge-Gerät gemäß Empfangen des Snowball Edge in diesem Handbuch ein.

Nachdem Ihr Gerät eingerichtet und ausgeführt wurde, konfigurieren und starten Sie Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten. Siehe Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.

Einrichten von IAM auf dem Snowball Edge

AWS Identity and Access Management (IAM) hilft Ihnen, den detaillierten 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-Service verwenden, um Rollen zu erstellen und ihnen IAM-Richtlinien anzufügen. 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-API:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"

        }
    ]
}
```

Weitere Beispiele für IAM-Richtlinien finden Sie im AWS Snowball Edge -Entwicklerhandbuch.

Starten des Amazon S3-kompatiblen Speichers auf dem Snow-Family-Geräteservice

Verwenden Sie die folgenden Anweisungen, um den Amazon S3-kompatiblen Speicher auf dem Snow-Family-Geräteservice auf einem Snowball-Edge-Gerät oder -Cluster zu starten.

> **Note**
>
> Wenn Sie eine benutzerfreundlichere Erfahrung bevorzugen, können Sie den Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten für ein eigenständiges Gerät oder einen Cluster von Geräten mit starten AWS OpsHub. Siehe Einrichten von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.

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 sind:

   - 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 über ein oder einen Cluster verfügen) wie folgt vor, um Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten zu starten:

a. Rufen Sie das des Geräts 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
```

Weitere Informationen zu diesen Befehlen finden Sie unter Erstellen einer virtuellen Netzwerkschnittstelle.

> **Note**
>
> Das Starten von Amazon S3-kompatiblem Speicher auf Geräten der Snow Family verbraucht Geräteressourcen.

4. Starten Sie den Amazon S3-kompatiblen Speicher auf Snow Family-Geräten, indem Sie den folgenden `start-service` Befehl ausführen. Dieser enthält die IP-Adressen Ihrer Geräte und die Amazon-Ressourcennamen (ARNs) der VNIs, die Sie für die `s3api` Endpunkte `s3control` und erstellt haben:

So starten Sie den Service auf einem einzigen Gerät:

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-
device-1-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2
```

So starten Sie den Service auf einem Cluster:

```
  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
```

`--virtual-network-interface-arns`Fügen Sie für ARNs für alle VNIs ein, 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 Servicestatus 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
```

Arbeiten mit S3-Buckets auf einem Snowball-Edge-Gerät

Sie können Amazon S3-Buckets auf Ihren Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging.

Verwenden der AWS CLI

Folgen Sie diesen Anweisungen, um mit Amazon S3-Buckets auf Ihrem Gerät mithilfe der zu arbeiten AWS CLI.

So richten Sie die ein AWS CLI

1. Erstellen Sie ein Profil für Objektendpunkte 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. Rufen Sie ein Zertifikat von Ihrem Gerät ab. Weitere Informationen finden Sie im Snowball Edge-Entwicklerhandbuch.
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 über API-Aufrufe mit der darauf zugreifen AWS CLI. In den folgenden Beispielen *cert* ist das Gerätezertifikat, das Sie gerade mit IAM erhalten haben.

Zugreifen auf Objektoperationen

```
aws s3api --profile your-profile list-objects-v2 --endpoint-url
https://s3api-endpoint-ip
```

Zugreifen auf Bucket-Operationen

```
aws s3control --profile your-profile list-regional-buckets --account-id
bucket-owner --endpoint-url https://s3ctrlapi-endpoint-ip
```

Verwenden des Java SDK

Verwenden Sie das folgende Beispiel, um mit Amazon S3-Objekten unter Verwendung des Java SDK 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 des Amazon-Ressourcennamens (ARN) verwenden, um einen Amazon S3-Bucket auf einem Snowball-Edge-Gerät zu identifizieren:

```
arn:partition:s3:snow:account-id:device/device-id/bucket/bucket-name
```

Wobei *`partition`* die Partition der Region ist, in der Sie Ihr Snowball-Edge-Gerät bestellt haben. *`device-id`* ist die job_id, wenn das Gerät ein eigenständiges Snowball-Edge-Gerät ist, oder die *`cluster_id`*, wenn Sie einen Snowball-Edge-Cluster haben.

Erstellen eines S3-Buckets auf einem Snowball-Edge-Gerät

Sie können Amazon S3-Buckets auf Ihrem Snowball-Edge-Gerät erstellen, um Objekte am Edge für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die Amazon S3 verwendet und darauf ausgelegt ist, Daten über mehrere Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen wie für Amazon S3-Buckets verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging.

Im folgenden Beispiel wird ein Amazon S3-Bucket für ein Snowball-Edge-Gerät mithilfe der erstellt AWS CLI. Um diesen Befehl auszuführen, ersetzen Sie die Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3control --profile your-profile create-bucket --bucket your-snow-bucket --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Erstellen und Verwalten einer Objektlebenszykluskonfiguration mit der AWS CLI

Sie können Amazon S3-Lebenszyklus verwenden, um die Speicherkapazität für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten 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 zum Amazon S3-Lebenszyklus finden Sie unter Verwalten Ihres Speicherlebenszyklus.

> **Note**
>
> Das AWS-Konto , das den Bucket erstellt, besitzt ihn und ist das einzige, das eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen kann.

Weitere Informationen zum Erstellen und Verwalten einer Lebenszykluskonfiguration für einen Amazon S3-kompatiblen Speicher auf einem Geräte-Bucket der Snow Family mithilfe der AWS Command Line Interface (AWS CLI) finden Sie in den folgenden Beispielen.

PUT für eine Lebenszykluskonfiguration in einem Snowball Edge-Bucket

Im folgenden AWS CLI Beispiel wird eine Lebenszykluskonfigurationsrichtlinie auf einen Snowball Edge-Bucket gesetzt. Diese Richtlinie legt fest, dass alle Objekte mit dem markierten Präfix (*myprefix*) und Tags nach 10 Tagen ablaufen. Um dieses Beispiel zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

Speichern Sie zunächst die Lebenszykluskonfigurationsrichtlinie in einer JSON-Datei. In diesem Beispiel heißt die Datei **`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, übermitteln Sie die JSON-Datei als Teil des `put-bucket-lifecycle-configuration` Befehls . Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3control put-bucket-lifecycle-configuration --bucket
                example-snow-bucket --profile your-profile
                --lifecycle-configuration file://lifecycle-example.json --endpoint-url
 https://s3ctrlapi-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter put-bucket-lifecycle-configuration in der AWS CLI -Befehlsreferenz.

Arbeiten mit S3-Buckets auf einem Snowball-Edge-Gerät

Mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten können Sie Amazon S3-Buckets auf Ihren Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Sie können Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten mithilfe der AWS Command Line Interface (AWS CLI) oder AWS SDKs verwenden.

Bestimmen, ob Sie auf einen Amazon S3-kompatiblen Speicher im Geräte-Bucket der Snow Family zugreifen können

Im folgenden Beispiel wird der `-head-bucket`Befehl verwendet, um zu ermitteln, ob ein Amazon S3-Bucket vorhanden ist und ob Sie über die Berechtigungen für den Zugriff auf diesen Bucket verfügen AWS CLI. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api head-bucket --bucket sample-bucket --profile your-profile --endpoint-url
 https://s3api-endpoint-ip
```

Abrufen einer Liste von Buckets oder regionalen Buckets

Verwenden Sie die `list-regional-buckets` oder `list buckets`, um Amazon S3-kompatiblen Speicher auf Geräte-Buckets der Snow Family mithilfe der aufzulisten AWS CLI.

```
aws s3control list-regional-buckets --account-id 123456789012 --profile your-profile --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Weitere Informationen über den Befehl `list-regional-buckets` finden Sie unter list-regional-buckets in der AWS CLI -Befehlsreferenz.

```
 aws s3 list-buckets --account-id 123456789012 --endpoint-url https://s3api-endpoint-ip
```

Weitere Informationen zum `list-buckets` Befehl finden Sie unter list-buckets in der -AWS CLI Befehlsreferenz.

Das folgende SDK für Java-Beispiel ruft eine Liste von Buckets auf Snowball Edge-Geräten ab. Weitere Informationen finden Sie unter ListBuckets in der API-Referenz zu Amazon Simple Storage Service.

```
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
```

Im folgenden .NET-Beispiel wird eine Liste von Buckets auf Snowball-Edge-Geräten abgerufen.

```
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"
        });
    }
}
```

Abrufen eines Buckets

Im folgenden Beispiel wird ein Amazon S3-kompatibler Speicher auf dem Geräte-Bucket der Snow Family mithilfe der abgerufen AWS CLI. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3control get-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter get-bucket in der AWS CLI - Befehlsreferenz.

Das folgende Beispiel für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten ruft einen Bucket mit dem SDK for Java 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());
}
```

Löschen eines Buckets

> **Important**
>
> - Das AWS-Konto , das den Bucket erstellt, besitzt ihn und ist das einzige, das ihn löschen kann.
> - Geräte-Buckets der Snow Family müssen leer sein, bevor sie gelöscht werden können.
> - Sie können einen Bucket nicht wiederherstellen, nachdem er gelöscht wurde.

Im folgenden Beispiel wird ein Amazon S3-kompatibler Speicher auf dem Geräte-Bucket der Snow Family mithilfe der gelöscht AWS CLI. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3control delete-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter delete-bucket in der AWS CLI - Befehlsreferenz.

Arbeiten mit S3-Objekten auf einem Snowball-Edge-Gerät

In diesem Abschnitt werden verschiedene Operationen beschrieben, die Sie mit Objekten auf Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten ausführen können.

Kopieren eines Objekts in einen Amazon S3-kompatiblen Speicher auf einem Geräte-Bucket der Snow Family

Im folgenden Beispiel wird eine Datei namens *sample-object.xml* in einen Amazon S3-kompatiblen Speicher auf dem Geräte-Bucket der Snow Family hochgeladen, für den Sie Schreibberechtigungen für die Verwendung der haben AWS CLI. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api put-object --bucket sample-bucket --key sample-object.xml --body sample-
object.xml --profile your-profile --endpoint-url s3api-endpoint-ip
```

Im folgenden Beispiel für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten wird ein Objekt mithilfe des SDK for Java in ein neues Objekt im selben Bucket kopiert. Um diesen Befehl zu verwenden, ersetzen Sie 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();
        }
    }
}
```

Abrufen eines Objekts aus einem Bucket

Im folgenden Beispiel wird ein Objekt namens *sample-object.xml* aus einem Amazon S3-kompatiblen Speicher auf dem Geräte-Bucket der Snow Family mit der abgerufen AWS CLI. Der SDK-Befehl lautet `s3-snow:GetObject`. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api get-object --bucket sample-bucket --key sample-object.xml --profile your-
profile --endpoint-url s3api-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter get-object in der AWS CLI -Befehlsreferenz.

Das folgende Beispiel für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten ruft ein Objekt mit dem SDK for Java ab. Um diesen Befehl zu verwenden, ersetzen Sie 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();
    }
}
```

Auflisten von Objekten in einem Bucket

Das folgende Beispiel listet Objekte in einem Amazon S3-kompatiblen Speicher auf dem Geräte-Bucket der Snow Family mithilfe der auf AWS CLI. Der SDK-Befehl lautet `s3-snow:ListObjectsV2`. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api list-objects-v2 --bucket sample-bucket --profile your-profile --endpoint-
url s3api-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter list-objects-v2 in der AWS CLI - Befehlsreferenz.

Im folgenden Beispiel für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten werden Objekte in einem Bucket unter Verwendung des SDK for Java aufgelistet. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

In diesem Beispiel wird ListObjectsV2 verwendet, die neueste Version der ListObjects -API-Operation. 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();
        }
    }
}
```

Löschen von Objekten in einem Bucket

Sie können ein oder mehrere Objekte aus einem Amazon S3-kompatiblen Speicher auf dem Geräte-Bucket der Snow Family löschen. Im folgenden Beispiel wird ein Objekt mit dem Namen *sample-object.xml* mithilfe der gelöscht AWS CLI. Um diesen Befehl zu verwenden, ersetzen Sie jeden Platzhalter für Benutzereingaben durch Ihre eigenen Informationen.

```
aws s3api delete-object --bucket sample-bucket --key key --profile your-profile --
endpoint-url s3api-endpoint-ip
```

Weitere Informationen zu diesem Befehl finden Sie unter delete-object in der AWS CLI - Befehlsreferenz.

Das folgende Beispiel für einen Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten löscht ein Objekt in einem Bucket mithilfe des SDK for Java. Um dieses Beispiel zu verwenden, geben Sie den Schlüsselnamen für das Objekt an, das Sie löschen möchten. Weitere Informationen finden Sie unter DeleteObject 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.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-kompatiblen Speicher auf Snow-Family-Geräten

Die folgenden Listen zeigen die API-Operationen, die von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten unterstützt werden, einschließlich Links zu den zugehörigen Operationen für Amazon S3 in AWS-Regionen.

Unterstützte Bucket-API-Operationen:

- 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

Clustering-Übersicht

Für den AWS Snowball Service ist ein Cluster ein Kollektive von Snowball Edge-Geräten, die als einzelne logische Einheit für lokale Speicher- und Rechenzwecke verwendet werden.

Ein Cluster bietet zwei Hauptvorteile gegenüber einem eigenständigen Snowball Edge-Gerät für lokale Speicherung und Datenverarbeitung:

- Höhere Haltbarkeit – Die in einem Cluster von Snowball Edge-Geräten gespeicherten Daten profitieren von einer höheren Datenbeständigkeit über ein einzelnes Gerät. Darüber hinaus bleiben die Daten auf dem Cluster sicher und umsetzbar wie zuvor, obwohl es zu möglichen Ausfällen von Snowball Edge im Cluster kommen kann. Cluster können dem Verlust eines Geräts in Clustern mit 3 und 4 Geräten und bis zu zwei Geräten in Clustern mit 5 bis 16 Geräten standhalten, bevor die Daten widerstandsfähig sind. Knoten können auch hinzugefügt oder ausgetauscht werden.
- Höherer Speicher – Mit speicheroptimierten Geräten von Snowball Edge können Sie einen einzelnen Cluster mit 16 Knoten mit bis zu 2,6 PB nutzbarer S3-compatible Speicherkapazität erstellen. Mit für die Datenverarbeitung optimierten Snowball Edge-Geräten können Sie einen einzelnen Cluster mit 16 Knoten mit bis zu 501 TB nutzbarer S3-compatible Speicherkapazität erstellen.

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten, Cluster-Fehlertoleranz und Speicherkapazität

Cluster-Größe	Fehlertoleranz	Speicherkapazität von Snowball Edge Compute Optimized-Geräten (mit AMD EPYC Gen1, HDD und optionaler GPU)	Speicherkapazität von Snowball Edge Compute Optimized (Datenverarbeitung soptimiert mit AMD EPYC Gen2 und NVMe)-Geräten	Speicherkapazität von Snowball Edge-Speicher-optimierten 210-TB-Geräten
3	Verlust von bis zu 1 Knoten	83	38	438
4	Verlust von bis zu 1 Knoten	125	57	657
5	Verlust von bis zu 2 Knoten	125	57	657
6	Verlust von bis zu 2 Knoten	167	76	904
7	Verlust von bis zu 2 Knoten	209	95	1096
8	Verlust von bis zu 2 Knoten	250	114	1315
9	Verlust von bis zu 2 Knoten	292	133	1534
10	Verlust von bis zu 2 Knoten	334	152	1754

Cluster-Größe	Fehlertoleranz	Speicherkapazität von Snowball Edge Compute Optimized-Geräten (mit AMD EPYC Gen1, HDD und optionaler GPU)	Speicherkapazität von Snowball Edge Compute Optimized (Datenverarbeitung soptimiert mit AMD EPYC Gen2 und NVMe)-Geräten	Speicherkapazität von Snowball Edge-Speicher-optimierten 210-TB-Geräten
11	Verlust von bis zu 2 Knoten	370	165	1970
12	Verlust von bis zu 2 Knoten	376	171	1973
13	Verlust von bis zu 2 Knoten	418	190	2192
14	Verlust von bis zu 2 Knoten	459	209	2411
15	Verlust von bis zu 2 Knoten	495	225	2625
16	Verlust von bis zu 2 Knoten	501	228	2631

Ein Cluster von Snowball Edge-Geräten besteht aus führenden Knoten. Jeder Knoten kann Daten in den gesamten Cluster schreiben und Daten aus diesem lesen, und alle Knoten sind in der Lage, die behind-the-scenes Verwaltung des Clusters durchzuführen.

Quorume von Snowball Edge-Clustern

Ein Quorum stellt die Mindestanzahl von Snowball Edge-Geräten in einem Cluster dar, die miteinander kommunizieren müssen, um ein Lese-/Schreib-Quorum aufrechtzuerhalten.

Angenommen, Sie laden Ihre Daten auf einen Cluster von Snowball-Edge-Geräten hoch. Wenn alle Geräte fehlerfrei sind, verfügen Sie über ein Quorum für Lese-/Schreibzugriff für Ihren Cluster. Wenn einer oder zwei dieser Knoten offline geht, reduzieren Sie die Betriebskapazität des Clusters. Sie können jedoch immer noch Lese- und Schreibvorgänge auf dem Cluster durchführen. In diesem Sinne hat der Cluster immer noch ein Quorum für Lese-/Schreibzugriff, wenn der Cluster alle außer einem oder zwei Knoten ausführt. Die Anzahl der Knoten, die offline gehen können, bevor die Betriebskapazität des Clusters beeinträchtigt wird, finden Sie unter this table.

Schließlich kann das Quorom verletzt werden, wenn ein Cluster mehr als die in angegebene Anzahl von Knoten verliertthis table. Wenn ein Quorom überschritten wird, 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 Stromereignis handelt und Sie die drei Snowball Edge-Geräte wieder einschalten und alle Knoten im Cluster entsperren können, sind Ihre Daten wieder verfügbar.

> **Important**
>
> Wenn kein Mindestquorum fehlerfreier Knoten vorhanden ist, wenden Sie sich an AWS den -Support.

Sie können den Quorum-Zustand Ihres Clusters ermitteln, indem Sie den Sperrstatus und die Netzwerkerreichbarkeit Ihres Knotens bestimmen. Der Befehl `snowballEdge describe-cluster` meldet die Sperre und den Netzwerkerreichbarkeitsstatus für jeden Knoten in einem freigegebenen Cluster zurück. Sicherzustellen, dass die Geräte in Ihrem Cluster funktionsfähig und verbunden sind, ist eine administrative Aufgabe, die Sie beim Anlegen des Cluster-Auftrags übernehmen. Weitere Informationen zu den verschiedenen Client-Befehlen finden Sie unter Befehle für den Snowball Edge Client.

Überlegungen zu Cluster-Aufträgen für Snowball-Edge-Geräte

Beachten Sie die folgenden Überlegungen, wenn Sie planen, einen Cluster von Snowball-Edge-Geräten zu verwenden:

- Wir empfehlen die Verwendung einer redundanten Stromversorgung, um potenzielle Leistungs- und Stabilitätsprobleme für Ihren Cluster zu minimieren.
- Wie bei eigenständigen lokalen Speicher- und Datenverarbeitungsaufträgen 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 Importauftragsgeräte übertragen.

- Um Daten aus Amazon S3 in einen Cluster zu übertragen, erstellen Sie einen separaten Exportauftrag und kopieren Sie die Daten von den Geräten des Exportauftrags in den Cluster.
- Sie können einen Cluster-Auftrag über die Konsole, die AWS CLI oder eines der AWS SDKs erstellen. Eine exemplarische Vorgehensweise für die Erstellung eines Auftrags finden Sie unter Erste Schritte.
- Cluster-Knoten haben Knoten-IDs. Eine Knoten-ID entspricht der Auftrags-ID für ein Gerät, das Sie von der Konsole, der AWS CLI, den AWS SDKs und dem Snowball Edge-Client abrufen können. Sie können die Knoten-IDs verwenden, um alte Knoten von Clustern zu entfernen. Mit dem Befehl `snowballEdge describe-device` erhalten Sie eine Liste der Knoten-IDs auf einem entsperrten Gerät, mit dem Befehl `describe-cluster` für einen entsperrten Cluster.
- 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 dieses Zeitraums reagieren die Geräte nicht mehr auf Lese-/Schreibanfragen. Wenn Sie ein oder mehrere Geräte länger als 360 Tage aufbewahren müssen, wenden Sie sich an AWS Support.
- Wenn ein zurückgegebenes Gerät AWS empfängt, 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.

Verwalten eines Clusters

Lesen und Schreiben von Daten in einen Cluster

Nachdem Sie einen Cluster entsperrt haben, können Sie Daten in diesem Cluster speichern und darauf zugreifen. Sie können den Amazon S3-kompatiblen Endpunkt verwenden, um Daten aus einem Cluster zu lesen und in einen Cluster zu schreiben.

Um Daten aus einem Cluster zu lesen oder in einen Cluster zu schreiben, müssen Sie über ein Quorum für Lese-/Schreibzugriff mit nicht mehr als der zulässigen Anzahl nicht verfügbarer Knoten in Ihrem Gerätecluster verfügen.

Erneutes Verbinden eines nicht verfügbaren Cluster-Knotens

Ein Knoten oder Gerät innerhalb eines Clusters kann aufgrund eines Problems wie Strom- oder Netzwerkverlusts vorübergehend nicht verfügbar sein, ohne die Daten auf dem Knoten zu beeinträchtigen. 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 `snowballEdge describe-cluster` Befehls 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 Netzwerkkabel auf der Back-Seite zugreifen, Labels oben für Knoten-IDs versenden und Bildschirme vor den Geräten für die IP-Adressen und andere administrative Informationen verwenden.

Wenn Sie feststellen, dass ein Knoten nicht verfügbar ist, empfehlen wir Ihnen, je nach 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 hochfahren müssen, warten Sie bis zu 20 Minuten, bis er abgeschlossen ist.
4. Führen Sie den `snowballEdge unlock-cluster` Befehl oder den `snowballEdge associate-device` Befehl aus. Ein Beispiel finden Sie unter Entsperren von Snowball-Edge-Geräten.

So stellen Sie die Verbindung zu einem nicht verfügbaren Knoten wieder her, der die Netzwerkverbindung verloren hat, 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 vorherigen Verfahren ausgeführt haben, sollten Ihre Knoten normal funktionieren. Sie sollten auch über ein Lese-/Schreib-Quorum verfügen. 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.

Hinzufügen oder Ersetzen eines Knotens in einem Cluster

Sie können einen neuen Knoten hinzufügen, nachdem Sie einen nicht betriebsbereiten Knoten aus einem Cluster entfernt haben. Sie können auch einen neuen Knoten hinzufügen, um den lokalen Speicherplatz zu erhöhen.

Um einen neuen Knoten hinzuzufügen, müssen Sie zuerst einen Ersatzknoten bestellen. Sie können einen Ersatzknoten über die Konsole, die AWS CLI oder eines der AWS SDKs bestellen. Wenn Sie einen Ersatzknoten über die Konsole bestellen, können Sie Ersatz für alle Aufträge bestellen, die nicht abgebrochen oder abgeschlossen wurden.

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 für Sie da. Wenn sie angekommen ist, gehen Sie wie folgt vor, um sie Ihrem Cluster hinzuzufügen.

Hinzufügen eines Ersatzknotens

1. Positionieren Sie den neuen Knoten für den Cluster so, dass Sie Zugang zur Vorder-, Rück- und Oberseite aller Knoten haben.
2. Stellen Sie sicher, dass der Knoten mit Strom versorgt wird.
3. Stellen Sie sicher, dass der Knoten mit demselben internen Netzwerk verbunden ist, in dem sich der Rest des Clusters befindet.

4. Warten Sie, bis der Knoten das Einschalten abgeschlossen hat (falls er eingeschaltet werden muss).
5. Führen Sie den Befehl `snowballEdge associate-device` aus. Ein Beispiel finden Sie unter Hinzufügen eines Knoten zu einem Cluster.

Konfigurieren von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten Ereignisbenachrichtigungen

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten unterstützt Amazon S3-Ereignisbenachrichtigungen für Objekt-API-Aufrufe, die auf dem MQTT-Protokoll basieren.

Sie können Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten verwenden, um Benachrichtigungen zu erhalten, wenn bestimmte Ereignisse in Ihrem S3-Bucket auftreten. Um Benachrichtigungen zu aktivieren, fügen Sie eine Benachrichtigungskonfiguration hinzu, die die Ereignisse identifiziert, die der Service veröffentlichen soll.

Amazon S3-kompatibler Speicher auf Snow-Family-Geräten unterstützt die folgenden Benachrichtigungstypen:

- Neues Objekt erstellte Ereignisse
- Ereignisse zum Entfernen von Objekten
- Ereignismarkierungen von Objekten

Konfigurieren von Amazon S3-Ereignisbenachrichtigungen

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.

   Geben Sie bei Aufforderung 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
```

Dies gibt den Broker-Endpunkt und das aktivierte Feld zurück.

Nachdem Sie den gesamten Cluster so konfiguriert haben, dass Benachrichtigungen an den MQTT-Broker im Netzwerk gesendet werden, führt jeder Objekt-API-Aufruf zu einer Ereignisbenachrichtigung.

> **Note**
>
> Sie müssen das Thema s3SnowEvents/*Device ID* (oder *Cluster-ID*, wenn es sich um einen Cluster handelt)/bucketName abonnieren. Sie können auch Platzhalter verwenden, z. B. kann der Themenname *#* oder *s3SnowEvents/#* sein.

Im Folgenden finden Sie ein Beispiel für einen Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten-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": "GZdTUOhYHvHgQgmaw2gl4w==",
"Host": "10.0.2.251",
"bucketName": "buckett",
"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-Ereignisbenachrichtigungen finden Sie unter Amazon S3-Ereignisbenachrichtigungen.

Konfigurieren lokaler SMTP-Benachrichtigungen

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 Servicestatus (Aktiv, Degradiert, Inaktiv) ändert oder wenn Sie Schwellenwerte für die Kapazitätsauslastung von 80 %, 90 % oder 100 % überschreiten.

Voraussetzungen

Bevor Sie beginnen, bestätigen Sie Folgendes:

- Sie haben Zugriff auf den neuesten Snowball Edge-Client.
- Ihr Gerät ist entsperrt und einsatzbereit.
- Ihr Gerät kann eine Verbindung zum Internet (bei Verwendung von Amazon Simple Email Service oder eines externen SMTP-Servers) oder zu einem lokalen SMTP-Server herstellen.

Konfigurieren des Geräts

Richten Sie Ihr Gerät so ein, dass Ihnen E-Mail-Benachrichtigungen gesendet werden.

So konfigurieren Sie das Gerät für SMTP-Benachrichtigungen

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 recepients, 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 sind.

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.

Remote-Überwachung für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten

Die Remote-Überwachung ermöglicht es AWS , Amazon S3-kompatiblen Speicher auf Geräten der Snow Family auf Snowball-Edge-Geräten zu überwachen, die mit einem verbunden sind AWS-Region. Wenn die Remote-Überwachung aktiviert ist, löst sie regelmäßige Serviceprotokoll-Uploads in die aus AWS-Region. AWS überwacht diese Informationen und kann Sie proaktiv benachrichtigen, wenn wir Probleme mit dem Service erkennen. Wenn die Remote-Überwachung nicht aktiviert ist oder das Snowball Edge-Gerät oder der Cluster nicht mit einem verbunden sind AWS-Region, versucht der Remote-Überwachungsservice nicht, interne Geräte- oder Servicetelemetrie in der Cloud zu veröffentlichen. Die Remote-Überwachung ist für eigenständige Snowball Edge-Geräte und Cluster von Snowball Edge-Geräten verfügbar.

> **Note**
>
> Die Remote-Überwachung ermöglicht derzeit nur die Überwachung des Amazon S3-kompatiblen Speichers auf dem Snow-Family-Geräteservice.

Sie können den `describe-features` Befehl verwenden, um zu sehen, ob der Remote-Überwachungsservice ausgeführt wird oder nicht. Weitere Informationen finden Sie unter Überprüfen des Feature-Status in diesem Handbuch.

So aktivieren Sie die Remote-Überwachung für ein eigenständiges Gerät

- Verwenden Sie den `set-features` Befehl und setzen Sie den Wert des `remote-monitoring-state` Parameters auf `INSTALLED_AUTOSTART`.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-local-ip
```

> **Note**
>
> Weitere Informationen zur Manifestdatei und zum Entsperrcode des Snow Family-Geräts finden Sie unter Abrufen Ihrer Anmeldeinformationen und Tools in diesem Handbuch.

Der Befehl gibt Folgendes zurück.

```
{
    "RemoteMonitoringState" : INSTALLED_AUTOSTART
}
```

So aktivieren Sie die Fernüberwachung für einen Gerätecluster

- Verwenden Sie den `set-features` Befehl und setzen Sie den Wert des `remote-monitoring-state` Parameters `INSTALLED_AUTOSTART` für jedes Snow Family-Gerät im Cluster auf .

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-1-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-2-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-3-local-ip
```

> **Note**
>
> Weitere Informationen zur Manifestdatei und zum Entsperrcode des Snow Family-Geräts finden Sie unter Abrufen Ihrer Anmeldeinformationen und Tools in diesem Handbuch.

Jedes Mal, wenn Sie den Befehl ausführen, wird Folgendes zurückgegeben.

```
{
    "RemoteMonitoringState" : INSTALLED_AUTOSTART
}
```

So deaktivieren Sie die Fernüberwachung für ein eigenständiges Gerät

- Verwenden Sie den `set-features` Befehl und setzen Sie den Wert des `remote-monitoring-state` Parameters auf `INSTALLED_ONLY`. Das Snow Family-Gerät lädt Protokolle nicht mehr regelmäßig hoch und überwacht oder benachrichtigt Sie AWS nicht, wenn Probleme mit dem Service auftreten, während die Fernüberwachung deaktiviert ist.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-local-ip
```

Der Befehl gibt Folgendes zurück.

```
{
    "RemoteMonitoringState" : INSTALLED_ONLY
}
```

So deaktivieren Sie die Remote-Überwachung für einen Gerätecluster

- Verwenden Sie den `set-features` Befehl und setzen Sie den Wert des `remote-monitoring-state` Parameters `INSTALLED_ONLY` für jedes Snow Family-Gerät im Cluster auf .

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-1-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-2-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-3-local-ip
```

Jedes Mal, wenn Sie den Befehl ausführen, wird Folgendes zurückgegeben.

```
{
    "RemoteMonitoringState" : INSTALLED_ONLY
}
```

Verwenden von Amazon EKS Anywhere in AWS Snow

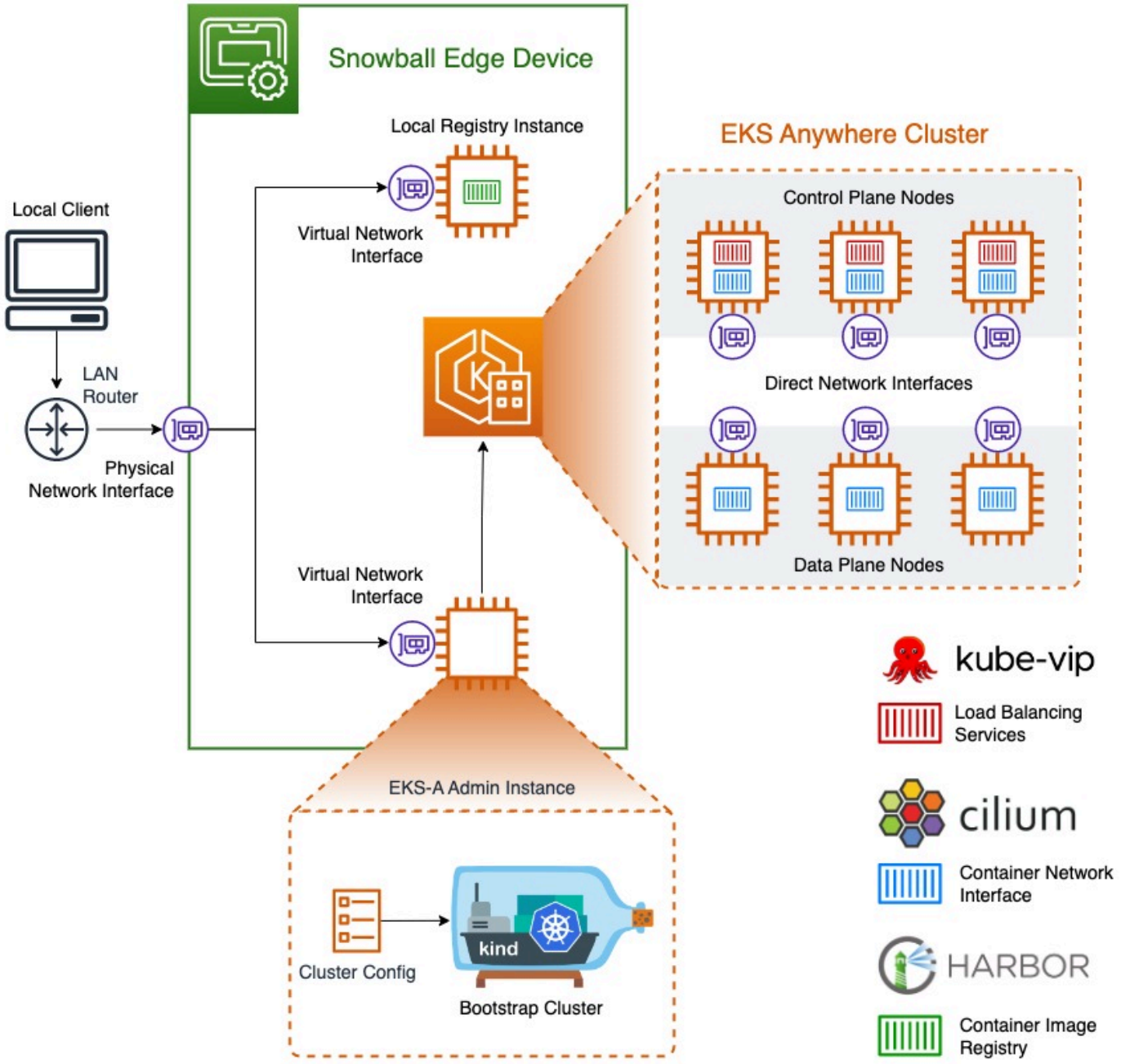
Amazon EKS Anywhere in AWS Snow unterstützt Sie beim Erstellen und Betreiben von Kubernetes-Clustern auf Snow-Family-Geräten. Kubernetes ist Open-Source-Software, die zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen verwendet wird. Sie können Amazon 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 Dokumentation zu Amazon EKS Anywhere.

Die Verwendung von Amazon EKS Anywhere in AWS Snow bietet Ihnen folgende Funktionen:

- Stellen Sie einen Kubernetes (K8s)-Cluster mit Amazon EKS Anywhere CLI (jede Stelle) auf für die Datenverarbeitung optimierten Snowball Edge-Geräten bereit. Sie können Amazon EKS Anywhere auf einem einzelnen Snowball-Edge-Gerät oder drei oder mehr Geräten für hohe Verfügbarkeit bereitstellen.
- Unterstützung für Cilium Container Network Interface (CNI).
- Unterstützung für Ubuntu 20.04 als Knotenbetriebssystem.

Dieses Diagramm veranschaulicht einen Amazon EKS 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 jede Version von Kubernetes, die im Standard- oder verlängerten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten von Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust des Supports für die Kubernetes-Version vermeiden, die Sie

verwenden möchten. Weitere Informationen finden Sie unter Amazon-EKS-Kubernetes-Release-Kalender.

Weitere Informationen zu Amazon EKS Anywhere in AWS Snow finden Sie in der Dokumentation zu Amazon EKS Anywhere.

Themen

Abzuschließende Aktionen, bevor Sie ein Snowball-Edge-Gerät für Amazon EKS Anywhere in AWS Snow bestellen

Derzeit ist Amazon EKS Anywhere mit Snowball Edge-Geräten für Datenverarbeitung und Datenverarbeitung kompatibel, die mit GPU-Geräten (Graphics Processing Unit) optimiert sind. Bevor Sie ein Snowball Edge-Gerät bestellen, sollten Sie einige Dinge vorbereiten.

- Erstellen und stellen Sie ein Betriebssystem-Image bereit, das zum Erstellen virtueller Maschinen auf dem Gerät verwendet werden soll.
- Ihr Netzwerk muss über eine statische IP-Adresse verfügen, die für den Endpunkt der K8s-Steuerebene verfügbar ist, und Address Resolution Protocol (ARP) zulassen.
- Ihr Snowball Edge-Gerät muss bestimmte Ports geöffnet haben. Weitere Informationen zu Ports finden Sie unter Ports und Protokolle in der Dokumentation zu Amazon EKS Anywhere.

Themen

Erstellen eines Ubuntu-EKS-Distro-AMI

Informationen zum Erstellen des Ubuntu EKS Distro AMI finden Sie unter Erstellen von Snow-Knoten-Images.

Der Name des generierten AMI folgt dem Muster `capa-ami-ubuntu-20.04-version-timestamp`. Beispiel: `capa-ami-ubuntu-20.04-v1.24-1672424524`

Erstellen eines AMI

Richten Sie ein AMI für die private Registrierung ein, das auf dem Snowball-Edge-Gerät enthalten ist, 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 über eine private Kubernetes-Registrierung in einem AMI verfügen, das Sie auf dem Gerät verwenden können, können Sie diesen Abschnitt überspringen.

Informationen zum Erstellen des lokalen Registrierungs-AMI finden Sie unter Erstellen eines AMI.

Bestellen eines Snowball Edge-Geräts zur Verwendung mit Amazon EKS Anywhere in AWS Snow

Informationen zum Bestellen Ihrer für Snowball Edge-Datenverarbeitung oder Datenverarbeitung, die mit einem GPU-Gerät optimiert ist, finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts in diesem Handbuch und beachten Sie diese Elemente während des Bestellvorgangs:

- Wählen Sie in Schritt 1 den Auftragstyp Lokale Datenverarbeitung und Nur-Speicher aus.
- Wählen Sie in Schritt 2 die Optionen Snowball Edge Compute Optimized oder Snowball Edge Compute Optimized mit GPU-Gerätetyp aus.
- Wählen Sie in Schritt 3 Amazon EKS Anywhere in AWS Snow und dann die benötigte Kubernetes-Version aus.

> **Note**
>
> Um die neueste Software bereitzustellen, konfigurieren wir das Gerät möglicherweise mit einer neueren Version von ESK Anywhere als der derzeit verfügbaren. Weitere Informationen finden Sie unter Versioning 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 jede Version von Kubernetes, die im Standard- oder verlängerten Support von Amazon EKS angeboten wird. Berücksichtigen Sie bei der Planung des Lebenszyklus Ihrer Bereitstellung die Veröffentlichungs- und Supportdaten von Kubernetes-Versionen. Auf diese Weise können Sie den potenziellen Verlust des Supports für die Kubernetes-Version vermeiden, die Sie verwenden möchten. Weitere Informationen finden Sie unter Amazon-EKS-Kubernetes-Release-Kalender.

- Wählen Sie AMIs aus, die auf Ihrem Gerät enthalten sein sollen, einschließlich des EKS-Distro-AMI (siehe Erstellen eines Ubuntu-EKS-Distro-AMI) und optional des von Ihnen erstellten AMI (siehe Erstellen eines AMI).
- Wenn Sie mehrere Snowball Edge-Geräte für hohe Verfügbarkeit benötigen, wählen Sie die Anzahl der benötigten Geräte unter Hochverfügbarkeit aus.

Nachdem Sie Ihr Snowball Edge-Gerät oder Ihre Geräte erhalten haben, konfigurieren Sie Amazon EKS Anywhere gemäß Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball-Edge-Geräten.

Konfigurieren und Ausführen 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 Konfigurieren von Amazon EKS Anywhere in AWS Snow für den getrennten Betrieb.

Themen

- Erstes Einrichten
- Automatisches Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball-Edge-Geräten
- Manuelles Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball-Edge-Geräten

Erstes Einrichten

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.

Durchführen der Ersteinrichtung

1. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter Herunterladen und Installieren des Snowball Edge-Clients.
2. Verbinden Sie das Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem lokalen Netzwerk.
3. Rufen Sie Anmeldeinformationen ab, um Ihr Gerät zu entsperren. Weitere Informationen finden Sie unter Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät.
4. Entsperren Sie das Gerät. Weitere Informationen finden Sie unter Entsperren des Snow Family-Geräts. Sie können auch ein Skript-Tool verwenden, anstatt Geräte manuell zu entsperren. Weitere Informationen finden Sie unter Entsperren von Geräten.

Automatisches Konfigurieren und Ausführen von Amazon EKS Anywhere auf Snowball-Edge-Geräten

Sie können Beispielskript-Tools verwenden, um die Umgebung einzurichten und eine Admin-Instance von Amazon EKS Anywhere auszuführen, oder Sie können dies manuell tun. Informationen zur Verwendung der Skript-Tools finden Sie unter Entsperren von Geräten und Einrichtungsumgebung für Amazon EKS Anywhere. Nachdem die Umgebung eingerichtet wurde und die Amazon EKS Anywhere-Admin-Instance ausgeführt wird, finden Sie weitere Informationen unter , wenn Sie Amazon EKS Anywhere für den Betrieb auf dem Snowball-Edge-Gerät konfigurieren müssen, während die Verbindung zu einem Netzwerk getrennt istKonfigurieren von Amazon EKS Anywhere in AWS Snow für den getrennten Betrieb. Andernfalls lesen Sie unter Erstellen und Verwalten von Clustern auf Snowball-Edge-Geräten weiter.

Informationen zum manuellen Einrichten der Umgebung und zum Ausführen einer Amazon EKS Anywhere-Administrator-Instance 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

Themen

Erstellen eines - AWS CLI Profils

Erstellen Sie ein - AWS CLI Profil, um Anmeldeinformationen für die Verwendung während der Konfiguration von Snowball-Edge-Geräten und der Amazon EKS Anywhere-Administrator-Instance zu speichern. Weitere Informationen zu AWS CLI Profilen finden Sie unter Benannte Profile für AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

Sie können ein Beispielskript-Tool verwenden, um das AWS CLI Profil und den lokalen IAM-Benutzer von Amazon EKS Anywhere automatisch zu erstellen. Weitere Informationen finden Sie unter Erstellen von Anmeldeinformationen und Zertifikaten. Nachdem Sie das Skript verwendet haben, fahren Sie mit fort(Optional) Erstellen und Importieren eines Secure Shell-Schlüssels. Andernfalls befolgen Sie dieses Verfahren und dann die Verfahren in Erstellen eines lokalen Amazon EKS Anywhere-IAM-Benutzers.

> **Note**
>
> Tun Sie dies für jedes Snowball Edge-Gerät, das Sie konfigurieren.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge list-access-keys --endpoint
 https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-code
{
 "AccessKeyIds" : [ "xxxx" ]
}
```

Verwenden Sie den Wert von `AccessKeyIds` als Wert des `-access-key-id`Parameters des `-get-secret-access-key`Befehls.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge get-secret-access-key --access-key-
id ACCESS_KEY_ID --endpoint https://snowball-ip --manifest-file path-to-manifest-file
 --unlock-code unlock-code
[snowballEdge]
aws_access_key_id = xxx
aws_secret_access_key = xxx
```

Verwenden Sie den Wert von `aws_access_key_id` und `aws_secret_access_key` als Werte von `AWS Access Key ID` und `AWS Secret Access Key` des AWS CLI Profils.

```
aws configure --profile profile-name
AWS Access Key ID [None]: aws_access_key_id
AWS Secret Access Key [None]: aws_secret_access_key
Default region name [None]: snow
```

Erstellen eines lokalen Amazon EKS Anywhere-IAM-Benutzers

Erstellen Sie für bewährte Sicherheitsmethoden einen lokalen IAM-Benutzer für Amazon EKS Anywhere auf dem Snowball-Edge-Gerät. Sie können dies mit den folgenden Verfahren manuell tun.

> **Note**
>
> Tun Sie dies für jedes Snowball Edge-Gerät, das Sie verwenden.

Erstellen eines lokalen Benutzers

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 einer Richtlinie für den lokalen Benutzer

Erstellen Sie ein Richtliniendokument, verwenden Sie es, um eine IAM-Richtlinie zu erstellen, und fügen Sie diese Richtlinie dem lokalen Benutzer von Amazon EKS Anywhere an.

So erstellen Sie ein Richtliniendokument und fügen es dem lokalen Benutzer von Amazon EKS Anywhere an

1. Erstellen Sie ein Richtliniendokument und speichern Sie es auf Ihrem Computer. Kopieren Sie die folgende Richtlinie in das -Dokument.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snowballdevice:DescribeDevice",
        "snowballdevice:CreateDirectNetworkInterface",
        "snowballdevice:DeleteDirectNetworkInterface",
        "snowballdevice:DescribeDirectNetworkInterfaces",
        "snowballdevice: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 basierend auf dem Richtliniendokument 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":
 "ANPACEMGEZDGNBVGY3TQOJQGEZAAAABP76TE5MKAAAABCCOTR2IJ43NBTJRZBU",
        "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 eines Zugriffsschlüssels und einer Datei mit Anmeldeinformationen

Erstellen Sie einen Zugriffsschlüssel für den lokalen Benutzer von Amazon EKS Anywhere IAM. Erstellen Sie dann eine Anmeldeinformationsdatei und fügen Sie die Werte von `AccessKeyId` und ein, die für den lokalen Benutzer `SecretAccessKey` generiert wurden. Die Datei mit den Anmeldeinformationen wird später von der Admin-Instance von Amazon EKS Anywhere verwendet.

1. Verwenden Sie den `create-access-key` Befehl , um einen Zugriffsschlüssel für den lokalen Benutzer von Amazon EKS Anywhere 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 Datei mit Anmeldeinformationen. 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 einer Zertifikatsdatei für die Admin-Instance

Die Amazon EKS Anywhere-Administrator-Instance benötigt die Zertifikate der Snowball-Edge-Geräte, um auf ihnen ausgeführt zu werden. Erstellen Sie eine Zertifikatsdatei mit dem Zertifikat, um auf Snowball Edge-Geräte zuzugreifen und sie später von der Amazon EKS Anywhere-Administrator-Instance zu verwenden.

So erstellen Sie eine Zertifikatsdatei

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. Platzieren Sie die Ausgabe von `get-certificate` in der Zertifikatsdatei. 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-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGVla3NhIHNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXDCCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----
```

4. Wiederholen Sie diesen VorgangErstellen eines lokalen Amazon EKS Anywhere-IAM-Benutzers, um einen lokalen IAM-Benutzer für Amazon EKS Anywhere auf allen Snowball-Edge-Geräten zu erstellen.

(Optional) Erstellen und Importieren eines Secure Shell-Schlüssels

Verwenden Sie dieses optionale Verfahren, um einen Secure Shell (SSH)-Schlüssel für den Zugriff auf alle Amazon EKS Anywhere-Knoten-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-Instance in gespeichert`${PWD}/${CLUSTER_NAME}/eks-a-id_rsa`.

Erstellen Sie einen SSH-Schlüssel und importieren Sie ihn in die Amazon EKS 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 gleich 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"
}
```

Ausführen einer Amazon EKS Anywhere-Admin-Instance und Übertragen von Anmeldeinformations- und Zertifikatsdateien in diese Instance

Ausführen einer Amazon EKS Anywhere-Admin-Instance

Gehen Sie wie folgt vor, um eine Admin-Instance von Amazon EKS Anywhere manuell auszuführen, eine 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 mit der Admin-Instance herzustellen. Sie können ein Beispielskript-Tool verwenden, um das Erstellen einer Amazon EKS Anywhere-Administrator-Instance und das Übertragen von Anmeldeinformations- und Zertifikatsdateien an diese Instance zu automatisieren. Weitere Informationen finden Sie unter Erstellen einer Amazon EKS Anywhere-Administrator-Instance. Nachdem das Skript-Tool abgeschlossen ist, können Sie in die Instance eintauchen und Cluster erstellen, indem Sie auf verweisenErstellen und Verwalten von Clustern auf Snowball-Edge-Geräten. Wenn Sie die Amazon EKS Anywhere-Instance manuell einrichten möchten, führen Sie die folgenden Schritte aus.

> **Note**
>
> Wenn Sie mehr als ein Snowball Edge-Gerät verwenden, um den Cluster bereitzustellen, können Sie eine Amazon EKS Anywhere-Admin-Instance auf jedem der Snowball Edge-Geräte starten.

So führen Sie eine Admin-Instance von Amazon EKS Anywhere aus

1. Verwenden Sie den `create-key-pair` Befehl , um einen SSH-Schlüssel für die Amazon EKS Anywhere-Admin-Instance zu erstellen. Der Befehl speichert den Schlüssel in `$PWD/key-file-name`.

```
aws ec2 create-key-pair --key-name key-name --query 'KeyMaterial' --output text --
endpoint http://snowball ip:8008 --profile profile-name > key-file-name
```

2. Verwenden Sie den `describe-images` Befehl , um den Image-Namen, der mit beginnt, `eks-anywhere-admin` aus der Ausgabe zu ermitteln.

```
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-Administrator-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-Instance zu überprüfen. Warten Sie, bis der Befehl anzeigt, dass der Instance-Status lautet, `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 verwenden dies, um eine 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 eine VNI für die Admin-Instance von Amazon EKS Anywhere. 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-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 über SSH eine Verbindung mit der Admin-Instance von Amazon EKS Anywhere her.

```
ssh -i path-to-key ec2-user@VNI-IP
```

Übertragen von Zertifikats- und Anmeldeinformationsdateien auf die Admin-Instance

Nachdem die Amazon EKS Anywhere-Administrator-Instance ausgeführt wurde, übertragen Sie die Anmeldeinformationen und Zertifikate Ihrer Snowball-Edge-Geräte auf die Administrator-Instance. Führen Sie den folgenden Befehl aus demselben Verzeichnis aus, in dem Sie die Anmeldeinformationen und Zertifikatsdateien in Erstellen eines Zugriffsschlüssels und einer Datei mit Anmeldeinformationen und gespeichert habenErstellen einer Zertifikatsdatei für die Admin-Instance.

```
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 Admin-Instance von Amazon EKS Anywhere. Im Folgenden finden Sie Beispiele für die Anmeldeinformations- und Zertifikatsdateien.

```
[192.168.1.1]
aws_access_key_id = EMGEZDGNBVGY3TQOJQGEZB5ULEAAIWHWUJDXEXAMPLE
aws_secret_access_key = AUHpqjO0GZQHEYXDbN0neLNlfR0gEXAMPLE
region = snow

[192.168.1.2]
aws_access_key_id = EMGEZDGNBVGY3TQOJQGEZG5O7F3FJUCMYRMI4KPIEXAMPLE
aws_secret_access_key = kY4Cl8+RJAwq/bu28Y8fUJepwqhDEXAMPLE
region = snow
```

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGVla3NhIHNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXDCCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
KJ0FPl2PAYPEjxr81/PoCXfZeARBzN9WLUH5yz1ta+sYUJouzhzWuLJYA1xqcCPY
mhVlkRsN4hVdlBNRnCCpRF766yjdJeibKVzXQxoXoZBjrOkuGwqRy3d3ndjK77h4
OR5Fv9mjGf7CjcaSjk/4iwmZvRSaQacb0YG5GVeb4mfUAuVtuFoMeYfnAgMBAAGj
azBpMAwGA1UdEwQFMAMBAf8wHQYDVR0OBBYEFL/bRcnBRuSM5+FcYFa8HfIBomdF
...
-----END CERTIFICATE-----
```

Konfigurieren von Amazon EKS Anywhere in AWS Snow für den getrennten Betrieb

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 auf die Ausführung in einer Umgebung ohne externe Netzwerkverbindung vorzubereiten.

Informationen zum Konfigurieren von Amazon EKS Anywhere für die getrennte Verwendung mit Ihrer eigenen lokalen, privaten Kubernetes-Registrierung finden Sie unter Registry Mirror-Konfiguration in der EKS Anywhere-Dokumentation.

Wenn Sie ein AMI für die private Registrierung erstellt haben, befolgen Sie die Verfahren in diesem Abschnitt.

Themen

- Konfigurieren der Bol-Registrierung auf einem Snowball-Edge-Gerät
- Verwenden Sie die Bol-Registrierung auf der Amazon EKS Anywhere-Admin-Instance

Konfigurieren der Bol-Registrierung auf einem Snowball-Edge-Gerät

Weitere Informationen finden Sie unter Configure Bol auf einem Snowball-Edge-Gerät.

Verwenden Sie die Bol-Registrierung auf der Amazon EKS Anywhere-Admin-Instance

Weitere Informationen finden Sie unter Importieren von Amazon EKS Anywhere-Container-Images in die lokale Bol-Registrierung auf einem Snowball-Edge-Gerät.

Erstellen und Verwalten von Clustern auf Snowball-Edge-Geräten

Bewährte Methoden für die Erstellung von Clustern

Informationen zum Erstellen eines Amazon EKS Anywhere-Clusters finden Sie unter Erstellen von Snow-Clustern.

Beachten Sie beim Erstellen von Amazon EKS Anywhere-Clustern auf Snowball-Edge-Geräten die folgenden bewährten Methoden:

- Bevor Sie einen Cluster in einem statischen IP-Adressbereich erstellen, stellen Sie sicher, dass sich keine anderen Cluster auf Ihrem Snowball-Edge-Gerät befinden, 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.
- Warten Sie beim Erstellen von mehr als einem Cluster, bis ein Cluster erfolgreich bereitgestellt wurde und ausgeführt wird, bevor Sie einen anderen erstellen.

Aktualisieren von Clustern

Um ein Amazon EKS Anywhere-Administrator-AMI oder EKS-Distro-AMI zu aktualisieren, wenden Sie sich an AWS Support. AWS Support stellt ein Snowball-Edge-Update bereit, das das aktualisierte AMI enthält. Laden Sie dann das Snowball Edge-Update herunter und installieren Sie es. Siehe Herunterladen von Updates und Installieren von Updates.

Nachdem Sie Ihr Amazon EKS Anywhere-AMI aktualisiert haben, müssen Sie eine neue Amazon EKS Anywhere-Administrator-Instance starten. Siehe Ausführen einer Amazon EKS Anywhere-Admin-Instance. Kopieren Sie dann Schlüsseldateien, den Cluster-Ordner, Anmeldeinformationen und Zertifikate von der vorherigen Admin-Instance in die aktualisierte Instance. Diese befinden sich in einem Ordner mit dem Namen für den Cluster.

Bereinigen von Cluster-Ressourcen

Wenn Sie mehrere Cluster auf Ihren Snowball Edge-Geräten erstellen und sie nicht korrekt löschen oder wenn es ein Problem im Cluster gibt und der Cluster nach der Wiederaufnahme Ersatzknoten erstellt, tritt ein Ressourcenleck auf. Ein Beispielskript-Tool steht Ihnen zur Verfügung, das Sie ändern und verwenden können, um Ihre Amazon EKS Anywhere-Admin-Instance und Ihre Snowball-Edge-Geräte zu bereinigen. Weitere Informationen finden Sie unter Amazon EKS Anywhere auf AWS Snow-Cleanup-Tools.

Lokales Verwenden von IAM

AWS Identity and Access Management(IAM) hilft Ihnen, den Zugriff auf AWS Ressourcen, die auf Ihrem AWS Snowball Edge Gerät laufen, 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 zuzuordnen. 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, aber seine Fähigkeit einschränken, neue Amazon EC2-kompatible Instances zu erstellen.

Darüber hinaus können Sie mit AWS Security Token Service (AWS STS) lokale, sitzungsbasierte Anmeldeinformationen auf Ihrem Gerät 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 den Zugriff explizit

zu verweigern. Wir empfehlen, dass Sie Ihre Root-Benutzerzugriffsschlüssel sichern und IAM-Benutzeranmeldeinformationen für die tägliche Interaktion mit Ihrem Gerät erstellen.

> **Important**
>
> Die Dokumentation in diesem Abschnitt bezieht sich auf die lokale Verwendung von IAM auf einem AWS Snowball Edge-Gerät. Hinweise zur Verwendung von IAM in der finden Sie AWS Cloud unterIdentity and Access Management in AWS Snowball.
> Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports.

Themen

Verwenden der AWS CLI und API-Operationen auf Snowball Edge

Wenn Sie die AWS CLI oder API-Operationen verwenden, um IAM-AWS STS, Amazon S3- und Amazon EC2-Befehle auf Snowball Edge auszuführen, müssen Sie das `region` als "“ angeben. `snow` 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
```

Or

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel, die lokal auf AWS Snowball Edge verwendet werden, 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— Hängt die angegebene verwaltete Richtlinie an die angegebene IAM-Rolle an.
- attach-user-policy— Hängt die angegebene verwaltete Richtlinie an den angegebenen Benutzer an.
- 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 Pfad, GUID, ARN und der Vertrauensrichtlinie der Rolle, die die Berechtigung zur Übernahme der Rolle erteilt.
- 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 zu den Zugriffsschlüssel-IDs zurück, die dem angegebenen IAM-Benutzer zugeordnet sind.
- 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 an den angegebenen IAM-Benutzer angehängt sind.
- list-entities-for-policy— Listet alle lokalen IAM-Benutzer, -Gruppen und -Rollen auf, an die die angegebene verwaltete Richtlinie angehängt ist.
  - `--EntityFilter`: Es werden ausschließlich die Werte `role` und `user` unterstützt.
- list-policies — Listet alle verwalteten Richtlinien auf, die in Ihrer Region 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 Berechtigung erteilt, eine Rolle anzunehmen.
- update-role — Aktualisiert die Beschreibung oder die Einstellung für die maximale Sitzungsdauer einer Rolle.
- update-user — Aktualisiert den Namen und/oder den Pfad des angegebenen IAM-Benutzers.

Unterstützte IAM-API-Operationen

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— Hängt die angegebene verwaltete Richtlinie an die angegebene IAM-Rolle an.
- AttachUserPolicy— Hängt die angegebene verwaltete Richtlinie an den angegebenen Benutzer an.
- CreateAccessKey— Erstellt einen neuen lokalen geheimen IAM-Zugriffsschlüssel und die entsprechende AWS Zugriffsschlüssel-ID für den angegebenen Benutzer.
- CreatePolicy— Erstellt eine neue von IAM verwaltete Richtlinie für Ihr Gerät.
- CreateRole— Erzeugt 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, an die die Richtlinie angehängt 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 Pfad, GUID, ARN und der Vertrauensrichtlinie der Rolle, die die Berechtigung zur Übernahme der Rolle erteilt.
- 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 zu den Zugriffsschlüssel-IDs zurück, die dem angegebenen IAM-Benutzer zugeordnet sind.

- ListAttachedRolePolicies— Listet alle verwalteten Richtlinien auf, die der angegebenen IAM-Rolle zugeordnet sind.
- ListAttachedUserPolicies— Listet alle verwalteten Richtlinien auf, die an den angegebenen IAM-Benutzer angehängt 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 sindAWS-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 Berechtigung erteilt, eine Rolle anzunehmen.
- UpdateRole— Aktualisiert die Beschreibung oder Einstellung für die maximale Sitzungsdauer einer Rolle.
- UpdateUser— Aktualisiert den Namen und/oder den Pfad des angegebenen IAM-Benutzers.

Version und Grammatik der unterstützten IAM-Richtlinie

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.

Richtlinientyp	Unterstützte Grammatik
Ressourcenbasierte Richtlinien (Rollenvertrauensrichtlinie)	„`Effect`“, „`Action`“ und „`Principal` “ **Note** Für Principal ist nur AWS-Konto ID oder Principal-ID zulässig.

IAM-Richtlinienbeispiele

Note

AWS Identity and Access Management(IAM) -Benutzer benötigen `"snowballdevice:*"` Berechtigungen, um die AWS OpsHub for Snow FamilyAnwendung zur Verwaltung von Snow Family-Geräten verwenden zu können.

Im Folgenden finden Sie Beispiele für Richtlinien, die Berechtigungen für ein Snowball Edge-Gerät gewähren.

Beispiel 1: Erlaubt den GetUser Aufruf für einen Beispielbenutzer über die IAM-API

Verwenden Sie die folgende Richtlinie, um den GetUser Aufruf für einen Beispielbenutzer über die IAM-API zuzulassen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:GetUser",
            "Resource": "arn:aws:iam:::user/example-user"
        }
    ]
}
```

Beispiel 2: Ermöglicht vollen Zugriff auf die Amazon S3-API

Verwenden Sie die folgende Richtlinie, um vollen Zugriff auf die Amazon S3-API zu gewähren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"

        }
    ]
}
```

Beispiel 3: Ermöglicht Lese- und Schreibzugriff auf einen bestimmten Amazon S3-Bucket

Mit der folgenden Richtlinie ermöglichen Sie den Lese- und Schreibzugriff auf einen bestimmten Bucket.

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

Beispiel 4: Ermöglicht List-, Get- und Put-Zugriff auf einen bestimmten Amazon S3-Bucket

Verwenden Sie die folgende Richtlinie, um List-, Get- und Put-Zugriff auf einen bestimmten S3-Bucket zuzulassen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::examplebucket/*"
        }
    ]
}
```

Beispiel 5: Ermöglicht vollen Zugriff auf die Amazon EC2-API

Verwenden Sie die folgende Richtlinie, um vollen Zugriff auf Amazon EC2 zu gewähren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```

Beispiel 6: Ermöglicht den Zugriff auf das Starten und Stoppen von Amazon EC2-kompatiblen Instances

Verwenden Sie die folgende Richtlinie, um den Zugriff auf das Starten und Stoppen von Amazon EC2-Instances zu gewähren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel 7: Lehnt Anrufe ab, lässt DescribeLaunchTemplates aber alle Anrufe an zu DescribeImages

Mit der folgenden Richtlinie können Sie Aufrufe von `DescribeLaunchTemplates` ablehnen, jedoch alle Aufrufe von `DescribeImages` zulassen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DescribeLaunchTemplates"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel 8: Richtlinie für API-Aufrufe

Listet alle verwalteten Richtlinien auf, die auf Ihrem Snow-Gerät verfügbar sind, einschließlich Ihrer eigenen kundendefinierten verwalteten Richtlinien. Weitere Details finden Sie in den Listenrichtlinien.

```
aws iam list-policies --endpoint http://ip-address:6078 --profile snowballEdge --region
 snow
{
    "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"
        }
    ]
}
```

TrustPolicyBeispiel

Eine Vertrauensrichtlinie gibt eine Reihe temporärer Sicherheitsanmeldeinformationen zurück, mit denen Sie auf AWS Ressourcen zugreifen können, auf die Sie normalerweise möglicherweise 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 AssumeRolein der AWS Security Token ServiceAPI-Referenz.

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

Verwenden von AWS Security Token Service

Das AWS Security Token Service (AWS STS) hilft Ihnen, temporäre Anmeldeinformationen mit eingeschränkten Rechten für IAM-Benutzer anzufordern.

> **Important**
>
> Damit AWS Dienste auf einem Snowball Edge ordnungsgemäß funktionieren, müssen Sie die Ports für die Dienste zulassen. Details hierzu finden Sie unter Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports.

Themen

- Verwenden der AWS CLI und API-Operationen auf Snowball Edge
- Unterstützte AWS STSAWS CLI Befehle auf einem Snowball Edge
- Unterstützte AWS STS-API-Operationen

Verwenden der AWS CLI und API-Operationen auf Snowball Edge

Wenn Sie die AWS CLI oder API-Operationen verwenden, um IAM-AWS STS, Amazon S3- und Amazon EC2-Befehle auf einem Snowball Edge-Gerät auszuführen, müssen Sie das `region` als "“ angeben. `snow` 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
```

Or

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel, die lokal auf AWS Snowball Edge verwendet werden, 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`

Beispiel für den Befehl

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 mit dem AWS CLI eine IAM-Rolle an?

Weitere Informationen zur Verwendung finden Sie unter AWS STS Using Temporary Security Credentials im IAM-Benutzerhandbuch.

Unterstützte AWS STS-API-Operationen

Nur die AssumeRoleAPI wird lokal unterstützt.

Die folgenden Parameter werden für `AssumeRole` unterstützt:

- `RoleArn`
- `RoleSessionName`
- `DurationSeconds`

Beispiel

Sie verwenden Folgendes, um eine Rolle anzunehmen.

```
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

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, Amazon S3 S3-kompatiblem Speicher auf Geräten der Snow Family, Amazon EC2 Systems Manager und AWS STS Snowball 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 inAWS 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 for Snow Family 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 auflisten

Verwenden Sie den `list-certificates` Befehl, um die Amazon-Ressourcennamen (ARNs) für das aktuelle Zertifikat anzuzeigen.

```
snowballEdge list-certificates
```

Example der Ausgabe **`list-certificates`**

```
{
 "Certificates" : [ {
   "CertificateArn" : "arn:aws:snowball-
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7",
   "SubjectAlternativeNames" : [ "192.0.2.0" ]
 } ]
}
```

Zertifikate erhalten

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 unterAngeben des S3-Adapters als AWS CLI Endpunkt.

Zertifikate löschen

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 Neustarten des Snow Family-Geräts oder verwenden Sie ihn`snowballEdge 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.
```

Für die Nutzung von AWS Diensten auf einem AWS Snowball Edge-Gerät erforderliche Ports

Damit AWS Dienste auf einem AWS Snowball Edge-Gerät ordnungsgemäß funktionieren, müssen Sie die Netzwerkanschlüsse für den Dienst zulassen.

Im Folgenden finden Sie eine Liste der Netzwerkports, die für jeden AWS Dienst erforderlich sind.

Port	Protocol (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
9091 (HTTP)	TCP	Endpunkt für die Gerätever waltung

Port	Protocol (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

Verwendung von AWS Snow Device Management für die Verwaltung von Geräten

AWS Snow Device Management Mit können Sie Ihr Snow-Family-Gerät und Ihre lokalen AWS Services remote verwalten. Alle Snow Family-Geräte unterstützen Snow Device Management und werden auf neuen Geräten in den meisten installiert, in AWS-Regionen denen Snow Family-Geräte verfügbar sind.

Mit Snow Device Management können Sie die folgenden Aufgaben ausführen:

- Erstellen einer Aufgabe
- Überprüfen des Aufgabenstatus
- Überprüfen der Aufgabenmetadaten
- Abbrechen einer Aufgabe
- Überprüfen der Geräteinformationen
- Überprüfen des Amazon EC2-compatible Instance-Status
- Auflisten von Befehlen und Syntax
- Auflisten von remote verwalteten Geräten
- Auflisten des Aufgabenstatus über Geräte hinweg
- Auflisten verfügbarer Ressourcen
- Auflisten von Aufgaben nach Status
- Auflisten von Geräte- oder Aufgaben-Tags
- Anwenden von Tags
- Entfernen von Tags

Themen

Auswählen des Snow Device Management-Status beim Bestellen eines Snow Family-Geräts

Wenn Sie einen Auftrag zum Bestellen eines Snow-Geräts erstellen, können Sie auswählen, in welchem Status sich die Snow-Geräteverwaltung befinden wird, wenn Sie das Gerät erhalten: installiert, aber nicht aktiviert oder installiert und aktiviert. Wenn es installiert, aber nicht aktiviert ist, müssen Sie AWS OpsHub oder den Snowball Edge-Client verwenden, um es zu aktivieren, bevor Sie es verwenden. Wenn es installiert und aktiviert ist, können Sie Snow Device Management verwenden, nachdem Sie das Gerät empfangen und mit Ihrem lokalen Netzwerk verbunden haben. Sie können den Status Snow Device Management auswählen, wenn Sie einen Auftrag erstellen, um ein Gerät über die Managementkonsole für die AWS Snow-Familie, den Snowball Edge-ClientAWS CLI, die oder die Snow Job Management API zu bestellen.

So wählen Sie den Status Snow Device Management aus Managementkonsole für die AWS Snow-Familie

1. Um auszuwählen, ob Snow Device Management installiert und aktiviert werden soll, wählen Sie Remote-Verwaltung Ihres Snow-Geräts mit AWS OpsHub oder Snowball-Client aus.
2. Um zu wählen, ob Snow Device Management installiert, aber nicht aktiviert werden soll, wählen Sie Snow-Gerät nicht remote mit AWS OpsHub oder Snowball-Client verwalten aus.

Weitere Informationen finden Sie unter Schritt 3: Wählen Sie Ihre Funktionen und Optionen in diesem Leitfaden.

So wählen Sie den Status Snow Device Management aus der AWS CLI, dem Snowball Edge-Client oder der Snow-Auftragsverwaltungs-API aus:

- Verwenden Sie den `remote-management` Parameter , um den Status Snow Device Management anzugeben. Der `INSTALLED_ONLY` Wert des Parameters bedeutet, dass Snow Device Management installiert, aber nicht aktiviert ist. Der `INSTALLED_AUTOSTART` Wert des Parameters bedeutet, dass Snow Device Management installiert und aktiviert ist. Wenn Sie keinen Wert für diesen Parameter angeben, `INSTALLED_ONLY` ist 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 ADID00000000-0000-0000-0000-000000000000 \
      --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 in der API-Referenz zur Auftragsverwaltung in der AWS Snowball API-Referenz zu .

Aktivieren der Snow Device Management

Gehen Sie wie folgt vor, um Snow Device Management mithilfe des Snowball Edge-Clients 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 Herunterladen und Installieren des Snowball-Clients.
- Laden Sie die Manifestdatei herunter und rufen Sie den Entsperrcode für das Snow Family-Gerät ab. Weitere Informationen finden Sie unter Abrufen Ihrer Anmeldeinformationen und Tools.
- Verbinden Sie das Snow Family-Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihren lokalen Netzwerkgerätespezifikationen.
- Entsperren Sie das Snow Family-Gerät. Weitere Informationen finden Sie unter Entsperren des Snowball-Edge

```
 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 Snow Device Management zu einer IAM-Rolle

Erstellen Sie in der , AWS-Konto aus der das Gerät bestellt wurde, eine AWS Identity and Access Management (IAM)-Rolle und fügen Sie der Rolle die folgende Richtlinie hinzu. Weisen Sie dann die Rolle dem IAM-Benutzer zu, der sich anmeldet, um Ihr Gerät mit Snow Device Management remote zu verwalten. Weitere Informationen finden Sie unter Erstellen von IAM-Rollen und Erstellen eines IAM-Benutzers in Ihrem AWS-Konto.

Richtlinie

```
{
    "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 Snow Device Management

In diesem Abschnitt werden die AWS CLI Befehle beschrieben, mit denen Sie Ihre Snow Family-Geräte remote mit Snow Device Management verwalten können. Sie können auch einige Remote-Verwaltungsaufgaben mit ausführenAWS OpsHub for Snow Family. Weitere Informationen finden Sie unter Verwalten von AWS Services auf Ihrem Gerät.

> **Note**
>
> Bevor Sie Ihr Gerät verwalten, stellen Sie sicher, dass es eingeschaltet und mit Ihrem Netzwerk verbunden ist und eine Verbindung zu dem herstellen kann, AWS-Region in dem es bereitgestellt wurde.

Themen

- Erstellen einer Aufgabe
- Überprüfen des Aufgabenstatus
- Überprüfen der Geräteinformationen
- Überprüfen des Amazon EC2-compatible Instance-Status
- Überprüfen der Aufgabenmetadaten
- Abbrechen einer Aufgabe
- Auflisten von Befehlen und Syntax
- Auflisten von remote verwalteten Geräten
- Auflisten des Aufgabenstatus über Geräte hinweg
- Auflisten verfügbarer Ressourcen
- Auflisten von Geräte- oder Aufgaben-Tags

- Auflisten von Aufgaben nach Status
- Anwenden von Tags
- Entfernen von Tags

Erstellen einer Aufgabe

Um ein oder mehrere Zielgeräte anzuweisen, eine Aufgabe auszuführen, z. B. Entsperren oder Neustarten, verwenden Sie `create-task`. Sie geben Zielgeräte an, indem Sie eine Liste der verwalteten Geräte-IDs mit dem `---targets`Parameter bereitstellen, und geben die Aufgaben an, die mit dem `---command`Parameter ausgeführt werden sollen. Es kann jeweils nur ein Befehl auf einem Gerät 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
InternalServerException
ThrottlingException
AccessDeniedException
ServiceQuotaExceededException
```

Ausgabe

```
{
    "taskId": "st-ficthmqoc2pht111",
    "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
cjkwhmqoc2pht111"
}
```

Überprüfen des Aufgabenstatus

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"
}
```

Überprüfen der Geräteinformationen

Verwenden Sie den `describe-device` Befehl , um gerätespezifische Informationen wie Gerätetyp, Softwareversion, IP-Adressen und Sperrstatus zu überprüfen. Die Ausgabe enthält auch Folgendes:

- `lastReachedOutAt` – als das Gerät zuletzt den kontaktiert hatAWS Cloud. Zeigt an, dass das Gerät online ist.
- `lastUpdatedAt` – Wann Daten zuletzt auf dem Gerät aktualisiert wurden. Gibt 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
InternalServerException
ThrottlingException
AccessDeniedException
```

Ausgabe


```
{
    "associatedWithJob": "JID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",
    "deviceCapacities": [
        {
            "available": 158892032000,
            "name": "HDD Storage",
            "total": 158892032000,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 0,
            "name": "SSD Storage",
            "total": 0,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 3,
            "name": "vCPU",
            "total": 3,
            "unit": "Number",
            "used": 0
        },
        {
            "available": 5368709120,
            "name": "Memory",
            "total": 5368709120,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 0,
            "name": "GPU",
            "total": 0,
            "unit": "Number",
            "used": 0
        }
    ],
    "deviceState": "UNLOCKED",
    "deviceType": "SNC1_HDD",
```

```
    "lastReachedOutAt": "2021-07-23T21:21:56.120000+00:00",
    "lastUpdatedAt": "2021-07-23T21:21:56.120000+00:00",
    "managedDeviceId": "smd-fictqic6gcldf111",
    "managedDeviceArn": "arn:aws:snow-device-management:us-west-2:000000000000:managed-
device/smd-fictqic6gcldf111"
    "physicalNetworkInterfaces": [
        {
            "defaultGateway": "10.0.0.1",
            "ipAddress": "10.0.0.2",
            "ipAddressAssignment": "DHCP",
            "macAddress": "ab:cd:ef:12:34:56",
            "netmask": "255.255.252.0",
            "physicalConnectorType": "RJ45",
            "physicalNetworkInterfaceId": "s.ni-530f866d526d4b111"
        },
        {
            "defaultGateway": "10.0.0.1",
            "ipAddress": "0.0.0.0",
            "ipAddressAssignment": "STATIC",
            "macAddress": "ab:cd:ef:12:34:57",
            "netmask": "0.0.0.0",
            "physicalConnectorType": "RJ45",
            "physicalNetworkInterfaceId": "s.ni-8abc787f0a6750111"
        }
    ],
    "software": {
        "installState": "NA",
        "installedVersion": "122",
        "installingVersion": "NA"
    },
    "tags": {
        "Project": "PrototypeA"
    }
}
```

Überprüfen des Amazon EC2-compatible Instance-Status

Verwenden Sie den `describe-ec2-instances` Befehl , um den aktuellen Status der Amazon EC2-Instance zu überprüfen. Die Ausgabe ähnelt der des `describe-device` Befehls , aber die Ergebnisse stammen aus dem Geräte-Cache in der AWS Cloud und enthalten eine Teilmenge der verfügbaren Felder.

Verwenden Sie den folgenden Befehl, um den Status der Amazon EC2-compatible 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
InternalServerException
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"
        }
    ]
}
```

Überprüfen der Aufgabenmetadaten

Verwenden Sie den `describe-task` Befehl , um die Metadaten für eine bestimmte Aufgabe auf einem Gerät zu überprüfen. Die Metadaten für eine Aufgabe enthalten die folgenden Elemente:

- Die Zielgeräte
- Der Status der Aufgabe
- Wann die Aufgabe erstellt wurde
- Wann Daten zuletzt auf dem Gerät aktualisiert wurden
- Wann die Aufgabe abgeschlossen wurde
- Die Beschreibung (falls vorhanden), die beim Erstellen der Aufgabe bereitgestellt 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
InternalServerException
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

Verwenden Sie den `cancel-task` Befehl , um eine Abbruchanforderung für eine bestimmte Aufgabe zu senden. Sie können nur Aufgaben im `QUEUED` Status abbrechen, die noch nicht ausgeführt wurden. Aufgaben, die bereits ausgeführt werden, können nicht abgebrochen werden.

> **Note**
>
> Eine Aufgabe, die Sie abbrechen möchten, kann weiterhin ausgeführt werden, wenn sie aus der Warteschlange verarbeitet wird, bevor der `cancel-task` Befehl den Status der Aufgabe ändert.

Verwenden Sie den folgenden Befehl, um eine Aufgabe abzubrechen. Ersetzen Sie jeden *`user input placeholder`* durch Ihre Informationen.

Befehl

```
aws snow-device-management cancel-task \
--task-id st-ficthmqoc2pht111
```

Ausnahmen

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
    "taskId": "st-ficthmqoc2pht111"
}
```

Auflisten von Befehlen und Syntax

Verwenden Sie den Befehl , um eine Liste aller unterstützten Befehle für die Snow Device Management API zurückzugebenhelp. Sie können den `help` Befehl auch verwenden, um detaillierte Informationen zu und zur 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 Syntax für einen Befehl zurückzugeben. Ersetzen Sie *command* durch den Namen des Befehls, an dem Sie interessiert sind.

Befehl

```
aws snow-device-management command help
```

Auflisten von remote verwalteten Geräten

Um eine Liste aller Geräte in Ihrem Konto zurückzugeben, für die Snow Device Management in der aktiviert istAWS-Region, in der der Befehl ausgeführt wird, verwenden Sie den `list-devices` Befehl . `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter Verwenden von AWS CLI Paginierungsoptionen im AWSBenutzerhandbuch für die -Befehlszeilenschnittstelle.

Verwenden Sie den folgenden Befehl, um remote verwaltete Geräte aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management list-devices \
--max-results 10
```

Ausnahmen

```
ValidationException
InternalServerException
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": {}
        }
    ]
}
```

Auflisten des Aufgabenstatus über Geräte hinweg

Verwenden Sie den `list-executions` Befehl , um den Status von Aufgaben für ein oder mehrere Zielgeräte zurückzugeben. Um die Rückgabeliste so zu filtern, dass Aufgaben angezeigt werden, die sich derzeit in einem einzigen spezifischen Zustand befinden, verwenden Sie den `--state` Parameter . `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter Verwenden von AWS CLI Paginierungsoptionen im AWSBenutzerhandbuch für die -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
InternalServerException
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
    "executions": [
        {
            "executionId": "1",
            "managedDeviceId": "smd-fictbgr3rbcje111",
            "state": "SUCCEEDED",
            "taskId": "st-ficthmqoc2pht111"
        }
    ]
}
```

Auflisten verfügbarer Ressourcen

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 Amazon EC2-compatible Instances der einzige unterstützte Ressourcentyp. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter Verwenden von AWS CLI Paginierungsoptionen im AWSBenutzerhandbuch für die -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
InternalServerException
ThrottlingException
AccessDeniedException
```

Ausgabe

```
{
    "resources": [
        {
            "id": "s.i-84fa8a27d3e15e111",
            "resourceType": "AWS::EC2::Instance"
        }
    ]
}
```

Auflisten von Geräte- oder Aufgaben-Tags

Verwenden Sie den Befehl , um eine Liste der Tags für ein verwaltetes Gerät oder eine verwaltete Aufgabe zurückzugeben`list-tags-for-resource`.

Verwenden Sie den folgenden Befehl, um die Tags für ein Gerät aufzulisten. Ersetzen Sie den Beispiel-ARN (Amazon Resource Name) 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
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Ausgabe

```
{
    "tags": {
        "Project": "PrototypeA"
    }
}
```

Auflisten von Aufgaben nach Status

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. Um die Ergebnisse nach `IN_PROGRESS`, `COMPLETED`oder `CANCELED` Status zu filtern, verwenden Sie den `---state`Parameter. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter Verwenden von AWS CLI Paginierungsoptionen im AWSBenutzerhandbuch für die -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 K8VAMqKiP2Cf4xGkmH8GMyZrgOF8FUb+d1OKTP9+P4pUb+8PhW+6MiXh4= \
```

```
--max-results 10
```

Ausnahmen

```
ValidationException
InternalServerException
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

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 Komma 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
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Entfernen von Tags

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
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Grundlegendes zu AWS Snowball-Edge-Aufträgen

Ein Auftrag in AWS Snowball ist eine diskrete Arbeitseinheit, die definiert wird, wenn Sie ihn in der Konsole oder der Auftragsverwaltungs-API erstellen. Mit dem AWS Snowball Edge Gerät gibt es drei verschiedene Auftragstypen, von denen alle lokale Speicher- und Rechenfunktionen bieten. Diese Funktionalität verwendet die Dateischnittstelle oder die Amazon S3-Schnittstelle zum Lesen und Schreiben von Daten. Es löst Lambda-Funktionen basierend auf Amazon S3-PUT-Objekt-API-Aktionen aus, die lokal auf dem AWS Snowball Edge Gerät ausgeführt werden.

- Importieren von Aufträgen in Amazon S3 – Die Übertragung von 80 TB oder weniger Ihrer lokalen Daten wurde auf ein einzelnes Gerät kopiert und dann nach Amazon S3 verschoben. Für Importaufträge haben Snowball-Geräte und -Aufträge 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 Auftragstyps zurückgeben, werden diese Daten darin in Amazon S3 importiert.
- Exportieren von Aufträgen aus Amazon S3 – Die Übertragung beliebiger Datenmengen (in Amazon S3), die auf eine beliebige Anzahl von Snowball Edge-Geräten kopiert und dann jeweils ein AWS Snowball Edge Gerät in Ihr On-Premises-Datenziel verschoben werden. Exportaufträge werden bei der Erstellung in Teilaufträge getrennt. Jedem Auftragsteil sind nicht mehr als 80 TB zugeordnet, und jedem Auftragsteil ist genau ein AWS Snowball Edge Gerät zugeordnet. Nach der Rückgabe eines Gerät für diese Auftragsart werden die Daten darauf gelöscht.
- Rein lokale Datenverarbeitungs- und Speicheraufträge – Diese Aufträge umfassen ein AWS Snowball Edge Gerät oder mehrere Geräte, die in einem Cluster verwendet werden. Diese Aufträge beginnen nicht mit Daten in ihren Buckets wie ein Exportauftrag und können am Ende keine Daten wie ein 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 Auftragstyp als Nur lokaler Speicher bezeichnet.

Auftragsdetails

Bevor Sie einen Auftrag erstellen, stellen Sie 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	Detailbeschreibung
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 Identifiz ierung des Auftrags. Die Auftrags-ID befindet sich unten auf dem Versandet ikett 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

Konsolen-ID	API-Kennung	Detailbeschreibung
		Informationen finden Sie unter Versandgeschwindigkeiten.
IAM role ARN (IAM-Rollen-ARN)	RoleARN	Dieser Amazon-Ressourcenname (ARN) ist die AWS Identity and Access Management (IAM)-Rolle, die während der Auftragserstellung mit Schreibberechtigungen für Ihre Amazon S3-Buckets erstellt wird. Der Erstellungsprozess erfolgt automatisch, und die IAM-Rolle, die Sie annehmen könnenAWS Snowball, wird nur verwendet, um Ihre Daten zwischen Ihren S3-Buckets und dem Snowball zu kopieren. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für die Verwendung der AWS Snowball-Konsole.

Konsolen-ID	API-Kennung	Detailbeschreibung
AWS KMS-Schlüssel	`KmsKeyARN`	In verschlüsselt AWS Snowball AWS Key Management Service (AWS KMS) die Schlüssel auf jedem Snowball. Bei der Auftragserstellung können Sie auch einen ARN für einen AWS KMS-Verschlüsselungsschlüssel in Ihrem Besitz auswählen oder erstellen. Weitere Informationen finden Sie unter AWS Key Management Service in AWS Snowball Edge.
Snowball capacity	`SnowballCapacityPreference`	Die Speicherkapazität des in diesem Auftrag geordneten AWS Snowball Geräts. Die verfügbare Größe hängt von Ihrem abAWS-Region.
Storage Service	N/A	Der AWS Speicherservice, der diesem Auftrag zugeordnet ist, in diesem Fall Amazon S3.
Ressourcen	`Resources`	Die AWS Speicherdienstressourcen, die Ihrem Auftrag zugeordnet sind. In diesem Fall sind dies die Amazon S3-Buckets, in die oder aus denen Ihre Daten übertragen werden.

Konsolen-ID	API-Kennung	Detailbeschreibung
Job type	`JobType`	Die Art des Auftrags – Import bzw. Export oder lokale Datenverarbeitung und Speicher.
Snowball type	`SnowballType`	Der Typ des in diesem Auftrag geordneten Snow Family-Ge räts.
Cluster ID	`ClusterId`	Eine eindeutige Bezeichnung mit 39 Zeichen zur Identifiz ierung Ihres Clusters.

Job Statuses

Jeder AWS Snowball Edge Geräteauftrag hat den Status , der sich ändert, um den aktuellen Status des Auftrags anzugeben. Der Auftragsstatus enthält keine Informationen zur Integrität, dem aktuellen Verarbeitungsstatus und dem auf den zugeordneten Geräten verbrauchten Speicher.

So zeigen Sie den Status eines Auftrags an

1. Melden Sie sich bei der anManagementkonsole für die AWS Snow-Familie.
2. Wählen Sie im Auftrags-Dashboard den Auftrag aus.
3. Klicken Sie in der Konsole auf Ihren Auftragsnamen.
4. Der Bereich Auftragsstatus befindet sich oben und gibt den Status des Auftrags an.

AWS Snowball Edge Status von Geräteaufträgen

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).
Vorbereiten der Appliance	`PreparingAppliance`	AWS bereitet ein Gerät für Ihren Auftrag vor.
Exporting	`InProgress`	AWS exportiert Ihre Daten aus Amazon S3 auf ein Gerät.
Preparing shipment	`PreparingShipment`	AWS bereitet sich darauf vor, ein Gerät an Sie zu senden. Die erwarteten Versandverfolgungsinformationen werden für Kunden mit dem 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
Während der Übertragung zu AWS	`InTransitToAWS`	Sie haben das Gerät an zurückgesendetAWS.
Im Sortierzentrum	`WithAWSSortingFacility`	Das Gerät, das für diesen Auftrag notwendig ist, befindet sich in unserem internen Sortierzentrum. Jede zusätzliche Verarbeitung für Importaufträge in Amazon S3 beginnt in Kürze, in der Regel innerhalb von 2 Tagen.
At AWS	`WithAWS`	Ihre Sendung ist bei angekommenAWS. 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).
Completed	`Complete`	Ihr Auftrag bzw. ein Teil Ihres Auftrags wurde erfolgreich abgeschlossen.

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
Canceled	`Cancelled`	Ihr Auftrag wurde abgebrochen.

Cluster-Status

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 Cluster-Anforderung zu beginnen. Damit ein Cluster erstellt werden kann, muss er über mindestens fünf Knoten verfügen.
Ausstehend	`Pending`	Der Cluster wurde erstellt. Wir bereiten die Knoten für den Versand vor. Sie können den Status der einzelnen Knoten über deren jeweilige

Konsolenbezeichner	API-Bezeichner	Statusbeschreibung
		n 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 an zurückgegebenAWS.
Canceled	`Cancelled`	Die Anforderung zur Erstellung eines Clusters wurde storniert. Cluster-A nforderungen können nur abgebrochen werden, wenn sie den ausstehenden Status noch nicht erreicht haben.

Importieren von Aufträgen in Amazon S3

Bei einem Importauftrag werden Ihre Daten mit dem integrierten Amazon S3-Adapter oder NFS-Mountingpunkt auf das AWS Snowball Edge Gerät 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 Funktionalität verwendet die Dateischnittstelle oder den Amazon S3-Adapter zum Lesen und Schreiben von Daten und löst Lambda-Funktionen aus, die auf Amazon S3-PUT-Objekt-API-Aktionen basieren, die lokal auf dem AWS Snowball Edge Gerät ausgeführt werden.

Wenn alle Ihre Daten in die angegebenen Amazon S3-Buckets in der importiert wurdenAWS Cloud, AWS führt eine vollständige Löschung des Geräts durch. 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.

Exportieren von Aufträgen aus Amazon S3

> **Note**
>
> Tags und Metadaten werden derzeit NICHT unterstützt, d. h. alle Tags und Metadaten werden beim Exportieren von Objekten aus S3-Buckets entfernt.

Ihre Datenquelle für einen Exportauftrag ist ein oder mehrere Amazon S3-Buckets. Nachdem die Daten für einen Auftragsteil von Amazon S3 auf ein AWS Snowball Edge Gerät verschoben 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 benötigt werden. Jedes AWS Snowball Edge Gerät für die Auftragsteile eines Exportauftrags wird nacheinander geliefert, wobei nachfolgende Geräte an Sie gesendet werden, nachdem der vorherige Auftragsteil in den Status Bei der Übertragung in AWS wechselt.

Wenn Sie Objekte mithilfe des Amazon S3-Adapters oder des NFS-Mounting-Punkts von einem Gerät in Ihr On-Premises-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 Funktionalität verwendet die Dateischnittstelle oder den Amazon S3-Adapter zum Lesen und Schreiben von Daten und löst Lambda-Funktionen aus, die auf Amazon S3-PUT-Objekt-API-Aktionen basieren, die lokal auf dem AWS Snowball Edge Gerät ausgeführt werden.

Wenn AWS ein zurückgeschicktes Gerät erhält, wird dieses vollständig gemäß NIST 800-88-Standard gelöscht.

> **Important**
>
> Daten, die Sie auf ein Snow-Gerät exportieren möchten, müssen sich in Amazon S3 befinden. Alle Daten in Amazon S3 Glacier , die Sie auf das Snow-Gerät exportieren möchten, müssen aufgetaut oder in die S3-Speicherklasse 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-Objekte erst, wenn Sie überprüfen können, ob der gesamte Inhalt für den gesamten Auftrag in Ihr On-Premises-Datenziel kopiert wurde.

Wenn Sie einen Exportauftrag erstellen, können Sie einen gesamten Amazon S3-Bucket oder einen bestimmten Bereich von Objektschlüsseln exportieren.

Verwenden von Exportbereichen

Wenn Sie einen Exportauftrag in der Managementkonsole für die AWS Snow-Familie oder mit der Auftragsverwaltungs-API erstellen, können Sie einen gesamten Amazon 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 sowohl vor englischen Groß- als auch 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 in Wikipedia .

Beispiele für Exportbereiche

Angenommen, Sie haben einen Bucket mit den folgenden Objekten und Präfixen, sortiert in binärer UTF-8-Reihenfolge:

- 01
- Aardvark
- Aardwolf
- Aasvogel/apple
- Aasvogel/Pfeil/Objekt1
- Aasvogel/Pfeil/Objekt2
- Aasvogel/banana
- Aasvogel/Banker/Objekt1
- Aasvogel/Banker/Objekt2
- Aasvogel/cherry
- Banana
- Car

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
(Keine)	(Keine)	Alle Objekte in Ihrem Bucket
(Keine)	Aasvogel	01 Aardvark

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
		Aardwolf Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2 Aasvogel/cherry

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
(Keine)	Aasvogel/banana	01 Aardvark Aardwolf Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Aasvogel	(Keine)	Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2 Aasvogel/cherry Banana Car

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Aardwolf	(Keine)	Aardwolf Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2 Aasvogel/cherry Banana Car

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Aar	(Keine)	Aardvark Aardwolf Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2 Aasvogel/cherry Banana Car

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im 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 das Auto gemäß den UTF-8-Binärwerten unter Auto sortiert ist.
Aar	Aarrr	Aardvark Aardwolf
Aasvogel/Pfeil	Aasvogel/ArSpeed	Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Aasvogel/apple	Aasvogel/banana	Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana
Aasvogel/apple	Aasvogel/Banker	Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Aasvogel/apple	Aasvogel/cherry	Aasvogel/apple Aasvogel/Pfeil/Objekt1 Aasvogel/Pfeil/Objekt2 Aasvogel/banana Aasvogel/Banker/Objekt1 Aasvogel/Banker/Objekt2 Aasvogel/cherry

Angenommen, Sie haben diese drei Buckets und möchten alle Objekte aus Ordner2 kopieren.

- s3://bucket/folder1/
- s3://bucket/folder2/
- s3://bucket/folder3/

Angegebener Bereich beginnt	Angegebenes Bereichsende	Objekte im Bereich, der exportiert werden soll
Ordner2/	Ordner2/	Alle Objekte im Bucket-Ordner2.

Bewährte Methoden für Exportaufträge

- Sicherstellen, dass sich die Daten in Amazon S3 befinden, Stapeln kleiner Dateien vor der Bestellung des Auftrags
- Sicherstellen, dass Schlüsselbereiche in der Definition des Exportauftrags angegeben sind, wenn sich Millionen von Objekten in Ihrem Bucket befinden
- Aktualisieren Sie Objektschlüssel, um den Schrägstrich im Namen zu entfernen, da Objekte mit abschließenden Schrägstrichen in ihren Namen (/ oder \) nicht an Snowball Edge übertragen werden
- Für S3-Buckets beträgt die Begrenzung der Objektlänge 255 Zeichen.
- Für S3-Buckets, die versionsfähig sind, wird nur die aktuelle Version von Objekten exportiert.
- Löschmarkierungen werden nicht exportiert.

Rein lokale Datenverarbeitungs- und Speicheraufträge

Lokale Datenverarbeitungs- und Speicheraufträge ermöglichen es Ihnen, Amazon S3-kompatiblen Speicher auf Geräten der Snow Family lokal 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

Lokale Speicheraufträge

Sie können Objekte mit Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten oder dem S3-Adapter auf ein AWS Snowball Edge Gerät lesen und schreiben. Wenn Sie ein Gerät bestellen und den S3-Adapter verwenden möchten, wählen Sie auch aus, welche Amazon S3-Buckets beim Empfang auf dem Gerät enthalten sein werden. Wenn Sie sich dafür entscheiden, Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten zu verwenden, sind beim Empfang keine Amazon S3-Buckets auf dem Gerät enthalten.

Sie können Amazon S3-Buckets auf den Snowball-Edge-Geräten erstellen, um Objekte On-Premises für Anwendungen zu speichern und abzurufen, die einen lokalen Datenzugriff, eine lokale Datenverarbeitung und eine lokale Datenresidenz erfordern. Amazon-S3-kompatibler Speicher auf Snow-Family-Geräten bietet eine neue Speicherklasse, `SNOW`, die die Amazon S3-APIs verwendet und darauf ausgelegt ist, Daten über mehrere Snowball-Edge-Geräte hinweg dauerhaft und redundant zu speichern. Sie können dieselben APIs und Funktionen für Snowball Edge-Buckets wie für Amazon S3 verwenden, einschließlich Bucket-Lebenszyklusrichtlinien, Verschlüsselung und Tagging. Wenn das Gerät oder die Geräte an zurückgegeben werdenAWS, werden alle Daten, die im Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten erstellt oder gespeichert werden, gelöscht. Weitere Informationen finden Sie unter Lokale Datenverarbeitungs- und reine Speicheraufträge.

Weitere Informationen finden Sie unter Amazon S3-kompatibler Speicher auf Snow-Family-Geräten in diesem Handbuch.

Wenn Sie das Gerät nicht mehr verwenden, geben Sie es an zurückAWS, und das Gerät wird gelöscht. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Lokale Cluster-Option

Ein Cluster ist eine logische Gruppierung von Snowball-Edge-Geräten in Gruppen von 3 bis 16 Geräten. Ein Cluster wird als einzelner Auftrag erstellt. Dies ermöglicht eine höhere Dauerhaftigkeit und mehr Speicher im Vergleich zu anderen AWS Snowball-Auftragsangeboten. Weitere Informationen zu Cluster-Aufträgen finden Sie unter Clustering-Übersicht in diesem Handbuch.

Klonen eines Auftrags in der Konsole

Wenn Sie zum ersten Mal einen Importauftrag oder einen lokalen Datenverarbeitungs- 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 Auftrags bedeutet, dass er genau neu erstellt wird, 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 Auftrag aus der Tabelle.
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 Aufträge erhalten Namen im Format ***`Auftragsname`***-clone-***`Zahl`***. 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 Auftrag AprilFinanceReports und DataCenterMigration-clone-42 für den vierzigsekündigen Klon des DataCenterMigration Auftrags.

Bewährte Methoden für die Verwendung des Snowball Edge-Geräts

Wir empfehlen Ihnen, diese bewährten Methoden zu befolgen, um den größtmöglichen Nutzen und die maximale Zustimmung zu Ihrem AWS Snowball Edge Gerät zu erzielen.

Sicherheit

Im Folgenden finden Sie Empfehlungen und bewährte Methoden für die Aufrechterhaltung der Sicherheit bei der Arbeit mit einem - AWS Snowball Edge Gerät.

Allgemeine Sicherheit

- Wenn Sie etwas bemerken, das beim AWS Snowball Edge Gerät verdächtig aussieht, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie sich stattdessen an AWS Support, um ein neues AWS Snowball Edge Gerät zu erhalten.
- Es wird empfohlen, keine Kopie des Entsperrcodes am selben Speicherort auf der Workstation als Manifest für diesen Auftrag zu speichern. Wenn Sie diese an verschiedenen Standorten speichern, können Sie verhindern, dass sich Unbefugte Zugriff auf das AWS Snowball Edge Gerät verschaffen. 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 Dateien haben, die auf dem Server gespeichert sind, und auf die E-Mail-Adresse des Benutzers.
- Die angezeigten Anmeldeinformationen sind ein Paar von Zugriffsschlüsseln, die für den Zugriff auf Ihr Gerät verwendet werden get-secret-access-key, wenn Sie die Snowball Edge-Clientbefehle list-access-keys und ausführen.

  Diese Schlüssel sind ausschließlich dem Auftrag und den lokalen Ressourcen auf dem Gerät zugeordnet. Sie sind nicht Ihrem AWS-Konto oder einem anderen zugeordnet AWS-Konto. Wenn Sie versuchen, diese Schlüssel für den Zugriff auf Services und Ressourcen in der zu verwenden AWS Cloud, schlagen sie fehl, da sie nur für die lokalen Ressourcen funktionieren, die Ihrem Auftrag zugeordnet sind.
- Wenn Sie der Meinung sind, dass Ihre Anmeldeinformationen verloren gehen oder kompromittiert wurden, fordern Sie eine neue Manifestdatei an und entsperren Sie Code, indem Sie den Prozess zum Aktualisieren des SSL-Zertifikats des Geräts befolgen. Siehe Aktualisieren des SSL-Zertifikats.

Weitere Informationen zur Verwendung von AWS Identity and Access Management (IAM)-Richtlinien zum Steuern des Zugriffs finden Sie unter AWS-verwaltete (vordefinierte) Richtlinien für AWS Snowball Edge.

Netzwerksicherheit

- Wir empfehlen, jeweils nur eine Methode zum Lesen und Schreiben von Daten in einen lokalen Bucket auf einem - AWS Snowball Edge Gerät zu verwenden. Die gleichzeitige Verwendung der Dateischnittstelle und des Amazon S3-Adapters auf demselben Amazon S3-Bucket kann zu Lese-/Schreibkonflikten führen.
- Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie das AWS Snowball Edge Gerät nicht und ändern Sie nicht dessen Netzwerkeinstellungen während der Übertragung von Daten.
- Dateien, die auf dem Gerät in geschrieben werden, sollten sich in einem statischen Zustand befinden. Dateien, die geändert werden, während sie in geschrieben werden, können zu Lese-/Schreibkonflikten führen.
- Weitere Informationen zur Verbesserung der Leistung Ihres AWS Snowball Edge Geräts finden Sie unter Leistung.

Ressourcenmanagement

Beachten Sie die folgenden bewährten Methoden für die Verwaltung von Aufträgen und Ressourcen auf Ihrem AWS Snowball Edge Gerät.

- Die 10 kostenlosen Tage für die Durchführung Ihrer On-Premises-Datenübertragung beginnen an dem Tag, nachdem das AWS Snowball Edge Gerät in Ihrem Rechenzentrum angekommen ist. Dies gilt nur für Snowball Edge-Gerätetypen.
- Sie können einen Auftrag nur im Status Job created (Job wurde erstellt) abbrechen. Wenn sich ein Auftrag in einen anderen Status ändert, können Sie den Auftrag nicht abbrechen. Dies gilt für Cluster.
- Löschen Sie bei Importaufträgen Ihre lokalen Kopien der übertragenen Daten erst, wenn der Import in Amazon S3 erfolgreich ist. Stellen Sie als Teil des Vorgangs sicher, die Ergebnisse der Datenübertragung zu überprüfen.

Leistung

> **Note**
>
> Die Datenübertragungsleistung variiert je nach Netzwerkumgebung, Betriebssystemen, Kopiermethode, Protokoll, Leseleistung der Quelldaten und Datensatzmerkmalen wie Dateigröße. Um die genauen Datenübertragungsraten und Datenübertragungszeiten zu ermitteln, empfehlen wir Ihnen, die Leistung durch 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 On-Premises-Umgebungen eine andere Art von Ausführung haben – unterschiedliche Netzwerktechnologien, unterschiedliche Hardware, verschiedene Betriebssysteme, unterschiedliche Verfahren usw.

In der folgenden Tabelle wird beschrieben, wie sich die Übertragungsrate Ihres Netzwerks auf die Dauer auswirkt, die benötigt wird, um ein Snowball-Edge-Gerät mit Daten zu füllen. Das Übertragen kleinerer Dateien reduziert Ihre Übertragungsgeschwindigkeit aufgrund des erhöhten Aufwands. Wenn Sie viele kleine Dateien haben, empfehlen wir Ihnen, sie in größere Archive zu komprimieren, bevor Sie sie auf ein Snowball-Edge-Gerät übertragen.

Geschwindigkeit (MB/s)	Übertragungszeit von 82 TB
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
60	15.53 Tage

Geschwindigkeit (MB/s)	Übertragungszeit von 82 TB
30	31.06 Tage
10	85.42 Tage

In den folgenden Abschnitten wird beschrieben, wie Sie bestimmen, wann das AWS Snowball Edge Gerät verwendet werden soll und wie Sie den Service optimal nutzen können.

Themen

Empfehlungen zur Leistung

Die folgenden Methoden werden dringend empfohlen, da sie die größten Auswirkungen 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 haben, die kleiner als 1 MB sind, empfehlen wir Ihnen, sie in größere Archive zu komprimieren, bevor Sie sie auf ein Snowball-Edge-Gerät übertragen.

Datenübertragung beschleunigen

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 auf das Gerät auf folgende Weise verbessern. Die folgende Liste ist von den größten bis hin zu den geringsten positiven Auswirkungen auf die Leistung angeordnet:

1. Führen Sie mehrere Schreibvorgänge gleichzeitig aus – Führen Sie dazu jeden Befehl von mehreren Terminalfenstern auf einem Computer mit einer Netzwerkverbindung zu einem einzigen AWS Snowball Edge Gerät aus.

2. Übertragen kleiner Dateien in Batches – Jeder Kopiervorgang hat aufgrund der Verschlüsselung einen gewissen Overhead. Um den Prozess zu beschleunigen, können Sie Dateien in einem einzigen Archiv zusammenfassen. Wenn Sie Dateien zusammenfassen, können sie automatisch extrahiert werden, wenn sie in Amazon S3 importiert werden. Weitere Informationen finden Sie unter Batching kleiner Dateien.
3. Führen Sie während der Übertragung keine anderen Operationen für Dateien aus – Das Umbenennen von Dateien während der Übertragung, das Ändern ihrer Metadaten oder das Schreiben von Daten in die Dateien während eines Kopiervorgangs hat negative Auswirkungen auf die Übertragungsleistung. Wir empfehlen, den Status der Dateien nicht zu verändern, während sie gesendet werden.
4. Reduzieren der lokalen Netzwerknutzung – Ihr AWS Snowball Edge Gerät kommuniziert über Ihr lokales Netzwerk. So können Sie die Datenübertragungsgeschwindigkeiten verbessern, indem Sie den übrigen 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 unnötiger Hops – Wir empfehlen Ihnen, Ihr AWS Snowball Edge Gerät, Ihre Datenquelle und den Computer einzurichten, auf dem die Terminalverbindung zwischen ihnen ausgeführt wird, damit sie die einzigen Maschinen sind, die über einen einzigen Schalter kommunizieren. Dies kann die Datenübertragungsgeschwindigkeit verbessern.

Aktualisieren von Software auf Snowball-Edge-Geräten

AWS benachrichtigt Sie, wenn neue Software für Ihre Snow-Family-Geräte verfügbar ist. Die Benachrichtigung wird per E-Mail AWS Health Dashboard und als CloudWatch Ereignis bereitgestellt. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die dem AWS Konto zugeordnet ist, das zum Bestellen des Snow Family-Geräts verwendet 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 Ihrer Nutzung des Geräts zu vermeiden. Weitere Informationen zu AWS Health Dashboard finden Sie im AWS Health -Benutzerhandbuch. Weitere Informationen zu - CloudWatch Ereignissen finden Sie im Amazon CloudWatch Events-Benutzerhandbuch.

Sie können Software-Updates von herunterladen AWS und auf Snowball Edge-Geräten in Ihren On-Premises-Umgebungen installieren. Diese Aktualisierungen erfolgen im Hintergrund. Sie können Ihre Geräte weiterhin wie gewohnt verwenden, während die neueste Software sicher von AWS auf Ihr Gerät heruntergeladen wird. Um heruntergeladene Updates anzuwenden, müssen Sie jedoch Workloads auf dem Gerät beenden und neu starten.

Softwareupdates, die von AWS für Snowball Edge/Snowcone-Geräte (-Appliances) bereitgestellt werden, sind Appliance Software gemäß Abschnitt 9 der -Servicebedingungen.

Die Software-Updates werden ausschließlich für die Installation der Software-Updates auf der entsprechenden Appliance im Namen von bereitgestellt AWS. Sie werden (oder versuchen, dies zu tun) und werden Dritten nicht erlauben oder autorisieren, (i) andere Kopien der Software-Updates als die für die Installation der Software-Updates auf der entsprechenden Appliance erforderlichen zu erstellen oder (ii) Features oder Maßnahmen in den Software-Updates zu umgehen oder zu deaktivieren, einschließlich, aber nicht beschränkt auf jegliche Verschlüsselung, die auf das Software-Update angewendet wird. Sobald die Softwareupdates auf der entsprechenden Appliance installiert wurden, erklären Sie sich damit einverstanden, die Softwareupdates von allen Medien zu löschen, die bei der Installation der Softwareupdates auf der Appliance verwendet werden.

> **Warning**
>
> Wir empfehlen dringend, alle Aktivitäten auf Ihrem Gerät auszusetzen, bevor Sie das Update installieren. Wenn Sie das Gerät aktualisieren und neu starten, werden keine Instances mehr ausgeführt und alle Schreibvorgänge in lokale Amazon S3-Buckets werden unterbrochen.

Themen

Voraussetzungen

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.
- Das Aktualisieren 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 mit dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients.
- (Optional) Wir empfehlen Ihnen, ein Profil für den Snowball-Edge-Client zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Profils für den Snowball Edge Client
- Für Amazon S3-kompatiblen Speicher auf Snow-Family-Geräten auf gruppierten Snowball-Edge-Geräten beenden Sie den S3-Snow-Service und deaktivieren Sie den automatischen Start dafür. Siehe Konfigurieren des Amazon S3-kompatiblen Speichers auf Snow-Family-Geräten für den automatischen Start.

> **Note**
>
> Bei gruppierten 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.

Herunterladen von Updates

Es gibt zwei primäre Möglichkeiten, ein Update für Snow Family-Geräte herunterzuladen:

- Sie können manuelle Updates jederzeit mit bestimmten Snowball Edge-Clientbefehlen 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 zum automatischen Aktualisieren Ihres Snowball-Edge-Geräts finden Sie `configure-auto-update-strategy` unter Aktualisieren eines Snowball-Edge.

> **Note**
>
> Wenn Ihr Gerät keinen Zugriff auf das Internet hat, können Sie eine Aktualisierungsdatei mit der GetSoftwareUpdates-API herunterladen. Verweisen Sie dann auf einen lokalen Dateispeicherort, wenn Sie `download-updates` mit dem `uri` Parameter aufrufen, wie im folgenden Beispiel.
>
> ```
> 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
> ```

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 mit dem `describe-device` Befehl entsperrt ist. Wenn das Gerät gesperrt ist, entsperren Sie es mit dem Befehl `unlock-device`. Weitere Informationen finden Sie unter Entsperren des Snow Family-Geräts.
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 aktuelle Version zurück, die auf dem Gerät installiert ist.

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 heruntergeladenen Datei aus, wie im folgenden Beispiel.
   >
   > ```
   > 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 Geräte-Cluster und laden sie herunter

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass alle Snowball Edge-Geräte im Cluster mit dem `snowballEdge describe-device` Befehl entsperrt werden. Wenn die Geräte gesperrt sind, entsperren Sie sie mit dem `snowballEdge unlock-cluster` Befehl . Weitere Informationen finden Sie unter Entsperren des Snowball Edge.
2. Wenn alle Geräte im Cluster entsperrt sind, führen Sie für jedes Gerät im Cluster den `check-for-updates` Befehl aus. Dieser Befehl gibt die neueste verfügbare Version der Snowball Edge-Software sowie die aktuelle Version zurück, die auf dem Gerät installiert ist.

```
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 eine Aktualisierung 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`, wird das Update heruntergeladen und kann installiert werden.

Installieren von Updates

Nach dem Herunterladen von Updates 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.

Bei Clustern von Snowball Edge-Geräten muss das Update auf jedes Gerät im Cluster heruntergeladen und installiert werden.

> **Note**
>
> Halten Sie alle Aktivitäten auf dem Gerät an, bevor Sie Softwareupdates installieren. Durch die Installation von Updates werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät unterbrochen. Dies kann zu Datenverlust führen

So installieren Sie Softwareupdates, die bereits auf eigenständige Snow-Family-Geräte heruntergeladen wurden

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das Snowball Edge-Gerät mit dem `describe-device` Befehl entsperrt ist. Wenn das Gerät gesperrt ist, entsperren Sie es mit dem Befehl `unlock-device`. Weitere Informationen finden Sie unter Entsperren des Snowball Edge.
2. Führen Sie den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Services anzuzeigen. Der Befehl gibt die Service-IDs jedes auf dem Gerät verfügbaren Services zurück.

   ```
   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 Service-ID den `describe-service` Befehl aus, um den Status anzuzeigen. Verwenden Sie diese Informationen, um Services zu identifizieren, die angehalten 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` Service aktiv ist und mit dem `stop-service` Befehl gestoppt werden muss.

4. Verwenden Sie den `stop-service` Befehl , um jeden Service zu beenden, bei dem sich der Wert des `State` Namens `ACTIVE` in der Ausgabe des `list-services` Befehls befindet. Wenn mehr als ein Service ausgeführt wird, beenden Sie jeden Service, bevor Sie fortfahren.

> **Note**
>
> Der Amazon S3-Adapter AWS STS, Amazon EC2 und die IAM-Services können nicht gestoppt werden. Wenn Amazon S3-kompatibler Speicher auf Snow-Family-Geräten ausgeführt wird, halten Sie ihn an, bevor Sie Updates installieren. Amazon S3-kompatibler Speicher auf Snow-Family-Geräten 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 **`stop-service`** Befehls

```
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 den Status mit diesem Befehl an.

   Beispielausgabe

   ```
   Install State: Installing //Possible values[NA, Installing, Requires
   Reboot]
   ```

   Sie haben erfolgreich ein Software-Update 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**
   >
   > Ein Neustart Ihres Snow Family-Geräts, ohne alle Aktivitäten auf dem Gerät zu beenden, kann zu Datenverlust führen.

7. Wenn alle Services auf dem Gerät angehalten 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 Neustarten des Geräts finden Sie unter Neustarten des Snow-Family-Geräts Weitere Informationen zum Entsperren des Geräts finden Sie unter Entsperren des 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, entsperren Sie sie mit dem `unlock-cluster` Befehl . Weitere Informationen finden Sie unter Entsperren des Snowball Edge.
2. Führen Sie für jedes Gerät im Cluster den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Services anzuzeigen. Der Befehl gibt die Service-IDs jedes auf dem Gerät verfügbaren Services zurück.

   ```
   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 Service-ID den `describe-service` Befehl aus, um den Status anzuzeigen. Verwenden Sie diese Informationen, um Services zu identifizieren, die angehalten 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` Service aktiv ist und mit dem `stop-service` Befehl gestoppt werden muss.

4. Verwenden Sie für jedes Gerät im Cluster den `stop-service` Befehl , um jeden Service zu beenden, bei dem sich der Wert des `State` Namens `ACTIVE` in der Ausgabe des `list-services` Befehls befindet. Wenn mehr als ein Service ausgeführt wird, beenden Sie jeden Service, bevor Sie fortfahren.

> **Note**
>
> Der Amazon S3-Adapter AWS STS, Amazon EC2 und die IAM-Services können nicht gestoppt werden. Wenn Amazon S3-kompatibler Speicher auf Snow-Family-Geräten ausgeführt wird, halten Sie ihn an, bevor Sie Updates installieren. Amazon S3-kompatibler Speicher auf Snow-Family-Geräten 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 **`stop-service`** Befehls

```
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 der `Install State` ist`Requires Reboot`, 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**
>
> Ein Neustart des Snowball Edge-Geräts, ohne alle Aktivitäten auf dem Gerät zu beenden, kann zu Datenverlust führen.

7. Starten Sie alle Geräte im Cluster neu, entsperren Sie den Cluster und starten Sie alle Geräte im Cluster erneut neu. Damit ist die Installation der heruntergeladenen Softwareupdates abgeschlossen. Weitere Informationen zum Neustarten der Geräte finden Sie unter Neustarten

des Snow Family-Geräts. Weitere Informationen zum Entsperren des Geräte-Clusters finden Sie unter Entsperren des Snowball Edge.

8. Nachdem jedes Gerät im Cluster zweimal neu gestartet wurde, entsperren Sie den Cluster und verwenden Sie dann den `check-for-updates` Befehl , um zu überprüfen, 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 nun das Snow Family-Gerät oder den Gerätecluster erfolgreich aktualisiert und bestätigt, dass das Update auf die neueste Snow Family-Software durchgeführt wurde.

Aktualisieren des SSL-Zertifikats

Wenn Sie planen, Ihr Snow Family-Gerät länger als 360 Tage aufzubewahren, müssen Sie das Secure Sockets Layer (SSL)-Zertifikat auf dem Gerät aktualisieren, um eine Unterbrechung Ihrer Gerätenutzung zu vermeiden. Wenn das Zertifikat abläuft, können Sie das Gerät nicht verwenden und müssen es an zurückgeben AWS.

AWS benachrichtigt Sie 30 Tage, bevor das SSL-Zertifikat für Ihre Snow-Family-Geräte abläuft. Die Benachrichtigung wird per E-Mail AWS Health Dashboard und als CloudWatch Ereignis bereitgestellt. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die dem AWS Konto zugeordnet ist, das zum Bestellen des Snow Family-Geräts verwendet 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 finden Sie AWS Health Dashboard im AWS Health - Benutzerhandbuch. Weitere Informationen zu - CloudWatch Ereignissen finden Sie im Amazon CloudWatch Events-Benutzerhandbuch.

Das Aktualisieren 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 mit dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter Verwenden des Snowball Edge Clients

In diesem Thema wird erläutert, wie Sie bestimmen, wann das Zertifikat abläuft und wie Sie Ihr Gerät aktualisieren.

1. Verwenden Sie den `snowballEdge describe-device-software` Befehl , um zu bestimmen, wann das Zertifikat abläuft. In der Ausgabe des Befehls `CertificateExpiry` enthält der Wert von das Datum und die Uhrzeit, zu der 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. Wenden Sie sich an AWS Support und fordern Sie ein SSL-Zertifikatsupdate an.
3. AWS Support stellt eine Aktualisierungsdatei bereit. Laden Sie die Aktualisierungsdatei herunter und install ieren Siesie.
4. Verwenden Sie den neuen Entsperrcode und die Manifestdatei, wenn Sie den Snowball Edge Entsperren eines Geräts entsperren.

Aktualisieren Ihrer Amazon Linux 2-AMIs auf Snow Family-Geräten

Als bewährte Methode für die Sicherheit sollten Sie Ihre Amazon Linux 2-AMIs up-to-date auf Geräten der Snow Family aufbewahren. Überprüfen Sie regelmäßig das Amazon Linux 2 AMI (HVM), SSD-Volume-Typ (64-Bit x86) in der AWS Marketplace auf Updates. Wenn Sie feststellen, dass Sie Ihr AMI aktualisieren müssen, importieren Sie das neueste Amazon Linux 2-Image auf das Snow-Gerät. Weitere Informationen finden Sie unter Importieren eines Images auf Ihr Gerät als Amazon EC2-compatible 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. Beispielsweise:

```
ami-0ccb473bada910e74
```

Sicherheit für AWS Snowball Edge

Cloud-Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die entwickelt wurde, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der ausführt AWS Cloud. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für gelten AWS Snowball, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -Services.
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. 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 geteilten Verantwortung bei der Verwendung von einsetzen können AWS Snowball. Die folgenden Themen veranschaulichen, wie Sie konfigurieren, AWS Snowball um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer - AWS Snowball Ressourcen unterstützen.

Themen

Datenschutz in AWS Snowball Edge

AWS Snowball entspricht dem AWS -Modell der übergreifenden Verantwortlichkeit, das Vorschriften und Richtlinien für den Datenschutz enthält. AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die alle - AWS Services ausführt. AWS behält die Kontrolle über die in dieser Infrastruktur gehosteten Daten, einschließlich der Sicherheitskonfigurationskontrollen für den Umgang mit Kundeninhalten und personenbezogenen Daten. - AWS Kunden und APN-Partner, die entweder als Datenverantwortliche oder Datenverarbeiter fungieren, sind für alle personenbezogenen Daten verantwortlich, die sie in der speichern AWS Cloud.

Aus Datenschutzgründen empfehlen wir, die AWS-Konto Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) einzurichten, damit jeder Benutzer nur die Berechtigungen erhält, die er für seine Aufgaben benötigt. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir empfehlen TLS 1.2 oder höher.

- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb AWS von -Services.
- 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 auf 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 oder anderen AWS -Services unter Verwendung der Konsole, API AWS CLI oder AWS SDKs arbeiten. Alle Daten, die Sie in AWS Snowball 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

AWS Snowball schützt Ihre Daten beim Importieren oder Exportieren von Daten in Amazon S3, wenn Sie einen Auftrag zum Bestellen eines Snow Family-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 in der Cloud interagieren.

Themen

Verschlüsselung für AWS Snowball Edge

Wenn Sie einen Snowball Edge verwenden, um Daten in S3 zu importieren, werden alle auf ein Gerät übertragenen Daten durch SSL-Verschlüsselung über das Netzwerk geschützt. Zum Schutz von Daten im Ruhezustand verwendet AWS Snowball Edge serverseitige Verschlüsselung (SSE).

Serverseitige Verschlüsselung in AWS Snowball Edge

AWS Snowball Edge unterstützt die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3). Bei der serverseitigen Verschlüsselung geht es um den Schutz von Daten im Ruhezustand, und SSE-S3 verfügt über eine starke Multifaktor-Verschlüsselung zum Schutz Ihrer Daten im Ruhezustand in Amazon S3. Weitere Informationen zu SSE-S3 finden Sie unter Schutz von Daten durch serverseitige Verschlüsselung mit von Amazon S3-Managed Verschlüsselungsschlüsseln (SSE-S3) im Benutzerhandbuch für Amazon Simple Storage Service.

Derzeit bietet AWS Snowball Edge keine serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C). Amazon S3-kompatibler Speicher auf Snow-Family-Geräten bietet SSS-C für lokale Datenverarbeitungs- und Speicheraufträge. 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 SSE-C verwenden möchten, um die Objekte zu verschlüsseln, die Sie in Amazon S3 importiert haben, sollten Sie erwägen, 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 Ihrem Bucket kopieren, um es mit SSE-C zu verschlüsseln. Ein Beispiel für einen CLI-Befehl, um dies zu erreichen, wird unten gezeigt:

  ```
  aws s3 cp s3://mybucket/object.txt s3://mybucket/object.txt --sse-c --sse-c-key
   1234567891SAMPLEKEY
  ```

  or

  ```
  aws s3 cp s3://mybucket s3://mybucket --sse-c --sse-c-key 1234567891SAMPLEKEY --
  recursive
  ```

- Export ieren– Wenn Sie mit SSE-C verschlüsselte Objekte exportieren möchten, kopieren Sie diese Objekte zunächst in einen anderen Bucket, der entweder keine serverseitige Verschlüsselung hat oder in der Bucket-Richtlinie dieses Buckets SSE-KMS oder SSE-S3 angegeben ist.

Aktivieren von SSE-S3 für Daten, die von einem Snowball-Edge in Amazon S3 importiert werden

Gehen Sie wie folgt in der Amazon S3-Managementkonsole vor, 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.

So aktivieren Sie SSE-S3 für Daten, die in Amazon S3 importiert werden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon 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.

```
{
  "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-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 Service, mit dem Sie die Verschlüsselungsschlüssel zum Verschlüsseln Ihrer Daten einfach erstellen und steuern können. AWS KMS verwendet Hardware-Sicherheitsmodule (HSMs), um die Sicherheit Ihrer Schlüssel zu schützen. Insbesondere wird der Amazon-Ressourcenname (ARN) für den AWS KMS Schlüssel, den Sie für einen Auftrag in AWS Snowball Edge 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 Snowball Edge AWS KMS schützt die Verschlüsselungsschlüssel, die zum Schutz von Daten auf jedem AWS Snowball Edge Gerät verwendet werden. Wenn Sie den Auftrag erstellen, wählen Sie auch einen vorhandenen KMS-Schlüssel. Durch die Angabe des ARN für einen - AWS KMS Schlüssel wird mitgeteilt AWS Snowball , welcher AWS KMS keys zum Verschlüsseln der eindeutigen Schlüssel auf dem AWS Snowball Edge Gerät verwendet werden soll. Weitere Informationen zu AWS Snowball Edge-unterstützten Amazon S3 server-side-encryption -Optionen finden Sie unter Serverseitige Verschlüsselung in AWS Snowball Edge.

Verwenden des Managed Customer AWS KMS keys für Snowball Edge

Wenn Sie den für Ihr Konto erstellten verwalteten Kunden AWS KMS keys für Snowball Edge verwenden möchten, gehen Sie folgendermaßen vor.

So wählen Sie die AWS KMS keys für Ihren Auftrag aus

1. Wählen Sie in der die Managementkonsole für die AWS Snow-Familie Option Auftrag erstellen aus.
2. Wählen Sie Ihren Auftragstyp 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 die Von AWS verwalteter Schlüssel oder einen benutzerdefinierten Schlüssel aus, der

zuvor in erstellt wurde AWS KMS, oder wählen Sie Schlüssel-ARN eingeben, wenn Sie einen Schlüssel eingeben müssen, der einem separaten Konto gehört.

> **Note**
>
> Der AWS KMS key ARN ist eine global eindeutige Kennung für vom Kunden verwaltete Schlüssel.

6. Wählen Sie Weiter, um die Auswahl Ihres abzuschließen AWS KMS key.
7. Geben 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 Verschlüsselungsschlüssel und öffnen Sie den KMS-Schlüssel, den Sie zum Verschlüsseln der Daten auf dem Gerät ausgewählt haben.

   b. Wählen Sie unter Schlüsselbenutzer die Option Hinzufügen aus, suchen Sie nach dem IAM-Benutzer des Snow-Geräts und wählen Sie Anfügen 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 Auftrag finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.

Schützen von Daten auf Ihrem Gerät

Sichern Ihres AWS Snowball Edge

Im Folgenden finden Sie einige Sicherheitspunkte, die Sie bei der Verwendung von AWS Snowball Edge berücksichtigen sollten, sowie einige allgemeine Informationen zu anderen Sicherheitsvorkehrungen, die wir treffen, wenn ein Gerät AWS zur Verarbeitung bei eintrifft.

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 Schutzausrüstung aufweist, kann das Wetter die stärkste 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 die Eigenschaft von AWS. Die Überschreitung eines Geräts stellt einen Verstoß gegen die Richtlinie AWS für zulässige Nutzung dar. Weitere Informationen finden Sie unter http://aws.amazon.com/aup/.

Wir führen die folgenden Sicherheitsschritte durch:

- Beim Übertragen von Daten mit dem Amazon S3-Adapter werden Objektmetadaten nicht beibehalten. 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]`
- Beim Übertragen von Daten über die Dateischnittstelle bleiben Objektmetadaten erhalten.
- Wenn ein Gerät bei eintrifft AWS, untersuchen wir es auf Anzeichen von Manipulationen und stellen sicher, dass vom Trusted Platform Module (TPM) keine Änderungen erkannt wurden. AWS Snowball Edge verwendet mehrere Sicherheitsebenen, die zum Schutz Ihrer Daten entwickelt wurden, darunter manipulationssichere Umschließungen, 256-Bit-Verschlüsselung und ein branchenübliches TPM, das sowohl Sicherheit als auch vollständige Schutzkette für Ihre Daten bietet.
- Sobald der Datenübertragungsauftrag verarbeitet und verifiziert wurde, AWS führt eine Softwarelöschung des Snowball-Geräts durch, die den Richtlinien des National Institute of Standards and Technology (NIST) für die Medienbereinigung entspricht.

Validieren von NFC-Tags

In Snowball Edge Compute Optimized- und Snowball Edge Storage Optimized-Geräte (für die Datenübertragung) sind microSD-Tags integriert. Sie können diese Tags mit der AWS Snowball Edge Verification 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 microSD-Tags umfasst die Verwendung des Snowball Edge-Clients zum Generieren eines gerätespezifischen QR-Codes, um zu überprüfen, ob die von Ihnen gescannten Tags für das richtige Gerät bestimmt sind.

Im folgenden Verfahren wird beschrieben, wie Sie die microSD-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-Auftrag. Weitere Informationen finden Sie unter Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts.
2. Eingang des Geräts Weitere Informationen finden Sie unter Empfangen des Snowball Edge.
3. Herstellen einer Verbindung mit dem lokalen Netzwerk Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem lokalen Netzwerk.
4. Abrufen von Anmeldeinformationen und Tools Weitere Informationen finden Sie unter Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät.
5. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter Herunterladen und Installieren des Snowball Edge-Clients.

So validieren Sie die microSD-Tags

1. Führen Sie den `snowballEdge get-app-qr-code` Snowball Edge-Clientbefehl 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 Anfordern Ihres QR-Codes für die NFC-Validierung.

   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 Verification App auf Android scannen.

> **Note**
>
> Die AWS Snowball Edge Verification 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 Optionen zur Optimierung der Snowball Edge Compute verfügt (mit oder ohne GPU).
- 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 Probleme weiterhin bestehen, wenden Sie sich an AWS Support.

Identity and Access Management in AWS Snowball

Jeder AWS Snowball Auftrag muss authentifiziert werden. Dazu erstellen und verwalten Sie die IAM-Benutzer in Ihrem Konto. Mit IAM können Sie Benutzer und Berechtigungen in erstellen und verwalten AWS.

AWS Snowball -Benutzer müssen über bestimmte IAM-bezogene Berechtigungen verfügen, um auf zugreifen zu können AWS Snowball AWS Management Console , um Aufträge 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 Auftrag verwendet werden sollen, AWS KMS Ressourcen, Amazon SNS-Thema und Amazon EC2-compatible AMI für Edge-Computing-Aufträge.

> **Important**
>
> Informationen zur lokalen Verwendung von IAM auf Ihrem Gerät finden Sie unter Lokales Verwenden von IAM.

Themen

Zugriffskontrolle für die Snow Family-Konsole und Erstellung von Aufgaben

Wie bei allen -AWSServices AWS Snowball erfordert der Zugriff auf Anmeldeinformationen, die zur Authentifizierung Ihrer Anfragen verwenden AWS kann. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf -AWSRessourcen verfügen, z. B. einen Amazon S3-Bucket oder eine -AWS LambdaFunktion. AWS Snowball unterscheidet sich auf zwei Arten:

1. Aufträge in AWS Snowball haben keinen Amazon-Ressourcennamen (ARN).
2. Die Steuerung des physischen Zugangs und des Netzwerkzugriffs eines Geräts bei Ihnen vor Ort liegt in Ihrer Verantwortung.

Weitere Identity and Access Management für AWS Snow Family Informationen zur Verwendung von AWS Identity and Access Management (IAM) und AWS Snowball zur Sicherung Ihrer Ressourcen durch Kontrolle darüber, wer auf sie in der zugreifen kannAWS Cloud, sowie Empfehlungen zur lokalen Zugriffskontrolle finden Sie unter .

Identity and Access Management für AWS Snow Family

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von - AWS Snow Family Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS Snow Family.

Service-Benutzer – Wenn Sie den AWS Snow Family Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS Snow Family Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für AWS Snow Family Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS Snow Family haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für AWS Snow Family Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS Snow Family. Ihre Aufgabe besteht darin, zu bestimmen, auf welche AWS Snow Family Funktionen und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit verwenden kann AWS Snow Family, finden Sie unter Funktionsweise AWS Snow Family von 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 Snow Family.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer -Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter Signieren von AWS API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS 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 Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, 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 und verwenden Sie diese, 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

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt

werden. Wenn Verbundidentitäten auf 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 eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und 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 in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen 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 Verwenden von IAM-Rollen 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 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 AWS-Services Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. 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 in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. 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.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das der Instance zugeordnet ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in 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 AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 über die AWS Management Console, die AWS CLI oder die 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 Erstellen von IAM-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 anfügen können AWS-Konto. Verwaltete Richtlinien umfassen AWS -verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete 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.
- Service-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs 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 dazu, wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

Funktionsweise AWS Snow Family von mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS Snow Family, erfahren Sie, welche IAM-Funktionen Sie mit verwenden 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 (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja

IAM-Feature	AWS Snow Family -Unterstützung
Service-verknüpfte Rollen	Nein

Einen Überblick über das Zusammenwirken von AWS Snow Family und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

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 Erstellen von IAM-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 Snow Family.

Ressourcenbasierte Richtlinien 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen 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 in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto der Prinzipal-Entität (Benutzer oder Rolle) auch die Berechtigung für den 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 Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Snow Family

Unterstützt Richtlinienaktionen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben in der Regel denselben Namen wie die zugehörige AWS API-Operation. 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 Von definierte Aktionen AWS Snow Family in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in AWS Snow Family verwenden das folgende Präfix vor der Aktion:

```
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 Snow Family.

Richtlinienressourcen für AWS Snow Family

Unterstützt Richtlinienressourcen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen 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 finden Sie unter Von definierte Ressourcen AWS Snow Family in der Service-Autorisierungs-Referenz. 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 Snow Family.

Richtlinienbedingungsschlüssel für AWS Snow Family

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was 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, AWS wertet 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 servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der AWS Snow Family Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Snow Family in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von definierte Aktionen AWS Snow Family.

Beispiele für AWS Snow Family identitätsbasierte Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Snow Family.

ACLs in AWS Snow Family

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit 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 werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anfügen. 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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? 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 der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. 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 zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfohlen, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Weiterleiten von Zugriffssitzungen für AWS Snow Family

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. 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**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die AWS Snow Family Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn dazu Anleitungen AWS Snow Family gibt.

Serviceverknüpfte Rollen für AWS Snow Family

Unterstützt serviceverknüpfte Rollen	Nein

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. 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 Snow Family

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 Management

Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen AWS Snow Family, die von definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snow Family in der Service-Autorisierungs-Referenz.

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:

- Erste Schritte mit - AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die für Ihre Anwendungsfälle spezifisch 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 Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum 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 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 Konfigurieren eines MFA-geschützten API-Zugriffs 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, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. 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.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. 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 weiterhin die AWS Snow Family Konsole verwenden können, fügen Sie den Entitäten auch die von AWS Snow Family *ConsoleAccess* oder *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 enthält Berechtigungen zum Abschließen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der - AWS CLI oder AWS -API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Fehlerbehebung für AWS Snow Family Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit AWS Snow Family und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in auszuführen AWS Snow Family
- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine - AWS Snow Family Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in auszuführen 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 autorisiert, 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 Familyübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in 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 meines AWS-Konto Zugriff auf meine - AWS Snow Family Ressourcen gewähren

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. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob diese Funktionen AWS Snow Family unterstützt, finden Sie unter Funktionsweise AWS Snow Family von mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen in Ihrem Besitz finden AWS-Konten Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Zugriffskontrolle im AWS Cloud

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen in zu authentifizierenAWS. Sofern Sie jedoch nicht über Berechtigungen verfügen, können Sie keine -AWSRessourcen erstellen oder darauf zugreifen. Sie müssen beispielsweise über Berechtigungen verfügen, um einen Auftrag zum Bestellen eines Snow Family-Geräts zu erstellen.

In den folgenden Abschnitten wird die Verwaltung von cloudbasierten Berechtigungen für AWS Snowball beschrieben. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihre -Ressourcen im AWS Cloud
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Snowball

Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihre -Ressourcen im AWS Cloud

Jede AWS-Ressource ist Eigentum eines AWS-Konto und die Berechtigungen für die Erstellung einer Ressource oder den Zugriff darauf werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien zuweisen. Manche Services (z. B. AWS Lambda) unterstützen auch die Zuweisung von Berechtigungsrichtlinien zu 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

In ist AWS Snowballdie primäre Ressource ein Auftrag . verfügt AWS Snowball auch über Geräte wie Snowball und das AWS Snowball Edge Gerät. Sie können diese Geräte jedoch nur im Kontext eines vorhandenen Auftrags verwenden. Amazon-S3-Buckets und Lambda-Funktionen sind Ressourcen von Amazon S3 bzw. Lambda.

Wie bereits erwähnt, haben Aufträge keinen zugeordneten Amazon-Ressourcennamen (ARN). Den Ressourcen anderer -Services, wie z. B. Amazon S3-Buckets, sind jedoch eindeutige (ARNs) zugeordnet, wie in der folgenden Tabelle gezeigt.

AWS Snowball bietet verschiedene Operationen zum Erstellen und Verwalten von Aufträgen. Eine Liste der verfügbaren Operationen finden Sie in der APIAWS Snowball-Referenz zu .

Grundlegendes zum Eigentum an Ressourcen

Das AWS-Konto ist Eigentümer aller Ressourcen, die innerhalb des Kontos erstellt werden, unabhängig davon, wer sie erstellt. Genauer gesagt ist das AWS-Konto der Prinzipal-Entität (d. h. das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), welche die Ressourcenerstellungsanforderung authentifiziert, der Ressourceneigentümer. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Root-Konto-Anmeldeinformationen Ihres verwenden, AWS-Konto um einen S3-Bucket zu erstellen, AWS-Konto ist Ihr der Eigentümer der Ressource (in ist AWS Snowballdie Ressource der Auftrag).
- Wenn Sie einen IAM-Benutzer in Ihrem erstellen AWS-Konto und Berechtigungen zum Erstellen eines Auftrags erteilen, um ein Snow-Family-Gerät an diesen Benutzer zu bestellen, kann der Benutzer einen Auftrag erstellen, um ein Snow-Family-Gerät zu bestellen. Eigentümer der Auftragsressource ist jedoch Ihr AWS-Konto, zu dem der Benutzer gehört.

- Wenn Sie in Ihrem eine IAM-Rolle AWS-Konto mit Berechtigungen zum Erstellen eines Auftrags erstellen, kann jeder, der die Rolle übernehmen kann, einen Auftrag erstellen, um ein Snow-Family-Gerät zu bestellen. Eigentümer der Auftragsressource ist Ihr , AWS-Kontozu dem die Rolle gehört.

Verwalten des Zugriffs auf -Ressourcen im AWS Cloud

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> Dieser Abschnitt behandelt die Verwendung von IAM um Zusammenhang mit AWS Snowball. 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 einer IAM-Identität zugeordnet sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. Richtlinien, die einer Ressource zugeordnet sind, werden als ressourcenbasierte Richtlinien bezeichnet. AWS Snowball unterstützt nur identitätsbasierte (IAM-Richtlinien).

Themen

- Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3-Bucket eine ressourcenbasierte Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. AWS Snowball bietet keine Unterstützung für ressourcenbasierte Richtlinien.

Festlegen der Richtlinienelemente: Aktionen, Effekte und Prinzipale

Für jeden Auftrag (siehe Ressourcen und Operationen) definiert der Service eine Reihe von API-Operationen (siehe AWS Snowball API-Referenz), um den betreffenden Auftrag zu erstellen und zu verwalten. Zur Erteilung von Berechtigungen für diese API-Operationen definiert AWS Snowball-

Aktionen, die Sie in einer Richtlinie angeben können. 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, AWS KMSund viele andere -Services unterstützt.
  > Snowball unterstützt nicht die Angabe eines Ressourcen-ARN im -`Resource`Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Snowball zu erlauben, geben Sie `“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. In ressourcenbasierten Richtlinien müssen Sie den

Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). AWS Snowball bietet keine Unterstützung für ressourcenbasierte 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-API-Aktionen finden Sie unter AWS Snowball-API-Berechtigungen: Referenzliste für Aktionen, Ressourcen und Bedingungen.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für AWS Snowball gibt es keine speziellen Bedingungsschlüssel. Stattdessen können Sie nach Bedarf die AWS-weiten Bedingungsschlüssel verwenden. Sie finden eine vollständige Liste der AWS-weiten Schlüssel unter Verfügbare Schlüssel für Bedingungen im IAM-Benutzerhandbuch enthalten.

Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Snowball

Dieses Thema enthält Beispiele für identitätsbasierte Richtlinien, die zeigen, wie ein Kontoadministrator IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuweisen kann. Diese Richtlinien gewähren dadurch Berechtigungen zum Ausführen von Operationen an AWS Snowball Ressourcen in der 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-Ressourcen erläutert werden. Weitere Informationen finden Sie unter Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihre -Ressourcen im AWS Cloud.

Dieses Thema besteht aus folgenden Abschnitten:

- Erforderliche Berechtigungen für die Verwendung der AWS Snowball-Konsole
- AWS-verwaltete (vordefinierte) Richtlinien für AWS Snowball Edge
- Beispiele für vom Kunden verwaltete Richtlinien

Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

```
{
  "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:GetBucketLocation`-Aktionen (`s3:GetObject`, und `s3:ListBucket`) für alle Amazon S3-Buckets, die den Amazon-Ressourcennamen (ARN) von verwendenarn:aws:s3:::*. Der ARN gibt ein Platzhalterzeichen (*) an, damit der Benutzer einen oder alle Amazon S3-Buckets auswählen kann, aus denen Daten exportiert werden sollen.
- Die zweite Anweisung erteilt Berechtigungen für alle AWS Snowball-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 Verwaltung von AWS Snowball-Aufträgen sowie den Ressourcen, auf die sie anwendbar sind, finden Sie unter AWS Snowball-API-Berechtigungen: Referenzliste für Aktionen, Ressourcen und Bedingungen.

Erforderliche Berechtigungen für die Verwendung der AWS Snowball-Konsole

In der Berechtigungsreferenztabelle sind die API-Operationen für die Verwaltung von AWS Snowball-Aufträgen sowie die erforderlichen Berechtigungen für jede Operation aufgeführt. Weitere Informationen zu API-Operationen zur Auftragsverwaltung finden Sie im Thema AWS Snowball-API-Berechtigungen: Referenzliste für Aktionen, Ressourcen und Bedingungen.

Zur Verwendung der Managementkonsole für die AWS Snow-Familie müssen Sie Berechtigungen für weitere Aktionen erteilen, wie in der folgenden Berechtigungsrichtlinie gezeigt:

```
{
    "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": "*",
            "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-Konsole benötigt diese zusätzlichen Berechtigungen aus folgenden Gründen:

- `ec2:` – Diese ermöglichen es dem Benutzer, AmazonEC2-compatible Instances zu beschreiben und ihre Attribute für lokale Datenverarbeitungszwecke zu ändern. Weitere Informationen finden Sie unter Verwenden von Amazon EC2-compatibleInstances.
- `kms:` – Diese ermöglichen es dem Benutzer, den KMS-Schlüssel zu erstellen oder auszuwählen, der Ihre Daten verschlüsselt. Weitere Informationen finden Sie unter AWS Key Management Service in AWS Snowball Edge.
- `iam:` – Diese ermöglichen es dem Benutzer, einen IAM-Rollen-ARN zu erstellen oder auszuwählen, der AWS Snowball übernimmt, um auf die AWS Ressourcen zuzugreifen, die mit der Auftragserstellung und -verarbeitung verknüpft sind.
- `sns:` – Diese ermöglichen es dem Benutzer, die Amazon SNS-Benachrichtigungen für die von ihm erstellten Aufträge zu erstellen oder auszuwählen. Weitere Informationen finden Sie unter Benachrichtigungen für Snow Family-Geräte.

AWS-verwaltete (vordefinierte) Richtlinien für AWS Snowball Edge

AWS Durch die Bereitstellung von eigenständigen IAM-Richtlinien, die von erstellt und verwaltet werden, deckt viele häufige Anwendungsfälle ab 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 von AWSverwalteten Richtlinien mit verwendenAWS Snowball.

Erstellen einer IAM-Rollenrichtlinie für Snowball Edge

Eine IAM-Rollenrichtlinie muss mit Lese- und Schreibberechtigungen für Ihre Amazon S3-Buckets erstellt werden. Die IAM-Rolle muss auch eine Vertrauensstellung mit Snowball haben. Eine Vertrauensstellung bedeutet, dass die Daten in den Snowball und in Ihre Amazon S3-Buckets schreiben AWS kann, je nachdem, ob Sie Daten importieren oder exportieren.

Wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts in der erstellenManagementkonsole für die AWS Snow-Familie, erfolgt das Erstellen der erforderlichen IAM-Rolle in Schritt 4 im Abschnitt Berechtigung. Dieser Prozess erfolgt automatisch. Die IAM-Rolle, die Sie Snowball erlauben, wird nur verwendet, um Ihre Daten in Ihren Bucket zu schreiben, wenn der Snowball mit Ihren übertragenen Daten bei eintrifftAWS. Der Vorgang wird wie folgt ausgeführt.

So erstellen Sie die IAM-Rolle für Ihren Importauftrag

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die -AWS SnowballKonsole 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 aus.
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, die zum Kopieren von Objekten in Ihre angegebenen Amazon S3-Buckets AWS verwendet.
5. Überprüfen Sie die Angaben auf dieser Seite und wählen Sie dann Allow (Zulassen) aus.

   Sie kehren zur Managementkonsole für die AWS Snow-Familie zurück. Hier ist der Amazon-Ressourcenname (ARN) für die soeben erstellte IAM-Rolle in Selected IAM role ARN (ARN der ausgewählten IAM-Rolle) enthalten.
6. Wählen Sie Weiter, um die Erstellung Ihrer IAM-Rolle abzuschließen.

Mit dem vorherigen Verfahren wird eine IAM-Rolle erstellt, die über Schreibberechtigungen für die Amazon S3-Buckets verfügt, 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

```
        {
  "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",
        "s3:HeadBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Wenn Sie die serverseitige Verschlüsselung mit AWS KMSvon verwalteten Schlüsseln (SSE-KMS) verwenden, um die Amazon 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-Client, der für den Importvorgang verwendet wird, einen mehrteiligen Upload. Wenn Sie einen mehrteiligen Upload mit SSE-KMS einleiten, werden alle hochgeladenen Teile mit dem angegebenen AWS KMS-Schlüssel verschlüsselt. Da die Teile verschlüsselt sind, müssen sie zuerst entschlüsselt werden, bevor sie zur Vervollständigung des mehrteiligen Uploads zusammengesetzt werden können. Sie müssen also über die Berechtigung zum Entschlüsseln des AWS KMS Schlüssels (`kms:Decrypt`) verfügen, 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Wenn Sie die serverseitige Verschlüsselung mit AWS KMSvon verwalteten Schlüsseln verwenden, um die Amazon 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 AWS Snowball Auftragsverwaltung zu gewähren. 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 Beispiele für Benutzerrichtlinien, die Berechtigungen für diverse AWS Snowball-Auftragsverwaltungsaktionen. Diese Richtlinien funktionieren, wenn Sie AWS -SDKs oder die verwendenAWS CLI. Bei Verwendung der Konsole müssen Sie zusätzliche konsolenspezifische Berechtigungen erteilen, die im Abschnitt Erforderliche Berechtigungen für die Verwendung der AWS Snowball-Konsole erläutert werden.

> **Note**
>
> In allen Beispielen werden die Region „us-west-2” und fiktive Konto-IDs verwendet.

Beispiele

- Beispiel 1: Rollenrichtlinie, die es einem Benutzer ermöglicht, einen Auftrag zu erstellen, um ein Snow Family-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-API-Berechtigungen: Referenzliste für Aktionen, Ressourcen und Bedingungen

Beispiel 1: Rollenrichtlinie, die es einem Benutzer ermöglicht, einen Auftrag zu erstellen, um ein Snow Family-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 -Anweisung wird als Grundsatzerklärung zur Vertrauensbeziehung für die Snowball-IAM-Rolle benötigt.

```
{
    "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 zum Erstellen von Importaufträgen für Snowball Edge, die von -AWS IoT GreengrassFunktionen AWS Lambda unterstützt werden.

```
                {
    "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:HeadBucket",
                "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 zum Erstellen von Exportaufträgen für Snowball Edge, die von -AWS IoT GreengrassFunktionen AWS Lambda unterstützt werden.

```
                {
    "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 erforderlich, damit eine vorhandene Servicerolle verwendet werden kann. Es ist ein einmaliges Setup.

```
{
    "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 erwartete Rollenvertrauensrichtlinie ist erforderlich, damit eine vorhandene Servicerolle sie verwenden kann. Es ist ein einmaliges Setup.

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

AWS Snowball-API-Berechtigungen: Referenzliste für 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 alle AWS Snowball-API-Operationen und die entsprechenden Aktionen zur Auftragsverwaltung, für die Sie Berechtigungen zur Ausführung der Aktion vergeben 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.

Zum Formulieren von Bedingungen können Sie AWS-weite Bedingungsschlüssel in Ihren AWS Snowball-Richtlinien verwenden. Eine vollständige Liste der AWS-weiten Schlüssel enthält der Abschnitt 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

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Snowball und Ihrer - AWS Lösungen aufrechtzuerhalten. Sie sollten Überwachungsdaten sammeln, damit Sie Ausfälle an mehreren Punkten leichter debuggen können. AWS bietet mehrere Tools zur Überwachung Ihrer AWS Snowball Ressourcen und zur Reaktion auf potenzielle Vorfälle:

AWS CloudTrail Protokolle

CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem - AWS Service in der AWS Snowball Auftragsverwaltungs-API oder bei Verwendung der - AWS Konsole durchgeführten Aktionen. Anhand der von CloudTrailgesammelten Informationen können Sie die an den AWS Snowball Service gestellte API-Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen. Weitere Informationen finden Sie unter Erfassen von AWS Snowball-Edge-API-Aufrufen mit AWS CloudTrail.

Compliance-Validierung für AWS Snowball

Informationen darüber, ob ein in den Geltungsbereich bestimmter Compliance-Programme AWS-Service fällt, finden Sie AWS-Services unter im Geltungsbereich nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten unter AWS Artifact .

Ihre Compliance-Verantwortung bei der Verwendung von 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 Unterstützung der Compliance bereit:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte für die Bereitstellung von Basisumgebungen in bereitgestellt AWS , die sich auf Sicherheit und Compliance konzentrieren.
- Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe AWS von HIPAA-berechtigte Anwendungen erstellen können.

  > **Note**
  >
  > Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden kann für Ihre Branche und Ihren Standort gelten.
- AWS Kunden-Compliance-Leitfäden – Verstehen Sie das Modell der übergreifenden Verantwortlichkeit anhand der Compliance. Die Leitfäden fassen die bewährten Methoden zur Sicherung zusammen AWS-Services und ordnen die Leitlinien den Sicherheitskontrollen in mehreren Frameworks zu (einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Officer (PCI) und International Organization for Standardization (ISO)).
- Bewertung von Ressourcen mit Regeln im -AWS Config Entwicklerhandbuch – Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub – Dies AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen.

Ausfallsicherheit

Die AWS globale -Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz 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 AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS Snowball

Als verwalteter Service AWS Snow Family ist durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um AWS Snow Family über das Netzwerk auf zuzugreifen. 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.

Datenvalidierung mit Snowball Edge-Aufträgen

Im Folgenden finden Sie Informationen darüber, wie AWS Snowball Edge Datenübertragungen validiert, und die manuellen Schritte, die Sie ergreifen können, um die Datenintegrität während und nach einem Auftrag sicherzustellen.

Themen

Prüfsummenvalidierung von übertragenen Daten

Wenn Sie eine Datei über die Amazon S3-Schnittstelle aus einer lokalen Datenquelle in den Snowball Edge kopieren, wird 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 den 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 Übertragungen 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.

Erstellung des lokalen Bestands während der Snowball-Übertragung

Erstellen Sie ein lokales Inventar der Dateien, die in den Snowball kopiert wurden, wenn Sie den Amazon S3-Adapter oder die CLI verwenden. Der Inhalt des lokalen Bestands kann verwendet werden, um mit dem zu vergleichen, was sich auf dem lokalen Speicher oder Server befindet.

Zum Beispiel

```
aws s3 cp folder/ s3://bucket --recursive > inventory.txt
```

Häufige Validierungsfehler

Wenn ein Validierungsfehler auftritt, werden die entsprechenden Daten (eine Datei oder ein Teil einer großen Datei) nicht in das Ziel geschrieben. Im Folgenden sind häufige Ursachen für Validierungsfehler aufgeführt:

- Versuch, symbolische Links zu kopieren.
- Der Versuch, Dateien zu kopieren, die aktiv geändert werden. Der Versuch schlägt die Prüfsummenvalidierung fehl und wird als fehlgeschlagene Übertragung markiert.
- Der Versuch, Dateien zu kopieren, die größer als 5 TB sind.
- Der Versuch, Teilegrößen zu kopieren, die größer als 2 GiB sind.
- Der Versuch, Dateien auf ein Snowball Edge-Gerät zu kopieren, das bereits über die volle Datenspeicherkapazität verfügt.
- Der Versuch, 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 identifizieren, welche Dateien validiert wurden und warum. Weitere Informationen finden Sie unter Manuelle Datenvalidierung für Snowball Edge nach dem Import in Amazon S3.

Manuelle Datenvalidierung für Snowball Edge nach dem Import in Amazon S3

Nachdem ein Importauftrag abgeschlossen ist, 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 Abrufen Ihres Auftragsabschlussberichts und der Protokolle auf der Konsole.

S3-Bestand

Wenn Sie in mehreren Aufträgen eine große Datenmenge in Amazon S3 übertragen haben, ist das Durchlaufen jedes Auftragsabschlussberichts möglicherweise keine effiziente Nutzung der Zeit. Stattdessen können Sie ein Inventar aller Objekte in einem oder mehreren Amazon S3-Buckets abrufen. Amazon S3 Inventory stellt eine CSV-Datei (durch Kommas getrennte Werte) bereit, in der Ihre Objekte und die entsprechenden Metadaten täglich oder wöchentlich angezeigt werden. Diese Datei deckt Objekte für einen Amazon S3-Bucket oder ein gemeinsames Präfix ab (d. h. Objekte, deren Namen mit einer gemeinsamen Zeichenfolge beginnen).

Wenn Sie das Inventar der Amazon S3-Buckets haben, in die Sie Daten importiert haben, können Sie sie einfach 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 des Amazon S3-Synchronisierungsbefehls

Wenn Ihre Workstation eine Verbindung mit dem Internet herstellen kann, können Sie eine finale Validierung aller übertragenen Dateien durchführen, indem Sie den AWS CLI-Befehl `aws s3 sync` ausführen. 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 Sicherung der Dateien haben, mit denen Sie synchronisieren. Diese Dateien werden durch den Inhalt in der angegebenen Amazon S3-Quelle überschrieben.

Benachrichtigungen für Snow Family-Geräte

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 Ihre Benachrichtigungseinstellungen.

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 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 der AWS Management Console an und öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Topics (Themen) aus.
3. Wählen Sie auf der Themenseite 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 AWSKMS-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 AWSKMS-Schlüssel ein.
6. Wählen Sie Änderungen speichern aus. Die serverseitige Verschlüsselung ist für Ihr Thema aktiviert und die Themenseite wird angezeigt.

Einrichtung einer vom Kunden verwalteten KMS-Schlüsselrichtlinie

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. `"mks:Decrypt"` `"mks:GenerateDataKey*"`

Um die Import-Export-Servicerolle in der KMS-Schlüsselrichtlinie zuzulassen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Key Management Service (AWS KMS)-Konsole unter https://console.aws.amazon.com/kms.
2. Wenn Sie die AWS-Region ändern möchten, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

3. Ändern Sie in der oberen rechten Ecke der Konsole den Namen 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 folgenden Richtlinien `"kms:Decrypt"` und `"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.

SNS-Benachrichtigungsbeispiele

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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-east-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" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.	SNS-Benachrichtigung (JSON)

```
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)

Appliance wird vorbereitet	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being prepared. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being Exported. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is in transit to you. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) was delivered to you. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is in transit to AWS. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-east-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" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-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" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being imported. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) complete.\nThanks for using AWS Snow Family.\nCan you take a quick survey on your experience? Survey here: http://bit.ly/1pLQJMY. More info - https://console.aws.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27:58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.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" } 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" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-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" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.	SNS-Benachrichtigung (JSON)

Erfassen von AWS Snowball-Edge-API-Aufrufen mit AWS CloudTrail

DerAWS Snowball- oderAWS CloudTrail SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS- CloudTrail erfasst alle API-API-API-fürAWS SSNS-SNS-SNS-SNS-API-für Zu den erfassten Aufrufen gehören Aufrufe von derAWS Snowball Family SNS-für die Family Job SNS-für die Family Job SNS-SNS-für dieAWS Snowball Family Job SNS-für die Family Job SNS-für Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen in einem SNS-Bucket, einschließlich Ereignissen für dieAWS Snowball Family SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS-SNS- Wenn Sie keinen Trail, können Sie die neuesten für Sie aktiviert haben, können Sie die CloudTrail neuesten für Sie aktiviert. Mit den von CloudTrail gesammelten Informationen können Sie die anAWS Snowball Family API gestellte Anfrage, die IP-Adresse der Anfrage, die IP-Adresse der Anfrage, den Zeitpunkt der Anfrage und weitere Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS SnowballEdge-Informationen in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität in Edge in Edge eine Aktivität inAWS Snowball Edge auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen Ereignissen desAWS -Service in Ereignisverlauf in Ereignisverlauf in Ereignisverlauf in Ereignisverlauf in Ereignisverlauf Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit CloudTrail Ereignisverlauf im AWS CloudTrail----------Benutzerhandbuch

Zur kontinuierlichen Aufzeichnung der in Ihrem für Sie aktiviertAWS-Konto, einschließlich der fürAWS Snowball Edge, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Protokolldateien in einem SNS-Trail-Trail-Trail-Trail-Trail-Trail-Trail-Trail-für Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen AWS-Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andereAWS -Services, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails

- CloudTrail Unterstützte Dienste und Integrationen
- CloudTrail
- Empfangen von den CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Regionen

Alle Aktionen der Auftragsverwaltung sind in der AWS SnowballAPI-Referenz dokumentiert und werden CloudTrail mit den folgenden Ausnahmen protokolliert:

- Der CreateAddressVorgang 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 Stammbenutzer- oderAWS Identity and Access Management (IAM-SNS-für Sie aktiviert wurde) -Anmeldeinformationen.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element im AWS CloudTrailBenutzerhandbuch.

Grundlagen zu Protokolldateieinträgen für AWS Snowball-Edge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Protokolleinträge enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolldateien sind kein geordnetes Stack-Trail-

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die DescribeJob-Operation 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 Verwendung des AWS Snowball Edge Geräts.

> **Important**
>
> Wenn Sie Daten mithilfe eines Snowball Edge in Amazon Simple Storage Service (Amazon S3) übertragen, beachten Sie, dass einzelne Amazon S3-Objekte eine Größe von mindestens 0 Byte bis maximal 5 Terabyte (TB) haben können.

Regionsverfügbarkeit für AWS Snowball Edge

Die folgende Tabelle hebt die Regionen hervor, in denen verfügbar AWS Snowball Edge ist.

Region	Snowball-Edge-Verfügbarkeit
US East (Ohio)	✓
USA Ost (Nord-Virginia)	✓
USA West (Nordkalifornien)	✓
USA West (Oregon)	✓
AWS GovCloud (USA-Ost)	✓
AWS GovCloud (USA-West)	✓
Kanada (Zentral)	✓
Asien-Pazifik (Jakarta)	✓
Asien-Pazifik (Mumbai)	✓
Asia Pacific (Osaka)	✓
Asia Pacific (Seoul)	✓

Region	Snowball-Edge-Verfügbarkeit
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 Snow Family-Endpunkte und -Kontingente im Allgemeine AWS-Referenz

Einschränkungen für - AWS Snowball Edge Aufträge

Für die Erstellung von AWS Snowball Edge Geräteaufträgen gelten die folgenden Einschränkungen:

- Aus Sicherheitsgründen müssen Aufträge, die ein - AWS Snowball Edge Gerät verwenden, innerhalb von 360 Tagen nach der Vorbereitung abgeschlossen werden. Wenn Sie ein oder mehrere Geräte länger als 360 Tage aufbewahren müssen, finden Sie weitere Informationen unter Aktualisieren des SSL-Zertifikats. 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 weiterhin in Amazon S3 übertragen.

- AWS Snowball Edge unterstützt die serverseitige Verschlüsselung mit S3-managed Verschlüsselungsschlüsseln (SSE-S3) und die serverseitige Verschlüsselung mit AWS Key Management Service von verwalteten Schlüsseln (SSE-KMS). Amazon S3-kompatibler Speicher auf Snow-Family-Geräten unterstützt SSS-C für lokale Datenverarbeitungs- und Speicheraufträge. 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-Gerät passen, erstellen Sie zusätzliche Aufträge. Jeder Exportauftrag kann mehrere Snowball Edge-Geräte verwenden.
- Das Standard-Servicelimit für die Anzahl der Snowball Edge-Geräte, die Sie gleichzeitig haben können, beträgt 1 pro Konto und AWS-Region. Wenn Sie Ihr Service-Limit erhöhen oder einen Cluster-Auftrag erstellen möchten, wenden Sie sich an AWS Support.
- Metadaten für Objekte, die auf ein Gerät übertragen werden, werden nicht beibehalten. Nur die Metadaten von `filename` und `filesize` bleiben unverändert. Alle anderen Metadaten werden im folgenden Beispiel als festgelegt:

  ```
  -rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]
  ```

Ratenlimits für AWS Snowball Edge

Der Rate Limiter wird verwendet, um die Rate der Anforderungen in einer Server-Cluster-Umgebung zu steuern.

Verbindungslimit für Amazon Snow S3 Adapter

Das maximale Verbindungslimit für Snowball Edge auf Amazon S3 beträgt 1 000. Alle Verbindungen über 1000 werden gelöscht.

Einschränkungen bei der Übertragung von On-Premises-Daten mit einem Snowball-Edge-Gerät

Für die Übertragung von Daten zu oder von einem On-Premises- 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 in ihren 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 Teilegröße 2 GiB .

Einschränkungen beim Versand eines Snowball Edge

Für den Versand eines AWS Snowball Edge Geräts gelten die folgenden Einschränkungen:

- AWS sendet ein Snowball Edge-Gerät nicht an eine Postbox.
- AWS sendet kein Snowball Edge-Gerät zwischen Nicht-US-Regionen, z. B. von der EU (Irland) zur EU (Frankfurt) oder nach Asien-Pazifik (Sydney).
- Das Verschieben eines Snowball Edge-Geräts an eine Adresse außerhalb des Landes, das bei der Erstellung des Auftrags angegeben wurde, ist nicht zulässig und stellt einen Verstoß gegen die AWS Servicebedingungen dar.

Weitere Informationen zum Versand finden Sie unter Überlegungen zum Versand von Snow-Family-Geräten.

Einschränkungen bei der Verarbeitung Ihres zurückgegebenen Snowball-Edge für den Import

Um Ihre Daten in zu importieren AWS, muss das Gerät die folgenden Anforderungen erfüllen:

- Das AWS Snowball Edge Gerät darf nicht kompromittiert sein. Öffnen Sie das AWS Snowball Edge Gerät aus irgendeinem Grund nicht, außer die drei Trichter vorn, zurück und oben zu öffnen oder den optionalen Airfilter hinzuzufügen und zu ersetzen.
- Das Gerät muss physisch unbeschädigt sein. Sie können eine Beschädigung verhindern, indem Sie die drei Kabel auf dem Snowball Edge-Gerät schließen, bis die -Klammern ein hörbares Klicken auslösen.
- Die E-Ink-Anzeige auf dem Snowball Edge-Gerät muss sichtbar sein. Außerdem muss die Rückgabebezeichnung angezeigt werden, die automatisch generiert wurde, als Sie Ihre Daten auf das AWS Snowball Edge Gerät übertragen haben.

> **Note**
>
> Alle zurückgegebenen Snowball Edge-Geräte, die diese Anforderungen nicht erfüllen, werden gelöscht, ohne dass Arbeit an ihnen ausgeführt wird.

Fehlerbehebung bei 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.

Objektname	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$gLAOoZCj$r8p`	`/.VfV/FqGC3QN$7BXys3KHYePfuIOMNjY83dVx ugPYlxVg/evpcQEJLT/rSwZc$MlVVf/$hwefVISRqwepB$/BiiD/PP`	135 Zeichen

Objektname	Bucket-Name	Pfad plus Bucket-Name	Schlüssellänge
		`F$twRAjrD/fIMp/0NY`	

- Aus Sicherheitsgründen müssen Aufträge, die ein - AWS Snowball Edge Gerät verwenden, innerhalb von 360 Tagen nach der Vorbereitung abgeschlossen werden. Wenn Sie ein oder mehrere Geräte länger als 360 Tage aufbewahren müssen, finden Sie weitere Informationen unter Aktualisieren des SSL-Zertifikats. 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 weiterhin in Amazon S3 übertragen.
- Wenn bei der Verwendung eines - AWS Snowball Edge Geräts unerwartete Fehler auftreten, möchten wir davon hören. Kopieren Sie die relevanten Protokolle und fügen Sie sie zusammen mit einer kurzen Beschreibung der Probleme ein, die in einer Nachricht an aufgetreten sind AWS Support. Weitere Informationen über Protokolle finden Sie unter Befehle für den Snowball Edge Client.

Themen

So identifizieren Sie Ihr Gerät

Verwenden Sie den `describe-device` Befehl , um den Gerätetyp zu finden, und suchen Sie dann den zurückgegebenen Wert von `DeviceType` in der folgenden Tabelle, um die Konfiguration zu bestimmen.

```
snowballEdge describe-device
```

Example der **`describe-device`** Ausgabe

```
{
"DeviceId" : "JID-206843500001-35-92-20-211-23-06-02-18-24",
"UnlockStatus" : {
  "State" : "UNLOCKED"
},
"ActiveNetworkInterface" : {
  "IpAddress" : "127.0.0.1"
},
"PhysicalNetworkInterfaces" : [ {
  "PhysicalNetworkInterfaceId" : "s.ni-8d0ef958ec860ac7c",
  "PhysicalConnectorType" : "RJ45",
  "IpAddressAssignment" : "DHCP",
  "IpAddress" : "172.31.25.194",
  "Netmask" : "255.255.240.0",
  "DefaultGateway" : "172.31.16.1",
  "MacAddress" : "02:38:30:12:a3:7b"
} ],
"DeviceCapacities" : [ {
  "Name" : "HDD Storage",
  "Unit" : "Byte",
  "Total" : 39736350227824,
  "Available" : 985536581632
}, {
  "Name" : "SSD Storage",
  "Unit" : "Byte",
  "Total" : 6979321856000,
  "Available" : 6979321856000
}, {
  "Name" : "vCPU",
```

```
    "Unit" : "Number",
    "Total" : 52,
    "Available" : 52
  }, {
    "Name" : "Memory",
    "Unit" : "Byte",
    "Total" : 223338299392,
    "Available" : 223338299392
  }, {
    "Name" : "GPU",
    "Unit" : "Number",
    "Total" : 0,
    "Available" : 0
  } ],
  "DeviceType" : "EDGE_C"
}
```

`DeviceType` und Snow Family Gerätekonfigurationen

`DeviceType` Wert	Gerätekonfiguration
`EDGE`	Snowball Edge-speicheroptimiert (mit EC2-Datenverarbeitungsfunktionalität)
`EDGE_C`	Snowball Edge-Datenverarbeitungsoptimiert mit AMD EPYC Gen1 und HDD
`EDGE_CG`	Snowball Edge-Datenverarbeitung optimiert mit AMD EPYC Gen1, HDD und GPU
`EDGE_S`	Speicheroptimiert für Snowball Edge
`V3_5C`	Snowball Edge-Datenverarbeitungsoptimiert mit AMD EPYC Gen2 und NVME
`V3_5S`	Speicheroptimiert für Snowball Edge 210 TB

Weitere Informationen zu Snowball Edge-Gerätekonfigurationen finden Sie unter AWS Snowball Edge-Geräteunterschiede.

Beheben von Problemen beim Hochfahren

Die folgenden Informationen können Ihnen bei der Behebung bestimmter Probleme helfen, die beim Starten Ihrer Snow Family-Geräte auftreten können.

- Warten Sie 10 Minuten, bis ein Gerät gestartet wird. Vermeiden Sie es, das Gerät während dieser Zeit zu verschieben oder zu verwenden.
- Stellen Sie sicher, dass beide Enden des Kabels, das Strom bereitstellt, sicher angeschlossen sind.
- Ersetzen Sie das Kabel, das Strom liefert, durch ein anderes Kabel, von dem Sie wissen, dass es gut ist.
- Schließen Sie das Kabel, das Strom bereitstellt, an eine andere Stromquelle an, von der Sie wissen, dass sie gut ist.

Beheben von Problemen mit der Bol-Anzeige beim Start

Manchmal kann es nach dem Einschalten eines Snowball Edge-Geräts zu einem Problem kommen.

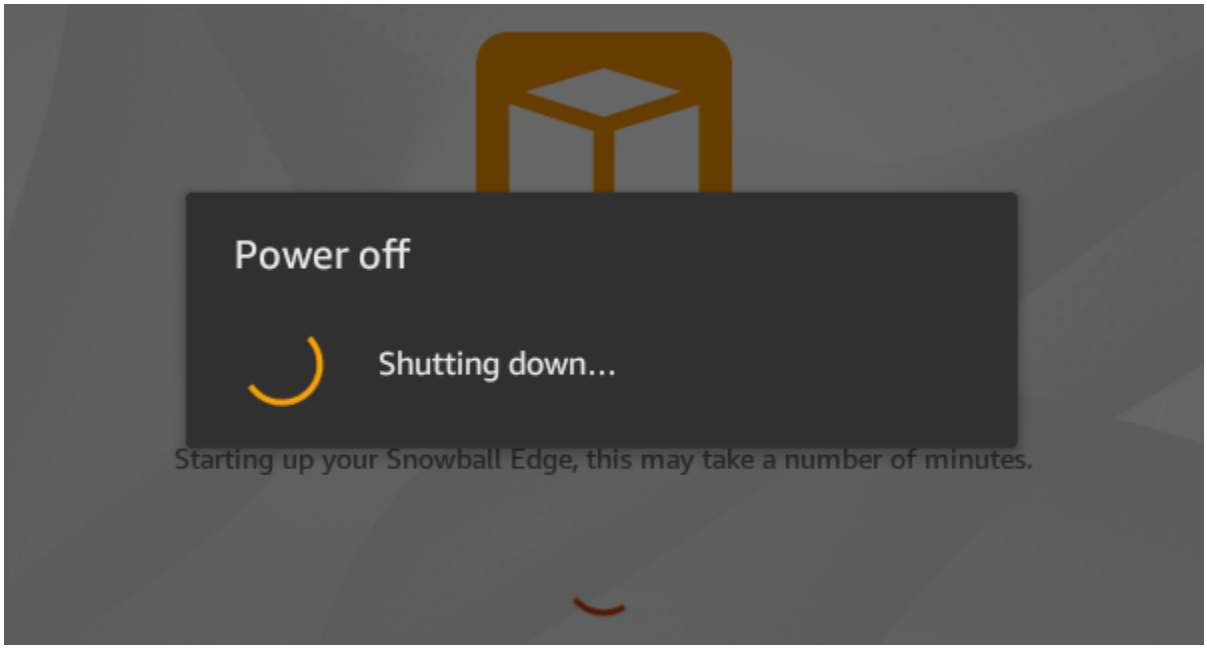
- Der Bol-Bildschirm ist schwarz und zeigt kein Bild an, nachdem Sie das Snowball Edge-Gerät angeschlossen haben, um es zu einschalten und die Einschalttaste über dem-Bildschirm zu drücken.
- Der Bol-Bildschirm geht nicht über die Einstellung Ihres Snowball Edge hinaus. Dies kann einige Minuten dauern. Die Nachricht und der Bildschirm zur Netzwerkkonfiguration werden nicht angezeigt.

Aktion, die ausgeführt werden soll, wenn der Bol-Bildschirm nach dem Drücken der Einschalttaste schwarz ist

1. Stellen Sie sicher, dass das Snowball Edge-Gerät mit einer Stromquelle verbunden ist und die Stromquelle Strom bereitstellt.
2. Lassen Sie das Gerät 1 bis 2 Stunden lang mit der Stromquelle verbunden. Stellen Sie sicher, dass die Kabel auf der Front- und Backseite des Geräts geöffnet sind.
3. Kehren Sie zum Gerät zurück und der Bildschirm ist einsatzbereit.

Zu ergreifende Aktion, wenn der Snowball Edge nicht zum Bildschirm für die Netzwerkkonfiguration übergeht

1. Lassen Sie den Bildschirm auf der Seite Setting your Snowball Edge bleiben. Dies kann einige Minuten dauern. Nachricht 10 Minuten.
2. Wählen Sie auf dem Bildschirm die Schaltfläche Anzeige neu starten aus. Die Meldung Herunterfahren... wird angezeigt, dann die Einstellung Ihres Snowball-Edge, dies kann einige Minuten dauern. Die Meldung wird angezeigt und das Gerät wird normal gestartet.



Wenn der Bildschirm „Einrichten“ nicht über die Einstellung Ihres Snowball-Edge hinausgeht, kann dies einige Minuten dauern. -Nachricht, nachdem Sie die Schaltfläche Anzeige neu starten verwendet haben, gehen Sie wie folgt vor.

Maßnahme

1. Drücken Sie über dem Bol-Bildschirm die Einschalttaste, um das Gerät auszuschalten.
2. Trennen Sie alle Kabel vom Gerät.
3. Lassen Sie das Gerät ausgeschaltet und 20 Minuten lang getrennt.
4. Schließen Sie die Strom- und Netzwerkkabel an.
5. Drücken Sie über dem Bildschirm die Einschalttaste, um das Gerät einzuschalten.

Wenn das Problem weiterhin besteht, wenden Sie sich an , AWS Support um das Gerät zurückzugeben und ein neues Snowball-Edge-Gerät zu erhalten.

Fehlerbehebung bei Verbindungsproblemen

Die folgenden Informationen können Ihnen bei der Behebung bestimmter Probleme helfen, die beim Herstellen einer Verbindung mit Ihrem Snowball Edge auftreten könnten:

- Router und Schalter, die mit einer Geschwindigkeit von 100 Megabyte pro Sekunde funktionieren, funktionieren nicht mit einem Snowball Edge. Wir empfehlen die Verwendung eines Switches mit einer Datenrate von 1 GB pro Sekunde (oder schneller).
- Wenn beim Gerät ungerade Verbindungsfehler auftreten, schalten Sie den Snowball Edge aus, trennen Sie alle Kabel und lassen Sie ihn 10 Minuten lang. 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 Dateischnittstelle und die Amazon 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 Anzeigen auf der Geräterückseite erhellen, verwenden Sie Telnet, um das Gerät auf den Ports 22, 9091 und 8080 zu testen. Das Testen von Port 22 bestimmt, ob der Snowball Edge ordnungsgemäß funktioniert. Der Testport 9091 bestimmt, ob die verwendet werden AWS CLI kann, um Befehle an das Gerät zu senden. Durch das Testen von Port 8080 wird sichergestellt, dass das Gerät nur mit dem S3-Adapter in die Amazon S3-Buckets darauf 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.

Fehlerbehebung bei **`unlock-device`** Befehlsproblemen

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

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.

a. Verwenden Sie den Bildschirm Bol auf dem Gerät, um zu überprüfen, 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 Managementkonsole für die AWS Snow-Familie, 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 erlaubt wird. Verwenden Sie den `ping` Befehl für Ihr Betriebssystem, um festzustellen, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen von Antivirensoftware, Firewall-Konfiguration, Virtual Private Network (VPN) oder anderen Konfigurationen Ihres Computers und Netzwerks.

Fehlerbehebung bei Problemen mit Manifestdateien

Jedem Auftrag ist eine bestimmte Manifestdatei zugeordnet. Wenn Sie mehrere Auftrags 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 Auftrag erneut herunterladen. Dazu verwenden Sie die -Konsole AWS CLI oder eine der AWS APIs .

Fehlerbehebung bei Problemen mit Anmeldeinformationen

Verwenden Sie die folgenden Themen, um Probleme mit Anmeldeinformationen mit dem Snowball Edge zu beheben.

Anmeldeinformationen konnten nicht gefunden AWS CLI werden

Wenn Sie über die Amazon S3-Schnittstelle über die mit dem AWS Snowball Edge Gerät kommunizieren AWS CLI, wird möglicherweise eine Fehlermeldung angezeigt, die besagt, dass die Anmeldeinformationen nicht gefunden werden können. Sie können Anmeldeinformationen konfigurieren, indem Sie „aws configure“ ausführen.

Maßnahme

Konfigurieren Sie die AWS Anmeldeinformationen, die die AWS CLI verwendet, um Befehle für Sie auszuführen. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI im AWS Command Line Interface -Leitfaden.

Fehlermeldung: Überprüfen Sie Ihren geheimen Zugriffsschlüssel und Ihre Signatur

Wenn Sie die Amazon S3-Schnittstelle verwenden, um Daten an 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/
RESTAuthentication.html#ConstructingTheAuthenticationHeader
```

Maßnahme

Rufen Sie Ihre Anmeldeinformationen vom Snowball Edge-Client ab. Weitere Informationen finden Sie unter Abrufen von Anmeldeinformationen.

Fehlerbehebung bei Problemen mit der NFS-Schnittstelle

Das Snow Family-Gerät kann angeben, dass der Status der NFS-Schnittstelle lautet`DEACTIVATED`. Dies kann auftreten, wenn das Snow Family-Gerät ausgeschaltet wurde, ohne zuerst die NFS-Schnittstelle zu stoppen.

Maßnahme

Um das Problem zu beheben, beenden Sie den NFS-Service und starten Sie ihn neu, indem Sie die folgenden Schritte ausführen.

1. Verwenden Sie den `describe-service` Befehl , um den Status des Services 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-Service zu beenden.

```
snowballEdge stop-service --service-id nfs
```

3. Verwenden Sie den `start-service` Befehl , um den NFS-Service zu starten. Weitere Informationen finden Sie unter Starten des NFS-Service auf dem Snow Family-Gerät .

```
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 Service ausgeführt wird.

```
snowballEdge describe-service --service-id nfs
```

Wenn der Wert des `State` Namens lautet`ACTIVE`, ist der NFS-Schnittstellenservice 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" ]
 }
}
```

Beheben von Datenübertragungsproblemen

Wenn bei der Übertragung der Daten auf die oder von einer Snowball Edge-Appliance Leistungsprobleme auftreten, finden Sie unter Leistung 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 des 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-Buckets, die Sie in den Auftrag 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, kann dies daran liegen, 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-Schnittstelle mit der 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 unter Angeben von Parameterwerten für AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

Fehlerbehebung bei AWS CLI Problemen

Verwenden Sie die folgenden Themen, um Probleme bei der Arbeit mit einem - AWS Snowball Edge Gerät und der zu beheben AWS CLI.

AWS CLI Fehlermeldung: „Profil darf nicht Null sein“

Bei der Arbeit mit der wird AWS CLI möglicherweise eine Fehlermeldung angezeigt, die besagt, dass Profile nicht null sein darf. Dieser Fehler kann auftreten, wenn die nicht installiert AWS CLI oder ein - AWS CLI Profil nicht konfiguriert wurde.

Maßnahme

Stellen Sie sicher, dass Sie die AWS CLI auf Ihrer Workstation heruntergeladen und konfiguriert haben. Weitere Informationen finden Sie unter Installieren von AWS CLI mit dem Bundled Installer (Linux, macOS oder Unix) im AWS Command Line Interface -Benutzerhandbuch.

Null-Zeigerfehler beim Übertragen von Daten mit der AWS CLI

Wenn Sie die AWS CLI zum Übertragen von Daten verwenden, kann ein Nullzeigerfehler auftreten. Dieser Fehler kann unter den folgenden Bedingungen auftreten:

- Wenn der angegebene Dateiname falsch geschrieben ist, z. B. `flowwer.png` oder `flower.npg` statt `flower.png`.
- Wenn der angegebene Pfad falsch ist, z. B. `C:\Doccuments\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 Problemen mit Importaufträgen

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. Für den erneuten Import ist möglicherweise ein neuer Auftrag für Snowball Edge erforderlich.

Der Import von Dateien in Amazon S3 ist aufgrund ungültiger Zeichen in Objektnamen fehlgeschlagen

Dieses Problem tritt auf, wenn ein Datei- oder Ordnername Zeichen enthält, die von Amazon S3 nicht unterstützt werden. Amazon S3 verfügt über Regeln darüber, welche Zeichen in Objektnamen enthalten sein können. Weitere Informationen finden Sie unter Erstellen von Objektschlüsselnamen im Amazon 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-Regeln entsprechen, und die Dateien erneut übertragen.

Wenn die Dateien klein sind und es keine große Anzahl davon gibt, können Sie sie über die AWS CLI oder die nach Amazon S3 kopieren AWS Management Console. Weitere Informationen finden Sie unter Wie lade ich Dateien und Ordner in einen S3-Bucket hoch? im Benutzerhandbuch für Amazon Simple Storage Service.

Fehlerbehebung bei Problemen mit Exportaufträgen

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. Für den erneuten Export ist möglicherweise ein neuer Auftrag 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 AWS Snowball Edge Protokolle.

2. Ändern Sie die Namen der Objekte in Amazon S3, die dazu führen, dass das Problem die nicht unterstützten Zeichen entfernt oder ersetzt.
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 keine große Anzahl davon gibt, kopieren Sie die umbenannten Objekte aus Amazon S3 über die AWS CLI oder die AWS Management Console. Weitere Informationen finden Sie unter Wie lade ich ein Objekt aus einem S3-Bucket herunter? im Benutzerhandbuch für Amazon Simple Storage Service.

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 veraltet	Die Tape Gateway-Funktionalität ist auf Snowball Edge-Geräten nicht mehr verfügbar.	14. März 2024
Dateischnittstelle veraltet	Die Dateischnittstelle ist nicht mehr für die Datenübertragung verfügbar.	1. März 2024
Amazon S3-kompatibler Speicher auf Snow-Family-Geräten, die auf Snowball-Edge-Speicher-optimierten 210-TB-Geräten verfügbar sind	Amazon S3-kompatibler Speicher auf Snow-Family-Geräten ist für S3-Speicher auf Snowball-Edge-speicheroptimierten 210-TB-Geräten verfügbar. Weitere Informationen finden Sie unter Verwenden von Amazon S3-kompatiblem Speicher auf Snow-Family-Geräten.	26. Februar 2024
Benutzerdefinierte AMIs bei der Bestellung von Geräten einschließen	Benutzerdefinierte Amazon Machine Images können jetzt während der Bestellung von AWS Snow Family Aufträgen vorinstalliert werden. Weitere Informationen finden Sie unter	15. November 2023

	Hinzufügen eines AMI von AWS Marketplace.	
Amazon S3-kompatibler Speicher auf Snow-Family-Geräten allgemein verfügbar	Amazon S3-kompatibler Speicher auf Geräten der Snow Family wird auf für die Datenverarbeitung optimiert en Snowball-Edge-Geräten unterstützt. Weitere Informati onen finden Sie unter Amazon S3-kompatibler Speicher auf Snow-Family-Geräten.	20. April 2023
Neue AWS-Region unterstüt zte	AWS Snowball wird jetzt in der Region Naher Osten (VAE) unterstützt. Informati onen zu Endpunkten für diese Region finden Sie unter Snowball Edge-Endpunkte und -Kontingente im Allgemeine AWS-Referenz. Informationen zum Versand finden Sie unter Überlegungen zum Versand für Snowball Edge.	6. März 2023
Neue AWS-Region unterstüt zte	AWS Snowball wird jetzt in der Region Asien-Pazifik (Jakarta) unterstützt. Informati onen zu Endpunkten für diese Region finden Sie unter Snowball Edge-Endpunkte und -Kontingente im Allgemein e AWS-Referenz. Weitere Informationen zum Versand finden Sie unter Überlegun gen zum Versand für Snowball Edge.	7. September 2022

Migration großer Daten für Snowball Edge	Snowball Edge unterstützt jetzt die Automatisierung eines großen Datenmigrationsplans. Weitere Informationen finden Sie unter Migration großer Daten (manuelle Schritte) und Erstellen eines Plans für die Migration großer Daten, um bei Bedarf Automatisierung zu initiieren.	27. April 2022
Einführung AWS Snow Device Management	Mit Snow Device Management können Sie Ihr Snowball Edge-Gerät und Ihre lokalen AWS Services remote verwalten . Alle Snowball Edge-Gerä te unterstützen Snow Device Management und sind in den meisten , in AWS-Regio nen denen Snowball Edge verfügbar ist, auf neuen Geräten vorinstalliert. Weitere Informationen finden Sie unter Verwenden von AWS Snow Device Management zur Verwaltung von Geräten	27. April 2022
NFS-Konfiguration für Snowball Edge	NFS-Konfiguration für Snowball Edge für speichero ptimierte Geräte hinzugefügt.	21. April 2022
Ratenlimits für Load Balancer	Snowball Edge unterstützt jetzt Ratenlimits, um Anfragen in einer Server-Cluster-Umg ebung zu verteilen.	19. April 2022

Unterstützung für Snowball Edge mit Tape Gateway	Sie können jetzt ein Snowball Edge-Gerät bestellen, das speziell für das Hosten des Tape Gateway-S ervice konfiguriert ist. Diese Kombination von Technologien ermöglicht die sichere Offline-Migration von Banddaten.	30. November 2021
Unterstützung für die Network Time Protocol (NTP)-Ser verkonfiguration	Snowball-Edge-Gerä te unterstützen jetzt die Konfiguration des externen Network Time Protocol (NTP)-Servers.	16. November 2021
Unterstützung für die Offline-D atenübertragung von NFS	Snowball Edge-Geräte unterstützen jetzt die Offline-Datenübertragung mit NFS. Weitere Informationen finden Sie unter Verwenden von NFS für Offline-Datenübert ragungen.	4. August 2021
Neue AWS-Region unterstüt zte	Snowball Edge-Geräte sind jetzt in der Region Afrika (Kapstadt) verfügbar AWS-Region. Weitere Informationen finden Sie unter Snowball-Edge-Endpunkte und -Kontingente im Allgemein e AWS-Referenz. Weitere Informationen zum Versand finden Sie unter Überlegun gen zum Versand für Snowball Edge.	23. November 2020

Unterstützung für den Import Ihres eigenen Images in Ihr Gerät	Sie können jetzt einen Snapshot Ihres Bildes in Ihr Snowball Edge-Gerät importieren und es als Amazon EC2-compatible Amazon Machine Image (AMI) registrieren. Weitere Informationen finden Sie unter Importieren eines Images auf Ihr Gerät als Amazon EC2-AMI.	9. November 2020
Neue AWS-Region unterstützte	Snowball Edge-Geräte sind jetzt in der Europa (Mailand) verfügbar AWS-Region. Weitere Informationen finden Sie unter Snowball-Edge-Endpunkte und -Kontingente im Allgemeine AWS-Referenz. Weitere Informationen zum Versand finden Sie unter Überlegungen zum Versand für Snowball Edge.	30. September 2020
Inhaltsumstrukturierung	Es wurde ein Abschnitt Erste Schritte erstellt, der dem Managementkonsole für die AWS Snow-Familie Workflow entspricht, und aus Gründen der Übersichtlichkeit andere Abschnitte aktualisiert. Weitere Informationen finden Sie unter Erste Schritte mit einem AWS Snowball Edge.	17. September 2020

Einführung AWS OpsHub for Snow Family	Die Snow Family-Geräte bieten jetzt ein benutzerf reundliches Tool AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen AWS Services verwalten können. Weitere Informationen finden Sie unter Verwenden von AWS OpsHub for Snow Family zur Verwaltun g von Snowball-Geräten.	16. April 2020
AWS Identity and Access Management (IAM) ist jetzt lokal auf dem AWS Snowball Edge Gerät verfügbar	Sie können jetzt AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf Ressourcen, die auf Ihrem AWS Snowball Edge Gerät ausgeführt werden, sicher zu AWS steuern. Weitere Informationen finden Sie unter Lokale Verwendung von IAM.	16. April 2020
Einführung einer neuen Geräteoption für Snowball Edge Storage Optimized (für die Datenübertragung)	Snowball fügt jetzt ein neues speicheroptimiertes Gerät hinzu, das auf den aktuellen für die Datenverarbeitung optimierten Geräten und GPU-Geräten basiert. Weitere Informationen finden Sie unter Optionen für Snowball Edge-Geräte.	23. März 2020

Unterstützung für die Validierung von microSD-Tags	In Snowball Edge Compute Optimized-Geräte (mit oder ohne GPU) sind microSD-Tags integriert. Sie können diese Tags mit der AWS Snowball Edge Verification App scannen, die auf Android verfügbar ist. Weitere Informationen finden Sie unter Validieren von NFC-Tags.	13. Dezember 2018
Sicherheitsgruppen sind jetzt für Datenverarbeitungs-Instances verfügbar	Sicherheitsgruppen in Snowball Edge-Geräten ähneln Sicherheitsgruppen in der AWS Cloud, mit einigen geringfügigen Unterschieden. Weitere Informationen finden Sie unter Sicherheitsgruppen in Snowball Edge Devices.	26. November 2018
Einführung eines On-Premises-Updates	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 Aktualisieren eines Snowball Edge.	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 Optionen für Snowball Edge-Geräte.	15. November 2018
Neue AWS-Region unterstützte	Snowball Edge-Geräte sind jetzt in der Asien-Pazifik (Mumbai) verfügbar. Beachten Sie, dass Rechen-Instances und von AWS Lambda unterstützte in dieser Region nicht unterstützt AWS IoT Greengrass werden.	24. September 2018
Einführung der Unterstützung für Amazon EC2-compatible Rechen-Instances auf Snowball Edge-Geräten	AWS Snowball unterstützt jetzt lokale Aufträge, die Amazon EC2-Rechen-Instances verwenden, die auf Snowball Edge-Geräten ausgeführt werden.	17. Juli 2018
Verbesserter Inhalt zur Fehlerbehebung	Die Kapitel "Fehlerbehebung" wurde aktualisiert und neu organisiert.	11. Juli 2018

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.