



AWS Snowcone

# AWS Snowcone Benutzerleitfaden



# AWS Snowcone Benutzerleitfaden: AWS Snowcone

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

# Table of Contents

Was ist AWS Snowcone? .....	1
Anwendungsfälle .....	2
Preisgestaltung .....	3
Wie AWS Snowcone funktioniert .....	4
AWS Snowcone Arbeitsablauf .....	5
So funktionieren Importaufträge .....	7
Online-Datenübertragung zwischen Snowcone und AWS Storage Services mit DataSync .....	7
Offline-Datenübertragung zwischen Snowcone und Amazon S3 .....	8
Für die Speicherung von Importaufträgen .....	9
Für Compute Job Storage .....	9
Technische Daten des Geräts .....	10
Übersicht .....	10
Hardware und Netzwerk .....	12
Ansicht von oben .....	12
Rückseite .....	12
Vorderteil .....	14
AWS Snowcone Wi-Fi-Spezifikationen .....	15
Spezifikationen zur Robustheit .....	15
Snowcone Stromversorgung und Zubehör .....	16
Festplatten- und CPU-Leistung .....	16
Einrichten .....	17
Melden Sie sich an für AWS .....	17
Bevor Sie bestellen .....	18
Über die lokale Umwelt .....	18
Mit Sonderzeichen arbeiten .....	19
Amazon EC2 .....	20
Unterschied zwischen Amazon EC2- und Amazon EC2-kompatiblen Instances auf Geräten der Snow Family .....	21
Preise für Compute-Instances auf Snowcone .....	21
Voraussetzungen .....	21
Überprüfung der Produktcodes und Plattformdetails von AMIs AWS Marketplace .....	22
Ein Linux-AMI aus einer Instance erstellen .....	23
Ein Linux-AMI aus einem Snapshot erstellen .....	23
Erste Schritte .....	28

Einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen .....	28
Schritt 1: Wählen Sie einen Jobtyp .....	29
Schritt 2: Wählen Sie Ihre Rechen- und Speicheroptionen .....	30
Schritt 3: Wählen Sie Ihre Funktionen und Optionen .....	33
Schritt 4: Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen .....	33
Schritt 5: Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job .....	36
Herunterladen AWS OpsHub .....	37
Stornierung eines Auftrags zur Bestellung eines Snow Family-Geräts .....	38
Zugangsdaten für den Zugriff auf ein Snow Family-Gerät abrufen .....	39
Entsperren des Snow Family-Geräts .....	40
Problembehandlung beim Entsperren eines Snow Family-Geräts .....	42
Das Snow Family-Gerät neu starten .....	42
AWS OpsHub Zur Verwaltung von Geräten verwenden .....	48
AWS OpsHub Für Snow Family-Geräte herunterladen .....	49
Ein Gerät entsperren .....	50
Lokales Entsperren eines Geräts .....	50
Ein Gerät aus der Ferne entsperren .....	53
Überprüfung der Signatur von AWS OpsHub .....	57
AWS Dienste verwalten .....	60
Lokale Verwendung von Datenverarbeitungs-Instances .....	61
Verwaltung der NFS-Schnittstelle .....	69
Wird verwendet AWS DataSync , um Dateien zu übertragen AWS .....	78
Übertragen von Dateien .....	79
Verwaltung Ihrer Geräte .....	80
Ihr Gerät neu starten .....	80
Ihr Gerät wird heruntergefahren .....	81
Bearbeitung des Gerätealias .....	82
Updates erhalten .....	83
Profile verwalten .....	84
Einstellung der NTP-Zeitserver für Ihr Gerät .....	86
Den AWS Snowball Edge Client verwenden .....	89
Den Snowball Edge-Client herunterladen und installieren .....	89
Befehle für den Snowball Edge-Client .....	89
Konfiguration eines Profils für den Snowball Edge-Client .....	91
Anfordern Ihres QR-Codes für die NFC-Validierung .....	92
Ein AWS Snowcone Gerät entsperren .....	92

Einen Snowcone aktualisieren .....	93
Abrufen von Anmeldeinformationen .....	96
Einen Dienst auf Ihrem Snowcone-Gerät starten .....	97
Einen Dienst auf Ihrem Snowcone-Gerät beenden .....	98
Abrufen des Zertifikats für die Datenübertragung .....	98
AWS Snowcone Protokolle .....	99
Abrufen des Gerätestatus .....	101
Abrufen des Servicestatus .....	103
Das AWS DataSync AMI starten .....	105
NFS starten und Zugriff einschränken .....	108
Beschränken des Zugriffs auf NFS-Freigaben, wenn NFS ausgeführt wird .....	109
Den Exportpfad für einen Amazon S3 S3-Bucket abrufen .....	109
Debugging für lokale AWS Operatoren aktivieren .....	109
Debugging für lokale Operatoren AWS deaktivieren .....	110
Eine direkte Netzwerkschnittstelle erstellen .....	110
Informationen über eine direkte Netzwerkschnittstelle abrufen .....	110
Aktualisierung einer direkten Netzwerkschnittstelle .....	111
Löschen einer direkten Netzwerkschnittstelle .....	111
Funktionsstatus wird überprüft .....	112
Funktionsstatus ändern .....	112
Zeitserver einrichten .....	113
Zeitquellen werden überprüft .....	114
Geräte mithilfe von Snow Device Management verwalten .....	117
Auswahl des Status „Snow Device Management“ bei der Bestellung eines Snow Family- Geräts .....	118
Snow Device Management aktivieren .....	119
Hinzufügen von Berechtigungen für Snow Device Management zu einer IAM-Rolle .....	120
CLI-Befehle für Snow Device Management .....	121
Erstellen Sie eine Aufgabe .....	122
Überprüfen Sie den Aufgabenstatus .....	123
Überprüfen Sie die Geräteinformationen .....	124
Überprüfen Sie den Status der Amazon EC2-kompatiblen Instanz .....	126
Überprüfen Sie die Metadaten der Aufgabe .....	128
Eine Aufgabe stornieren .....	129
Befehle und Syntax auflisten .....	130
Geräte auflisten, die per Fernzugriff verwaltet werden können .....	131

Den Aufgabenstatus geräteübergreifend auflisten .....	132
Verfügbare Ressourcen auflisten .....	133
Geräte- oder Aufgaben-Tags auflisten .....	134
Aufgaben nach Status auflisten .....	135
Tags anwenden .....	136
Tags entfernen .....	137
AWS Dienste nutzen .....	138
Amazon EC2 für Compute verwenden .....	138
Übersicht .....	139
Voraussetzungen .....	140
Anlegen eines Auftrags mit Datenverarbeitungs-Instances .....	141
Netzwerkconfiguration für Datenverarbeitungs-Instances .....	146
Mit SSH eine Verbindung zu Ihrer Compute-Instance auf einem Snowcone herstellen .....	153
Snowcone-Client-Befehle für Compute-Instances .....	154
Verwenden von Instance Metadata Service for Snow mit Amazon EC2-kompatiblen Instances .....	160
Verwenden des Amazon EC2-kompatiblen Endpunkts .....	170
Automatisches Starten von Amazon EC2-kompatiblen Instances mit Startvorlagen .....	187
Verwenden Sie Block Storage mit Ihren EC2-kompatiblen Instances .....	189
Sicherheitsgruppen in Snow-Geräten .....	190
Unterstützte Instance-Metadaten und Benutzerdaten .....	191
Problembhebung bei Amazon EC2 .....	193
Zum DataSync Übertragen von Dateien verwenden .....	195
Verwaltung der NFS-Schnittstelle .....	196
NFS-Konfiguration für Geräte der Snow Family .....	197
Verwendung auf EC2-kompatiblen Instances AWS IoT Greengrass .....	202
Einrichtung Ihrer Amazon EC2-kompatiblen Instance .....	202
Für die Nutzung der AWS Dienste erforderliche Ports .....	206
Rückgabe des Snowcone-Geräts .....	207
Trennen Sie das Snowcone-Gerät .....	207
Daten auf Ihrem Gerät schützen .....	208
Sicherung Ihres AWS Snowcone .....	208
Validieren von NFC-Tags .....	209
Grundlegendes zum Jobstatus .....	211
Benachrichtigungen .....	213
So verwendet Snow Amazon SNS .....	213

Verschlüsselung von SNS-Themen für Statusänderungen bei Snow Jobs .....	213
Einrichtung einer vom Kunden verwalteten KMS-Schlüsselrichtlinie .....	214
SNS-Benachrichtigungsbeispiele .....	216
Den Bestellvorgang verstehen .....	238
Den Versandprozess verstehen .....	238
Rückgabe eines Snowcone-Geräts .....	238
Mit dem AWS Management Console .....	239
Den Snowcone von der Konsole aus bestellen .....	239
Verwenden der Job Management API .....	239
Allgemeine Verwendungszwecke von JMAPI .....	239
JMAPI Erforderliche Zeichenketten .....	240
JMAPI-Endpunkte .....	240
JMAPI-CLI-Befehle .....	240
Beispiele .....	241
EC2-Jobs .....	242
Konfiguration eines AMI für die Verwendung von SSH für die Connect zu Compute- Instances, die auf dem Gerät gestartet wurden .....	243
Erstellen Sie Ihren Job mithilfe der Konsole .....	244
Erstellen Sie Ihren Job mit der AWS CLI .....	244
Versandüberlegungen .....	246
Ein AWS Snowcone Gerät für den Versand vorbereiten .....	246
Versandeinschränkungen nach Regionen .....	247
Versand eines AWS Snowcone Geräts .....	248
Versandanbieter .....	248
Snowcone-Geräte aktualisieren .....	257
Voraussetzungen .....	258
Updates werden heruntergeladen .....	258
Updates werden installiert .....	260
Aktualisierung des SSL-Zertifikats .....	263
Aktualisierung Ihrer Amazon Linux 2-AMIs auf Geräten der Snow Family .....	265
Bewährte Methoden .....	266
Sicherheit .....	266
Network (Netzwerk) .....	267
Ressourcenmanagement .....	267
Verwaltung von EC2-kompatiblen Instances .....	267
Leistung .....	268

---

Snowcone-Kontingente .....	269
Ressourcenkontingente berechnen .....	269
Einschränkungen für den Versand eines Snowcone-Geräts .....	270
Einschränkungen bei der Bearbeitung Ihres zurückgesandten Snowcone-Geräts für den Import .....	271
Verfügbar AWS-Regionen .....	271
Fehlerbehebung .....	272
Fehlerbehebung bei Compute-Instances .....	272
Probleme mit dem Netzwerk .....	272
Die IP-Adresse ist 0.0.0.0 .....	272
Das Gerät konnte nicht entsperrt werden .....	273
Probleme mit einer EC2-kompatiblen Instance bei Datasync .....	273
Fehler: Die Instance konnte nicht gestartet werden .....	273
Probleme mit der Datenübertragung .....	273
Zugriff vom Server verweigert .....	273
Die Verbindung wird während der Datenübertragung unterbrochen .....	274
Spawn Showmount ENOENT .....	274
Behebung von Problemen bei der Rückgabe von Snow Family-Geräten .....	275
API-Referenz .....	276
Dokumentverlauf .....	277
AWS Glossar .....	283
.....	cclxxxiv



# Was ist AWS Snowcone?

AWS Snowcone ist ein tragbares, robustes und sicheres Gerät für Edge-Computing und Datenübertragung. Sie können ein Snowcone-Gerät verwenden, um Daten zu sammeln, zu verarbeiten und dorthin zu übertragen AWS Cloud, entweder offline, indem Sie das Gerät an senden AWS, oder online, indem Sie es verwenden AWS DataSync.

Es kann schwierig sein, Anwendungen in rauen Edge-Umgebungen (außerhalb des Rechenzentrums) oder in Umgebungen auszuführen, in denen es an konsistenter Netzwerkkonnektivität mangelt. An diesen Standorten fehlen häufig der Platz, die Stromversorgung und die Kühlung, die für die IT-Ausrüstung von Rechenzentren erforderlich sind.

Snowcone ist in zwei Geschmacksrichtungen erhältlich:

- Snowcone — Snowcone verfügt über zwei vCPUs, 4 GB Arbeitsspeicher und 8 TB Festplattenspeicher (HDD).
- Snowcone SSD — Snowcone SSD verfügt über zwei vCPUs, 4 GB Arbeitsspeicher und 14 TB Solid-State-Drive-Speicher (SSD).

Mit zwei CPUs und Terabyte Speicher kann ein Snowcone-Gerät Edge-Computing-Workloads ausführen, die Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwenden, und Daten sicher speichern.

Snowcone-Geräte sind klein (8,94 Zoll x 5,85 Zoll x 3,25 Zoll/227 mm x 148,6 mm x 82,65 mm), sodass sie neben Maschinen in einer Fabrik aufgestellt werden können, um Daten zu sammeln, zu formatieren und zur Speicherung und Analyse zurück zu transportieren. AWS Ein Snowcone-Gerät wiegt etwa 4,5 lbs. (2 kg), sodass Sie es in einem Rucksack tragen, es mit Batteriebetrieb verwenden und die Wi-Fi-Schnittstelle verwenden können, um Sensordaten zu sammeln.

## Note

Wi-Fi ist nur in AWS-Regionen Nordamerika verfügbar.

Snowcone-Geräte bieten eine Schnittstelle mit NFS-Unterstützung (Network File System). Snowcone-Geräte unterstützen die Datenübertragung von lokalen Windows-, Linux- und macOS-Servern und dateibasierten Anwendungen über die NFS-Schnittstelle.

Like AWS Snowball AWS Snowcone verfügt über mehrere Ebenen von Sicherheitsverschlüsselungsfunktionen. Sie können jeden dieser Services verwenden, um Daten zu sammeln, zu verarbeiten und zu übertragen und Edge-Computing-Workloads auszuführen AWS, die Amazon EC2-kompatible Instances verwenden. Snowcone wurde für Datenmigrationsanforderungen von bis zu Dutzenden von Terabyte konzipiert. Es kann in Umgebungen mit begrenztem Platzangebot verwendet werden, in die Snowball Edge-Geräte nicht passen.

## Anwendungsfälle

Sie können AWS Snowcone Geräte für die folgenden Anwendungsfälle verwenden:

- Für Edge-Computing-Anwendungen, um Daten zu sammeln, zu verarbeiten, um sofortige Erkenntnisse zu gewinnen, und die Daten dann online zu übertragen AWS.
- Um Daten, die kontinuierlich von Sensoren oder Maschinen generiert werden, online AWS an eine Fabrik oder an andere Edge-Standorte zu übertragen.
- Um Medien, wissenschaftliche oder andere Inhalte von AWS Speicherdiensten an Ihre Partner und Kunden zu verteilen.
- Um Inhalte zu aggregieren, indem Medien, wissenschaftliche oder andere Inhalte von Ihren Edge-Standorten zu übertragen AWS werden.
- Für einmalige Datenmigrationsszenarien, in denen Ihre Daten für die Übertragung bereit sind, bietet Snowcone eine schnelle und kostengünstige Möglichkeit, bis zu 8 TB oder 14 TB an Daten auf die zu übertragen, AWS Cloud indem Sie das Gerät zurückschicken. AWS

Für mobile Bereitstellungen kann ein Snowcone-Gerät mit einer bestimmten Akkuleistung betrieben werden. Bei einer geringen Arbeitslast bei 25 Prozent CPU-Auslastung kann das Gerät bis zu etwa 6 Stunden im Akkubetrieb betrieben werden. Sie können die Wi-Fi-Schnittstelle Ihres Snowcone-Geräts verwenden, um Daten von drahtlosen Sensoren zu sammeln. Ein AWS Snowcone Gerät ist stromsparend, tragbar, leicht und vibrationsfest, sodass Sie es an einer Vielzahl von abgelegenen und abgelegenen Orten verwenden können.

### Note

WLAN ist nur AWS-Regionen in Nordamerika verfügbar.

# Preisgestaltung

Sie können ein Snowcone-Gerät gegen Bezahlung pro Nutzung bestellen und das Gerät bis zu vier Jahre lang behalten. Informationen zu AWS Snowcone Preisen und Gebühren finden Sie unter [AWS Snowcone Preise](#).

# Wie AWS Snowcone funktioniert

AWS Snowcone ist ein tragbares Gerät, das für Edge-Computing und Datenübertragung verwendet wird. Zu Beginn fordern Sie ein oder mehrere Snowcone-Geräte an, AWS Management Console je nachdem, wie viele Daten Sie übertragen müssen und welche Rechenleistung erforderlich ist. Die Buckets, Daten und Amazon Elastic Compute Cloud (Amazon EC2) Amazon Machine Images (AMIs) von Amazon Simple Storage Service (Amazon S3), die Sie auswählen, werden automatisch konfiguriert, verschlüsselt und auf Ihren Geräten vorinstalliert. Der AWS DataSync Agent ist außerdem vorinstalliert, bevor Ihre Geräte an Sie versendet werden.

Wenn Ihr Gerät ankommt, verbinden Sie es mit Ihrem lokalen Netzwerk und legen die IP-Adresse entweder manuell oder automatisch mit dem Dynamic Host Configuration Protocol (DHCP) fest. Sie müssen eine Anwendung mit grafischer Benutzeroberfläche (GUI) zur Verwaltung Ihres Snowcone-Geräts herunterladen und installieren AWS OpsHub for Snow Family. Sie können es auf jedem Windows- oder MacOS-Client-Computer installieren, z. B. auf einem Laptop.

Wenn Sie das Gerät öffnen AWS OpsHub und entsperren, wird ein Dashboard mit Ihrem Gerät und seinen Systemmetriken angezeigt. Anschließend können Sie mit nur wenigen Klicks Instances starten, um Ihre Edge-Anwendungen bereitzustellen oder Ihre Daten auf das Gerät zu migrieren AWS OpsHub.

Wenn Ihr Rechen- oder Datenübertragungsauftrag abgeschlossen ist und das Gerät zur Rücksendung bereit ist, aktualisiert das E Ink-Versandetikett automatisch die Absenderadresse und stellt so sicher, dass das Snowcone-Gerät an die richtige AWS Einrichtung geliefert wird. Wenn das Gerät ausgeliefert wird, können Sie den Status der Sendungsverfolgung über Nachrichten erhalten, die von Amazon Simple Notification Service (Amazon SNS) gesendet werden, generierte Texte und E-Mails oder direkt von der Konsole aus gesendet werden.

## Themen

- [AWS Snowcone Arbeitsablauf](#)
- [So funktionieren Importaufträge](#)
- [Für die Speicherung von Importaufträgen](#)
- [Für Compute Job Storage](#)

# AWS Snowcone Arbeitsablauf

Sie können drei verschiedene Jobtypen erstellen. Obwohl sich die Auftragstypen in ihren Anwendungsfällen unterscheiden, haben sie alle den folgenden Arbeitsablauf für die Bestellung, den Empfang und die Rückgabe des Geräts.

## Der Arbeitsablauf

1. Job erstellen — Sie erstellen jeden Job auf der Managementkonsole für die AWS Snow-Familie oder programmgesteuert über die Job-Management-API und wählen je nach Anwendungsfall einen Gerätetyp — Snowcone oder Snowcone SSD — aus. Sie können den Status des Jobs auf der AWS Management Console oder über die Snowcone-API verfolgen.
2. Ein Gerät ist für Ihren Job vorbereitet — AWS bereitet ein AWS Snowcone Gerät für Ihren Job vor, und der Status Ihres Jobs ändert sich zu Preparing Snowcone.
3. Ein Gerät wird vom Transporteur in Ihrer Region an Sie versandt. Der Spediteur übernimmt von hier aus, und der Status Ihres Auftrags ändert sich jetzt in „Auf dem Weg zu Ihnen“. Du findest deine Tracking-Nummer und einen Link zur Tracking-Website auf der Managementkonsole für die AWS Snow-Familie Konsole oder mit der Job-Management-API. Informationen darüber, wer der Mobilfunkanbieter Ihrer Region ist, finden Sie unter [Überlegungen zum Versand für AWS Snowcone](#).
4. Besorgen Sie sich ein Snowcone-Netzteil — Um den Platzbedarf möglichst gering zu halten, werden Snowcone-Geräte nicht mit einem Netzteil geliefert. Snowcone verwendet ein 45-Watt-Netzteil mit USB-C-Anschluss. Es kann auch mit einer tragbaren Batterie betrieben werden. Weitere Informationen finden Sie unter [AWS Snowcone Stromversorgung und Zubehör](#).
5. Gerät erhalten — Wenige Tage später liefert der Spediteur Ihrer Region das AWS Snowcone Gerät an die Adresse, die Sie bei der Erstellung des Auftrags angegeben haben. Der Status Ihres Auftrags ändert sich in „An Sie geliefert“. Das Gerät wird nicht in einer Box geliefert, da es sich bei dem Gerät um einen eigenen Versandbehälter handelt.
6. Holen Sie sich Ihre Anmeldeinformationen und laden Sie die Anwendung AWS OpsHub oder den Snowball Edge-Client für Snow Family herunter — Machen Sie sich bereit, mit der Datenübertragung zu beginnen, indem Sie Ihre Anmeldeinformationen, Ihr Jobmanifest und den Entsperrcode des Manifests abrufen und dann den Snowball Edge-Client herunterladen.
  - Rufen Sie das Manifest für Ihr Gerät von der Konsole oder mit der Job-Management-API ab, wenn sich das Gerät an Ihrem Standort vor Ort befindet. Das Manifest wird verwendet, um Ihren Zugriff auf das Gerät zu authentifizieren. Das Manifest ist verschlüsselt, sodass es nur mit dem Entsperrcode entschlüsselt werden kann.

- Der Entsperrcode umfasst 29 Zeichen und dient zum Entschlüsseln des Manifests. Sie erhalten den Entsperrcode in der Konsole; oder über die API zur Auftragsverwaltung. Um unbefugten Zugriff auf das Gerät zu verhindern, während es sich in Ihrer Einrichtung befindet, empfehlen wir, den Entsperrcode an einem sicheren Ort aufzubewahren, der sich vom Speicherort des Manifests unterscheidet.
- AWS OpsHub for Snow Family ist eine Anwendung zur Verwaltung von Snow Family-Geräten, einschließlich Snowcone. Die AWS OpsHub for Snow Family GUI hilft Ihnen bei der Einrichtung und Verwaltung von Snowcone-Geräten, sodass Sie Ihre Edge-Computing-Workloads schnell ausführen und Daten auf die migrieren können. AWS Cloud Mit nur wenigen Klicks können AWS OpsHub Sie Ihr Snowcone-Gerät entsperren und konfigurieren, Daten per Drag-and-Drop verschieben, Anwendungen starten oder Gerätekenzzahlen überwachen. Sie können es auf Windows- oder MacOS-Client-Computern, z. B. einem Laptop, herunterladen und installieren. Bei der Nutzung des AWS OpsHub-Service fallen keine Kosten an.

Laden Sie es AWS OpsHub von [AWS Snowball Ressourcen](#) herunter. Weitere Informationen zu finden AWS OpsHub Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

- Der Snowball Edge-Client ist das Tool, mit dem Sie den Datenfluss vom Gerät zu Ihrem lokalen Datenziel verwalten.
7. Platzieren Sie die Hardware — Platzieren Sie das Gerät in Ihrem Rechenzentrum und öffnen Sie es gemäß den Anweisungen auf dem Gehäuse. Connect das Gerät an eine Stromversorgung und Ihr lokales Netzwerk an.
  8. Gerät einschalten — Schalten Sie das Gerät ein, indem Sie den Netzschalter über dem LCD-Display drücken. Nach einigen Minuten erscheint im Display die Meldung Ready (Bereit).
  9. Rufen Sie die IP-Adresse für das Gerät ab — Auf dem LCD-Display befindet sich die Registerkarte CONNECTION. Tippen Sie auf diese Registerkarte und rufen Sie die IP-Adresse für das AWS Snowcone Gerät ab.
  10. Zum Entsperren des Geräts verwenden AWS OpsHub — Um das AWS Snowcone Gerät zu entsperren, geben Sie die IP-Adresse des Geräts ein, laden Ihr Manifest und den Entsperrcode hoch. AWS OpsHub entschlüsselt das Manifest und authentifiziert damit Ihren Zugriff auf das Gerät. Weitere Informationen zu finden Sie AWS OpsHub unter. [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#)
  11. Gerät verwenden — Dient AWS OpsHub zum Einrichten und Verwalten von AWS Snowcone Geräten, sodass Sie Ihre Edge-Computing-Workloads schnell ausführen und Daten an das AWS Cloud übertragen können. Mit nur wenigen Klicks können AWS OpsHub Sie Ihr Snowcone-Gerät

entsperren und konfigurieren, Daten per Drag-and-Drop verschieben, Anwendungen starten oder Gerätekenzahlen überwachen. Details hierzu finden Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

12 Ziehen Sie nicht das Ethernet- oder Stromversorgungskabel ab — Ziehen Sie das Ethernet-Kabel oder die USB-C-Stromversorgung oder den Akku nicht während der Datenübertragung oder bei Rechengvorgängen ab. Um das Snowcone-Gerät auszuschalten, nachdem Ihre Datenübertragung oder Ihr Rechenjob abgeschlossen ist, drücken Sie den Netzschalter.

13 Bereiten Sie das Gerät für die Rückreise vor — Nachdem Sie das Gerät an Ihrem Standort vor Ort aufgestellt haben, drücken Sie den Netzschalter über dem LCD-Display, um das Gerät auszuschalten. Trennen Sie das Gerät vom Stromnetz, verstauen Sie die Netzkabel in der Kabelnische auf der Oberseite des Geräts und schließen Sie alle drei Türen des Geräts. Das Gerät ist nun versandfertig für die Rückgabe.

14 Der Mobilfunkanbieter Ihrer Region sendet das Gerät zurück an AWS— Wenn der Mobilfunkanbieter das AWS Snowcone Gerät hat, ändert sich der Status des Auftrags in Auf dem Weg zu. AWS

## So funktionieren Importaufträge

Sie können Snowcone verwenden, um Daten online zwischen Ihrem Gerät und AWS Speicherdiensten zu übertragen, indem Sie AWS DataSync Sie können Daten auch offline von Ihren lokalen Speichergeräten auf Ihr Snowcone-Gerät übertragen.

## Online-Datenübertragung zwischen Snowcone und AWS Storage Services mit DataSync

[AWS DataSync](#) ist ein Online-Datenübertragungsdienst, der das Kopieren großer Datenmengen zu und von AWS Speicherdiensten über das Internet vereinfacht, automatisiert und beschleunigt. AWS Direct Connect Auf Ihrem Snowcone-Gerät ist ein AWS DataSync Agent vorinstalliert, der für die Übertragung von Daten zwischen dem Gerät und Amazon S3 S3-Buckets, Amazon Elastic File System (Amazon EFS) -Dateisystemen und Amazon FSx for Windows File Server verwendet wird. DataSync kümmert sich automatisch um das Verschieben von Dateien und Objekten, die Planung von Datenübertragungen, die Überwachung des Übertragungsfortschritts, die Verschlüsselung von Daten, die Überprüfung von Datenübertragungen und die Benachrichtigung von Kunden über Probleme.

Der DataSync Agent ist während der Snowcone-Auftragsvorbereitung als Amazon Machine Image (AMI) auf Ihrem Snowcone-Gerät vorinstalliert. Um Daten online zu übertragen AWS, verbinden Sie das Snowcone-Gerät mit dem externen Netzwerk und verwenden Sie AWS OpsHub for Snow Family oder AWS Command Line Interface (AWS CLI), um das DataSync Agenten-AMI zu starten. Aktivieren Sie den DataSync Agenten mit dem AWS Management Console oder dem AWS CLI. Richten Sie dann Ihre Online-Datenübertragungsaufgabe zwischen dem AWS Snowcone Network File System (NFS) -Speicher und Amazon S3, Amazon EFS oder Amazon FSx ein.

Du kannst DataSync das Laufen auf Snowcone für Folgendes nutzen:

- Für Edge-Computing-Anwendungen, um Daten zu sammeln, zu verarbeiten, um sofortige Erkenntnisse zu gewinnen, und die Daten dann online zu AWSübertragen.
- Um Daten, die kontinuierlich von Sensoren oder Maschinen generiert werden, online AWS an eine Fabrik oder an andere Edge-Standorte zu übertragen.
- Um Medien, wissenschaftliche oder andere Inhalte online von AWS Speicherdiensten an Ihre Partner und Kunden zu verteilen.
- Um Inhalte zu aggregieren, indem Medien, wissenschaftliche oder andere Inhalte online von Ihren Edge-Standorten nach übertragen AWS werden.

Für einmalige Edge-Computing- oder Datenübertragungswflows oder für Snowcone-Workflows an Edge-Standorten ohne WAN-Verbindung (Wide Area Network) oder unzureichender WAN-Bandbreite empfehlen wir, das Snowcone-Gerät zurückzusenden, AWS um die Datenübertragung abzuschließen.

## Offline-Datenübertragung zwischen Snowcone und Amazon S3

Für Offline-Datenimportaufträge verbinden Sie das Snowcone-Gerät mit Ihrem lokalen Netzwerk und verwenden es dann, um das Gerät AWS OpsHub zu entsperren. Laden Sie es AWS OpsHub von der [AWS Snowball Ressourcenseite](#) herunter. Sie können Daten von lokalen Speichergeräten über die NFS-Schnittstelle auf Ihr Snowcone-Gerät kopieren. Nachdem Sie die Daten auf Ihr Snowcone-Gerät kopiert haben, sorgt das E Ink-Versandetikett auf dem Gerät dafür, dass das Gerät automatisch an die richtige AWS Einrichtung gesendet wird. Sie können das Snowcone-Gerät mithilfe von Amazon SNS-generierten Textnachrichten oder E-Mails und der Konsole verfolgen.



## Für die Speicherung von Importaufträgen

Intern enthält ein Snowcone-Gerät 8 TB oder 14 TB Festplattenspeicher, der mit dem internen Network File System (NFS) -Service oder lokalen Amazon EC2-kompatiblen Instances über eine lokale Volumenpräsentation im Amazon Elastic Block Store (Amazon EBS) verwendet werden kann. Sie können 8 TB oder 14 TB für das NFS-Speichervolume und 150 GB für das kapazitätsoptimierte HDD (sbg1) Amazon EBS-Speichervolume verwenden.

## Für Compute Job Storage

Wenn es sich bei dem Auftragsstyp um lokale Datenverarbeitung handelt, können Sie insgesamt 8 TB oder 14 TB an lokalen kapazitätsoptimierten Amazon EBS-Volumes mit HDD (sbg1) erstellen und diese Amazon EC2-kompatiblen Instances zuordnen. Durch die Verwendung von Amazon EBS-Volumes können die lokalen Amazon EC2-kompatiblen Instances auf mehr lokale Kapazität zugreifen als auf das Root-Volume allein. Da es sich nur um lokalen Speicher handelt, gehen auf die Amazon EBS-Volumes geschriebene Daten verloren, wenn das Gerät zurückgegeben wird, AWS da sie nicht in Amazon S3 importiert werden können.

### Note

Der NFS-Server ist für Rechenaufträge nicht verfügbar. Wenn Sie Daten in oder aus dem oder zum Ausführen eines AWS DataSync Agenten importieren AWS Cloud oder exportieren müssen, wählen Sie bei der Bestellung nicht den lokalen Rechenauftragstyp.

# AWS Snowcone Technische Daten des Geräts

Dieser Abschnitt enthält Informationen zu AWS Snowcone Gerätespezifikationen und Anforderungen für Hardware, Netzwerk, WLAN und Stromversorgung.


## Themen

- [Zusammenfassung der Funktionen und Spezifikationen](#)
- [Hardware und Netzwerk](#)
- [AWS Snowcone Wi-Fi-Spezifikationen](#)
- [Spezifikationen zur Robustheit](#)
- [AWS Snowcone Stromversorgung und Zubehör](#)
- [Festplatten- und CPU-Leistung](#)

## Zusammenfassung der Funktionen und Spezifikationen

In der folgenden Tabelle sind die Funktionen und Spezifikationen des Snowcone-Geräts zusammengefasst.

Item	Spezifikation
Nutzungsszenario	Industrielles Internet der Dinge (IoT), Transport, IoT im Gesundheitswesen, Inhaltsverteilung, taktisches Edge-Computing, Logistik, autonomes Fahrzeug, Datenmigration
Größe des Geräts	9 Zoll lang, 6 Zoll breit und 3 Zoll hoch (227 mm x 148,6 mm x 82,65 mm)
Gewicht des Geräts	4,5 lbs. (2,04 kg) für Snowcone und 4,6 lbs (2,09 kg) Snowcone SSD
Speicherkapazität	8 TB nutzbar für Snowcone und 14 TB nutzbar für Snowcone SSD
Integrierte Rechenoptionen	Amazon EC2 Amazon Machine Images (AMIs)
Verschlüsselung	Ja, 256-Bit

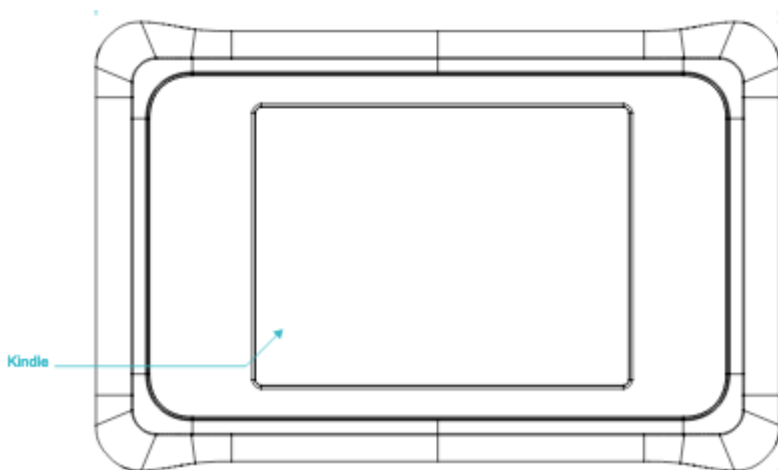
Item	Spezifikation
Übertragungen über das Network File System (NFS)	Ja
Übertragungen über die Amazon S3 S3-API	Nein
Mobilität	Batteriegestützter Betrieb
Drahtlos	WLAN <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b> WLAN ist nur AWS-Regionen in Nordamerika verfügbar.</p> </div>
Anzahl verwendbarer vCPUs	2 vCPUs
Verfügbarer Arbeitsspeicher	4 GB
Netzwerkschnittstellen	2 x 1/10 Gigabit (Gb) — RJ45
AWS DataSync Agent vorinstalliert	Ja
Typische Berufslebensdauer	Offline- oder Online-Datenübertragung: Tage bis Wochen Edge-Computing: Wochen bis Monate
Max. Auftragsdauer	Edge-Computing oder laufende Datenübertragung: Bis zu 360 Tage

# Hardware und Netzwerk

Ein Snowcone-Gerät bietet 8 TB oder 14 TB verfügbaren Speicherplatz. Es führt spezifische Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit zwei verfügbaren CPUs und 4 GB verfügbarem Speicher aus, um Ihre Anwendungen und AWS IoT Greengrass Funktionen zu unterstützen. In diesem Abschnitt finden Sie Informationen über das physische Gerät, wie z. B. die Schnittstellen, den Netzschalter und den Strombedarf, wie sie in den verschiedenen Ansichten des Geräts angezeigt werden.

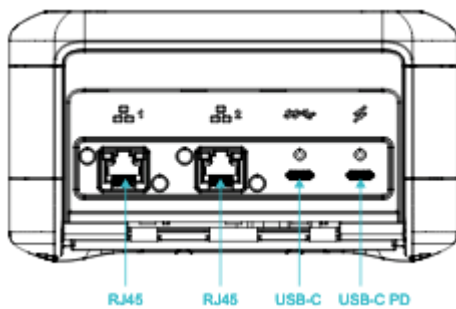
## Ansicht von oben

Auf der Oberseite des Snowcone-Geräts befindet sich ein integriertes E-Ink-Touch-Display, das als Bedienoberfläche für die Einrichtung von verkabelten und drahtlosen Netzwerken verwendet wird. Es dient auch als Display für ein elektronisches Versandetikett. Das elektronische Versandetikett ist mit Versandetiketten für ausgehende und eingehende Sendungen vorprogrammiert, die sich nach dem ersten Einschalten des Geräts automatisch ändern.



## Rückseite

Sie stellen alle Kabelverbindungen auf der Rückseite her. In diesem Abschnitt werden die einzelnen Anschlüsse beschrieben.



## Stromversorgung

Das Gerät wird über den USB-C-Anschluss ganz rechts mit einem geeigneten Netzteil, das mindestens 45 W liefern kann, mit Strom versorgt.

### **i** Note

AWS Snowcone ist nicht im Lieferumfang enthalten, da es mit dem kleinstmöglichen Formfaktor geliefert wird. Details hierzu finden Sie unter [AWS Snowcone Stromversorgung und Zubehör](#).

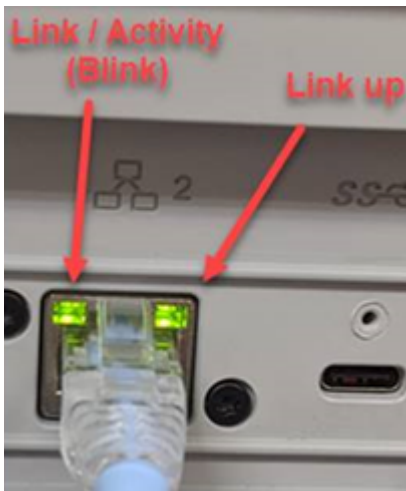
## USB

Die erste USB-C-Verbindung ist nicht aktiv.

## Ethernet-Anschlüsse 1 und 2

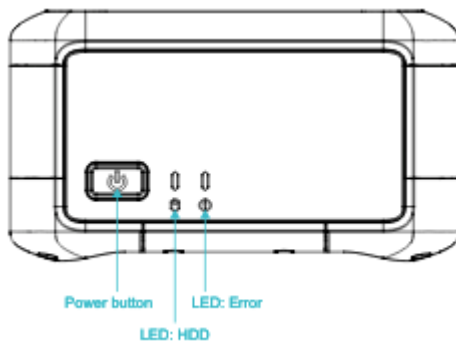
Für verkabelte Netzwerke bietet das Snowcone-Gerät zwei Anschlüsse, die automatisch für 1-Gigabit- (Gb) - oder 10-Gbit-Ethernet-Netzwerke aushandeln.

RJ45 10/1G Base-T-Ethernet-Ports — Diese Ports handeln automatisch zwischen 10 Gb und 1 Gb auf der Grundlage der Fernverbindungsfähigkeit aus. Sie handeln keine Geschwindigkeiten unter 1 Gb aus (z. B. 100 MB oder 10 MB). Die Link-LED befindet sich rechts neben jedem Anschluss und die Aktivitäts-LED befindet sich links.



## Vorderteil

Auf der Vorderseite befinden sich der Netzschalter und die Status-LED-Anzeigen.



### Netzschalter

Um das Gerät einzuschalten, drücken Sie kurz den Netzschalter. Die Taste leuchtet auf, die E-Ink-Anzeige ändert sich in einen Fortschrittsbalken, und Please wait wird angezeigt.

Um das Gerät auszuschalten, halten Sie den Netzschalter zwei Sekunden lang gedrückt, oder bis auf dem E-Ink-Display Please wait (Bitte warten) angezeigt wird.

#### Note

Wenn Sie den Netzschalter länger als fünf Sekunden gedrückt halten, wird das Gerät ausgeschaltet. Dies wird nicht empfohlen, da dadurch Daten in Puffern verloren gehen können. Nach einem Stromausfall stellt das Gerät automatisch den letzten Betriebszustand wieder her.

## Status-LEDs

Zwei Status-LEDs befinden sich neben dem Netzschalter. Die linke LED blinkt bei Festplattenaktivität und die rechte LED leuchtet auf, wenn ein Fehler vorliegt.

## AWS Snowcone Wi-Fi-Spezifikationen

AWS Snowcone unterstützt Gigabit-Wi-Fi-Netzwerke mit dem IEEE 802.11ac-Standard sowie 802.11abgn-Netzwerke. Um den drahtlosen Durchsatz für Snowcone zu maximieren, verwenden Sie 2x2 802.11ac 160-MHz-Kanäle, die bis zu 10-mal schneller sein können als 1x1-802.11bgn-Basisnetzwerke. Die Snowcone Wi-Fi-Spezifikationen sind IEEE 802.11abgn+ac, 2x2, MIMO, Dualband 2 GHz und 5 G (160 MHz). Die Betriebsfrequenzen sind 2 GHz und 5 GHz.

Sie können Snowcone über ein physisches Ethernet-Kabel mit Ihrem lokalen Netzwerk verbinden, oder Sie können es drahtlos über WLAN verbinden. Mit der Wi-Fi-Verbindung können Sie das Snowcone-Gerät mithilfe von Snowcone und lokalen Speichergeräten verwalten AWS OpsHub und Daten zwischen Snowcone und lokalen Speichergeräten übertragen.

### Note

WLAN ist nur AWS-Regionen in Nordamerika verfügbar.

## Spezifikationen zur Robustheit

AWS Snowcone Geräte sind so konzipiert, dass sie strenge Normen für die Robustheit erfüllen, darunter ISTA-3A, ASTM D4169 und MIL-STD-810G für Stöße bei freiem Fall, Betriebsvibrationen und mehr. Sie sind so konzipiert, dass sie Stürze bis zu 3,8 Fuß (1,15 Meter) aushalten. Sie erfüllen außerdem die IEC-Norm IP65 zur internationalen Schutzkennzeichnung, d. h. sie sind sowohl staubdicht (sodass kein Staub in das Gehäuse gelangt, wenn sie versiegelt sind) als auch wasserdicht (einschließlich Schutz vor allseitigem Strahlwasser).

Die Geräte haben einen weiten Betriebstemperaturbereich von Gefriertemperaturen (0 Grad C oder 32 Grad F) bis hin zu wüstenähnlichen Bedingungen (Snowcone: 38 Grad C oder 100 Grad F; Snowcone SSD: 45 Grad C oder 113 Grad F). Bei Lagerung oder Versand halten Snowcone-Geräte noch härteren Temperaturen stand (-32 Grad C oder -25,6 Grad F bis 63 Grad C oder 145,4 Grad F).

# AWS Snowcone Stromversorgung und Zubehör

AWS Snowcone Geräte enthalten weder ein Netzteil noch ein Ethernet-Kabel (RJ45), da sie mit dem kleinstmöglichen Formfaktor geliefert werden. Sie haben die Möglichkeit, Ihr Snowcone-Gerät über eine Plug-in-Stromquelle oder eine Batterie zu betreiben. Hier sind die Informationen, die Ihnen bei der Bestellung eines Netzteils und eines Ethernet-Kabels als Leitfaden dienen sollen:

**USB-C-Netzteil** — Verwenden Sie zusammen mit dem Snowcone-Gerät einen USB-C-Netzadapter für die Stromversorgung oder für stationäre (nicht mobile) Betriebsumgebungen. Um Ihr Snowcone-Gerät mit Strom zu versorgen, können Sie einen der folgenden AWS getesteten USB-C-Netzadapter erwerben:

- [Apple 61-W-USB-C-Netzadapter](#)
- [Lenovo USB-C 65-W-Standard-Netzadapter](#)

Sie können auch jeden USB-C-Netzadapter verwenden, der für 45 W+ und Ihre Umgebungstemperatur ausgelegt ist.

**USB-C-Batterie** — Verwenden Sie eine USB-C-Batterie, um das Snowcone-Gerät in mobilen oder tragbaren Betriebsumgebungen mit Strom zu versorgen. Um Ihr Snowcone-Gerät mit Strom zu versorgen, können Sie eine [Dell Notebook Power Bank Plus — USB C, 65 Wh — PW7018LC](#) oder einen beliebigen USB-C-Akku verwenden, der für mindestens 45 W ausgelegt ist.

**Ethernet-Kabel (RJ45)** — Verwenden Sie ein Ethernet-Kabel (RJ45), um das Snowcone-Gerät mit Ihrem lokalen Netzwerk zu verbinden. Wenn Sie keins haben, sollten Sie eines kaufen.

## Festplatten- und CPU-Leistung

AWS Snowcone ist ein speziell entwickeltes Edge-Compute-/Datenübertragungsgerät. Die Festplatten- und CPU-Leistung hängt von einer Vielzahl von Faktoren ab. Einige Beispiel-Leistungszahlen für die Übertragung befinden sich in [Snowcone Performance](#)



# Einrichtung AWS für AWS Snowcone

Bevor Sie Ihren ersten AWS Snowcone Job erstellen, befolgen Sie diese Anweisungen, um sicherzustellen, dass Sie Ihre Umgebung angemessen vorbereiten.

Themen

- [Melden Sie sich an für AWS](#)

## Melden Sie sich an für AWS

Wenn Sie sich für Amazon Web Services (AWS) registrieren, wird Ihr Konto automatisch für alle AWS Dienste registriert. AWS berechnet Ihnen nur die Dienste, die Sie nutzen. Nachdem Sie Ihr Konto eingerichtet haben, können Sie Ihr AWS Snowcone Gerät über den bestellen, konfigurieren und verwalten Managementkonsole für die AWS Snow-Familie. Weitere Informationen zu Preisen und Gebühren für Snowcone finden Sie unter [AWS Snowcone Preise](#).

Wenn Sie bereits eine haben AWS-Konto, notieren Sie sich Ihre AWS-Konto Nummer. Wenn Sie noch keine haben AWS-Konto, gehen Sie wie folgt vor:

Um eine zu erstellen AWS-Konto

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

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

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

Notieren Sie sich Ihre AWS-Konto Nummer, die Sie für den nächsten Schritt benötigen.

# Bevor Sie ein Snowcone-Gerät bestellen

AWS Snowcone ist ein regionsspezifischer Service. Stellen Sie daher sicher, dass der Service in Ihrer Region verfügbar ist, bevor Sie den Job planen. Stellen Sie sicher, dass sich Ihr Standort und Ihr Amazon S3 S3-Bucket innerhalb desselben Bereichs befinden, AWS-Region da dies Ihre Möglichkeit beeinträchtigt, das Gerät zu bestellen. Es gibt Einschränkungen beim Versand des Snowcone-Geräts außerhalb der Landesgrenzen einer Region. Weitere Informationen finden Sie unter [Versandeinschränkungen nach Regionen](#).

Internationale Lieferungen an Standorte außerhalb Ihres Landes AWS-Region werden Managementkonsole für die AWS Snow-Familie für Kunden auf der Zulassungsliste für ausgewählte Standorte in bestimmten Regionen (z. B. USA nach Mexiko) unterstützt. Sie sollten das Zielziel, die Kosten und den Zeitplan für die Bearbeitung dieser Anfragen mit Ihrem Account-Team besprechen.

Im Rahmen des Bestellvorgangs erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle und einen AWS Key Management Service (AWS KMS) -Schlüssel. Das KMS schützt die Verschlüsselungsschlüssel, die zum Schutz der Daten auf jedem Gerät verwendet werden. Weitere Informationen finden Sie unter [Einen Auftrag zur Bestellung eines Snow Family-Geräts](#) erstellen.

## Themen

- [Fragen zur lokalen Umgebung](#)
- [Arbeiten mit Dateien mit Sonderzeichen](#)
- [Amazon EC2 auf Snowcone verwenden](#)

## Fragen zur lokalen Umgebung

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

Wird während der Übertragung auf die Daten zugegriffen?

Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie ein Snowcone-Gerät nicht vom Computer und ändern Sie nicht dessen Netzwerkeinstellungen, während Sie Daten übertragen. Dateien müssen beim Schreiben auf das Gerät in statischem Zustand sein. Dateien, die während des Schreibens auf das Gerät geändert werden, können zu Lese-/Schreibkonflikten führen.

## Arbeiten mit Dateien mit Sonderzeichen

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

- Umgekehrter Schrägstrich ("`\`")
- Linke geschweifte Klammer ("`{`")
- Rechte geschweifte Klammer ("`}`")
- Linke eckige Klammer ("`[`")
- Rechte eckige Klammer ("`]`")
- Das Symbol „Weniger als“ ("`<`")
- Symbol „Weniger als“ ("`,`")
- Nicht darstellbare ASCII-Zeichen (128-255 Dezimalzeichen)
- Caret ("`^`")
- Prozentzeichen ("`%`")
- Accent Grave ("```")
- Anführungszeichen
- Tilde ("`~`")
- Pfundzeichen ("`#`")
- Vertikaler Strich ("`|`")

Wenn Ihre Dateien eines oder mehrere dieser Zeichen enthalten, benennen Sie sie um, bevor Sie sie auf das AWS Snowcone Gerät kopieren. Windows-Benutzer, deren Dateinamen Leerzeichen enthalten, sollten vorsichtig sein, wenn sie einzelne Objekte kopieren oder einen rekursiven Befehl ausführen. Umgeben Sie einzelne Objekte, deren Name Leerzeichen enthält, mit Anführungszeichen. Im Folgenden finden Sie Beispiele für solche Dateien.

Betriebssystem	Name der Datei: <b>test file.txt</b>
Windows	<code>„C:\Users\&lt;&lt;username&gt;\ desktop\ test file.txt“</code>
Mac	<code>&lt;username&gt;/Benutzer/ /test\ file.txt</code>

Betriebssystem	Name der Datei: <b>test file.txt</b>
Linux	<username>/home/ /test\ file.txt

### Note

Die einzigen Objektmetadaten, die übertragen werden, sind der Objektname und die Objektgröße. AWS DataSync Behält jedoch die Zugriffskontrolllisten (ACLs) bei. Weitere Informationen finden Sie im AWS DataSync Benutzerhandbuch unter [DataSync Umgang mit Metadaten und Spezialdateien](#).

## Amazon EC2 auf Snowcone verwenden

Dieser Abschnitt bietet einen Überblick über die Verwendung von Amazon EC2-kompatiblen Compute-Instances auf einem AWS Snowcone Gerät.

Sie sollten die Amazon EC2-kompatiblen Instances verwenden, wenn Sie eine Anwendung am Edge ausführen, die als virtuelle Maschine (Amazon Machine Image oder AMI) verwaltet und bereitgestellt wird. Snowcone unterstützt den SNC1-Instance-Typ mit drei Instances, darunter snc1.micro (1 CPU und 1 GB RAM), snc1.small (1 CPU und 2 GB RAM) und snc1.medium (2 CPU und 4 GB RAM). Die Unterstützung für EC2-kompatible Instances auf Snowcone ermöglicht es Ihnen, Ihre Anwendung auf Amazon EC2 zu erstellen und zu testen. Sie können EC2-kompatible AMIs während der AWS Snowcone Auftragserstellung entweder mit dem SDK oder aktivieren und bereitstellen. AWS Management Console AWS Snowball AWS CLI

### Unterstützte Amazon-EC2-Instance-Typen

Verwenden Sie die folgenden Amazon EC2 EC2-Instance-Typen für Ihre Rechenjobs.

snc1.micro — 1 CPU-Kern, 1 GB RAM

snc1.small — 1 CPU-Kern, 2 GB RAM

snc1.medium — 2 CPU-Kerne, 4 GB RAM

Verwenden Sie es AWS OpsHub , um Ihre Instanzen auf Snowcone zu verwalten. Laden Sie es AWS OpsHub von der [AWS Snowball Ressourcen-Website](#) herunter. Nachdem Sie das Gerät mit entsperrt haben AWS OpsHub, navigieren Sie zur Amazon EC2-Seite. Wählen Sie Create instance, um eine

EC2-kompatible Instance zu erstellen, die auf dem AMI basiert, das Sie bei der Erstellung des Jobs auf das Gerät vorinstalliert hatten. Anschließend können Sie eine Verbindung zu den Instances herstellen und Ihre Edge-Anwendung ausführen. AWS OpsHub bietet außerdem Schaltflächen zum Starten, Stoppen, Beenden und Neustarten Ihrer EC2-kompatiblen Instances mit nur einem Klick. Weitere Informationen finden Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

Wenn Sie mit Ihrem Gerät fertig sind, geben Sie es an zurück. AWS Wenn das Gerät in einem Importauftrag verwendet wurde, werden die über die Dateischnittstelle übertragenen Daten mithilfe der Snowcone NFS-Schnittstelle in Amazon S3 importiert. Andernfalls löschen wir das Gerät vollständig, wenn es zurückgegeben wird. AWS Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

#### Important

Daten in Compute-Instances, die auf einem Snowcone laufen, werden nicht importiert AWS.

## Unterschied zwischen Amazon EC2- und Amazon EC2-kompatiblen Instances auf Geräten der Snow Family

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

## Preise für Compute-Instances auf Snowcone

Die Verwendung von Datenverarbeitungs-Instances verursacht zusätzliche Kosten. Weitere Informationen finden Sie unter [AWS Snowcone Preise](#).

## Voraussetzungen

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

- Bevor Sie Ihrem Job AMIs hinzufügen können, müssen Sie über ein AMI verfügen AWS-Konto und es muss sich um einen unterstützten Image-Typ handeln. Derzeit basieren die unterstützten AMIs auf den Images [Amazon Linux 2](#), [CentOS 7 \(x86\\_64\) — mit Updates HVM](#) oder [Ubuntu 16.04 LTS — Xenial \(HVM\)](#). Sie erhalten diese Images über das [AWS Marketplace](#).

Bevor Sie Ihrer Jobanfrage AMIs hinzufügen, stellen Sie sicher, dass Sie mindestens ein unterstütztes AMIs in Ihrer haben. AWS-Konto Wenn Sie ein AMI aus dem Marketplace auswählen, stellen Sie sicher, dass es über einen unterstützten Produktcode und eine unterstützte Plattform verfügt. Weitere Informationen finden Sie unter [Überprüfung der Produktcodes und Plattfordetails von AMIs AWS Marketplace](#).

- Alle AMIs müssen auf Amazon Elastic Block Store (Amazon EBS) mit einem einzigen Volume basieren.
- Wenn Sie eine Verbindung zu einer Compute-Instance herstellen, die auf einem Snowcone läuft, müssen Sie Secure Shell (SSH) verwenden. Hierzu müssen Sie zunächst das Schlüsselpaar hinzufügen.

## Überprüfung der Produktcodes und Plattfordetails von AMIs AWS Marketplace

Bevor Sie mit dem Hinzufügen eines AMI AWS Marketplace zu Ihrem Snow Family-Gerät beginnen, stellen Sie sicher, dass der Produktcode und die Plattfordetails 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 von der aus Sie den Auftrag zur Bestellung des Snow Family-Geräts erstellen. Sie können jede 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 zum Beispiel für AMIs AWS Marketplace, die von bereitgestellt werden, Öffentliche Images aus. Verwenden Sie dann die Suchoptionen, um die Liste der angezeigten AMIs weiter einzugrenzen:
  - (Neue Konsole) Wählen Sie in der Suchleiste aus dem Menü die Option Owner-Alias, dann den Operator = und anschließend den Wert amazon aus.
  - (Alte Konsole) Wählen Sie die Search bar (Suchleiste) aus und anschließend im Menü den Punkt Owner (Besitzer). Wählen Sie dann den Wert Amazon Images (Amazon-Images) aus.

**Note**

AMIs 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 Bildübersicht des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der Tabelle unten.

#### Unterstützte AWS Marketplace AMI-Produktcodes

AMI-Betriebssystem	Produktcode
Ubuntu Server 14.04 LTS	b3dl4415quatdnd14qa6kcu45
CentOS 7 (x86_64)	aw0evgkw8e5c1q413zgy5pjce
Ubuntu 16.04 LTS	csv6h7oyg29b7epjzg7qdr7no
Amazon Linux 2	avyfzznywektkgl5qv5f57ska
Ubuntu 20.04 LTS	a8jyyfnf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkj189a13aqe

7. Stellen Sie anschließend sicher, dass die Plattformdetails einen der Einträge aus der folgenden Liste enthalten.
  - Amazon Linux, Ubuntu oder Debian
  - Red Hat Linux bring-your-own-license
  - Amazon RDS for Oracle bring-your-own-license
  - Windows bring-your-own-license

## Ein Linux-AMI aus einer Instance erstellen

Sie können ein AMI über die Konsole oder die 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 und konfigurieren Sie es vor dem Start nach Bedarf. Weitere Informationen finden Sie unter [Starten einer Instance mit dem Launch Instance Wizard](#).
2. Wählen Sie Launch (Starten), um eine Instance des EBS-gestützten AMI zu starten, das Sie gewählt haben. 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 von Software und Anwendungen
  - Kopieren von Daten
  - Reduzieren der Startdauer durch das Löschen temporärer Dateien, Defragmentieren Ihrer Festplatte und Bereitstellen von freiem Speicherplatz
  - Zusätzliche Amazon EBS-Volumes anhängen
4. (Optional) Erstellen Sie Snapshots von allen Volumes, die an Ihre Instance angefügt sind. Weitere Informationen zum Erstellen von Snapshots finden Sie unter [Amazon EBS-Snapshots erstellen](#).
5. Klicken Sie im Navigationsbereich auf Instances und wählen Sie Ihre Instance aus. Wählen Sie für Aktionen die Optionen Image, Create Image

 Tip

Wenn diese Option deaktiviert ist, handelt es sich bei Ihrer Instance nicht um eine Amazon EBS-gestützte Instance.

6. Geben Sie im Dialogfeld Create Image (Abbild erstellen) die folgenden Informationen an und wählen Sie anschließend Create Image (Abbild erstellen).
  - Bildname — Ein eindeutiger Name für das Bild.
  - 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 Kein Neustart, um zu verhindern, dass Ihre Instance heruntergefahren wird.



**⚠ Warning**

Wenn Sie No reboot (Kein Neustart) wählen, können wir die Dateisystemintegrität des erstellten Abbilds nicht garantieren.

- Instance-Volumes — Mit den Feldern in diesem Abschnitt können Sie das Root-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. Nachfolgend sind einige wichtige Punkte 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 Kündigung löschen auswählen und die mit diesem AMI erstellte Instance beenden, wird das Amazon EBS-Volume gelöscht. Wenn Sie beim Beenden der Instance die Option Bei Kündigung löschen deaktivieren, wird das Amazon EBS-Volume nicht gelöscht. Weitere Informationen finden Sie unter [Beibehalten von Amazon EBS-Volumes bei der Beendigung einer Instance](#) im Amazon EC2-Benutzerhandbuch.
  - Um ein Amazon EBS-Volume hinzuzufügen, wählen Sie Add New Volume (wodurch eine neue Zeile hinzugefügt wird). 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](#). Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden zusätzliche Volumes automatisch initialisiert und gemountet. Diese Volumes enthalten keine Daten aus den Instance-Speicher-Volumes der ausgeführten Instance, auf der Ihr AMI basiert.
- 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 auf 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](#).
9. Die neue ausgeführte Instance enthält alle Anpassungen, die Sie in den letzten Schritten vorgenommen haben.

## So erstellen Sie mithilfe der Befehlszeile ein AMI aus einer Instance

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen finden Sie unter [Accessing Amazon EC2](#).

- [create-image](#) (AWS CLI)
- [New-EC2Image](#) (AWS Tools for Windows PowerShell)

## Ein Linux-AMI aus einem Snapshot erstellen

Wenn Sie über einen Snapshot des Root-Geräte-Volumes einer Instance verfügen, können Sie mit der AWS Management Console oder der Befehlszeile aus diesem Snapshot 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 und dann Actions (Aktionen) und Create Image (Image erstellen) aus.
4. Füllen Sie im Dialogfeld Create Image from EBS Snapshot die Felder aus, um Ihr AMI zu erstellen, und wählen Sie dann Create aus. Wenn Sie eine übergeordnete Instance neu erstellen, wählen Sie dieselben Optionen wie für die übergeordnete Instance.
  - Architecture: Wählen Sie i386 für "32 Bit" oder x86\_64 für "64 Bit" aus.
  - Root device name: Geben Sie den richtigen Namen für das Stamm-Volumen ein. Weitere Informationen finden Sie unter [Gerätebenennung auf Linux-Instances](#).
  - Virtualization type (Virtualisierungstyp): Geben Sie an, ob für Instances, die über dieses AMI gestartet werden, die PV-Virtualisierung (Paravirtual) oder HVM-Virtualisierung (Hardware Virtual Machine) verwendet wird. Weitere Informationen finden Sie unter [Linux-AMI-Virtualisierungstypen](#).
  - (Nur PV-Virtualisierung) Kernel ID und RAM disk ID: Wählen Sie in den Listen die AKI- und ARI-Werte aus. Wenn Sie den AKI-Standardwert oder keinen AKI-Wert auswählen, müssen

Sie bei jedem Start einer Instance mithilfe dieses AMI einen AKI-Wert angeben. Darüber hinaus kann es sein, dass Ihre Instance die Integritätsprüfungen nicht besteht, wenn die Standard-AKI nicht mit der Instance kompatibel ist.

- (Optional) Block Device Mappings (Blockgerät-Zuweisung): Fügen Sie Volumes hinzu oder erweitern Sie die Standardgröße des Stamm-Volumes für das AMI. Weitere Informationen zur Größenänderung des Dateisystems auf Ihrer Instance für ein größeres Volume finden Sie unter [Erweitern eines Linux-Dateisystems nach der Größenänderung eines Volumes](#).

So erstellen Sie mithilfe der Befehlszeile ein AMI aus einem Snapshot

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen finden Sie unter [Accessing Amazon EC2](#).

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

# Erste Schritte

Dieser Abschnitt enthält allgemeine Anweisungen zum Erstellen und Abschließen Ihres ersten AWS Snowcone Jobs in der Managementkonsole für die AWS Snow-Familie. Eine Übersicht über das AWS Snowcone Gerät finden Sie unter [Wie AWS Snowcone funktioniert](#).

In dieser Dokumentation für die ersten Schritte wird davon ausgegangen, dass Sie den verwenden, [Managementkonsole für die AWS Snow-Familie](#) um Ihren Job zu erstellen, und dass Sie den Snowball Edge-Client oder die AWS OpsHub for Snow Family Anwendung verwenden, um das AWS Snowcone Gerät zu entsperren. 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 Snowcone -API-Referenz](#).

Bevor Sie beginnen können, müssen Sie in AWS Identity and Access Management (IAM) einen Administratorbenutzer AWS-Konto und einen Administratorbenutzer erstellen. Weitere Informationen finden Sie unter [Einrichtung AWS für AWS Snowcone](#).

Informationen zu den ersten Schritten AWS Snowcone finden Sie unter [Einen Auftrag zur Bestellung eines Snow Family-Geräts](#) erstellen.

## Themen

- [Einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen](#)
- [Stornieren eines Jobs über den Managementkonsole für die AWS Snow-Familie](#)
- [Zugangsdaten für den Zugriff auf ein Snow Family-Gerät abrufen](#)
- [Entsperren des Snow Family-Geräts](#)
- [Das Snow Family-Gerät neu starten](#)

## Einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen

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

Datenverarbeitung und Speicherung. Weitere Informationen finden Sie unter [Grundlegendes zu AWS Snowball Edge-Jobs](#).

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

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

## Themen

- [Schritt 1: Wählen Sie einen Jobtyp](#)
- [Schritt 2: Wählen Sie Ihre Rechen- und Speicheroptionen](#)
- [Schritt 3: Wählen Sie Ihre Funktionen und Optionen](#)
- [Schritt 4: Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen](#)
- [Schritt 5: Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job](#)
- [Herunterladen AWS OpsHub](#)

## Schritt 1: Wählen Sie einen Jobtyp

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

Um Ihren Jobtyp auszuwählen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#). Wenn Sie hier zum ersten Mal einen Job erstellen AWS-Region, wird die AWS Snow Family-Seite angezeigt. Andernfalls wird die Liste der vorhandenen Jobs angezeigt.
2. Wenn dies Ihr erster Job ist, wählen Sie Ein AWS Snow Family-Gerät bestellen. Wenn Sie davon ausgehen, dass mehrere Jobs mehr als 500 TB an Daten migrieren, wählen Sie Create your large data migration plan more than 500 TB. Andernfalls wählen Sie in der linken

Navigationsleiste Job erstellen. Wählen Sie „Nächster Schritt“, um die Seite „Job planen“ zu öffnen.

3. Geben Sie im Abschnitt Jobname im Feld Jobname einen Namen für Ihren Job ein.
4. Wählen Sie je nach Bedarf einen der folgenden Jobtypen aus:
  - In Amazon S3 importieren — Lassen Sie sich AWS ein leeres Snowcone-Gerät zusenden. Sie verbinden das Gerät mit Ihrem lokalen Netzwerk und konfigurieren das Gerät mithilfe von OpsHub. Sie kopieren Daten mit NFS Share auf das Gerät, senden sie zurück an AWS und Ihre Daten werden auf Amazon S3 hochgeladen.
  - Nur lokale Datenverarbeitung und Speicherung — Führen Sie Rechen- und Speicher-Workloads auf dem Gerät aus, ohne Daten zu übertragen.

**Choose a job type**

- Import into Amazon S3** [Info](#)  
AWS will ship an empty device to you for storage and compute workloads. You'll transfer your data onto it, and ship it back. After AWS gets it, your data will be moved.
- Export from Amazon S3** [Info](#)  
Choose what data you want to export from your S3 buckets for storage and compute workloads. AWS will load that data onto a device and ship it to you. When you're done ship the device back for erasing.
- Local compute and storage only** [Info](#)  
Perform local compute and storage workloads without transferring data. You can order multiple devices in a cluster for increased durability and storage capacity. Includes rugged and rack-mountable devices.

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

## Schritt 2: Wählen Sie Ihre Rechen- und Speicheroptionen

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

Um die Rechen- und Speicheroptionen Ihres Geräts auszuwählen

1. Wählen Sie im Bereich Snow-Geräte das Snow Family-Gerät aus, das Sie bestellen möchten.

**Note**

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

Snow devices <small>Info</small>					
	Name	Compute	Memory	Storage (HDD)	Storage (SSD)
<input checked="" type="radio"/>	Snowcone	2 vCPUs	4 GB	8 TB	-
<input type="radio"/>	Snowcone SSD	2 vCPUs	4 GB	-	14 TB
<input type="radio"/>	Snowball Edge Compute Optimized	52 vCPUs	208 GB	39.5 TB	7.68 TB
<input type="radio"/>	Snowball Edge Compute Optimized with GPU	52 vCPUs, GPU	208 GB	39.5 TB	7.68 TB
<input type="radio"/>	Snowball Edge Compute Optimized	104 vCPUs	416 GB	-	28 TB

- Wählen Sie im Bereich Snowcone-Stromversorgung die Option Ich stelle mein eigenes Netzteil und mein eigenes Ethernet-Kabel bereit. Informationen zu Netzteilen finden Sie unter [AWS Snowcone Stromversorgung und Zubehör](#).
- Wählen Sie im Abschnitt Wählen Sie Ihre Preisoption im Menü Wählen Sie Ihre Preisoption aus, welche Preisgestaltung für diesen Job gelten soll. Die Preise für Geräte finden Sie unter [AWS Snowcone Preise](#).
- Treffen Sie im Abschnitt Speichertyp auswählen eine Auswahl, die Ihren Anforderungen entspricht:
  - NFS-basierte Datenübertragung: Verwenden Sie die auf dem Network File System (NFS) basierende Datenübertragung, um Dateien per Drag-and-Drop von Ihrem Computer in Amazon S3 S3-Buckets auf Snow Family-Geräten zu ziehen.

**Warning**

Die NFS-basierte Datenübertragung unterstützt den S3-Adapter nicht. Wenn Sie mit der NFS-basierten Datenübertragung fortfahren, müssen Sie die NFS-Freigabe bereitstellen,

um Objekte zu übertragen. Die Verwendung von AWS CLI zum Übertragen von Objekten schlägt fehl.


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

5. Wenn Sie NFS-basierte Datenübertragung als Speichertyp ausgewählt haben, führen Sie im Abschnitt Wählen Sie Ihre S3-Buckets einen oder mehrere der folgenden Schritte aus, um einen oder mehrere S3-Buckets auszuwählen:
  - a. Wählen Sie den S3-Bucket, den Sie verwenden möchten, in der Liste der S3-Bucket-Namen aus.
  - b. Geben Sie im Feld Nach einem Artikel suchen einen Bucketnamen ganz oder teilweise ein, um die Liste der verfügbaren Buckets nach Ihrem Eintrag zu filtern, und wählen Sie dann den Bucket aus.
  - c. Wählen Sie Neuen S3-Bucket erstellen, um einen neuen S3-Bucket zu erstellen. Der neue Bucket-Name wird in der Liste der Bucket-Namen angezeigt. Wählen Sie diese aus.

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

### Choose your NFS storage

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

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

The NFS storage limit is 80 TB

[Create a new S3 bucket](#)

<input type="checkbox"/>	S3 bucket name	Date created
<input type="checkbox"/>	this-unique-bucket-name	6/14/2023, 12:20:08 PM EDT

6. Wählen Sie im Abschnitt Compute using EC2-compatible Instances — optional Amazon EC2-kompatible AMIs aus Ihrem Konto aus, die auf dem Gerät hinzugefügt werden sollen. Oder geben Sie im 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 in diesem Handbuch unter [Einen Job mit Compute Instances erstellen](#).

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

7. Klicken Sie auf die Schaltfläche Next.

## Schritt 3: Wählen Sie Ihre Funktionen und Optionen

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

Um Ihre Funktionen und Optionen auszuwählen

1. Um Ihr drahtloses Netzwerk auf Ihrem Snowcone-Gerät zu aktivieren, wählen Sie WLAN auf Snowcone aktivieren.
2. Um die Fernverwaltung Ihres Snow Family-Geräts mit AWS OpsHub oder dem Snowball Edge-Client zu aktivieren, wählen Sie Ihr Snow-Gerät remote verwalten mit AWS OpsHub oder Snowball-Client aus.
3. Wählen Sie die Schaltfläche Weiter.

## Schritt 4: Wählen Sie die Einstellungen für Sicherheit, Versand und Benachrichtigungen

Themen

- [Wählen Sie Sicherheitseinstellungen](#)
- [Wählen Sie Ihre Versandpräferenzen](#)
- [Wählen Sie Ihre Benachrichtigungseinstellungen](#)

## Wählen Sie Sicherheitseinstellungen

Durch das Einstellen der Sicherheitseinstellungen werden die Berechtigungen und Verschlüsselungseinstellungen für Ihre AWS Snow Family-Geräte hinzugefügt, um Ihre Daten während der Übertragung zu schützen.

Um die Sicherheit für Ihren Job festzulegen

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


## Wählen Sie Ihre Versandpräferenzen

Der Empfang und die Rücksendung eines Snow Family-Geräts beinhaltet den Hin- und Rückversand des Geräts. Daher ist es wichtig, dass Sie genaue Versandinformationen angeben.

Um Versandinformationen bereitzustellen

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

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

 Note

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

2. Wählen Sie im Abschnitt Versandgeschwindigkeit eine Versandgeschwindigkeit für den Auftrag aus. Diese Geschwindigkeit gibt an, wie schnell das Gerät zwischen Zielen versendet wird, und gibt nicht an, wie schnell es nach dem heutigen Datum ankommen wird. Die Versandgeschwindigkeiten, die Sie wählen können, sind:
  - Versand innerhalb eines Tages (1 Werktag)
  - Zweitägiger Versand (2 Arbeitstage)
  - Siehe [Spediteure](#).

## Wählen Sie Ihre Benachrichtigungseinstellungen

Benachrichtigungen informieren Sie über den aktuellen Status der Jobs auf Ihren AWS Snow Family-Geräten. Sie erstellen ein SNS-Thema und erhalten E-Mails von Amazon Simple Notification Service (Amazon SNS), wenn sich Ihr Jobstatus ändert.

Richten Sie Benachrichtigungen wie folgt ein

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

**Note**

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

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

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

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


Wählen Sie „Weiter“.

## Schritt 5: Überprüfen Sie die Jobübersicht und erstellen Sie Ihren Job


Nachdem Sie alle erforderlichen Informationen für Ihren AWS Snow Family-Geräteauftrag eingegeben haben, überprüfen Sie den Job und erstellen Sie ihn. Nachdem Sie den Auftrag erstellt haben, AWS wird mit der Vorbereitung des Snow Family-Geräts für den Versand an Sie begonnen.

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

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

 Note

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

 Note

Snowcone-Geräte sind nicht mit Netzkabeln ausgestattet, und eines muss separat geliefert werden. Weitere Informationen finden Sie unter [AWS Snowcone Stromversorgung](#) und Zubehör.

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

## Herunterladen AWS OpsHub

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

Wenn es 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 Instanzen, die auf Geräten der Snow Family ausgeführt werden.

Weitere Informationen finden Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

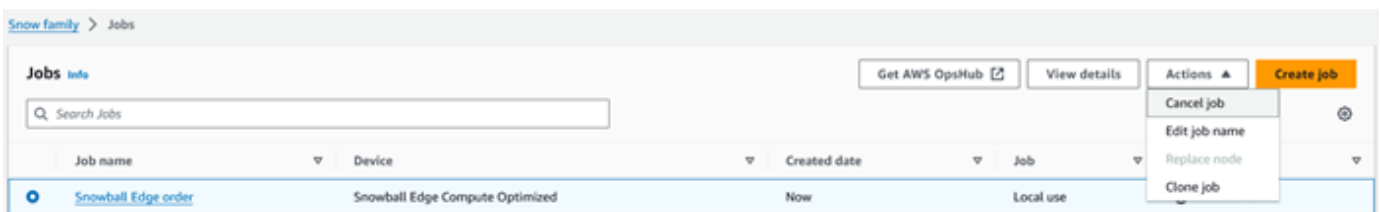
Zum Herunterladen und Installieren AWS OpsHub for Snow Family

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 für die Installation AWS OpsHub für Ihr Betriebssystem aus.
2. Wählen Sie im AWS OpsHub Abschnitt Herunterladen für Ihr Betriebssystem aus und folgen Sie den Installationsschritten. Wählen Sie danach Next aus.

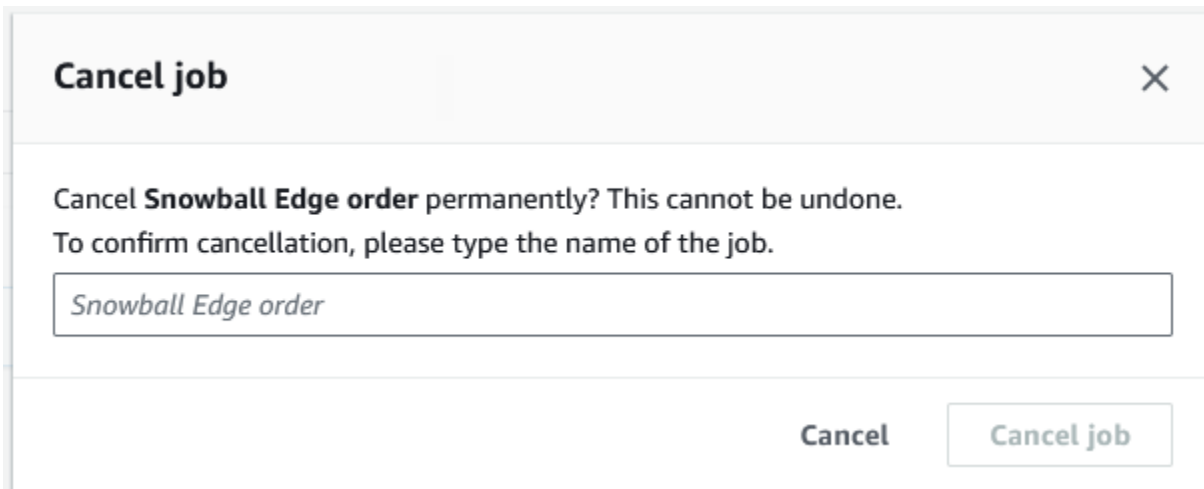
## Stornieren eines Jobs über den Managementkonsole für die AWS Snow-Familie

Nachdem Sie einen Auftrag zur Bestellung eines Snow Family-Geräts erstellt haben, können Sie den Auftrag über den stornieren Managementkonsole für die AWS Snow-Familie. Wenn Sie den Auftrag stornieren, erhalten Sie das bestellte Gerät nicht. Sie können den Job nur stornieren, solange der Jobstatus Job created lautet. Sobald der Job diesen Status überschritten hat, können Sie ihn nicht mehr stornieren. Weitere Informationen finden Sie unter [Jobstatus](#).

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



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



## Zugangsdaten für den Zugriff auf ein Snow Family-Gerät abrufen

Jeder Job hat eine Reihe von Anmeldeinformationen, die Sie von der Managementkonsole für die AWS Snow-Familie oder der Job-Management-API abrufen müssen, um Ihren Zugriff auf 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 Jobs in der Managementkonsole für die AWS Snow-Familie sehen. Weitere Informationen finden Sie unter [Grundlegendes zum AWS Snowcone Jobstatus](#).

Um Ihre Anmeldeinformationen über die Konsole abzurufen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#).
2. Suchen Sie auf der Konsole in der Tabelle nach dem spezifischen Job, für den Sie das Auftragsmanifest herunterladen möchten, und wählen Sie dann diesen Job aus.
3. Erweitern Sie den Bereich Jobstatus und wählen Sie Jobdetails anzeigen aus.
4. Erweitern Sie im angezeigten Detailbereich die Option Credentials (Anmeldeinformationen) und führen Sie dann die folgenden Schritte aus:

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

#### Note

Es wird empfohlen, keine Kopie des Entsperrcodes an derselben Stelle auf dem Computer zu speichern wie das Manifest für diesen Job. Weitere Informationen finden Sie unter [Bewährte Methoden für das AWS Snowcone Gerät](#).

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

Weiter: [Den AWS Snowball Edge Client verwenden](#)

## 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 mithilfe AWS OpsHub einer grafischen Benutzeroberfläche (GUI) für Snow Family-Geräte finden Sie unter Gerät [entsperren](#).

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

Bevor Sie ein Gerät entsperren, muss das Gerät an die Stromversorgung und das Netzwerk angeschlossen, eingeschaltet und eine IP-Adresse zugewiesen werden. Siehe [AWS Snowcone-Gerätespezifikationen](#). 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 [Den AWS Snowball Edge Client verwenden](#).



- Holen Sie sich die Anmeldeinformationen von der Managementkonsole für die AWS Snow-Familie. Bei einem oder mehreren eigenständigen Geräten die Entsperrcodes und die Manifestdatei für jedes Snow Family-Gerät. Weitere Informationen zum Herunterladen von Anmeldeinformationen finden Sie unter [Zugangsdaten für den Zugriff auf ein Snow Family-Gerät abrufen](#).
- Schalten Sie jedes Gerät ein und verbinden Sie es mit Ihrem Netzwerk. Weitere Informationen finden Sie unter [AWS Snowcone Technische Daten des Geräts](#).

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

1. Suchen Sie die IP-Adresse für den Snowcone auf dem LCD-Display des Geräts. 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 gibt mit der folgenden Meldung an, dass es erfolgreich entsperrt wurde.

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

Wenn der Befehl `zurückkehrtconnection refused`, finden Sie weitere Informationen unter [Problembehandlung beim Entsperrn eines Snow Family-Geräts](#).

Example des **unlock-device** Befehls

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

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

## Problembehandlung beim Entsperrren eines Snow Family-Geräts

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

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.
  - a. Überprüfen Sie anhand des LCD-Bildschirms des Geräts, ob die im Befehl verwendete IP-Adresse korrekt ist.
  - b. Stellen Sie sicher, dass der Pfad zur im Befehl verwendeten Manifestdatei korrekt ist, einschließlich des Dateinamens.
  - c. Verwenden Sie den [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 möglich ist. Ermitteln Sie anhand des `ping` Befehls für Ihr Betriebssystem, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen der Antivirensoftware, der Firewall-Konfiguration, des virtuellen privaten Netzwerks (VPN) oder anderer Konfigurationen Ihres Computers und Netzwerks.

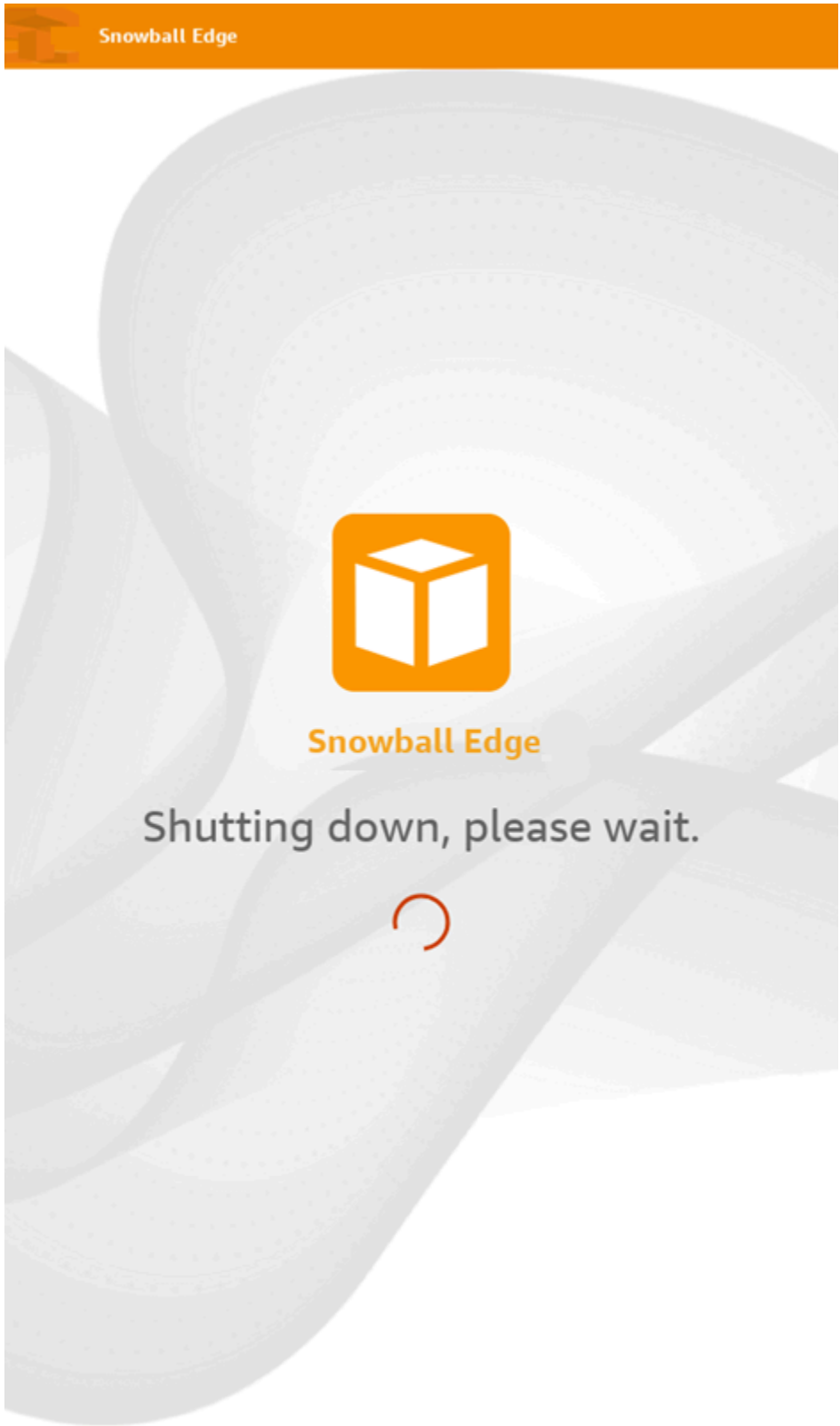
Jetzt können Sie mit der Verwendung des Snow Family-Geräts beginnen.


## Das Snow Family-Gerät neu starten

Bevor Sie ein Snow Family-Gerät neu starten, stellen Sie sicher, dass die gesamte Datenübertragung zum Gerät gestoppt wurde. Wenn Sie die NFS-Schnittstelle zum Übertragen von Daten verwendet haben, deaktivieren Sie sie, bevor Sie das Gerät ausschalten. Weitere Informationen finden Sie unter [Stoppen der NFS-Schnittstelle](#).

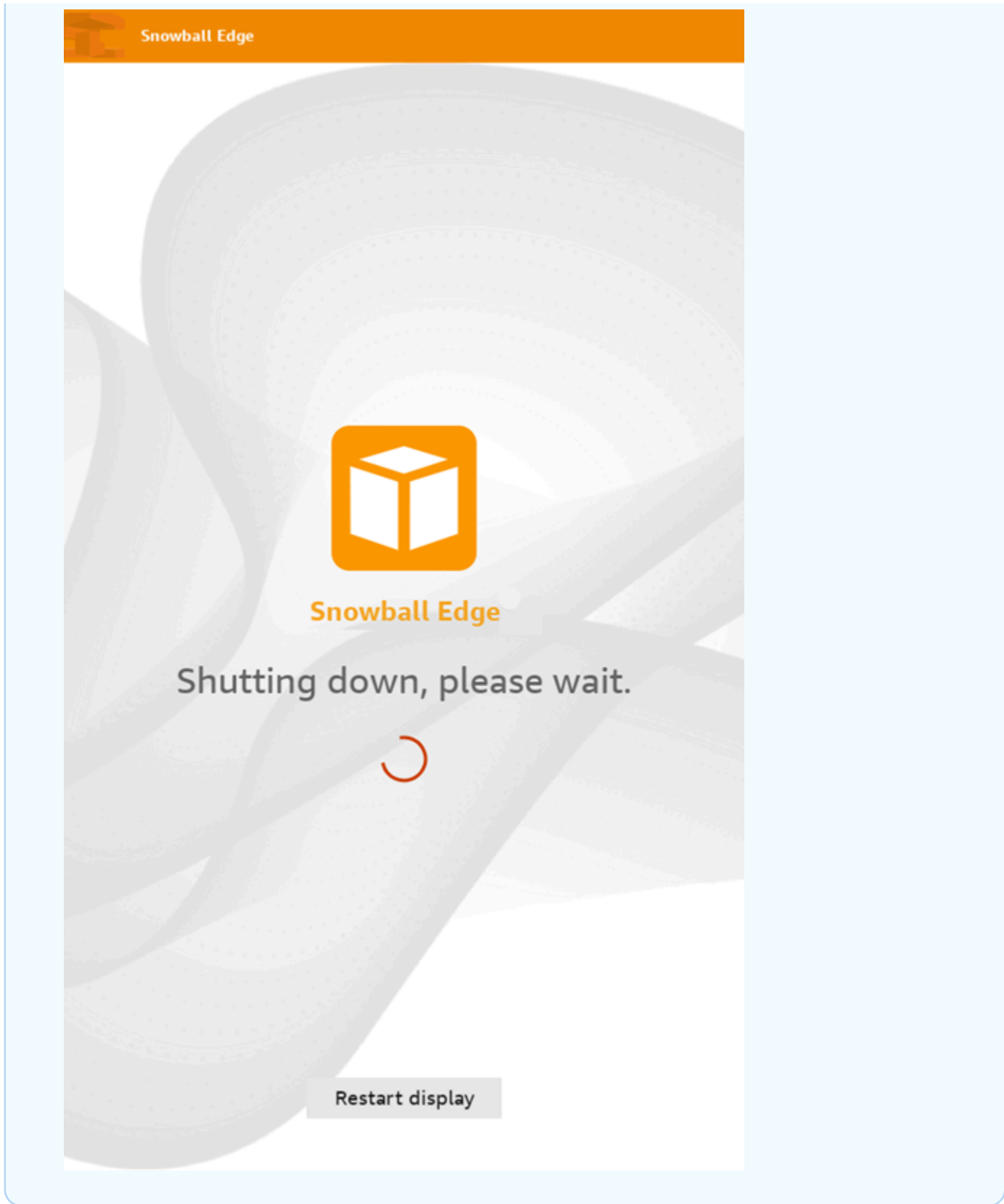
Um das Gerät mit dem Netzschalter neu zu starten:

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



 **Note**

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



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

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

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

```
snowballEdge reboot-device
```

2. Entsperren Sie das Gerät. Siehe [Ein AWS Snowcone Gerät entsperren](#).

# AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden

Die Snow Family-Geräte bieten jetzt ein benutzerfreundliches Tool AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen AWS Dienste verwalten können. Sie verwenden es AWS OpsHub auf einem Client-Computer, um Aufgaben wie das Entsperren und Konfigurieren einzelner oder geclusterter Geräte, das Übertragen von Dateien und das Starten und Verwalten von Instanzen auszuführen, die auf Snow Family-Geräten ausgeführt werden. Sie können AWS OpsHub damit sowohl die Speicheroptimierten als auch die Computeroptimierten Snow-Gerätetypen verwalten. Die AWS OpsHub Anwendung steht Ihnen ohne zusätzliche Kosten zur Verfügung.

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

AWS OpsHub bietet einen einheitlichen Überblick über die AWS Dienste, die auf Snow Family-Geräten ausgeführt werden, und automatisiert betriebliche Aufgaben durch AWS Systems Manager. Damit AWS OpsHub können Benutzer mit unterschiedlichem technischen Fachwissen eine große Anzahl von Snow Family-Geräten verwalten. Mit wenigen Klicks können Sie Geräte entsperren, Dateien übertragen, Amazon EC2-kompatible Instances verwalten und Gerätemetriken überwachen.

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

Nachdem Sie [die AWS OpsHub Anwendung heruntergeladen](#) und auf einem Client-Computer installiert haben, AWS OpsHub kann eine Verbindung zum AWS Snowcone Gerät im selben Netzwerk hergestellt werden, unabhängig davon, ob das Gerät über WLAN oder ein physisches Kabel verbunden ist. Dann öffnen AWS OpsHub und entsperren Sie das Gerät. Anschließend wird ein Dashboard angezeigt, in dem Ihr Gerät und seine Systemmetriken angezeigt werden. Anschließend können Sie mit der Bereitstellung Ihrer Edge-Anwendungen oder der Migration Ihrer



Daten auf das Gerät beginnen. AWS OpsHub macht Datenübertragungen auf Ihr Snowcone-Gerät einfach, indem Sie drag-and-drop Dateien oder Ordner auf dem Gerät speichern können. Mit können Sie auch leicht sehen AWS OpsHub, was auf dem Gerät gespeichert ist.

## Themen

- [AWS OpsHub Für Snow Family-Geräte herunterladen](#)
- [Ein Gerät entsperren](#)
- [Überprüfung der PGP-Signatur von AWS OpsHub \(optional\)](#)
- [AWS Dienste auf Ihrem Gerät verwalten](#)
- [Wird verwendet DataSync , um Dateien zu übertragen AWS](#)
- [Verwaltung Ihrer Geräte](#)
- [Einstellung der NTP-Zeitserver für Ihr Gerät](#)

# AWS OpsHub Für Snow Family-Geräte herunterladen

Zum Herunterladen AWS OpsHub

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

### ← PAGE CONTENT

#### What's New

#### [OpsHub](#)

#### Snowball Edge Client

#### Featured Content

#### Documentation

#### Webinars

#### Videos

#### Blog Posts

#### Free Training

## OpsHub

**OpsHub** is a graphical user interface you can use to manage Snowball devices. OpsHub makes it easy to setup and manage Snowball devices enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. With just a few clicks in OpsHub, you have the full functionality of the Snow Family of devices at your fingertips; you can unlock and configure devices, drag-and-drop data to devices, launch applications, and monitor device metrics.

- [OpsHub documentation](#)

	OpsHub
Windows 7 or higher	<a href="#">Download</a>
Mac OS X 10.10 or higher	<a href="#">Download</a>
Linux (Ubuntu version 14 or higher, and Fedora version 24 or higher)	<a href="#">Download</a>
	<a href="#">(Signature)</a>

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

# Ein Gerät entsperren

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

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

Informationen zur Aktivierung der Fernverwaltung und zum Erstellen eines zugehörigen Kontos finden Sie unter [Snow Device Management aktivieren](#).

## Themen

- [Lokales Entsperren eines Geräts](#)
- [Ein Gerät aus der Ferne entsperren](#)

## Lokales Entsperren eines Geräts

Um Ihr Gerät lokal zu verbinden und zu entsperren

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



## Get started with OpsHub

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

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

**Sign in**

5. Wählen Sie auf der Seite „Auf 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.



## Sign into your Snowball Edge

Sign in with an unlock code and manifest file


Device IP address

*Eg 12.34.45.678*

Unlock code

*7c0e1-bab84-f7675-0a2b6-bfcc3*

Manifest file

 Choose file

No file chosen

Back

Sign in

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

**Note**

Der verfügbare Speicherplatz auf dem Snowcone-Gerät ist erst korrekt, wenn der NFS-Dienst gestartet wird. Siehe [Verwaltung der NFS-Schnittstelle](#).

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

## Ein Gerät aus der Ferne entsperren

Um ein Snow Family-Gerät zu entsperren, nicht

Um Ihr Gerät aus der Ferne zu verbinden und zu entsperren

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

**Note**

Um aus der Ferne entsperren zu werden, muss Ihr Gerät eine Verbindung herstellen *device-order-region*.amazonaws.com können.

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



## Get started with OpsHub

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

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

**Sign in**

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



## Sign into remote devices

Sign in with an access key and secret key

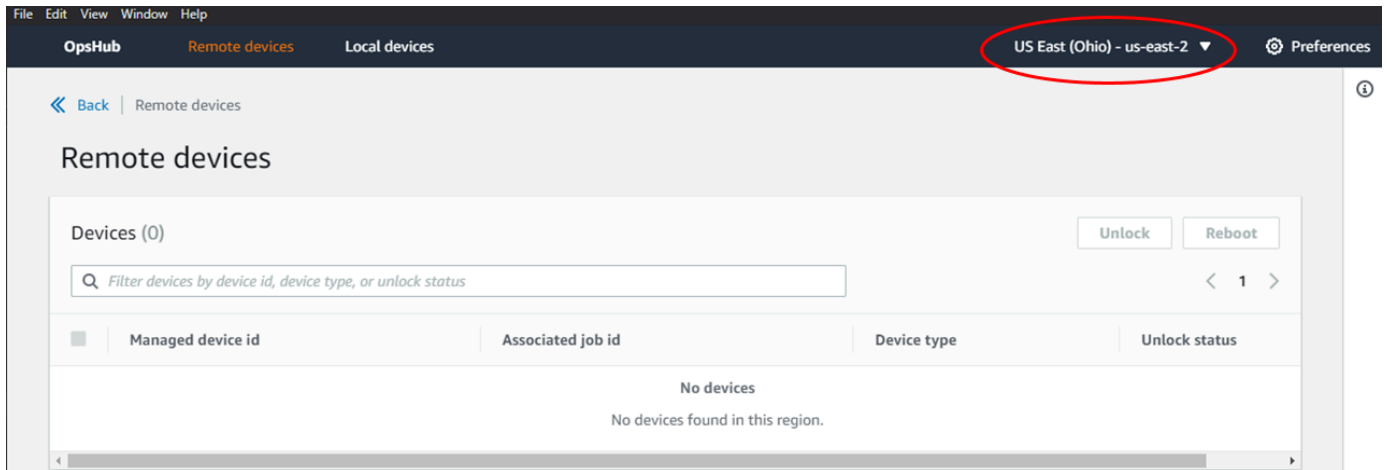
Access key

Secret key

Back

Sign in

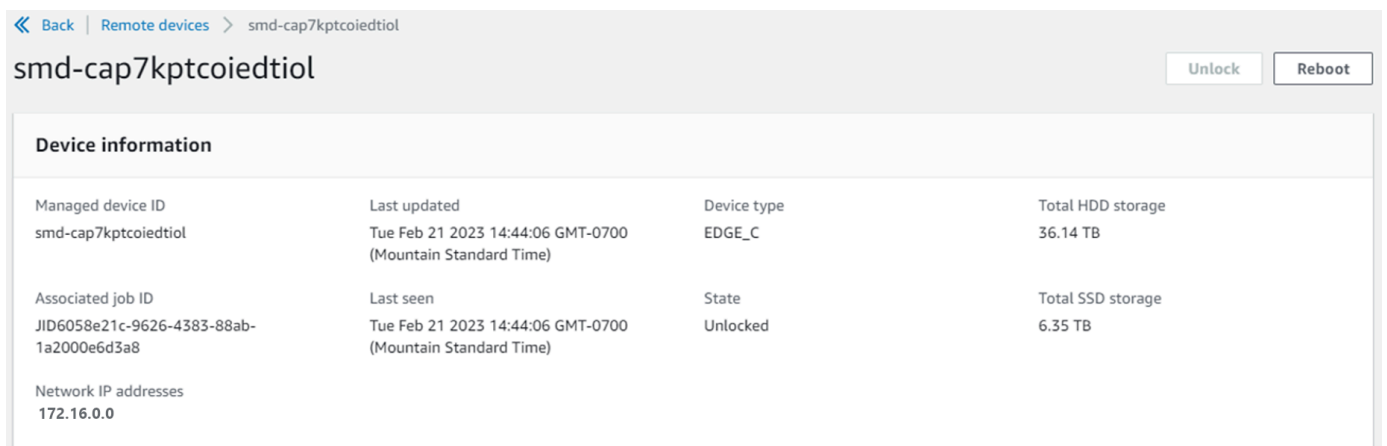
6. Wählen Sie oben auf der Registerkarte „Remote-Geräte“ die Region des Snow-Geräts aus, das per Fernzugriff entsperrt werden soll.



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

#### Note

Der verfügbare Speicherplatz auf dem Snowcone-Gerät ist erst korrekt, wenn der NFS-Dienst gestartet wird. Siehe [Verwaltung der NFS-Schnittstelle](#).



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



## Überprüfung der PGP-Signatur von AWS OpsHub (optional)

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

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

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

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

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBF/hGf8BEAC9HCDV8uljDX02Jxspi6kmPu4xqf4ZZLQsSqJcHU61oL/c
/zAN+mUqJT9aJ1rr0QFGVD1bMogecUPf1TW1DkEEpG8ZbX5P8vR+EE10/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmI07j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZXCi/+u+99YLaugJIP6ZYIeDfpxnghqyVtaappBFTAyfG67Y
N/5mea1VqJzd8liFpIFQn1+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvfTb47bbv9Z28V1284
4lw2w1B107Fo02v/Y0ukrN3VHCpmJQ51IiqZbYRa0DVK6UR5QNvUlJ5fwWs
4qW9UDPHt/HDuaMrMFCEjEn/7wvRUrGVtzCT9F56A1/dwRSxBejQqEb1AC8j
uuyi7gJaPdyNntR0EFTD7i02L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTp0ry/
Wvw0iKZFbo4AkiI0aLyBCK9HBXhUKA9x06g0nhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90w1RBUAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZIenrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQ54NAwARAQABzTlBV1MgT3BzSHVi
IGZvciBTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFA1/hGf8GCwkHCAMCBBUICgIEFgIBAAIZAQIBAwIeAQAh
CRAhgc9adPNF8RYhBDcvpelIaY930b0vqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIaw0SXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmXWwBg
cxg1g0GXNXCM4lAd68CmbA0LoLTaWSQX30ZbswzhbtX2ADAlOpV8RLBik7fm
bS9FYuubDRhfYRQq0fPjUGXFiEgwg6aMFxsrGLlv4QD7t+6ftFIe/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+F0VMMpeEN5JRazEeUr1
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDW0q/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty251o8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4ED119Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEza/2upDJ1m+40HK4p
```

```

8DrEzP/3jTahT8q5ofFWSRDL17d31TSU+JBmPE3mz311FNXgi08w+taY320z
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
07vxM05xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFZvzT/tDi5FiEEi+09
V+UAYN9Gnw36EVm/NP+00LnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvg0tUBxqmC0jr+8AKH00tiBWSu0
lsS8JU5rindEsKURkTwcG2wyZFoe1z1E8xPkLRSRN5ZbbgKsTz16l1HgCCId
Do+WJdDkWGwXmtDvzjm32EI/PVBd108ga9aPwXdhLwOdKAjZ4JrJXLUQJjRI
IVDSyM0bEH0UM6a/+mWNZazNfo0LsGWqGva6Xn5WJWlwr1S78vPNf03BQYu0
YRjaVQR+kPtB9aSAZNi5swfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7Xl03o/VjblneZ0hJK6kAKU172tnPJTJ31Jb0xX73wsMWDYZRZVcK
9X9+GFrpwhKHWKkpjM0t/FRxNepvqR172TkgBPqGH2TM0FdB1f/uQprvqge
PBbS0JrmBIH9/anIqgtMdtcNQB/0erLdCdQI5af0uD10LcLwdJwG9/bSrfwT
TVEE3WbXmJ8pZgmZlHUiZE6V2DSadV/YItk50I0j jrOVH0Hv1FMwGCEAIFzf
9P/pNi8hpEmLRphRi0VVcdQ30bH0M0gPHu5V9f1IhyCL1zU3LjYTHkq0yJD5
YDA1x01MYq3DcSM5130VBbLmuVS2GpcsTCYq1gQA6h/zzMwz+/70wU0EX+EZ
/wEQAOAY8ULmcJIQWIr14V0jy1pJeD3qw7wd+QsBzJ+m0p0B/3ZFAhQiN01
9yCD1HeiZeAmWYX90IXrNiIdcHy+WTAp4G+NaMpqE52qhbDjz+IbvLp11yDH
bYEHpjnthXEy21bvKAJ0Kkw/2RcQ0i4dodGnq5icyYj+9gcuHvnVwbrQ96Ia
0D7c+b5T+bzFqk90nIcztrMRuhDLJnJpi70jpvQwfq/TkkZA+mzupxfSkq/Y
N9qXNEToT/VI2gn/LS0X4Ar1l2KxBjzNESQkwGSiWSYtMA5J+Tj5ED0uZ/qe
omNb1A1D4bm7Na8NAoLxctAiDq/f3To9Xb181Hsnd0mfLCb/BVgP4edQKTii
C/OZHy9QJlfnM0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXM0d3I
e6NUvU7pw0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQqYZe0
jXD3IJ7T+X2XA8M/BmypoMw0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcPxzehwsSVq1lzaL2ureJBL0KkBgYxUJYXpbS01ax1TsFG
09ldAN0s9Ej8CND37GsNnuygj0gWXB6MNgbvPs3H3zi/AbMunQ1VB1w07JX
zdm1hBQZh6w+NeiEsK1T6wHi7IhxABEBAHCwXYEGAEIAAkFA1/hGf8CGwwA
IQkQIYHPWnTzRfEWIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PvBF
ywKvwi3GL01pY7BXn81QaHyunMGUavm080faRR0ynkH0ZqLHCp6bIajF0fvF
b7c0Jamzx8Hg+SIdl6yRpRY+fA4RQ6PNnmT93ZgWW3EbjPyJGlm0/rt03SR
+0yn4/ldlg2KfBX4ppMoPCMKUdWxGrimDETXsGihwZ0gmCZqXe81K122PYkSN
JQQ+LlfjKvCaxfPKEjXYTbIbfyyhCR6NzA0VZxCrzSz2xDrYwP/V002K1xda
0ix6r2aEHf+xYEUh0aBt80HY5nXTuRReCVU789MUVtCMqD2u6amdo4BR0kWA
QNg4yavKwV+LVtyYh2Iju9VSyv4xL1Q4xKHvcAUrSH73bHG7b7jkUJckD0f4
twhjJk/Lfwe6RdnVo2WoeTvE93w+NAq2FXmvbiG7elt10XfQecvQU3QNbrvH
U8B96W0w8UXJdvTKg4f0NbjSw7iJ3x5naixQ+rA8hLV8x0gn2LX6wvxT/SEu
mn20KX+fPtJELK7v/NheFLX1jsKLXYo4jHrkfIXNsNUhg/x2E71kAjbeT3s+
t9kCtxt2iXDDZvpIbmG04QkvLFvoR0aSmN6+8fupe3e+e2yN0e6xGTuE60gX
I2+X1p1g9IduDYPoI20X1eHyyMqGeeIb4g0iisloTp5oi3EuAYRGf1XuqAT
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.gpg
```

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

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

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

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

Der Fingerabdruck sollte folgenden Angaben entsprechen:

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

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

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

## GPG

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

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

## GPG

```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for 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
```

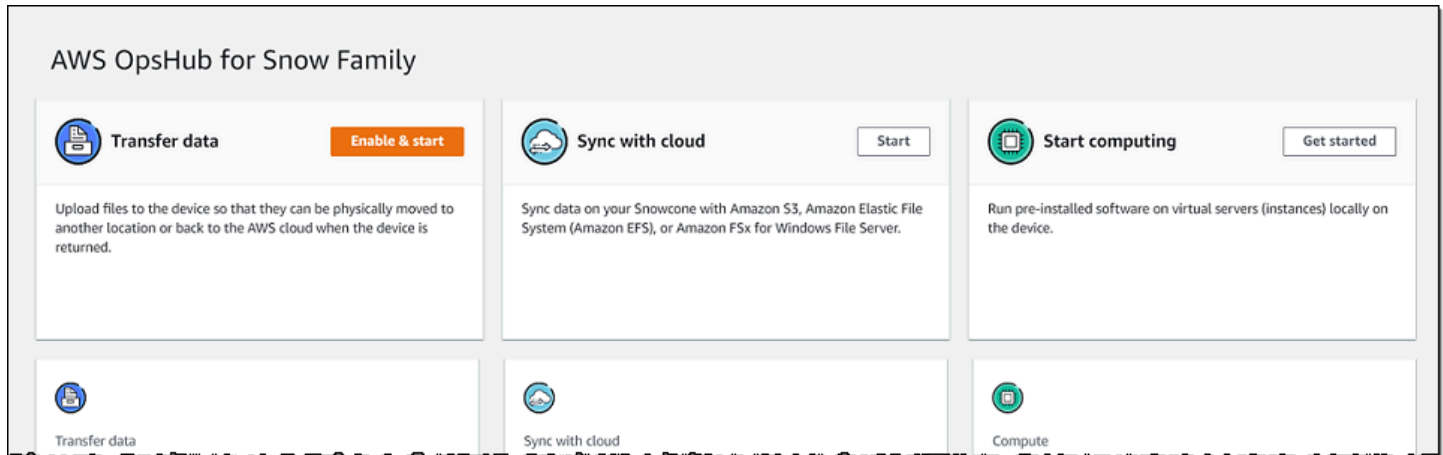
Wenn Sie GPG verwenden und die Ausgabe den Ausdruck enthält `BAD signature`, überprüfen Sie, ob Sie das Verfahren korrekt ausgeführt haben. Wenn Sie weiterhin diese Antwort erhalten, wenden Sie sich an den Agenten AWS Support und installieren Sie ihn nicht. Die Warnmeldung bezüglich des Vertrauens bedeutet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

## AWS Dienste auf Ihrem Gerät verwalten

Mit AWS OpsHub können Sie AWS Dienste auf Ihren Snow Family-Geräten nutzen und verwalten. AWS OpsHub unterstützt derzeit die folgenden Ressourcen:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instances — Verwenden Sie Amazon EC2-kompatible Instances, um auf einem virtuellen Server installierte Software auszuführen, ohne sie zur Verarbeitung an den AWS Cloud zu senden.
- AWS DataSync—Übertragen Sie eine große Anzahl von Dateien zwischen Ihrem lokalen Speicher und anderen AWS Cloud Speicherorten, z. B. Dateisystemen oder Amazon S3.

- **Network File System (NFS)** — Verwenden Sie Dateifreigaben, um Daten auf Ihr Gerät zu verschieben. Sie können das Gerät versenden, AWS an das Ihre Daten übertragen werden AWS Cloud, oder es für die Übertragung DataSync an andere AWS Cloud Standorte verwenden.



## Themen

- [Lokale Verwendung von Amazon EC2-kompatiblen Recheninstanzen](#)
- [Verwaltung der NFS-Schnittstelle](#)

## Lokale Verwendung von Amazon EC2-kompatiblen Recheninstanzen

Sie können AWS OpsHub damit vorinstallierte Software auf virtuellen Servern (Instances) lokal auf Ihrem Gerät ausführen und auch Amazon EC2 EC2-Instances auf Ihrem Gerät verwalten.

## Themen

- [Starten einer Amazon EC2-kompatiblen Instance](#)
- [Stoppen einer Amazon EC2-kompatiblen Instance](#)
- [Starten einer Amazon EC2-kompatiblen Instance](#)
- [Mit Schlüsselpaaren arbeiten](#)
- [Beenden einer Amazon EC2-kompatiblen Instance](#)
- [Speicher-Volumes lokal verwenden](#)

## Starten einer Amazon EC2-kompatiblen Instance

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

## Um eine Amazon EC2-kompatible Instance zu starten

1. Öffnen Sie die Anwendung AWS OpsHub .
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. 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 Sie Amazon EC2-kompatible Instances auf Ihrem Gerät ausführen, werden diese in der Spalte Instanzname unter Instances angezeigt. Sie können auf dieser Seite Details zu den einzelnen Instances anzeigen.
4. Wählen Sie Launch Instance (Instance starten) aus. Der Launch Instance Wizard wird geöffnet.
5. Wählen Sie unter Gerät das Snow-Gerät aus, auf dem Sie das Amazon EC2-kompatible Gerät starten möchten.

## Launch instance ✕

Device

192.0.2.0 ▼

Image (AMI)

snow-al2-test-ami-1.0.2 ▼

Instance type

sbe-c.small ▼

Create public IP address (VNI)  Use existing IP address (VNI)  Do not attach IP address

Physical network interface

SFP+:a.bc-1d2ef456gg678gi9j ▼

IP Address assignment

DHCP ▼

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 mithilfe einer physischen Netzwerkschnittstelle zu erstellen. Wählen Sie eine physische Netzwerkschnittstelle und eine IP-Adresszuweisung aus.
  - Bestehende IP-Adresse (VNI) verwenden — Wählen Sie diese Option, um eine vorhandene IP-Adresse und anschließend vorhandene virtuelle Netzwerkschnittstellen zu verwenden. Wählen Sie eine physische und eine virtuelle Netzwerkschnittstelle aus.
  - Keine IP-Adresse anhängen — Wählen Sie diese Option, wenn Sie keine IP-Adresse anhängen möchten.
9. Wählen Sie aus, wie Sie ein key pair an die Instance anhängen möchten. Ihnen stehen folgende Optionen zur Verfügung:

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

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

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

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

## Stoppen einer Amazon EC2-kompatiblen Instance

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

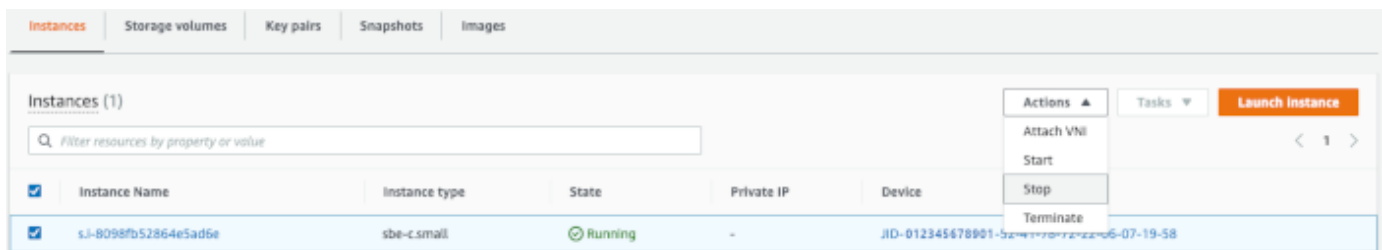


## So beenden Sie eine Amazon EC2-kompatible Instance

1. Öffnen Sie die Anwendung AWS OpsHub .
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. 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 Sie Amazon EC2-kompatible Instances auf Ihrem Gerät ausführen, werden diese in der Spalte Instanzname unter Instances angezeigt.
4. Wählen Sie die Instance aus, die Sie beenden möchten, wählen Sie das Menü Aktionen und dann Stopp. Der State (Status) wird in Stopping (Wird angehalten) und anschließend nach Abschluss in Stopped (Angehalten) geändert.



## Starten einer Amazon EC2-kompatiblen Instance

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

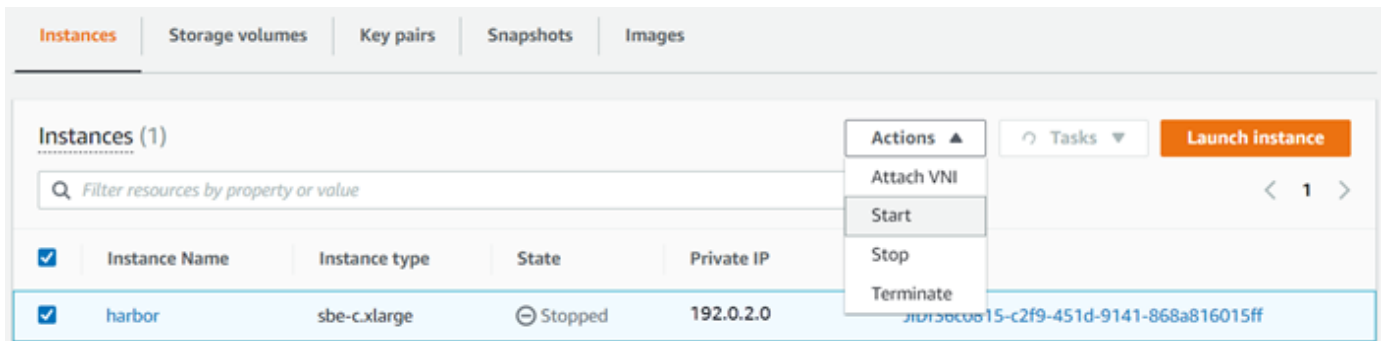
Um eine Amazon EC2-kompatible Instance zu starten

1. Öffnen Sie die Anwendung AWS OpsHub .
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. 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.

- 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.



## Mit Schlüsselpaaren arbeiten

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

Um Schlüsselpaare zu erstellen, zu importieren oder zu verwalten

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

## Beenden einer Amazon EC2-kompatiblen Instance

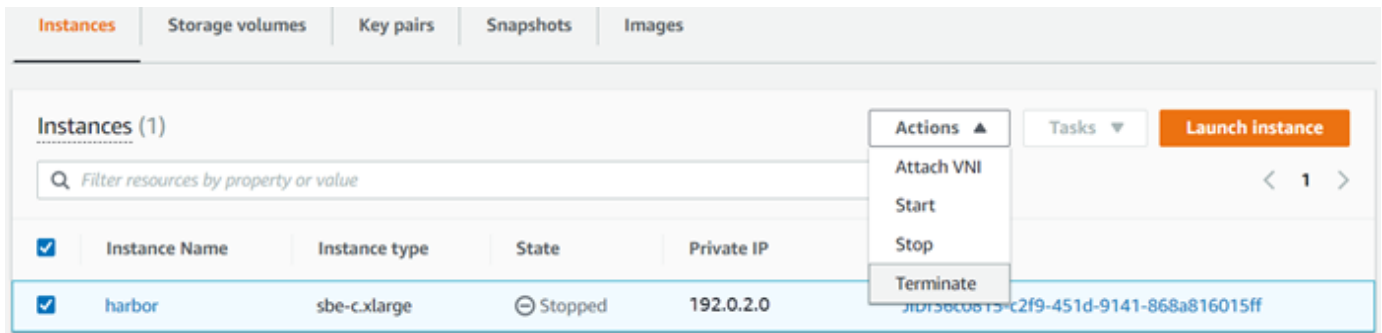
Nachdem Sie eine Amazon EC2-kompatible Instance beendet haben, können Sie die Instance nicht neu starten.

Um eine Amazon EC2-kompatible Instance zu beenden

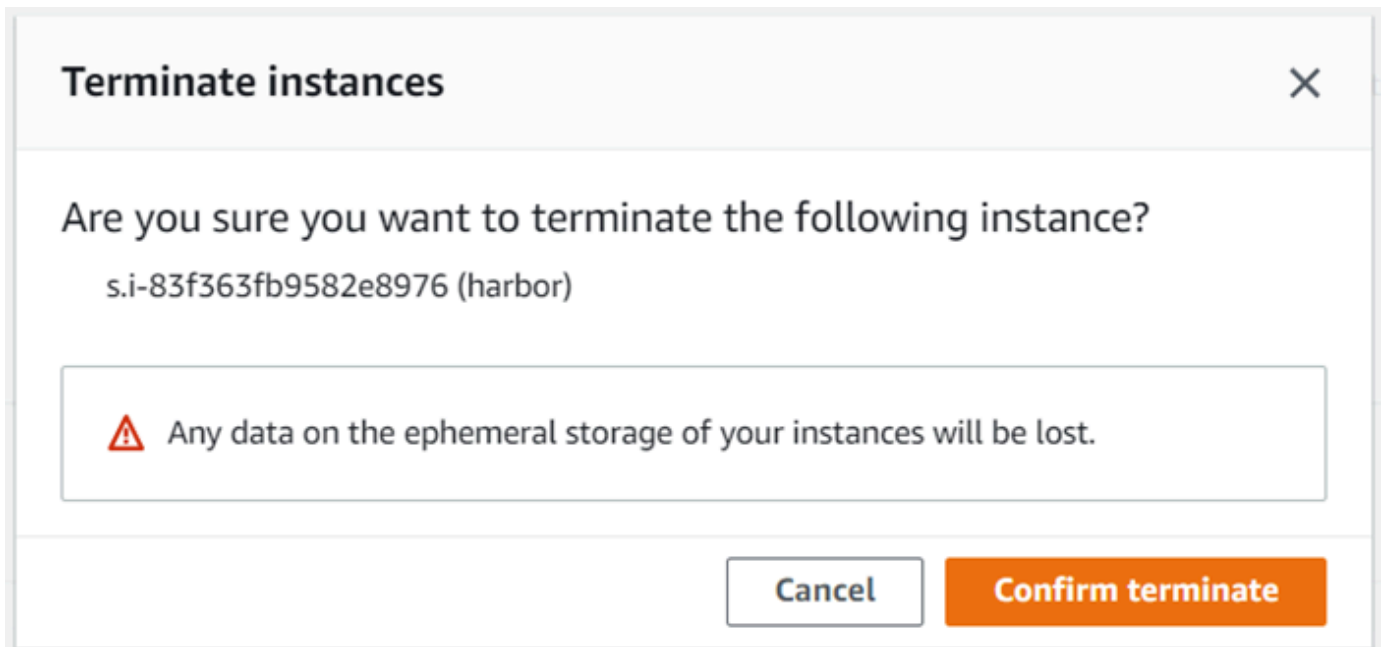
- Öffnen Sie die Anwendung AWS OpsHub .
- Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und

anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Sie können alle Ihre Datenverarbeitungsressourcen im Abschnitt Resources (Ressourcen) anzeigen.

- Suchen Sie in der Spalte Instance name (Instance-Name) unter Instances (Instanzen) die Instance aus, die Sie beenden möchten.
- Wählen Sie die Instanz und anschließend das Menü Aktionen aus. Wählen Sie im Menü „Aktionen“ die Option „Beenden“.



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



#### Note

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

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

## Speicher-Volumes lokal verwenden

Amazon EC2-kompatible Instances verwenden Amazon EBS-Volumes für die Speicherung. In diesem Verfahren erstellen Sie ein Speicher-Volume und fügen es Ihrer Instance mithilfe von hinzu. AWS OpsHub

So erstellen Sie ein Speichervolume

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. 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.

« Back | Compute (EC2) » Create volume

### Create Volume

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

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

**Size**  
Define the size of the volume, in GiBs.

100

**Volume Type**  
Select a performance type for your volume.

Capacity-optimized HDD volume (sbg1)

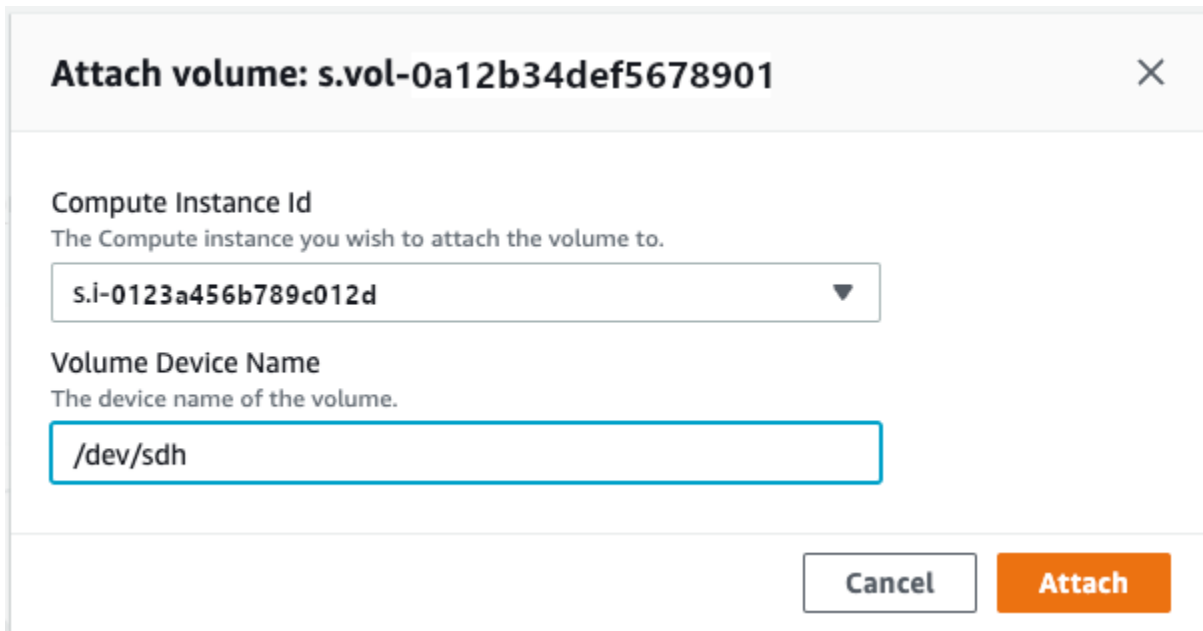
Cancel Submit

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

- 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

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



**Attach volume: s.vol-0a12b34def5678901**

**Compute Instance Id**  
The Compute instance you wish to attach the volume to.

s.i-0123a456b789c012d

**Volume Device Name**  
The device name of the volume.

/dev/sdh

Cancel Attach

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

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

## Verwaltung der NFS-Schnittstelle

Verwenden Sie die NFS-Schnittstelle (Network File System), um Dateien auf das Snow Family-Gerät hochzuladen, als ob es sich bei dem Gerät um einen lokalen Speicher Ihres Betriebssystems handeln würde. Dies ermöglicht einen benutzerfreundlicheren Ansatz beim Übertragen von Daten, da

Sie Funktionen Ihres Betriebssystems wie das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche verwenden können. Jeder S3-Bucket auf dem Gerät ist als Endpunkt der NFS-Schnittstelle verfügbar und kann für das Kopieren von Daten bereitgestellt werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

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

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

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

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, wenn möglich NFSv4.1 zu verwenden und Dateinamen mit Unicode UTF-8 zu codieren, um einen erfolgreichen Datenimport sicherzustellen. Dateinamen, die nicht mit UTF-8 codiert sind, werden je nach verwendeter NFS-Kodierung möglicherweise nicht nach S3 oder mit einem anderen Dateinamen nach S3 hochgeladen.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Geräte der Snow Family unterstützen keine Dateipfade mit mehr als 1024 Zeichen. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateiimport.
- Weitere Informationen finden Sie unter [Objektschlüssel](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Bei NFS-basierten Übertragungen werden standardmäßige Metadaten im POSIX-Stil zu Ihren Objekten hinzugefügt, wenn sie von Geräten der Snow Family in Amazon S3 importiert werden. Darüber hinaus werden Sie die Metadaten „x-amz-meta-user-agent aws-datasync“ sehen, wie wir sie derzeit AWS DataSync als Teil des internen Importmechanismus in Amazon S3 für den Geräteimport von Snow Family mit NFS-Option verwenden.

 Note

Auf der Seite mit den Gerätedetails in AWS OpsHub ist der verfügbare Speicherplatz auf Snowcone-Geräten erst korrekt, wenn die NFS-Schnittstelle gestartet wird.

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


## Themen

- [Den NFS-Dienst auf einem Windows-Betriebssystem starten](#)
- [Automatische Konfiguration der NFS-Schnittstelle](#)
- [Manuelles Konfigurieren der NFS-Schnittstelle](#)
- [Verwaltung von NFS-Endpunkten auf dem Snow Family-Gerät](#)
- [Mounten von NFS-Endpunkten auf Client-Computern](#)
- [Stoppen der NFS-Schnittstelle](#)

## Den NFS-Dienst auf einem Windows-Betriebssystem starten

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

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

 Note

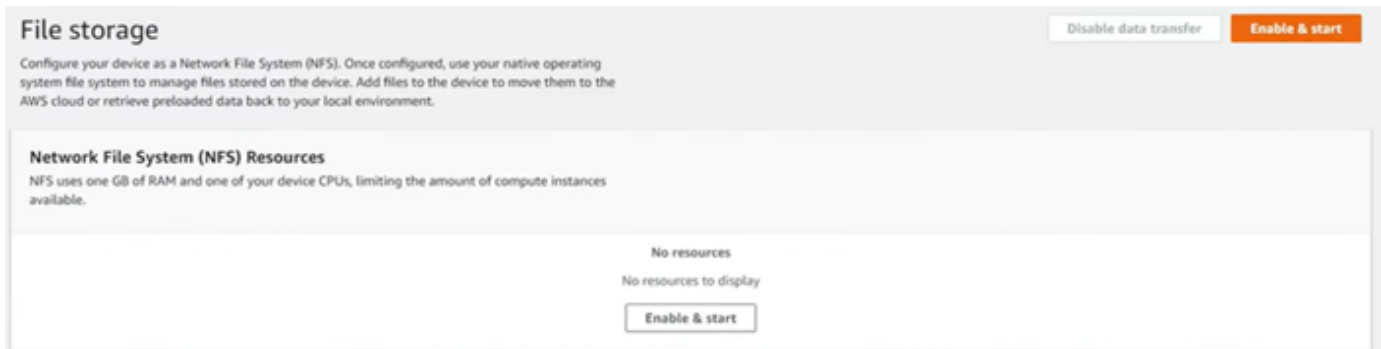
Um die Windows-Funktionen zu aktivieren, müssen Sie möglicherweise einen Administratorbenutzernamen und ein Administratorkennwort für Ihren Computer angeben.

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

## Automatische Konfiguration der NFS-Schnittstelle

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt. Sie müssen sie daher 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). Der Vorgang kann ein oder zwei Minuten dauern.



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

### Note

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

## Manuelles Konfigurieren der NFS-Schnittstelle

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt. Sie müssen sie daher starten, um die Datenübertragung auf dem Gerät zu aktivieren. Sie können die NFS-Schnittstelle manuell konfigurieren, indem Sie die IP-Adresse eines Virtual Network Interface (VNI)



angeben, das 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 Compute-Instances](#).

Sie können auch festlegen, dass das Snow Family-Gerät die NFS-Schnittstelle automatisch konfiguriert. Weitere Informationen finden Sie unter [Automatische Konfiguration der NFS-Schnittstelle](#).

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

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

## Start NFS ✕

Physical network interface

RJ45: s.ni-8459d6c7273eed333 ▼

Create IP address (VNI)  Use existing IP address (VNI)

IP Address assignment

DHCP ▼

Restrict NFS to allowed hosts  Allow all hosts

Allowed hosts

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

192.0.2.0/24 ✕

0.0.0.0/0 ✕

**Add allowed hosts**

Allow instances on this device to access NFS

Enable

**Cancel** **Start NFS**

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


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

 **Important**

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

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

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

 **Note**

Wenn Sie „NFS auf zulässige Hosts beschränken“ wählen und keine zulässigen CIDR-Blöcke angeben, lehnt das Snow Family-Gerät alle Anfragen zum Mounten der NFS-Schnittstelle ab.

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

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

**⚠ Important**

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

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

## Verwaltung von NFS-Endpunkten auf dem Snow Family-Gerät

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

### Um einen Endpunkt zu mounten

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

### Um einen Endpunkt auszuhängen

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

2. Wählen Sie Endpoint unmount aus. Das Snow Family-Gerät entfernt den Endpoint und er kann nicht mehr verwendet werden.

 Note

Stellen Sie vor dem Aushängen eines Endpunkts sicher, dass keine Daten von oder dorthin kopiert werden.

## Mounten von NFS-Endpunkten auf Client-Computern

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

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

- Windows:

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

- Linux:

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

- macOS:

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

## Stoppen der NFS-Schnittstelle

Stoppen Sie die NFS-Schnittstelle auf dem Snow Family-Gerät, wenn Sie mit der Übertragung von Dateien zum oder vom Gerät fertig sind.

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

## Wird verwendet DataSync , um Dateien zu übertragen AWS

Sie können AWS OpsHub damit einen AWS DataSync Agenten auf Ihrem Snowcone-Gerät erstellen. Sie können damit Dateien zwischen Ihrem Gerät und Amazon S3, Amazon Elastic File System (Amazon EFS) oder FSx for Windows File Server in der AWS Cloud übertragen.

AWS DataSync ist ein Online-Datenübertragungsservice, der das Kopieren großer Datenmengen zu und von AWS Speicherdiensten vereinfachen, automatisieren und beschleunigen soll. DataSync kopiert Daten über das Internet oder AWS Direct Connect. Da es sich um einen vollständig verwalteten Dienst handelt, fällt ein Großteil der Notwendigkeit, Anwendungen zu ändern, Skripts zu entwickeln oder die Infrastruktur zu verwalten.

DataSync unterstützt die Datenübertragung zwischen Network File System (NFS) und Amazon EFS, Amazon S3 oder Amazon FSx for Windows File Server.

Informationen zur Quell- und Zielortkombination, die von unterstützt wird AWS DataSync, finden Sie unter [Arbeiten mit Speicherorten](#) im AWS DataSync Benutzerhandbuch.

Snowcone wird mit dem DataSync Agenten geliefert, bei dem es sich um eine virtuelle Maschine (VM) handelt, die zum Lesen oder Schreiben von Daten aus einem lokalen Speichersystem verwendet wird. Um ihn zu verwenden DataSync, starten Sie zuerst den Agenten und aktivieren ihn dann in der DataSync Konsole. Informationen zu DataSync finden Sie unter [Erste Schritte mit AWS DataSync](#).

Um den DataSync Agenten zu starten

1. Bevor Sie den DataSync Agenten starten, aktivieren Sie NFS auf Ihrem Snowcone-Gerät. Siehe [Automatische Konfiguration der NFS-Schnittstelle](#) und [NFS starten und Zugriff einschränken](#).

2. Wählen Sie auf dem AWS OpsHub Dashboard im Abschnitt Mit Cloud synchronisieren die Option Start aus, um den Assistenten zum Starten des DataSync Agenten zu öffnen. Das DataSyncStart-Agent-Formular enthält die Felder Geräte-IP-Adresse und Physikalische Netzwerkschnittstelle.
3. Wählen Sie Create IP address (IP-Adresse erstellen) (VNI), um eine virtuelle IP-Adresse zu erstellen, oder wählen Sie Use existing IP address (Vorhandene IP-Adresse verwenden).
4. Wenn Sie Create IP Address (VNI) wählen, wählen Sie DHCP oder Static IP im Listenfeld IP-Adresszuweisung aus.

Wenn Sie Use existing IP address (Vorhandene IP-Adresse verwenden) wählen, wählen Sie im Listenfeld Virtual network interface (Virtuelle Netzwerkschnittstelle) eine virtuelle Schnittstelle aus.

5. Wählen Sie Start agent (Agent starten). Sie werden zur DataSync Ressourcenseite weitergeleitet. Es kann bis zu fünf Minuten dauern, bis die IP-Adresse des Agenten angezeigt wird.
6. Verwenden Sie das Kopiersymbol, um den IP-Adresswert des Agenten aus der Agent-IP-Adressdatei zu kopieren, und wählen Sie DataSync Konsole öffnen aus.

Dadurch wird die DataSync Konsole geöffnet, in der Sie den Agenten aktivieren und Ihre Dateien übertragen. Der Rest der Einrichtung erfolgt in der AWS DataSync Konsole.

## Dateien übertragen mit DataSync

AWS Snowcone hat den Agenten bereits erstellt, sodass Sie ihn nur aktivieren, Ihren Quell- und Zielort konfigurieren, eine Aufgabe erstellen und die Aufgabe starten müssen.

Um den DataSync Agenten zu aktivieren und den DataSync Dienst zu nutzen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Fügen Sie im Abschnitt Aktivierung auf der Seite Create Agent die kopierte IP-Adresse in das Feld Agentenadresse ein und wählen Sie Get Key aus. Ihr Browser verbindet sich mit der IP-Adresse und erhält von Ihrem Agenten einen eindeutigen Aktivierungsschlüssel.
3. Nachdem der Agent aktiviert wurde, konfigurieren Sie das auf Ihrem Snowcone-Gerät ausgeführte NFS als Quellverzeichnis für. DataSync Anweisungen finden [Sie unter Konfiguration eines Quellverzeichnisses](#) im AWS DataSync Benutzerhandbuch.

**Note**

Der DataSync Agent, der auf Ihrem Snowcone-Gerät ausgeführt wird, kann Dateien zu und von einem Standort übertragen, der in Ihrem Netzwerk erreichbar ist.

4. Wählen und konfigurieren Sie auf der Seite Ziel konfigurieren das Ziel, an das Sie Dateien übertragen möchten. Anweisungen finden [Sie im AWS DataSync Benutzerhandbuch unter Einen Zielort konfigurieren](#).
5. Konfigurieren der Aufgabeneinstellungen. Anweisungen finden [Sie im AWS DataSync Benutzerhandbuch unter Konfigurieren von Aufgabeneinstellungen](#).
6. Überprüfen Sie Ihre Einstellungen, und Erstellen Sie Ihre Aufgabe. Anweisungen finden Sie im AWS DataSync Benutzerhandbuch unter [Überprüfen Sie Ihre Einstellungen und erstellen Sie Ihre Aufgabe](#).
7. Starten Sie Ihre Aufgabe, und warten Sie, bis Ihre Dateien übertragen werden. Anweisungen finden Sie im AWS DataSync Benutzerhandbuch unter [Starten Sie Ihre Aufgabe](#).

## Verwaltung Ihrer Geräte

Sie verwenden den AWS OpsHub , um Ihre Snow Family-Geräte zu verwalten. Auf der Seite mit den Gerätedetails können Sie dieselben Aufgaben ausführen wie mit dem AWS CLI, z. B. den Alias Ihres Geräts ändern, das Gerät neu starten und nach Updates suchen.

### Themen

- [Ihr Gerät neu starten](#)
- [Ihr Gerät wird heruntergefahren](#)
- [Bearbeitung des Gerätealias](#)
- [Updates für Ihr Gerät und die AWS OpsHub Anwendung erhalten](#)
- [Profile verwalten](#)

## Ihr Gerät neu starten

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

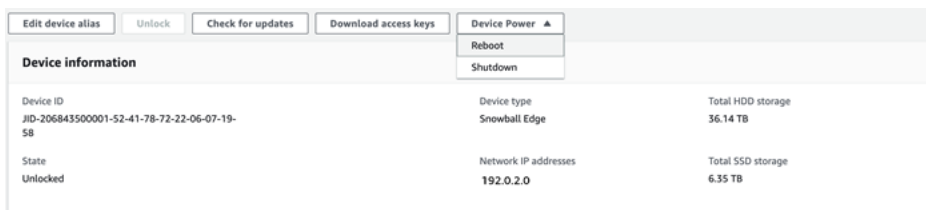


**⚠ Important**

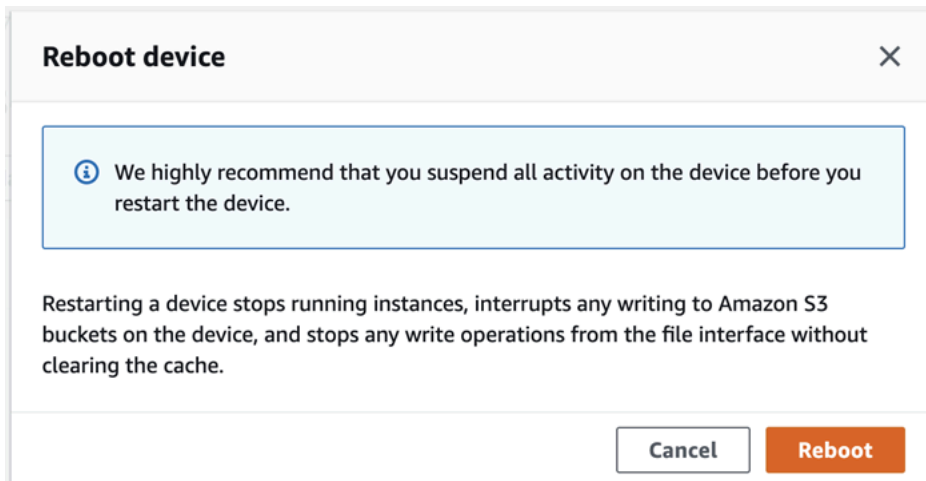
Es wird nachdrücklich empfohlen, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät neu starten. Durch den Neustart eines Geräts werden die laufenden Instances gestoppt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen.

**So starten Sie ein Gerät neu**

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



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

**Ihr Gerät wird heruntergefahren**

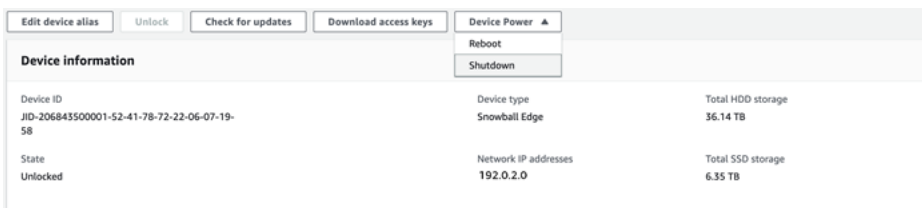
Gehen Sie AWS OpsHub wie folgt vor, um Ihr Snow-Gerät herunterzufahren.

### ⚠ Important

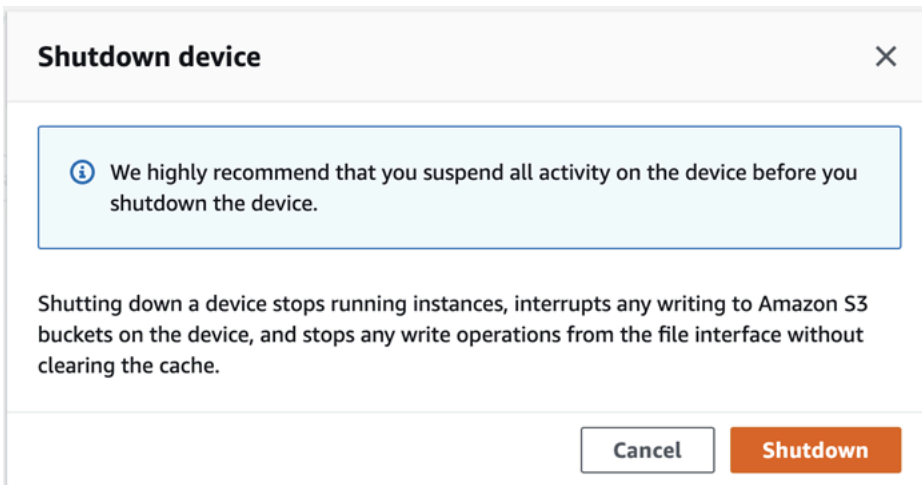
Wir empfehlen dringend, alle Aktivitäten auf dem Gerät zu unterbrechen, bevor Sie das Gerät herunterfahren. Beim Herunterfahren eines Geräts werden Instances nicht mehr ausgeführt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät werden unterbrochen.

## Um ein Gerät herunterzufahren

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



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

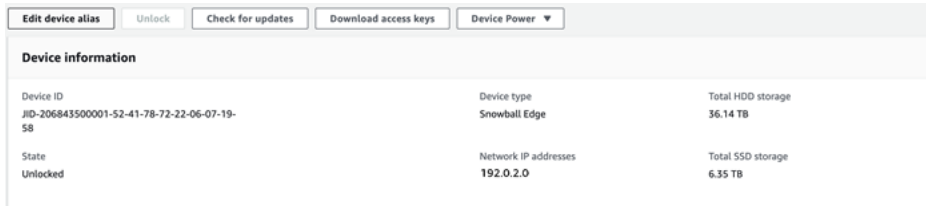


## Bearbeitung des Gerätealias

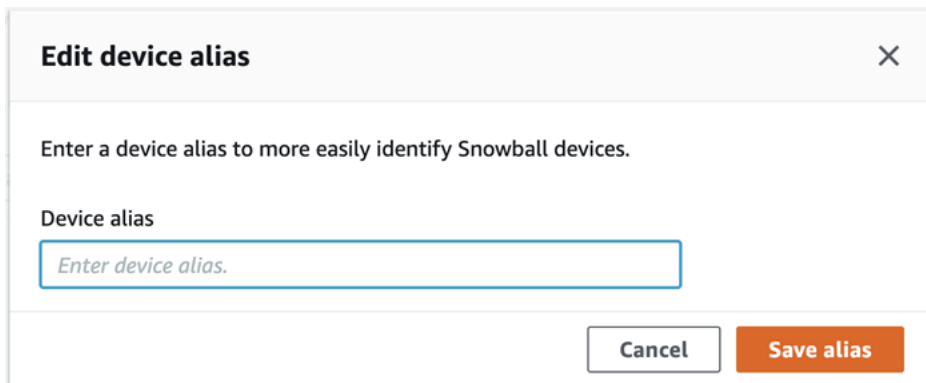
Gehen Sie wie folgt vor, um Ihren Gerätealias mit zu bearbeiten AWS OpsHub.

## So bearbeiten Sie den Alias Ihres Geräts

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



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



## Updates für Ihr Gerät und die AWS OpsHub Anwendung erhalten

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

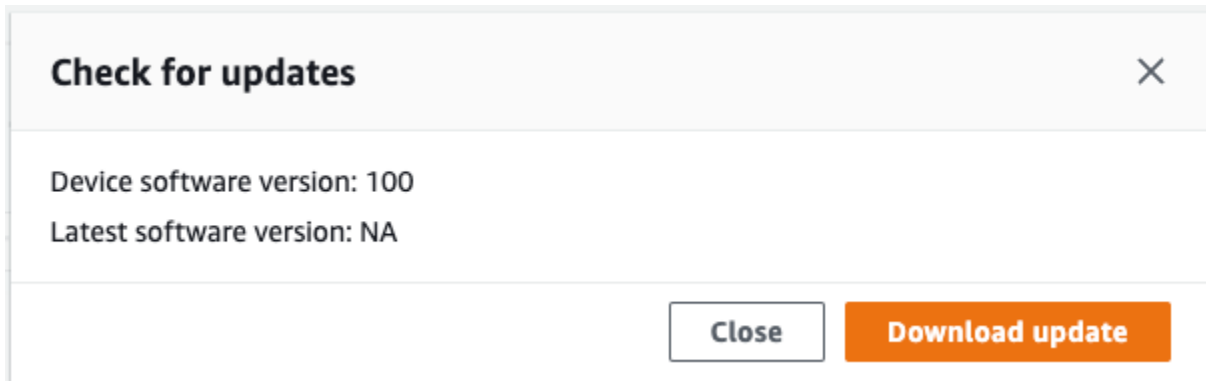
### Ihr Gerät aktualisieren

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

### So aktualisieren Sie Ihr Gerät

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. Wählen Sie die Registerkarte Check for updates (Nach Updates suchen) aus.

Auf der Seite Check for updates (Nach Updates suchen) werden die aktuelle Softwareversion auf Ihrem Gerät und die neueste Softwareversion angezeigt, wenn vorhanden.



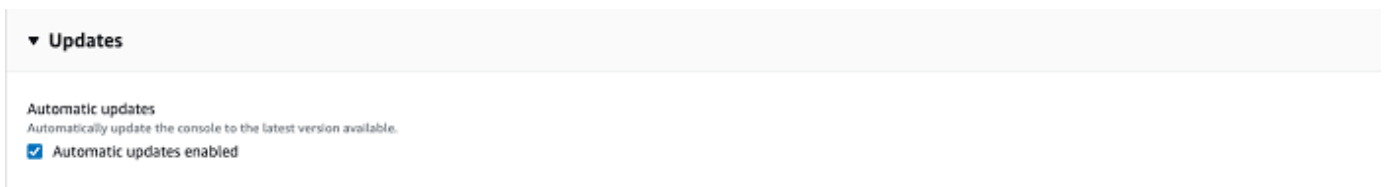
3. Wenn es ein Update gibt, wählen Sie Update herunterladen. Wählen Sie andernfalls Close aus.

### Aktualisieren Sie Ihre AWS OpsHub Anwendung

AWS OpsHub aktualisiert die Anwendung automatisch auf die neueste Version. Gehen Sie wie folgt vor, um sicherzustellen, dass das automatische Update aktiviert ist.

Um zu überprüfen, ob automatische Updates aktiviert sind für AWS OpsHub

1. Wählen Sie im AWS OpsHub Dashboard Einstellungen aus.
2. Öffnen Sie den Tab Updates.
3. Vergewissern Sie sich, dass Automatische Updates aktiviert ausgewählt ist. Automatisches Update ist standardmäßig aktiviert.



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

## Profile verwalten

Sie können ein Profil für die dauerhafte Speicherung Ihrer Anmeldeinformationen in Ihrem lokalen Dateisystem erstellen. Mit dieser Option haben Sie die Möglichkeit AWS OpsHub, jedes Mal, wenn

Sie das Gerät entsperren, ein neues Profil mithilfe der Geräte-IP-Adresse, des Entsperrcodes und der Manifestdatei zu erstellen.

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

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—

SnowDevice1profile, SnowDevice2profile, und SnowDevice3profile.

```
{
  "version": 1,
  "profiles": [
    {
      "SnowDevice1profile": {
        "name": "SnowDevice1profile",
        "jobId": "JID12345678-136f-45b4-b5c2-847db8adc749",
        "unlockCode": "db223-12345-dbe46-44557-c7cc2",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-136f-45b4-b5c2-847db8adc749_manifest-1670622989203.bin",
        "defaultEndpoint": "https://10.16.0.1",
        "isCluster": false,
        "deviceIps": []
      },
    },
    {
      "SnowDevice2profile": {
        "name": "SnowDevice2profile",
        "jobId": "JID12345678-fdb2-436a-a4ff-7c510dec1bae",
        "unlockCode": "b893b-54321-0f65c-6c5e1-7f748",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-fdb2-436a-a4ff-7c510dec1bae_manifest-1670623746908.bin",
        "defaultEndpoint": "https://10.16.0.2",
        "isCluster": false,
        "deviceIps": []
      },
    },
    {
      "SnowDevice3profile": {
        "name": "SnowDevice3profile",
        "jobId": "JID12345678-c384-4a5e-becd-ab5f38888463",
```

```
    "unlockCode": "64c89-13524-4d054-13d93-c1b80",
    "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-
c384-4a5e-becd-ab5f38888463_manifest-1670623999136.bin",
    "defaultEndpoint": "https://10.16.0.3",
    "isCluster": false,
    "deviceIps": []
  }
}
```

## So erstellen Sie ein Profil

1. Entsperren Sie Ihr Gerät lokal und melden Sie sich gemäß den Anweisungen unter an [Ein Gerät entsperren](#).
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 auf den Profilnamen folgen, und den Inhalt innerhalb dieser Klammern enthält.
3. Speichern und schließen Sie die Datei.

## Einstellung der NTP-Zeitserver für Ihr Gerät

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

## Um Zeitquellen zu überprüfen

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

Die Tabelle mit den Zeitquellen 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 Zustände:
  - **AKTUELL:** Die Zeitquelle wird derzeit zum Synchronisieren der Uhrzeit verwendet
  - **KOMBINIERT:** Die Zeitquelle wird mit der aktuellen Quelle kombiniert
  - **AUSGESCHLOSSEN:** Die Zeitquelle ist durch den Kombinationsalgorithmus ausgeschlossen
  - **VERLOREN:** Die Verbindung mit der Zeitquelle wurde unterbrochen
  - **UNVERFÜGBARKEIT:** Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder ein falscher Ticker oder eine zu große Variabilität erkannt hat
- **Typ:** Bei den NTP-Quellen (Network Time Protocol) kann es sich um einen Server oder einen Peer handeln. Ein Server kann vom Benutzer mithilfe des `update-time-server` Befehls eingerichtet werden, wohingegen ein Peer nur mit anderen Snowball Edge-Geräten im Cluster eingerichtet werden kann und automatisch eingerichtet wird, wenn der Cluster zugeordnet wird.
- **Schicht:** Die Schicht der Quelle. Stratum 1 weist auf eine Quelle mit einer lokal angeschlossenen Referenzuhr hin. Eine Quelle, die mit einer Stratum 1-Quelle synchronisiert ist, ist auf Stratum 2 eingestellt. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert ist, wird auf Stratum 3 gesetzt usw.

## Um die Zeitserver zu aktualisieren

1. Suchen Sie im AWS OpsHub Dashboard unter Geräte nach Ihrem Gerät. Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.

2. In der Tabelle Zeitquellen wird eine Liste der Zeitquellen angezeigt, mit denen Ihr Gerät die Zeit synchronisiert.
3. Wählen Sie in der Tabelle Zeitquellen die Option Zeitserver aktualisieren aus.
4. Geben Sie den DNS-Namen oder die IP-Adresse der Zeitserver ein, mit denen Ihr Gerät die Uhrzeit synchronisieren soll, und wählen Sie Aktualisieren aus.

Update time servers

Update time servers on JID-206843500001-52-41-78-72-22-06-07-19-58

**Overriding Existing Settings**  
Updating the time servers will override existing time server settings.

NTP server IP address or DNS name

You can add up to 4 more time servers.



# Den AWS Snowball Edge Client verwenden

Der Snowball Edge-Client ist eine eigenständige Terminalanwendung, die Sie auf Ihrem lokalen Server ausführen, um Ihr AWS Snowcone Gerät zu entsperren und Anmeldeinformationen, Protokolle und Statusinformationen abzurufen. Wenn Sie den Snowball Edge-Client verwenden, können Sie zusätzliche Supportinformationen abrufen, indem Sie den `snowballEdge help` Befehl ausführen.

Wenn Sie Daten auf das AWS Snowcone Gerät lesen und darauf schreiben, verwenden Sie die NFS-Schnittstelle. Sie können die AWS OpsHub for Snow Family Anwendung auch zur Verwaltung von Snow Family-Geräten, einschließlich Snowcone-Geräten, verwenden. Weitere Informationen finden Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

## Den Snowball Edge-Client herunterladen und installieren

Sie können den Snowball Edge-Client unter [AWS Snowball Ressourcen](#) herunterladen und installieren. Suchen Sie auf dieser Seite das Installationspaket für Ihr Betriebssystem und folgen Sie den Anweisungen zur Installation des Snowball Edge-Clients. Wenn Sie den Snowball Edge-Client von einem Terminal auf Ihrer Workstation aus ausführen, müssen Sie je nach Betriebssystem möglicherweise einen bestimmten Pfad verwenden:

- Microsoft Windows — Wenn der Client installiert ist, können Sie ihn ohne zusätzliche Vorbereitung von jedem Verzeichnis aus ausführen.
- Linux — Der Snowball Edge-Client muss vom `~/snowball-client-linux-build_number/bin/` Verzeichnis aus ausgeführt werden. Beachten Sie, dass der Snowball Edge-Client nur auf 64-Bit-Linux-Distributionen unterstützt wird.
- macOS — Das `install.sh` Skript kopiert Ordner aus der TAR-Datei des Snowball Edge-Clients in das `/usr/local/bin/snowball` Verzeichnis. Wenn Sie dieses Skript ausführen, können Sie den Snowball Edge-Client dann von jedem Verzeichnis aus ausführen, wenn `/usr/local/bin` es sich um einen Pfad in Ihrem `bash_profile` handelt. Sie können Ihren Pfad mit dem `echo $PATH`-Befehl überprüfen.

## Befehle für den Snowball Edge-Client

Im Folgenden finden Sie Informationen zu Snowball Edge-Clientbefehlen, einschließlich Anwendungsbeispielen und Beispielausgaben.

**Note**

Das AWS Snowcone Gerät verwendet dieselben Snowball Edge-CLI-Befehle, unterstützt jedoch keine Befehle, die für Clustering gelten.

**Themen**

- [Konfiguration eines Profils für den Snowball Edge-Client](#)
- [Anfordern Ihres QR-Codes für die NFC-Validierung](#)
- [Ein AWS Snowcone Gerät entsperren](#)
- [Einen Snowcone aktualisieren](#)
- [Abrufen von Anmeldeinformationen](#)
- [Einen Dienst auf Ihrem Snowcone-Gerät starten](#)
- [Einen Dienst auf Ihrem Snowcone-Gerät beenden](#)
- [Abrufen des Zertifikats für die Datenübertragung](#)
- [AWS Snowcone Protokolle](#)
- [Abrufen des Gerätestatus](#)
- [Abrufen des Servicestatus](#)
- [Das AWS DataSync AMI starten](#)
- [NFS starten und Zugriff einschränken](#)
- [Beschränken des Zugriffs auf NFS-Freigaben, wenn NFS ausgeführt wird](#)
- [Den Exportpfad für einen Amazon S3 S3-Bucket abrufen](#)
- [Debugging für lokale AWS Operatoren aktivieren](#)
- [Debugging für lokale Operatoren AWS deaktivieren](#)
- [Eine direkte Netzwerkschnittstelle erstellen](#)
- [Informationen über eine direkte Netzwerkschnittstelle abrufen](#)
- [Aktualisierung einer direkten Netzwerkschnittstelle](#)
- [Löschen einer direkten Netzwerkschnittstelle](#)
- [Funktionsstatus wird überprüft](#)
- [Funktionsstatus ändern](#)
- [Zeitserver einrichten](#)
- [Zeitquellen werden überprüft](#)

## Konfiguration eines Profils für den Snowball Edge-Client

Jedes Mal, wenn Sie einen Befehl für den Snowball Edge-Client ausführen, geben Sie Ihre Manifestdatei, den Entsperrcode und eine IP-Adresse an. Die ersten beiden können Sie über die Job-Management-API Managementkonsole für die AWS Snow-Familie oder über die Job-Management-API abrufen. Weitere Informationen zum Abrufen der Manifestdatei und des Entsperrcodes finden Sie unter [Abrufen von Anmeldeinformationen](#).

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 Job manuell eingeben zu müssen. Nachdem Sie den Snowball Edge-Client konfiguriert haben, werden die Informationen in einem Klartext-JSON-Format unter gespeichert. *home directory*/.aws/snowball/config/snowball-.config

Der Endpunkt ist die IP-Adresse, zu der `https://` hinzugefügt wird. Sie können die IP-Adresse des AWS Snowcone Geräts auf dem LCD-Display des AWS Snowcone Geräts finden. Wenn das AWS Snowcone Gerät zum ersten Mal mit Ihrem Netzwerk verbunden wird, 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 [AWS Dienste verwenden auf AWS Snowcone](#).

### Important

Jeder, der auf die Konfigurationsdatei zugreifen kann, kann auf die Daten auf Ihrem Snowcone-Gerät 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 Beispielausgabe

```
Configuration will be stored at home directory\.aws\snowball\config\snowball-.config
```

```
Snowcone Manifest Path: Path/to/manifest/file  
Unlock Code: 29 character unlock code  
Default Endpoint: https://192.0.2.0
```

Sie können mehrere Profile haben, wenn Sie mehrere Jobs gleichzeitig haben. 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 Snowcone Verifizierungs-App zu generieren. Sie können diese App aus dem Apple App Store oder Google Play Store herunterladen. Weitere Informationen zur NFC-Validierung finden Sie unter [Validieren von NFC-Tags](#)

### Usage

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

### Example Beispielausgabe

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

## Ein AWS Snowcone Gerät entsperren

Führen Sie den `snowballEdge unlock-device` Befehl aus, um ein eigenständiges AWS Snowcone Gerät zu entsperren. Diese Befehle authentifizieren Ihren Zugriff auf das AWS Snowcone Gerät.

Wenn Sie einen dieser Entsperrbefehle ausführen, können Sie den Pfad zur Manifestdatei, den 29-stelligen Entsperrcode und die IP-Adresse für Ihr eigenständiges Gerät manuell eingeben. Dieser Vorgang kann mühsam werden, daher empfehlen wir, stattdessen Ihren Snowball Edge-Client zu konfigurieren. Wenn Sie den Snowball Edge-Client bereits konfiguriert haben, müssen Sie nur den Befehl selbst ohne den Pfad zum Manifest, den Entsperrcode oder die IP-Adresse eingeben.

### Note

Um das mit Ihrem Job verknüpfte Gerät zu entsperren, muss sich das Gerät vor Ort befinden, an die Stromversorgung und das Netzwerk angeschlossen und eingeschaltet sein. Darüber

hinaus muss das LCD-Display an der Vorderseite des AWS Snowcone Geräts anzeigen, dass das Gerät betriebsbereit ist.

### Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge unlock-device
```

### Example

#### Example Ausgabe entsperren

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

## Einen Snowcone aktualisieren

Verwenden Sie die folgenden Befehle, um Updates für Ihr Snowcone-Gerät herunterzuladen und zu installieren. Prozeduren, die diese Befehle verwenden, finden Sie unter [Einen Snowcone aktualisieren](#).

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

### Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

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

`snowballEdge describe-device-software`— Gibt die aktuelle Softwareversion für das Gerät zurück. Wenn die Aktualisierung derzeit heruntergeladen wird, wird auch der Downloadstatus angezeigt. Wenn derzeit eine Softwareaktualisierung durchgeführt wird, werden auch die Manifestversion der Aktualisierung und der Status der Installation angezeigt. Nachstehend werden mögliche Ausgaben aufgelistet:

- **NA**— Derzeit werden keine Softwareupdates durchgeführt.
- **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. Durch den Neustart eines Geräts werden die laufenden Instances gestoppt und jegliche Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen. Alle diese Prozesse können zu Datenverlust führen.

### Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

```
Installed version: 101  
Installing version: 102  
Install State: Downloading
```

`snowballEdge download-updates`— Beginnt mit dem Herunterladen der neuesten Softwareupdates für Ihr Snowcone-Gerät.

### Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge download-updates
```

### Example Beispielausgabe

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

`snowballEdge install-updates`— Beginnt mit der Installation der neuesten Softwareupdates für Ihr Snowcone-Gerät, die bereits heruntergeladen wurden.

## Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge install-updates
```

### Example Beispielausgabe

```
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. Durch den Neustart eines Geräts werden die laufenden Instances gestoppt und jegliche Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen. Alle diese Prozesse können zu Datenverlust führen.

## Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge reboot-device
```

### Example Beispielausgabe

```
Rebooting device now.
```

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

## Verwendung (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 Beispielausgabe

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

`snowballEdge describe-auto-update-strategies`— Gibt jede aktuell konfigurierte Strategie für automatische Updates zurück.

## Verwendung (konfigurierter Snowball Edge-Client)

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

## Example Beispielausgabe

```
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 Befehlen `snowballEdge list-access-keys` und `snowballEdge get-secret-access-key` können Sie die lokalen Anmeldeinformationen abrufen. Sie verwenden diese, um Ihre Anfragen zu authentifizieren, wenn Sie das AWS CLI oder mit einem AWS SDK verwenden. Diese Anmeldeinformationen sind nur mit einem einzelnen Auftrag für Snowcone verknüpft, und Sie können sie nur auf dem Gerät verwenden. Das Gerät hat keine AWS Identity and Access Management (IAM-) Berechtigungen in der AWS Cloud.

Weitere Informationen finden Sie unter [AWS Anmeldeinformationen](#) und [Verwendung des Amazon EC2 EC2-Endpunkts](#).



**Note**

Wenn Sie das AWS CLI mit Snowball verwenden, müssen Sie diese Anmeldeinformationen bei der Konfiguration der CLI verwenden. Informationen zur Konfiguration der Anmeldeinformationen für die CLI finden Sie unter [Schnellkonfiguration](#) im AWS Command Line Interface Benutzerhandbuch.

**Verwendung (konfigurierter Snowball Edge-Client)**

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

**Example Beispielausgabe**

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

**Verwendung (konfigurierter Snowball Edge-Client)**

```
snowballEdge get-secret-access-key --access-key-id Access Key
```

**Example Beispielausgabe**

```
[snowballEdge]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

## Einen Dienst auf Ihrem Snowcone-Gerät starten

Snowcone unterstützt mehrere Dienste, darunter Recheninstanzen, die NFS-Dateischnittstelle, Amazon EC2 und AWS DataSync. Sie können diese Dienste mit dem Befehl `snowballEdge start-service` starten. 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](#).

## Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

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

## Einen Dienst auf Ihrem Snowcone-Gerät beenden

Um einen Dienst zu beenden, der auf Ihrem Snowcone-Gerät läuft, können Sie den snowballEdge stop-service Befehl verwenden. Die Amazon EC2 EC2-Dienste können nicht gestoppt werden.

### Warning

Datenverlust kann auftreten, wenn die Dateischnittstelle gestoppt wird, bevor die verbleibenden gepufferten Daten auf das Gerät geschrieben werden.

## Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

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

## Abrufen des Zertifikats für die Datenübertragung

Um Daten auf ein Snowcone-Gerät zu übertragen, verwenden Sie die NFS-Schnittstelle oder AWS DataSync. Wenn Sie Ihr Snowcone-Gerät mit einer anderen IP-Adresse entsperren, wird ein neues Zertifikat generiert, und das alte Zertifikat ist für die Verwendung mit dem Endpunkt nicht mehr gültig. Mit dem get-certificate Befehl können Sie das neue, aktualisierte Zertifikat erneut vom Snowcone-Gerät abrufen.

Sie können diese Zertifikate auflisten und mit den folgenden Befehlen von Ihrem Snowcone-Gerät herunterladen:

- `list-certificates` – Führt die Amazon-Ressourcennamen (ARNs) für die Zertifikate auf, die Ihnen zur Verfügung stehen.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-certificates
```

Example Beispielausgabe

```
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7",
    "SubjectAlternativeNames" : [ "192.0.2.0" ]
  } ]
}
```

- `get-certificate` – Ruft basierend auf dem angegebenen ARN ein bestimmtes Zertifikat ab.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge get-certificate --certificate-arn arn:aws:snowball-
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

Example Beispielausgabe

```
-----BEGIN CERTIFICATE-----
Certificate
-----END CERTIFICATE-----
```

## AWS Snowcone Protokolle

Wenn Sie Daten zwischen Ihrem lokalen Rechenzentrum und einem Snowcone-Gerät übertragen, werden automatisch Protokolle generiert. Sollten während der Datenübertragung auf das Gerät

unerwartete Fehler auftreten, können Sie mit den folgenden Befehlen eine Kopie der Protokolle auf Ihrem lokalen Server speichern.

Im Zusammenhang mit Protokollen gibt es drei verschiedene Befehle:

- `list-logs`— Gibt eine Liste von Protokollen im JSON-Format zurück. In dieser Liste sind die Größe der Protokolle in Byte, die ARNs und die Service-ID für die Protokolle sowie die Art der Protokolle enthalten.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-logs
```

Example Beispielausgabe

```
{
  "Logs" : [ {
    "LogArn" : "arn:aws:snowball-device::log/s3-storage-JIEXAMPLE2f-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "SUPPORT",
    "ServiceId" : "datasync",
    "EstimatedSizeBytes" : 53132614
  }, {
    "LogArn" : "arn:aws:snowball-device::log/fileinterface-JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "CUSTOMER",
    "ServiceId" : "nfs",
    "EstimatedSizeBytes" : 4446
  } ]
}
```

- `get-log`— Lädt eine Kopie eines bestimmten Protokolls vom Snowcone-Gerät unter einem angegebenen Pfad auf Ihren Server herunter. CUSTOMERProtokolle werden in diesem `.zip` Format gespeichert, und Sie können diese Art von Protokoll extrahieren, um sich den Inhalt anzusehen. SUPPORTProtokolle sind verschlüsselt und können nur von AWS Support Technikern gelesen werden. Sie haben die Möglichkeit, einen Namen und einen Pfad für das Protokoll anzugeben.

Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

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

- `get-support-logs`— Lädt eine Kopie aller SUPPORT Arten von Protokollen vom Snowcone-Gerät unter einem angegebenen Pfad auf Ihren Service herunter.

### Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

```
Logs are being saved to download/path/snowball--logs-1515716135711.bin
```

#### Important

CUSTOMERProtokolle können vertrauliche Informationen über Ihre eigenen Daten enthalten. Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir Ihnen dringend, diese Protokolle zu löschen, nachdem Sie mit ihnen fertig sind.

## Abrufen des Gerätestatus

Sie können den Status und den allgemeinen Zustand Ihres Snowcone-Geräts mit den folgenden Snowball Edge-Client-Befehlen ermitteln:

- `describe-device`

### Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge describe-device
```

## Example Beispielausgabe

```
{
  "DeviceId" : "JIDbEXAMPLE-7eed-1234-ABCD-7EXAMPLE123c",
  "UnlockStatus" : {
    "State" : "UNLOCKED"
  },
  "ActiveNetworkInterface" : {
    "IpAddress" : "192.168.1.2"
  },
  "PhysicalNetworkInterfaces" : [ {
    "PhysicalNetworkInterfaceId" : "s.ni-8bEXAMPLE5EXAMPLE",
    "PhysicalConnectorType" : "RJ45",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.168.1.13",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-84EXAMPLE3EXAMPLE",
    "PhysicalConnectorType" : "RJ45_2",
    "IpAddressAssignment" : "STATIC",
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-87EXAMPLE5EXAMPLE",
    "PhysicalConnectorType" : "WIFI",
    "IpAddressAssignment" : "STATIC",
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  } ],
  "DeviceCapacities" : [ {
    "Name" : "HDD Storage",
    "Unit" : "Byte",
    "Total" : 157242114048,
    "Used" : 81604378624,
    "Available" : 75637735424
  }, {
    "Name" : "SSD Storage",
```

```
    "Unit" : "Byte",
    "Total" : 0,
    "Used" : 0,
    "Available" : 0
  }, {
    "Name" : "vCPU",
    "Unit" : "Number",
    "Total" : 3,
    "Used" : 3,
    "Available" : 0
  }, {
    "Name" : "Memory",
    "Unit" : "Byte",
    "Total" : 5368709120,
    "Used" : 5368709120,
    "Available" : 0
  }, {
    "Name" : "GPU",
    "Unit" : "Number",
    "Total" : 0,
    "Used" : 0,
    "Available" : 0
  } ],
  "DeviceType" : "SNC1_HDD"
}
```

## Abrufen des Servicestatus

Mithilfe des `describe-service` Befehls können Sie den Status und den allgemeinen Zustand der Dienste ermitteln, die auf einem Snowcone-Gerät ausgeführt werden. Sie können zunächst den `list-services`-Befehl ausführen, um zu sehen, welche Services ausgeführt werden.

- `list-services`

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-services
```

Example Beispielausgabe

```
{
```

```
"ServiceIds" : [ "nfs", "datasync", "ec2" ]
}
```

- `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.
- **INACTIVE** – Der Service wird nicht ausgeführt und steht nicht zur Verfügung.

Verwendung (konfigurierter Snowball Edge-Client)

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

### Example Beispielausgabe

```
{
  "ServiceId" : "ec2",
  "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"
    }
  } ]
}
```



```
}
```

## Das AWS DataSync AMI starten

Starten Sie das AWS DataSync AMI auf Snowcone.

Verwendung (konfigurierter Snowball Edge-Client)

AWS DataSync muss mit dem `snc1.medium` Instanztyp gestartet werden. Das Starten DataSync mit einem anderen Instance-Typ kann zu einem instabilen Betrieb und potenziellem Datenverlust führen. Verwenden Sie den `describe-images` Befehl, um das Image zu finden, von dem aus eine Instance gestartet werden soll. Die Ausgabe sieht wie folgt aus.

```
{
  "ImageId": "s.ami-0c046f119de4f752f",
  "Public": false,
  "State": "AVAILABLE",
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sda",
      "Ebs": {
        "DeleteOnTermination": true,
        "Iops": 0,
        "SnapshotId": "s.snap-0d7558ce444ab09bf",
        "VolumeSize": 20,
        "VolumeType": "sbp1"
      }
    }
  ],
  "Description": "AWS DataSync AMI for online data transfer",
  "EnaSupport": false,
  "Name": "scn-datasync-ami",
  "RootDeviceName": "/dev/sda"
}
```

```
aws ec2 describe-images --endpoint http://${snowcone_ip}:8008
```

### Example Beispielausgabe

```
{
  "Reservations": [
```

```
{
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "ImageId": "s.image id",
      "InstanceId": "s.instance id",
      "InstanceType": "snc1.medium",
      "LaunchTime": "2020-03-06T18:58:36.609Z",
      "PrivateIpAddress": "ip address",
      "State": {
        "Code": 16,
        "Name": "running"
      },
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/sda",
          "Ebs": {
            "AttachTime": "2020-03-06T19:14:21.336Z",
            "DeleteOnTermination": true,
            "Status": "attached",
            "VolumeId": "s.volume id"
          }
        }
      ],
      "EbsOptimized": false,
      "EnaSupport": false,
      "RootDeviceName": "/dev/sda",
      "SecurityGroups": [
        {
          "GroupName": "default",
          "GroupId": "s.security group id"
        }
      ],
      "SourceDestCheck": false,
      "CpuOptions": {
        "CoreCount": 2,
        "ThreadsPerCore": 1
      }
    }
  ],
  "ReservationId": "s.r-80c8ee6b041b29eb4"
},
]
```

```
}
```

Führen Sie die Instanz aus.

```
aws ec2 run-instances --image-id s.ami id \--instance-type snc1.medium --endpoint  
http://${snowcone_ip}:8008
```

Example Beispielausgabe

```
{  
  "Instances": [  
    {  
      "AmiLaunchIndex": 0,  
      "ImageId": "s.ami-0623310b494365cc5",  
      "InstanceId": "s.i-80c8ee6b041b29eb4",  
      "InstanceType": "snc1.medium",  
      "State": {  
        "Code": 0,  
        "Name": "pending"  
      },  
      "EbsOptimized": false,  
      "EnaSupport": false,  
      "RootDeviceName": "/dev/sda",  
      "SecurityGroups": [  
        {  
          "GroupName": "default",  
          "GroupId": "s.sg-80c8ee6b041b29eb4"  
        }  
      ],  
      "SourceDestCheck": false,  
      "CpuOptions": {  
        "CoreCount": 2,  
        "ThreadsPerCore": 1  
      }  
    }  
  ],  
  "ReservationId": "s.r-80c8ee6b041b29eb4"  
}
```

## NFS starten und Zugriff einschränken

### 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, NFS-Speicher Amazon EBS neu zuzuweisen, auch wenn der NFS-Service beendet ist.

### Note

Der verfügbare Speicherplatz auf dem Snowcone-Gerät ist erst korrekt, wenn der NFS-Dienst gestartet wird.

Sie können CIDR-Blöcke für IP-Adressbereiche bereitstellen, die zum Mounten der vom Gerät offengelegten NFS-Freigaben berechtigt sind. z. B. `10.0.0.0/16`. Wenn Sie keine zulässigen CIDR-Blöcke angeben, werden alle Mount-Anforderungen abgelehnt.

Daten, die über NFS übertragen werden, werden bei der Übertragung nicht verschlüsselt.

Abgesehen von den durch CIDR-Blöcken zugelassenen Hosts bietet Snowcone keinen Authentifizierungs- oder Autorisierungsmechanismus für die NFS-Shares.

Starten Sie NFS mit dem Befehl `snowballEdge start-service` Um die Service-ID für den NFS-Dienst 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 S3-Buckets einschränken und sehen, welche Einschränkungen derzeit gelten. Sie tun dies, indem Sie CIDR-Blöcke für zugelassene Hosts zuweisen, die auf Ihre Dateifreigabe und Ihre S3-Buckets zugreifen können, wenn Sie den NFS-Service starten.

Verwendung (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-Freigaben, wenn NFS ausgeführt wird

Sie können den Zugriff auf Ihre Dateifreigaben und Daten in Ihren Amazon S3 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 Ihre S3-Buckets zugreifen können, wenn Sie den NFS-Dienst starten. Nachfolgend finden Sie ein Beispielbefehl.

Verwendung (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 zu sehen.

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

## Den Exportpfad für einen Amazon S3 S3-Bucket abrufen

Es gibt keinen speziellen Snowcone-Befehl zum Abrufen des Exportpfads eines Amazon S3 S3-Buckets. Das Format des Exportpfads sieht wie folgt aus.

```
/buckets/bucket-name.
```

## Debugging für lokale AWS Operatoren aktivieren

- `enable-local-aws-operator-debugging`— Aktiviert das Gerät für das Debuggen durch lokales AWS Bedienpersonal, indem der SSH-Port 22 geöffnet wird.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge enable-local-aws-operator-debugging
```

## Debugging für lokale Operatoren AWS deaktivieren

- `disable-local-aws-operator-debugging`— Deaktiviert das Gerät für das Debugging durch lokales AWS Bedienpersonal, indem der SSH-Port 22 geschlossen wird. Standardmäßig ist der SSH-Port 22 geschlossen. Wenn das Snowcone-Gerät ausgeschaltet oder neu gestartet wird, ist das Debugging für den lokalen AWS Bediener deaktiviert.

Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge disable-local-aws-operator-debugging
```

## Eine direkte Netzwerkschnittstelle erstellen

- `create-direct-network-interface` — [Erzeugt eine direkte Netzwerkschnittstelle \(DNI\)](#). Erstellt eine direkte Netzwerkschnittstelle zur Verwendung mit Amazon EC2 EC2-Recheninstanzen auf Ihrem Gerät. Sie können die direkten Netzwerkschnittstellen, die auf Ihrem Gerät verfügbar sind, mithilfe des `describe-direct-network-interfaces` Befehls finden.

Verwendung (konfigurierter Snowball Edge-Client)

```
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]
```

## Informationen über eine direkte Netzwerkschnittstelle abrufen

- `describe-direct-network-interface` — Ruft die direkten Netzwerkschnittstellen auf Ihrem Gerät ab. Eine direkte Netzwerkschnittstelle kann verwendet werden, um Netzwerke für Amazon EC2 EC2-Recheninstanzen und -Services auf Ihrem Gerät zu konfigurieren. Mit dem `create-direct-network-interface` Befehl können Sie eine neue direkte Netzwerkschnittstelle erstellen.

## Verwendung (konfigurierter Snowball Edge-Client)

```
describe-direct-network-interfaces [--endpoint endpoint] [--manifest-file manifestFile]
  [--profile profile] [--unlock-code unlockCode]
```

## Aktualisierung einer direkten Netzwerkschnittstelle

- `update-direct-network-interface` — Aktualisiert eine direkte Netzwerkschnittstelle. Verwenden Sie diesen Befehl, um eine direkte Netzwerkschnittstelle zu aktualisieren, die mit Amazon EC2 EC2-Compute-Instances auf Ihrem 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 mit einer Amazon EC2 EC2-Instance verbunden ist, wird die Schnittstelle zunächst getrennt.

## Verwendung (konfigurierter Snowball Edge-Client)

```
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 direkten Netzwerkschnittstelle

- `delete-direct-network-interface`— Löscht eine direkte Netzwerkschnittstelle, die nicht mehr verwendet wird. Um eine direkte Netzwerkschnittstelle zu löschen, die mit Ihrer Amazon EC2 EC2-Compute-Instance verknüpft ist, müssen Sie zuerst die direkte Netzwerkschnittstelle von Ihrer Instance trennen.

## Verwendung (konfigurierter Snowball Edge-Client)

```
delete-direct-network-interface [--direct-network-interface-arn directNetworkInterfaceArn]
  [--endpoint endpoint]
  [--manifest-file manifestFile] [--profile profile] [--unlock-code unlockCode]
```

## Funktionsstatus wird überprüft

Verwenden Sie den `describe-features` Befehl, um den Status der auf Ihrem Gerät verfügbaren Funktionen aufzulisten AWS Snow Device Management, einschließlich der Funktionen, mit denen Sie Ihr Snowcone-Gerät und lokale AWS Dienste aus der Ferne verwalten können.

`RemoteManagementState` zeigt den Status von Snow Device Management an und gibt einen der folgenden Zustände zurück:

- `INSTALLED_ONLY`— Die Funktion ist installiert, aber nicht aktiviert.
- `INSTALLED_AUTOSTART`— Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu ihrer herzustellen AWS-Region, wenn es eingeschaltet ist.
- `NOT_INSTALLED`— Das Gerät unterstützt die Funktion nicht oder war vor der Markteinführung bereits im Einsatz.

### Verwendung (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
}
```

## Funktionsstatus ändern

Verwenden Sie den `set-features` Befehl, um den Status der auf Ihrem AWS Snowcone Gerät verfügbaren Funktionen zu ändern. Verwenden Sie den `--remote-management-state` Parameter AWS Snow Device Management, um Ihr Snowcone-Gerät und lokale Dienste aus der Ferne zu aktivieren oder zu deaktivieren, sodass Sie Ihr Snowcone-Gerät und lokale AWS Dienste remote verwalten können. Das Gerät muss entsperrt sein, bevor Sie diesen Befehl ausführen können.



Sie können Snow Device Management auf die folgenden Zustände einstellen:

- **INSTALLED\_ONLY**— Die Funktion ist installiert, aber nicht aktiviert.
- **INSTALLED\_AUTOSTART**— Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu ihrer herzustellen AWS-Region , wenn es eingeschaltet ist.

#### Note

Der **NOT\_INSTALLED** Status dient nur zur Identifizierung von Geräten, die Snow Device Management nicht unterstützen oder die vor der Markteinführung bereits im Einsatz waren. Es ist nicht möglich, die Funktion auf Geräten zu installieren oder zu deinstallieren, die bereits bereitgestellt wurden. Um Snow Device Management verwenden zu können, müssen Sie ein neues Gerät bestellen, auf dem die Funktion vorinstalliert ist.

## Verwendung (konfigurierter Snowball Edge-Client)

```
snowballEdge set-features
--remote-management-state INSTALLED_AUTOSTART
--manifest-file ./JID2bf11d5a-fict-414a-b5b1-3bf7e6a6e83d_manifest.bin
--unlock-code 73bb0-f8ke1-69a4a-f4288-4f88d
--endpoint https://10.0.0.25
```

## Beispielausgabe

```
{
  "RemoteManagementState" : "INSTALLED_AUTOSTART"
}
```

## Zeitserver einrichten

Sie können einen externen NTP-Server (Network Time Protocol) einrichten. Sie können die NTP-CLI-Befehle verwenden, wenn sich das Gerät sowohl im gesperrten als auch im entsperrten Zustand befindet. Das Manifest und der 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 verwenden können AWS Snowcone.

Es liegt in Ihrer Verantwortung, einen sicheren NTP-Zeitserver bereitzustellen. Verwenden Sie den `update-time-servers` CLI-Befehl, um festzulegen, mit welchen NTP-Zeitservern das Gerät eine Verbindung herstellt.

### Note

Der `update-time-servers` Befehl überschreibt die vorherigen NTP-Zeitserver-Einstellungen.

## Usage

```
snowballEdge update-time-servers time.google.com
```

## Example Beispielausgabe

```
Updating time servers now.
```

## Zeitquellen werden überprüft

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 der Zeitquellenstatus zurück. Jeder Zeitquellenstatus enthält die Stratum Felder `Address`, `State`, `Type`, und `Stratum`. Im Folgenden sind die Bedeutungen dieser Felder aufgeführt.

- **Address**— Der DNS-Name/die IP-Adresse der Zeitquelle.
- **State**— Der aktuelle Verbindungsstatus zwischen dem Gerät und dieser Zeitquelle. Es gibt fünf mögliche Zustände:
  - **CURRENT**— Die Zeitquelle wird derzeit verwendet, um die Zeit zu synchronisieren.
  - **COMBINED**— Die Zeitquelle wird mit der aktuellen Quelle kombiniert.
  - **EXCLUDED**— Die Zeitquelle wird durch den Kombinationsalgorithmus ausgeschlossen.
  - **LOST**— Die Verbindung mit der Zeitquelle wurde unterbrochen.
  - **UNACCEPTABLE**— Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder als Falschticker oder als zu stark variabel eingestuft wurde.
- **Type**— Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Server können mit dem `update-time-servers` Befehl festgelegt werden. Peers können nur andere Snowball Edge-Geräte im Cluster sein und werden automatisch eingerichtet, wenn der Cluster verknüpft wird.
- **Stratum**— Dieses Feld zeigt das Stratum der Quelle. Stratum 1 weist auf eine Quelle mit einer lokal angeschlossenen Referenzuhr hin. Eine Quelle, die mit einer Stratum-1-Quelle synchronisiert ist, befindet sich in Stratum 2. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert ist, befindet sich in Stratum 3 usw.

Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Ein Server kann vom Benutzer mit dem `update-time-servers` Befehl eingerichtet werden, wohingegen ein Peer nur andere Snowball Edge-Geräte im Cluster sein kann. 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 eine Schicht von 10, während der Server eine Schicht von 1 hat. Daher wird der Server als aktuelle Zeitquelle ausgewählt.

# AWS Snow Device Management Zur Verwaltung von Geräten verwenden

AWS Snow Device Management ermöglicht es Ihnen, Ihr Snow Family-Gerät und lokale AWS Dienste aus der Ferne zu verwalten. Alle Snow Family-Geräte unterstützen Snow Device Management und es ist auf den meisten Geräten, auf AWS-Regionen denen Snow Family-Geräte verfügbar sind, auf neuen Geräten installiert.

Mit Snow Device Management können Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine Aufgabe
- Überprüfen Sie den Aufgabenstatus
- Überprüfen Sie die Metadaten der Aufgabe
- Stornieren Sie eine Aufgabe
- Überprüfen Sie die Geräteinformationen
- Überprüfen Sie den Status der Amazon EC2-kompatiblen Instanz
- Befehle und Syntax auflisten
- Listet Geräte auf, die per Fernzugriff verwaltet werden können
- Listet den Aufgabenstatus geräteübergreifend auf
- Verfügbare Ressourcen auflisten
- Aufgaben nach Status auflisten
- Geräte- oder Aufgaben-Tags auflisten
- Schlagworte anwenden
- Tags entfernen

## Themen

- [Auswahl des Status „Snow Device Management“ bei der Bestellung eines Snow Family-Geräts](#)
- [Snow Device Management aktivieren](#)
- [Hinzufügen von Berechtigungen für Snow Device Management zu einer IAM-Rolle](#)
- [CLI-Befehle für Snow Device Management](#)

# Auswahl des Status „Snow Device Management“ bei der Bestellung eines Snow Family-Geräts

Wenn Sie einen Auftrag zur Bestellung eines Snow-Geräts erstellen, können Sie wählen, in welchem Status sich Snow Device Management befinden soll, wenn Sie das Gerät erhalten: installiert, aber nicht aktiviert oder installiert und aktiviert. Wenn es installiert, aber nicht aktiviert ist, müssen Sie den Snowball Edge-Client verwenden AWS OpsHub , um es zu aktivieren, bevor Sie es verwenden können. Wenn es installiert und aktiviert ist, können Sie Snow Device Management verwenden, nachdem Sie das Gerät erhalten und es mit Ihrem lokalen Netzwerk verbunden haben. Sie können den Status „Snow Device Management“ wählen, wenn Sie einen Auftrag erstellen Managementkonsole für die AWS Snow-Familie, um ein Gerät über den Snowball Edge-Client AWS CLI, die oder die Snow Job Management API zu bestellen.

Um den Status „Snow Device Management“ aus dem Managementkonsole für die AWS Snow-Familie

1. Um festzulegen, dass Snow Device Management installiert und aktiviert werden soll, wählen Sie Ihr Snow-Gerät remote mit AWS OpsHub oder Snowball-Client verwalten.
2. Wenn Sie festlegen möchten, dass Snow Device Management installiert, aber nicht aktiviert wird, wählen Sie Ihr Snow-Gerät nicht remote mit AWS OpsHub oder dem Snowball-Client verwalten aus.

Weitere Informationen finden Sie unter [Schritt 3: Wählen Sie Ihre Funktionen und Optionen](#) in diesem Handbuch.

So wählen Sie den Status „Snow Device Management“ über die AWS CLI Snowball Edge-Client- oder Snow-Job-Management-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 dies der Standardwert.

Example der Syntax des **remote-management** Parameters des **create-job** Befehls

```
aws snowball create-job \
  --job-type IMPORT \
  --remote-management INSTALLED_AUTOSTART \
  --device-configuration '{"SnowconeDeviceConfiguration": {"WirelessConnection":
{"IsWifiEnabled": false} } }' \
  --resources '{"S3Resources":[{"BucketArn":"arn:aws:s3:::bucket-name"}]}' \
  --description "Description here" \
  --address-id 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 unter [Job Management API Reference](#) in der AWS Snowball API-Referenz.

## Snow Device Management aktivieren

Gehen Sie wie folgt vor, um Snow Device Management mit dem Snowball Edge-Client zu aktivieren.

Bevor Sie dieses Verfahren verwenden, gehen Sie wie folgt vor:

- Laden Sie die neueste Version des Snowball Edge-Clients herunter und installieren Sie sie. Weitere Informationen finden Sie unter [Snowball-Client herunterladen und installieren](#).
- Laden Sie die Manifestdatei herunter und holen Sie sich den Entsperrcode für das Snow Family-Gerät. Weitere Informationen finden Sie unter [Zugangsdaten und Tools abrufen](#).
- Connect das Snow Family-Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter [AWS Snowcone Gerätespezifikationen](#) für .
- Entsperren Sie das Snow Family-Gerät. Weitere Informationen finden Sie unter Lokales [Entsperren eines Geräts](#).

```
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 auf AWS-Konto dem Gerät, über das das Gerät bestellt wurde, eine AWS Identity and Access Management (IAM-) Rolle und fügen Sie der Rolle die folgende Richtlinie hinzu. Weisen Sie die Rolle dann dem IAM-Benutzer zu, der sich anmeldet, um Ihr Gerät mit 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 AWS CLI werden die Befehle beschrieben, mit denen Sie Ihre Snow Family-Geräte mit Snow Device Management remote verwalten können. Sie können einige Fernverwaltungsaufgaben auch mit ausführen AWS OpsHub for Snow Family. Weitere Informationen finden Sie unter [AWS Dienste auf Ihrem Gerät](#) verwalten.

### Note

Stellen Sie vor der Verwaltung Ihres Geräts sicher, dass es eingeschaltet und mit Ihrem Netzwerk verbunden ist und eine Verbindung zu dem Gerät herstellen kann, auf AWS-Region dem es bereitgestellt wurde.

### Themen

- [Erstellen Sie eine Aufgabe](#)
- [Überprüfen Sie den Aufgabenstatus](#)
- [Überprüfen Sie die Geräteinformationen](#)
- [Überprüfen Sie den Status der Amazon EC2-kompatiblen Instanz](#)
- [Überprüfen Sie die Metadaten der Aufgabe](#)
- [Eine Aufgabe stornieren](#)
- [Befehle und Syntax auflisten](#)
- [Geräte auflisten, die per Fernzugriff verwaltet werden können](#)
- [Den Aufgabenstatus geräteübergreifend auflisten](#)
- [Verfügbare Ressourcen auflisten](#)
- [Geräte- oder Aufgaben-Tags auflisten](#)
- [Aufgaben nach Status auflisten](#)

- [Tags anwenden](#)
- [Tags entfernen](#)

## Erstellen Sie eine 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 zusammen mit dem `--targets` Parameter bereitstellen, und geben die Aufgaben an, die mit dem Parameter ausgeführt werden sollen. `--command` Auf einem Gerät kann jeweils nur ein einziger Befehl ausgeführt werden.

Unterstützte Befehle:

- `unlock`(keine Argumente)
- `reboot`(keine Argumente)

Verwenden Sie den folgenden Befehl, um eine Aufgabe zu erstellen, die von den Zielgeräten ausgeführt werden soll. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

```
aws snow-device-management create-task
--targets smd-fictbgr3rbcjeqa5
--command reboot={}
```

Ausnahmen

```
ValidationException
ResourceNotFoundException
InternalServerError
ThrottlingException
AccessDeniedException
ServiceQuotaExceededException
```

Ausgabe

```
{
  "taskId": "st-ficthmqoc2pht111",
  "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
cjkwhmqoc2pht111"
}
```

## Überprüfen Sie den 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-ficthmqoc2pht1ef \
--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 Sie die Geräteinformationen

Verwenden Sie den Befehl, um gerätespezifische Informationen wie Gerätetyp, Softwareversion, IP-Adressen und Sperrstatus zu überprüfen. `describe-device` Die Ausgabe umfasst außerdem Folgendes:

- `lastReachedOutAt`— Wann das Gerät das letzte Mal Kontakt mit dem aufgenommen hat AWS Cloud. Zeigt an, dass das Gerät online ist.
- `lastUpdatedAt`— Wann die Daten auf dem Gerät zuletzt aktualisiert wurden. Zeigt an, wann der Gerätecache aktualisiert wurde.

Verwenden Sie den folgenden Befehl, um die Geräteinformationen zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

### Befehl

```
aws snow-device-management describe-device \  
--managed-device-id smd-fictqic6gcldf111
```

### Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## 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 Sie den Status der Amazon EC2-kompatiblen Instanz

Verwenden Sie den `describe-ec2-instances` Befehl, um den aktuellen Status der Amazon EC2 EC2-Instance zu überprüfen. Die Ausgabe ähnelt der des `describe-device` Befehls, die Ergebnisse stammen jedoch aus dem Geräte-Cache im AWS Cloud und enthalten eine Teilmenge der verfügbaren Felder.

Verwenden Sie den folgenden Befehl, um den Status der Amazon EC2-kompatiblen Instance zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

## Befehl

```
aws snow-device-management describe-device-ec2-instances \  
--managed-device-id smd-fictbgr3rbcje111 \  
--instance-ids s.i-84fa8a27d3e15e111
```

## Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## Ausgabe

```
{  
  "instances": [  
    {  
      "instance": {  
        "amiLaunchIndex": 0,  
        "blockDeviceMappings": [  
          {  
            "deviceName": "/dev/sda",  
            "ebs": {  
              "attachTime": "2021-07-23T15:25:38.719000-07:00",  
              "deleteOnTermination": true,  
              "status": "ATTACHED",  
              "volumeId": "s.vol-84fa8a27d3e15e111"  
            }  
          }  
        ],  
        "cpuOptions": {  
          "coreCount": 1,  
          "threadsPerCore": 1  
        }  
      }  
    }  
  ]  
}
```

```
    },
    "createdAt": "2021-07-23T15:23:22.858000-07:00",
    "imageId": "s.ami-03f976c3cadaa6111",
    "instanceId": "s.i-84fa8a27d3e15e111",
    "state": {
      "name": "RUNNING"
    },
    "instanceType": "snc1.micro",
    "privateIpAddress": "34.223.14.193",
    "publicIpAddress": "10.111.60.160",
    "rootDeviceName": "/dev/sda",
    "securityGroups": [
      {
        "groupId": "s.sg-890b6b4008bdb3111",
        "groupName": "default"
      }
    ],
    "updatedAt": "2021-07-23T15:29:42.163000-07:00"
  },
  "lastUpdatedAt": "2021-07-23T15:29:58.
071000-07:00"
}
]
}
```

## Überprüfen Sie die Metadaten der Aufgabe

Verwenden Sie den `describe-task` Befehl, um die Metadaten für eine bestimmte Aufgabe auf einem Gerät zu überprüfen. Die Metadaten für eine Aufgabe umfassen die folgenden Elemente:

- Die Zielgeräte
- Der Status der Aufgabe
- Wann die Aufgabe erstellt wurde
- Wann wurden die Daten auf dem Gerät zuletzt aktualisiert
- Wann wurde die Aufgabe abgeschlossen
- Die Beschreibung (falls vorhanden), die bei der Erstellung der Aufgabe angegeben wurde

Verwenden Sie den folgenden Befehl, um die Metadaten einer Aufgabe zu überprüfen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.



## Befehl

```
aws snow-device-management describe-task \  
--task-id st-ficthmqoc2pht111
```

## Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## Ausgabe

```
{  
  "completedAt": "2021-07-22T15:29:46.758000+00:00",  
  "createdAt": "2021-07-22T15:28:42.613000+00:00",  
  "lastUpdatedAt": "2021-07-22T15:29:46.758000+00:00",  
  "state": "COMPLETED",  
  "tags": {},  
  "targets": [  
    "smd-fictbgr3rbcje111"  
  ],  
  "taskId": "st-ficthmqoc2pht111",  
  "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-ficthmqoc2pht111"  
}
```

## Eine Aufgabe stornieren

Verwenden Sie den `cancel-task` Befehl, um eine Stornierungsanfrage für eine bestimmte Aufgabe zu senden. Sie können nur Aufgaben in dem `QUEUED` Status stornieren, die noch nicht ausgeführt wurden. Aufgaben, die bereits ausgeführt werden, können nicht storniert werden.

**Note**

Eine Aufgabe, die Sie abbrechen möchten, wird möglicherweise trotzdem ausgeführt, wenn sie aus der Warteschlange bearbeitet wird, bevor der `cancel-task` Befehl den Status der Aufgabe ändert.

Verwenden Sie den folgenden Befehl, um eine Aufgabe abzubrechen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

**Befehl**

```
aws snow-device-management cancel-task \  
--task-id st-ficthmqoc2pht111
```

**Ausnahmen**

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

**Ausgabe**

```
{  
  "taskId": "st-ficthmqoc2pht111"  
}
```

**Befehle und Syntax auflisten**

Verwenden Sie den `help` Befehl, um eine Liste aller unterstützten Befehle für die Snow Device Management API zurückzugeben. Sie können den `help` Befehl auch verwenden, um detaillierte Informationen zu und die Syntax für einen bestimmten Befehl zurückzugeben.

Verwenden Sie den folgenden Befehl, um alle unterstützten Befehle aufzulisten.

#### Befehl

```
aws snow-device-management help
```

Verwenden Sie den folgenden Befehl, um detaillierte Informationen und die Syntax für einen Befehl zurückzugeben. *command* Ersetzen Sie ihn durch den Namen des Befehls, an dem Sie interessiert sind.

#### Befehl

```
aws snow-device-management command help
```

## Geräte auflisten, die per Fernzugriff verwaltet werden können

Verwenden Sie den Befehl, um eine Liste aller Geräte in Ihrem Konto zurückzugeben, auf denen Snow Device Management aktiviert ist, auf AWS-Region denen der Befehl ausgeführt wird. `list-devices --max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um Geräte aufzulisten, die per Fernzugriff verwaltet werden können. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

#### Befehl

```
aws snow-device-management list-devices \  
--max-results 10
```

#### Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException
```

```
AccessDeniedException
```

## Ausgabe

```
{
  "devices": [
    {
      "associatedWithJob": "ID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",
      "managedDeviceId": "smd-fictbgr3rbcjeqa5",
      "managedDeviceArn": "arn:aws:snow-device-management:us-
west-2:000000000000:managed-device/smd-fictbgr3rbcje111"
      "tags": {}
    }
  ]
}
```

## Den Aufgabenstatus geräteübergreifend auflisten

Verwenden Sie den `list-executions` Befehl, um den Status von Aufgaben für ein oder mehrere Zielgeräte zurückzugeben. Verwenden Sie den `--state` Parameter, um die Rückgabeliste so zu filtern, dass Aufgaben angezeigt werden, die sich derzeit in einem bestimmten Status befinden. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Eine Aufgabe kann einen der folgenden Status haben:

- QUEUED
- IN\_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED\_OUT

Verwenden Sie den folgenden Befehl, um den Aufgabenstatus geräteübergreifend aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

## Befehl

```
aws snow-device-management list-executions \  
--taskId st-ficthmqoc2pht1ef \  
--state SUCCEEDED \  
--max-results 10
```

## Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## Ausgabe

```
{  
  "executions": [  
    {  
      "executionId": "1",  
      "managedDeviceId": "smd-fictbgr3rbcje111",  
      "state": "SUCCEEDED",  
      "taskId": "st-ficthmqoc2pht111"  
    }  
  ]  
}
```

## Verfügbare Ressourcen auflisten

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-kompatible Instances der einzige unterstützte Ressourcentyp. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um die verfügbaren Ressourcen für ein Gerät aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

## Befehl

```
aws snow-device-management list-device-resources \  
--managed-device-id smd-fictbgr3rbcje111 \  
--type AWS::EC2::Instance \  
--next-  
token YAQGPwAT9L3wVKaGYjt4yS34MiQLWvzcShe9oIeDJr05AT4rXSprqcqQhhBEYRfcerAp0YYbJmRT= \  
--max-results 10
```

## Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## Ausgabe

```
{  
  "resources": [  
    {  
      "id": "s.i-84fa8a27d3e15e111",  
      "resourceType": "AWS::EC2::Instance"  
    }  
  ]  
}
```

## Geräte- oder Aufgaben-Tags auflisten

Verwenden Sie den `list-tags-for-resource` Befehl, um eine Liste von Tags für ein verwaltetes Gerät oder eine verwaltete Aufgabe zurückzugeben.

Verwenden Sie den folgenden Befehl, um die Tags für ein Gerät aufzulisten. Ersetzen Sie das Beispiel Amazon Resource Name (ARN) durch den ARN für Ihr Gerät.

## Befehl

```
aws snow-device-management list-tags-for-resource
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/
smd-fictbgr3rbcjeqa5
```

## Ausnahmen

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

## Ausgabe

```
{
  "tags": {
    "Project": "PrototypeA"
  }
}
```

## Aufgaben nach Status auflisten

Verwenden Sie den `list-tasks` Befehl, um eine Liste der Aufgaben von den Geräten in der AWS Region zurückzugeben, in der der Befehl ausgeführt wird. Verwenden Sie den `--state` Parameter `IN_PROGRESS`, um die Ergebnisse nach `COMPLETED`, oder `CANCELED` Status zu filtern. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im "Benutzerhandbuch für die AWS Befehlszeilenschnittstelle".

Verwenden Sie den folgenden Befehl, um Aufgaben nach Status aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

## Befehl

```
aws snow-device-management list-tasks \
--state IN_PROGRESS \
--next-token K8VAMqKiP2Cf4xGkmH8GMyZrg0F8FUb+d10KTP9+P4pUb+8PhW+6MiXh4= \
```

```
--max-results 10
```

## Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

## Ausgabe

```
{  
  "tasks": [  
    {  
      "state": "IN_PROGRESS",  
      "tags": {},  
      "taskId": "st-ficthmqoc2phtlef",  
      "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-  
ficthmqoc2phtlef"  
    }  
  ]  
}
```

## Tags anwenden

Verwenden Sie den `tag-resource` Befehl, um ein Tag für ein Gerät oder für eine Aufgabe auf einem Gerät hinzuzufügen oder zu ersetzen. Der `--tags` Parameter akzeptiert eine durch Kommas getrennte Liste von `Key=Value` Paaren.

Verwenden Sie den folgenden Befehl, um Tags auf ein Gerät anzuwenden. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

### Befehl

```
aws snow-device-management tag-resource \  
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/  
smd-fictbgr3rbcjeqa5 \  

```



```
--tags Project=PrototypeA
```

## Ausnahmen

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

## Tags entfernen

Verwenden Sie den `untag-resources` Befehl, um ein Tag von einem Gerät oder von einer Aufgabe auf einem Gerät zu entfernen.

Verwenden Sie den folgenden Befehl, um Tags von einem Gerät zu entfernen. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

### Befehl

```
aws snow-device-management untag-resources \  
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/  
smd-fictbgr3rbcjeqa5 \  
--tag-keys Project
```

## Ausnahmen

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

# AWS Dienste verwenden auf AWS Snowcone

Im Folgenden finden Sie eine Übersicht über das AWS Snowcone Gerät. AWS Snowcone ist ein physisch robustes Gerät, das durch AWS Key Management Service (AWS KMS) geschützt ist und das Sie für lokale Speicherung und Datenverarbeitung oder für die Übertragung von Daten zwischen Ihren lokalen Servern und Amazon Simple Storage Service (Amazon S3) verwenden können.

Informationen zum Entsperren eines AWS Snowcone Geräts finden Sie unter [Den AWS Snowball Edge Client verwenden](#)

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 uns [AWS Support](#), damit Ihnen ein neues Gerät zugeschickt wird.

Sobald Ihr Gerät eingetroffen und eingeschaltet ist, können Sie es verwenden.

## Themen

- [Verwenden von Amazon EC2-kompatiblen Recheninstanzen](#)
- [Zum AWS DataSync Übertragen von Dateien verwenden](#)
- [Verwaltung der NFS-Schnittstelle](#)
- [Wird verwendet AWS IoT Greengrass , um vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen](#)
- [Für die Nutzung von AWS Diensten auf einem AWS Snowcone Gerät erforderliche Ports](#)

# Verwenden von Amazon EC2-kompatiblen Recheninstanzen

In diesem Thema finden Sie einen Überblick über die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) -Recheninstanzen auf einem AWS Snowcone Gerät. Das Thema enthält konzeptionelle Informationen, Verfahren und Beispiele.

**Note**

Diese Funktionen werden im asiatisch-pazifischen Raum (Mumbai) AWS-Region nicht unterstützt.

## Übersicht

Sie können Amazon EC2-kompatible Compute-Instances, die auf einem Snowcone gehostet werden, mit den unterstützten EC2-kompatiblen Instance-Typen ausführen. Wie ihre cloudbasierten Pendanten benötigen diese Instances Amazon-Systemabbilder (Amazon Machine Images, AMIs) zum Starten. Sie wählen das AMI als Basis-Image für eine Instanz in der Cloud aus, bevor Sie Ihren Snowcone-Job erstellen. Weitere Informationen zu unterstützten Instance-Typen finden Sie unter [Amazon EC2 auf Snowcone verwenden](#).

Wenn es sich bei dem Auftragstyp um lokale Datenverarbeitung handelt, können Sie insgesamt 8 TiB lokale EBS-Volumes erstellen und diese an Amazon EC2-kompatible Instances anhängen. Dadurch können lokale EC2-kompatible Instances auf mehr lokale Kapazität zugreifen als auf das Root-Volume allein. Dies ist nur lokaler Speicher, sodass auf die EBS-Volumes geschriebene Daten verloren gehen, wenn das Gerät zurückgegeben wird, AWS da sie nicht in Amazon S3 importiert werden können.

**Note**

Der NFS-Server ist für Rechenaufträge nicht verfügbar. Wenn Sie Daten in oder aus dem importieren oder exportieren müssen AWS Cloud, wählen Sie bei der Bestellung nicht den lokalen Rechenauftragstyp.

Um eine Compute-Instance auf einem Snowcone zu verwenden, erstellen Sie einen Job, um ein Snow Family-Gerät zu bestellen, und geben Sie Ihre AMIs an. Sie können dies über das [Managementkonsole für die AWS Snow-Familie](#), mit dem AWS CLI oder mit einem der AWS SDKs tun. In der Regel müssen Sie einige Voraussetzungen für die Verwaltung erfüllen, bevor Sie Ihren Job erstellen, um Ihre Instances verwenden zu können.

Wenn Ihr Gerät eingetroffen ist, können Sie mit der Verwaltung Ihrer AMIs und Instances beginnen. Sie können Ihre Compute-Instances auf einem Snowcone über einen Amazon EC2-kompatiblen Endpunkt verwalten. Dieser Endpunkttyp unterstützt viele der Amazon EC2 EC2-CLI-Befehle und -

Aktionen für die AWS SDKs. Sie verwenden das AWS OpsHub for Snow Family Tool, um Ihre AMIs, Compute-Instances und AWS Services zu verwalten. Weitere Informationen finden Sie unter [AWS OpsHub for Snow Family Zur Verwaltung von Geräten verwenden](#).

Wenn Sie mit Ihrem Gerät fertig sind, geben Sie es an zurück AWS. Wenn das Gerät in einem Importauftrag verwendet wurde, werden die über die NFS-Schnittstelle übertragenen Daten in Amazon S3 importiert. Andernfalls löschen wir das Gerät vollständig, wenn es zurückgegeben wird. AWS Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

#### Important

- Die Verwendung verschlüsselter AMIs auf Snowcone-Geräten wird nicht unterstützt.
- Daten in Compute-Instances, die auf einem Snowcone laufen, werden nicht importiert AWS.

## Preise für Compute-Instances auf Snowcone

Die Verwendung von Datenverarbeitungs-Instances verursacht zusätzliche Kosten. Weitere Informationen finden Sie unter [AWS Snowcone Preise](#).

## Voraussetzungen

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

- Bevor Sie Ihrem Job AMIs hinzufügen können, müssen Sie über ein AMI verfügen AWS-Konto, und es muss sich um einen unterstützten Image-Typ handeln. Derzeit basieren unterstützte AMIs auf den folgenden Betriebssystemen:
  - [Amazon Linux 2](#)

#### Note

Die neueste Version dieses AMI wird zu dem Zeitpunkt bereitgestellt, zu dem Ihr Snow Family-Gerät für den Versand vorbereitet wird AWS. Informationen zum Ermitteln der Version dieses AMI auf dem Gerät, wenn Sie es erhalten, finden Sie unter [Ermitteln der Version des Amazon Linux 2 AMI für Snow Family](#).

- [CentOS 7 \(x86\\_64\) - mit Updates HVM](#)
- [Ubuntu 16.04 LTS - Xenial \(HVM\), Ubuntu 20.04 LTS - Focal oder Ubuntu 22.04 LTS - Jammy](#)

#### Note

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

Sie erhalten diese Images über das [AWS Marketplace](#).

Bevor Sie Ihrer Anfrage zur Auftragserstellung AMIs hinzufügen, stellen Sie sicher, dass Sie über mindestens ein unterstütztes AMIs verfügen. AWS-Konto

- Alle AMIs müssen auf Amazon Elastic Block Store (Amazon EBS) mit einem einzigen Volume basieren.
- Wenn Sie eine Verbindung zu einer Compute-Instance herstellen möchten, die auf einem Snowcone läuft, müssen Sie Secure Shell (SSH) verwenden. Hierzu müssen Sie zunächst das Schlüsselpaar hinzufügen.

## Anlegen eines Auftrags mit Datenverarbeitungs-Instances

In diesem Abschnitt erstellen Sie Ihren ersten Datenverarbeitungs-Instance-Auftrag.

#### Important

Beachten Sie die folgenden Punkte, bevor Sie Ihren Auftrag anlegen:

- Wenn Sie ein AMI von verwenden möchten, stellen Sie sicher AWS Marketplace, dass es über einen unterstützten Produktcode und einen Code für den Verwendungsvorgang verfügt. Weitere Informationen finden Sie unter [Überprüfung der Produkt- und Nutzungsoptionscodes für AMIs AWS Marketplace](#).
- Stellen Sie sicher, dass die Ihrem AMI zugeordneten vCPU-, Arbeitsspeicher- und Datenspeicherungswerte mit dem Typ der zu erstellenden Instance übereinstimmen.
- Wenn Sie SSH verwenden möchten, um sich mit der Instance zu verbinden, nachdem Sie die Instance auf Ihrem Snowcone gestartet haben, müssen Sie zunächst das folgende Verfahren ausführen.

- Die Verwendung verschlüsselter AMIs oder verschlüsselter Amazon EBS-Volumes auf AWS Snowcone Geräten wird nicht unterstützt.

## Überprüfung der Produkt- und Nutzungsoptionscodes für AMIs AWS Marketplace

Bevor Sie mit dem Hinzufügen eines AMI AWS Marketplace zu Ihrem Snow Family-Gerät beginnen, stellen Sie sicher, dass die Produkt- und Verwendungscodes des AMI in Ihrem unterstützten 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 von der aus Sie den Auftrag zur Bestellung des Snow Family-Geräts erstellen. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
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. Um beispielsweise alle Linux-AMIs aufzulisten, die bereitgestellt werden AWS, wählen Sie Öffentliche Images aus. Nutzen Sie dann die Optionen von Search (Suche), um die Liste der angezeigten AMIs weiter anzupassen.

(Neue Konsole) Wählen Sie in der Suchleiste aus dem Menü die Option Owner-Alias, dann den Operator = und anschließend den Wert amazon aus. Wählen Sie wiederum in der Suchleiste Platform (Plattform), dann den Operator = aus. Klicken Sie dann auf das Betriebssystem in der Liste.

(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. Wählen Sie (wieder in der Search bar (Suchleiste)) den Punkt Platform (Plattform) aus. Klicken Sie dann auf das Betriebssystem in der Liste.

### 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 Bildübersicht des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der Tabelle unten.

 Note

Der Produktcode avyfzznywektkgl5qv5f57ska wird in allen Regionen unterstützt.

#### 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	a8jyyfnf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkkjt189a13aqe

7. Stellen Sie für alle Regionen sicher, dass der Operationscode „Nutzung“ lautet. RunInstances

#### Ermitteln 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 im AWS Command Line Interface Benutzerhandbuch unter Installation oder Aktualisierung AWS CLI auf die neueste Version von.](#)

- Verwenden Sie den `describe-images` AWS CLI Befehl, um die Beschreibung des AMI anzuzeigen. Die Version ist in der Beschreibung enthalten. Stellen Sie das Public-Key-Zertifikat aus dem vorherigen Schritt bereit. Weitere Informationen finden Sie unter [describe-images](#) in der AWS CLI Befehlsreferenz.

```
aws ec2 describe-images --endpoint http://snow-device-ip:8008 --region snow
```

## Example der Ausgabe des Befehls **describe-images**

```
{
  "Images": [
    {
      "CreationDate": "2024-02-12T23:24:45.705Z",
      "ImageId": "s.ami-02ba84cb87224e16e",
      "Public": false,
      "ProductCodes": [
        {
          "ProductCodeId": "avyfzzywekktgl5qv5f57ska",
          "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 ist im Wert des Description Namens enthalten.

## Konfigurieren eines AMI zur Verwendung von SSH zum Herstellen einer Verbindung mit auf dem Gerät gestarteten Datenverarbeitungs-Instances

Um Secure Shell (SSH) zu verwenden, um eine Verbindung zu Ihren Recheninstanzen auf Snowcone-Geräten herzustellen, 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.

So fügen Sie einen SSH-Schlüssel einem AMI hinzu

1. Starten Sie eine neue Instance in dem auf der [Amazon Linux 2 for Snow Family AWS Cloud](#) basierenden [CentOS 7 \(x86\\_64\) — mit Updates HVM oder Ubuntu 16.04 LTS — Xenial \(HVM\)](#) - Image.

Wenn Sie Ihre Instance starten, stellen Sie sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihre spätere Verwendung auf dem Snowcone geeignet ist. In der Amazon EC2 EC2-Konsole tun Sie dies in Schritt 4: Speicher hinzufügen. Eine Liste der unterstützten Größen für Compute-Instance-Speicher-Volumes auf einem Snowcone finden Sie unter [AWS Snowcone Kontingente](#).

2. Installieren und konfigurieren Sie die Anwendungen, die Sie auf dem Snowcone ausführen möchten, und testen Sie, ob sie erwartungsgemäß 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 Snowcone 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 EC2-Benutzerhandbuch.
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 zur Bestellung eines Snow Family-Geräts zu erstellen. Ihr Auftrag kann ein beliebiger Auftragstyp sein, einschließlich eines Clusters. Um das zu verwenden [Managementkonsole für die AWS Snow-Familie](#), folgen Sie den Anweisungen unter [Erste Schritte](#).

## Erstellen Sie Ihren Job 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 snowballEdge 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 SNOWCONE
```

Nachdem Ihr Gerät angekommen ist und Sie es entsperrt haben, verwenden Sie den Snowball Edge-Client, um Ihre lokalen Anmeldeinformationen abzurufen. Weitere Informationen finden Sie unter [Abrufen von Anmeldeinformationen](#).

## Netzwerkconfiguration für Datenverarbeitungs-Instances

Nachdem Sie Ihre Compute-Instances auf einem Snow Family-Gerät gestartet haben, müssen Sie dem Gerät eine IP-Adresse zuweisen, indem Sie eine Netzwerkschnittstelle erstellen. Geräte der Snow Family unterstützen zwei Arten von Netzwerkschnittstellen, eine virtuelle Netzwerkschnittstelle und eine direkte Netzwerkschnittstelle.

### Virtuelle Netzwerkschnittstelle (VNI)

Eine virtuelle Netzwerkschnittstelle ist die Standard-Netzwerkschnittstelle für die Verbindung zu einer EC2-kompatiblen Instanz auf Ihrem Snow Family-Gerät. Sie müssen für jede Ihrer EC2-kompatiblen Instances ein VNI erstellen, unabhängig davon, ob Sie auch eine direkte Netzwerkschnittstelle verwenden oder nicht. Der Datenverkehr, der über ein VNI fließt, wird durch die von Ihnen eingerichteten Sicherheitsgruppen geschützt. Sie können 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 zur Verwaltung des Snow Family-Geräts verwendet wird. Das Erstellen eines VNI auf einer anderen physischen Schnittstelle als der, die für die Geräteverwaltung verwendet wird, kann zu unerwarteten Ergebnissen führen.

## Direkte Netzwerkschnittstelle (DNI)

Eine direkte Netzwerkschnittstelle (DNI) ist eine erweiterte Netzwerkfunktion, die Anwendungsfälle wie Multicast-Streams, transitives Routing und Lastenausgleich ermöglicht. Indem Sie Instances mit Layer-2-Netzwerkzugriff ohne zwischengeschaltete Übersetzung oder Filterung bereitstellen, können Sie mehr Flexibilität bei der Netzwerkkonfiguration Ihres Snow Family-Geräts und eine verbesserte Netzwerkleistung erzielen. DNIs unterstützen VLAN-Tags und das Anpassen der MAC-Adresse. Der Verkehr auf DNIs ist nicht durch Sicherheitsgruppen geschützt.

Snowcone-Geräte unterstützen acht DNIs pro EC2-kompatibler Instance, maximal 8 pro Gerät.

### Themen

- [Voraussetzungen](#)
- [Einrichtung einer virtuellen Netzwerkschnittstelle \(VNI\)](#)
- [Einrichtung einer direkten Netzwerkschnittstelle \(DNI\)](#)

## Voraussetzungen

Bevor Sie ein VNI oder ein DNI konfigurieren, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben.

1. Stellen Sie sicher, dass Ihr Gerät mit Strom versorgt wird und dass eine Ihrer physischen Netzwerkschnittstellen, z. B. 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 [Konfiguration eines Profils für den Snowcone-Client](#) .

4. Entsperren Sie das Gerät. Wir empfehlen die Verwendung AWS OpsHub for Snow Family , um Ihr Gerät zu entsperren. Anweisungen finden Sie unter Gerät [entsperren Gerät](#) .

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 Geräteanzeige-Update zeigt an, dass es entsperrt ist.

6. Starten Sie eine EC2-kompatible Instanz auf dem Gerät. Sie verknüpfen das VNI mit dieser Instanz.
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.

## Einrichtung einer virtuellen Netzwerkschnittstelle (VNI)

Nachdem Sie die ID für Ihre physische Netzwerkschnittstelle identifiziert haben, können Sie eine virtuelle Netzwerkschnittstelle (VNI) einrichten. Gehen Sie wie folgt vor, um ein VNI einzurichten. Stellen Sie sicher, dass Sie die erforderlichen Aufgaben ausführen, bevor Sie eine VNI erstellen.

Erstellen Sie ein VNI und ordnen Sie eine IP-Adresse zu

1. 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 zu einem späteren Zeitpunkt im Prozess.

Wann immer Sie diese IP-Adresse benötigen, können Sie den `snowballEdge describe-virtual-network-interfaces` Snowball Edge-Client-Befehl oder den `aws ec2 describe-addresses` AWS CLI Befehl verwenden, um sie abzurufen.

- Um Ihre neu erstellte IP-Adresse mit Ihrer Instance zu verknüpfen, 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
```

## Einrichtung einer direkten Netzwerkschnittstelle (DNI)


### Note

Die direkte Netzwerkschnittstellenfunktion ist am oder nach dem 12. Januar 2021 verfügbar und auf allen AWS-Regionen Geräten von Snow Family verfügbar.

## Voraussetzungen

Bevor Sie eine direkte Netzwerkschnittstelle (DNI) einrichten, müssen Sie die Aufgaben im Abschnitt **Voraussetzungen** ausführen.

1. Führen Sie die erforderlichen Aufgaben aus, bevor Sie das DNI einrichten. Anweisungen finden Sie unter [Voraussetzungen](#).
2. Darüber hinaus müssen Sie eine Instanz auf Ihrem Gerät starten, eine VNI erstellen und diese der Instanz zuordnen. Anweisungen finden Sie unter [Einrichtung einer virtuellen Netzwerkschnittstelle \(VNI\)](#).

 Note

Wenn Sie Ihrem vorhandenen Gerät durch ein in-the-field Softwareupdate direkte Netzwerke hinzugefügt haben, müssen Sie das Gerät zweimal neu starten, um die Funktion vollständig zu aktivieren.

Erstellen Sie ein DNI und ordnen Sie die IP-Adresse zu

1. Erstellen Sie eine direkte Netzwerkschnittstelle und fügen Sie sie der Amazon EC2-kompatiblen Instance hinzu, indem Sie den folgenden Befehl ausführen. Für den nächsten Schritt benötigen Sie die MAC-Adresse des Geräts.

```
create-direct-network-interface [--endpoint endpoint] [--instance-id instanceId]
  [--mac macAddress]
  [--physical-network-interface-
id physicalNetworkInterfaceId]
  [--unlock-code unlockCode] [--vlan vlanId]
```

## OPTIONS

**--endpoint <endpoint>**Der Endpunkt, an den diese Anfrage gesendet werden soll. Der Endpunkt für Ihre Geräte ist eine URL, die das https Schema verwendet, gefolgt von einer IP-Adresse. Wenn die IP-Adresse für Ihr Gerät beispielsweise 123.0.1.2 lautet, wäre der Endpunkt für Ihr Gerät `https://123.0.1.2`.

**--instance-id <instanceId>**Die EC2-kompatible Instanz-ID, an die die Schnittstelle angehängt werden soll (optional).

**--mac <macAddress>**Legt die MAC-Adresse der Netzwerkschnittstelle fest (optional).

**--physical-network-interface-id <physicalNetworkInterfaceId>**Die ID für die physische Netzwerkschnittstelle, auf der eine neue virtuelle Netzwerkschnittstelle erstellt werden

soll. Mit dem `describe-device` Befehl können Sie die auf Ihrem Snowball Edge verfügbaren physischen Netzwerkschnittstellen ermitteln.

**--vlan <vlanId>** Stellen Sie das zugewiesene VLAN für die Schnittstelle ein (optional). Wenn angegeben, wird der gesamte von der Schnittstelle gesendete Datenverkehr mit der angegebenen VLAN-ID gekennzeichnet. Eingehender Datenverkehr wird nach der angegebenen VLAN-ID gefiltert und alle VLAN-Tags werden entfernt, bevor er an die Instanz weitergeleitet wird.

2. Wenn Sie Ihren DNI in Schritt 1 keiner Instanz zugeordnet haben, können Sie ihn verknüpfen, indem Sie den Befehl ausführen. [Aktualisierung einer direkten Netzwerkschnittstelle](#)
3. Nachdem Sie ein DNI erstellt und es mit Ihrer EC2-kompatiblen Instance verknüpft haben, müssen Sie zwei Konfigurationsänderungen in Ihrer Amazon EC2-kompatiblen Instance vornehmen.
  - Die erste Änderung besteht darin, sicherzustellen, dass Pakete, die für das VNI bestimmt sind, das der EC2-kompatiblen Instance zugeordnet ist, über `eth0` gesendet werden.
  - Die zweite Änderung konfiguriert Ihre direkte Netzwerkschnittstelle so, dass sie beim Booten entweder DHCP oder statische IP verwendet.

Im Folgenden finden Sie Beispiele für Shell-Skripte für Amazon Linux 2 und CentOS Linux, die diese Konfigurationsänderungen vornehmen.

## Amazon Linux 2

```
# Mac address of the direct network interface.
# You got this when you created the direct network interface.
DNI_MAC=[MAC ADDRESS FROM CREATED DNI]

# Configure routing so that packets meant for the VNI always are sent through
eth0.
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo "from $PRIVATE_IP table $ROUTE_TABLE" > /etc/sysconfig/network-scripts/
rule-eth0
echo "default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE" > /etc/
sysconfig/network-scripts/route-eth0
echo "169.254.169.254 dev eth0" >> /etc/sysconfig/network-scripts/route-eth0
```

```
# Query the persistent DNI name, assigned by udev via ec2net helper.
# changable in /etc/udev/rules.d/70-persistent-net.rules
DNI=$(ip --oneline link | grep -i $DNI_MAC | awk -F ': ' '{ print $2 }')

# Configure DNI to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
HWADDR=$DNI_MAC
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
MAINROUTETABLE=no
EOF

# Make all changes live.
systemctl restart network
```

## CentOS Linux

```
# Mac address of the direct network interface. You got this when you created the
direct network interface.
DNI_MAC=[MAC ADDRESS FROM CREATED DNI]
# The name to use for the direct network interface. You can pick any name that
isn't already in use.
DNI=eth1

# Configure routing so that packets meant for the VNIC always are sent through
eth0
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo from $PRIVATE_IP table $ROUTE_TABLE > /etc/sysconfig/network-scripts/rule-
eth0
echo default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE > /etc/sysconfig/
network-scripts/route-eth0

# Configure your direct network interface to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
```



```
HWADDR="$DNI_MAC"
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
EOF

# Rename DNI device if needed.
CURRENT_DEVICE_NAME=$(LANG=C ip -o link | awk -F ': ' -vIGNORECASE=1 '!/link\//
ieee802\.\d{1,2}/ && /'"$DNI_MAC"'/ { print $2 }')
ip link set $CURRENT_DEVICE_NAME name $DNI

# Make all changes live.
systemctl restart network
```

## Zusätzliche Befehle

Alle verfügbaren Befehle für AWS Snowcone Geräte finden Sie unter [Verwenden des Snowball Edge-Clients](#).

## Mit SSH eine Verbindung zu Ihrer Compute-Instance auf einem Snowcone herstellen

Um SSH für die Verbindung zu Ihren Recheninstanzen auf Snowcone-Geräten zu verwenden, müssen Sie zuerst den SSH-Schlüssel für das AMI bereitstellen, bevor Sie Ihren Job erstellen. Weitere Informationen zu dieser Vorgehensweise finden Sie unter [Konfigurieren eines AMI zur Verwendung von SSH zum Herstellen einer Verbindung mit auf dem Gerät gestarteten Datenverarbeitungs-Instances](#). Wenn Sie die Vorgehensweise nicht befolgt haben, können Sie sich nicht per SSH mit Ihren Instances verbinden.

So stellen Sie eine Verbindung zu Ihrer Instance per SSH her

1. Stellen Sie sicher, dass Ihr Gerät eingeschaltet, mit dem Netzwerk verbunden und entsperrt ist.
2. Stellen Sie sicher, dass Sie die Netzwerkeinstellungen für Ihre Datenverarbeitungs-Instances konfiguriert haben. Weitere Informationen finden Sie unter [Netzwerkkonfiguration für Datenverarbeitungs-Instances](#).

- 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.
- 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 [Netzwerkconfiguration 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 zu Ihrer Linux-Instance mithilfe von SSH](#) im Amazon EC2 EC2-Benutzerhandbuch.

## Snowcone-Client-Befehle für Compute-Instances

Der Snowball Edge-Client ist eine eigenständige Terminalanwendung, die Sie auf Ihrem lokalen Server ausführen können. Es ermöglicht Ihnen, einige administrative Aufgaben auf Ihrem Snowcone-Gerät durchzuführen. Weitere Informationen zur Verwendung des Snowball Edge-Clients, einschließlich zum Starten und Beenden von Diensten damit, finden Sie unter [Den AWS Snowball Edge Client verwenden](#).

Im Folgenden finden Sie Informationen zu den Snowball Edge-Clientbefehlen, die spezifisch für Compute-Instances sind, einschließlich Anwendungsbeispielen. Eine Liste der Amazon EC2-kompatiblen Befehle, die Sie auf Ihrem AWS Snowcone Gerät verwenden können, finden Sie unter [Unterstützte Amazon EC2-kompatible AWS CLI Befehle auf einem Snowcone](#)

### Note

Befehle, die sich auf Cluster beziehen, werden nicht unterstützt und geben einen Fehler zurück.

## Eine Startkonfiguration für den automatischen Start von Amazon EC2-kompatiblen Instances erstellen

Um Amazon EC2-kompatible Compute-Instances auf Ihrem AWS Snowcone Gerät automatisch zu starten, nachdem es entsperrt wurde, können Sie eine Startkonfiguration erstellen. Hierzu verwenden

Sie den Befehl `snowballEdge create-autostart-configuration`. Im Folgenden wird gezeigt, wie Sie diesen verwenden.

## Usage

```
snowballEdge create-autostart-configuration --physical-connector-type
[SFP_PLUS or RJ45]
--ip-address-assignment [DHCP or STATIC]
[--static-ip-address-configuration
IpAddress=[IP address],NetMask=[Netmask]]
--launch-template-id
[--launch-template-version]
```

## Aktualisierung einer Startkonfiguration auf Autostart EC2-kompatible Instances

Verwenden Sie den `snowballEdge update-autostart-configuration` Befehl, um eine bestehende Startkonfiguration auf Ihrem Snowcone 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]]
--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 für Autostart EC2-kompatible Instances

Um eine Startkonfiguration zu löschen, die nicht mehr verwendet wird, verwenden Sie den Befehl `snowballEdge delete-autostart-configuration`. Im Folgenden wird gezeigt, wie Sie ihn verwenden.

## Usage

```
snowballEdge delete-autostart-configuration --autostart-configuration-arn
```

## Startkonfigurationen für Autostart EC2-kompatible Instances auflisten

Verwenden Sie den `describe-autostart-configurations` Befehl, um die Startkonfigurationen aufzulisten, die Sie auf Ihrem Snowcone erstellt haben. Im Folgenden wird gezeigt, wie Sie ihn verwenden.

## Usage

```
snowballEdge describe-autostart-configurations
```

## Erstellen einer virtuellen Netzwerkschnittstelle

Um eine Recheninstanz auf Ihrem Snowcone auszuführen oder die NFS-Schnittstelle auf Ihrem Snowcone zu starten, erstellen Sie zunächst eine virtuelle Netzwerkschnittstelle (VNIC). Jeder Snowcone hat drei Netzwerkschnittstellen (NICs), die physischen Netzwerkschnittstellen-Controller für das Gerät. Dies sind die RJ45-Anschlüsse 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 konfigurierbarem Snowball Edge-Client oder ohne konfigurierbaren Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfigurierbarem 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 konfigurierbaren 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 konfigurierbarem Snowball Edge-Client oder ohne konfigurierbaren Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfigurierbarem Snowball Edge-Client.

```
snowballEdge describe-virtual-network-interfaces
```

Das folgende Anwendungsbeispiel zeigt die Methode ohne konfigurierbaren 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-Ressourcenamens (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 konfigurierbarem Snowball Edge-Client oder ohne konfigurierbaren Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfigurierbarem 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 konfigurierbaren 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 konfigurierbarem Snowball Edge-Client oder ohne konfigurierbaren Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfigurierbarem 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 von Instance Metadata Service for Snow mit Amazon EC2-kompatiblen Instances

IMDS for Snow bietet den Instance Metadata Service (IMDS) für Amazon EC2-kompatible Instances auf Snow. Instance-Metadaten sind Kategorien von Informationen über Instances. Dazu gehören Kategorien wie Hostname, Ereignisse und Sicherheitsgruppen. Mit IMDS for Snow können Sie Instance-Metadaten verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Start Ihrer Amazon EC2-kompatiblen Instance angegeben haben. Sie können beispielsweise IMDS for Snow verwenden, um Parameter für die Konfiguration Ihrer Instance anzugeben oder diese Parameter in ein einfaches Skript aufzunehmen. Sie können generische AMIs erstellen und mit Hilfe von Benutzerdaten die beim Start ausgelieferten Konfigurationsdateien ändern.

Informationen zu Instanz-Metadaten und Benutzerdaten sowie Snow EC2-kompatiblen Instances finden Sie unter [Unterstützte Instanz-Metadaten und Benutzerdaten in diesem Handbuch](#).

### Important

Sie können nur innerhalb der Instance selbst auf Instance-Metadaten und Benutzerdaten zugreifen. Die Daten sind nicht durch Authentifizierungs- oder kryptografische Verfahren geschützt. Jeder, der direkten Zugriff auf die Instance hat, und möglicherweise auch jede Software, die auf der Instance läuft, kann deren Metadaten einsehen. Daher sollten Sie sensible Daten wie Passwörter oder langlebige Verschlüsselungscodes nicht als Benutzerdaten speichern.



**Note**

Die Beispiele in diesem Abschnitt verwenden die IPv4-Adresse des Instance-Metadatendienstes: 169.254.169.254. Wir unterstützen den Abruf von Instanz-Metadaten unter Verwendung der link-lokalen IPv6-Adresse nicht.

## Themen

- [IMDS-Versionen](#)
- [Beispiele für das Abrufen von Instanz-Metadaten mithilfe von IMDSv1 und IMDSv2](#)

## IMDS-Versionen

Mit IMDS Version 2 oder IMDS Version 1 können Sie von einer laufenden Instanz aus auf Instanz-Metadaten zugreifen:

- Instance Metadata Service Version 2 (IMDSv2), eine sitzungorientierte Methode
- Instance Metadata Service Version 1 (IMDSv1), eine Anfrage-Antwort-Methode

Abhängig von der Version Ihrer Snow-Software können Sie IMDSv1, IMDSv2 oder beide verwenden. Dies hängt auch vom AMI-Typ ab, der in der EC2-kompatiblen Instanz ausgeführt wird. Für einige AMIs, z. B. solche, auf denen Ubuntu 20.04 ausgeführt wird, ist IMDSv2 erforderlich. Der Instanz-Metadatendienst unterscheidet zwischen IMDSv1- und IMDSv2-Anfragen anhand des Vorhandenseins von OR-Headern. PUT GET IMDSv2 verwendet diese beiden Header. IMDSv1 verwendet nur den Header. GET

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-Metadataservice, um Abwehr von offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen an EC2-Instance-Metadataservice](#).

## IMDSv2

IMDSv2 verwendet sitzungorientierte Anfragen. Bei sitzungorientierten Anfragen 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 future Anfragen erstellen.

Das folgende Beispiel verwendet ein Linux-Shell-Skript und IMDSv2, um die Metadatenelemente der Instanz auf oberster Ebene abzurufen. Dieses Beispiel:

1. Erstellt mithilfe der PUT Anfrage ein Sitzungstoken mit einer Dauer von sechs Stunden (21.600 Sekunden).
2. Speichert den Sitzungs-Token-Header in einer Variablen mit dem Namen `TOKEN`.
3. Fordert mithilfe des Tokens die Metadatenelemente der obersten Ebene an.

Sie können zwei Befehle getrennt ausführen oder sie 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 mithilfe des folgenden Befehls Metadatenelemente der obersten Ebene zu generieren.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

## Kombinierte Befehle

Sie können das Token speichern und die Befehle kombinieren. Das folgende Beispiel kombiniert die beiden obigen Befehle und speichert den Sitzungs-Token-Header in einer Variablen namens `TOKEN`.

### Note

Wenn beim Erstellen des Tokens ein Fehler auftritt, wird statt eines gültigen Tokens eine Fehlermeldung in der Variablen gespeichert und der Befehl funktioniert nicht.

## Example von kombinierten Befehlen

```
[ec2-user ~]$ TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/)
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Der folgende Beispielbefehl ruft die ID des AMI ab, das zum Starten der Instance verwendet wurde, und speichert sie in dem im vorherigen Beispiel `$TOKEN` erstellten.

## Example der Wiederverwendung eines Tokens

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
```

Wenn Sie IMDSv2 verwenden, um Instanz-Metadaten anzufordern, muss die Anfrage 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 instanzspezifischer Schlüssel. Das Token ist auf anderen EC2-kompatiblen Instances nicht gültig und wird zurückgewiesen, 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 PUT Anfragen ein Response-Hop-Limit (Time-to-Live) von 1 auf IP-Protokollebene. IMDS for Snow ist nicht in der Lage, das Hop-Limit für PUT Antworten zu ändern.

## IMDSv1

IMDSv1 verwendet das Request-Response-Modell. Um Instanz-Metadaten anzufordern, senden Sie eine GET Anfrage an den Instanz-Metadatendienst.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

## Abrufen von Instance-Metadaten

Ihre Instance-Metadaten sind in Ihrer laufenden Instance verfügbar, sodass Sie nicht die Amazon EC2 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.

Verwenden Sie den folgenden IPv4-URI, um alle Kategorien von Instanz-Metadaten innerhalb einer laufenden Instance anzuzeigen:

```
http://169.254.169.254/latest/meta-data/
```

Die IP-Adressen sind lokale Adressen (Link-local Addresses) und nur von der Instance aus gültig. Weitere Informationen finden Sie unter [Link-local address](#) in Wikipedia.

## Antworten und Fehlermeldungen

Alle Instance-Metadaten werden als Text zurückgegeben (HTTP-Inhaltstyp `text/plain`).

Eine Anfrage nach einer bestimmten Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode 404 — Not Found zurück, wenn die Ressource nicht verfügbar ist.

Eine Anfrage nach einer allgemeinen Metadatenressource (wenn der URI mit einem `/` Zeichen endet) gibt eine Liste verfügbarer Ressourcen zurück oder einen HTTP-Fehlercode 404 — Not Found, wenn es keine solche Ressource gibt. Die Listenelemente befinden sich in separaten Zeilen, die durch Zeilenvorschübe (ASCII-Zeichencode 10) abgeschlossen werden.

Für Anfragen, die mit IMDSv1 gestellt wurden, können die folgenden HTTP-Fehlercodes zurückgegeben werden:

- 400 - Fehlende oder ungültige Parameter — Die PUT Anfrage ist nicht gültig.
- 401 - Nicht autorisiert — Die GET Anfrage verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.
- 403 - Forbidden — Die Anfrage ist nicht zulässig oder der Instanz-Metadatendienst ist deaktiviert.

## Beispiele für das Abrufen von Instanz-Metadaten mithilfe von IMDSv1 und IMDSv2

Die folgenden Beispiele enthalten Befehle, die Sie für eine Linux-Instance verwenden können.

## Example zum Abrufen der verfügbaren Versionen der Instanz-Metadaten

In diesem Beispiel werden die verfügbaren Versionen der Instance-Metadaten abgerufen. Jede Version bezieht sich auf einen Instance-Metadaten-Build, wenn neue Instance-Metadatenkategorien veröffentlicht wurden. Es stehen frühere Versionen zur Verfügung, für den Fall dass Skripte angewendet werden, die auf den Strukturen und Daten dieser früheren Versionen aufbauen.

### IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://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    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 zum Abrufen der Metadatenelemente der obersten Ebene

In diesem Beispiel werden die Metadatenelemente der obersten Ebene abgerufen. Informationen zu Metadatenelementen der obersten Ebene finden Sie in diesem Handbuch unter [Unterstützte Instanz-Metadaten und Benutzerdaten](#).

## IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://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 zum Abrufen von Werten von Metadaten der obersten Ebene

In den folgenden Beispielen werden die Werte einiger der Metadatenelemente der obersten Ebene abgerufen, die im vorherigen Beispiel abgerufen wurden. Die IMDSv2-Anfragen verwenden das gespeicherte Token, das im vorhergehenden Beispielbefehl erstellt wurde (vorausgesetzt, es ist nicht abgelaufen).

### ami-idIMDSv2

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/latest/meta-data/ami-id ami-0abcdef1234567890
```

### ami-idIMDS v1

```
curl http://192.0.2.0/latest/meta-data/ami-id ami-0abcdef1234567890
```

### reservation-idIMDS v2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/latest/meta-data/reservation-id r-0efghijk987654321
```

### reservation-idIMDS v1

```
[ec2-user ~]$ curl http://192.0.2.0/latest/meta-data/reservation-id \
r-0efghijk987654321
```

## local-hostnameIMDS v2

```
[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-hostnameIMDS v1

```
[ec2-user ~]$ curl http://192.0.2.0/latest/meta-data/local-hostname ip-00-000-00-00
```

## Verwenden des Amazon EC2-kompatiblen Endpunkts

Im Folgenden finden Sie eine Übersicht über den Amazon Elastic Compute Cloud-kompatiblen (Amazon EC2) Endpunkt. Mit diesem Endpunkt können Sie Ihre Amazon Machine Images (AMIs) verwalten und Instances mithilfe von Amazon EC2-kompatiblen API-Vorgängen programmgesteuert berechnen.

### Themen

- [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#)
- [Nicht unterstützte Amazon EC2 EC2-Funktionen für Snowcone](#)
- [Unterstützte Amazon EC2-kompatible AWS CLI Befehle auf einem Snowcone](#)
- [Unterstützte Amazon EC2 EC2-API-Operationen](#)

## Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI

Wenn Sie den verwenden AWS CLI , um einen Befehl an das AWS Snowcone Gerät zu senden, können Sie angeben, dass der Endpunkt der Amazon EC2-kompatible 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 Snowcone bei jeder Entsperrung generiert 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-kompatiblen Endpunkt

1. Connect den Snowcone an die Stromversorgung und das Netzwerk an und schalten Sie ihn ein.
2. Notieren Sie nach dem Entsperren des Geräts seine IP-Adresse im lokalen Netzwerk.
3. Stellen Sie sicher, dass Sie das Snowcone-Gerät von einem Terminal in Ihrem Netzwerk aus pingen können.
4. Führen Sie den `snowballEdge get-certificate`-Befehl in Ihrem Terminal aus. Weitere Informationen zu diesem Befehl finden Sie unter [Abrufen des Zertifikats für die Datenübertragung](#).
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.snowcone.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.

## Nicht unterstützte Amazon EC2 EC2-Funktionen für Snowcone

Mithilfe des Amazon EC2-kompatiblen Endpunkts können Sie Ihre AMIs und Compute-Instances auf einem Snowcone mit Amazon EC2-kompatiblen API-Operationen programmgesteuert verwalten. Allerdings werden nicht alle Funktionen und API-Operationen für die Verwendung mit einem Snowcone-Gerät unterstützt.

Alle Funktionen oder Aktionen, die in diesem Leitfaden nicht explizit als unterstützt aufgeführt sind, werden nicht unterstützt. Beispielsweise werden die folgenden Amazon EC2 EC2-Aktionen für die Verwendung mit Snowcone nicht unterstützt:

- [create-nat-gateway](#)

- [create-key-pair](#)

## Unterstützte Amazon EC2-kompatible AWS CLI Befehle auf einem Snowcone

Sie können Ihre Compute-Instances auf einem Snow Family-Gerät über einen Amazon EC2-kompatiblen Endpunkt verwalten. Dieser Endpunkttyp unterstützt viele der Amazon EC2 EC2-CLI-Befehle und -Aktionen der AWS SDKs. Informationen zur Installation und Einrichtung von AWS CLI, einschließlich der Angabe, gegen wen AWS-Regionen Sie AWS CLI Anrufe tätigen möchten, finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

### Liste der unterstützten Amazon EC2-kompatiblen AWS CLI Befehle auf einem Snowcone

Im Folgenden finden Sie eine Beschreibung der Teilmenge der AWS CLI Befehle und Optionen für Amazon EC2, die auf Snowcone-Geräten unterstützt werden. Wenn ein Befehl oder eine Option im Folgenden nicht aufgeführt ist, wird diese(r) nicht unterstützt. Sie können einige nicht unterstützte Optionen in Kombination mit einem Befehl angeben. Diese werden jedoch ignoriert.

- [associate-address](#) – Verknüpft eine virtuelle IP-Adresse mit einer Instance, damit diese über eine der drei physischen Netzwerkschnittstellen auf dem Gerät verwendet werden kann:
  - `--instance-id` – Die ID einer einzelnen sbe-Instance.
  - `--public-ip` – Die virtuelle IP-Adresse, mit der Sie auf Ihre Instance zugreifen möchten.
- [attach-volume](#) — Hängt ein Amazon EBS-Volume an eine gestoppte oder laufende Instance auf Ihrem AWS Snowcone Gerät an und macht es der Instance mit dem angegebenen Gerätenamen zugänglich.
  - `--device value` Der Gerätename.
  - `--instance-id` — Die ID einer Amazon EC2 EC2-Zielinstanz.
  - `--volume-id value` — Die ID des EBS-Volumes.
- [authorize-security-group-egress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln zur Verwendung mit einem Snowcone-Gerät hinzu. Insbesondere diese Aktion erlaubt Instances, Datenverkehr an eine oder mehrere IPv4-CIDR-Zieladressbereiche zu senden. Weitere Informationen finden Sie unter [Sicherheitsgruppen in Snow-Geräten](#).
  - `--group-id value` — Die ID der Sicherheitsgruppe
  - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
- [authorize-security-group-ingress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Eingangsregeln hinzu. Wenn Sie `authorize-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.

- `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
- `[--group-idvalue]` — Die ID der Sicherheitsgruppe
- `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
- `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (-1) angegeben.
- `[--portvalue]` — Für TCP oder UDP der Bereich der Ports, die zugelassen werden sollen. Dieser Wert kann eine einzelne Ganzzahl oder ein Bereich (Minimum—Maximum) sein.

Für ICMP eine einzelne Ganzzahl oder ein Bereich (`type-code`), wobei bei `type` die Nummer des ICMP-Typs und `code` die ICMP-Codenummer darstellen. Der Wert -1 steht für alle ICMP-Codes für alle ICMP-Typen. Der Wert -1 nur für `type` gibt alle ICMP-Codes für den angegebenen ICMP-Typ an.

- `[--cidrvalue]` — Der CIDR-IP-Bereich.
- [create-launch-template](#) — Erstellt eine Startvorlage. Eine Startvorlage enthält die Parameter zum Starten einer Instance. Wenn Sie eine Instance über `RunInstances` starten, können Sie eine Startvorlage angeben, statt die Startparameter in der Anfrage bereitzustellen. Sie können bis zu 100 Vorlagen pro AWS Snowcone 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"
    }
  ]
}
```

- `[--version-descriptionstring]` — Eine Beschreibung für die erste Version der Startvorlage.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [create-launch-template-version](#) — Erstellt eine neue Version für eine Startvorlage. Sie können eine vorhandene Version einer Startvorlage angeben, auf der die neue Version basieren soll. Die Startvorlagenversionen werden in der Reihenfolge markiert, in der sie erstellt werden. Sie können die Nummerierung von Startvorlagenversionen nicht angeben, ändern oder ersetzen. Sie können bis zu 100 Versionen jeder Startvorlage erstellen.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `-- launch-template-data structure` — Die Informationen für die Startvorlage. Folgende Attribute werden unterstützt:
  - `ImageId`
  - `InstanceType`
  - `SecurityGroupIds`
  - `TagSpecifications`
  - `UserData`

## JSON-Syntax:

```
'{
  "ImageId":"string",
  "InstanceType":"sbe-c.large",
  "SecurityGroupIds":["string", ...],
  "TagSpecifications":[{"ResourceType":"instance","Tags":
[{"Key":"Name","Value":"Test"},
  {"Key":"Stack","Value":"Gamma"}]}],
  "UserData":"this is my user data"
}'
```

- `--source-versionstring` — Die Versionsnummer der Startvorlage, auf der die neue Version basieren soll. Die neue Version übernimmt alle Startparameter der Quellversion, ausgenommen der von Ihnen in `launch-template-data` angegebenen Parameter.
- `--version-descriptionstring` — Eine Beschreibung für die erste Version der Startvorlage.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [create-tags](#) — [Fügt ein oder mehrere Tags](#) für die angegebene Ressource hinzu oder überschreibt es. Jede Ressource kann maximal 50 Tags haben. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Tag-Schlüssel müssen für eine Ressource eindeutig sein. Folgende Ressourcen werden unterstützt:
  - AMI
  - Instance
  - Startvorlage
  - Sicherheitsgruppe
- [create-security-group](#) — Erstellt eine Sicherheitsgruppe auf Ihrem Snowcone-Gerät. Sie können bis zu 50 Sicherheitsgruppen erstellen. Wenn Sie eine Sicherheitsgruppe erstellen, geben Sie einen Anzeigenamen Ihrer Wahl an:
  - `--group-name value` — Der Name der Sicherheitsgruppe.
  - `--description value` — Eine Beschreibung der Sicherheitsgruppe. Dies dient nur zu Informationszwecken. Dieser Wert kann bis zu 255 Zeichen lang sein.
- [create-volume](#) — Erstellt ein Amazon EBS-Volume, das an eine Instance auf Ihrem Gerät angehängt werden kann. AWS Snowcone
  - `--sizevalue` — Die Größe des Volumes in GiBs, die zwischen 1 GiB und 1 TB (1000 GiBs) liegen kann.

- `[--snapshot-id value]` — Der Snapshot, aus dem das Volume erstellt werden soll.
- `[--volume-type]` — Der Volume-Typ `value`. 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 bei der Erstellung auf das Volume angewendet werden sollen.
- [delete-launch-template](#) — Löscht eine Startvorlage. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [delete-launch-template-version](#) — Löscht eine oder mehrere Versionen einer Startvorlage. Sie können die Standardversion einer Startvorlage erst löschen, nachdem Sie eine andere Version als Standardversion festgelegt haben. Wenn die Standardversion die einzige Version der Startvorlage ist, löschen Sie die gesamte Startvorlage, indem Sie den Befehl `delete-launch-template` verwenden.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `--versions (Liste) "string" "string"` — Die Versionsnummern einer oder mehrerer Versionen der Startvorlage, die gelöscht werden sollen.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können.
- [delete-security-group](#) — Löscht eine Sicherheitsgruppe.

Wenn Sie versuchen, eine Sicherheitsgruppe zu löschen, die mit einer Instance verknüpft ist, oder auf die von einer anderen Sicherheitsgruppe verwiesen wird, schlägt die Operation mit `DependencyViolation` fehl.



- `--group-name value` — Der Name der Sicherheitsgruppe.
- `--description value` — Eine Beschreibung der Sicherheitsgruppe. Dies dient nur zu Informationszwecken. Dieser Wert kann bis zu 255 Zeichen lang sein.
- [delete-tags](#) — Löscht den angegebenen Satz von Tags aus der angegebenen Ressource (AMI, Compute-Instance, Startvorlage oder Sicherheitsgruppe).
- [delete-volume](#) — Löscht das angegebene Amazon EBS-Volume. Das Volume muss den `available`-Status aufweisen (nicht an eine Instance angefügt).
  - `value--volume-id` — Die ID des Volumes.
- [describe-addresses](#) — Beschreibt eine oder mehrere Ihrer virtuellen IP-Adressen, die derselben Anzahl von sbe Instanzen auf Ihrem Gerät zugeordnet sind.
  - `--public-ips` – Eine oder mehrere der virtuellen IP-Adressen, die Ihren Instances zugeordnet sind.
- [describe-images](#) — Beschreibt eines oder mehrere der Images (AMIs), die Ihnen zur Verfügung stehen. Ihnen zur Verfügung stehende Bilder werden dem Snowcone-Gerät bei der Auftragserstellung hinzugefügt.
  - `--image-id` — Die Snowcone-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 beim Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
  - `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.

- `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- [describe-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 mit IDs der Startvorlagen.
- `-- launch-template-names` (Liste) "string" "string" — Eine Liste mit Namen für die Startvorlagen.
- `--page-size` — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [describe-launch-template-versions](#) — Beschreibt eine oder mehrere Versionen einer bestimmten Startvorlage. Sie können alle Versionen, einzelne Versionen oder eine Reihe von Versionen beschreiben. Beim Befehl `describe-launch-template-versions` handelt es sich um eine paginierte Operation. Sie können mehrere Aufrufe ausführen, um den gesamten 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 (Liste)"string" "string"]` — Die Versionsnummern einer oder mehrerer Versionen der Startvorlage, die gelöscht werden sollen.
- `[--min-versionstring]` — Die Versionsnummer, nach der die Versionen der Startvorlagen beschrieben werden sollen.
- `[--max-versionstring]` — Die Versionsnummer, bis zu der die Versionen der Startvorlagen beschrieben werden sollen.
- `--page-size` — Die Größe jeder Seite, die im Aufruf abgerufen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token` — Ein Token, um anzugeben, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [describe-security-groups](#) — Beschreibt eine oder mehrere Ihrer Sicherheitsgruppen.

Beim Befehl `describe-security-groups` handelt es sich um eine paginierte Operation. Sie können mehrere API-Aufrufe ausführen, um den gesamten Ergebnissatz abzurufen.

- `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
- `[--group-idvalue]` — Die ID der Sicherheitsgruppe.
- `[--page-sizevalue]` — Die Größe jeder Seite, die beim Serviceaufruf abgerufen werden soll. AWS Diese Größe hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Einstellen einer kleineren Seitengröße führt zu mehr Aufrufen des AWS Dienstes, wodurch bei jedem Aufruf weniger Elemente abgerufen werden. Durch diesen Ansatz kann verhindert werden, dass bei AWS Serviceaufrufen ein Timeout auftritt. Anwendungsbeispiele finden Sie unter [Pagination](#) im AWS Command Line Interface Benutzerhandbuch.

- `[--max-itemsvalue]` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an. Verwenden Sie das `NextToken` Antwortelement nicht direkt außerhalb von. AWS CLI Anwendungsbeispiele finden Sie unter [Pagination](#) im AWS Command Line Interface Benutzerhandbuch.
- `[--starting-tokenvalue]` — Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort. Anwendungsbeispiele finden Sie unter [Pagination](#) im Benutzerhandbuch.AWS Command Line Interface
- [describe-tags](#) — Beschreibt eines oder mehrere der Tags für die angegebene Ressource (`image`, `instance`, oder Sicherheitsgruppe). Mit diesem Befehl werden die folgenden Filter unterstützt:
  - `launch-template`
  - `resource-id`
  - Ressourcentyp: `image` oder `instance`
  - `key`
  - Wert
- [describe-volumes](#) — Beschreibt die angegebenen Amazon EBS-Volumes.
  - `[--max-itemsvalue]` — Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
  - `[--starting-tokenvalue]` — Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
  - `[--volume-ids]` — Eine oder mehrere `Volume-IDsvalue`.
- [detach-volume](#) — Trennt ein Amazon EBS-Volume von einer gestoppten oder laufenden Instance.
  - `[--device]` — Der Geräte**namevalue**.
  - `[--instance-id]` — Die ID einer Amazon EC2 EC2-Zielinstanz.
  - `--volume-id` — Die ID `value` des Volumes.
- [disassociate-address](#) — Entfernt eine virtuelle IP-Adresse von der Instance.

- `--public-ip` — Die virtuelle IP-Adresse, die Sie von Ihrer Instance trennen möchten.
- [get-launch-template-data](#)— Ruft die Konfigurationsdaten der angegebenen Instanz ab. Sie können diese Daten verwenden, um eine Startvorlage zu erstellen.
  - `--instance-id` – Die ID einer einzelnen sbe-Instance.
  - `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [modify-launch-template](#)— Ändert eine Startvorlage. Sie können angeben, welche Version der Startvorlage als Standardversion festgelegt werden soll. Wenn Sie eine Instance ohne Angabe einer Startvorlagenversion starten, wird die Standardversion der Startvorlage angewendet.

Geben Sie in der Anfrage entweder die Startvorlagen-ID oder den Startvorlagennamen an.

- `-- launch-template-id string` — Die ID der Startvorlage.
- `-- launch-template-name string` — Ein Name für die Startvorlage.
- `--default-version string` — Die Versionsnummer der Startvorlage, die als Standardversion festgelegt werden soll.
- `--endpoint snowballEndpoint` — Ein Wert, mit dem Sie Ihre Compute-Instances mithilfe von Amazon EC2 EC2-API-Vorgängen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Den Amazon EC2-kompatiblen Endpunkt als Endpunkt angeben AWS CLI](#).
- [modify-instance-attribute](#)— Ändert ein Attribut der angegebenen Instance. Folgende Attribute werden unterstützt:
  - `instanceInitiatedShutdownBehavior`
  - `userData`
- [revoke-security-group-egress](#)— Entfernt eine oder mehrere Ausgangsregeln aus einer Sicherheitsgruppe:
  - `[--group-idvalue]` — Die ID der Sicherheitsgruppe
  - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.
- [revoke-security-group-ingress](#)— Widerruft eine oder mehrere Regeln für den Zugriff auf eine Sicherheitsgruppe. Wenn Sie `revoke-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
  - `[--group-namevalue]` — Der Name der Sicherheitsgruppe.
  - `[--group-idvalue]` — Die ID der Sicherheitsgruppe.
  - `[--ip-permissionsvalue]` — Ein oder mehrere Sätze von IP-Berechtigungen.

- `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (`-1`) angegeben.
- `[--portvalue]` — Für TCP oder UDP der Bereich der Ports, die zugelassen werden sollen. Eine einzelne Ganzzahl oder ein Bereich (Minimal—Maximum).

Für ICMP eine einzelne Ganzzahl oder ein Bereich (`type-code`), wobei bei `type` die Nummer des ICMP-Typs und `code` die ICMP-Codenummer darstellen. Der Wert `-1` steht für alle ICMP-Codes für alle ICMP-Typen. Der Wert `-1` nur für `type` gibt alle ICMP-Codes für den angegebenen ICMP-Typ an.

- `[--cidrvalue]` — Der CIDR-IP-Bereich.
- [run-instances](#) — Startet eine Reihe von Compute-Instances mithilfe einer Snowcone-AMI-ID für ein AMI.

#### Note

Je nach Größe und Typ der Instanz kann es bis zu anderthalb Stunden dauern, bis eine Recheninstanz auf einem Snowcone-Gerät gestartet wird.

- `[-- block-device-mappings (list)]` — Die blockierten Gerätezuordnungseinträge. Die Parameter `DeleteOnTermination`, `VolumeSize` und `VolumeType` werden unterstützt. Start-Volumes müssen den Typ `sbp1` 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 Snowcone-AMI-ID des AMI, die Sie durch einen Anruf abrufen können. `describe-images` Um eine Instance zu starten, wird ein AMI benötigt.
- `-- InstanceInitiatedShutdownBehavior` — Wenn Sie von Ihrer Instance aus ein Herunterfahren einleiten (mit einem Befehl wie `Shutdown` oder `Poweroff`), wird die Instance standardmäßig gestoppt. Sie können das Verhalten stattdessen ändern, sodass sie beendet wird. Die Parameter `stop` und `terminate` werden unterstützt. Der Standardwert ist `stop`. Weitere Informationen finden Sie unter [Ändern des Verhaltens beim initiierten Herunterfahren der Instance](#) im Amazon EC2 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 erstellen mit [CreateSecurityGroup](#). Wenn kein Wert angegeben wird, wird die ID für die Standard-Sicherheitsgruppe den erstellten Instances zugewiesen.
- `--tag-specifications` — Die Tags, die beim Start auf die Ressourcen angewendet werden sollen. Instances können nur beim Start markiert werden. Die angegebenen Tags werden auf alle Instances angewendet, die beim Start erstellt werden. Um eine Ressource mit einem Tag zu versehen, nachdem sie erstellt wurde, verwenden Sie `create-tags`.
- `--user-data` — Die Benutzerdaten, die der Instanz zur Verfügung gestellt werden sollen. Wenn Sie die verwenden AWS CLI, wird die Base64-Kodierung für Sie durchgeführt, und Sie können den Text aus einer Datei laden. Andernfalls müssen Sie einen base64-kodierten Text bereitstellen.
- [start-instances](#) — Startet eine sbe Instanz, die Sie zuvor gestoppt haben. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.



- `--instance-ids` – Die IDs einer oder mehrerer sbe-Instances, die auf dem Gerät gestoppt wurden.
- [stop-instances](#) — Stoppt eine sbe Instance, die gerade läuft. 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](#) — **Führt** 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 das `InstanceInitiatedShutdownBehavior` Attribut jedoch verwenden, um dieses Verhalten so zu ändern, dass diese Befehle Ihre Instance beenden. Weitere Informationen finden Sie unter [Ändern des Verhaltens beim initiierten Herunterfahren der Instance](#) im Amazon EC2 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.

## Unterstützte Amazon EC2 EC2-API-Operationen

Im Folgenden finden Sie Amazon EC2 EC2-API-Operationen, die Sie mit einem Snowcone-Gerät verwenden können, mit Links zu ihren Beschreibungen in der Amazon EC2 EC2-API-Referenz. Amazon EC2 EC2-API-Aufrufe erfordern eine Signatur mit Signature Version 4 (Sigv4). Wenn Sie das AWS CLI oder ein AWS SDK verwenden, um diese API-Aufrufe zu tätigen, wird die SigV4-Signatur für Sie erledigt. Andernfalls müssen Sie Ihre eigene SigV4 Signatur-Lösung implementieren.


- [AssociateAddress](#)— Ordnet eine Elastic IP-Adresse einer Instance oder einer Netzwerkschnittstelle zu.
- [AttachVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:



- Device
- InstanceId
- VolumeId
- [AuthorizeSecurityGroupEgress](#)— Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln zur Verwendung mit einem Snowcone-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 Aufrufen `AuthorizeSecurityGroupIngress` müssen Sie entweder einen Wert für `GroupName` oder `GroupId` angeben.
- [CreateVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
  - SnapshotId
  - Size
  - VolumeType
  - TagSpecification.N
- [CreateLaunchTemplate](#)— Die folgenden Anforderungsparameter werden unterstützt:
  - ImageId
  - InstanceType
  - SecurityGroupIds
  - TagSpecifications
  - UserData
- [CreateLaunchTemplateVersion](#)
- [CreateTags](#)— Die folgenden Anforderungsparameter werden unterstützt:
  - AMI
  - Instance
  - Launch template
  - Security group
- [CreateSecurityGroup](#)— Erzeugt eine Sicherheitsgruppe auf Ihrem Snowcone. 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`
- [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 Compute-Instance
  - `key`
  - `value`
- [DescribeVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
  - `MaxResults`
  - `NextToken`
  - `VolumeId.N`
- [DetachVolume](#)— Die folgenden Anforderungsparameter werden unterstützt:
  - `Device`
  - `InstanceId`
  - `VolumeId`

- [DisassociateAddress](#)
- [GetLaunchTemplateData](#)
- [ModifyLaunchTemplate](#)
- [ModifyInstanceAttribute](#)— Nur das `userData` Attribut wird unterstützt.
- [RevokeSecurityGroupEgress](#)— Entfernt eine oder mehrere Ausgangsregeln aus einer Sicherheitsgruppe.
- [RevokeSecurityGroupIngress](#)— Widerruft eine oder mehrere Eingangsregeln für eine Sicherheitsgruppe. Beim Aufrufen `RevokeSecurityGroupIngress` müssen Sie entweder einen Wert für `group-name` oder angeben. `group-id`
- [RunInstances](#) –

 Note

Je nach Größe und Typ der Instance kann es bis zu anderthalb Stunden dauern, bis eine Compute-Instance auf einem Snowcone gestartet wird.


- [StartInstances](#)
- [StopInstances](#)— Ressourcen, die einer gestoppten Instanz zugeordnet sind, bleiben bestehen. Sie können die Instance beenden, um diese Ressourcen freizugeben. Alle zugehörigen Daten werden jedoch gelöscht.
- [TerminateInstances](#)

## Automatisches Starten von Amazon EC2-kompatiblen Instances mit Startvorlagen

Sie können Ihre Amazon EC2-kompatiblen Instances auf Ihrem AWS Snowcone Gerät mithilfe von Startvorlagen und Startkonfigurationsbefehlen für den Snowball Edge-Client automatisch starten. Wenn eine Instance beendet wird, wird sie von Autostart gestartet. Wenn Sie jedoch die Instance löschen oder die Autostart-Konfiguration der Instance aktualisieren, startet der Autostart eine neue Instance.

Eine Startvorlage enthält die Konfigurationsinformationen, die zum Erstellen einer Amazon EC2-kompatiblen Instance auf Ihrem Snowcone erforderlich sind. Sie können eine Startvorlage verwenden, um Startparameter zu speichern, sodass Sie sie nicht jedes Mal angeben müssen, wenn Sie eine EC2-kompatible Instance auf dem Snowcone starten.

Wenn Sie Autostart-Konfigurationen auf Ihrem Snowcone verwenden, konfigurieren Sie die Parameter, mit denen Ihre Amazon EC2-kompatible Instance beginnen soll. Nachdem Ihr Snowcone konfiguriert ist und Sie ihn neu starten und entsperren, verwendet er Ihre Autostart-Konfiguration, um eine Instanz mit den von Ihnen angegebenen Parametern zu starten. Wenn eine von Ihnen mithilfe einer Autostart-Konfiguration gestartete Instance angehalten wird, wird die Instance ab dem Moment ausgeführt, in dem Sie Ihr Gerät entsperren.


 Note

Starten Sie Ihr Gerät nach der Konfiguration einer Autostart-Konfiguration neu, um sie zu starten. Alle nachfolgenden Instanzstarts (nach geplanten oder ungeplanten Neustarts) erfolgen automatisch, nachdem Ihr AWS Snowcone Gerät entsperrt wurde.

Eine Startvorlage kann die Amazon Machine Image (AMI) -ID, den Instance-Typ, Benutzerdaten, Sicherheitsgruppen und Tags für eine Amazon EC2-kompatible Instance angeben, wenn Sie diese Instance starten.

Gehen Sie wie folgt vor, um automatisch EC2-kompatible Instances auf dem Snowcone zu starten:

1. Wenn Sie Ihr AWS Snowcone Gerät bestellen, erstellen Sie einen Auftrag zur Bestellung eines Snow Family-Geräts mit Recheninstanzen. Weitere Informationen finden Sie unter [Anlegen eines Auftrags mit Datenverarbeitungs-Instances](#).
2. Nachdem Sie Ihren Snowcone erhalten haben, entsperren Sie ihn.
3. Verwenden Sie den EC2-API-Befehl `aws ec2 create-launch-template`, um eine Startvorlage zu erstellen. Weitere Informationen finden Sie unter [Liste der unterstützten Amazon EC2-kompatiblen AWS CLI Befehle auf einem Snowcone](#).

 Note

Der Amazon EC2 EC2-Endpunkt ist der Geräteendpunkt.

4. Verwenden Sie den Snowball Edge-Client-Befehl `snowballEdge create-autostart-configuration`, um Ihre EC2-kompatible Startvorlage an Ihre Netzwerkkonfiguration zu binden. Weitere Informationen finden Sie unter [Eine Startkonfiguration für den automatischen Start von Amazon EC2-kompatiblen Instances erstellen](#).

5. Starten Sie Ihr Gerät neu und entsperren Sie es anschließend. AWS Snowcone Ihre EC2-kompatiblen Instances werden automatisch mit den in Ihrer Startvorlage und Ihrem Snowcone-Client-Befehl angegebenen Attributen gestartet. `create-autostart-configuration`

Um den Status Ihrer ausgeführten Instances anzuzeigen, verwenden Sie den EC2-API-Befehl `describe-autostart-configurations`.

#### Note

Es gibt keine Konsole oder Job-Management-API zur AWS Snowball Unterstützung beim Starten von Vorlagen. Sie verwenden EC2- und Snowball Edge-Client-CLI-Befehle, um automatisch EC2-kompatible Instances auf Ihrem Gerät zu starten. AWS Snowcone

## Verwenden von Block Storage mit Ihren Amazon EC2-kompatiblen Instances

Blockspeicher auf Snowcone ermöglicht es Ihnen, Blockspeicher je nach den Anforderungen Ihrer Anwendungen hinzuzufügen oder zu entfernen. Volumes, die an eine Amazon EC2-kompatible Instance angehängt sind, werden als Speichervolumen bereitgestellt, die unabhängig von der Lebensdauer der Instance bestehen bleiben. Sie können Blockspeicher mit der vertrauten Amazon EBS-API verwalten.

Bestimmte Amazon EBS-Befehle werden durch die Verwendung des EC2-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 Amazon EC2-kompatiblen AWS CLI Befehle auf einem Snowcone](#).

#### Important

Stellen Sie sicher, dass Sie alle Dateisysteme auf dem Gerät innerhalb Ihres Betriebssystems unmounten, bevor Sie das Volume trennen. Andernfalls kann es zu Datenverlusten kommen.

Im Folgenden finden Sie Amazon EBS-Volumenkontingente und Unterschiede zwischen Amazon EBS-Volumes auf Ihrem AWS Snowcone Gerät und Amazon EBS-Volumes in der Cloud:

- Amazon EBS-Volumes sind nur für EC2-kompatible Instances verfügbar, die auf dem AWS Snowcone Gerät ausgeführt werden, das die Volumes hostet.
- Volume-Typen sind entweder auf kapazitätsoptimierte HDD (sbg1) oder leistungsoptimierte SSD (sbp1) beschränkt. Der Standard-Volume-Typ ist sbg1.
- Amazon EC2 EC2-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 zwischen 1 GB und 8 TB groß sein.
- Bis zu 10 Amazon EBS-Volumes können an eine einzelne EC2-kompatible Instance angehängt werden.
- Es gibt kein formelles Limit für die Anzahl der Amazon EBS-Volumes, die Sie auf Ihrem AWS Snowcone Gerät haben können. Die gesamte Amazon EBS-Volumenkapazität ist jedoch durch den verfügbaren Speicherplatz auf Ihrem AWS Snowcone Gerät begrenzt.

## Sicherheitsgruppen in Snow-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 EC2-Benutzerhandbuch.

Sicherheitsgruppen in Snowcone-Geräten ähneln den Sicherheitsgruppen in der AWS Cloud. Virtual Private Clouds (VPCs) werden auf Snowcone-Geräten nicht unterstützt.

Im Folgenden finden Sie die weiteren Unterschiede zwischen Snowcone-Sicherheitsgruppen und EC2-VPC-Sicherheitsgruppen:

- Jeder Snowcone hat ein Limit von 50 Sicherheitsgruppen.
- Die Standard-Sicherheitsgruppe lässt den gesamten ein- und ausgehenden Datenverkehr zu.
- Für den Datenverkehr zwischen lokalen Instances kann entweder die private Instance-IP-Adresse oder eine öffentliche IP-Adresse verwendet werden. Angenommen, Sie möchten per SSH eine

Verbindung von Instance A mit Instance B herstellen. In diesem Fall kann Ihre Ziel-IP-Adresse entweder die öffentliche IP-Adresse oder die private IP-Adresse der Instance B sein, sofern die Sicherheitsgruppenregel den Datenverkehr zulässt.

- Nur die für AWS CLI Aktionen und API-Aufrufe aufgelisteten Parameter werden unterstützt. Dabei handelt es sich in der Regel um einen Teilsatz der in EC2-VPC-Instances unterstützten Parameter.

Weitere Informationen zu unterstützten AWS CLI Aktionen finden Sie unter [Liste der unterstützten Amazon EC2-kompatiblen AWS CLI Befehle auf einem Snowcone](#). Weitere Informationen zu unterstützten API-Vorgängen finden Sie unter [Unterstützte Amazon EC2 EC2-API-Operationen](#).

## Unterstützte Instance-Metadaten und Benutzerdaten

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Snowcone unterstützt eine Teilmenge von Instanz-Metadatenkategorien für Ihre Compute-Instances. Weitere Informationen finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im Amazon-EC2-Benutzerhandbuch.

Die folgenden Kategorien werden unterstützt. Bei Verwendung anderer Kategorien wird eine 404 Fehlermeldung zurückgegeben.

### Unterstützte Instanz-Metadatenkategorien auf einem Snowcone

Daten	Beschreibung
ami-id	Die für den Start der Instance verwendete AMI-ID
hostname	Der private IPv4-DNS-Hostname der Instance.
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.

Daten	Beschreibung
<code>network/interfaces/mac</code> / <i>mac</i> / <code>local-hostname</code>	Der lokale Hostname der Schnittstelle
<code>network/interfaces/mac</code> / <i>mac</i> / <code>local-ipv4s</code>	Die privaten IPv4-Adressen, die mit der Netzwerkschnittstelle verknüpft sind
<code>network/interfaces/mac</code> / <i>mac</i> / <code>mac</code>	Die MAC-Adresse der Instance
<code>network/interfaces/mac</code> / <i>mac</i> / <code>public-ipv4s</code>	Die Elastic IP-Adressen, die mit der Schnittstelle verknüpft sind.
<code>public-ipv4</code>	Die öffentliche IPv4-Adresse.
<code>public-keys/0/openssh-key</code>	Der öffentliche Schlüssel. Nur verfügbar, wenn bei der Instance-Startzeit angegeben.
<code>reservation-id</code>	Die ID der Reservierung
<code>userData</code>	Shell-Scripts zum Übermitteln von Anweisungen an eine Instance beim Start.

### Unterstützte dynamische Instanzdatenkategorien auf einem Snowcone

Daten	Beschreibung
<code>instance-identity/document</code>	JSON-Daten mit Instance-Attributen. Nur <code>instanceId</code> , <code>imageId</code> , <code>privateIp</code> und <code>instanceType</code> verfügen über Werte, und die anderen zurückgegebenen Attribute sind auf Null gesetzt. Weitere Informationen finden Sie unter <a href="#">Dokumente zur Instance-Identität</a> im Amazon EC2 EC2-Benutzerhandbuch.



## Benutzerdaten in Snowcone Compute Instances ändern

Benutzerdaten werden für die Verwendung mit Shell-Skripten für Recheninstanzen auf einem Snowcone-Gerät unterstützt. Durch die Nutzung von Shell-Scripts können Sie einer Instance beim Start Anweisungen übermitteln. Sie können Benutzerdaten mit dem `modify-instance-attribute` AWS CLI Befehl oder der `ModifyInstanceAttribute` API-Aktion ändern.

So ändern Sie Benutzerdaten

1. Stoppen Sie Ihre Recheninstanz mit dem `stop-instances` AWS CLI Befehl.
2. Ändern Sie das `userData` Attribut mithilfe des `modify-instance-attribute` AWS CLI Befehls.
3. Starten Sie Ihre Compute-Instanz mit dem `start-instances` AWS CLI Befehl neu.

Es werden nur Shell-Skripts mit Datenverarbeitungs-Instances unterstützt. `cloud-init` Paketdirektiven auf Compute-Instances, die auf einem Snowcone laufen, werden nicht unterstützt. Weitere Informationen zum Arbeiten mit AWS CLI Befehlen finden Sie in der [AWS CLI Befehlsreferenz](#).

## Fehlerbehebung bei Compute-Instances auf Snowcone-Geräten

Im Folgenden finden Sie Tipps zur Fehlerbehebung für Snowcone-Jobs mit Compute-Instances.

Themen

- [Die virtuelle Netzwerkschnittstelle hat die IP-Adresse 0.0.0.0](#)
- [Snowcone hängt beim Starten einer großen Recheninstanz](#)
- [Meine Instance hat ein Stamm-Volumen](#)
- ["Ungeschützte private Schlüsseldatei"-Fehler](#)

### 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). Dies kann auch passieren, wenn Sie die falsche RJ45-Schnittstelle verwenden. Der Snowcone hat zwei RJ45-Schnittstellen. Möglicherweise haben Sie die falsche physische Schnittstelle angegeben

## 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 [Netzwerkconfiguration für Datenverarbeitungs-Instances](#).
- Aktualisieren Sie eine bestehende VNIC. Weitere Informationen finden Sie unter [Aktualisieren einer virtuellen Netzwerkschnittstelle](#).

## Snowcone hängt beim Starten einer großen Recheninstanz

Es kann den Anschein haben, dass Ihr Snowcone aufgehört hat, eine Instance zu starten. Dies ist im Allgemeinen nicht der Fall. Es kann jedoch eine Stunde oder länger dauern, bis große Datenverarbeitungs-Instances gestartet werden. Sie können den Status Ihrer Instances überprüfen, indem Sie den AWS CLI Befehl `aws ec2 describe-instances` run für den HTTP- oder HTTPS-Amazon EC2-Endpunkt auf dem Snowcone verwenden.

## Meine Instance hat ein Stamm-Volumen

Instances besitzen standardmäßig ein Stamm-Volume. Alle sbe-Instances haben ein einzelnes Root-Volume.

Weitere Informationen zum Hinzufügen zusätzlicher Volumes finden Sie unter <https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-snowcone-ebs.html>

## "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
```

## Zum AWS DataSync Übertragen von Dateien verwenden

AWS DataSync ist ein Online-Datenübertragungsdienst, der das Kopieren großer Datenmengen zu und von AWS Speicherdiensten über das Internet oder AWS Direct Connect von Speicherdiensten vereinfacht, automatisiert und beschleunigt. DataSync Der Agent ist auf Ihrem Snowcone-Gerät vorinstalliert. Es kann Daten zwischen dem Gerät und Amazon S3 S3-Buckets, Amazon EFS und Amazon FSx for Windows File Server übertragen. AWS DataSync kümmert sich automatisch um das Verschieben von Dateien und Objekten, die Planung von Datenübertragungen, die Überwachung des Übertragungsfortschritts, die Verschlüsselung, die Überprüfung von Datenübertragungen und die Benachrichtigung von Kunden über Probleme.

Bevor Sie den DataSync Agenten starten, aktivieren Sie das Network File System (NFS) auf Ihrem Snowcone-Gerät. Siehe [Automatische Konfiguration der NFS-Schnittstelle](#) und [NFS starten und Zugriff einschränken](#).

Der DataSync Agent ist während der Snowcone-Auftragsvorbereitung als AMI auf Ihrem Snowcone-Gerät vorinstalliert. Um Daten online zu übertragen AWS, verbinden Sie das Snowcone-Gerät mit dem externen Netzwerk und verwenden Sie AWS OpsHub oder die CLI, um das DataSync Agenten-AMI zu starten. Aktivieren Sie den DataSync Agenten, die AWS Management Console oder verwenden Sie die CLI und richten Sie Ihre Online-Datenübertragungsaufgabe zwischen dem Snowcone NFS-Speicher und Amazon S3, Amazon EFS oder Amazon FSx for Windows File Server ein.

Du kannst AWS DataSync das Laufen auf Snowcone für Folgendes nutzen:

- Edge-Computing-Anwendungen, um Daten zu sammeln, zu verarbeiten, um sofortige Erkenntnisse zu gewinnen, und die Daten dann online zu AWS übertragen.
- Übertragen Sie Daten, die kontinuierlich von Sensoren oder Maschinen generiert werden, online AWS in eine Fabrik oder an andere Edge-Standorte.
- Verteilen Sie Medien, wissenschaftliche oder andere Inhalte online von AWS Speicherdiensten an Ihre Partner und Kunden.
- Aggregieren Sie Inhalte, indem Sie Medien, wissenschaftliche oder andere Inhalte online von Ihren Edge-Standorten zu übertragen AWS.

- Stellen Sie sicher, dass Sie eine statische IP-Adresse für das VNI für den DataSync Agenten verwenden. Die Verwendung von DHCP kann zu Problemen führen, da jeder Gerätereustart bedeuten kann, dass Sie eine andere IP-Adresse verwenden, sodass sowohl der DataSync Agent als auch die Aktivierung in der Cloud neu konfiguriert werden müssen. DataSync AWS
- Um den Datasync-Agent auf Snowcone zu verwenden, müssen Sie sicherstellen, dass die Einträge „AllowedHosts“ die DataSync Agenten-IP-Adresse in Ihrer NFS-Konfiguration auf dem Snowcone enthalten. Möglicherweise müssen Sie den NFS-Dienst auf Snowcone beenden und neu starten, um den DataSync Agenten zu aktivieren.
- Immer wenn Sie den NFS-Dienst beenden, sollten Sie auch den DataSync Agenten beenden. Hinweis: Wenn Sie den NFS-Dienst beenden, der den aufgelisteten DataSync Agenten zugelassen hat, wird der Datasync-Agent nicht mehr funktionieren.
- Überprüfen Sie die [AWS DataSync Aufgabenkontingente](#) für die maximale Anzahl von Dateien pro Aufgabe für ein Snowcone-Gerät. Wenn Sie das Limit von 200.000 Dateien überschreiten, meldet die DataSync Aufgabe einen Fehler bei der Speicherzuweisung und bricht die Ausführung ab.

Für einmalige Edge-Compute- oder Datenübertragungsworkflows oder für Snowcone-Workflows an Edge-Standorten ohne WAN-Verbindung (Wide Area Network) oder unzureichender WAN-Bandbreite sollten Sie das Snowcone-Gerät zurücksenden, AWS um die Datenübertragung abzuschließen.

## Verwaltung der NFS-Schnittstelle

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

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

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

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

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, wenn möglich NFSv4.1 zu verwenden und Dateinamen mit Unicode UTF-8 zu codieren, um einen erfolgreichen Datenimport sicherzustellen. Dateinamen, die nicht mit UTF-8 codiert sind, werden je nach verwendeter NFS-Kodierung möglicherweise nicht nach S3 oder mit einem anderen Dateinamen nach S3 hochgeladen.
- Stellen Sie sicher, dass die maximale Länge Ihres Dateipfads weniger als 1024 Zeichen beträgt. Geräte der Snow Family unterstützen keine Dateipfade mit mehr als 1024 Zeichen. Eine Überschreitung dieser Dateipfadlänge führt zu Fehlern beim Dateimport.
- Weitere Informationen finden Sie unter [Objektschlüssel](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Bei NFS-basierten Übertragungen werden standardmäßige Metadaten im POSIX-Stil zu Ihren Objekten hinzugefügt, wenn sie von Geräten der Snow Family in Amazon S3 importiert werden. Darüber hinaus werden Sie die Metadaten „x-amz-meta-user-agent aws-datasync“ sehen, wie wir sie derzeit AWS DataSync als Teil des internen Importmechanismus in Amazon S3 für den Geräteimport von Snow Family mit NFS-Option verwenden.

#### Note

Der verfügbare Speicherplatz auf dem Snowcone-Gerät ist erst korrekt, wenn der NFS-Dienst gestartet wird.

Sie können die NFS-Schnittstelle auch mit AWS OpsHub einem GUI-Tool konfigurieren und verwalten. Weitere Informationen finden Sie unter [für die Offline-Dateiübertragung](#).

## NFS-Konfiguration für Geräte der Snow Family

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt. Sie müssen sie daher starten, um die Datenübertragung zum Gerät zu ermöglichen. Sie können die

NFS-Schnittstelle konfigurieren, indem Sie die IP-Adresse eines Virtual Network Interface (VNI) angeben, das auf dem 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 [Netzwerkconfiguration für Compute-Instances](#).

## Konfigurieren Sie Geräte der Snow Family 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-Dienstes zurück, `ACTIVE` oder `INACTIVE`

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  }
}
```

Wenn der Wert des `State` Namens lautet `ACTIVE`, ist der NFS-Schnittstellendienst aktiv und Sie können das 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 den Client-Computern.](#)

[Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und MacOS-Betriebssysteme aufgeführt.](#)

- [Windows:](#)

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

- Linux:

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

- macOS:

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

. Wenn der Wert lautet `INACTIVE`, müssen Sie den Dienst starten.

## Den NFS-Dienst auf dem Snow Family-Gerät starten

Starten Sie bei Bedarf eine virtuelle Netzwerkschnittstelle (VNI) und starten Sie dann den NFS-Dienst auf dem Snow Family-Gerät. Falls erforderlich, geben Sie beim Starten des NFS-Dienstes einen Block zulässiger Netzwerkadressen an. Wenn Sie keine Adressen angeben, ist der Zugriff auf die NFS-Endpunkte uneingeschränkt.

1. Verwenden Sie den `describe-virtual-network-interface` Befehl, um die auf dem Snow Family-Gerät verfügbaren VNIs anzuzeigen.

```
snowballEdge describe-virtual-network-interfaces
```

Wenn ein 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 des VNI, der mit der NFS-Schnittstelle verwendet werden soll.

2. Wenn keine VNIs verfügbar sind, verwenden Sie den `create-virtual-network-interface` Befehl, um ein VNI für die NFS-Schnittstelle zu erstellen. Weitere Informationen finden Sie unter [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\)](#).
3. Verwenden Sie den `start-service` Befehl, um den NFS-Dienst zu starten und ihn dem VNI zuzuordnen. Um den Zugriff auf die NFS-Schnittstelle einzuschränken, fügen Sie die `AllowedHosts` Parameter `service-configuration` und in den Befehl ein.

```

snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id
nfs --service-configuration AllowedHosts=CIDR-address-range

```

4. Verwenden Sie den `describe-service` Befehl, um den Dienststatus zu überprüfen. Es läuft, wenn der Wert des `State` Namens ist `ACTIVE`.

```

snowballEdge describe-service --service-id nfs

```



Der Befehl gibt den Dienststatus sowie die IP-Adresse und Portnummer des NFS-Endpunkts sowie die CIDR-Bereiche zurück, die für den Zugriff auf den Endpunkt zulässig sind.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Endpoints" : [ {
    "Protocol" : "nfs",
    "Port" : 2049,
    "Host" : "192.0.2.0"
  } ],
  "ServiceConfiguration" : {
    "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]
  }
}
```

## Mounten von NFS-Endpunkten auf Client-Computern

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

Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und MacOS-Betriebssysteme aufgeführt.

- Windows:

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

- Linux:

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

- macOS:

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

## Stoppen der NFS-Schnittstelle

Wenn Sie mit der Übertragung von Dateien über die NFS-Schnittstelle fertig sind und bevor Sie das Snow Family-Gerät ausschalten, beenden Sie den `stop-service` NFS-Dienst mit dem Befehl.

```
snowballEdge stop-service --service-id nfs
```

## Wird verwendet AWS IoT Greengrass , um vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen

AWS IoT Greengrass ist ein Open-Source-Edge-Runtime- und Cloud-Dienst für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können. Sie können AWS IoT Greengrass damit Software entwickeln, mit der Ihre Geräte lokal auf die von ihnen generierten Daten reagieren, Vorhersagen auf der Grundlage von Modellen für maschinelles Lernen ausführen und Gerätedaten filtern und aggregieren können. Ausführliche Informationen zu AWS IoT Greengrass finden Sie unter [Was ist AWS IoT Greengrass?](#) im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

Durch die Verwendung AWS IoT Greengrass auf Ihrem 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.

## Einrichtung Ihrer Amazon EC2-kompatiblen Instance


### Note

Um die Installation AWS IoT Greengrass Version 2 auf einem Snow Family-Gerät durchzuführen, stellen Sie sicher, dass Ihr Gerät mit dem Internet verbunden ist. Nach der

Installation ist kein Internet erforderlich, damit ein Snow Family-Gerät verwendet werden kann AWS IoT Greengrass.

Um eine EC2-kompatible Instanz einzurichten für AWS IoT Greengrass V2


1. Starten Sie das AWS IoT Greengrass validierte AMI mit einer öffentlichen IP-Adresse und einem SSH-Schlüssel:
  - a. Verwenden der AWS CLI: [Run-Instances](#).
  - b. Verwenden AWS OpsHub: [Starten einer Amazon EC2-kompatiblen Instance](#).

 Note

Notieren Sie sich die öffentliche IP-Adresse und den SSH-Schlüsselnamen, die der Instance zugeordnet sind.

2. Stellen Sie über SSH eine Connect zur EC2-kompatiblen Instance her. Führen Sie dazu den folgenden Befehl auf dem Computer aus, der mit Ihrem Gerät verbunden ist. Ersetzen Sie *ssh-key* durch den *Schlüssel*, mit dem Sie die EC2-kompatible Instance gestartet haben. *public-ip-address* Ersetzen Sie 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, einen kostenlosen Open-Source-SSH-Client, installieren und konfigurieren. Sie müssen den SSH-Schlüssel vom .pem Format in das PuTTY-Format konvertieren und eine Verbindung zu Ihrer EC2-Instance herstellen. Anweisungen zur Konvertierung vom .pem PuTTY-Format finden Sie unter [Konvertieren Ihres privaten Schlüssels mithilfe von PuTTYgen](#) im Amazon EC2 EC2-Benutzerhandbuch.

## Installation AWS IoT Greengrass

Als Nächstes richten Sie Ihre EC2-kompatible Instance als AWS IoT Greengrass Core-Gerät ein, das Sie für die lokale Entwicklung verwenden können.

Um zu installieren AWS IoT Greengrass

1. Verwenden Sie den folgenden Befehl, um die erforderliche Software für zu installieren AWS IoT Greengrass. Dieser Befehl installiert AWS Command Line Interface (AWS CLI) v2, Python 3 und Java 8.

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
&& unzip awscliv2.zip && sudo ./aws/install && sudo yum -y install python3
java-1.8.0-openjdk
```

2. Erteilen Sie dem Root-Benutzer die Berechtigung, die AWS IoT Greengrass Software auszuführen, und ändern Sie die Root-Rechte von root ALL=(ALL) ALL bis root ALL=(ALL:ALL) ALL in der Sudoers-Konfigurationsdatei.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Verwenden Sie den folgenden Befehl, um die AWS IoT Greengrass Core-Software herunterzuladen.

```
curl -s https://d2s8p88vqu9w66.cloudfront.net/releases/greengrass-nucleus-
latest.zip > greengrass-nucleus-latest.zip && unzip greengrass-nucleus-latest.zip -
d GreengrassCore && rm greengrass-nucleus-latest.zip
```

4. Verwenden Sie die folgenden Befehle, um Anmeldeinformationen für die Installation der AWS IoT Greengrass Core-Software bereitzustellen. Ersetzen Sie die Beispielwerte durch Ihre Anmeldeinformationen:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

**Note**

Dies sind Anmeldeinformationen des IAM-Benutzers in der AWS Region, nicht des Snow Family-Geräts.

5. Verwenden Sie den folgenden Befehl, um die AWS IoT Greengrass Core-Software zu installieren. Der Befehl erstellt AWS Ressourcen, die die Kernsoftware für den Betrieb benötigt, und richtet die Kernsoftware als Systemdienst ein, der beim Start des AMI ausgeführt wird.

Ersetzen Sie die folgenden Parameter im Befehl:

- `region`: Die AWS Region, in der Ressourcen gesucht oder erstellt werden sollen.
- `MyGreengrassCore`: Der Name der AWS IoT Sache für Ihr AWS IoT Greengrass Kerngerät.
- `MyGreengrassCoreGroup`: Der Name der AWS IoT Dinggruppe für Ihr AWS IoT Greengrass Kerngerät.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE \  
-jar ./GreengrassInstaller/lib/Greengrass.jar \  
--aws-region region \  
--thing-name MyGreengrassCore \  
--thing-group-name MyGreengrassCoreGroup \  
--thing-policy-name GreengrassV2IoTThingPolicy \  
--tes-role-name GreengrassV2TokenExchangeRole \  
--tes-role-alias-name GreengrassCoreTokenExchangeRoleAlias \  
--component-default-user ggc_user:ggc_group \  
--provision true \  
--setup-system-service true \  
--deploy-dev-tools true
```

**Note**

Dieser Befehl gilt für eine Amazon EC2-kompatible Instance, auf der ein Amazon Linux 2-AMI ausgeführt wird. Informationen zu einem Windows-AMI finden [Sie unter Installieren der AWS IoT Greengrass Core-Software](#).

Wenn Sie fertig sind, wird auf Ihrem Snow Family-Gerät ein AWS IoT Greengrass Core für Ihren lokalen Gebrauch ausgeführt.

## Für die Nutzung von AWS Diensten auf einem AWS Snowcone Gerät erforderliche Ports

Damit AWS Dienste auf einem AWS Snowcone 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	Protokoll	Kommentar
22	SSH	Gerätezustandsprüfung und für EC2 SSH
2049	NFS	NFS-Endpunkt
8008	HTTP	EC2-HTTP-Endpunkt
8243	HTTPS	EC2-HTTPS-Endpunkt
9091	HTTP	Endpunkt für die Geräteverwaltung

## Rückgabe des Snowcone-Geräts

Wenn Sie mit der Übertragung von Daten auf das Snowcone-Gerät fertig sind, bereiten Sie es für die Rückreise nach AWS vor. Vergewissern Sie sich vorher, dass alle Datenübertragungen an das Gerät zum Abschluss gebracht wurden.

Wenn die gesamte Kommunikation mit dem Gerät beendet ist, schalten Sie es einfach aus, indem Sie den Netzschalter drücken. Das Herunterfahren des Geräts dauert ca. 20 Sekunden.

## Trennen Sie das Snowcone-Gerät

Trennen Sie die Snowcone-Kabel. Das Gerät ist für die Rücklieferung bereit, sobald auf ihrer Oberseite auf dem E-Ink-Display das Rücksendeetikett erscheint. Welcher Kurierdienst für Ihre Region zuständig ist, erfahren Sie unter [Überlegungen zum Versand für AWS Snowcone](#).

### Auftragstypbezogene Überlegung

#### Important

Wenn Sie Daten importieren, löschen Sie Ihre lokalen Kopien der übertragenen Daten erst, wenn der Import erfolgreich abgeschlossen AWS ist und Sie die Ergebnisse der Datenübertragung überprüfen können.

#### Note

Sobald Sie das Snow-Gerät für den Import in Amazon S3 zurücksenden, AWS beginnt es 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 Ziel-S3-Bucket aufgenommen werden, können Sie beantragen, dass der Snow-Job storniert wird. Wenn Sie den Auftrag stornieren, überspringen wir die Datenübertragung und löschen das Gerät gemäß den festgelegten Verfahren sicher. Aufgrund unserer strengen Aufbewahrungskette und unserer strengen Betriebsverfahren können wir kein Gerät mit Ihren Daten in unseren Einrichtungen aufbewahren.

Informationen zum Versand des Geräts finden Sie unter [Überlegungen zum Versand für AWS Snowcone](#).

# Daten auf Ihrem Gerät schützen

Beachten Sie die folgenden Empfehlungen, um die Daten auf Ihrem AWS Snowcone Gerät zu schützen.

Themen

- [Sicherung Ihres AWS Snowcone](#)
- [Validieren von NFC-Tags](#)

## Sicherung Ihres AWS Snowcone

Im Folgenden finden Sie einige Sicherheitspunkte, die Sie bei der Verwendung von Snowcone beachten sollten, sowie einige allgemeine Informationen zu anderen Sicherheitsvorkehrungen, die wir treffen, wenn ein Gerät AWS zur Verarbeitung ankommt.

Wir empfehlen die folgenden Sicherheitsansätze:

- Nachdem Sie das Gerät erhalten haben, sollten Sie nach Beschädigungen und offensichtlichen Manipulationen suchen. Wenn Ihnen am Gerät irgendetwas Verdächtiges auffällt, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie sich stattdessen an den [AWS Support](#), um ein neues Gerät zu erhalten.
- Vermeiden Sie es möglichst, die Anmeldeinformationen für Ihren Auftrag offenzulegen. Jede Person mit Zugang zum Auftragsmanifest und zum Entsperrcode kann auf die Inhalte des Geräts für diesen Auftrag zugreifen.
- Lassen Sie das Gerät nicht auf einer Laderampe liegen. Auf einer Ladestation kann sie den Elementen ausgesetzt sein. Obwohl jedes Snowcone-Gerät robust ist, kann Wetter die robusteste Hardware beschädigen. Melden Sie gestohlene, vermisste oder defekte Geräte so schnell wie möglich. Je schneller ein Problem mit einer Appliance gemeldet wird, umso zügiger kann ein Ersatz versendet werden, um Ihren Auftrag abzuschließen.

### Note

Das Snowcone-Gerät ist Eigentum von. AWS Die Manipulation eines Geräts stellt einen Verstoß gegen die Nutzungsbedingungen dar AWS . Weitere Informationen finden Sie unter <http://aws.amazon.com/aup/>.



Wir führen die folgenden Sicherheitsschritte durch:

- Bei der Übertragung von Daten mit der Dateischnittstelle bleiben Objektmetadaten erhalten.
- Wenn ein Gerät bei uns ankommt AWS, überprüfen wir es auf Anzeichen von Manipulation und stellen sicher, dass das Trusted Platform Module (TPM) keine Änderungen festgestellt hat. Snowcone verwendet mehrere Sicherheitsebenen zum Schutz Ihrer Daten, darunter manipulationssichere Gehäuse, 256-Bit-Verschlüsselung und ein branchenübliches TPM, das sowohl Sicherheit als auch eine vollständige Aufbewahrungskette für Ihre Daten bietet.
- AWS führt nach der Verarbeitung und Überprüfung des Datenübertragungsauftrags eine Softwarelöschung des Snowcone-Geräts gemäß den Richtlinien des National Institute of Standards and Technology (NIST) zur Medienbereinigung durch.

## Validieren von NFC-Tags

AWS Snowcone In Geräte sind NFC-Tags eingebaut. Sie können diese Tags mit der Snowcone 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 NFC-Tags umfasst die Verwendung des Snowball Edge-Clients zur Generierung eines gerätespezifischen QR-Codes, um zu überprüfen, ob die Tags, die Sie scannen, für das richtige Gerät sind. Weitere Informationen finden Sie unter [Anfordern Ihres QR-Codes für die NFC-Validierung](#).

Das folgende Verfahren beschreibt, wie Sie die NFC-Tags auf einem Snowcone-Gerät validieren. Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden ersten Schritte der Übung „Erste Schritte“ durchgeführt haben:

1. Erstellen des ersten Auftrags Weitere Informationen finden Sie unter [Einen Auftrag zur Bestellung eines Snow Family-Geräts](#) erstellen.
2. Eingang des Geräts
3. Herstellen einer Verbindung mit dem lokalen Netzwerk
4. Abrufen von Anmeldeinformationen und Tools Weitere Informationen finden Sie unter [Abrufen von Anmeldeinformationen](#).
5. Laden Sie den Snowball Edge-Client herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Den AWS Snowball Edge Client verwenden](#).

## Um die NFC-Tags in einem AWS Snowcone Gerät zu validieren

1. Führen Sie den `snowballEdge get-app-qr-code` Snowball Edge-Client-Befehl aus. 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. Um die NFC-Tags mit Ihrem Telefon zu scannen, laden Sie die Snowcone Verification App herunter und installieren Sie sie. Laden Sie die App aus dem Google Play Store herunter, wenn Sie ein Android-Smartphone 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:

- Laden Sie die App auf ein anderes Smartphone herunter und versuchen Sie es erneut.
- Bringen Sie das Gerät in einen isolierten Bereich des Raums, fern von Störungen durch andere NFC-Tags, und versuchen Sie es erneut.
- Wenn die Probleme weiterhin bestehen, wenden Sie sich an [AWS Support](#)

# Grundlegendes zum AWS Snowcone Jobstatus

Wenn Sie einen AWS Snowcone Job erstellen, durchläuft er den Jobstatus, und der Status wird auf der Managementkonsole für die AWS Snow-Familie angezeigt.

Um den Status eines Jobs zu sehen

1. Loggen Sie sich in die [Managementkonsole für die AWS Snow-Familie](#).
2. Wählen Sie im Job-Dashboard den Job aus.
3. Klicken Sie in der Konsole auf Ihren Jobnamen.
4. Der Bereich Auftragsstatus befindet sich ganz oben und gibt den Status des Jobs wieder.

## Note

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

## AWS Snowcone Jobstatus des Geräts

Aufgabenstatus	Bedeutung
Job created	Ihr Auftrag ist gerade erstellt worden. Nur in diesem Status können Sie einen Auftrag abbrechen (einen Exportauftrag auch teilweise).
Gerät wird vorbereitet	AWS bereitet ein Gerät für Ihren Job vor.
Preparing shipment	AWS bereitet den Versand eines Geräts an Sie vor.

Aufgabenstatus	Bedeutung
In transit to you	Das Gerät wurde an die Adresse versendet, die Sie bei Erstellung des Auftrags angegeben haben.
Delivered to you	Das Gerät ist an die Adresse ausgeliefert worden, die Sie bei Erstellung des Auftrags angegeben haben.
Auf dem Weg nach AWS	Sie haben das Gerät zurückgeschickt an AWS.
Im Sortierzentrum	Das Gerät, das für diesen Auftrag notwendig ist, befindet sich in unserem internen Sortierzentrum. Jede weitere Verarbeitung von Importaufträgen in Amazon S3 wird in Kürze beginnen, normalerweise innerhalb von 2 Tagen.
Bei AWS	Ihre Sendung ist bei eingetroffen AWS. Wenn Sie Daten importieren, beginnt der Import in der Regel innerhalb eines Tages nach Ankunft der Sendung.
Importing	AWS importiert Ihre Daten in Amazon S3.
Completed	Ihr Auftrag bzw. ein Teil Ihres Auftrags wurde erfolgreich abgeschlossen.
Canceled	Ihr Auftrag wurde abgebrochen.

# 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 zum Ausführen 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 an AWS Management Console und öffnen Sie die Amazon SNS SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Wählen Sie im Navigationsbereich 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 AWS KMS-Schlüssel und dann den benutzerdefinierten KMS-KMS aus der Liste aus. Anweisungen zum Erstellen eines benutzerdefinierten KMS finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Um einen benutzerdefinierten KMS-ARN von Ihrem AWS Konto oder einem anderen AWS Konto zu verwenden, geben Sie den KMS-Schlüssel-ARN in das Feld AWS KMS-Schlüssel ein.

6. Wählen Sie Änderungen speichern 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 Key Management Service (AWS KMS) -Konsole an AWS Management Console und öffnen Sie sie unter <https://console.aws.amazon.com/kms>.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

3. Ändern Sie in der oberen rechten Ecke der Konsole die Region AWS-Region der Konsole auf dieselbe Region, in der das Snow-Gerät bestellt wurde.
4. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
5. Wählen Sie in der Liste der KMS-Schlüssel den Alias oder die Schlüssel-ID des KMS-Schlüssels aus, der aktualisiert werden soll.
6. Wählen Sie die Registerkarte Schlüsselrichtlinie. In den wichtigsten Richtlinienanweisungen können Sie die Prinzipale sehen, denen durch die Schlüsselrichtlinie Zugriff auf den KMS-Schlüssel gewährt wurde, und Sie können sehen, welche Aktionen sie ausführen können.
7. Fügen Sie für den Snow Service Principal "importexport.amazonaws.com" die folgende Richtlinienerklärung "kms:Decrypt" und die folgenden "kms:GenerateDataKey\*" Aktionen hinzu:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "service.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:service:region:customer-account-id:resource-type/customer-resource-id"
    }
  },
  "StringEquals": {
    "kms:EncryptionContext:aws:sns:topicArn": "arn:aws:sns:your_region:customer-account-id:your_sns_topic_name"
  }
}
```

8. Wählen Sie Änderungen speichern, um die Änderungen zu übernehmen und den Policy-Editor zu beenden.

## 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" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) has been created. More
info - https://console.aws.amazon.
com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neexw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaliEGLrIIIL4esi11lhIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJIiYPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.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" : "FMG5t1ZhJNHLHUXvZgtZz1k24FzVa7oX0T4P03neeXw8ZEXZx6z35j2F0TuNYShn2h0bKNC/zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAIkP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi111hIkgerCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7Ta1MD01zmJu0rExtnSIbZew3foxgx8GT+1bZkLd0ZdtRJIYPRP44eyq78sU0Eo/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" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being Exported.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtDRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

In transit to you

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is in transit to
you. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtRJIYPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Delivered to you

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) was delivered to
you. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtDRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```



Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Auf dem Weg nach AWS

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is in transit to
AWS. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtDRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Im Sortierzentrum

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is at AWS sorting
facility. More info - https://
console.aws.amazon.com/impor
texport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAikP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkg
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd507lX1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD0lzmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

```
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Bei AWS

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is at AWS. More info
- https://console.aws.amazon.com/
importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtRJIYPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

### Importing

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being imported.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtDRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```



Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Completed

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) complete.\nThanks
for using AWS Snow Family.\nCan you
take a quick survey on your experienc
e? Survey here: http://bit.ly/1pLQ
JMY. More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi11lhIkg
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtdRJIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

### SNS-Benachrichtigung (JSON)

```
22223333:ExampleTopic1:e103  
9402-24e7-40a3-a0d4-797da162b297"  
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

## SNS-Benachrichtigung (JSON)

Abgebrochen

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) was canceled. More
info - https://console.aws.amazon.
com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+T0yaLiEGLrIIIL4esi111hIkG
ErCuy5btPcWXBdio2fpCRD5x9oR
6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/
iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7
Ta1MD01zmJu0rExtnSIbZew3foxgx8GT
+1bZkLd0ZdtDRJlIyPRP44eyq78sU0Eo/
LsDr0Iak4ZDpg8dXg==",
  "SigningCertURL" : "https://
sns.us-east-1.amazonaws.com/
SimpleNotificationService-010a507c1
833636cd94bdb98bd93083a.pem",
  "UnsubscribeURL" : "https://
sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn
=arn:aws:sns:us-east-2:1111
22223333:ExampleTopic1:e103
9402-24e7-40a3-a0d4-797da162b297"
}
```

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

# Den AWS Snowcone Bestellvorgang verstehen

Bei der Bestellung eines gibt es zwei Möglichkeiten. AWS Snowcone Sie können über die bestellen Managementkonsole für die AWS Snow-Familie oder Sie können die Job Management API (JMAPI) verwenden.

## Den Versandprozess verstehen

In diesem Abschnitt finden Sie Informationen darüber, wie der Versand für ein AWS Snowcone Gerät abgewickelt wird, sowie eine Liste der AWS-Regionen unterstützten Geräte. Informationen zu den unterstützten Regionen und Endpunkten finden Sie unter [AWS Snow Family-Endpunkte und -Kontingente](#) in der. Allgemeine AWS-Referenz Der Versandtarif, den Sie für einen Auftrag wählen, gilt für den Versand und Empfang des für diesen Auftrag verwendeten Snowcone-Geräts. Informationen zu den Versandkosten finden Sie unter [AWS Snowcone Preise](#).

### Note

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

## Rückgabe eines Snowcone-Geräts

Die vorausbezahlten Versandinformationen auf dem E Ink-Display enthalten die richtige Adresse für die Rücksendung des Geräts. Informationen zur Rückgabe Ihres Snowcone-Geräts finden Sie unter [Versandanbieter](#). Das Snowcone-Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. Der Kurierdienst für Ihre Region bietet die Möglichkeit zur Sendungsverfolgung. Sie können Statusänderungen Ihrer Aufträge über die Managementkonsole für die AWS Snow-Familie verfolgen.

### Important

Bringen Sie kein separates Versandetikett auf dem Snowcone-Gerät an AWS, sofern Sie nicht persönlich etwas anderes angewiesen haben. Verwenden Sie immer das Versandetikett, das auf dem E-Ink-Display des Geräts angezeigt wird.

## Mit dem AWS Management Console

Sie können ein Snowcone-Gerät über die Managementkonsole für die AWS Snow-Familie bestellen.

### Den Snowcone von der Konsole aus bestellen

Eine schrittweise Anleitung zur Bestellung eines Snowcone über die AWS Snowball Konsole finden Sie unter. [Erste Schritte](#)

## Verwenden der Job Management API

Die Job Management API (JMAPI) bietet programmatischen Zugriff auf dieselben Funktionen, die in der Managementkonsole für die AWS Snow-Familie verfügbar sind. Auf diese Weise können Sie die Auftragsfunktionalität automatisieren. Mithilfe der JMAPI können Sie den Auftragsstatus einsehen, Jobs erstellen, die Manifestdatei herunterladen, den Code entsperren und Berichte über den Auftragsabschluss einsehen. Da die Aufrufe über die API erfolgen, können Sie diese Aufrufe in eine benutzerdefinierte Anwendung oder ein Web-Frontend integrieren.

### Themen

- [Allgemeine Verwendungszwecke von JMAPI](#)
- [JMAPI Erforderliche Zeichenketten](#)
- [JMAPI-Endpunkte](#)
- [JMAPI-CLI-Befehle](#)
- [Beispiele](#)

### Allgemeine Verwendungszwecke von JMAPI

- Automatisieren der Bestellung von Snowcone-Geräten
- Die Manifest-Datei wird heruntergeladen
- Die Entsperrdatei wird heruntergeladen
- Liste der aktuellen Snowcone-Jobs
- Den Snowcone-Auftragsabschlussbericht herunterladen

## JMAPI Erforderliche Zeichenketten

Wenn Sie eine Bestellung über die Job-Management-API aufgeben, verwenden Sie die folgenden erforderlichen Parameter, die anhand von Beispielen veranschaulicht werden.

```
--job-type
--resources
--address-id
--region
--role-arn
--kms-key-arn
--shipping-option
--device-type
--description
```

## JMAPI-Endpunkte

### API-Endpunkt

Um Aufrufe an jeden Endpunkt zu tätigen, ist das FormatsnowballEdge.*region*.amazonaws.com. Im Folgenden finden Sie einige Beispiele, die Ihnen helfen sollen, die Aufschlüsselung des Endpunkts zu verstehen.

### Example

Region	Endpunkt
USA Ost (Nord-Virginia)	snowball.us-east-1.amazonaws.com
USA West (Oregon)	snowball.us-west-2.amazonaws.com

## JMAPI-CLI-Befehle

### Befehlsverwaltungs-CLI

Im Folgenden sind die CLI-Aufrufe aufgeführt, die Sie für die Job-Management-API ausführen können.



Befehl	Beispiel
Auflisten von Aufträgen	<code>aws snowball list-jobs</code>
Describe Job	<code>aws snowball describe-job --job-id [JOB ID]</code>
Beschreiben Sie die Adresse	<code>aws snowball describe-address --address-id</code>
Adresse erstellen	<code>aws snowball create-address --cli-input-json file://create-address.json</code>
Erstellen von Aufträgen	<code>aws snowball create-job --cli-input-json file://create-job.json</code>
Auftrag abbuchen	<code>aws snowball cancel-job --job-id [JOB ID]</code>

## Beispiele

Im Folgenden finden Sie Beispiele für Befehle, die die Job-Management-API verwenden.

### KMS JSON-Beispiel

Das folgende JSON-Beispiel ist eine ordnungsgemäß formatierte JSON-Datei für die Verwendung der AWS KMS Richtliniendatei.

```
{
  "KeyMetadata": {
    "Origin": "AWS_KMS",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Description": "",
    "KeyManager": "CUSTOMER",
    "Enabled": true,
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "Enabled",
    "CreationDate": 1502910355.475,
```

```
"Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "AWSAccountId": "111122223333"
}
```

## Beispiel für eine Adresse erstellen

Die folgenden Beispiele zeigen Ihnen, wie Sie den Befehl formatieren würden, um Ihre Adresse zu erstellen, und wie die Antwort lautet, wenn er erfolgreich ist.

```
aws snowball create-address --address "Name=Bob,Company=AWS,Street1=1234 Fake
St.,City=All,StateOrProvince=Any,Country=US,PostalCode=12345,PhoneNumber=1234567890"
```

## Beispielausgabe

```
{
  "AddressId": "ADID3be640c8-1111-1111-1111-917f201ffa42"
}
```

## Beispiel für einen Job erstellen

Der folgende Befehl zeigt Ihnen einen Beispielbefehl zum Ausführen des `create-job` Befehls.

```
aws snowball create-job --job-type IMPORT --resources file://path/to/resources.json
--address-id ADID3be640c8-1111-1111-1111-917f201ffa42 --region us-east-1 --role-
arn arn:aws:iam::123456789123:role/example_role --kms-key-arn arn:aws:kms:us-
west-2:000000000000:key/Example --snowball-capacity-preference T14 --device-
configuration file://path/to/configuration.json --shipping-option SECOND_DAY --
snowball-type SNC1_SSD
```

Mit dem obigen `create-job` Befehl wird ein Importauftrag in der Region `us-east-1` mit einem Snowcone-Gerät vom Typ `SNC1_SSD` mit der Kapazitätspräferenz `T14` und der Versandoption `SECOND_DAY` erstellt.

## Exportieren eines AMI zur Verwendung mit Amazon EC2 EC2-Jobs

Dieser Abschnitt bietet einen Überblick darüber, wie Sie Ihr Amazon Machine Image (AMI) zur Verwendung mit Amazon EC2-kompatiblen Recheninstanzen auf einem AWS Snowcone Gerät exportieren.

## Themen

- [Konfiguration eines AMI für die Verwendung von SSH für die Connect zu Compute-Instances, die auf dem Gerät gestartet wurden](#)
- [Erstellen Sie Ihren Job mithilfe der Konsole](#)
- [Erstellen Sie Ihren Job mit der AWS CLI](#)

## Konfiguration eines AMI für die Verwendung von SSH für die Connect zu Compute-Instances, die auf dem Gerät gestartet wurden

Um Secure Shell (SSH) für die Verbindung zu Ihren Recheninstanzen auf Snowcone-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 mit SSH keine Verbindung zu Ihren Instances herstellen, wenn Sie Ihr Snowcone-Gerät erhalten.

So fügen Sie einen SSH-Schlüssel einem AMI hinzu

1. Starten Sie eine neue Instance unter AWS Cloud Verwendung eines kompatiblen AMI-Images (siehe <https://docs.aws.amazon.com/snowball/latest/developer-guide/using-ami.html>).

Wenn Sie Ihre Instance starten, stellen Sie sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihre spätere Verwendung auf dem Snowcone-Gerät geeignet ist. In der Amazon EC2 EC2-Konsole tun Sie dies in Schritt 4: Speicher hinzufügen. Eine Liste der unterstützten Größen für Compute-Instance-Speichervolumen auf einem Snowcone finden Sie unter "[ec2-snowcone-limits](#)".

2. Installieren und konfigurieren Sie die Anwendungen, die Sie auf dem Snowcone ausführen möchten, und testen Sie, ob sie erwartungsgemäß 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 Snowcone 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](#).
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 Sie Ihren Job mithilfe der Konsole

Ihr nächster Schritt besteht darin, einen Auftrag zur Bestellung eines Snow Family-Geräts zu erstellen. Ihr Auftrag kann ein beliebiger Auftragstyp sein, einschließlich eines Clusters. Folgen Sie mit dem den Anweisungen unter [Auftrag erstellen Managementkonsole für die AWS Snow-Familie, um ein Snow Family-Gerät zu bestellen](#). Wenn Sie im Assistenten zur Auftragserstellung zur Seite Schritt 3: Jobdetails angeben gelangen, fügen Sie die folgenden zusätzlichen Schritte hinzu.

1. Wählen Sie **Datenverarbeitung mit EC2 aktivieren** aus.
2. Wählen Sie **Ein AMI hinzufügen** aus.
3. Wählen Sie im sich öffnenden Dialogfenster ein AMI aus und wählen Sie **Speichern** aus.
4. Fügen Sie Ihrem Job je nach Gerätetyp insgesamt bis zu 20 AMIs hinzu.
5. Legen Sie Ihren Auftrag wie gewohnt an.

## Erstellen Sie Ihren Job mit der AWS CLI

Sie können Ihren Job auch mit AWS Command Line Interface (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::123456789012:role/snowcone-import-snowcone-role --shipping-option SECOND_DAY --snowball-type SNC1_HDD --snowball-capacity-preference T8
```

```
--device-configuration '{"SnowconeDeviceConfiguration":{"WirelessConnection":  
{"IsWifiEnabled": false}}}'
```

Nachdem das Gerät angekommen ist und Sie Ihr Gerät entsperrt haben, verwenden Sie den Snowball Edge-Client, um Ihre lokalen Anmeldeinformationen abzurufen. Weitere Informationen finden Sie unter [Abrufen von Anmeldeinformationen](#).

# Überlegungen zum Versand für AWS Snowcone

Im Folgenden finden Sie Informationen darüber, wie der Versand für ein AWS Snowcone Gerät abgewickelt wird, sowie eine Liste, in der alle AWS-Region unterstützten Geräte aufgeführt sind. Der Versandtarif, den Sie für einen Auftrag wählen, gilt sowohl für den Versand als auch für den Empfang des für diesen Auftrag verwendeten AWS Snowcone Geräts. Informationen zu den Versandkosten finden Sie unter [AWS Snowcone Preise](#).

## Themen

- [Ein AWS Snowcone Gerät für den Versand vorbereiten](#)
- [Versandeinschränkungen nach Regionen](#)
- [Versand eines AWS Snowcone Geräts](#)

Wenn Sie einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen, geben Sie eine Lieferadresse und eine Versandgeschwindigkeit an. Diese Versandgeschwindigkeit gibt nicht an, wie schnell Sie ab dem Tag, an dem Sie den Auftrag erstellt haben, mit dem Erhalt des AWS Snowcone Geräts rechnen können. Es wird nur die Uhrzeit angezeigt, zu der sich das Gerät zwischen AWS und Ihrer Lieferadresse befindet. In dieser Zeit ist keine Bearbeitungszeit enthalten, was von Faktoren wie der Auftragsart abhängt (Exporte dauern in der Regel länger als Importe). Außerdem holen Mobilfunkanbieter ausgehende AWS Snowcone Geräte in der Regel nur einmal am Tag ab. Daher kann die Bearbeitungszeit vor dem Versand auch länger dauern als einen Tag.

### Note

Geräte von Snow Family können nur dort zurückgegeben werden AWS-Region , wo sie bestellt wurden. In einigen AWS Regionen wird der Versand von Snow Family-Geräten in ein anderes Land unterstützt als das, in dem das Gerät bestellt wurde. Weitere Informationen finden Sie unter [Versandeinschränkungen nach Regionen](#).

## Ein AWS Snowcone Gerät für den Versand vorbereiten

Im Folgenden wird erklärt, wie Sie einen Snowcone vorbereiten und an AWS ihn zurücksenden.

## Um ein AWS Snowcone Gerät für den Versand vorzubereiten

1. Vergewissern Sie sich, dass Sie die Übertragung aller Daten für diesen Auftrag zum oder vom AWS Snowcone Gerät abgeschlossen haben. [Entsperren Sie das Gerät.](#)
2. Drücken Sie den Netzschalter an der Vorderseite des Geräts, der sich in der Nähe der Anzeigelampen gegenüber den Netzwerkanschlüssen befindet. Das Herunterfahren des Geräts dauert ca. 20 Sekunden.

Wenn Sie Ihr Snowcone-Gerät ausgeschaltet und vom Stromnetz getrennt haben und die Versandinformationen nach etwa einer Minute nicht auf dem E Ink-Bildschirm erscheinen, finden Sie weitere Informationen unter. [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten](#)

## Versandeinschränkungen nach Regionen

Bevor Sie einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen, sollten Sie sich von der Konsole aus, auf der sich Ihre Daten befinden AWS-Region , bei der Konsole anmelden. Snow Family-Geräte werden nicht zwischen internationalen Ländern versendet, z. B. vom asiatisch-pazifischen Raum (Indien) nach dem asiatisch-pazifischen Raum (Australien).

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

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

Lieferungen im Inland innerhalb desselben Landes sind zulässig. Beispiele:

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

 Note

AWS versendet Snow Family-Geräte nicht an Postfächer.

## Versand eines AWS Snowcone Geräts

Die vorausbezahlten Versandinformationen auf dem E Ink-Display enthalten die richtige Adresse für die Rücksendung des AWS Snowcone Geräts. Informationen darüber, wie Sie Ihr AWS Snowcone Gerät zurücksenden können, finden Sie unter [the section called “Versandanbieter”](#). Das AWS Snowcone Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. Der Kurierdienst für Ihre Region bietet die Möglichkeit zur Sendungsverfolgung. Sie können Statusänderungen für Ihren Job verfolgen, indem Sie den verwenden Managementkonsole für die AWS Snow-Familie.

Wenn Sie Ihr Snowcone-Gerät ausgeschaltet und vom Stromnetz getrennt haben und die Versandinformationen nach etwa einer Minute nicht auf dem E Ink-Bildschirm erscheinen, finden Sie weitere Informationen unter [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten](#)

## Versandanbieter

Wenn Sie einen Auftrag zur Bestellung eines Snow Family-Geräts erstellen, geben Sie die Adresse an, an die das Gerät versendet werden soll. AWS Snowcone Der Transporteur, der Ihre Region unterstützt, kümmert sich AWS um den Versand der AWS Snowcone Geräte von zu Ihnen und zurück AWS. Wenn ein AWS Snowcone Gerät versendet wird, erhalten Sie eine Sendungsverfolgungsnummer. Sie finden die Tracking-Nummer jedes Jobs und einen Link zur Tracking-Website im [Managementkonsole für die AWS Snow-Familie](#) Job-Dashboard oder mithilfe von API-Aufrufen an die Job-Management-API.

Im Folgenden finden Sie eine Liste der unterstützten Mobilfunkanbieter für AWS Snowcone Geräte nach Regionen:

- In Indien erfolgt der Versand durch Blue Dart.
- Für Südkorea, Japan, Australien, Indonesien, Israel und Singapur ist Kühne + Nagel der Mobilfunkanbieter.
- Für China ist S.F. Express der Transporteur.
- In allen anderen Regionen erfolgt der Versand per [UPS](#).



## AWS Snowcone Abholungen in Kanada, der EU, Südafrika und den USA

Beachten Sie in Kanada, der EU, Südafrika und den USA die folgenden Informationen, damit UPS ein AWS Snowcone Gerät abholen kann:

- Vereinbaren Sie, dass UPS das AWS Snowcone Gerät abholt, indem Sie direkt eine Abholung mit UPS vereinbaren, oder bringen Sie das Gerät zu einer UPS-Paketabgabestelle, an die es versendet werden soll. AWS
- Das vorausbezahlte UPS-Versandetikett auf dem E Ink-Display enthält die richtige Adresse für die Rücksendung des AWS Snowcone Geräts.
- Das AWS Snowcone Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. UPS stellt automatisch eine Sendungsverfolgungsnummer für Ihre Sendung zur Verfügung.

Der UPS-Service für Snow Family-Geräte ist nur innerhalb eines Landes im Inland verfügbar.

## AWS Snowcone Abholungen in Brasilien

Beachten Sie in Brasilien die folgenden Informationen, damit UPS einen Snowcone abholen kann:

- Wenn Sie bereit sind, einen Snowcone zurückzugeben, rufen Sie 0800-770-9035 an, um eine Abholung mit UPS zu vereinbaren.
- Snowcone ist im Inland in Brasilien erhältlich, das 26 Bundesstaaten und den Distrito Federal umfasst.
- Halten Sie, sofern vorhanden, Ihre Betriebszulassungsnummer (Cadastro Nacional de Pessoa Juridica, CNPJ) bereit, bevor Sie einen Auftrag erstellen.
- Sie sollten das entsprechende Dokument für die Rücksendung des Snowcone-Geräts ausstellen. Bestätigen Sie mit Ihrer Steuerabteilung, welche der folgenden Dokumente in Ihrem Staat gemäß Ihrer ICMS-Anmeldung erforderlich sind:
  - Innerhalb von São Paulo sind in der Regel eine Nicht-ICMS-Erklärung und eine elektronische Steuerrechnung (NF-e) erforderlich.
  - Außerhalb von São Paulo — Folgendes ist in der Regel erforderlich:
    - Eine Erklärung zur Befreiung von der Warenumlaufsteuer
    - Eine Nota Fiscal
    - Elektronische Steuerrechnung (NF-e)

**Note**

Bei Unternehmen ohne ICMS-Steuererklärung empfehlen wir, vier Kopien der Erklärung zu erstellen: eine für Ihre Unterlagen, die anderen drei für den Transport.

## AWS Snowcone Abholungen in Israel

Vereinbaren Sie in Israel die Abholung, indem Sie sich AWS per E-Mail an [snowball-shipping@amazon.com](mailto:snowball-shipping@amazon.com) wenden. Geben Sie Snowcone Pickup Request als Betreff ein und fügen Sie folgende Informationen hinzu:

- Job-ID — Die Job-ID, die dem Snow-Gerät zugeordnet ist, das Sie zurückgeben. Sie finden die Job-ID in der [Managementkonsole für die AWS Snow-Familie](#).
- Abholadresse — Die Adresse, an der das Gerät abgeholt wird.
- Abholdatum — Das früheste Datum, an dem das Gerät abgeholt werden soll.
- Kontaktdetails — Der Name, die E-Mail-Adresse und die lokale Telefonnummer, die der Versanddienstleister Kühne + Nagel bei Bedarf für Informationen zur Abholung verwenden kann.

In Kürze erhalten Sie eine Folge-E-Mail von AWS Support mit Informationen zur Abholung Ihres Geräts an der von Ihnen angegebenen Adresse. Bereiten Sie das Gerät für den Versand vor und bereiten Sie es für die Abholung vor, normalerweise vor 12:00 Uhr Ortszeit. Siehe [Ein AWS Snowcone Gerät für den Versand vorbereiten](#).

## AWS Snowcone Abholungen in Großbritannien

Beachten Sie im Vereinigten Königreich die folgenden Informationen, damit UPS ein AWS Snowcone Gerät abholen kann.

- Sie veranlassen, dass UPS das AWS Snowcone Gerät abholt, indem Sie direkt eine Abholung mit UPS vereinbaren oder das Gerät zu einer UPS-Paketabgabestelle bringen, an die es versendet werden soll. AWS
- Das vorausbezahlte UPS-Versandetikett auf dem E Ink-Display enthält die richtige Adresse für die Rücksendung des AWS Snowcone Geräts.
- Das AWS Snowcone Gerät wird an eine AWS Sortieranlage geliefert und an das AWS Rechenzentrum weitergeleitet. UPS übermittelt Ihnen automatisch eine Sendungsverfolgungsnummer zu Ihrem Auftrag.

**⚠ Important**

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

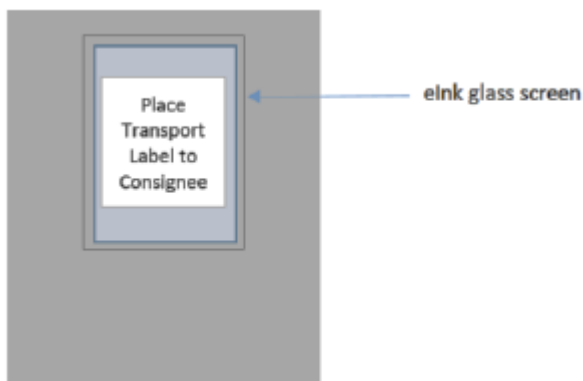
Der UPS-Service für die Produkte der Snow-Produktfamilie ist nur innerhalb eines Landes verfügbar.

**ℹ Note**

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

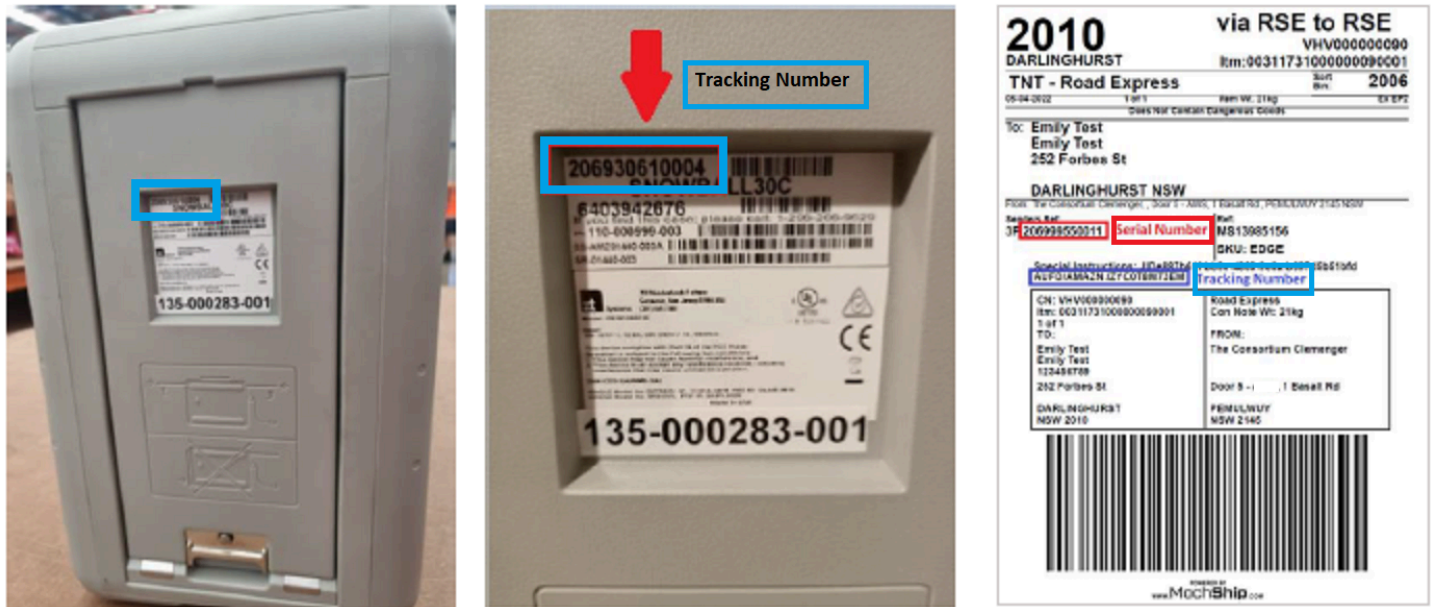
## AWS Snowcone Abholungen in Australien

Wenn du in Australien ein AWS Snowcone Gerät zurücksendest AWS, lege das Rücksendetikett (in dem Beutel mit diesen Anweisungen) auf das eInk-Etikett auf dem Snowgerät.



Wenn Sie kein Rücksendetikett zusammen mit Ihrem Snow-Gerät erhalten haben, senden Sie bitte eine E-Mail mit Ihrer Geräteseriennummer oder Referenznummer an [knau.snowball\\_return@kuehne-nagel.com](mailto:knau.snowball_return@kuehne-nagel.com).

### Example where to locate tracking number and serial number



Um die Rückgabe des Snow-Geräts zu vereinbaren, senden Sie bitte eine E-Mail an [knau.snowball\\_return@kuehne-nagel.com](mailto:knau.snowball_return@kuehne-nagel.com) mit den folgenden Informationen:

- Ihr Name
- Tracking-Nummer (wie blau dargestellt)
- Seriennummer des Geräts (wie rot dargestellt)
- Vollständige Abholadresse
- Kontaktperson bei der Abholung
- Kontakttelefonnummer bei der Abholung
- Datum der Abholung
- Abholfenster (mindestens 3 Stunden innerhalb der Geschäftszeiten)

#### Note

Tag und Uhrzeit der Abholung müssen ein Werktag innerhalb der Geschäftszeiten sein  
Das Team von Kühne + Nagel wird Ihnen antworten, um den Eingang der Abholanfrage zu bestätigen.

## AWS Snowcone Abholungen in Indien

In Indien nimmt Blue Dart das Snowcone-Gerät auf. Wenn Sie bereit sind, Ihr Snowcone-Gerät zurückzugeben, schalten Sie es aus und bereiten Sie es für den Rückversand vor. Um die Abholung zu vereinbaren, senden Sie eine E-Mail [an\\_snowball-pickup@amazon.com](mailto:an_snowball-pickup@amazon.com) mit dem Betreff Snowcone Pickup Request. Geben Sie in der E-Mail folgende Informationen an:

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

Das Snowcone-Team arrangiert die Abholung mit Blue Dart und sendet Ihnen eine Bestätigungs-E-Mail. Blue Dart stellt Ihnen ein Versandetikett aus paper zur Verfügung und holt das Snowcone-Gerät ab.

### Important

Wenn Sie einen Snowcone in Indien verwenden, denken Sie daran, alle relevanten Steuerunterlagen bei Ihrem Bundesstaat einzureichen.

## AWS Snowcone Abholung in Südkorea

In Südkorea kümmert sich Kühne + Nagel um Ihre Abholungen. Wenn Sie bereit sind, Ihr Gerät zurückzugeben, senden Sie eine E-Mail an [snowball-shipping@amazon.com](mailto:snowball-shipping@amazon.com) mit dem Betreff Snowcone Pickup Request, damit wir die Abholung für Sie vereinbaren können. Geben Sie im Text der E-Mail folgende Informationen an:

- Job-ID — Die Job-ID, die dem Snowcone zugeordnet ist, zu dem Sie zurückkehren möchten AWS.
- Abholadresse — Die Adresse, an der das Gerät abgeholt wird.
- Abholdatum — Der früheste Tag, an dem Sie das Gerät abholen möchten.

- Kontaktdaten für einen Ansprechpartner – Name, E-Mail-Adresse und Telefonnummer, damit Kühne+Nagel Kontakt aufnehmen kann, wenn notwendig.

In Kürze erhalten Sie von der eine Folge-E-Mail AWS Support mit Informationen zur Abholung Ihres Geräts an der von Ihnen angegebenen Adresse. Bereiten Sie das Gerät für den Versand vor (siehe [Ein AWS Snowcone Gerät für den Versand vorbereiten](#)) und bereiten Sie es in der Regel zwischen 13:00 und 15:00 Uhr Ortszeit zur Abholung vor.

## AWS Snowcone Abholungen in Hongkong

In Hongkong kümmert sich S.F. Express um Ihre Abholungen. Wenn Sie bereit sind, Ihr Gerät zurückzugeben, senden Sie eine E-Mail an [snowball-shipping-ap-east-1@amazon.com](mailto:snowball-shipping-ap-east-1@amazon.com) mit dem Betreff Snowcone Pickup Request, damit wir die Abholung für Sie vereinbaren 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 das Gerät abgeholt werden soll.
- Früheste bevorzugte Abholzeit
- Späteste bevorzugte Abholzeit
- Abholadresse

### Note

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

Das Gerät wird AWS von S.F. Express geliefert. Verwenden Sie die S.F. Express-Tracking-Nummer der Rücksendung, um zu erfahren, wann die Lieferung abgeschlossen wurde.

## AWS Snowcone Abholungen in Indonesien, Japan und Singapur

Wenn Sie in Indonesien, Japan und Singapur bereit sind, Ihr Gerät zurückzugeben, scannen Sie den auf dem E-Ink-Rücksendeetikett angezeigten QR-Code mit Ihrem Handy. Dadurch gelangen Sie direkt zu einer E-Mail-Vorlage. Bitte geben Sie Datum, Uhrzeit und Kontaktdaten der Abholung ein.

### RETURN

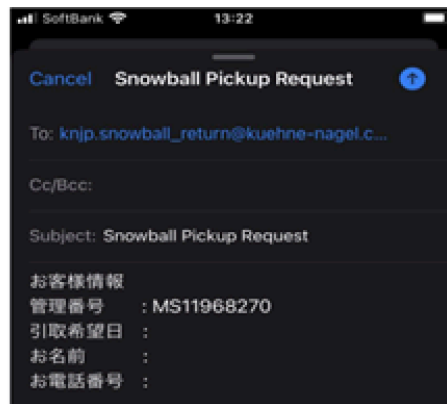
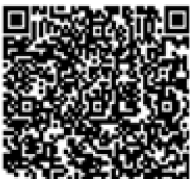
AWS Jobs ID QF6LNZGKTZPF  
 シリアル番号 2R 207138750022  
 管理番号 MS14003547



#### 返送のご案内

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

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



## Versandzeit

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

- Australien, Indonesien, Japan, Singapur, Südkorea — Beim Versand innerhalb dieser Länder haben Sie Zugriff auf die Standardversandgeschwindigkeit von 1 bis 3 Tagen.
- Brasilien — Beim Versand innerhalb Brasiliens haben Sie Zugriff auf den Versand mit UPS Domestic Express Saver, der während der Geschäftszeiten innerhalb von zwei Werktagen zustellt. Die Transportdauer kann durch Verspätungen an den zwischenstaatlichen Grenzen verlängert werden.
- Europäische Union (EU) — Beim Versand in eines der Länder innerhalb der EU haben Sie Zugang zum Expressversand. In der Regel werden Snowcone-Geräte, die per Express versendet werden, innerhalb von etwa einem Tag geliefert. Außerdem ist in den meisten EU-Ländern der Standardversand möglich. In der Regel dauert dieser für einen Weg weniger als eine Woche.

- Indien — Beim Versand innerhalb Indiens werden die AWS Snowcone Geräte innerhalb von 7 Arbeitstagen nach AWS Erhalt aller zugehörigen Steuerdokumente versandt.
- Israel — Beim Versand in Israel haben Sie Zugriff auf den Versand am selben Tag.
- Vereinigte Staaten von Amerika (USA) und Kanada — Beim Versand in die USA und Kanada haben Sie Zugang zu eintägigem Versand und zweitägigem Versand.
- Großbritannien (UK) — Beim Versand innerhalb des Vereinigten Königreichs haben Sie Zugriff auf Expressversand. In der Regel werden Snowcone-Geräte, die per Express versendet werden, innerhalb von etwa einem Tag geliefert. Darüber hinaus haben Sie Zugriff auf den Standardversand, der in der Regel weniger als eine Woche dauert, und zwar in einer Richtung.



# Software auf Snowcone-Geräten aktualisieren

AWS benachrichtigt Sie, wenn neue Software für Ihre Snow Family-Geräte verfügbar ist. Die Benachrichtigung erfolgt per E-Mail AWS Health Dashboard und als CloudWatch Ereignis. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, mit dem das Snow Family-Gerät bestellt wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und laden Sie das Update so schnell wie möglich herunter und installieren Sie es, um eine Unterbrechung der Nutzung des Geräts zu vermeiden. Weitere Informationen zu AWS Health Dashboard finden Sie im [AWS Health Benutzerhandbuch](#). Weitere Informationen zu CloudWatch Veranstaltungen finden Sie im [Amazon CloudWatch Events-Benutzerhandbuch](#).

Sie können Softwareupdates von Snowcone-Geräten in Ihren lokalen Umgebungen herunterladen AWS und auf diesen installieren. Diese Aktualisierungen erfolgen im Hintergrund. Sie können Ihre Geräte weiterhin wie gewohnt verwenden, während die neueste Software sicher von AWS Ihrem Gerät heruntergeladen wird. Um heruntergeladene Updates zu installieren, müssen Sie jedoch die auf dem Gerät ausgeführten Dienste beenden und das Gerät nach Abschluss des Updates neu starten.

Softwareupdates, die von AWS für Snowball Edge/Snowcone-Geräte (Appliances) bereitgestellt werden, sind Appliance-Software gemäß Abschnitt 9 der Servicebedingungen.

Die Softwareupdates werden ausschließlich zum Zweck der Installation der Softwareupdates auf dem jeweiligen Gerät im Namen von bereitgestellt. AWS Sie werden keine (oder versuchen), und Sie werden es Dritten nicht gestatten oder autorisieren, (i) Kopien der Softwareupdates anzufertigen, die nicht für die Installation der Softwareupdates auf dem jeweiligen Gerät erforderlich sind, oder (ii) Funktionen oder Maßnahmen der Softwareupdates zu umgehen oder zu deaktivieren, einschließlich, aber nicht beschränkt auf die Verschlüsselung, die auf das Softwareupdate angewendet wird. Sobald die Softwareupdates auf dem entsprechenden Gerät installiert wurden, erklären Sie sich damit einverstanden, die Softwareupdates von allen Medien zu löschen, die bei der Installation der Softwareupdates auf dem Gerät verwendet wurden.

## Warning

Wir empfehlen dringend, dass Sie alle Aktivitäten auf Ihrem Gerät unterbrechen, bevor Sie das Update installieren. Durch die Aktualisierung des Geräts und den Neustart werden die

laufenden Instances gestoppt und alle Schreibvorgänge in lokale Amazon S3 S3-Buckets unterbrochen.

## Themen

- [Voraussetzungen](#)
- [Updates werden heruntergeladen](#)
- [Updates werden installiert](#)
- [Aktualisierung des SSL-Zertifikats](#)
- [Aktualisierung Ihrer Amazon Linux 2-AMIs auf Geräten der Snow Family](#)

## 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](#).
- Die Aktualisierung von Snowcone-Geräten erfolgt über den Snowball Edge-Client. Die neueste Version des Snowball Edge-Clients muss heruntergeladen und auf einem Computer in Ihrer lokalen Umgebung installiert werden, der über eine Netzwerkverbindung zu dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter [Verwenden des AWS Snowball Edge-Clients](#).
- (Optional) Wir empfehlen, ein Profil für den Snowball Edge-Client zu konfigurieren. Weitere Informationen finden Sie unter [Konfiguration eines Profils für den Snowball Edge-Client](#).

Nachdem Sie diese Aufgaben abgeschlossen haben, können Sie Updates für Snowcone-Geräte herunterladen und installieren.

## Updates werden heruntergeladen

Es gibt hauptsächlich zwei Möglichkeiten, ein Update für Snow Family-Geräte herunterzuladen:

- Sie können manuelle Updates jederzeit mithilfe bestimmter Snowball Edge-Clientbefehle auslösen.
- Sie können programmgesteuert einen Zeitpunkt für die automatische Aktualisierung des Geräts bestimmen.

Das folgende Verfahren beschreibt den Vorgang zum manuellen Herunterladen von Aktualisierungen. Informationen zur automatischen Aktualisierung Ihres Snowcone-Geräts finden Sie unter `configure-auto-update-strategy` [Aktualisieren eines Snowcone-Geräts](#).

### Note

Wenn Ihr Gerät keinen Internetzugang hat, können Sie mithilfe der API eine Aktualisierungsdatei herunterladen. [GetSoftwareUpdates](#) Zeigen Sie dann beim Aufrufen `download-updates` mithilfe des `uri` Parameters auf einen lokalen Dateispeicherort, wie im folgenden Beispiel.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Bei Windows-Betriebssystemen formatieren Sie den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

Um nach Snowcone-Softwareupdates zu suchen und diese herunterzuladen

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das Snowcone-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 aktuell auf dem Gerät installierte Version zurück.
3. Wenn Ihre Gerätesoftware nicht mehr auf dem neuesten Stand ist, führen Sie den Befehl `snowballEdge download-updates` aus.

### Note

Wenn Ihr Gerät nicht mit dem Internet verbunden ist, laden Sie zunächst eine Aktualisierungsdatei über die [GetSoftwareUpdates](#) API herunter. Führen Sie dann den `snowballEdge download-updates` Befehl mit dem `uri` Parameter mit einem lokalen Pfad zu der Datei aus, die Sie heruntergeladen haben, wie im folgenden Beispiel gezeigt.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Formatieren Sie für Windows-Betriebssysteme den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

4. Sie können den Status dieses Downloads mit dem Befehl `snowballEdge describe-device-software` überprüfen. Während ein Update heruntergeladen wird, zeigen Sie den Status mit diesem Befehl an.

Example Ausgabe des **describe-device-software** Befehls

```
Install State: Downloading
```

## Updates werden installiert

Nachdem Sie Updates heruntergeladen haben, müssen Sie sie installieren und Ihr Gerät neu starten, damit die Updates wirksam werden. Das folgende Verfahren führt Sie durch die manuelle Installation von Updates.

### Note

Unterbrechen Sie alle Aktivitäten auf dem Gerät, bevor Sie Softwareupdates installieren. Durch die Installation von Updates werden laufende Instances gestoppt und alle Schreibvorgänge in Amazon S3 S3-Buckets auf dem Gerät unterbrochen. Dies kann zu Datenverlusten führen

Um Softwareupdates zu installieren, die bereits auf eigenständige Snow Family-Geräte heruntergeladen wurden

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das Snowcone-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 [Entsperrern eines Snow Family-Geräts](#).

2. Führen Sie den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Dienste anzuzeigen. Der Befehl gibt die Dienst-IDs aller auf dem Gerät verfügbaren Dienste 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 Dienst-ID den `describe-service` Befehl aus, um den Status zu überprüfen. Verwenden Sie diese Informationen, um Dienste zu identifizieren, die beendet werden sollen.

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

Example der Ausgabe des **describe-service** Befehls

```
{
  "ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Storage" : {
    "TotalSpaceBytes" : 99608745492480,
    "FreeSpaceBytes" : 99608744468480
  },
  "Endpoints" : [ {
    "Protocol" : "http",
    "Port" : 8080,

```

```

"Host" : "192.0.2.0"
}, {
"Protocol" : "https",
"Port" : 8443,
"Host" : "192.0.2.0",
"CertificateAssociation" : {
"CertificateArn" : "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}

```

Diese Ausgabe zeigt, dass der s3 Dienst aktiv ist und mit dem `stop-service` Befehl beendet werden muss.

4. Verwenden Sie den `stop-service` Befehl, um jeden Dienst zu beenden, bei dem der Wert des State Namens `ACTIVE` in der Ausgabe des `list-services` Befehls enthalten ist. Wenn mehr als ein Dienst ausgeführt wird, beenden Sie jeden Dienst, bevor Sie fortfahren.

#### Note

Der Amazon S3 S3-Adapter, Amazon EC2 und die IAM-Dienste können nicht gestoppt werden. AWS STS Wenn Amazon S3 S3-kompatibler Speicher auf Snow Family-Geräten läuft, beenden Sie ihn, bevor Sie Updates installieren. Amazon S3 S3-kompatibler Speicher auf Snow Family-Geräten hat `s3-snow alsserviceId`.

```

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 mit diesem Befehl den Status an.

#### Beispielausgabe

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Sie haben erfolgreich ein Software-Update für Ihr Snowcone-Gerät installiert. Wenn eine Aktualisierung aktualisiert wird, wird sie nicht automatisch auf das Gerät angewandt. Um die Installation der Aktualisierung abzuschließen, muss das Gerät neu gestartet werden.

#### Warning

Wenn Sie Ihr Snow Family-Gerät neu starten, ohne alle Aktivitäten auf dem Gerät zu beenden, kann dies zu Datenverlusten führen.

7. Wenn alle Dienste auf dem Gerät beendet wurden, starten Sie das Gerät neu, entsperren Sie das Gerät und starten Sie es erneut. Damit ist die Installation der heruntergeladenen Softwareupdates abgeschlossen. Weitere Informationen zum Neustarten des Geräts finden Sie unter [Neustarten des Snow Family-Geräts](#) . Weitere Informationen zum Entsperren des Geräts finden Sie unter [Snow Family-Gerät entsperren](#).
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 Snowcone-Software sowie die aktuelle Version zurück, die auf dem Gerät installiert ist.

Sie haben das Snow Family-Gerät oder den Gerätecluster jetzt erfolgreich aktualisiert und bestätigt, dass das Update auf die neueste Snow Family-Software durchgeführt wurde.

## Aktualisierung des SSL-Zertifikats

Wenn Sie Ihr Snow Family-Gerät länger als 360 Tage behalten möchten, müssen Sie das Secure Sockets Layer (SSL) -Zertifikat auf dem Gerät aktualisieren, um eine Unterbrechung der Nutzung

des Geräts zu vermeiden. Wenn das Zertifikat abläuft, können Sie das Gerät nicht verwenden und müssen es an zurückgeben AWS.

AWS benachrichtigt Sie 30 Tage vor Ablauf des SSL-Zertifikats für Ihre Snow Family-Geräte. Die Benachrichtigung erfolgt per E-Mail AWS Health Dashboard und als CloudWatch Ereignis. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, mit dem das Snow Family-Gerät bestellt wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und fordern Sie so schnell wie möglich ein Update an, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Weitere Informationen zu AWS Health Dashboard finden Sie im [AWS Health Benutzerhandbuch](#). Weitere Informationen zu CloudWatch Veranstaltungen finden Sie im [Amazon CloudWatch Events-Benutzerhandbuch](#).

In diesem Thema wird erklärt, wie Sie feststellen, wann das Zertifikat abläuft, und wie Sie Ihr Gerät aktualisieren können.

1. Verwenden Sie den `snowballEdge describe-device-software` Befehl, um zu bestimmen, wann das Zertifikat abläuft. In der Ausgabe des Befehls `CertificateExpiry` beinhaltet der Wert von das Datum und die Uhrzeit, an dem das Zertifikat abläuft.

#### Example der **describe-device-software** Ausgabe

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

2. Kontaktieren Sie uns AWS Support und fordern Sie eine Aktualisierung des SSL-Zertifikats an.
3. AWS Support stellt eine Aktualisierungsdatei zur Verfügung. [Laden Sie die Aktualisierungsdatei herunter](#) und [installieren Sie](#) sie.
4. Verwenden Sie den neuen Entsperrcode und die neue Manifestdatei, wenn Sie [entsperren](#).



# Aktualisierung Ihrer Amazon Linux 2-AMIs auf Geräten der Snow Family

Als bewährte Methode zur Sicherheit sollten Sie Ihre Amazon Linux 2-AMIs up-to-date auf Geräten der Snow Family aufbewahren. Suchen Sie regelmäßig nach Updates für [Amazon Linux 2 AMI \(HVM\)](#), [SSD Volume Type \(64-Bit x86\)](#). AWS Marketplace Wenn Sie feststellen, dass Ihr AMI aktualisiert werden muss, importieren Sie das neueste Amazon Linux 2-Image auf das Snow-Gerät. Weitere Informationen finden Sie unter [Importieren eines Images auf Ihr Gerät als Amazon EC2-kompatibles AMI](#).

Sie können die neueste Amazon Linux 2-Image-ID auch mit dem `ssm get-parameters` Befehl in der abrufen AWS CLI.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Der Befehl gibt die neueste Image-ID des AMI zurück. Beispielsweise:

```
ami-0ccb473bada910e74
```

# Bewährte Methoden für das AWS Snowcone Gerät

Um den größtmöglichen Nutzen aus Ihrem Gerät zu ziehen und die Zufriedenheit mit Ihrem AWS Snowcone Gerät zu maximieren, empfehlen wir Ihnen, diese bewährten Methoden zu befolgen.

## Themen

- [Sicherheit](#)
- [Network \(Netzwerk\)](#)
- [Ressourcenmanagement](#)
- [Verwaltung von EC2-kompatiblen Instances](#)

## Sicherheit

- Wenn Sie etwas an dem AWS Snowcone Gerät bemerken, das verdächtig aussieht, verbinden Sie es nicht mit Ihrem internen Netzwerk. Setzen Sie [AWS Support](#)sich stattdessen mit uns in Verbindung und ein neues AWS Snowcone Gerät wird Ihnen zugeschickt.
- Wir empfehlen, dass Sie auf der Workstation an dem Speicherort, der das Manifest des Auftrags enthält, keine Kopie des Entsperrcodes für diesen Auftrag speichern. Wenn Sie diese separat speichern, können Sie verhindern, dass Unbefugte Zugriff auf das AWS Snowcone Gerät erhalten. Beispielsweise können Sie eine Kopie des Manifests auf Ihrem lokalen Server speichern und den Code, der das Gerät entsperrt, per E-Mail an den Benutzer senden. Dieser Ansatz beschränkt den Zugriff auf das AWS Snowcone Gerät auf Personen, die Zugriff auf die auf dem Server gespeicherten Dateien und auch auf die E-Mail-Adresse dieses Benutzers haben.
- Die Anmeldeinformationen, die angezeigt werden, wenn Sie den Snowball Edge-Client-Befehl `snowballEdge list-access-keys` gefolgt von `ausführen`, `snowballEdge get-secret-access-key` sind ein Schlüsselpaar: ein Zugriffsschlüssel und ein geheimer Schlüssel. Diese Schlüssel sind ausschließlich dem Auftrag und den lokalen Ressourcen auf dem Gerät zugeordnet. Sie lassen sich AWS-Konto weder Ihrem noch einem anderen AWS-Konto zuordnen. Wenn Sie versuchen, diese Schlüssel für den Zugriff auf Dienste und Ressourcen in der zu verwenden AWS Cloud, schlagen sie fehl, da sie nur für die lokalen Ressourcen funktionieren, die mit Ihrem Job verknüpft sind.
- Sie können den Zugriff auf NFS-Shares einschränken. Details hierzu finden Sie unter [Beschränken des Zugriffs auf NFS-Freigaben, wenn NFS ausgeführt wird](#).

- Wenn Sie ein Snowcone-Gerät ausschalten oder ein- und ausschalten, geht es in einen gesperrten Zustand über.

## Network (Netzwerk)

- Es wird empfohlen, jeweils nur eine Methode zum Lesen und Schreiben von Daten in einen lokalen Bucket auf einem AWS Snowcone Gerät zu verwenden. Verwenden Sie beide NFS-Mount und der DataSync auf demselben S3-Bucket gleichzeitig können zu Lese-/Schreibkonflikten führen.
- Um zu verhindern, dass Ihre Daten beschädigt werden, sollten Sie während der Übertragung keine Verbindung zu einem AWS Snowcone Gerät trennen oder dessen Netzwerkeinstellungen ändern.
- Dateien müssen beim Schreiben auf das Gerät in statischem Zustand sein. Wenn Dateien während des Schreibvorgangs geändert werden, kann dies zu Lese-/Schreib-Konflikten führen.
- Weitere Informationen zur Verbesserung der Leistung Ihres AWS Snowcone Geräts finden Sie unter [Leistung von Snowcone](#)

## Ressourcenmanagement

- Die fünf freien Tage für die Durchführung Ihrer lokalen Datenübertragung beginnen am Tag nach der Ankunft des AWS Snowcone Geräts in Ihrem Rechenzentrum.

## Verwaltung von EC2-kompatiblen Instances

Um zu verhindern, dass die Amazon EC2-kompatiblen Instances, die Sie auf Ihrem AWS Snowcone Gerät erstellen, versehentlich gelöscht werden, sollten Sie Ihre Instances nicht über das Betriebssystem herunterfahren. Beispielsweise dürfen Sie die Befehle `shutdown` oder `reboot` nicht verwenden. Das Herunterfahren einer Instance über das Betriebssystem hat den gleichen Effekt wie der Aufruf des Befehls [terminate-instances](#).

Verwenden Sie stattdessen den Befehl [stop-instances](#), um Amazon EC2-kompatible Instances zu suspendieren, die Sie beibehalten möchten.

## Leistung von Snowcone

Die folgende Tabelle zeigt, wie sich die Übertragungsrate Ihres Netzwerks darauf auswirkt, wie lange es dauert, ein Netzwerk AWS Snowcone mit Daten zu füllen.

Geschwindigkeit (MB/s)	8 TB Übertragungszeit	4 TB Übertragungszeit
100	21,17 Stunden	10,59 Stunden
60	36,57 Stunden	18,29 Stunden
30	68,57 Stunden	34,29 Stunden
10	210,29 Stunden	105,15 Stunden

# AWS Snowcone Kontingente

Im Folgenden finden Sie Informationen zu den Kontingenten für die Nutzung Ihres Snowcone-Geräts.

## Snowcone Festplattenspeicher

Intern enthält Ihr Snowcone-Gerät 8 TB oder 14 TB Festplattenspeicher, den Sie mit dem internen Network File System (NFS) -Service oder mit lokalen Amazon EC2-kompatiblen Instances über eine lokale Volumenpräsentation im Amazon Elastic Block Store (Amazon EBS) verwenden können. Sie können diesen Speicher entweder für NFS oder Amazon EBS verwenden, aber nicht für beide. Sie können Ihren Speicher je nach Anwendungsfall zuweisen. Beachten Sie, dass der Speicherplatz bereits zugewiesen ist, wenn Sie Ihre Snowcone-Bestellung aufgeben.

## Auftragsspeicher berechnen

Wenn es sich bei dem Auftragsstyp um lokale Datenverarbeitung handelt, können Sie insgesamt 8 TB oder 14 TB an lokalen Amazon EBS-Volumes erstellen und diese an Amazon EC2-kompatible Instances anhängen. Durch die Verwendung von Amazon EBS-Volumes können die lokalen Amazon EC2-Instances auf mehr lokale Kapazität zugreifen als auf das Root-Volume allein. Da es sich nur um lokalen Speicher handelt, gehen auf die Amazon EBS-Volumes geschriebene Daten verloren, wenn das Gerät zurückgegeben wird, AWS da sie nicht in Amazon S3 importiert werden können.

## Themen

- [Ressourcenkontingente berechnen](#)
- [Einschränkungen für den Versand eines Snowcone-Geräts](#)
- [Einschränkungen bei der Bearbeitung Ihres zurückgesandten Snowcone-Geräts für den Import](#)
- [Verfügbar AWS-Regionen](#)

## Ressourcenkontingente berechnen

### Verfügbare Rechenressourcen für Snowcone-Geräte: Speicherkontingente

In der folgenden Tabelle sind die verfügbaren Rechenressourcen für Snowcone-Geräte und ihre Speicherkontingente aufgeführt.

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	Kontingent
snc1.micro	1	1	2
snc1.small	1	2	2
snc1.medium	2	4	1

## Kapazitätskontingente für Amazon Machine Image (AMI) und Amazon EC2 für Snowcone-Geräte

In der folgenden Tabelle sind die AMI- und Amazon EC2-kompatiblen Instance-Kapazitätskontingente für ein Snowcone-Gerät aufgeführt.

Amazon EC2	Größe
Amazon EC2-kompatible AMIs	125 GB (die Gesamtgröße aller AMIs, die bei der Arbeit eines Kunden verwendet werden)
Amazon EC2-kompatible Instances	150 GB (steht für den verfügbaren Speicherplatz für die Backup-Speichervolumen der Instances)

## Einschränkungen für den Versand eines Snowcone-Geräts

Im Folgenden sind die Einschränkungen für den Versand eines Snowcone-Geräts aufgeführt:

- AWS versendet ein Snowcone-Gerät nicht an ein Postfach.
- Das Verschieben eines Snowcone-Geräts an eine Adresse außerhalb des Landes, das bei der Erstellung des Jobs angegeben wurde, ist nicht zulässig und stellt einen Verstoß gegen die AWS Servicebedingungen dar.

Weitere Informationen zum Versand finden Sie unter [Überlegungen zum Versand für AWS Snowcone](#).

# Einschränkungen bei der Bearbeitung Ihres zurückgesandten Snowcone-Geräts für den Import

Um Ihre Daten in das zu importieren AWS Cloud, muss das Snowcone-Gerät die folgenden Anforderungen erfüllen:

- Das Snowcone-Gerät darf nicht kompromittiert werden. Öffnen Sie das Snowcone-Gerät aus keinem Grund, außer wenn Sie die Türen an der Vorder- und Rückseite öffnen.
- Das Gerät muss physisch unbeschädigt sein. Um Beschädigungen zu vermeiden, schließen Sie die beiden Türen des Snowcone-Geräts und drücken Sie, bis die Riegel ein hörbares Klickgeräusch von sich geben.
- Sofern kein Versandetikett von bereitgestellt wird AWS, muss das E Ink-Display auf dem Snowcone-Gerät sichtbar sein und das Rücksendetikett anzeigen, das automatisch generiert wurde, als Sie die Übertragung Ihrer Daten auf das Snowcone-Gerät abgeschlossen haben.

## Note

Alle zurückgesandten Snowcone-Geräte, die diese Anforderungen nicht erfüllen, werden gelöscht, ohne dass daran gearbeitet wurde.

## Verfügbar AWS-Regionen

Informationen zu den unterstützten Endpunkten AWS-Regionen und Endpunkten finden Sie unter [AWS Snow Family-Endpunkte und -Kontingente](#) in der. Allgemeine AWS-Referenz

# Behebung von Problemen mit Snowcone

Dieser Abschnitt bietet Anleitungen und Einblicke in das AWS Snowcone Gerät/den Dienst, um einige der aufgetretenen Probleme zu beheben.

## Themen

- [Fehlerbehebung bei Compute-Instances](#)
- [Behebung von Netzwerkproblemen](#)
- [Problembehandlung einer Amazon EC2-kompatiblen Instance auf Datasync](#)
- [Behebung von Problemen bei der Datenübertragung](#)
- [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten](#)

## Fehlerbehebung bei Compute-Instances

Die Fehlerbehebung bei Compute Instances [ist hier](#) dokumentiert.

## Behebung von Netzwerkproblemen

### Die IP-Adresse ist 0.0.0.0

Sie sind mit dem Netzwerk und den Stromkabeln verbunden, aber die IP-Adresse des Geräts zeigt 0.0.0.0

#### Maßnahme

Stellen Sie sicher, dass die Verkabelung zwischen dem Snowcone und den Netzwerkgeräten ordnungsgemäß überprüft wurde.

Wenn das Gerät immer noch keine IP-Adresse anzeigt, überprüfen Sie den Router auf Probleme im Zusammenhang mit Fehlfunktionen oder Konfigurationen, die zu einem Ausfall der IP-Konfiguration führen können.

Wenn im Netzwerk DHCP nicht aktiviert ist, stellen Sie sicher, dass Sie mit der Option STATIC auf dem Snowcone-Display eine statische IP auf dem Gerät einrichten und das Gerät mit der entsprechenden statischen IP-Adresse programmieren.



## Das Gerät konnte nicht entsperrt werden

Sie können das Gerät nicht mit OpsHub unserem Snowball Edge-Client entsperren.

### Maßnahme

Stellen Sie sicher, dass sich der Client im selben Subnetz und im selben Netzwerk wie das AWS Snowcone Gerät befindet.

Wenn der Snowcone mehrere IP-Adresszuweisungen hat (z. B. WiFi und Ethernet), stellen Sie sicher, dass Sie dieselbe IP-Adresse für die Verbindung verwenden, falls mehrere Clients versuchen, auf Snowcone zu antworten. Beachten Sie, dass Sie jeweils nur eine Schnittstelle verwenden können.

Wenn die oben genannten Schritte nicht funktionieren, AWS Support stellen Sie bitte die Protokolle vom Gerät bereit. Verwenden Sie den Snowball Edge-Client und den Befehl: `SnowballEdge get-support-logs`

## Problembehandlung einer Amazon EC2-kompatiblen Instance auf Datasync

### Fehler: Die Instance konnte nicht gestartet werden

Snowcone hat nicht genügend Kapazität, um die Instance für diese Anfrage zu starten.

### Maßnahme

Die Anforderungen für die Ausführung DataSync auf einem AWS Snowcone Gerät als Agent verwenden die Standardinstanz `snc1.medium`, die 2 CPU-Kerne und 4 GiB Arbeitsspeicher bereitstellt. Stellen Sie sicher, dass Sie über genügend Ressourcen auf dem Snowcone-Gerät verfügen, um die neue Amazon EC2-kompatible Instance-Startanfrage bereitzustellen.

## Behebung von Problemen bei der Datenübertragung

### Zugriff vom Server verweigert

Fehler: `mount.nfs` — Der Zugriff wurde vom Server beim Mounten von `192.168.1.214` verweigert

## Maßnahme

Wenn Sie NFS mit Quick Setup konfiguriert haben, hat standardmäßig nur Ihr System Zugriff auf die Übertragung von Dateien auf dieses Gerät. Wenn Sie anderen Hosts erlauben möchten, Daten auf den Snowcone hochzuladen, deaktivieren Sie den NFS-Dienst und aktivieren Sie den Dienst erneut mit der Liste der IP-Adressen, die Sie in der NFS-Konfiguration zulassen möchten.

## Die Verbindung wird während der Datenübertragung unterbrochen

Beim Versuch, Daten über die Amazon S3 S3-Schnittstelle (via AWS CLI) zu AWS Snowcone übertragen, wird die Verbindung unterbrochen.

Grund für dieses erwartete Verhalten

Das AWS Snowcone Gerät unterstützt nur Übertragungen über den NFS-Mount für Offline-Übertragungen und AWS DataSync für Online-Übertragungen. Die Amazon S3 S3-Schnittstelle wird derzeit nicht unterstützt. Dies würde erklären, warum es beim Herstellen einer Verbindung mit dem zu Timeouts kommt. AWS CLI

## Spawn Showmount ENOENT

Fehler: Nicht erfasster Fehler — Showmount ENOENT erzeugen. Es ist eine Abkürzung für Error NO ENTrY (oder Error NO ENtity) und kann tatsächlich für mehr als Dateien/Verzeichnisse verwendet werden.

## Maßnahme

Dieser Fehler kann auftreten, wenn der NFS-Client nicht auf der Workstation läuft. Wenn der NFS-Dienst vor der Konfiguration von NFS nicht gestartet wurde AWS OpsHub, wird möglicherweise dieser Fehler angezeigt.

Auf einem Windows-Client können Sie überprüfen, ob der NFS-Dienst ausgeführt wird, indem Sie die folgenden Schritte ausführen:

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.
3. Wählen Sie unter Services for NFS (Dienste für NFS) die Option Client for NFS (Client für NFS) aus und klicken Sie auf OK. Referenz: [Mounten von NFS auf einem Windows-Client](#)

Dieser Fehler kann auch auftreten, wenn sich zwischen der laufenden Workstation AWS OpsHub und dem Gerät eine Firewall/ein Antivirenprogramm befindet, das die Verbindung blockieren könnte.

Führen Sie auf der Workstation den Befehl `telnet to the AWS Snowcone device IP address auf der NFS-Portnummer 2049 aus`, um zu überprüfen, ob die Verbindung erfolgreich hergestellt wurde.

## Behebung von Problemen bei der Rückgabe von Snow Family-Geräten

Manchmal werden nach dem Ausschalten des Snow Family-Geräts zur Vorbereitung der Rücksendung die Versandinformationen nicht auf dem E Ink-Display angezeigt.

### Maßnahme

1. Melden Sie sich bei der an Managementkonsole für die AWS Snow-Familie.
2. Sehen Sie sich den Job für das Gerät an.
3. Wählen Sie im Abschnitt Details im Abschnitt Rücksendetikett die Option Um Ihr Rücksendetikett anzusehen und auszudrucken, folgen Sie diesem Link.
4. Drucken Sie das Etikett aus und befestigen Sie es am Gerät.
5. Senden Sie das Gerät entsprechend zurück [Rückgabe eines Snowcone-Geräts](#).

# Job Management-API-Referenz

- [Job Management-API-Referenz](#)
  - [Aktionen](#)
  - [Datentypen](#)
  - [Geläufige Parameter](#)
  - [Häufige Fehler](#)

# Dokumentenverlauf für AWS Snowcone das Benutzerhandbuch

In der folgenden Tabelle wird die Dokumentation für diese Version von beschrieben AWS Snowcone.

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 25. August 2023

Änderung	Beschreibung	Datum
<a href="#">Fügen Sie bei der Bestellung von Geräten benutzerdefinierte AMIs hinzu</a>	Benutzerdefinierte Amazon Machine Images können jetzt bei der Bestellung von AWS Snow Family Aufträgen vorgeladen werden. Weitere Informationen finden Sie unter <a href="#">Amazon EC2 auf Snowcone verwenden</a> .	15. November 2023
<a href="#">Neu unterstützt AWS-Region</a>	AWS Snowcone SSD-Geräte sind jetzt in Israel (Tel Aviv) erhältlich AWS-Region. Informationen zur Abholung für diese Region wurden hinzugefügt. Weitere Informationen finden Sie unter <a href="#">AWS Snow Family -Endpunkte und -Kontingente</a> in der Allgemeine AWS-Referenz. Informationen zum Versand finden Sie unter <a href="#">Überlegungen zum Versand für AWS Snowcone</a> .	25. August 2023
<a href="#">Neu AWS-Region unterstützt</a>	Snowcone-Geräte sind jetzt in Europa (Paris) AWS-Regio	29. Juni 2022

n erhältlich. Weitere Informationen finden Sie unter [AWS Snow Family -Endpunkte und -Kontingente](#) in der Allgemeine AWS-Referenz. Informationen zum Versand finden Sie unter [Überlegungen zum Versand für AWS Snowcone](#).

### [Neue Tipps zur Fehlerbehebung bei Snowcone](#)

AWS Snowcone Der Abschnitt mit Tipps zur Fehlerbehebung wurde ähnlich wie bei Snowball Edge hinzugefügt. Einen neuen Abschnitt finden Sie unter [Fehlerbehebung bei Snowcone-Problemen](#).

15. April 2022

### [Neu unterstützt AWS-Region](#)

AWS Snowcone ist jetzt in den Regionen Asien-Pazifik (Mumbai) und Brasilien verfügbar. Informationen zur Abholung für die EU, Kanada, Singapur und Brasilien wurden hinzugefügt. Weitere Informationen finden Sie unter [AWS Snow Family-Endpunkte und Kontingente](#) im Allgemeine AWS-Referenz.

23. Februar 2022

### [Neu unterstützt AWS-Region](#)

AWS Snowcone ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen finden Sie unter [AWS Snow Family-Endpunkte und Kontingente](#) in der Allgemeine AWS-Referenz.

5. Januar 2022

<a href="#">Support für die Network Time Protocol (NTP) -Serverkonfiguration</a>	Snowcone-Geräte unterstützen jetzt die externe Network Time Protocol (NTP) -Serverkonfiguration.	16. November 2021
<a href="#">Neu unterstützt AWS-Region</a>	AWS Snowcone SSD ist jetzt in den Regionen USA West (Nordkalifornien), USA Ost (Ohio), Asien-Pazifik (Singapur), Asien-Pazifik (Tokio) und Asien-Pazifik (Sydney) verfügbar. Weitere Informationen finden Sie unter <a href="#">AWS Snow Family-Endpunkte und Kontingente</a> in der Allgemeinen AWS-Referenz.	3. November 2021
<a href="#">Neu unterstützt AWS-Region</a>	AWS Snowcone ist jetzt in den Regionen USA West (Nordkalifornien), USA Ost (Ohio) und Südamerika (São Paulo) verfügbar. Weitere Informationen finden Sie unter <a href="#">AWS Snow Family-Endpunkte und Kontingente</a> in der Allgemeinen AWS-Referenz.	29. September 2021
<a href="#">Neu unterstützt AWS-Region</a>	AWS Snowcone ist jetzt in den Regionen Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) verfügbar. Weitere Informationen finden Sie unter <a href="#">AWS Snow Family-Endpunkte und Kontingente</a> in der Allgemeinen AWS-Referenz.	26. August 2021

[Support für den Offline-Datenexport aus Amazon S3 mit Snowcone-Geräten](#)

Sie können jetzt AWS den Export Ihrer Amazon S3 S3-Daten beantragen, indem Sie sie auf Snowcone-Geräte übertragen, die dann physisch an Ihren Standort geliefert werden. Weitere Informationen finden Sie unter [So funktionieren Import- und Exportaufträge](#).

4. August 2021

[Wir stellen vor AWS Snow Device Management](#)

Mit Snow Device Management können Sie Ihr AWS Snowcone Gerät und Ihre lokalen AWS Dienste aus der Ferne verwalten. Alle Snowcone-Geräte unterstützen Snow Device Management und es ist auf neuen Geräten in den meisten Ländern, in AWS-Regionen denen Snowcone erhältlich ist, vorinstalliert. Weitere Informationen finden Sie unter Geräte [AWS Snow Device Management zur Verwaltung verwenden](#).

4. August 2021

[Neu AWS-Region unterstützt](#)

AWS Snowcone ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen finden Sie unter [AWS Snow Family-Endpunkte und Kontingente](#) in der Allgemeine AWS-Referenz.

28. April 2021



---

<a href="#"><u>Neu unterstützt AWS-Region</u></a>	AWS Snowcone ist jetzt in der Region Asien-Pazifik (Sydney) verfügbar. Weitere Informationen finden Sie unter <a href="#"><u>AWS Snow Family-Endpunkte und Kontingente</u></a> in der Allgemeine AWS-Referenz.	24. März 2021
<a href="#"><u>Support für direkte Netzwerkschnittstelle</u></a>	AWS Snowcone fügt jetzt eine direkte Netzwerkschnittstellenkonfiguration (DNI) hinzu, eine erweiterte Netzwerkfunktion, die Anwendungsfälle wie Multicast-Streams, Routing und Lastenausgleich ermöglicht. Weitere Informationen finden Sie unter <a href="#"><u>Netzwerkconfiguration für Compute-Instances</u></a> .	12. Januar 2021
<a href="#"><u>Neu AWS-Region unterstützt</u></a>	AWS Snowcone ist jetzt in der Region Europa (Frankfurt) verfügbar. Weitere Informationen finden Sie unter <a href="#"><u>AWS Snow Family-Endpunkte und Kontingente</u></a> in der Allgemeine AWS-Referenz.	18. November 2020
<a href="#"><u>Neu unterstützt AWS-Region</u></a>	AWS Snowcone ist jetzt in der Region Europa (Irland) verfügbar. Weitere Informationen finden Sie unter <a href="#"><u>AWS Snow Family-Endpunkte und Kontingente</u></a> in der Allgemeine AWS-Referenz.	16. September 2020

## [Wir stellen vor AWS Snowcone](#)

AWS Snowcone ist ein tragbares, robustes und sicheres Gerät für Edge-Computing und Datenübertragung. Sie können AWS Snowcone verwenden, um Daten zu sammeln, zu verarbeiten und zu AWS übertragen, entweder offline, indem Sie das Gerät an AWS senden, oder online mit AWS DataSync. Weitere Informationen finden Sie unter [Was ist AWS Snowcone?](#).

17. Juni 2020

# 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.