



AWS Snowcone

AWS Snowcone Benutzerhandbuch für



AWS Snowcone Benutzerhandbuch für: 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
Funktionsweise AWS Snowcone von	4
AWS Snowcone Workflow	5
Funktionsweise von Importaufträgen	7
Online-Datenübertragung zwischen Snowcone und AWS Storage Services mit DataSync	7
Offline-Datenübertragung zwischen Snowcone und Amazon S3	8
Für den Import von Auftragsspeicher	9
Für Datenverarbeitungsauftragsspeicher	9
Gerätespezifikationen	10
Übersicht	10
Hardware und Netzwerk	12
Ansicht von oben	12
Trichterfenster	12
Frontbereich	14
AWS Snowcone Wi-Fi-Spezifikationen	15
Spezifikationen für die Klassifizierung	15
Snowcone-Netzteil und -Kabel	16
Festplatten- und CPU-Leistung	16
Einrichten	17
Registrieren bei AWS	17
Vor der Bestellung	18
Informationen zur lokalen Umgebung	18
Arbeiten mit Sonderzeichen	19
Amazon EC2	20
Unterschied zwischen Amazon EC2- und AmazonEC2-compatible Instances auf Snow- Family-Geräten	21
Preise für Compute Instances auf Snowcone	21
Voraussetzungen	21
Überprüfen von Produktcodes und Plattfordetails von AWS Marketplace AMIs	22
Erstellen eines Linux-AMI aus einer Instance	23
Erstellen eines Linux-AMI aus einem Snapshot	23
Erste Schritte	28

Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts	28
Schritt 1: Auswählen eines Auftragstyps	29
Schritt 2: Auswählen Ihrer Datenverarbeitungs- und Speicheroptionen	30
Schritt 3: Auswählen Ihrer Funktionen und Optionen	33
Schritt 4: Auswählen von Sicherheits-, Versand- und Benachrichtigungseinstellungen	33
Schritt 5: Überprüfen der Auftragsübersicht und Erstellen Ihres Auftrags	36
Herunterladen AWS OpsHub	37
Stornieren eines Auftrags zum Bestellen eines Snow-Family-Geräts	38
Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät	39
Entsperren des Snow Family-Geräts	40
Fehlerbehebung beim Entsperren eines Snow Family-Geräts	42
Neustarten des Snow Family-Geräts	42
Verwenden von AWS OpsHub zum Verwalten von Geräten	48
AWS OpsHub Für Snow Family-Geräte herunterladen	49
Entsperren eines Geräts	50
Lokales Entsperren eines Geräts	50
Entsperren eines Geräts aus der Ferne	53
Überprüfen der Signatur von AWS OpsHub	57
Verwalten von - AWS Services	60
Lokale Verwendung von Datenverarbeitungs-Instances	61
Verwalten der NFS-Schnittstelle	69
Verwenden von AWS DataSync zum Übertragen von Dateien in AWS	78
Übertragen von Dateien	79
Verwaltung Ihrer Geräte	80
Neustarten Ihres Geräts	81
Herunterfahren Ihres Geräts	81
Bearbeitung des Gerätealias	82
Abrufen von Updates	83
Verwalten von Profilen	85
Festlegen der NTP-Zeitserver für Ihr Gerät	87
Verwenden des AWS Snowball Edge Clients	89
Herunterladen und Installieren des Snowball Edge Clients	89
Befehle für den Snowball Edge Client	89
Konfigurieren eines Profils für den Snowball Edge Client	91
Anfordern Ihres QR-Codes für die NFC-Validierung	92
Entsperren eines - AWS Snowcone Geräts	92

Aktualisieren eines Snowcone	93
Abrufen von Anmeldeinformationen	96
Starten eines Services auf Ihrem Snowcone-Gerät	97
Stoppen eines Services auf Ihrem Snowcone-Gerät	98
Abrufen des Zertifikats für die Datenübertragung	98
AWS Snowcone Protokolle	99
Abrufen des Gerätestatus	101
Abrufen des Servicestatus	103
Starten des AWS DataSync AMI	105
Starten von NFS und Einschränken des Zugriffs	108
Beschränken des Zugriffs auf NFS-Anteile, wenn NFS ausgeführt wird	109
Abrufen des Exportpfads für einen Amazon S3-Bucket	109
Aktivieren des lokalen AWS Operator-Debuggings	109
Deaktivieren des Debuggings von lokalen AWS Operatoren	110
Erstellen einer direkten Netzwerkschnittstelle	110
Abrufen von Informationen zu einer Direct Network Interface	110
Aktualisieren einer Direct Network Interface	111
Löschen einer Direct Network Interface	111
Überprüfen des Feature-Status	112
Ändern des Feature-Status	112
Einstellen von Zeitservern	113
Überprüfen von Zeitquellen	114
Verwenden von Snow Device Management zur Verwaltung von Geräten	117
Auswählen des Snow Device Management-Status beim Bestellen eines Snow Family-Geräts ..	118
Aktivieren der Snow Device Management	119
Hinzufügen von Berechtigungen für Snow Device Management zu einer IAM-Rolle	120
CLI-Befehle für Snow Device Management	121
Erstellen einer Aufgabe	122
Überprüfen des Aufgabenstatus	123
Überprüfen der Geräteinformationen	124
Überprüfen des Amazon EC2-compatible Instance-Status	126
Überprüfen der Aufgabenmetadaten	128
Abbrechen einer Aufgabe	129
Auflisten von Befehlen und Syntax	130
Auflisten von remote verwalteten Geräten	131
Auflisten des Aufgabenstatus über Geräte hinweg	132

Auflisten verfügbarer Ressourcen	133
Auflisten von Geräte- oder Aufgaben-Tags	134
Auflisten von Aufgaben nach Status	135
Anwenden von Tags	136
Entfernen von Tags	137
AWS-Dienste nutzen	138
Verwenden von Amazon EC2 für Datenverarbeitung	139
Übersicht	139
Voraussetzungen	140
Anlegen eines Auftrags mit Datenverarbeitungs-Instances	141
Netzwerkconfiguration für Datenverarbeitungs-Instances	146
Herstellen einer Verbindung mit Ihrer Compute Instance auf einem Snowcone mithilfe von SSH	153
Snowcone-Client-Befehle für Compute-Instances	154
Verwenden von Instance Metadata Service für Snow mit Amazon EC2-compatible Instances	160
Verwenden des AmazonEC2-compatible Endpunkts	170
Automatisches Starten von Amazon EC2-compatible Instances mit Startvorlagen	187
Verwenden von Block Storage mit Ihren EC2-compatible Instances	189
Sicherheitsgruppen in Snow Devices	190
Unterstützte Instance-Metadaten und Benutzerdaten	191
Fehlerbehebung bei Amazon EC2	193
Zum DataSync Übertragen von Dateien verwenden	195
Verwalten der NFS-Schnittstelle	196
NFS-Konfiguration für Snow Family-Geräte	197
Verwenden AWS IoT Greengrass auf EC2-kompatiblen Instances	202
Richten Sie Ihre Amazon EC2-kompatible Instance ein	203
Für die Nutzung der AWS Dienste erforderliche Ports	206
Rückgabe des Snowcone-Geräts	207
Trennen Sie das Snowcone-Gerät	207
Schutz von Daten auf Ihrem Gerät	208
Sichern 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
Verstehen der Ablaufverfolgung.	238
Verstehen der Ablaufverfolgung.	238
Rückgabe eines Snowcone-Geräts	238
Verwendung der AWS Management Console	239
Den Snowcone von der Konsole aus bestellen	239
Verwenden der Job Management-API	239
Häufige Verwendungen von JMAPI	239
JMAPI Erforderliche Strings	240
JMAPI-Endpoints	240
JMAPI-CLI-Befehle	240
Beispiele	241
EC2-Aufträge	242
Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden	243
Erstellen Ihres Auftrags mit der Konsole	244
Erstellen Ihres Auftrags mit der -AWSCLI	244
Versandüberlegungen	246
Vorbereiten eines -AWS SnowconeGeräts für den Versand	246
Versandeinschränkungen nach Regionen	247
Versand eines -AWS SnowconeGeräts	248
Versandanbieter	248
Aktualisieren von Snowcone-Geräten	257
Voraussetzungen	258
Herunterladen von Updates	258
Installieren von Updates	260
Aktualisieren des SSL-Zertifikats	263
Aktualisieren Ihrer Amazon Linux 2-AMIs auf Snow Family-Geräten	264
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 Verarbeitung Ihres zurückgegebenen Snowcone-Geräts für den Import	271
VerfügbarAWS-Regionen	271
Fehlerbehebung	272
Problembehandlung bei Compute-Instances	272
Probleme mit dem Netzwerk	272
Die IP-Adresse ist 0.0.0.0	272
Gerät kann nicht entsperrt werden	273
EC2-kompatible Instance bei Datensynchronisierungsproblemen	273
Fehler: Instanz konnte nicht gestartet werden	273
Probleme bei der Datenübertragung	273
Zugriff vom Server verweigert	273
Verbindungszeitüberschreitung während der Datenübertragung	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 portables, Telefonie- und sicheres Gerät für Edge-Computing und Datenübertragung. Sie können ein Snowcone-Gerät verwenden, um Daten entweder offline zu erfassen, zu verarbeiten und in die zu verschieben AWS Cloud, indem Sie das Gerät an senden AWS, oder online mithilfe von AWS DataSync.

Es kann schwierig sein, Anwendungen in strengen (nicht im Rechenzentrum befindlichen) Edge-Umgebungen auszuführen oder wenn keine konsistente Netzwerkkonnektivität besteht. Diese Standorte verfügen häufig nicht über den Platz, die Stromversorgung und die Stromversorgung, die für IT-Geräte von Rechenzentren erforderlich sind.

Snowcone ist in zwei Varianten verfügbar:

- 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 (SSD)-basierten Speicher.

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" x 5,85" x 3,25" / 227 mm x 148,6 mm x 82,65 mm), sodass sie in einer Fabrik neben den Geräten platziert werden können, um Daten AWS zur Speicherung und Analyse zu sammeln, zu formatieren und zurück zu transportieren. Ein Snowcone-Gerät wiegt etwa 4,5 Bol. (2 Bol), sodass Sie eines in einem Kabel tragen, es mit batteriebasiertem Betrieb verwenden und die Wi-Fi-Schnittstelle verwenden können, um Sensordaten zu sammeln.

Note

WLAN ist nur in AWS-Regionen in Nordamerika verfügbar.

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

Wie verfügt AWS Snowball AWS Snowcone über mehrere Ebenen von Sicherheitsverschlüsselungsfunktionen. Sie können einen dieser Services verwenden, um Daten zu sammeln, zu verarbeiten und zu übertragen und Edge-Computing-Workloads auszuführen AWS, die Amazon-ECEC2-compatible verwenden. Snowcone ist für Datenmigrationsanforderungen von bis zu Dutzenden von Terabyte konzipiert. Es kann in Umgebungen mit eingeschränktem Speicherplatz verwendet werden, in denen Snowball Edge-Geräte nicht passen.

Anwendungsfälle

Sie können AWS Snowcone Geräte für die folgenden Anwendungsfälle verwenden:

- Damit Edge-Computing-Anwendungen Daten sammeln, verarbeiten Sie die Daten, um sofortige Einblicke zu erhalten, und übertragen Sie die Daten dann online an AWS.
- So übertragen Sie Daten, die kontinuierlich von Sensoren oder Maschinen online zu AWS in einer Fabrik oder an anderen Edge-Standorten generiert werden.
- Um Medien, wissenschaftliche oder andere Inhalte von - AWS Speicherservices an Ihre Partner und Kunden zu verteilen.
- So aggregieren Sie Inhalte, indem Sie Medien, wissenschaftliche oder andere Inhalte von Ihren Edge-Standorten an übertragen AWS.
- Für einmalige Datenmigrationsszenarien, in denen Ihre Daten übertragen werden können, bietet Snowcone eine schnelle und kostengünstige Möglichkeit, bis zu 8 TB oder 14 TB an Daten an zu übertragen, AWS Cloud indem das Gerät zurück an gesendet wird AWS.

Bei mobilen Bereitstellungen kann ein Snowcone-Gerät mit bestimmter Batterieleistung ausgeführt werden. Bei einer geringen Workload bei einer CPU-Auslastung von 25 Prozent kann das Gerät bis zu etwa 6 Stunden lang auf einer Batterie laufen. Sie können die Wi-Fi-Schnittstelle auf Ihrem Snowcone-Gerät verwenden, um Daten von WLAN-Sensoren zu sammeln. Ein AWS Snowcone Gerät ist stromsparend, portabel, leicht und widerstandsfähig, sodass Sie es an einer Vielzahl von Remote- und strengen Standorten verwenden können.

Note

WLAN ist nur in AWS-Regionen in Nordamerika verfügbar.

Preisgestaltung

Sie können ein Snowcone-Gerät für die Zahlung pro Nutzung bestellen und das Gerät bis zu vier Jahre lang aufbewahren. Weitere Informationen zu AWS Snowcone Preisen und Gebühren finden Sie unter [-AWS Snowcone Preise](#).

Funktionsweise AWS Snowcone von

AWS Snowcone ist ein portables Gerät, das für Edge-Computing und Datenübertragung verwendet wird. Um zu beginnen, fordern Sie ein oder mehrere Snowcone-Geräte in der AWS Management Console an, basierend auf der Menge der zu übertragenden Daten und der erforderlichen Rechenleistung. Die von Ihnen ausgewählten Amazon Simple Storage Service (Amazon S3)-Buckets, Daten und Amazon Machine Images (AMIs) von Amazon Elastic Compute Cloud (Amazon EC2) werden automatisch auf Ihren Geräten konfiguriert, verschlüsselt und vorinstalliert. Der AWS DataSync Agent ist auch vorinstalliert, bevor Ihre Geräte an Sie geliefert werden.

Wenn Ihr Gerät eintrifft, verbinden Sie es mit Ihrem On-Premises-Netzwerk und legen die IP-Adresse entweder manuell oder automatisch mit dem Dynamic Host Configuration Protocol (DHCP) fest. Sie müssen AWS OpsHub for Snow Family, eine grafische Benutzeroberfläche (GUI)-Anwendung für die Verwaltung Ihres Snowcone-Geräts, herunterladen und installieren. 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 Instances starten, um Ihre Edge-Anwendungen bereitzustellen oder Ihre Daten mit nur wenigen Klicks in auf das Gerät zu migrieren AWS OpsHub.

Wenn Ihr Datenverarbeitungs- oder Datenübertragungsauftrag abgeschlossen ist und das Gerät zur Rückgabe bereit ist, aktualisiert das E-Ink-Versandetikett automatisch die Rückgabeadresse und stellt sicher, dass das Snowcone-Gerät an die richtige AWS Einrichtung geliefert wird. Wenn das Gerät ausgeliefert wird, können Sie den Nachverfolgungsstatus über Nachrichten erhalten, die von Amazon Simple Notification Service (Amazon SNS), generierten Texten und E-Mails oder direkt von der Konsole gesendet werden.

Themen

- [AWS Snowcone Workflow](#)
- [Funktionsweise von Importaufträgen](#)
- [Für den Import von Auftragsspeicher](#)
- [Für Datenverarbeitungsauftragsspeicher](#)

AWS Snowcone Workflow

Sie können drei verschiedene Auftragsstypen erstellen. Obwohl sich die Auftragsstypen in ihren Anwendungsfällen unterscheiden, verfügen sie alle über den folgenden Workflow für die Bestellung, den Empfang und die Rückgabe des Geräts.

Der Workflow

1. Erstellen des Auftrags – Sie erstellen jeden Auftrag auf der Managementkonsole für die AWS Snow-Familie oder programmgesteuert über die Auftragsverwaltungs-API und wählen je nach Anwendungsfall einen Gerätetyp aus – Snowcone oder Snowcone SSD. Sie können den Status des Auftrags auf der AWS Management Console oder über die Snowcone-API verfolgen.
2. Ein Gerät ist für Ihren Auftrag vorbereitet – AWS bereitet ein AWS Snowcone Gerät für Ihren Auftrag vor und der Status Ihres Auftrags ändert sich in Vorbereiten von Snowcone.
3. Ein Gerät wird Ihnen vom Transporteur Ihrer Region zugestellt – Der Versandeur übernimmt von hier aus und der Status Ihres Auftrags ändert sich jetzt in Bei der Übertragung an Sie. Sie finden Ihre Nachverfolgungsnummer und einen Link zur Nachverfolgungswebsite auf der - Managementkonsole für die AWS Snow-Familie Konsole oder mit der Auftragsverwaltungs-API. Informationen darüber, wer der Mobilfunkanbieter Ihrer Region ist, finden Sie unter [Versandüberlegungen für AWS Snowcone](#).
4. Holen Sie sich eine Snowcone-Leistung – Um den geringsten Platzbedarf zu erhalten, werden Snowcone-Geräte nicht mit einer Stromversorgung geliefert. Snowcone verwendet eine angeschlossene 45- USB-C-Leistung. Sie kann auch mit einer portablen Batterie betrieben werden. Weitere Informationen finden Sie unter [AWS Snowcone Stromversorgung und Kabel](#).
5. Empfangen des Geräts – Ein paar Tage später liefert der Versandeur 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 übermittelt . Das Gerät wird nicht in einem Rahmen ankommen, da es sich bei dem Gerät um einen eigenen Versandcontainer handelt.
6. Abrufen Ihrer Anmeldeinformationen und Herunterladen des AWS OpsHub oder Snowball Edge-Clients für die Snow Family-Anwendung – Bereiten Sie sich auf die Übertragung von Daten vor, indem Sie Ihre Anmeldeinformationen, Ihr Auftragsmanifest und den Entsperrcode des Manifests abrufen und dann den Snowball Edge-Client herunterladen.
 - Rufen Sie das Manifest für Ihr Gerät von der Konsole oder mit der Auftragsverwaltungs-API ab, wenn sich das Gerät an Ihrem Standort On-Premises befindet. Das Manifest wird verwendet, um Ihren Zugriff auf das Gerät zu authentifizieren. Das Manifest ist verschlüsselt, sodass nur der Entsperrcode es entschlüsseln 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 Ihnen, 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 in die migrieren können AWS Cloud. Mit nur wenigen Klicks können Sie mit Ihr Snowcone-Gerät AWS OpsHub entsperren und konfigurieren, Daten ziehen und ablegen, Anwendungen starten oder Gerätemetriken überwachen. Sie können es auf Windows- oder macOS-Client-Computern herunterladen und installieren, z. B. auf einem Laptop. Bei der Nutzung des AWS OpsHub-Service fallen keine Kosten an.

Laden Sie AWS OpsHub von [AWS Snowball -Ressourcen](#) herunter. Weitere Informationen zu finden Sie AWS OpsHub unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

- Der Snowball Edge-Client ist das Tool, mit dem Sie den Datenfluss vom Gerät zu Ihrem On-Premises-Datenziel verwalten.
7. Positionieren der Hardware – Verschieben Sie das Gerät in Ihr Rechenzentrum und öffnen Sie es gemäß den Anweisungen zum Fall. Verbinden Sie das Gerät mit einer Stromversorgung und Ihrem lokalen Netzwerk.
 8. Einschalten des Geräts – Schalten Sie das Gerät ein, indem Sie die Einschalttaste über der Bol-Anzeige drücken. Nach einigen Minuten erscheint im Display die Meldung Ready (Bereit).
 9. Abrufen der IP-Adresse für das Gerät – Auf der Bol-Anzeige befindet sich eine Registerkarte CONNECTION. Gehen Sie auf diese Registerkarte und rufen Sie die IP-Adresse für das AWS Snowcone Gerät ab.
 10. Zum AWS OpsHub Entsperren des Geräts verwenden – Um das AWS Snowcone Gerät zu entsperren, geben Sie die IP-Adresse des Geräts ein, laden Ihr Manifest hoch und den Entsperrcode. AWS OpsHub entschlüsselt das Manifest und verwendet es, um Ihren Zugriff auf das Gerät zu authentifizieren. Weitere Informationen zu finden Sie AWS OpsHub unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).
 11. Verwenden des -Geräts – Verwenden Sie , AWS OpsHub um AWS Snowcone Geräte einzurichten und zu verwalten, damit Sie Ihre Edge-Computing-Workloads schnell ausführen und Daten an die übertragen können AWS Cloud. Mit nur wenigen Klicks können Sie mit Ihr Snowcone-Gerät AWS

OpsHub entsperren und konfigurieren, Daten ziehen und ablegen, Anwendungen starten oder Gerätemetriken überwachen. Details hierzu finden Sie unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

12. Trennen Sie die Ethernet- oder Netzkabel nicht – Trennen Sie das Ethernet-Kabel oder die USB-C-Netzkabel oder -batterie während Datenübertragungs- oder Datenverarbeitungsvorgängen nicht. Um das Snowcone-Gerät zu deaktivieren, nachdem Ihre Datenübertragung oder Ihr Datenverarbeitungsauftrag abgeschlossen ist, drücken Sie die Einschalttaste.
13. Vorbereiten des Geräts auf seinen Rücklauf – Nachdem Sie mit dem Gerät an Ihrem On-Premises-Standort fertig sind, drücken Sie die Einschalttaste über der Anzeige, um das Gerät auszuschalten. Trennen Sie das Gerät und speichern Sie seine Stromkabel im Kabelknoten oben am Gerät. Schließen Sie dann alle drei Kabel des Geräts. Das Gerät ist nun versandfertig für die Rückgabe.
14. Der Mobilfunkanbieter Ihrer Region gibt das Gerät an zurück AWS – Wenn der Mobilfunkanbieter über das AWS Snowcone Gerät verfügt, ändert sich der Status des Auftrags in Während der Übertragung an AWS.

Funktionsweise von Importaufträgen

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

Online-Datenübertragung zwischen Snowcone und AWS Storage Services mit DataSync

[AWS DataSync](#) ist ein Online-Datenübertragungsservice, der das Kopieren großer Datenmengen in und aus - AWS Speicherservices über das Internet oder vereinfacht, automatisiert und beschleunigt AWS Direct Connect. Ein AWS DataSync Agent ist auf Ihrem Snowcone-Gerät vorinstalliert und wird verwendet, um Daten zwischen dem Gerät und Amazon S3-Buckets, Amazon Elastic File System (Amazon EFS)-Dateisystemen und Amazon FSx for Windows File Server zu übertragen. verarbeitet DataSync automatisch das Verschieben von Dateien und Objekten, die Planung von Datenübertragungen, die Überwachung des Fortschritts von Übertragungen, 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 an 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 mithilfe der AWS Management Console oder der 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.

Sie können die DataSync Ausführung von auf Snowcone für Folgendes verwenden:

- Damit Edge-Computing-Anwendungen Daten sammeln, verarbeiten Sie die Daten, um sofortige Einblicke zu erhalten, und übertragen Sie die Daten dann online an AWS.
- Um Daten zu übertragen, die kontinuierlich von Sensoren oder Maschinen online an AWS in einer Fabrik oder an anderen Edge-Standorten generiert werden.
- Um Medien, wissenschaftliche oder andere Inhalte online von - AWS Speicherservices an Ihre Partner und Kunden zu verteilen.
- So aggregieren Sie Inhalte, indem Sie Medien, wissenschaftliche oder andere Inhalte online von Ihren Edge-Standorten an übertragen AWS.

Für einmalige Edge-Datenverarbeitungs- oder Datenübertragungsworkflows oder für Snowcone-Workflows an Edge-Standorten ohne eine Wide Area Network (WAN)-Verbindung oder unzureichende WAN-Bandbreite empfehlen wir, das Snowcone-Gerät zurück an zu senden AWS , um die Datenübertragung abzuschließen.

Offline-Datenübertragung zwischen Snowcone und Amazon S3

Bei Offline-Datenimportaufträgen verbinden Sie das Snowcone-Gerät mit Ihrem On-Premises-Netzwerk und verwenden dann , AWS OpsHub um das Gerät zu entsperren. Laden Sie AWS OpsHub von der [AWS Snowball Ressourcenseite](#) herunter. Sie können Daten über die NFS-Schnittstelle von On-Premises-Speichergeräten auf Ihr Snowcone-Gerät kopieren. Nachdem Sie die Daten auf Ihr Snowcone-Gerät kopiert haben, trägt das E-Ink-Versandetikett auf dem Gerät dazu bei, 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 den Import von Auftragsspeicher

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

Für Datenverarbeitungsauftragsspeicher

Wenn der Auftragstyp lokale Datenverarbeitung ist, können Sie insgesamt 8 TB oder 14 TB an lokalen kapazitätsoptimierten HDD-Volumes (sbg1) erstellen und sie an AmazonEC2-compatible Instances anfügen. Die Verwendung von Amazon-EBS-Volumes ermöglicht es den lokalen AmazonEC2-compatible Instances, auf mehr lokale Kapazität zuzugreifen als das Root-Volume allein. Da es sich nur um lokalen Speicher handelt, gehen auf die Amazon-EBS-Volumes geschriebene Daten verloren, wenn das Gerät an zurückgegeben wird, AWS da es nicht in Amazon S3 importiert werden kann.

Note

Der NFS-Server ist nicht für Datenverarbeitungsaufträge verfügbar. Wenn Sie Daten in die oder aus importieren oder exportieren müssen AWS Cloud oder einen AWS DataSync Agenten ausführen müssen, wählen Sie bei der Bestellung nicht den lokalen Datenverarbeitungsauftragstyp aus.

AWS Snowcone Gerätespezifikationen

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 für die Klassifizierung](#)
- [AWS Snowcone Stromversorgung und Kabel](#)
- [Festplatten- und CPU-Leistung](#)

Zusammenfassung der Funktionen und Spezifikationen

In der folgenden Tabelle sind die Funktionen und Spezifikationen für das Snowcone-Gerät zusammengefasst.

Item	Spezifikation
Nutzungsszenario	Industrielles Internet der Dinge (IoT), Transport, Gesundheits-IoT, Inhaltsverteilung, taktisches Edge-Computing, Logistik, autonomes Fahrzeug, Datenmigration
Gerätegröße	9" lang, 6" breit und 3" hoch (227 mm x 148,6 mm x 82,65 mm)
Gerätegewicht	4,5 Bol. (2.04) für Snowcone und 4.6 Bol (2.09) Snowcone SSD
Speicherkapazität	8 TB verwendbar für Snowcone und 14 TB verwendbar für Snowcone SSD
Onboarding-Datenverarbeitungsoptionen	Amazon EC2 Amazon Machine Images (AMIs)

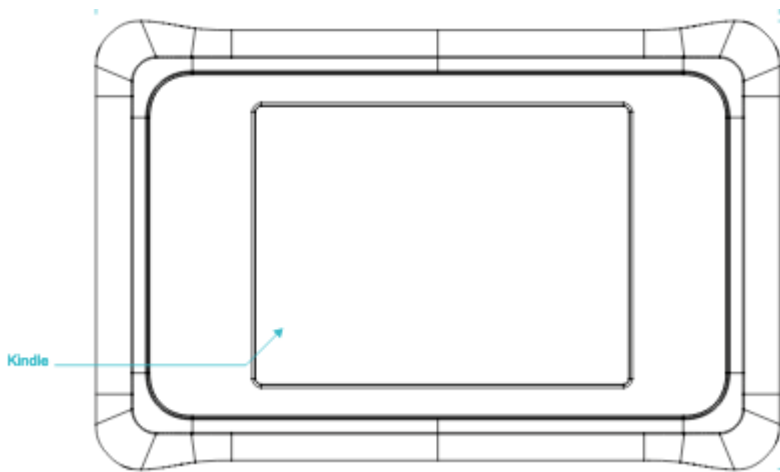
Item	Spezifikation
Verschlüsselung	Ja, 256-Bit
Übertragungen über das Network File System (NFS)	Ja
Übertragungen über die Amazon S3-API	Nein
Mobilität	Telefonie-basierter Vorgang
WLAN	WLAN <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note WLAN ist nur in AWS-Regionen in Nordamerika verfügbar.</p> </div>
Anzahl der verwendbaren vCPUs	2 vCPUs
Verfügbarer Speicher	4 GB
Netzwerkschnittstellen	2x 1/10 Gigabit (Gb) – RJ45
AWS DataSync Agent vorinstalliert	Ja
Typische Lebensdauer von Aufträgen	Offline- oder Online-Datenübertragung: Tage zu Wochen Edge-Datenverarbeitung: Wochen bis Monate
Maximale Auftragslänge	Edge-Datenverarbeitung oder laufende Datenübertragung: Bis zu 360 Tage

Hardware und Netzwerk

Ein Snowcone-Gerät bietet 8 TB oder 14 TB verfügbaren Speicher. Es führt bestimmte Amazon Elastic Compute Cloud (Amazon EC2)-Instances mit zwei verfügbaren CPUs und 4 GB verfügbarem Speicher zur Unterstützung Ihrer Anwendungen und AWS IoT Greengrass Funktionen aus. In diesem Abschnitt finden Sie Informationen über das physische Gerät, z. B. die Schnittstellen, die Einschalttaste und die Stromanforderungen, wie sie in verschiedenen Ansichten des Geräts angezeigt werden.

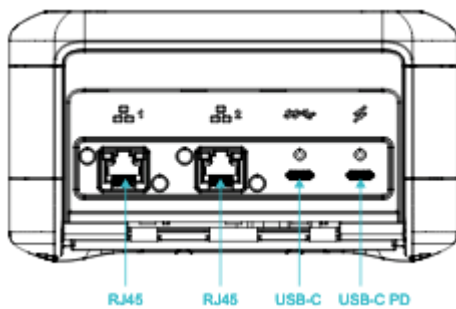
Ansicht von oben

Die obere Oberfläche des Snowcone-Geräts enthält ein integriertes E-Ink-Kontakt-Display, das als Operatorschnittstelle verwendet wird, um sowohl kabelgebundene als auch WLAN-Netzwerke einzurichten. Sie dient auch als Display für ein elektronisches Versandetikett. Das elektronische Versandetikett ist sowohl mit ausgehenden als auch mit eingehenden Versandetiketten vorprogrammiert, die sich automatisch ändern, nachdem das Gerät zum ersten Mal eingeschaltet wurde.



Trichterfenster

Sie stellen alle Kabelverbindungen auf der Rückwand her. In diesem Abschnitt werden die einzelnen Konnektoren beschrieben.



Stromversorgung

Die Stromversorgung des Geräts erfolgt über die USB-C-Verbindung ganz rechts. Dazu wird ein passender Netzadapter verwendet, der mindestens 45 W liefern kann.

i Note

AWS Snowcone enthält keine Stromversorgung, da sie mit dem kleinstmöglichen Formfaktor geliefert wird. Details hierzu finden Sie unter [AWS Snowcone Stromversorgung und Kabel](#).

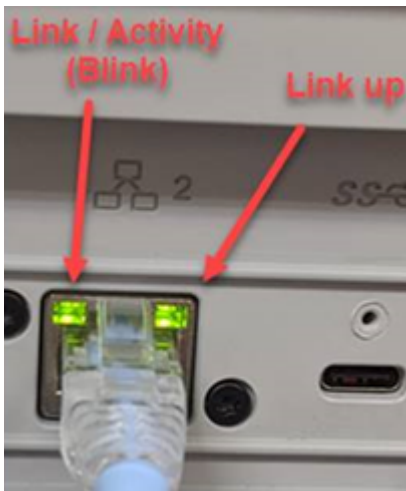
USB

Die erste USB-C-Verbindung ist nicht aktiv.

Ethernet-Konnektoren 1 und 2

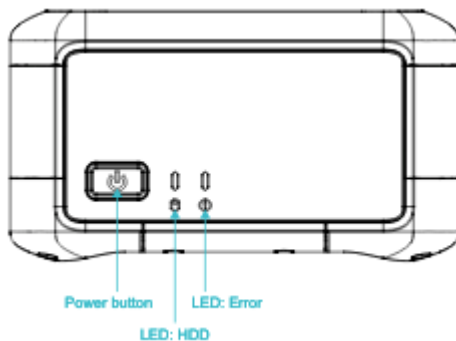
Für kabelgebundene Netzwerke bietet das Snowcone-Gerät zwei Ports, die automatisch für Ethernet-Netzwerke mit 1 Gigabit (Gb) oder 10 GB aushandeln.

RJ45 10/1G Base-T Ethernet-Ports – Diese Ports verhandeln automatisch zwischen 10 Gb und 1 Gb, basierend auf der Funktion für Verbindungen am anderen Ende. Sie verhandeln keine Geschwindigkeiten unter 1 GB (z. B. 100 MB oder 10 MB). Die Verknüpfung befindet sich rechts neben jedem Konnektor und die Aktivität befindet sich links.



Frontbereich

Die Frontleiste enthält die Einschalttaste und die Statusanzeige.



Netzschalter

Um das Gerät einzuschalten, drücken Sie die Einschalttaste kurz. Die Schaltfläche wird angezeigt, die E-Ink-Anzeige ändert sich in eine Fortschrittsleiste und Bitte warten wird angezeigt.

Um das Gerät auszuschalten, halten Sie den Netzschalter zwei Sekunden lang oder bis die E-Ink-Anzeige Bitte warten anzeigt.

Note

Schalten Sie die Einschalttaste länger als fünf Sekunden lang ein, um das Gerät auszuschalten. Dies wird nicht empfohlen, da dies dazu führen kann, dass Daten in Puffern verloren gehen. Nach einem Stromausfall stellt das Gerät die Stromversorgung automatisch auf den letzten Betriebszustand wieder her.

LEDs

Neben der Einschalttaste befinden sich zwei LEDs. Das linke wird mit Festplattenaktivität ausgelöst und das rechte wird bei einer Fehlerbedingung ausgelöst.

AWS Snowcone Wi-Fi-Spezifikationen

AWS Snowcone unterstützt Gigabit-WLAN-Netzwerke mit dem IEEE-Standard 802.11ac sowie 802.11abgn-Netzwerke. Um den WLAN-Durchsatz für Snowcone zu maximieren, verwenden Sie 2x2 802.11ac 160 MHz-Kanäle, die bis zu zehnmal schneller sein können als Baseline-1x1 802.11bgn-Netzwerke. 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 On-Premises-Netzwerk verbinden, oder Sie können es über WLAN kabellos verbinden. Mit der WLAN-Verbindung können Sie das Snowcone-Gerät mithilfe von verwalteten AWS OpsHub und Daten zwischen Snowcone und On-Premises-Speichergeräten übertragen.

Note

WLAN ist nur in AWS-Regionen in Nordamerika verfügbar.

Spezifikationen für die Klassifizierung

AWS Snowcone -Geräte sind so konzipiert, dass sie strenge Standards für die Abschwächung erfüllen, einschließlich ISTA-3A , Bol D4169 und MIL-STD-810G für Freifall, betriebliche Abschwächung und mehr. Sie sind so konzipiert, dass sie 1,15 Meter (3,8 Fuß) tolerieren. Sie erfüllen auch den Standard IP65 International Protection Marking, was bedeutet, dass sie sowohl Telefonie (und bei dichtem Zustand keine Kabel innerhalb der Umschließung zulassen) als auch Wasserresistent sind (einschließlich Schutz vor Wasserströmen auf allen Seiten).

Die Geräte haben einen großen Betriebstemperaturbereich von der Einfrierung (0 Grad C oder 32 Grad F) bis hin zu sertähnlichen Bedingungen (Snowcone: 38 Grad C oder 100 Grad F; Snowcone SSD: 45 Grad C oder 113 Grad F). Wenn Snowcone-Geräte im Speicher oder ausgeliefert werden, stehen sie auch gleichmäßigeren Temperatur stand (-32 Grad C oder -25,6 Grad F bis 63 Grad C oder 145,4 Grad F).

AWS Snowcone Stromversorgung und Kabel

AWS Snowcone -Geräte enthalten keine Stromversorgung oder kein Ethernet-Kabel (RJ45), da sie mit dem geringstmöglichen Formfaktor geliefert werden. Sie haben die Möglichkeit, Ihr Snowcone-Gerät über eine Plug-In-Netzquelle oder eine Batterie auszuführen. Im Folgenden finden Sie die Details, die Sie bei der Bestellung einer Stromversorgung und eines Ethernet-Kabels unterstützen sollten:

USB-C-Netzadapter – Verwenden Sie einen USB-C-Netzadapter mit dem Snowcone-Gerät, um Netzteile einstecken zu können oder um Umgebungen mit Kabeln (nicht mobile) zu betreiben. Um Ihr Snowcone-Gerät zu betreiben, können Sie einen der folgenden AWS-getesteten USB-C-Netzadapter erwerben:

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

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

USB-C-Kabel – Verwenden Sie eine USB-C-Kabel, um das Snowcone-Gerät in mobilen oder portablen Betriebsumgebungen zu betreiben. Um Ihr Snowcone-Gerät zu betreiben, können Sie eines der folgenden AWS-getesteten USB-C-Kabel kaufen:

- [Dell Notebook Power Bank Plus – USB C, 65Wh – PW7018LC](#)
- [Omni 20c+](#)

Sie können auch jede USB-C-Kabel verwenden, die für 45 W+ geeignet ist.

Ethernet-Kabel (RJ45) – Um das Snowcone-Gerät mit Ihrem lokalen Netzwerk zu verbinden, verwenden Sie ein Ethernet-Kabel (RJ45). Wenn Sie noch keine haben, sollten Sie eine kaufen.

Festplatten- und CPU-Leistung

AWS Snowcone ist ein speziell entwickeltes Edge-Datenverarbeitungs-/Datenübertragungsgerät. Die Leistung von Datenträger und CPU hängt von einer Vielzahl von Faktoren ab. Einige Beispielleistungsnummern für die Übertragung sind in [Snowcone Performance](#) angegeben

Einrichten von 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

- [Registrieren bei AWS](#)

Registrieren bei AWS

Bei der Registrierung für Amazon Web Services wird Ihr -Konto automatisch für alle AWS Dienste registriert. AWS AWSEs werden Ihnen aber nur die Services, die Sie nutzen. Nachdem Sie Ihr Konto eingerichtet haben, können Sie Ihr AWS Snowcone Gerät über die bestellen, konfigurieren und verwalten Managementkonsole für die AWS Snow-Familie. Weitere Informationen zu Preisen und Gebühren für Snowcone finden Sie unter [AWS Snowcone Preisgestaltung](#).

Wenn Sie bereits eine haben AWS-Konto, notieren Sie sich Ihre AWS-Konto Nummer. Wenn Sie noch nicht über ein verfügen AWS-Konto, führen Sie die folgenden Schritte aus:

So erstellen Sie ein AWS-Konto

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

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

Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Stammbenutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Methode zur Gewährleistung der Sicherheit sollten Sie den [administrativen Zugriff einem administrativen Benutzer zuweisen](#) und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, die einen Root-Benutzerzugriff erfordern](#).

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 Auftrag planen. Stellen Sie sicher, dass sich Ihr Standort und Ihr Amazon S3-Bucket innerhalb desselben befinden, AWS-Region da dies sich auf Ihre Fähigkeit auswirkt, das Gerät zu bestellen. Es gibt Einschränkungen beim Versand des Snowcone-Geräts außerhalb der Ländergrenzen einer Region. Weitere Informationen finden Sie unter [Versandeinschränkungen nach Regionen](#).

Internationale Sendungen an Standorte außerhalb Ihres AWS-Region werden auf der Managementkonsole für die AWS Snow-Familie für bereits aufgeführte Kunden für eine ausgewählte Reihe von Standorten aus bestimmten Regionen (z. B. USA nach Mexiko) unterstützt. Sie sollten das Zielziel, die Kosten und den Zeitplan für diese Anfragen mit Ihrem Kontoteam besprechen.

Im Rahmen des Bestellprozesses 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 von Daten auf jedem Gerät verwendet werden. Weitere Informationen finden Sie unter [Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts](#).

Themen

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

Fragen zur lokalen Umgebung

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

Wird während der Übertragung auf die Daten zugegriffen?

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

Arbeiten mit Dateien mit Sonderzeichen

Beachten Sie unbedingt, dass bei Dateien, die Sonderzeichen enthalten, Fehler auftreten können. Obwohl Amazon S3 Sonderzeichen zulässt, empfehlen wir dringend, die folgenden Zeichen zu vermeiden:

- Umgekehrter Schrägstrich ("`\`")
- Linke geschweifte Klammer ("`{`")
- Rechte geschweifte Klammer ("`}`")
- Linke eckige Klammer ("`[`")
- Rechte eckige Klammer ("`]`")
- Kleiner als-Symbol ("`<`")
- „Größer als“-Symbol ("`>`")
- 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 beim Kopieren einzelner Objekte oder beim Ausführen eines rekursiven Befehls vorsichtig sein. Umschließen Sie einzelne Objekte, die einen Abstand im Namen enthalten, mit Anführungszeichen. Im Folgenden finden Sie Beispiele für solche Dateien.

Betriebssystem	Dateiname: test file.txt
Windows	„C:\Users\ <code><username></code> \desktop\test file.txt“
Mac	/Users/ <code><username></code> /test\ file.txt

Betriebssystem	Dateiname: test file.txt
Linux	/home/<username>/test\ file.txt

Note

Die einzigen übertragenen Objektmetadaten sind der Objektname und die Größe. AWS DataSync behält jedoch Zugriffssteuerungslisten (ACLs) bei. Weitere Informationen finden Sie unter [So DataSync verarbeitet Metadaten und spezielle Dateien](#) im AWS DataSync - Benutzerhandbuch.

Verwenden von Amazon EC2 auf Snowcone

Dieser Abschnitt bietet einen Überblick über die Verwendung von AmazonEC2-compatible Rechen-Instances auf einem AWS Snowcone -Gerät.

Sie sollten die Amazon EC2-compatible Instances verwenden, wenn Sie eine Anwendung auf dem Edge ausführen, die als virtuelle Maschine (ein 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-compatible Instances auf Snowcone ermöglicht es Ihnen, Ihre Anwendung auf Amazon EC2 zu erstellen und zu testen. Sie können EC2-compatible AMIs während der AWS Snowcone Auftragserstellung entweder mit AWS Management Console, AWS Snowball SDK oder aktivieren und bereitstellen AWS CLI.

Unterstützte Amazon-EC2-Instance-Typen

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

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 AWS OpsHub , um Ihre Instances auf Snowcone zu verwalten. Laden Sie AWS OpsHub von der [AWS Snowball Ressourcen](#)-Website herunter. Nachdem Sie das Gerät mit entsperrt

haben AWS OpsHub, navigieren Sie zur Amazon-EC2-Amazon EC2-Seite. Wählen Sie Instance erstellen aus, um eine EC2-compatible Instance basierend auf dem AMI zu erstellen, das Sie beim Erstellen des Auftrags auf das Gerät vorinstalliert haben. Anschließend können Sie eine Verbindung zu den Instances herstellen und Ihre Edge-Anwendung ausführen. bietet AWS OpsHub auch Schaltflächen mit einem Klick zum Starten, Stoppen, Beenden und Neustarten Ihrer EC2-compatible Instances. Weitere Informationen finden Sie unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

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 führen wir ein vollständiges Löschen des Geräts durch, wenn es an zurückgegeben wird AWS. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Important

Daten in Datenverarbeitungs-Instances, die auf einem Snowcone ausgeführt werden, werden nicht in importiert AWS.

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

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

Preise für Compute Instances auf 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 Auftrag AMIs hinzufügen können, müssen Sie über ein AMI in Ihrem AWS-Konto verfügen und es muss sich um einen unterstützten Image-Typ handeln. Derzeit basieren

unterstützte AMIs auf den Images [Amazon Linux 2](#), [CentOS 7 \(x86_64\) – mit Updates für HVM](#) oder [Ubuntu 16.04 LTS – Xenial \(HVM\)](#). Sie erhalten diese Images über das [AWS Marketplace](#).

Bevor Sie Ihrer Auftragsanforderung AMIs hinzufügen, stellen Sie sicher, dass Sie über ein oder mehrere unterstützte AMIs in Ihrem verfügbaren AWS-Konto. Stellen Sie bei der Auswahl eines AMI im Marketplace sicher, dass es über einen unterstützten Produktcode und plattform verfügt. Weitere Informationen finden Sie unter [Überprüfen von Produktcodes und Plattfordetails von AWS Marketplace AMIs](#).

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

Überprüfen von Produktcodes und Plattfordetails von AWS Marketplace AMIs

Bevor Sie mit dem Prozess zum Hinzufügen eines AMI von AWS Marketplace zu Ihrem Snow Family-Gerät beginnen, stellen Sie sicher, dass der Produktcode und die Plattfordetails 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 erstellen Sie den Auftrag, um das Snow Family-Gerät zu bestellen. Sie können eine beliebige Region auswählen, die Ihnen zur Verfügung steht, unabhängig von Ihrem Standort.
3. Wählen Sie im Navigationsbereich die Option AMIs.
4. Verwenden Sie die Filter- und Suchoptionen, um die Liste der angezeigten AMIs so einzugrenzen, dass nur die AMIs angezeigt werden, die Ihren Kriterien entsprechen. Wählen Sie beispielsweise AMIs, die von der bereitgestellt werden AWS Marketplace, Öffentliche Images aus. Verwenden Sie dann die Suchoptionen, um die Liste der angezeigten AMIs weiter einzugrenzen:
 - (Neue Konsole) Wählen Sie die Suchleiste und dann im Menü Besitzeralias , dann den Operator = und dann den Wert amazon aus.
 - (Alte Konsole) Wählen Sie die Search bar (Suchleiste) aus und anschließend im Menü den Punkt Owner (Besitzer). Wählen Sie dann den Wert Amazon Images (Amazon-Images) aus.

Note

AMIs von AWS Marketplace enthalten aws-marketplace in der Spalte Quelle.

5. Wählen Sie in der Spalte AMI-ID die AMI-ID des AMI aus.
6. Stellen Sie in der Image-Zusammenfassung des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der folgenden Tabelle.

Unterstützte AWS Marketplace AMI-Produktcodes

AMI-Betriebssystem	Produktcode
Ubuntu Server 14.04 LTS	b3dl4415quatdnd14qa6kcu45
CentOS 7 (x86_64)	aw0evgkw8e5c1q413zgy5pjce
Ubuntu 16.04 LTS	csv6h7oyg29b7epjzg7qdr7no
Amazon Linux 2	avyfzznywektml5qv5f57ska
Ubuntu 20.04 LTS	a8jynf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkjt189a13aqe

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

Erstellen eines Linux-AMI aus einer Instance

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 aus 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 Anforderungen 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
 - Anfügen zusätzlicher Amazon EBS-Volumes
4. (Optional) Erstellen Sie Snapshots von allen Volumes, die an Ihre Instance angefügt sind. Weitere Informationen zum Erstellen von Snapshots finden Sie unter [Erstellen von Amazon-EBS-Snapshots](#).
5. Klicken Sie im Navigationsbereich auf Instances und wählen Sie Ihre Instance aus. Wählen Sie für Aktionen die Option Image , Image erstellen aus.

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).
 - Image name – Ein eindeutiger Name für das Image.
 - Bildbeschreibung – Eine optionale Beschreibung des Bildes mit bis zu 255 Zeichen.
 - Kein Neustart – Diese Option ist standardmäßig nicht ausgewählt. Amazon EC2 fährt die Instance herunter, erstellt Snapshots von allen angefügten Volumes, erstellt und registriert das AMI und startet dann die Instance neu. Wählen Sie Kein Neustart, um zu vermeiden, 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 Stamm-Volume ändern und weitere Amazon EBS- und Instance-Speicher-Volumes hinzufügen. Sie erhalten weitere Informationen zu den einzelnen Feldern, indem Sie jeweils auf das i-Symbol neben den Feldern klicken; dadurch wird die QuickInfo zum jeweiligen Feld angezeigt. Einige wichtige Punkte sind im Folgenden aufgeführt.
 - Um die Größe des Root-Volumes zu ändern, suchen Sie in der Spalte Volume-Typ nach Root. Geben Sie für Größe (GiB) den erforderlichen Wert ein.
 - Wenn Sie Bei Beendigung löschen auswählen, wird das Amazon-EBS-Volume gelöscht, wenn Sie die aus diesem AMI erstellte Instance beenden. Wenn Sie Delete on Termination deaktivieren, wird das Amazon-EBS-Volume beim Beenden der Instance nicht gelöscht. Weitere Informationen finden Sie unter [Beibehalten von Amazon-EBS-Volumes bei der Instance-Beendigung](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.
 - Um ein Amazon-EBS-Volume hinzuzufügen, wählen Sie Neues Volume hinzufügen (was eine neue Zeile hinzufügt). Wählen Sie unter Volume Type (Volumetyp) die Option EBS und füllen Sie die Felder in der Zeile aus. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden diese zusätzlichen Volumes automatisch der Instance zugeordnet. Leere Volumes müssen formatiert und „gemountet“ werden. Volumes, die auf einem Snapshot basieren, müssen „gemountet“ werden.
 - Informationen zum Hinzufügen eines Instance-Speicher-Volumes finden Sie unter [Hinzufügen von Instance-Speicher-Volumes zu einem AMI](#). 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 in verfügbar ändern.

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

8. Starten Sie eine Instance über Ihr neues AMI. Weitere Informationen finden Sie unter [Starten einer Instance mit dem Launch Instance Wizard](#).
9. Die neue ausgeführte Instance enthält alle Anpassungen, die Sie in den letzten Schritten vorgenommen haben.

So erstellen Sie ein AMI aus einer Instance mithilfe der Befehlszeile

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

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

Erstellen eines Linux-AMI aus einem Snapshot

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

So erstellen Sie mit der Konsole ein AMI aus einem Snapshot

1. Öffnen Sie die Amazon EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich unter Elastic Block Store die Option Snapshots.
3. Wählen Sie den Snapshot und dann Actions (Aktionen) und Create Image (Image erstellen) aus.
4. Füllen Sie im Dialogfeld Image aus EBS-Snapshot erstellen die Felder aus, um Ihr AMI zu erstellen, und wählen Sie dann Erstellen aus. Wenn Sie eine übergeordnete Instance neu erstellen, wählen Sie dieselben Optionen wie für die übergeordnete Instance aus.
 - 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 besteht die Möglichkeit, dass Ihre Instance die Zustandsprüfungen 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 Größenanpassung des Dateisystems auf Ihrer Instance für ein größeres Volume finden Sie unter [Erweitern eines Linux-Dateisystems nach der Größenanpassung eines Volumes](#).

So erstellen Sie ein AMI aus einem Snapshot mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen finden Sie unter [Zugriff auf 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 Auftrags im Managementkonsole für die AWS Snow-Familie. Eine Übersicht über das AWS Snowcone Gerät finden Sie unter [Funktionsweise AWS Snowcone von](#).

In dieser Dokumentation zu den ersten Schritten wird davon ausgegangen, dass Sie die verwenden, [Managementkonsole für die AWS Snow-Familie](#) um Ihren Auftrag 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 ein AWS-Konto und einen Administratorbenutzer in AWS Identity and Access Management (IAM) erstellen. Weitere Informationen finden Sie unter [Einrichten von AWS für AWS Snowcone](#).

Informationen zu den ersten Schritten mit finden Sie unter Erstellen eines Auftrags zum AWS Snowcone Bestellen eines Snow-Family-Geräts. <https://docs.aws.amazon.com/snowball/latest/snowcone-guide/create-job-common.html>

Themen

- [Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts](#)
- [Stornieren eines Auftrags über die Managementkonsole für die AWS Snow-Familie](#)
- [Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät](#)
- [Entsperren des Snow Family-Geräts](#)
- [Neustarten des Snow Family-Geräts](#)

Erstellen eines Auftrags zum Bestellen eines Snow Family-Geräts

Um ein Snow-Family-Gerät zu bestellen, erstellen Sie einen Auftrag zum Bestellen eines Snow-Family-Geräts in der Managementkonsole für die AWS Snow-Familie. Ein Auftrag ist ein Begriff, der AWS verwendet, um den Lebenszyklus der Verwendung eines Snow-Family-Geräts durch einen Kunden zu beschreiben. Ein Auftrag beginnt mit der Bestellung eines Geräts, wird fortgesetzt, wenn das Gerät AWS vorbereitet und an Sie sendet und Sie es verwenden, und wird abgeschlossen, nachdem das Gerät AWS empfangen und verarbeitet hat, nachdem Sie es zurückgegeben haben.

Aufträge werden nach Typ kategorisiert: Export, Import sowie lokale Rechenleistung und Speicher. Weitere Informationen finden Sie unter [Grundlegendes zu AWS Snowball-Edge-Aufträgen](#).

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

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

Themen

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

Schritt 1: Auswählen eines Auftragstyps

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

So wählen Sie Ihren Auftragstyp aus

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#). Wenn Sie zum ersten Mal einen Auftrag in dieser erstellen AWS-Region, wird die Seite AWS Snow Family angezeigt. Andernfalls wird die Liste der vorhandenen Aufträge angezeigt.
2. Wenn dies Ihr erster Auftrag ist, wählen Sie Ein AWS Snow Family-Gerät bestellen aus. Wenn Sie erwarten, dass mehrere Aufträge mehr als 500 TB Daten migrieren, wählen Sie Erstellen Sie

Ihren großen Datenmigrationsplan mit mehr als 500 TB aus. Wählen Sie andernfalls in der linken Navigationsleiste Auftrag erstellen aus. Wählen Sie Nächster Schritt, um die Seite Planen Ihres Auftrags zu öffnen.

3. Geben Sie im Abschnitt Auftragsname einen Namen für Ihren Auftrag im Feld Auftragsname ein.
4. Wählen Sie je nach Bedarf einen der folgenden Auftragstypen aus:
 - In Amazon S3 importieren – Lassen Sie AWS ein leeres Snowcone-Gerät an Sie senden. Sie verbinden das Gerät mit Ihrem lokalen Netzwerk und konfigurieren das Gerät mit OpsHub. Sie kopieren Daten mithilfe der NFS-Freigabe auf das Gerät, senden sie zurück an AWS und Ihre Daten werden auf Amazon S3 hochgeladen.
 - Nur lokale Datenverarbeitung und Speicher – Führen Sie Datenverarbeitungs- und Speicher-Workloads auf dem Gerät durch, 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: Auswählen Ihrer Datenverarbeitungs- und Speicheroptionen

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

So wählen Sie die Rechen- und Speicheroptionen Ihres Geräts aus

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

Note

Einige Snow Family-Geräte sind möglicherweise nicht verfügbar, je nachdem, bei dem AWS-Region Sie bestellen und welchen Auftragsstyp Sie ausgewählt haben.

Snow devices Info					
	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

2. Wählen Sie im Abschnitt Snowcone-Netzteile die Option Ich werde mein eigenes Netzteil und Ethernet-Kabel bereitstellen aus. Weitere Informationen zu Netzteilen finden Sie unter [AWS Snowcone Netzteile und Kabel](#).
3. Wählen Sie im Abschnitt Preisoption auswählen im Menü Preisoption auswählen den Preistyp aus, der auf diesen Auftrag angewendet werden soll. Informationen zu den Preisen für Geräte finden Sie unter [-AWS Snowcone Preise](#).
4. Treffen Sie im Abschnitt Speichertyp auswählen eine Auswahl je nach Bedarf:
 - NFS-basierte Datenübertragung: Verwenden Sie Network File System (NFS)-basierte Datenübertragung, um Dateien von Ihrem Computer in Amazon S3-Buckets auf Snow-Family-Geräten zu ziehen und abzulegen.

Warning

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

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


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

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

Sie können einen oder mehrere S3-Buckets einschließen. 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 Datenverarbeitung mit EC2-compatible Instances – optional die Option Amazon EC2-compatible AMIs aus Ihrem Konto aus, die auf dem Gerät enthalten sein sollen. Oder geben Sie in das Suchfeld den Namen eines AMI ganz oder teilweise ein, um die Liste der verfügbaren AMIs nach Ihrem Eintrag zu filtern, und wählen Sie dann das AMI aus.

Weitere Informationen finden Sie unter [Erstellen eines Auftrags mit Compute Instances](#) in diesem Handbuch.

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: Auswählen Ihrer Funktionen und Optionen

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

So wählen Sie Ihre Funktionen und Optionen aus

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

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

Themen

- [Auswählen von Sicherheitseinstellungen](#)
- [Wählen Sie Ihre Versandeinstellungen](#)
- [Wählen Sie Ihre Benachrichtigungseinstellungen](#)

Auswählen von Sicherheitseinstellungen

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

So legen Sie die Sicherheit für Ihren Auftrag fest

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

Wählen Sie Ihre Versandeinstellungen

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

So geben Sie Versanddetails an

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

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

Note

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

2. Wählen Sie im Abschnitt Versandgeschwindigkeit eine Versandgeschwindigkeit für den Auftrag aus. Diese Geschwindigkeit zeigt, wie schnell das Gerät zwischen Zielen geliefert wird und nicht widerspiegelt, wie schnell es nach dem heutigen Datum eintrifft. Die Versandgeschwindigkeiten, die Sie wählen können, sind:
 - Eintägiger Versand (ein Werktag)
 - Zweitägiger Versand (2 Werktage)
 - Weitere Informationen finden Sie unter [Versandunternehmen](#).

Wählen Sie Ihre Benachrichtigungseinstellungen

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

Richten Sie Benachrichtigungen wie folgt ein

- Führen Sie im Abschnitt Benachrichtigungen festlegen einen der folgenden Schritte aus:
 - Wenn Sie ein vorhandenes SNS-Thema verwenden möchten, wählen Sie Ein vorhandenes SNS-Thema verwenden und wählen Sie das Thema Amazon-Ressourcenname (ARN) aus der Liste aus.
 - Wenn Sie ein neues SNS-Thema erstellen möchten, wählen Sie Neues SNS-Thema erstellen aus. Geben Sie einen Namen für Ihr Thema und eine E-Mail-Adresse ein.

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

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

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

Wählen Sie die Nächste aus.

Schritt 5: Überprüfen der Auftragsübersicht und Erstellen Ihres Auftrags

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

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

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

Note

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

Note

Snowcone-Geräte werden nicht mit Stromkabeln geliefert, und eines muss separat bereitgestellt werden. Weitere Informationen finden Sie unter [AWS Snowcone Stromversorgung und Telefonie](#).

Nachdem Ihr Auftrag erstellt wurde, können Sie den Status des Auftrags im Abschnitt Auftragsstatus sehen. Ausführliche Informationen zu Auftragsstatus finden Sie unter <https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-job-statuses.html>.

Herunterladen AWS OpsHub

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

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

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

Weitere Informationen finden Sie unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

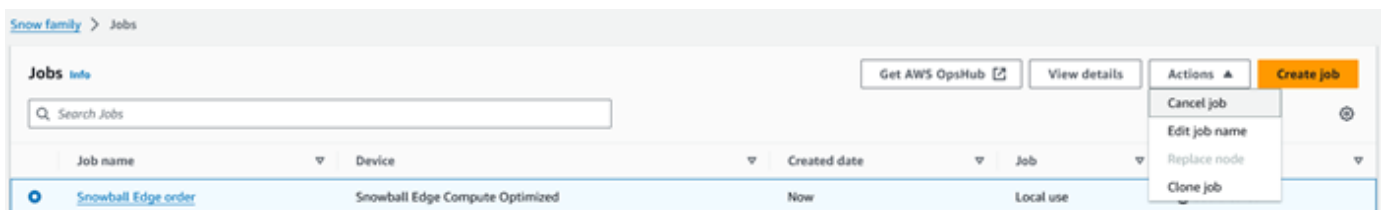
So laden Sie herunter und installieren es AWS OpsHub for Snow Family

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

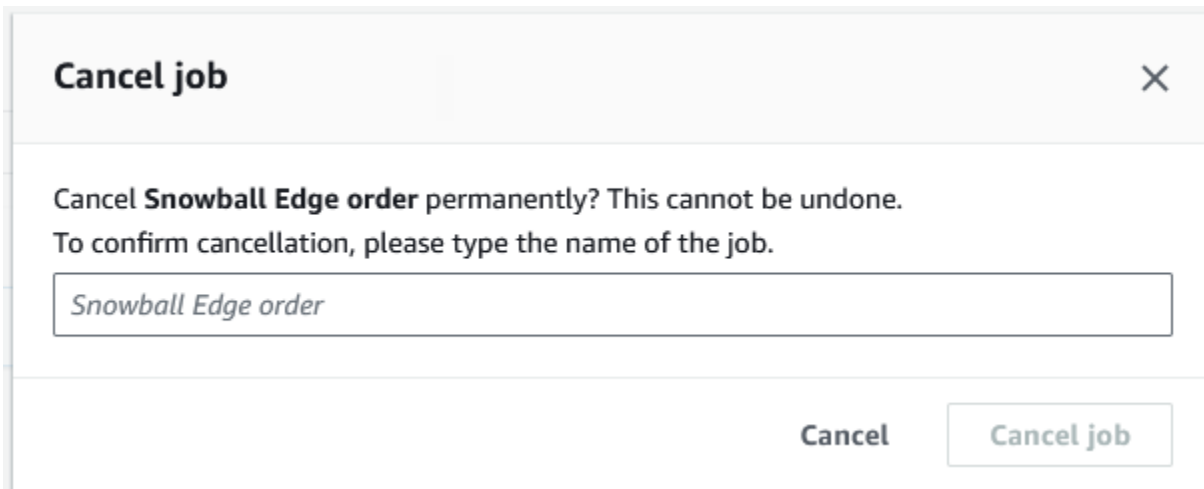
Stornieren eines Auftrags über die Managementkonsole für die AWS Snow-Familie

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

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



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



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

Jeder Auftrag verfügt über einen Satz von Anmeldeinformationen, die Sie von der Managementkonsole für die AWS Snow-Familie oder der Auftragsverwaltungs-API abrufen müssen, um Ihren Zugriff auf das Snow Family-Gerät zu authentifizieren. Bei diesen Anmeldeinformationen handelt es sich um eine verschlüsselte Manifestdatei und einen zugehörigen Entsperrcode. Die Manifestdatei enthält wichtige Informationen zu dem Auftrag und zu den damit verbundenen Berechtigungen.

Note

Sie erhalten Ihre -Anmeldeinformationen, nachdem das Gerät zu Ihnen übertragen wurde. Sie können den Status Ihres Auftrags in der anzeigenden Managementkonsole für die AWS Snow-Familie. Weitere Informationen finden Sie unter [VerständnisAWS SnowconeJobstatus](#).

So rufen Sie Ihre Anmeldeinformationen mit der Konsole ab

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die [Managementkonsole für die AWS Snow-Familie](#).
2. Suchen Sie in der -Konsole in der Tabelle nach dem spezifischen Auftrag, für den das Auftragsmanifest heruntergeladen werden soll, und wählen Sie dann diesen Auftrag aus.
3. Erweitern Sie diesen Bereich Auftragsstatus und wählen Sie Auftragsdetails anzeigen aus.

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

Note

Es wird empfohlen, keine Kopie des Entsperrcodes am selben Speicherort auf dem Computer als Manifest für diesen Auftrag zu speichern. Weitere Informationen finden Sie unter [Bewährte Methoden für das AWS Snowcone Gerät](#).

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

Weiter: [Verwenden des AWS Snowball Edge Clients](#)

Entsperren des Snow Family-Geräts

In diesem Abschnitt wird das Entsperren des Snow Family-Geräts mithilfe der Snowball Edge CLI beschrieben. Informationen zum Entsperren des Geräts mit AWS OpsHub, einem Tool für die grafische Benutzeroberfläche (GUI) für Snow-Family-Geräte, finden Sie unter [Entsperren eines Geräts](#).

Bevor Sie ein Gerät der Snow Family verwenden, um Daten zu übertragen oder Edge-Computing-Aufgaben auszuführen, müssen Sie das Gerät entsperren. Beim Entsperren des Geräts authentifizieren Sie Ihre Fähigkeit, darauf zuzugreifen, indem Sie zwei Arten von Anmeldeinformationen angeben: einen 29-stelligen Entsperrcode und eine Manifestdatei. Nachdem Sie das Gerät entsperrt haben, können Sie das Gerät weiter konfigurieren, Daten zu oder von diesem verschieben, Amazon-ECEC2-compatible einrichten und verwenden und vieles mehr.

Vor dem Entsperren eines Geräts muss das Gerät an Strom und Netzwerk angeschlossen, aktiviert und eine IP-Adresse zugewiesen werden. Siehe [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 [Verwenden des AWS Snowball Edge Clients](#).
- Rufen Sie die Anmeldeinformationen von der ab Managementkonsole für die AWS Snow-Familie. Für ein oder mehrere eigenständige Geräte die Entsperrcodes und die Manifestdatei für jedes Snow Family-Gerät. Weitere Informationen zum Herunterladen von Anmeldeinformationen finden Sie unter [Abrufen von Anmeldeinformationen für den Zugriff auf ein Snow Family-Gerät](#).
- Schalten Sie jedes Gerät ein und verbinden Sie es mit Ihrem Netzwerk. Weitere Informationen finden Sie unter [AWS Snowcone Gerätespezifikationen](#).

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

1. Suchen Sie die IP-Adresse für den Snowcone auf der-Anzeige 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 zeigt an, dass es erfolgreich entsperrt wurde, mit der folgenden Meldung.

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

Wenn der Befehl zurückgibt `connection refused`, finden Sie weitere Informationen unter [Fehlerbehebung beim Entsperren eines Snow Family-Geräts](#).

Example des **unlock-device** Befehls

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

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

Fehlerbehebung beim Entsperren eines Snow Family-Geräts

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

1. Stellen Sie sicher, dass der Befehl korrekt eingegeben wurde.
 - a. Verwenden Sie den Bildschirm Bol auf dem Gerät, um zu überprüfen, ob die im Befehl verwendete IP-Adresse korrekt ist.
 - b. Stellen Sie sicher, dass der Pfad zur im Befehl verwendeten Manifestdatei korrekt ist, einschließlich des Dateinamens.
 - c. Verwenden Sie die [Managementkonsole für die AWS Snow-Familie](#), um zu überprüfen, ob der im Befehl verwendete Entsperrcode korrekt ist.
2. Stellen Sie sicher, dass sich der Computer, den Sie verwenden, im selben Netzwerk und Subnetz wie das Snow-Gerät befindet.
3. Stellen Sie sicher, dass der Computer, den Sie verwenden, und das Netzwerk so konfiguriert sind, dass der Zugriff auf das Snow-Gerät erlaubt wird. Verwenden Sie den `ping` Befehl für Ihr Betriebssystem, um festzustellen, ob der Computer das Snow-Gerät über das Netzwerk erreichen kann. Überprüfen Sie die Konfigurationen von Antivirensoftware, Firewall-Konfiguration, Virtual Private Network (VPN) oder anderen Konfigurationen Ihres Computers und Netzwerks.

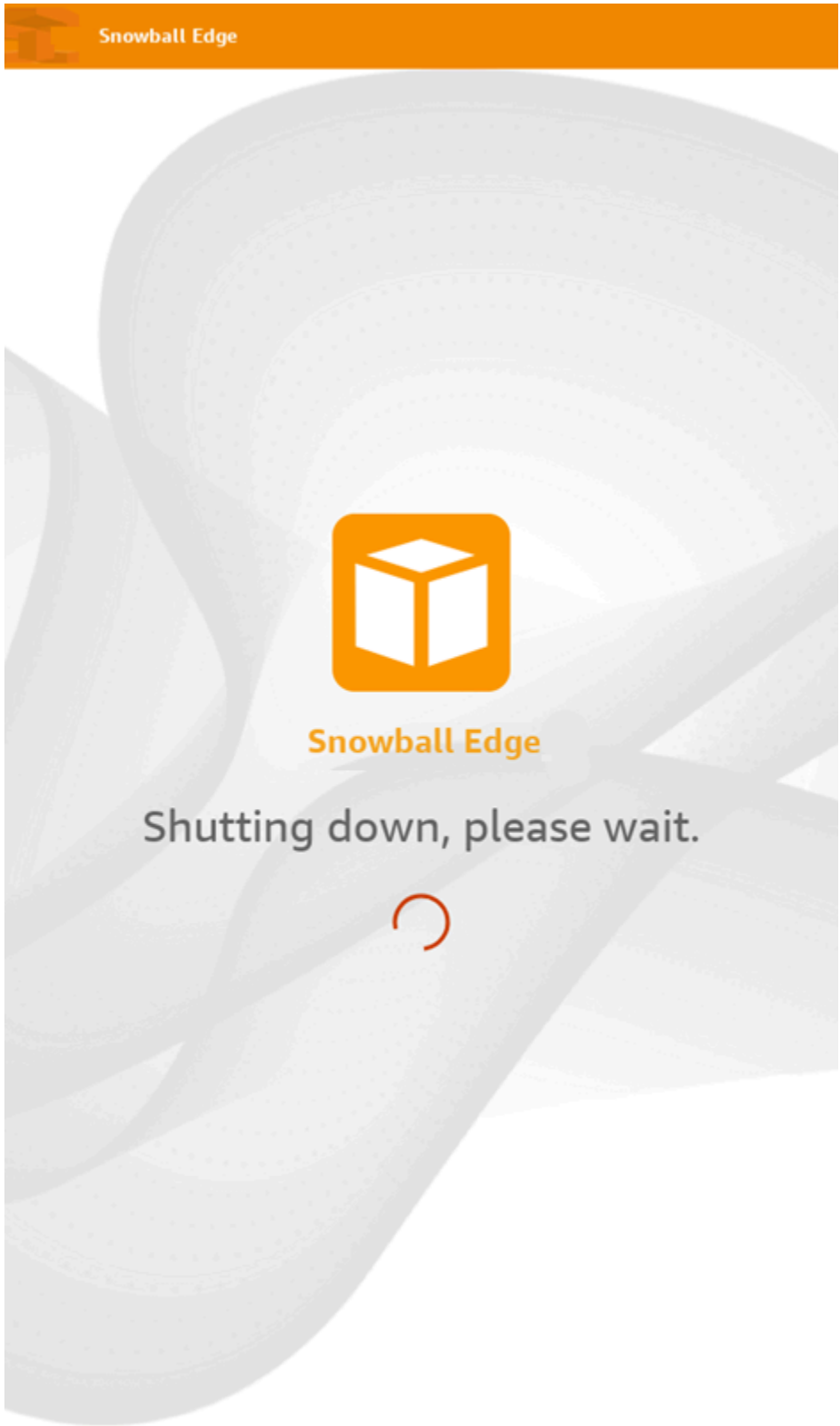
Jetzt können Sie das Snow Family-Gerät verwenden.


Neustarten des Snow Family-Geräts

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 [Anhalten der NFS-Schnittstelle](#).

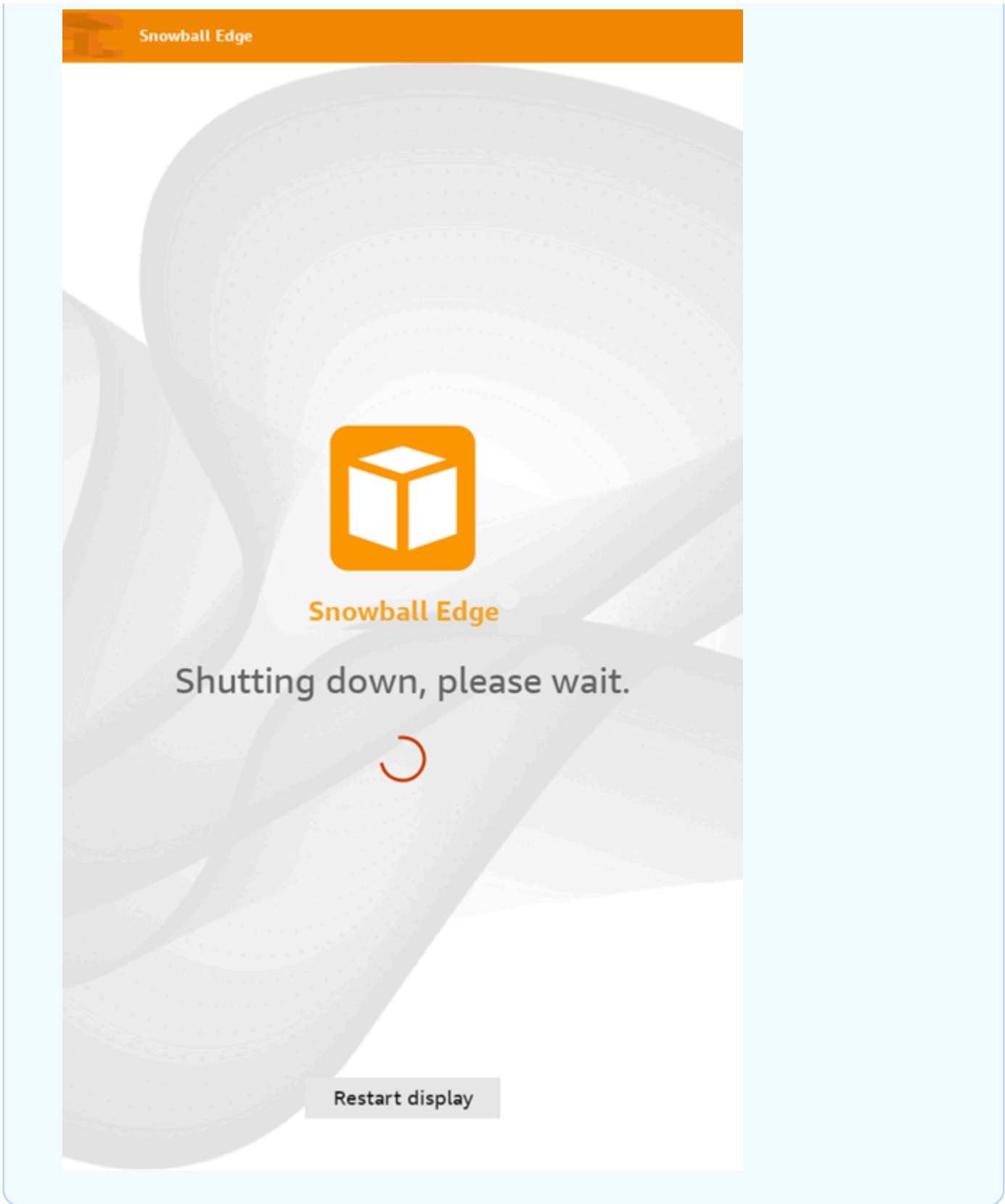
So starten Sie das Gerät mit der Einschalttaste neu:

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



 **Note**

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



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

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

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

```
snowballEdge reboot-device
```

2. Entsperren Sie das Gerät. Siehe [Entsperren eines - AWS Snowcone Geräts](#).

Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten

Die Snow Family-Geräte bieten jetzt ein benutzerfreundliches Tool AWS OpsHub for Snow Family, mit dem Sie Ihre Geräte und lokalen AWS Services verwalten können. Sie verwenden AWS OpsHub auf einem Client-Computer, um Aufgaben wie das Entsperren und Konfigurieren einzelner oder geclusterter Geräte, das Übertragen von Dateien und das Starten und Verwalten von Instances auszuführen, die auf Snow Family-Geräten ausgeführt werden. Sie können verwenden AWS OpsHub, um sowohl die Gerätetypen Storage Optimized als auch Compute Optimized Snow zu verwalten. Die AWS OpsHub Anwendung ist ohne zusätzliche Kosten für Sie verfügbar.

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

AWS OpsHub bietet eine einheitliche Ansicht der AWS Services, die auf Snow Family-Geräten ausgeführt werden, und automatisiert Betriebsaufgaben über AWS Systems Manager. Mit können AWS OpsHub Benutzer mit unterschiedlichem technischem Fachwissen eine große Anzahl von Snow Family-Geräten verwalten. Mit wenigen Klicks können Sie Geräte entsperren, Dateien übertragen, AmazonEC2-compatible 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 es lokal verwalten und unterstützte - AWS Services verwenden. AWS OpsHub bietet ein Dashboard, das wichtige Metriken wie Speicherkapazität und aktive Instances auf Ihrem Gerät zusammenfasst. Es bietet auch eine Auswahl von AWS Services, die auf den Snow Family-Geräten unterstützt werden. Innerhalb weniger Minuten können Sie mit der Übertragung von Dateien zum Gerät beginnen.

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 herstellen, unabhängig davon, ob das Gerät über WLAN oder ein physisches Kabel verbunden ist. Dann öffnen AWS OpsHub und entsperren Sie das Gerät. Anschließend wird Ihnen ein Dashboard angezeigt, das Ihr Gerät und seine Systemmetriken anzeigt. 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](#)
- [Entsperrern eines Geräts](#)
- [Überprüfen der PGP-Signatur von AWS OpsHub \(optional\)](#)
- [Verwalten von AWS Services auf Ihrem Gerät](#)
- [Verwenden von DataSync zum Übertragen von Dateien in AWS](#)
- [Verwaltung Ihrer Geräte](#)
- [Festlegen der NTP-Zeitserver für Ihr Gerät](#)

AWS OpsHub Für Snow Family-Geräte herunterladen

So laden Sie herunter AWS OpsHub

1. Navigieren Sie zur [AWS Website für Snowball-Ressourcen](#) .

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](#)

Windows 7 or higher

OpsHub

[Download](#)

Mac OS X 10.10 or higher

[Download](#)

Linux (Ubuntu version 14 or higher, and Fedora version 24 or higher)

[Download](#)

[\(Signature\)](#)

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

Entsperren eines Geräts

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

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

Informationen zum Aktivieren der Remote-Verwaltung und zum Erstellen eines zugehörigen Kontos finden Sie unter [Aktivieren der Snow Device Management](#).

Themen

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

Lokales Entsperren eines Geräts

So stellen Sie eine lokale Verbindung her und entsperren Ihr Gerät

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



Get started with OpsHub

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

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

Sign in

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

Note

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

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

Entsperren eines Geräts aus der Ferne

So entsperren Sie ein Snow Family-Gerät nicht

So verbinden und entsperren Sie Ihr Gerät remote

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

Note

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

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



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 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

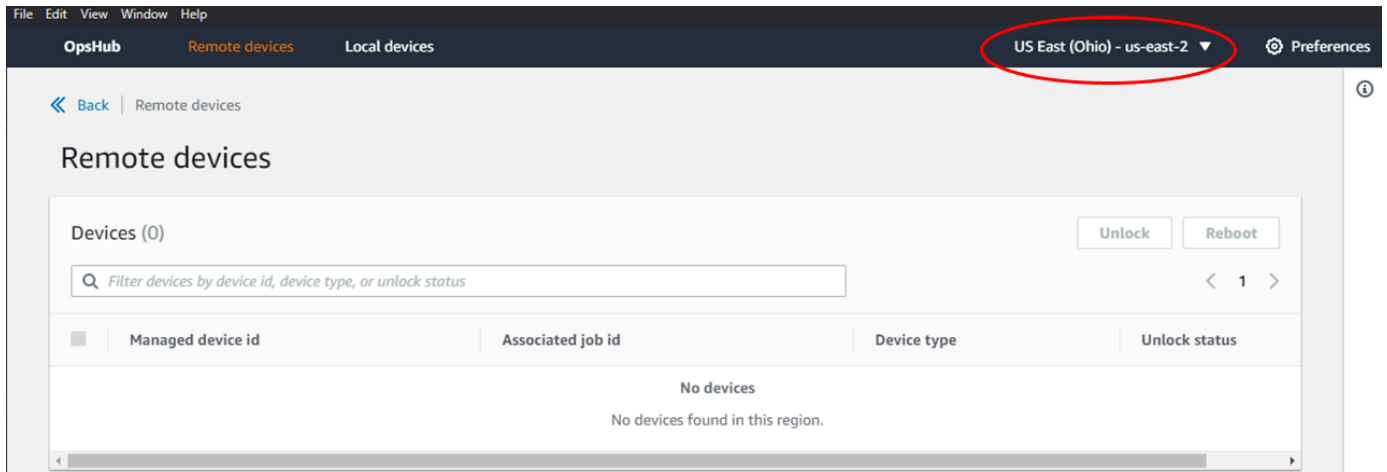
Access key

Secret key

Back

Sign in

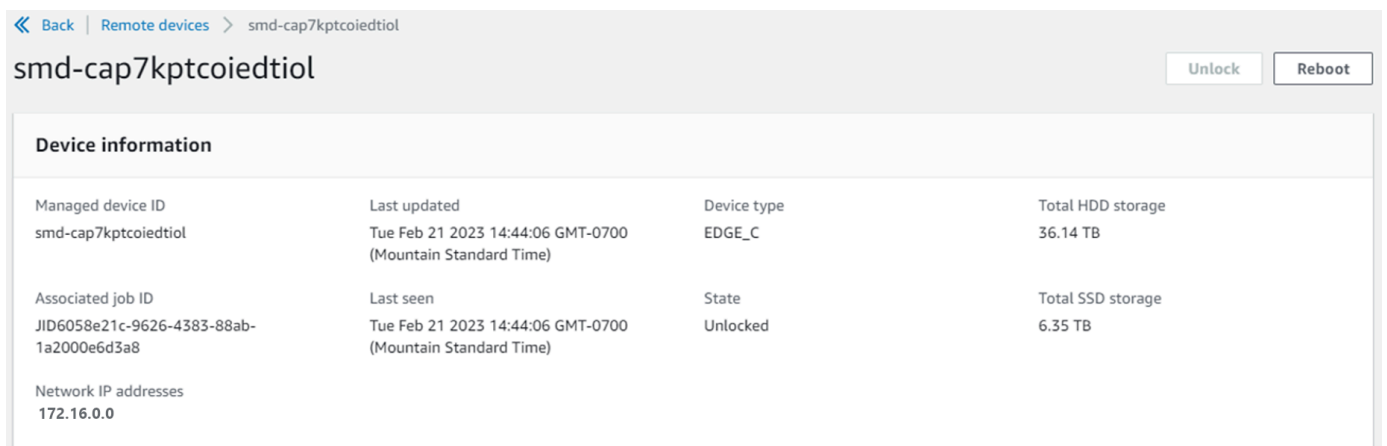
6. Wählen Sie oben auf der Registerkarte Remote-Geräte die Region des Snow-Geräts aus, das remote entsperrt werden soll.



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

Note

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



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

Überprüfen der PGP-Signatur von AWS OpsHub (optional)

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

Sie können die SIGNATURE-Datei für das Linux-Betriebssysteminstallationsprogramm unter [AWS Snowcone Ressourcen](#) oder [Snowball-Edge-Ressourcen](#) herunterladen.

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

1. Kopieren Sie den folgenden öffentlichen Schlüssel, speichern Sie ihn in einer Datei und benennen Sie die Datei. Beispiel: `opshub-public-key.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
4lw2w1B1007Fo02v/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
lsS8JU5rindEsKURkTwcG2wyZFoe1z1E8xPkLRSRN5ZbbgKsTz1611HgCCId
Do+WJdDkWGwmtDvzjm32EI/PVBd108ga9aPwXdhLwOdKAjZ4JrJXLUQJjRI
IVDSyM0bEH0UM6a/+mWNZazNfo0LsGWqGva6Xn5WJWlwr1S78vPNf03BQYu0
YRjaVQR+kPtB9aSAZNi5swfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7X103o/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/LS0X4Ar112KxBjzNESQkwGSiWSYtMA5J+Tj5ED0uZ/qe
omNb1A1D4bm7Na8NAoLxctAiDq/f3To9Xb181Hsnd0mfLCb/BVgP4edQKTii
C/OZHy9QJlfnM0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXM0d3I
e6NUvU7pw0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQqYZe0
jXD3IJ7T+X2XA8M/BmypoMw0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcPxzehwsSVq11zaL2ureJBL0KkBgYxUJYXpbS01ax1TsFG
09ldAN0s9Ej8CND37GsNnuygj0gWXB6MNgbvPs3H3zi/AbMunQ1VB1w07JX
zdm1hBQZh6w+NeiEsK1T6wHi7IhxABEBAAHcWXYEGAEIAAkFA1/hGf8CGwwA
IQkQIYHPWntZrFEWIIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PvBF
ywKvwi3GL01pY7BXn81QaHyunMGUavm080faRR0ynkH0ZqLHCp6bIajF0fvF
b7c0Jamzx8Hg+SIId16yRpRY+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+X1p1g9IduDYPoI20X1eHyyMqGEEIb4g0iis1oTp5oi3EuAYRGf1XuqAT
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 Stellen Sie sicher, dass Sie durch *key-value* den Wert aus dem vorherigen Schritt ersetzen. Wir empfehlen, GPG zur Überprüfung des Fingerabdrucks zu verwenden.

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

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

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

Der Fingerabdruck sollte wie folgt aussehen:

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

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

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

GPG

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

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

GPG

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

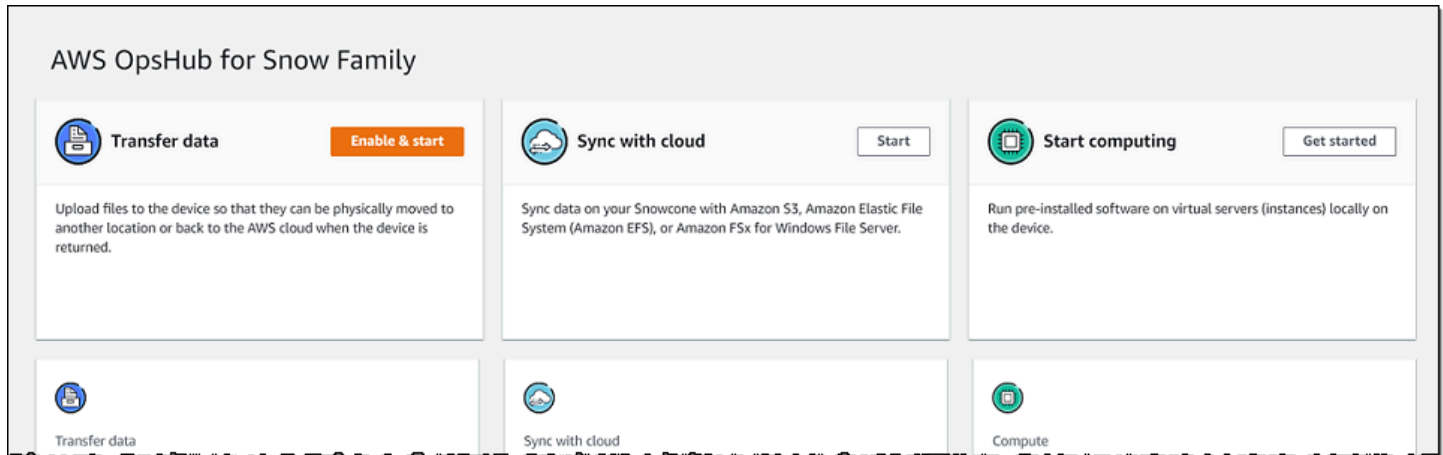
Wenn die Ausgabe bei Verwendung von GPG den Satz enthält, überprüfen SieBAD `signature`, ob Sie das Verfahren korrekt ausgeführt haben. Wenn Sie diese Antwort weiterhin erhalten, wenden Sie sich an AWS Support und installieren Sie den Kundendienstmitarbeiter nicht. Die Warnmeldung über die Vertrauensstellung bedeutet nicht, dass die Signatur nicht gültig ist, sondern nur, dass Sie den öffentlichen Schlüssel nicht verifiziert haben. Beachten Sie die Warnung zu vertrauenswürdigen Inhalten.

Verwalten von AWS Services auf Ihrem Gerät

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

- Amazon Elastic Compute Cloud (Amazon EC2)-Instances – Verwenden Sie Amazon EC2-compatible Instances, um Software auszuführen, die auf einem virtuellen Server installiert ist, ohne sie zur Verarbeitung an den AWS Cloud zu senden.
- AWS DataSync– Übertragen Sie eine große Anzahl von Dateien zwischen Ihrem On-Premises-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 an senden AWS , um Ihre Daten an die zu übertragen AWS Cloud, oder verwenden, DataSync um an andere - AWS Cloud Standorte zu übertragen.



Themen

- [Lokales Verwenden von Amazon EC2-compatible Rechen-Instances](#)
- [Verwalten der NFS-Schnittstelle](#)

Lokales Verwenden von Amazon EC2-compatible Rechen-Instances

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

Themen

- [Starten einer Amazon EC2-compatible Instance](#)
- [Anhalten einer Amazon EC2-compatible Instance](#)
- [Starten einer Amazon EC2-compatible Instance](#)
- [Arbeiten mit Schlüsselpaaren](#)
- [Beenden einer Amazon EC2-compatible Instance](#)
- [Lokale Verwendung von Speicher-Volumes](#)

Starten einer Amazon EC2-compatible Instance

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

So starten Sie eine Amazon EC2-compatible Instance

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen. Alle Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.
3. Wenn auf Ihrem Gerät Amazon EC2-compatible Instances ausgeführt werden, werden diese in der Spalte Instance-Name unter Instances angezeigt. Sie können auf dieser Seite Details zu den einzelnen Instances anzeigen.
4. Wählen Sie Launch Instance (Instance starten) aus. Der Launch Instance Wizard wird geöffnet.
5. Wählen Sie für Gerät das Snow-Gerät aus, das Sie die AmazonEC2-compatible starten möchten.

Launch instance ✕

Device

192.0.2.0 ▼

Image (AMI)

snow-al2-test-ami-1.0.2 ▼

Instance type

sbe-c.small ▼

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

Physical network interface

SFP+:a.bc-1d2ef456gg678gi9j ▼

IP Address assignment

DHCP ▼

Key pair

Create key pair Use existing key pair Do not attach key pair

Name

test-instance-key-pair

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

Create key pair

Cancel **Launch**

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

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

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

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

Weitere Informationen finden Sie unter [Arbeiten mit Schlüsselpaaren](#).

10. Wählen Sie Launch (Starten) aus. Die Instance sollte im Abschnitt Compute instances (Datenverarbeitungs-Instances) gestartet werden. Der State (Status) ist Pending (Ausstehend) und wird nach Abschluss in Running (Wird ausgeführt) geändert.

Anhalten einer Amazon EC2-compatible Instance

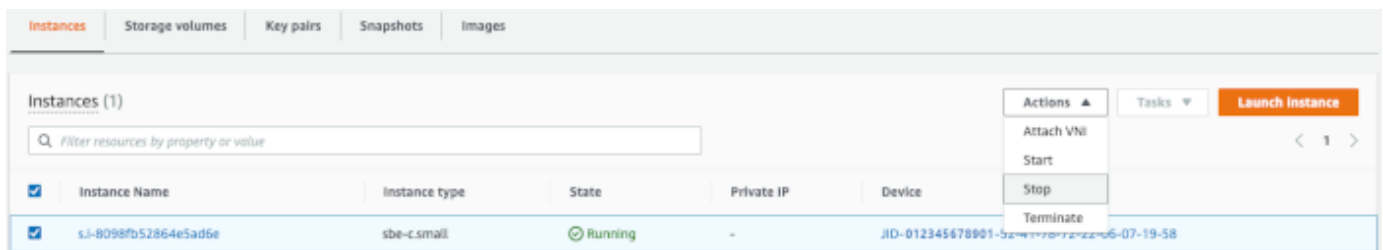
Führen Sie die folgenden Schritte aus, um eine Amazon EC2-compatible Instance AWS OpsHub mit anzuhalten.

So halten Sie eine Amazon EC2-compatible Instance an

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen.

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

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



Starten einer Amazon EC2-compatible Instance

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

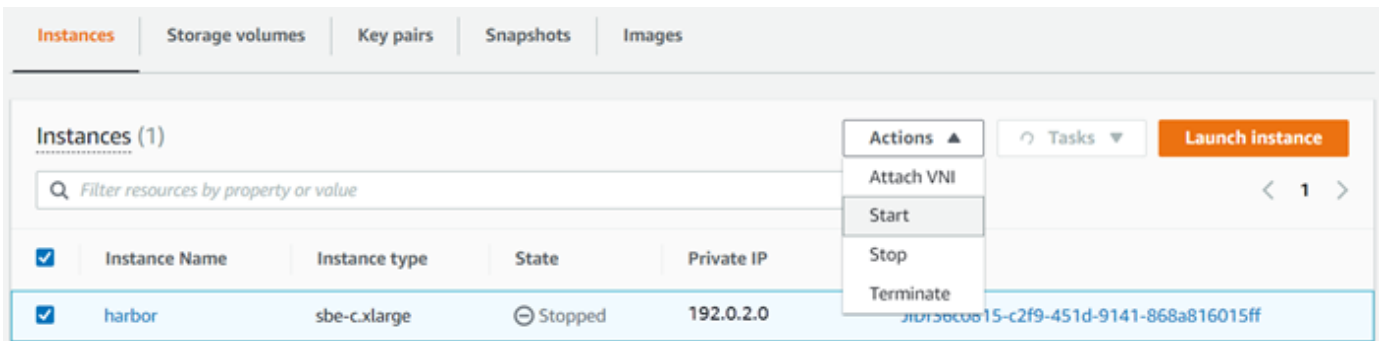
So starten Sie eine Amazon EC2-compatible Instance

1. Öffnen Sie die AWS OpsHub Anwendung.
2. Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und anschließend Compute (EC2) (Datenverarbeitung (EC2)) auswählen, um die Seite Computing (Computing) zu öffnen.

Ihre Datenverarbeitungsressourcen werden im Abschnitt Resources (Ressourcen) angezeigt.

3. Suchen Sie in der Spalte Instance name (Instance-Name) unter Instances (Instanzen) die Instance, die Sie starten möchten.

- Wählen Sie die Instance und anschließend Start (Starten) aus. Der State (Status) wird in Pending (Ausstehend) und anschließend nach Abschluss in Running (Wird ausgeführt) geändert.



Arbeiten mit Schlüsselpaaren

Wenn Sie eine AmazonEC2-compatible Instance starten und eine Verbindung mit ihr über SSH herstellen möchten, müssen Sie ein Schlüsselpaar angeben. Sie können Amazon EC2 verwenden, um ein neues Schlüsselpaar zu erstellen, oder Sie können ein vorhandenes Schlüsselpaar importieren oder Ihre Schlüsselpaare verwalten.

So erstellen, importieren oder verwalten Sie Schlüsselpaare

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

Beenden einer Amazon EC2-compatible Instance

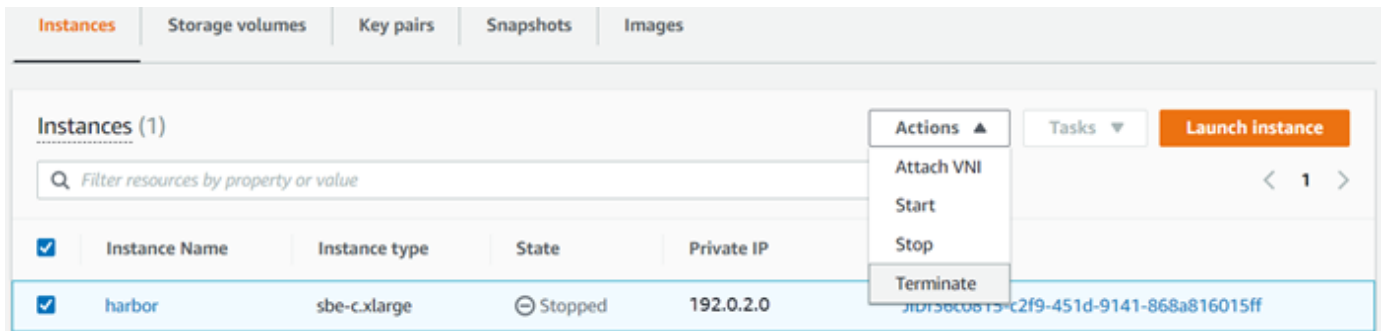
Nachdem Sie eine Amazon EC2-compatible Instance beendet haben, können Sie die Instance nicht neu starten.

So beenden Sie eine Amazon EC2-compatible Instance

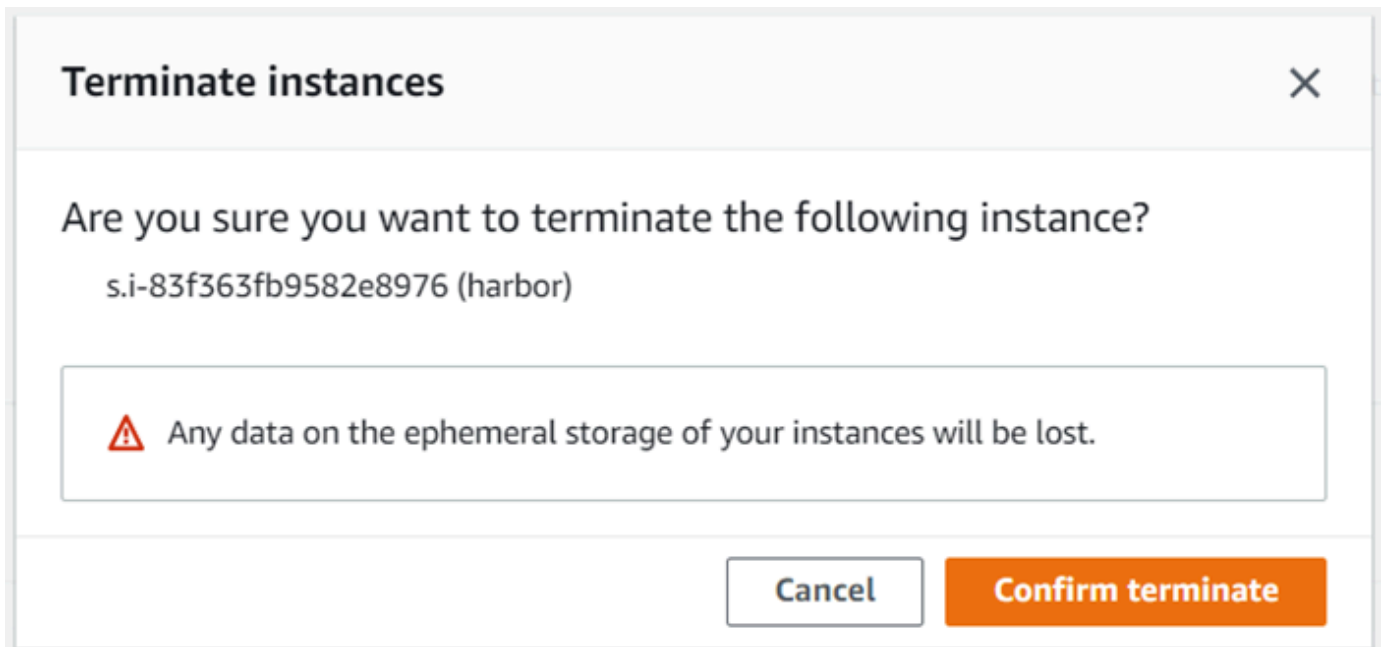
- Öffnen Sie die AWS OpsHub Anwendung.
- Wählen Sie im Abschnitt Start computing (Computing starten) des Dashboards die Option Get started (Erste Schritte) aus. Sie können auch oben das Menü Services (Services) und

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 Instance und dann das Menü Aktionen aus. Wählen Sie im Menü Aktionen die Option Beenden aus.



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



Note

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

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

Lokale Verwendung von Speicher-Volumes

Amazon EC2-compatible Instances verwenden Amazon EBS-Volumes für die Speicherung. In diesem Verfahren erstellen Sie ein Speicher-Volume und fügen es mit an Ihre Instance an AWS OpsHub.

So erstellen Sie ein Speichervolume

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

<< 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)

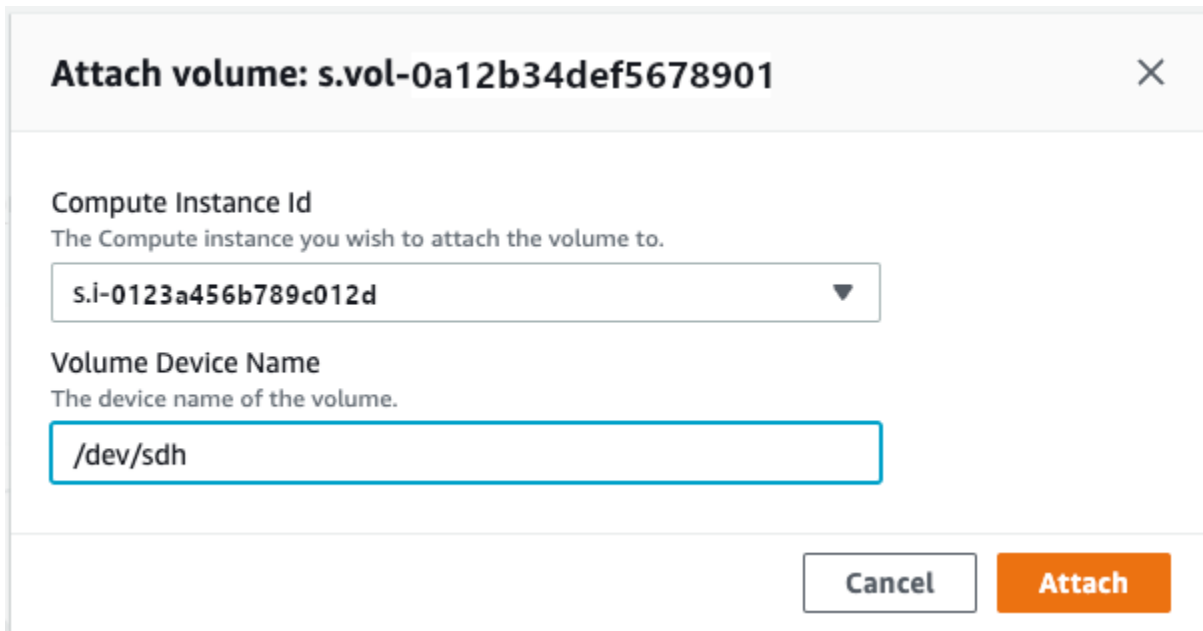
Cancel Submit

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 Volume-Typ 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-Gerätenamen) 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.

Verwalten der NFS-Schnittstelle

Verwenden Sie die Network File System (NFS)-Schnittstelle, um Dateien auf das Snow Family-Gerät hochzuladen, als wäre das Gerät lokaler Speicher auf Ihrem Betriebssystem. Dies ermöglicht einen benutzerfreundlicheren Ansatz für die Übertragung von Daten, da Sie Funktionen Ihres

Betriebssystemen verwenden können, z. B. das Kopieren von Dateien, das Ziehen und Ablegen von Dateien oder andere Funktionen der grafischen Benutzeroberfläche. Jeder S3-Bucket auf dem Gerät ist als NFS-Schnittstellenendpunkt verfügbar und kann zum Kopieren von Daten gemountet werden. Die NFS-Schnittstelle ist für Importaufträge verfügbar.

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

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

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

Note

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

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

Themen

- [Starten des NFS-Service auf einem Windows-Betriebssystem](#)
- [Automatisches Konfigurieren der NFS-Schnittstelle](#)
- [Manuelles Konfigurieren der NFS-Schnittstelle](#)
- [Verwalten von NFS-Endpunkten auf dem Snow Family-Gerät](#)
- [Mounten von NFS-Endpunkten auf Client-Computern](#)
- [Anhalten der NFS-Schnittstelle](#)

Starten des NFS-Service auf einem Windows-Betriebssystem

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

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

Note

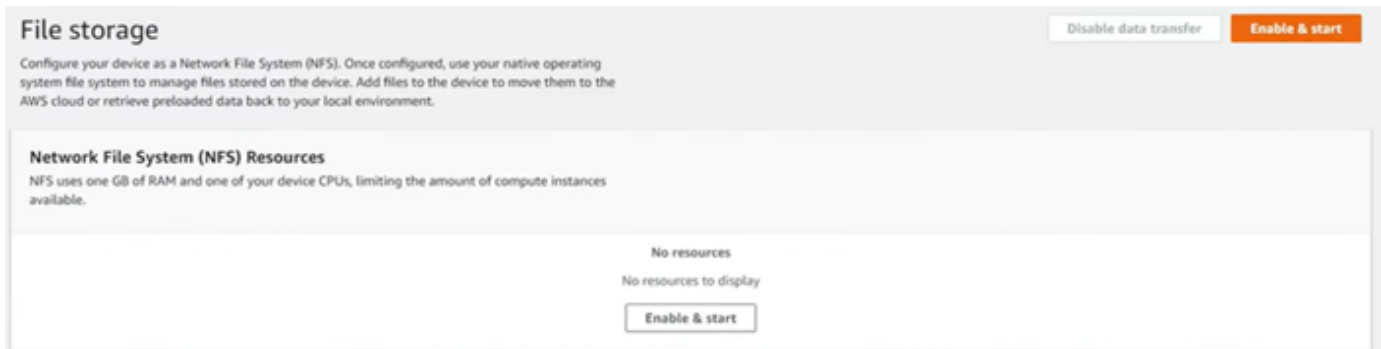
Um Windows-Funktionen einzuschalten, müssen Sie möglicherweise einen Administratorbenutzernamen und ein Passwort für Ihren Computer angeben.

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

Automatisches Konfigurieren der NFS-Schnittstelle

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

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



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

Note

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

Manuelles Konfigurieren der NFS-Schnittstelle

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

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

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

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

Start NFS ✕

Physical network interface

RJ45: s.ni-8459d6c7273eed333 ▼

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

IP Address assignment

DHCP ▼

Restrict NFS to allowed hosts Allow all hosts

Allowed hosts

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

192.0.2.0/24 ✕

0.0.0.0/0 ✕

Add allowed hosts

Allow instances on this device to access NFS

Enable

Cancel Start NFS

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


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

 **Important**

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

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

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

 **Note**

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

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

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

 **Important**

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

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

Verwalten von NFS-Endpunkten auf dem Snow Family-Gerät

Jeder S3-Bucket auf dem Snow Family-Gerät wird als Endpunkt dargestellt und unter Mount-Pfade aufgeführt. Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie einen Endpunkt, um Dateien zu oder von diesem Endpunkt zu übertragen. Es kann jeweils nur ein Endpunkt gemountet werden. Um einen anderen Endpunkt zu mounten, heben Sie zuerst das Mounting des aktuellen Endpunkts auf.

So mounten Sie einen Endpunkt

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

So heben Sie das Mounting eines Endpunkts auf

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

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

 Note

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

Mounten von NFS-Endpunkten auf Client-Computern

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

- Wählen Sie unter Mount-Pfade das Kopiersymbol des zu mountenden Endpunkts aus. Fügen Sie es beim Mounten des Endpunkts in Ihr Betriebssystem ein.
- Im Folgenden sind die Standard-Mounting-Befehle für Windows-, Linux- und macOS-Betriebssysteme aufgeführt.

- Windows:

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

- Linux:

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

- macOS:

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

Anhalten der NFS-Schnittstelle

Halten Sie die NFS-Schnittstelle auf dem Snow Family-Gerät an, wenn Sie mit der Übertragung von Dateien zu oder von diesem fertig sind.

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

Verwenden von DataSync zum Übertragen von Dateien in AWS

Sie können verwenden AWS OpsHub , um einen AWS DataSync Agenten auf Ihrem Snowcone-Gerät zu 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 übertragen AWS Cloud.

AWS DataSync ist ein Online-Datenübertragungsservice, der das Kopieren großer Datenmengen in und aus - AWS Speicherservices vereinfacht, automatisiert und beschleunigt. DataSync kopiert Daten über das Internet oder AWS Direct Connect. Als vollständig verwalteter Service DataSync entfällt 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 für Windows File Server.

Informationen zur Kombination aus Quell- und Zielspeicherort, die von unterstützt wird AWS DataSync, finden Sie unter [Arbeiten mit Standorten](#) 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 On-Premises-Speichersystem verwendet wird. Um zu verwenden DataSync, starten Sie zuerst den Agenten und wechseln dann zur DataSync Konsole und aktivieren sie. Weitere Informationen zu finden Sie DataSyncunter [Erste Schritte mit AWS DataSync](#).

So starten Sie den DataSync Agenten

1. Bevor Sie den DataSync Agenten starten, aktivieren Sie NFS auf Ihrem Snowcone-Gerät. Siehe [Automatisches Konfigurieren der NFS-Schnittstelle](#) und [Starten von NFS und Einschränken des Zugriffs](#).

2. Wählen Sie im AWS OpsHub Dashboard im Abschnitt Mit Cloud synchronisieren die Option Start enaus, um den Assistenten zum Starten von DataSync Kundendienstmitarbeitern zu öffnen. Das Formular Start DataSync DataSync agent (DataSync-Agent starten) wird mit den Feldern Device IP address (Geräte-IP-Adresse) und Physical network interface (Physische Netzwerkschnittstelle) ausgefüllt.
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 IP-Adresse erstellen (VNI) auswählen, wählen Sie DHCP oder Statische 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 Seite DataSync resource (Ressource) 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 Agenten-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.


Übertragen von Dateien mit DataSync

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

So aktivieren Sie den DataSync Agenten und verwenden den DataSync Service

1. Öffnen Sie die - AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Fügen Sie im Abschnitt Aktivierung auf der Seite Kundendienstmitarbeiter erstellen die kopierte IP-Adresse in das Feld Kundendienstmitarbeiteradresse ein und wählen Sie Schlüssel abrufen 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 NFS, das auf Ihrem Snowcone-Gerät ausgeführt wird, als Quellspeicherort für DataSync. Anweisungen finden Sie unter [Konfigurieren eines Quellspeicherorts](#) im AWS DataSync -Benutzerhandbuch.

 Note

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

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

Verwaltung Ihrer Geräte

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

Themen

- [Neustarten Ihres Geräts](#)
- [Herunterfahren Ihres Geräts](#)
- [Bearbeitung des Gerätealias](#)
- [Abrufen von Updates für Ihr Gerät und die AWS OpsHub Anwendung](#)
- [Verwalten von Profilen](#)

Neustarten Ihres Geräts

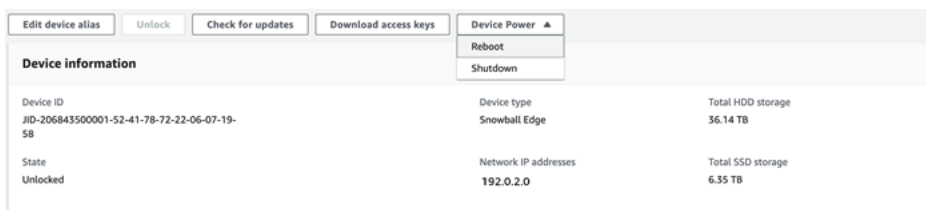
Gehen Sie wie folgt vor, um Ihr Snow-Gerät mit neu AWS OpsHub zu starten.

Important

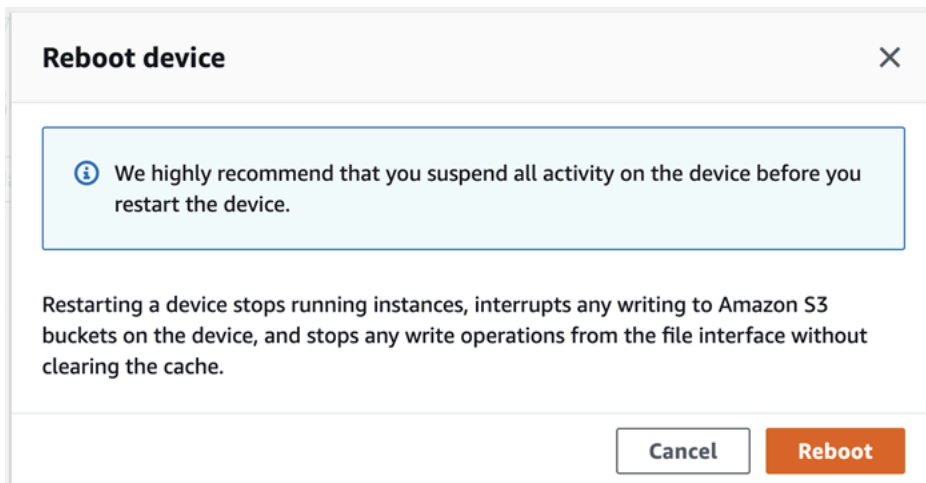
Es wird nachdrücklich empfohlen, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät neu starten. Beim Neustart eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen.

So starten Sie ein Gerät neu

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



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



Herunterfahren Ihres Geräts

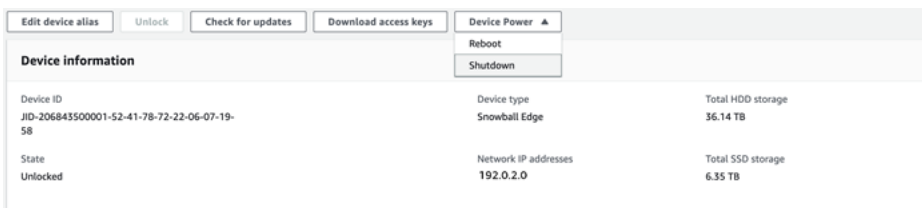
Gehen Sie wie folgt vor, AWS OpsHub um Ihr Snow-Gerät mit herunterzufahren.

⚠ Important

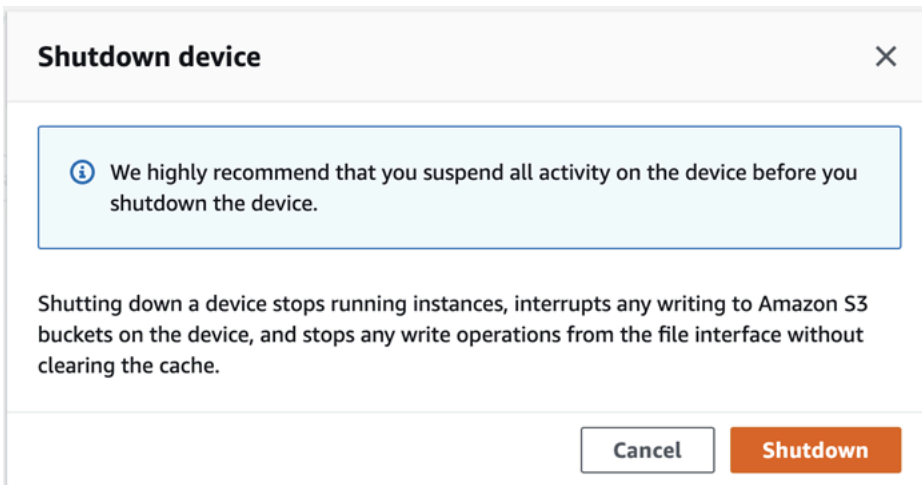
Es wird dringend empfohlen, alle Aktivitäten auf dem Gerät auszusetzen, bevor Sie das Gerät herunterfahren. Beim Herunterfahren eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen.

So fahren Sie ein Gerät herunter

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



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

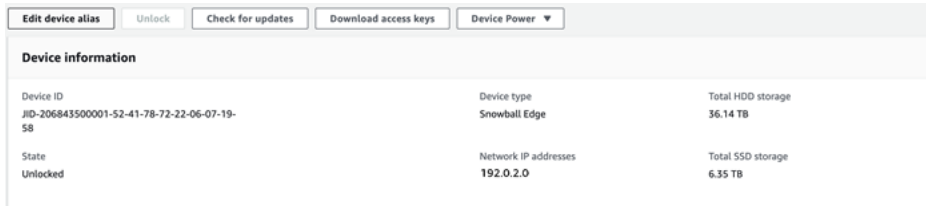


Bearbeitung des Gerätealias

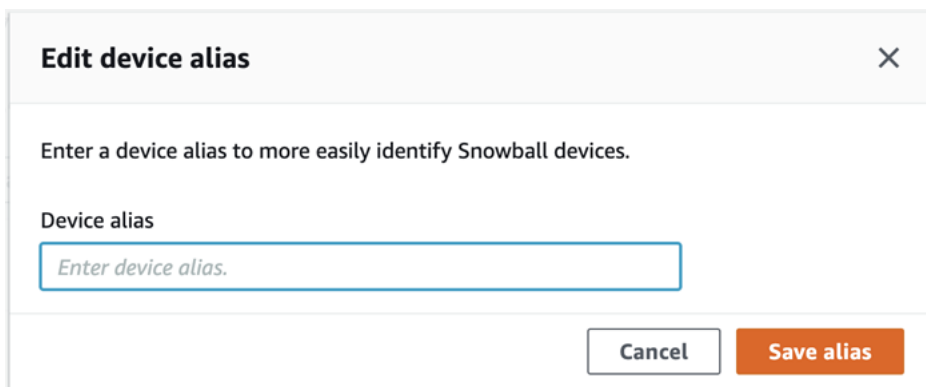
Gehen Sie wie folgt vor, um Ihren Gerätealias mit zu bearbeiten AWS OpsHub.

So bearbeiten Sie den Alias Ihres Geräts

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



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



Abrufen von Updates für Ihr Gerät und die AWS OpsHub Anwendung

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

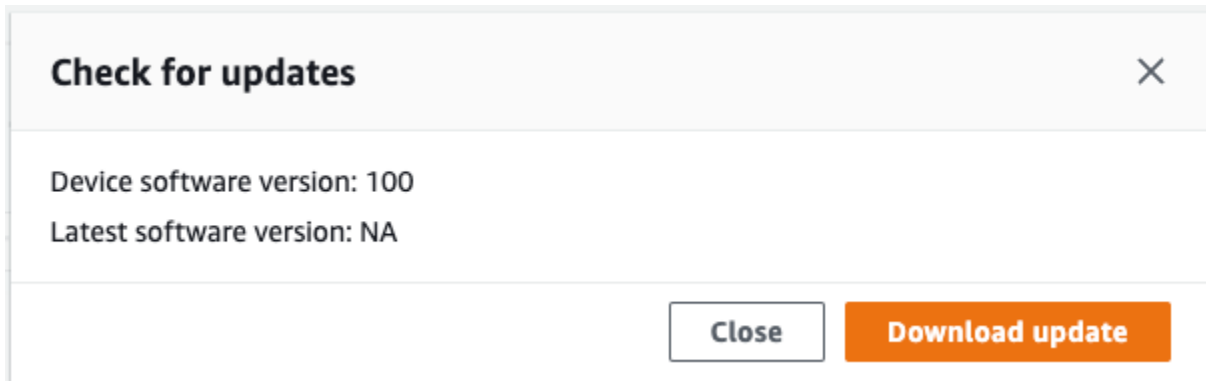
Aktualisieren Ihres Geräts

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

So aktualisieren Sie Ihr Gerät

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

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



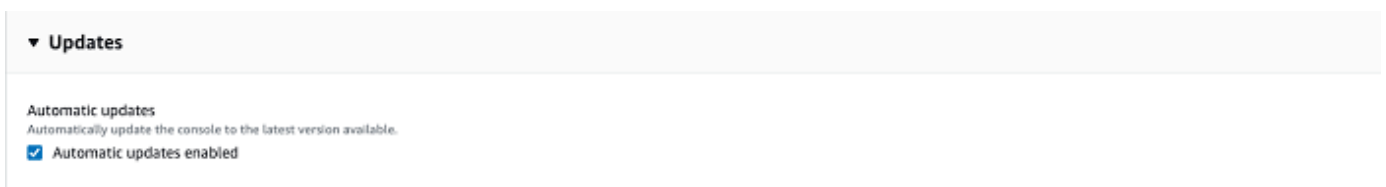
3. Wenn ein Update vorliegt, wählen Sie Update herunterladen aus. Wählen Sie andernfalls Close aus.

Aktualisieren Ihrer AWS OpsHub Anwendung

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

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

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



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

Verwalten von Profilen

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

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

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

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

Dieses Beispiel zeigt eine Profildatei mit drei Profilen – SnowDevice1profileSnowDevice2profile, und SnowDevice3profile.

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

```
  },
  "SnowDevice3profile":
  {
    "name":"SnowDevice3profile",
    "jobId":"JID12345678-c384-4a5e-becd-ab5f38888463",
    "unlockCode":"64c89-13524-4d054-13d93-c1b80",
    "manifestPath":"C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-
c384-4a5e-becd-ab5f38888463_manifest-1670623999136.bin",
    "defaultEndpoint":"https://10.16.0.3",
    "isCluster":false,
    "deviceIps":[]
  }
}
```

So erstellen Sie ein Profil

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

So bearbeiten Sie ein Profil

1. Öffnen Sie in einem Texteditor `snowball-edge.config` von `home directory\\.aws\\snowball\\config`.
2. Bearbeiten Sie die Datei nach Bedarf. Um beispielsweise die IP-Adresse eines Geräts im Profil zu ändern, ändern Sie den `defaultEndpoint` Eintrag .
3. Speichern und schließen Sie die Datei.

So löschen Sie ein Profil

1. Öffnen Sie mit einem Texteditor `snowball-edge.config` von `home directory\\.aws\\snowball\\config`.
2. Löschen Sie die Zeile, die den Profilnamen, die geschweiften Klammern `{}`, die dem Profilnamen folgen, und den Inhalt innerhalb dieser Klammern enthält.
3. Speichern und schließen Sie die Datei.

Festlegen der NTP-Zeitserver für Ihr Gerät

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

So überprüfen Sie Zeitquellen

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

Die Tabelle „Zeitquellen“ hat vier Spalten:

- **Adresse** : Der DNS-Name/die IP-Adresse der Zeitquelle
- **Status** : Der aktuelle Verbindungsstatus zwischen dem Gerät und dieser Zeitquelle, es gibt 5 mögliche Status:
 - **AKTUELL**: Die Zeitquelle wird derzeit zum Synchronisieren der Zeit verwendet
 - **COMBINED** : Die Zeitquelle wird mit der aktuellen Quelle kombiniert
 - **AUSGESCHLAGEN**: Die Zeitquelle wird durch den Kombinationsalgorithmus ausgeschlossen
 - **LOST**: Die Verbindung mit der Zeitquelle wurde unterbrochen
 - **NICHT VERFÜGBARKEIT**: Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder als falscher angesehen hat oder zu viel Variabilität aufweist
- **Typ** : Network Time Protocol (NTP)-Quellen können ein Server oder ein Peer sein. Ein Server kann vom Benutzer mit dem update-time-server Befehl eingerichtet werden, während ein Peer nur mit anderen Snowball Edge-Geräten im Cluster eingerichtet werden kann und automatisch eingerichtet wird, wenn der Cluster zugeordnet ist.
- **Bolum** : Die Stratum der Quelle. Bolum 1 gibt eine Quelle mit einer lokal angefügten Referenzuhr an. Eine Quelle, die mit einer Stratum-1-Quelle synchronisiert ist, wird aufum 2 festgelegt. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert wird, wird aufum 3 usw. festgelegt.

So aktualisieren Sie die Zeitserver

1. Suchen Sie im AWS OpsHub Dashboard Ihr Gerät unter Geräte . Wählen Sie das Gerät aus, um die Gerätedetailseite zu öffnen.
2. In der Tabelle „Zeitquellen“ wird eine Liste der Zeitquellen angezeigt, mit denen Ihr Gerät Zeit synchronisiert.
3. Wählen Sie in der Tabelle Zeitquellen die Option Zeitserver aktualisieren aus.
4. Geben Sie den DNS-Namen oder die IP-Adresse der Zeitserver an, mit denen Ihr Gerät die Zeit synchronisieren soll, und wählen Sie Aktualisieren aus.

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.

Verwenden des AWS Snowball Edge Clients

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. Während Sie den Snowball Edge-Client verwenden, können Sie zusätzliche Support-Informationen erhalten, indem Sie den `snowballEdge help` Befehl ausführen.

Wenn Sie Daten auf das AWS Snowcone Gerät lesen und schreiben, verwenden Sie die NFS-Schnittstelle. Sie können die AWS OpsHub for Snow Family Anwendung auch verwenden, um Snow Family-Geräte zu verwalten, einschließlich Snowcone-Geräten. Weitere Informationen finden Sie unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

Herunterladen und Installieren des Snowball Edge Clients

Sie können den Snowball Edge-Client von [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. Das Ausführen des Snowball Edge-Clients von einem Terminal auf Ihrer Workstation erfordert möglicherweise die Verwendung eines bestimmten Pfads, abhängig von Ihrem Betriebssystem:

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

Befehle für den Snowball Edge Client

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

Note

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

Themen

- [Konfigurieren eines Profils für den Snowball Edge Client](#)
- [Anfordern Ihres QR-Codes für die NFC-Validierung](#)
- [Entsperren eines - AWS Snowcone Geräts](#)
- [Aktualisieren eines Snowcone](#)
- [Abrufen von Anmeldeinformationen](#)
- [Starten eines Services auf Ihrem Snowcone-Gerät](#)
- [Stoppen eines Services auf Ihrem Snowcone-Gerät](#)
- [Abrufen des Zertifikats für die Datenübertragung](#)
- [AWS Snowcone Protokolle](#)
- [Abrufen des Gerätestatus](#)
- [Abrufen des Servicestatus](#)
- [Starten des AWS DataSync AMI](#)
- [Starten von NFS und Einschränken des Zugriffs](#)
- [Beschränken des Zugriffs auf NFS-Anteile, wenn NFS ausgeführt wird](#)
- [Abrufen des Exportpfads für einen Amazon S3-Bucket](#)
- [Aktivieren des lokalen AWS Operator-Debuggings](#)
- [Deaktivieren des Debuggings von lokalen AWS Operatoren](#)
- [Erstellen einer direkten Netzwerkschnittstelle](#)
- [Abrufen von Informationen zu einer Direct Network Interface](#)
- [Aktualisieren einer Direct Network Interface](#)
- [Löschen einer Direct Network Interface](#)
- [Überprüfen des Feature-Status](#)
- [Ändern des Feature-Status](#)
- [Einstellen von Zeitservern](#)
- [Überprüfen von Zeitquellen](#)

Konfigurieren eines Profils für den Snowball Edge Client

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

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

Der Endpunkt ist die IP-Adresse, zu der `https://` hinzugefügt wird. Sie können die IP-Adresse für das AWS Snowcone Gerät auf der AWS Snowcone Geräteanzeige suchen. Wenn das AWS Snowcone Gerät zum ersten Mal mit Ihrem Netzwerk verbunden ist, erhält es automatisch eine DHCP-IP-Adresse, sofern ein DHCP-Server verfügbar ist. Wenn Sie eine andere IP-Adresse verwenden möchten, können Sie diese auf dem LCD-Display ändern. Weitere Informationen finden Sie unter [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 Aufträge 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 Verification App zu generieren. Sie können diese App aus dem Apple App Store oder Google Play Store herunterladen. Weitere Informationen zur Bol-Validierung finden Sie unter [Validieren von NFC-Tags](#).

Usage

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

Example Beispielausgabe

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

Entsperren eines - AWS Snowcone Geräts

Um ein eigenständiges AWS Snowcone Gerät zu entsperren, führen Sie den `snowballEdge unlock-device` Befehl aus. 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 Prozess kann mühsam werden, daher empfehlen wir Ihnen, stattdessen Ihren Snowball Edge-Client zu konfigurieren. Wenn Sie den Snowball Edge-Client bereits konfiguriert haben, müssen Sie nur den Befehl selbst eingeben, ohne den Pfad zum Manifest, zum Entsperrcode oder zur IP-Adresse.

Note

Um das Gerät zu entsperren, das Ihrem Auftrag zugeordnet ist, muss das Gerät vor Ort, an die Stromversorgung und das Netzwerk angeschlossen und aktiviert sein. Darüber hinaus

muss die Bol-Anzeige auf der Front des AWS Snowcone Geräts darauf hinweisen, dass das Gerät einsatzbereit ist.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge unlock-device
```

Example

Example Entsperren der Ausgabe

```
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.
```

Aktualisieren eines Snowcone

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

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

Nutzung (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 ausgeführt.
- **Downloading** – Neue Software wird heruntergeladen.
- **Installing** – Neue Software wird installiert.
- **Requires Reboot** – Neue Software wurde installiert und das Gerät muss neu gestartet werden.

Warning

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

Nutzung (konfigurierter Snowball Edge-Client)

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

Example Beispielausgabe

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

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

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge download-updates
```

Example Beispielausgabe

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

`snowballEdge install-updates` – Startet die Installation der neuesten Softwareupdates für Ihr Snowcone-Gerät, die bereits heruntergeladen wurden.

Nutzung (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. Beim Neustart eines Geräts werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät werden unterbrochen. Alle diese Prozesse können zu Datenverlust führen.

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge reboot-device
```

Example Beispielausgabe

```
Rebooting device now.
```

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

Nutzung (konfigurierter Snowball Edge-Client)

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

```
endpoint]
```

Example Beispielausgabe

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

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

Nutzung (konfigurierter Snowball Edge-Client)

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

Example 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 die AWS CLI oder mit einem AWS -SDK verwenden. Diese Anmeldeinformationen sind nur einem einzelnen Auftrag für Snowcone zugeordnet, und Sie können sie nur auf dem Gerät verwenden. Das Gerät verfügt über keine AWS Identity and Access Management (IAM)-Berechtigungen in der AWS Cloud.

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

Note

Wenn Sie die AWS CLI mit Snowball verwenden, müssen Sie diese Anmeldeinformationen beim Konfigurieren der CLI verwenden. Informationen zum Konfigurieren von Anmeldeinformationen für die CLI finden Sie unter [Schnellkonfiguration](#) im AWS Command Line Interface -Benutzerhandbuch.

Nutzung (konfigurierter Snowball-Edge-Client)

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

Example Beispielausgabe

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

Nutzung (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
```

Starten eines Services auf Ihrem Snowcone-Gerät

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

Nutzung (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.
```

Stoppen eines Services auf Ihrem Snowcone-Gerät

Um einen Service zu beenden, der auf Ihrem Snowcone-Gerät ausgeführt wird, können Sie den `snowballEdge stop-service` Befehl verwenden. Die Amazon EC2-Services können nicht angehalten werden.

Warning

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

Nutzung (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 nicht mehr für die Verwendung mit dem Endpunkt gültig. Sie können das neue, aktualisierte Zertifikat erneut vom Snowcone-Gerät mit dem `get-certificate` Befehl abrufen.

Sie können diese Zertifikate auflisten und sie 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.

Nutzung (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.

Nutzung (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 On-Premises-Rechenzentrum und einem Snowcone-Gerät übertragen, werden Protokolle automatisch generiert. Sollten während der Datenübertragung auf das

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

Im Zusammenhang mit Protokollen gibt es drei verschiedene Befehle:

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

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-logs
```

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

Nutzung (konfigurierter Snowball-Edge-Client)

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

Example Beispielausgabe

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

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

Nutzung (konfigurierter Snowball Edge-Client)

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

Example Beispielausgabe

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

Important

CUSTOMER -Protokolle können vertrauliche Informationen zu Ihren eigenen Daten enthalten. Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir dringend, diese Protokolle zu löschen, nachdem Sie damit fertig sind.

Abrufen des Gerätestatus

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

- `describe-device`

Nutzung (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

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

- `list-services`

Nutzung (konfigurierter Snowball Edge-Client)

```
snowballEdge list-services
```

Example 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.

Nutzung (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"
}
} ]
}

```

Starten des AWS DataSync AMI

Starten Sie das AWS DataSync AMI auf Snowcone.

Nutzung (konfigurierter Snowball Edge-Client)

AWS DataSync muss mit dem `Instancesnc1.medium`-Typ gestartet werden. Der Start DataSync mit einem anderen Instance-Typ kann zu einem instabilen Betrieb und potenziellen 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-instances --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 Instance 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"
}

```

Starten von NFS und Einschränken des Zugriffs

Important

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

Note

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

Sie können CIDR-Blöcke für IP-Adressbereiche bereitstellen, die die vom Gerät bereitgestellten NFS-Freigaben mounten dürfen. Beispiel: `10.0.0.0/16` Wenn Sie keine zulässigen CIDR-Blöcke angeben, werden alle Mount-Anforderungen abgelehnt.

Über NFS übertragene Daten werden während der Übertragung nicht verschlüsselt.

Neben den zulässigen Hosts durch CIDR-Blöcke bietet Snowcone keinen Authentifizierungs- oder Autorisierungsmechanismus für die NFS-Freigaben.

Starten Sie NFS mit dem `snowballEdge start-service` Befehl. Um die Service-ID für den NFS-Service abzurufen, können Sie den `snowballEdge list-services` Befehl verwenden.

Bevor Sie diesen Befehl ausführen, erstellen Sie eine einzige virtuelle Netzwerkschnittstelle, die Sie an den Service bindet, den Sie gerade starten. Weitere Informationen finden Sie unter [Erstellen einer virtuellen Netzwerkschnittstelle](#). Sie können den Zugriff auf Ihre Dateifreigaben und Daten in Ihren Amazon S3-Buckets einschränken und sehen, welche Einschränkungen derzeit gelten. Dazu weisen Sie CIDR-Blöcke für zulässige Hosts zu, die auf Ihre Dateifreigabe und S3-Buckets zugreifen können, wenn Sie den NFS-Service starten.

Nutzung (konfigurierter Snowball-Edge-Client)

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

Example Beispielausgabe

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

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

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

Nutzung (konfigurierter Snowball Edge-Client)

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

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

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

Abrufen des Exportpfads für einen Amazon S3-Bucket

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

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

Aktivieren des lokalen AWS Operator-Debuggings

- `enable-local-aws-operator-debugging` – Aktiviert das Gerät für das Debuggen lokaler AWS Operatoren durch Öffnen von SSH-Port 22.

Nutzung (konfigurierter Snowball Edge-Client)

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

Deaktivieren des Debuggings von lokalen AWS Operatoren

- `disable-local-aws-operator-debugging` – Deaktiviert das Gerät für das Debuggen lokaler AWS Operatoren durch Schließen von SSH-Port 22. Standardmäßig ist SSH-Port 22 geschlossen. Wenn das Snowcone-Gerät ausgeschaltet oder mit Strom versorgt wird, ist das Debuggen lokaler AWS Operatoren deaktiviert.

Nutzung (konfigurierter Snowball Edge-Client)

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

Erstellen einer direkten Netzwerkschnittstelle

- `create-direct-network-interface` – [Erstellt eine Direct Network Interface \(DNI\)](#). Erstellt eine direkte Netzwerkschnittstelle zur Verwendung mit Amazon EC2-Computing-Instances auf Ihrem Gerät. Sie finden die auf Ihrem Gerät verfügbaren direkten Netzwerkschnittstellen mithilfe des `describe-direct-network-interfaces` Befehls .

Nutzung (konfigurierter Snowball-Edge-Client)

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

Abrufen von Informationen zu einer Direct Network Interface

- `describe-direct-network-interface` – Ruft die direkten Netzwerkschnittstellen auf Ihrem Gerät ab. Eine direkte Netzwerkschnittstelle kann verwendet werden, um Netzwerke für Amazon EC2-Computing-Instances und -Services auf Ihrem Gerät zu konfigurieren. Sie können eine neue direkte Netzwerkschnittstelle erstellen, indem Sie den `create-direct-network-interface` Befehl verwenden.

Nutzung (konfigurierter Snowball-Edge-Client)

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

Aktualisieren einer Direct Network Interface

- `update-direct-network-interface` – Aktualisiert eine direkte Netzwerkschnittstelle. Verwenden Sie diesen Befehl, um eine direkte Netzwerkschnittstelle zu aktualisieren, die mit Amazon EC2-Computing-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 an eine Amazon EC2-Instance angefügt ist, wird die Schnittstelle zuerst getrennt.

Nutzung (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 Direct Network Interface

- `delete-direct-network-interface` – Löscht eine direkte Netzwerkschnittstelle, die nicht mehr verwendet wird. Um eine direkte Netzwerkschnittstelle zu löschen, die Ihrer Amazon EC2-Computing-Instance zugeordnet ist, müssen Sie zuerst die Zuordnung der direkten Netzwerkschnittstelle zu Ihrer Instance aufheben.

Nutzung (konfigurierter Snowball-Edge-Client)

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

Überprüfen des Feature-Status

Um den Status der auf Ihrem Gerät verfügbaren Funktionen aufzulisten, einschließlich AWS Snow Device Management, mit denen Sie Ihr Snowcone-Gerät und Ihre lokalen AWS Services remote verwalten können, verwenden Sie den `describe-features` Befehl .

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

- `INSTALLED_ONLY` – Die Funktion ist installiert, aber nicht aktiviert.
- `INSTALLED_AUTOSTART` – Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu seinem herzustellen, AWS-Region wenn es eingeschaltet ist.
- `NOT_INSTALLED` – Das Gerät unterstützt das Feature nicht oder war bereits vor dem Start im Feld .

Nutzung (konfigurierter Snowball-Edge-Client)

```
snowballEdge describe-features
--manifest-file manifest.bin path
--unlock-code unlock-code
--endpoint https://device-local-ip:9091
```

Beispielausgabe

```
{
  "RemoteManagementState" : String
}
```

Ändern des Feature-Status

Verwenden Sie den `set-features` Befehl , um den Status der auf Ihrem AWS Snowcone Gerät verfügbaren Funktionen zu ändern. Um zu aktivieren oder zu deaktivieren AWS Snow Device Management, mit dem Sie Ihr Snowcone-Gerät und Ihre lokalen AWS Services remote verwalten können, verwenden Sie den `--remote-management-state` Parameter . Das Gerät muss entsperrt werden, bevor Sie diesen Befehl ausführen.

Sie können Snow Device Management auf die folgenden Status setzen:

- `INSTALLED_ONLY` – Die Funktion ist installiert, aber nicht aktiviert.
- `INSTALLED_AUTOSTART` – Die Funktion ist aktiviert und das Gerät versucht, eine Verbindung zu seinem herzustellen, AWS-Region wenn es eingeschaltet ist.

Note

Der `NOT_INSTALLED` Status ist nur vorhanden, um Geräte zu identifizieren, die Snow Device Management nicht unterstützen oder sich bereits vor dem Start im Feld befanden. Es ist nicht möglich, die Funktion auf bereits bereitgestellten Geräten zu installieren oder zu deinstallieren. Um Snow Device Management verwenden zu können, müssen Sie ein neues Gerät mit vorinstalliertem Feature bestellen.

Nutzung (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"
}
```

Einstellen von Zeitservern

Sie können einen externen Network Time Protocol (NTP)-Server einrichten. Sie können die NTP-CLI-Befehle verwenden, wenn sich das Gerät sowohl im gesperrten als auch im entsperrten Zustand befindet. Der Manifest- und Entsperrcode sind erforderlich. Sie können diese entweder mit dem `snowballEdge configure` Befehl oder mit den `--unlock-code` Optionen `--manifest-file` und festlegen. Beachten Sie, dass Sie die `snowballEdge` CLI sowohl auf AWS Snowcone Edge als auch auf verwenden können AWS Snowcone.

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

Note

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

Usage

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

Example Beispielausgabe

```
Updating time servers now.
```

Überprüfen von Zeitquellen

Verwenden Sie den `describe-time-sources` Snowball Edge CLI-Befehl , um zu sehen, mit welchen NTP-Zeitquellen das Gerät derzeit verbunden ist.

Usage

```
snowballEdge describe-time-sources
```

Example Beispielausgabe

```
{
  "Sources" : [ {
    "Address" : "172.31.2.71",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.3.203",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }
]
```

```
}, {
  "Address" : "172.31.0.178",
  "State" : "LOST",
  "Type" : "PEER",
  "Stratum" : 10
}, {
  "Address" : "172.31.3.178",
  "State" : "LOST",
  "Type" : "PEER",
  "Stratum" : 10
}, {
  "Address" : "216.239.35.12",
  "State" : "CURRENT",
  "Type" : "SERVER",
  "Stratum" : 1
} ]
}
```

Der `describe-time-sources` Befehl gibt eine Liste von Zeitquellenstatus zurück. Jeder Quellstatus enthält die Stratum Felder `Address`, `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 Status:
 - `CURRENT` – Die Zeitquelle wird derzeit zum Synchronisieren der Zeit verwendet.
 - `COMBINED` – Die Zeitquelle wird mit der aktuellen Quelle kombiniert.
 - `EXCLUDED` – Die Zeitquelle wird durch den Kombinationsalgorithmus ausgeschlossen.
 - `LOST` – Die Verbindung mit der Zeitquelle wurde unterbrochen.
 - `UNACCEPTABLE` – Eine ungültige Zeitquelle, bei der der Kombinationsalgorithmus entweder als `false-ticker` angesehen wurde oder zu viel Variabilität aufweist.
- `Type` – Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Server können mit dem `update-time-servers` Befehl festgelegt werden. Peers können nur andere Snowball Edge-Geräte im Cluster sein und werden automatisch eingerichtet, wenn der Cluster zugeordnet ist.
- `Stratum` – Dieses Feld zeigt die Stratum der Quelle an. Bolum 1 gibt eine Quelle mit einer lokal angefügten Referenzuhr an. Eine Quelle, die mit einer Stratum-1-Quelle synchronisiert wird, befindet sich in Stratum 2. Eine Quelle, die mit einer Stratum-2-Quelle synchronisiert wird, befindet sich in Stratum 3 usw.

Eine NTP-Zeitquelle kann entweder ein Server oder ein Peer sein. Ein Server kann vom Benutzer mit dem `update-time-servers` Befehl festgelegt werden, während ein Peer nur andere Snowball Edge-Geräte im Cluster sein könnte. In der Beispielausgabe `describe-time-sources` wird auf einem Snowball Edge aufgerufen, der sich in einem Cluster von 5 befindet. Die Ausgabe enthält 4 Peers und 1 Server. Die Peers haben ein -Stratum von 10, während der Server ein -Stratum von 1 hat. Daher wird der Server als aktuelle Zeitquelle ausgewählt.

Verwendung von AWS Snow Device Management für die Verwaltung von Geräten

AWS Snow Device Management Mit können Sie Ihr Snow-Family-Gerät und Ihre lokalen AWS Services remote verwalten. Alle Snow Family-Geräte unterstützen Snow Device Management und werden auf neuen Geräten in den meisten installiert, in AWS-Regionen denen Snow Family-Geräte verfügbar sind.

Mit Snow Device Management können Sie die folgenden Aufgaben ausführen:

- Erstellen einer Aufgabe
- Überprüfen des Aufgabenstatus
- Überprüfen der Aufgabenmetadaten
- Abbrechen einer Aufgabe
- Überprüfen der Geräteinformationen
- Überprüfen des Amazon EC2-compatible Instance-Status
- Auflisten von Befehlen und Syntax
- Auflisten von remote verwalteten Geräten
- Auflisten des Aufgabenstatus über Geräte hinweg
- Auflisten verfügbarer Ressourcen
- Auflisten von Aufgaben nach Status
- Auflisten von Geräte- oder Aufgaben-Tags
- Anwenden von Tags
- Entfernen von Tags

Themen

- [Auswählen des Snow Device Management-Status beim Bestellen eines Snow Family-Geräts](#)
- [Aktivieren der Snow Device Management](#)
- [Hinzufügen von Berechtigungen für Snow Device Management zu einer IAM-Rolle](#)
- [CLI-Befehle für Snow Device Management](#)

Auswählen des Snow Device Management-Status beim Bestellen eines Snow Family-Geräts

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

So wählen Sie den Status Snow Device Management aus Managementkonsole für die AWS Snow-Familie

1. Um auszuwählen, ob Snow Device Management installiert und aktiviert werden soll, wählen Sie Remote-Verwaltung Ihres Snow-Geräts mit AWS OpsHub oder Snowball-Client aus.
2. Um zu wählen, ob Snow Device Management installiert, aber nicht aktiviert werden soll, wählen Sie Snow-Gerät nicht remote mit AWS OpsHub oder Snowball-Client verwalten aus.

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

So wählen Sie den Status Snow Device Management aus der AWS CLI, dem Snowball Edge-Client oder der Snow-Auftragsverwaltungs-API aus:

- Verwenden Sie den `remote-management` Parameter , um den Status Snow Device Management anzugeben. Der `INSTALLED_ONLY` Wert des Parameters bedeutet, dass Snow Device Management installiert, aber nicht aktiviert ist. Der `INSTALLED_AUTOSTART` Wert des Parameters bedeutet, dass Snow Device Management installiert und aktiviert ist. Wenn Sie keinen Wert für diesen Parameter angeben, `INSTALLED_ONLY` ist der Standardwert.

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

```
aws snowball create-job \
```

```

--job-type IMPORT \
--remote-management INSTALLED_AUTOSTART
--device-configuration '{"SnowconeDeviceConfiguration": {"WirelessConnection":
{"IsWifiEnabled": false} } }' \
--resources '{"S3Resources":[{"BucketArn":"arn:aws:s3::bucket-name"}]}' \
--description "Description here" \
--address-id ADID00000000-0000-0000-0000-000000000000 \
--kms-key-arn arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--role-arn arn:aws:iam::000000000000:role/SnowconeImportGamma \
--snowball-capacity-preference T8 \
--shipping-option NEXT_DAY \
--snowball-type SNC1_HDD \
--region us-west-2 \

```

Weitere Informationen finden Sie in der API-[Referenz zur Auftragsverwaltung](#) in der AWS Snowball API-Referenz zu .

Aktivieren der Snow Device Management

Gehen Sie wie folgt vor, um Snow Device Management mithilfe des Snowball Edge-Clients zu aktivieren.

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

- Laden Sie die neueste Version des Snowball Edge-Clients herunter und installieren Sie sie. Weitere Informationen finden Sie unter [Herunterladen und Installieren des Snowball-Clients](#).
- Laden Sie die Manifestdatei herunter und rufen Sie den Entsperrcode für das Snow Family-Gerät ab. Weitere Informationen finden Sie unter [Abrufen Ihrer Anmeldeinformationen und Tools](#).
- Verbinden Sie das Snow Family-Gerät mit Ihrem lokalen Netzwerk. Weitere Informationen finden Sie unter [AWS Snowcone](#).
- Entsperren Sie das Snow Family-Gerät. Weitere Informationen finden Sie unter [Entsperren eines Geräts lokal](#).

```

snowballEdge set-features /
--remote-management-state INSTALLED_AUTOSTART /
--manifest-file JID1717d8cc-2dc9-4e68-aa46-63a3ad7927d2_manifest.bin /
--unlock-code 7c0e1-bab84-f7675-0a2b6-f8k33 /

```

```
--endpoint https://192.0.2.0:9091
```

Der Snowball Edge-Client gibt Folgendes zurück, wenn der Befehl erfolgreich ist.

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

Hinzufügen von Berechtigungen für Snow Device Management zu einer IAM-Rolle

Erstellen Sie in der , AWS-Konto aus der das Gerät bestellt wurde, eine AWS Identity and Access Management (IAM)-Rolle und fügen Sie der Rolle die folgende Richtlinie hinzu. Weisen Sie dann die Rolle dem IAM-Benutzer zu, der sich anmeldet, um Ihr Gerät mit Snow Device Management remote zu verwalten. Weitere Informationen finden Sie unter [Erstellen von IAM-Rollen](#) und [Erstellen eines IAM-Benutzers in Ihrem AWS-Konto](#).

Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snow-device-management:ListDevices",
        "snow-device-management:DescribeDevice",
        "snow-device-management:DescribeDeviceEc2Instances",
        "snow-device-management:ListDeviceResources",
        "snow-device-management:CreateTask",
        "snow-device-management:ListTasks",
        "snow-device-management:DescribeTask",
        "snow-device-management:CancelTask",
        "snow-device-management:DescribeExecution",
        "snow-device-management:ListExecutions",
        "snow-device-management:ListTagsForResource",

```



```
        "snow-device-management:TagResource",
        "snow-device-management:UntagResource"
    ],
    "Resource": "*"
}
]
```

CLI-Befehle für Snow Device Management

In diesem Abschnitt werden die AWS CLI Befehle beschrieben, mit denen Sie Ihre Snow Family-Geräte remote mit Snow Device Management verwalten können. Sie können auch einige Remote-Verwaltungsaufgaben mit ausführenAWS OpsHub for Snow Family. Weitere Informationen finden Sie unter [Verwalten von AWS Services auf Ihrem Gerät](#)

Note

Bevor Sie Ihr Gerät verwalten, stellen Sie sicher, dass es eingeschaltet und mit Ihrem Netzwerk verbunden ist und eine Verbindung zu dem herstellen kann, AWS-Region in dem es bereitgestellt wurde.

Themen

- [Erstellen einer Aufgabe](#)
- [Überprüfen des Aufgabenstatus](#)
- [Überprüfen der Geräteinformationen](#)
- [Überprüfen des Amazon EC2-compatible Instance-Status](#)
- [Überprüfen der Aufgabenmetadaten](#)
- [Abbrechen einer Aufgabe](#)
- [Auflisten von Befehlen und Syntax](#)
- [Auflisten von remote verwalteten Geräten](#)
- [Auflisten des Aufgabenstatus über Geräte hinweg](#)
- [Auflisten verfügbarer Ressourcen](#)
- [Auflisten von Geräte- oder Aufgaben-Tags](#)

- [Auflisten von Aufgaben nach Status](#)
- [Anwenden von Tags](#)
- [Entfernen von Tags](#)

Erstellen einer Aufgabe

Um ein oder mehrere Zielgeräte anzuweisen, eine Aufgabe auszuführen, z. B. Entsperren oder Neustarten, verwenden Sie `create-task`. Sie geben Zielgeräte an, indem Sie eine Liste der verwalteten Geräte-IDs mit dem `--targets`Parameter bereitstellen, und geben die Aufgaben an, die mit dem `--command`Parameter ausgeführt werden sollen. Es kann jeweils nur ein Befehl auf einem Gerät ausgeführt werden.

Unterstützte Befehle:

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

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

Befehl

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

Ausnahmen

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

Ausgabe

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

Überprüfen des Aufgabenstatus

Verwenden Sie den `describe-execution` Befehl, um den Status einer Remote-Aufgabe zu überprüfen, die auf einem oder mehreren Zielgeräten ausgeführt wird.

Eine Aufgabe kann einen der folgenden Status haben:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

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

Befehl

```
aws snow-device-management describe-execution \
--taskId st-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 der Geräteinformationen

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

- `lastReachedOutAt` – als das Gerät zuletzt den kontaktiert hatAWS Cloud. Zeigt an, dass das Gerät online ist.
- `lastUpdatedAt` – Wann Daten zuletzt auf dem Gerät aktualisiert wurden. Gibt an, wann der Geräte-Cache aktualisiert wurde.

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

Befehl

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

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
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 des Amazon EC2-compatible Instance-Status

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

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

Befehl

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

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
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 der Aufgabenmetadaten

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

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

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

Befehl

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

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerErrorException  
ThrottlingException  
AccessDeniedException
```

Ausgabe

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

Abbrechen einer Aufgabe

Verwenden Sie den `cancel-task` Befehl, um eine Abbruchanforderung für eine bestimmte Aufgabe zu senden. Sie können nur Aufgaben im QUEUED Status abbrechen, die noch nicht ausgeführt wurden. Aufgaben, die bereits ausgeführt werden, können nicht abgebrochen werden.

Note

Eine Aufgabe, die Sie abbrechen möchten, kann weiterhin ausgeführt werden, wenn sie aus der Warteschlange verarbeitet wird, bevor der `cancel-task` Befehl den Status der Aufgabe ändert.

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

Befehl

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

Ausnahmen

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

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

Auflisten von Befehlen und Syntax

Verwenden Sie den Befehl `aws snow-device-management list-commands`, um eine Liste aller unterstützten Befehle für die Snow Device Management API zurückzugeben. Sie können den `aws snow-device-management list-commands --help` Befehl auch verwenden, um detaillierte Informationen zu und zur Syntax für einen bestimmten Befehl zurückzugeben.

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

Befehl

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

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

Befehl

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

Auflisten von remote verwalteten Geräten

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

Verwenden Sie den folgenden Befehl, um remote verwaltete Geräte aufzulisten. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Befehl

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

Ausnahmen

```
ValidationException  
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": {}
    }
  ]
}
```

Auflisten des Aufgabenstatus über Geräte hinweg

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

Eine Aufgabe kann einen der folgenden Status haben:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

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

Befehl

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

Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

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

Auflisten verfügbarer Ressourcen

Verwenden Sie den `list-device-resources` Befehl , um eine Liste der für ein Gerät verfügbaren AWS Ressourcen zurückzugeben. Verwenden Sie den `--type` Parameter , um die Liste nach einem bestimmten Ressourcentyp zu filtern. Derzeit sind Amazon EC2-compatible Instances der einzige unterstützte Ressourcentyp. `--max-results` und `--next-token` sind optional. Weitere Informationen finden Sie unter [Verwenden von AWS CLI Paginierungsoptionen](#) im AWSBenutzerhandbuch für die -Befehlszeilenschnittstelle.

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

Befehl

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

Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

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

Auflisten von Geräte- oder Aufgaben-Tags

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

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

Befehl

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

Ausnahmen

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Ausgabe

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

Auflisten von Aufgaben nach Status

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

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

Befehl

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

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

Ausnahmen

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Ausgabe

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

Anwenden von Tags

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

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

Befehl

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



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

Ausnahmen

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

Entfernen von Tags

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

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

Befehl

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

Ausnahmen

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

AWS Dienste verwenden auf AWS Snowcone

Unten sehen Sie eine Übersicht über das
ÜbersichtsÜbersichtsÜbersichtsÜbersichtsÜbersichtsÜbersichtsÜbersichtsÜbersichtsÜbersichtsAWS
Snowcone. 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 [Verwenden des AWS Snowball Edge Clients](#).

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

Warning

Wenn Ihnen am Gerät irgendetwas Verdächtiges auffällt, verbinden Sie es nicht mit Ihrem internen Netzwerk. Wenden Sie [AWS Support](#) sich stattdessen an und ein neues wird Ihnen zugeschickt.

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

Themen

- [Verwenden von Amazon EC2-compatible Rechen-Instances](#)
- [Zum AWS DataSync Übertragen von Dateien verwenden](#)
- [Verwalten der NFS-Schnittstelle](#)
- [Benutzen AWS IoT Greengrass um vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen](#)
- [Für die Nutzung der AWS Dienste auf einem AWS Snowcone Gerät erforderliche Ports](#)

Verwenden von Amazon EC2-compatible Rechen-Instances

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

Note

Diese Funktionen werden in der Asien-Pazifik (Mumbai) nicht unterstützt AWS-Region.

Übersicht

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

Wenn der Auftragsstyp lokale Datenverarbeitung ist, können Sie insgesamt 8 TiB lokale EBS-Volumes erstellen und sie an Amazon EC2-compatible Instances anfügen. Auf diese Weise können lokale EC2-compatible Instances auf mehr lokale Kapazität zugreifen als das Root-Volume allein. Dies ist nur lokaler Speicher, sodass Daten, die auf die EBS-Volumes geschrieben werden, verloren gehen, wenn das Gerät an zurückgegeben wird, AWS da sie nicht in Amazon S3 importiert werden können.

Note

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

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

Wenn Ihr Gerät eingetroffen ist, können Sie mit der Verwaltung Ihrer AMIs und Instances beginnen. Sie können Ihre Datenverarbeitungs-Instances auf einem Snowcone über einen Amazon EC2-kompatiblen Endpunkt verwalten. Diese Art von Endpunkt unterstützt viele der Amazon EC2-CLI-Befehle und -Aktionen für die - AWS SDKs. Sie verwenden das - AWS OpsHub for Snow Family Tool, um Ihre AMIs, Datenverarbeitungs-Instances und AWS Services zu verwalten. Weitere Informationen finden Sie unter [Verwenden von AWS OpsHub for Snow Family zum Verwalten von Geräten](#).

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 führen wir ein vollständiges Löschen des Geräts durch, wenn es an zurückgegeben wird AWS. Diese Löschung folgt dem National Institute of Standards and Technology (NIST)-Standard 800-88.

Important

- Die Verwendung verschlüsselter AMIs auf Snowcone-Geräten wird nicht unterstützt.
- Daten in Datenverarbeitungs-Instances, die auf einem Snowcone ausgeführt werden, werden nicht in 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 Auftrag AMIs hinzufügen können, müssen Sie über ein AMI in Ihrem verfügen AWS-Konto und es muss sich um einen unterstützten Image-Typ handeln. Derzeit basieren unterstützte AMIs auf folgenden Betriebssystemen:
 - [Amazon Linux 2](#)

Note

Die neueste Version dieses AMI wird zu dem Zeitpunkt bereitgestellt, an dem Ihr Snow Family-Gerät bereit ist, von zu versenden AWS. Informationen zum Ermitteln der Version

dieses AMI auf dem Gerät, wenn Sie es erhalten, finden Sie unter [Bestimmen der Version des Amazon Linux 2 AMI für Snow Family](#).

- [CentOS 7 \(x86_64\) – mit Updates für HVM](#)
- Ubuntu 16.04 LTS – Xenial (HVM), [Ubuntu 20.04 LTS – Focal](#) oder [Ubuntu 22.04 LTS – Jammy](#)

 Note

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

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

Bevor Sie Ihrer Anforderung zur Auftragserstellung AMIs hinzufügen, stellen Sie sicher, dass Sie über ein oder mehrere unterstützte AMIs in Ihrem verfügen AWS-Konto.

- Alle AMIs müssen auf Amazon Elastic Block Store (Amazon EBS) mit einem einzigen Volume basieren.
- Wenn Sie eine Verbindung zu einer Rechen-Instance herstellen möchten, die auf einem Snowcone ausgeführt wird, 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 aus dem verwenden möchten AWS Marketplace, stellen Sie sicher, dass es über einen unterstützten Produkt- und Nutzungsoperationscode verfügt. Weitere Informationen finden Sie unter [Überprüfen von Produkt- und Nutzungsoptionscodes für AWS Marketplace AMIs](#).
- Stellen Sie sicher, dass die Ihrem AMI zugeordneten vCPU-, Arbeitsspeicher- und Datenspeicherungswerte mit dem Typ der zu erstellenden Instance übereinstimmen.

- Wenn Sie SSH verwenden, um eine Verbindung mit der Instance herzustellen, nachdem Sie die Instance auf Ihrem Snowcone gestartet haben, müssen Sie zuerst das folgende Verfahren ausführen.
- Die Verwendung verschlüsselter AMIs oder verschlüsselter Amazon-EBS-Volumes auf AWS Snowcone Geräten wird nicht unterstützt.

Überprüfen von Produkt- und Nutzungsoptionscodes für AWS Marketplace AMIs

Bevor Sie mit dem Prozess zum Hinzufügen eines AMI von AWS Marketplace zu Ihrem Snow Family-Gerät beginnen, stellen Sie sicher, dass die Produkt- und Nutzungscode 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 erstellen Sie den Auftrag, um das Snow Family-Gerät zu bestellen. 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 von bereitgestellten Linux-AMIs aufzulisten 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 die Suchleiste und dann im Menü Besitzeralias , dann den Operator = und dann 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 Image-Zusammenfassung des AMI sicher, dass die Produktcodes von Ihrer Region unterstützt werden. Weitere Informationen finden Sie in der folgenden Tabelle.

 Note

Der Produktcode avyfzznywektml5qv5f57ska 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	avyfzznywektml5qv5f57ska
Ubuntu 20.04 LTS	a8jynf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkjtt189a13aqe

7. Stellen Sie für alle Regionen sicher, dass der Code für den Nutzungsvorgang lautet `RunInstances`.

Bestimmen der Version des Amazon Linux 2 AMI für Snow Family

Gehen Sie wie folgt vor, um die Version des Amazon Linux 2 AMI für Snow Family auf dem Snow Family-Gerät zu bestimmen. Installieren Sie die neueste Version von `awscli`, AWS CLI bevor Sie fortfahren. Weitere Informationen finden Sie unter [Installieren oder Aktualisieren auf die neueste Version von im AWS CLI](#) AWS Command Line Interface -Benutzerhandbuch.

- Verwenden Sie den `describe-images` AWS CLI Befehl, um die Beschreibung des AMI anzuzeigen. Die Version ist in der Beschreibung enthalten. Geben Sie das öffentliche Schlüsselzertifikat aus dem vorherigen Schritt an. Weitere Informationen finden Sie unter [describe-images](#) in der `awscli` - AWS CLI Befehlsreferenz.

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

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

```
{
  "Images": [
    {
      "CreationDate": "2024-02-12T23:24:45.705Z",
      "ImageId": "s.ami-02ba84cb87224e16e",
      "Public": false,
      "ProductCodes": [
        {
          "ProductCodeId": "avyfzzywektkg15qv5f57ska",
          "ProductCodeType": "marketplace"
        }
      ],
      "State": "AVAILABLE",
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/xvda",
          "Ebs": {
            "DeleteOnTermination": true,
            "Iops": 0,
            "SnapshotId": "s.snap-0efb49f2f726fde63",
            "VolumeSize": 8,
            "VolumeType": "sbp1"
          }
        }
      ],
      "Description": "Snow Family Amazon Linux 2 AMI 2.0.20240131.0 x86_64
HVM gp2",
      "EnaSupport": false,
      "Name": "amzn2-ami-snow-family-hvm-2.0.20240131.0-x86_64-gp2-
b7e7f8d2-1b9e-4774-a374-120e0cd85d5a",
      "RootDeviceName": "/dev/xvda"
    }
  ]
}
```


In diesem Beispiel ist die Version des Amazon Linux 2 AMI für Snow Family **2.0.20240131.0**. Sie finden sie im Wert des `Description` Namens.

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

Um Secure Shell (SSH) zum Herstellen einer Verbindung mit Ihren Datenverarbeitungs-Instances 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.

So fügen Sie einen SSH-Schlüssel einem AMI hinzu

1. Starten Sie eine neue Instance in der , die auf dem Image [Amazon Linux 2 for Snow Family, CentOS 7 \(x86_64\) – mit Updates HVM](#) oder [Ubuntu 16.04 LTS – Xenial \(HVM\)](#) AWS Cloud basiert.

Stellen Sie beim Starten Ihrer Instance sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihre spätere Verwendung auf Snowcone geeignet ist. In der Amazon EC2-Konsole tun Sie dies in Schritt 4: Hinzufügen von Speicher . Eine Liste der unterstützten Größen für Rechen-Instance-Speicher-Volumes auf einem Snowcone finden Sie unter [AWS Snowcone-Kontingente](#) .

2. Installieren und konfigurieren Sie die Anwendungen, die Sie auf Snowcone ausführen möchten, und testen Sie, ob sie wie erwartet funktionieren.
3. Erstellen Sie eine Kopie der PEM/PPK-Datei, die Sie für das SSH-Schlüsselpaar zur Erstellung dieser Instance verwendet haben. Speichern Sie diese Datei auf dem Server, den Sie für die Kommunikation mit 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-Benutzerhandbuch für Linux-Instances.

5. Wiederholen Sie dieses Verfahren für jede der Instances, mit der Sie über SSH eine Verbindung herstellen möchten. Erstellen Sie unbedingt eine Kopie der verschiedenen SSH-Schlüsselpaare und notieren Sie sich die dazugehörigen AMIs.

Erstellen des Auftrags in der Konsole

Ihr nächster Schritt besteht darin, einen Auftrag zum Bestellen eines Snow Family-Geräts zu erstellen. Ihr Auftrag kann ein beliebiger Auftragstyp sein, einschließlich eines Clusters. Um die zu verwenden [Managementkonsole für die AWS Snow-Familie](#), folgen Sie den Anweisungen unter [Erste Schritte](#).

Erstellen Ihres -Auftrags in der AWS CLI

Außerdem können Sie einen Auftrag mithilfe der AWS CLI erstellen. Öffnen Sie dazu ein Terminal und führen Sie den folgenden Befehl aus, wobei Sie den roten Text durch Ihre tatsächlichen Werte ersetzen.

```
aws 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 eintrifft und Sie es entsperren, verwenden Sie den Snowball Edge-Client, um Ihre lokalen Anmeldeinformationen zu erhalten. Weitere Informationen finden Sie unter [Abrufen von Anmeldeinformationen](#).

Netzwerkconfiguration für Datenverarbeitungs-Instances

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

Virtuelle Netzwerkschnittstelle (VNI)

Eine virtuelle Netzwerkschnittstelle ist die Standardnetzwerkschnittstelle für die Verbindung mit einer EC2-compatible Instance auf Ihrem Snow Family-Gerät. Sie müssen für jede Ihrer

EC2-compatible Instances eine VNI erstellen, unabhängig davon, ob Sie auch eine direkte Netzwerkschnittstelle verwenden oder nicht. Der Datenverkehr, der durch eine VNI geleitet wird, ist durch die Sicherheitsgruppen geschützt, die Sie eingerichtet haben. Sie können VNIs nur dem physischen Netzwerkport zuordnen, den Sie zur Steuerung Ihres Snow-Family-Geräts verwenden.

Note

VNI verwendet dieselbe physische Schnittstelle (RJ45, SFP+ oder QSFP), die für die Verwaltung des Snow Family-Geräts verwendet wird. Das Erstellen einer VNI auf einer anderen physischen Schnittstelle als der, die für die Geräteverwaltung verwendet wird, kann zu unerwarteten Ergebnissen führen.

Direkte Netzwerkschnittstelle (DNI)

Eine Direct Network Interface (DNI) ist ein erweitertes Netzwerkfeature, das Anwendungsfälle wie Multicast-Streams, transitives Routing und Load Balancing ermöglicht. Indem Sie Instances Netzwerkzugriff auf Layer 2 ohne Zwischenübersetzung oder -filterung gewähren, können Sie eine größere Flexibilität bei der Netzwerkkonfiguration Ihres Snow Family-Geräts und eine verbesserte Netzwerkleistung erzielen. DNIs unterstützen VLAN-Tags und die Anpassung der MAC-Adresse. Der Datenverkehr auf DNIs ist nicht durch Sicherheitsgruppen geschützt.

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

Themen

- [Voraussetzungen](#)
- [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\)](#)
- [Einrichten einer Direct Network Interface \(DNI\)](#)

Voraussetzungen

Bevor Sie eine VNI oder eine DNI konfigurieren, müssen Sie die folgenden Voraussetzungen erfüllen.

1. Stellen Sie sicher, dass Ihr Gerät mit Strom versorgt ist und dass eine Ihrer physischen Netzwerkschnittstellen, wie der RJ45-Port, mit einer IP-Adresse verbunden ist.
2. Rufen Sie die IP-Adresse ab, die der physischen Netzwerkschnittstelle zugeordnet ist, die Sie auf dem Snow Family-Gerät verwenden.

3. Konfigurieren Sie Ihren Snowball Edge-Client. Weitere Informationen finden Sie unter [Konfigurieren eines Profils für den Snowcone-Client](#)
4. Entsperren Sie das Gerät. Wir empfehlen, AWS OpsHub for Snow Family zum Entsperren Ihres Geräts zu verwenden. Anweisungen finden Sie unter [Entsperren eines Geräts](#)

Wenn Sie den CLI-Befehl verwenden möchten, führen Sie den folgenden Befehl aus und geben Sie die Informationen ein, die im Dialogfeld angezeigt werden.

```
snowballEdge configure
```

Snowball Edge Manifest Path: `manifest.bin`

Unlock Code: *unlock code*

Default Endpoint: `https://device ip`

5. Führen Sie den folgenden Befehl aus.

```
snowballEdge unlock-device
```

Das Update der Geräteanzeige zeigt an, dass es entsperrt ist.

6. Starten Sie eine EC2-compatible Instance auf dem Gerät. Sie verknüpfen die VNI mit dieser Instance.
7. Führen Sie den Befehl `snowballEdge describe-device` aus, um die Liste der IDs der physischen Netzwerkschnittstellen abzurufen.
8. Identifizieren Sie die ID der physischen Netzwerkschnittstelle, die Sie verwenden möchten. Notieren Sie diese.

Einrichten einer 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 eine VNI einzurichten. Stellen Sie sicher, dass Sie die erforderlichen Aufgaben ausführen, bevor Sie eine VNI erstellen.

Erstellen einer VNI und Zuordnen einer IP-Adresse

1. Führen Sie den Befehl `snowballEdge create-virtual-network-interface` aus. Die folgenden Beispiele zeigen die Ausführung des Befehls mit den beiden verschiedenen IP-

Adressvergabemethoden DHCP oder STATIC. Die DHCP-Methode verwendet das Dynamic Host Configuration Protocol (DHCP).

```
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment DHCP  
  
//OR//  
  
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment STATIC \  
--static-ip-address-configuration IpAddress=192.0.2.0,Netmask=255.255.255.0
```

Der Befehl gibt eine JSON-Struktur zurück, die die IP-Adresse enthält. Notieren Sie sich diese IP-Adresse für den `ec2 associate-address` AWS CLI Befehl später im Prozess.

Jedes Mal, wenn 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 Ihrer Instance zuzuordnen, verwenden Sie den folgenden Befehl und ersetzen Sie den roten Text durch Ihre Werte:

```
aws ec2 associate-address --public-ip 192.0.2.0 --instance-id s.i-01234567890123456  
--endpoint http://Snow Family device physical IP address:8008
```

Einrichten einer Direct Network Interface (DNI)


Note

Das Feature für direkte Netzwerkschnittstellen ist am oder nach dem 12. Januar 2021 verfügbar und ist in allen verfügbar, in AWS-Regionen denen Snow Family-Geräte verfügbar sind.

Voraussetzungen

Bevor Sie eine Direct Network Interface (DNI) einrichten, müssen Sie die Aufgaben im Abschnitt **Voraussetzungen** ausführen.

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

 Note

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

Erstellen einer DNI und Zuordnen einer IP-Adresse

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

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

OPTIONS

--endpoint <endpoint> Der Endpunkt, an den diese Anforderung gesendet werden soll. Der Endpunkt für Ihre Geräte ist eine URL mit dem `https` Schema 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-compatible Instance-ID, an die die Schnittstelle angehängt werden soll (optional).

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

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

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

--vlan <vlanId> Legen Sie das zugewiesene VLAN für die Schnittstelle fest (optional).

Wenn angegeben, wird der gesamte von der Schnittstelle gesendete Datenverkehr mit der angegebenen VLAN-ID markiert. Eingehender Datenverkehr wird nach der angegebenen VLAN-ID gefiltert und alle VLAN-Tags werden entfernt, bevor sie an die Instance übergeben werden.

2. Wenn Sie Ihre DNI in Schritt 1 nicht mit einer Instance verknüpft haben, können Sie sie verknüpfen, indem Sie den [Aktualisieren einer Direct Network Interface](#) Befehl ausführen.
3. Nachdem Sie eine DNI erstellt und mit Ihrer EC2-compatible Instance verknüpft haben, müssen Sie zwei Konfigurationsänderungen in Ihrer Amazon EC2-compatible Instance vornehmen.
 - Stellen Sie zunächst sicher, dass Pakete, die für die VNI bestimmt sind, die der EC2-compatible Instance zugeordnet ist, über eth0 gesendet werden.
 - Die zweite Änderung konfiguriert Ihre direkte Netzwerkschnittstelle so, dass beim Start entweder DHCP oder statische IP verwendet wird.

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

Amazon Linux 2

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

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

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

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

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

CentOS Linux

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

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

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



```
BOOTPROTO=dhcp
TYPE=Ethernet
EOF

# Rename DNI device if needed.
CURRENT_DEVICE_NAME=$(LANG=C ip -o link | awk -F ': ' -vIGNORECASE=1 '!/link\/
ieee802\.\.11/ && /'"$DNI_MAC"'/ { print $2 }')
ip link set $CURRENT_DEVICE_NAME name $DNI

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

Zusätzliche Befehle

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

Herstellen einer Verbindung mit Ihrer Compute Instance auf einem Snowcone mithilfe von SSH

Um SSH für die Verbindung mit Ihren Datenverarbeitungs-Instances auf Snowcone-Geräten zu verwenden, müssen Sie zuerst den SSH-Schlüssel für das AMI bereitstellen, bevor Sie Ihren Auftrag 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 [Netzwerkconfiguration für Datenverarbeitungs-Instances](#).
3. Überprüfen Sie Ihre Notizen zum Suchen des PPK- oder PEM-Schlüsselpaars aus, das Sie für diese spezifische Instance verwendet haben. Erstellen Sie eine Kopie dieser Dateien an einem beliebigen Ort auf Ihrem Computer. Notieren Sie sich den Pfad zur PEM-Datei.

4. Verbinden Sie sich wie im folgenden Beispielbefehl per SSH mit Ihrer Instance. Die IP-Adresse ist die IP-Adresse der virtuellen Netzwerkschnittstelle (VNIC), die Sie in [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 mit Ihrer Linux-Instance mit SSH](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Snowcone-Client-Befehle für Compute-Instances

Der Snowball Edge-Client ist eine eigenständige Terminalanwendung, die Sie auf Ihrem lokalen Server ausführen können. Damit können Sie einige administrative Aufgaben auf Ihrem Snowcone-Gerät ausführen. Weitere Informationen zur Verwendung des Snowball Edge-Clients, einschließlich des Startens und Stoppens von Services, finden Sie unter [Verwenden des AWS Snowball Edge Clients](#).

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

Note

Befehle im Zusammenhang mit Clustern werden nicht unterstützt und geben einen Fehler zurück.

Erstellen einer Startkonfiguration zum automatischen Starten von Amazon EC2-compatible Instances

Um AmazonEC2-compatible Rechen-Instances automatisch auf Ihrem AWS Snowcone Gerät 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]

```

Aktualisieren einer Startkonfiguration zum Autostart von EC2-compatible Instances

Verwenden Sie den `snowballEdge update-autostart-configuration` Befehl, um eine vorhandene 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 zum Autostart von EC2-compatible 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
```

Auflisten von Startkonfigurationen zum Autostart von EC2-compatible Instances

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 Rechen-Instance auf Ihrem Snowcone auszuführen oder die NFS-Schnittstelle auf Ihrem Snowcone zu starten, erstellen Sie zunächst eine virtuelle Netzwerkschnittstelle (VNIC). Jeder Snowcone verfügt über drei Netzwerkschnittstellen (NICs), die physischen Netzwerkschnittstellencontroller für das Gerät. Dies sind die RJ45-Ports auf der Geräterückseite.

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 konfigurierten Snowball Edge-Client.

```
snowballEdge create-virtual-network-interface --endpoint https://[ip address]
--manifest-file /path/to/manifest --unlock-code [unlock code] --ip-address-
assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface
id] --static-ip-address-configuration IPAddress=[IP address],NetMask=[Netmask]
```

Example Beispiel: Erstellen von VNICs (mit DHCP)

```
snowballEdge create-virtual-network-interface --ip-address-assignment dhcp --physical-
network-interface-id s.ni-8EXAMPLEaEXAMPLEd
{
  "VirtualNetworkInterface" : {
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-8EXAMPLE8EXAMPLEf",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45"
  }
}
```

Beschreibung Ihrer virtuellen Netzwerkschnittstellen

Um die zuvor auf Ihrem Gerät erstellten VNICs zu beschreiben, verwenden Sie den Befehl `snowballEdge describe-virtual-network-interfaces`. Im Folgenden wird gezeigt, wie Sie ihn verwenden.

Verwendung

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

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

Das folgende Anwendungsbeispiel zeigt die `-`Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge describe-virtual-network-interfaces --endpoint https://[ip address] --
manifest-file /path/to/manifest --unlock-code [unlock code]
```

Example Beispiel: Beschreiben von VNICs

```
snowballEdge describe-virtual-network-interfaces
[
  {
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-8EXAMPLE8EXAMPLE8",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45"
  },{
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-1EXAMPLE1EXAMPLE1",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.2",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "12:34:5E:XA:MP:LE"
  }
]
```

Aktualisieren einer virtuellen Netzwerkschnittstelle

Nach der Erstellung einer virtuellen Netzwerkschnittstelle (Virtual Network Interface, VNIC) können Sie ihre Konfiguration mit dem Befehl `snowballEdge update-virtual-network-interface` aktualisieren. Nach der Bereitstellung des Amazon-Ressourcennamens (ARN) für eine bestimmte VNIC geben Sie nur für die Elemente Werte ein, die Sie aktualisieren.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge update-virtual-network-interface --virtual-network-interface-arn [virtual network-interface-arn] --ip-address-assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface id] --static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]
```

Das folgende Anwendungsbeispiel zeigt die -Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge update-virtual-network-interface --endpoint https://[ip address] --manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-interface-arn [virtual network-interface-arn] --ip-address-assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface id] --static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]
```

Example Beispiel: Aktualisieren einer VNIC (mit DHCP)

```
snowballEdge update-virtual-network-interface --virtual-network-interface-arn arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd --ip-address-assignment dhcp
```

Löschen einer virtuellen Netzwerkschnittstelle

Um eine virtuelle Netzwerkschnittstelle zu löschen, können Sie den Befehl `snowballEdge delete-virtual-network-interface` verwenden.

Usage

Sie können diesen Befehl auf zwei Arten verwenden: mit konfiguriertem Snowball Edge-Client oder ohne konfigurierten Snowball Edge-Client. Das folgende Anwendungsbeispiel zeigt die Methode mit konfiguriertem Snowball Edge-Client.

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn [virtual network-interface-arn]
```

Das folgende Anwendungsbeispiel zeigt die -Methode ohne konfigurierten Snowball Edge-Client.

```
snowballEdge delete-virtual-network-interface --endpoint https://[ip address] --manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-interface-arn [virtual network-interface-arn]
```

Example Beispiel: Löschen einer VNIC

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn  
arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd
```

Verwenden von Instance Metadata Service für Snow mit Amazon EC2-compatible Instances

IMDS for Snow stellt Instance Metadata Service (IMDS) für AmazonEC2-compatible Instances in Snow bereit. Instance-Metadaten sind Kategorien von Informationen zu Instances. Sie enthält Kategorien wie Hostname , Ereignisse und Sicherheitsgruppen . Mit IMDS für Snow können Sie Instance-Metadaten verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Starten Ihrer Amazon-EC2-compatible angegeben haben. Sie können beispielsweise IMDS für Snow verwenden, um Parameter für die Konfiguration Ihrer Instance anzugeben oder diese Parameter in ein einfaches Skript aufzunehmen. Sie können generische AMIs erstellen und mit Hilfe von Benutzerdaten die beim Start ausgelieferten Konfigurationsdateien ändern.

Weitere Informationen zu Instance-Metadaten und Benutzerdaten sowie SnowEC2-compatible Instances finden Sie unter [Unterstützte Instance-Metadaten und Benutzerdaten](#) in diesem Handbuch.

Important

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

Note

In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des Instance-Metadatenservices verwendet: 169.254.169.254. Das Abrufen von Instance-Metadaten mit der Link-lokalen IPv6-Adresse wird nicht unterstützt.

Themen

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

IMDS-Versionen

Sie können mit IMDS Version 2 oder IMDS Version 1 auf Instance-Metadaten von einer laufenden Instance zugreifen:

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

Je nach Version Ihrer Snow-Software können Sie IMDSv1, IMDSv2 oder beides verwenden. Dies hängt auch vom Typ des AMI ab, das in der EC2-compatible Instance ausgeführt wird. Einige AMIs, z. B. solche, auf denen Ubuntu 20.04 ausgeführt wird, erfordern IMDSv2. Der Instance-Metadatenservice unterscheidet zwischen IMDSv1- und IMDSv2-Anforderungen basierend auf dem Vorhandensein von -PUT oder -GET-Headern. IMDSv2 verwendet beide Header. IMDSv1 verwendet nur den -GET-Header.

AWS empfiehlt die Verwendung von IMDSv2 anstelle von IMDSv1, da IMDSv2 eine höhere Sicherheit bietet. Weitere Informationen finden Sie unter [Erweitern Sie den EC2-Instance-Metadataservice, um Abwehr von offenen Firewalls, Reverse-Proxy und SSRF-Schwachstellen mit Verbesserungen an EC2-Instance-Metadataservice](#).

IMDSv2

IMDSv2 verwendet sitzungsorientierte Anfragen. Bei sitzungsorientierten 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 zukünftige Anfragen erstellen.

Im folgenden Beispiel werden ein Linux-Shell-Skript und IMDSv2 verwendet, um die Metadatenelemente der Instance der obersten Ebene abzurufen. Dieses Beispiel:

1. Erstellt mithilfe der PUT-Anforderung ein Sitzungstoken von sechs Stunden (21 600 Sekunden).
2. Speichert den Sitzungstoken-Header in einer Variablen mit dem Namen TOKEN.
3. Fordert die Top-Level-Metadatenelemente mit dem Token an.

Sie können zwei Befehle separat ausführen oder kombinieren.

Separate Befehle

Generieren Sie zuerst ein Token mit dem folgenden Befehl.

Note

`X-aws-ec2-metadata-token-ttl-seconds` ist ein erforderlicher Header. Wenn dieser Header nicht enthalten ist, erhalten Sie den Fehlercode 400 – Fehlende oder ungültige Parameter.

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

Verwenden Sie dann das Token, um mit dem folgenden Befehl Metadatenelemente der obersten Ebene zu generieren.

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

Kombinierte Befehle

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

Note

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

Example kombinierte Befehle

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

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

Example Wiederverwenden eines Tokens

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

Wenn Sie IMDSv2 verwenden, um Instance-Metadaten anzufordern, muss die Anforderung den folgenden Regeln entsprechen:

1. Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance-Metadaten-Service zu starten. Die PUT-Anfrage gibt ein Token zurück, das in nachfolgenden GET-Anfragen an den Instance-Metadaten-Service enthalten sein muss. Das Token wird für den Zugriff auf Metadaten mit IMDSv2 benötigt.
2. Nehmen Sie das Token in alle GET-Anfragen an den Instance-Metadaten-Service auf.
 - a. Das Token ist ein Instance-spezifischer Schlüssel. Das Token ist auf anderen EC2-compatible Instances nicht gültig und wird abgelehnt, wenn Sie versuchen, es außerhalb der Instance zu verwenden, auf der es generiert wurde.
 - b. Die PUT-Anfrage muss einen Header enthalten, der die Time To Live (TTL) für das Token in Sekunden bis zu maximal sechs Stunden (21 600 Sekunden) angibt. Das Token stellt eine logische Sitzung dar. Die TTL gibt die Gültigkeitsdauer des Token und damit die Dauer der Sitzung an.
 - c. Nachdem ein Token abgelaufen ist, müssen Sie eine neue Sitzung mit einer anderen PUT-Anfrage erstellen, um auf die Instance-Metadaten zuzugreifen.

- d. Sie können auswählen, ob Sie ein Token wiederverwenden oder bei jeder Anforderung ein neues Token erstellen möchten. Für eine kleine Anzahl von Anfragen kann es einfacher sein, bei jedem Zugriff auf den Instance-Metadaten-Service ein Token zu generieren und sofort zu verwenden. Aus Effizienzgründen können Sie jedoch eine längere Dauer für das Token festlegen und es wiederverwenden, anstatt jedes Mal eine PUT-Anfrage stellen zu müssen, wenn Sie Instance-Metadaten anfordern müssen. Es gibt keine praktische Begrenzung der Anzahl der gleichzeitigen Tokens, die jeweils eine eigene Sitzung darstellen.

In PUT-Instance-Metadatenanfragen sind HTTP GET- und HEAD-Methoden zulässig. -Anfragen werden abgelehnt, wenn sie einen X-Forwarded-For-Header enthalten.

Standardmäßig hat die Antwort auf -PUTAnfragen ein Antwort-Hop-Limit (Time to Live) von 1 auf IP-Protokollebene. IMDS für Snow kann das Hop-Limit für PUT Antworten nicht ändern.

IMDSv1

IMDSv1 verwendet das Anfrage-Antwort-Modell. Um Instance-Metadaten anzufordern, senden Sie eine GET Anforderung an den Instance-Metadaten-Service.

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

Abrufen von Instance-Metadaten

Ihre Instance-Metadaten sind von Ihrer laufenden Instance aus verfügbar, sodass Sie nicht die Amazon EC2-Konsole oder die verwenden müssen, AWS CLI um darauf zuzugreifen. Dies kann sehr hilfreich sein, wenn Sie ein Skript schreiben möchten, das in der Instance ausgeführt werden soll. So können Sie z. B. über die Instance-Metadaten auf die lokale IP-Adresse Ihrer Instance zugreifen, um die Verbindung zu einer externen Anwendung zu verwalten. Instance-Metadaten werden in vier Kategorien unterteilt. Eine Beschreibung der einzelnen Instance-Metadatenkategorien finden Sie unter [Unterstützte Instance-Metadaten und Benutzerdaten](#) in diesem Handbuch.

Um alle Kategorien von Instance-Metadaten innerhalb einer laufenden Instance anzuzeigen, verwenden Sie den folgenden IPv4-URI:

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

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

Antworten und Fehlermeldungen

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

Eine Anforderung für eine bestimmte Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode 404 – Not Found zurück, wenn die Ressource nicht verfügbar ist.

Eine Anforderung für eine allgemeine Metadatenressource (wenn der URI mit einem `/` Zeichen endet) gibt eine Liste der verfügbaren Ressourcen oder einen HTTP-Fehlercode 404 – Not Found zurück, wenn es keine solche Ressource gibt. Die Listenelemente befinden sich in separaten Zeilen, die durch Zeilenvorschübe (ASCII-Zeichencode 10) beendet werden.

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

- 400 – Fehlende oder ungültige Parameter – Die PUT Anforderung ist ungültig.
- 401 – Nicht autorisiert – Die GET Anforderung verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.
- 403 – Verboten – Die Anforderung ist nicht zulässig oder der Instance-Metadatenservice ist deaktiviert.

Beispiele für das Abrufen von Instance-Metadaten mit IMDSv1 und IMDSv2

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

Example Abrufen der verfügbaren Versionen der Instance-Metadaten

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

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://192.0.2.0/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/
```

```

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload  Total   Spent    Left  Speed
 100    56    100     56      0      0     3733    0    --:--:--
--:--:-- --:--:-- 3733
* Trying 192.0.2.0...
* TCP_NODELAY set
* Connected to 192.0.2.0 (192.0.2.0) port 80 (#0)
> GET / HTTP/1.1
> Host: 192.0.2.0
> User-Agent: curl/7.61.1
> Accept: */*
> X-aws-ec2-metadata-token:
MDAXcxNFLbAwJIYx8KzgNckcHTdxT4Tt69TzpKExlXKTULHIQnjEtXvD
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Date: Mon, 12 Sep 2022 21:58:03 GMT
< Content-Length: 274
< Content-Type: text/plain
< Server: EC2ws
<
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27

```

```
2021-01-03
2021-03-23
* Closing connection 0
```

IMDSv1

```
[ec2-user ~]$ curl http://192.0.2.0/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
latest
```

Example Abrufen der Top-Level-Metadatenelemente

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

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://192.0.2.0/latest/api/token" -H "X-aws-ec2-  
metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v  
http://192.0.2.0/latest/meta-data/  
ami-id  
hostname  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
network/  
reservation-id  
security-groups
```

IMDSv1

```
[ec2-user ~]$ curl http://192.0.2.0/latest/meta-data/  
ami-id  
hostname  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
network/  
reservation-id  
security-groups
```

Example Abrufen von Werten von Top-Level-Metadaten

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

ami-id IMDSv2


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

ami-id IMDSv1

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

reservation-id IMDSv2

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

reservation-id IMDSv1

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

local-hostname IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://192.0.2.0/latest/meta-data/local-hostname ip-00-000-00-00
```

local-hostname IMDSv1

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

Verwenden des AmazonEC2-compatible 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) und Datenverarbeitungs-Instances mithilfe von Amazon EC2-compatible API-Operationen programmgesteuert verwalten.

Themen

- [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#)
- [Nicht unterstützte Amazon EC2-Funktionen für Snowcone](#)
- [Unterstützte Amazon EC2-compatible AWS CLI Befehle auf einem Snowcone](#)
- [Unterstützte Amazon EC2-API-Operationen](#)

Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt

Wenn Sie die verwenden, AWS CLI um einen Befehl an das AWS Snowcone Gerät auszugeben, können Sie angeben, dass der Endpunkt der Amazon EC2-compatible Endpunkt ist. Sie können den HTTPS-Endpunkt oder einen ungesicherten HTTP-Endpunkt, wie hier gezeigt, verwenden.

Gesicherter HTTPS-Endpunkt

```
aws ec2 describe-instances --endpoint https://192.0.2.0:8243 --ca-bundle path/to/certificate
```

Ungesicherter HTTP-Endpunkt

```
aws ec2 describe-instances --endpoint http://192.0.2.0:8008
```

Wenn Sie den HTTPS-Endpunkt 8243 verwenden, werden Ihre Daten während der Übertragung verschlüsselt. Diese Verschlüsselung wird mit einem Zertifikat gewährleistet, das von Snowcone generiert wird, wenn es entsperrt wird. Nachdem Sie Ihr Zertifikat erhalten haben, können Sie es in einer lokalen `ca-bundle.pem`-Datei speichern. Anschließend können Sie Ihr AWS CLI -Profil so konfigurieren, dass der Pfad zu Ihrem Zertifikat wie unten beschrieben hinzugefügt wird.

So verknüpfen Sie Ihr Zertifikat mit dem Amazon EC2-compatible Endpunkt

1. Verbinden Sie Snowcone mit dem Strom und dem Netzwerk und schalten Sie es ein.

2. Notieren Sie nach dem Entsperren des Geräts seine IP-Adresse im lokalen Netzwerk.
3. Stellen Sie von einem Terminal in Ihrem Netzwerk sicher, dass Sie das Snowcone-Gerät anpingen 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-Funktionen für Snowcone

Mit dem Amazon EC2-compatible Endpunkt können Sie Ihre AMIs und Rechen-Instances auf einem Snowcone mit Amazon EC2-compatible 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. Die folgenden Amazon EC2-Aktionen werden beispielsweise nicht für die Verwendung mit Snowcone unterstützt:

- [create-nat-gateway](#)
- [create-key-pair](#)

Unterstützte Amazon EC2-compatible AWS CLI Befehle auf einem Snowcone

Sie können Ihre Datenverarbeitungs-Instances auf einem Snow Family-Gerät über einen Amazon EC2-compatible Endpunkt verwalten. Diese Art von Endpunkt unterstützt viele der Amazon EC2-CLI-Befehle und -Aktionen der - AWS SDKs. Informationen zum Installieren und Einrichten der AWS CLI, einschließlich der Angabe, für welche AWS-Regionen Sie AWS CLI Aufrufe tätigen möchten, finden Sie im [AWS Command Line Interface -Benutzerhandbuch](#).

Liste der unterstützten Amazon EC2-compatible 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](#) – Fügt ein Amazon EBS-Volume an eine angehaltene oder ausgeführte Instance auf Ihrem AWS Snowcone Gerät an und stellt es der Instance mit dem angegebenen Gerätenamen zur Verfügung.
 - `--device value` – Der Gerätename.
 - `--instance-id` – Die ID einer Amazon EC2-Ziel-Instance.
 - `--volume-id value` – Die ID des EBS-Volumes.
- [authorize-security-group-egress](#) – Fügt einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln für die 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 Devices](#).
 - `--group-id value` – Die ID der Sicherheitsgruppe
 - `[--ip-permissions value]` – Ein oder mehrere Sätze von IP-Berechtigungen.
- [authorize-security-group-ingress](#) – Fügt einer Sicherheitsgruppe eine oder mehrere Eingangsregeln hinzu. Wenn Sie `authorize-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
 - `[--group-name value]` – Der Name der Sicherheitsgruppe.
 - `[--group-id value]` – Die ID der Sicherheitsgruppe
 - `[--ip-permissions value]` – Ein oder mehrere Sätze von IP-Berechtigungen.
 - `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (-1) angegeben.
 - `[--port value]` – Für TCP oder UDP der Bereich der zuzulassenden Ports. Dieser Wert kann eine einzelne Ganzzahl oder ein Bereich (Minimum–Maximum) sein.

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

- [--cidr value] – Der CIDR-IP-Bereich.
- [create-launch-template](#) – Erstellt eine Startvorlage. Eine Startvorlage enthält die Parameter zum Starten einer Instance. Wenn Sie eine Instance über RunInstances starten, können Sie eine Startvorlage angeben, statt die Startparameter in der Anfrage bereitzustellen. Sie können bis zu 100 Vorlagen pro 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-description string]` – Eine Beschreibung für die erste Version der Startvorlage.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [create-launch-template-version](#) – Erstellt eine neue Version für eine Startvorlage. Sie können eine vorhandene Version einer Startvorlage angeben, auf der die neue Version basieren soll. Die Startvorlagenversionen werden in der Reihenfolge markiert, in der sie erstellt werden. Sie können die Nummerierung von Startvorlagenversionen nicht angeben, ändern oder ersetzen. Sie können bis zu 100 Versionen jeder Startvorlage erstellen.

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

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

JSON-Syntax:

```

' {
  "ImageId": "string",
  "InstanceType": "sbe-c.large",
  "SecurityGroupIds": ["string", ...],
  "TagSpecifications": [{"ResourceType": "instance", "Tags":
    [{"Key": "Name", "Value": "Test"},
     {"Key": "Stack", "Value": "Gamma"}]}],

```

```
"UserData":"this is my user data"
}'
```

- [--source-version string] – Die Versionsnummer der Startvorlage, auf der die neue Version basieren soll. Die neue Version übernimmt alle Startparameter der Quellversion, ausgenommen der von Ihnen in launch-template-data angegebenen Parameter.
- [--version-description string] – Eine Beschreibung für die erste Version der Startvorlage.
- --endpoint snowballEndpoint – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [create-tags](#) – Fügt ein oder mehrere Tags für die angegebene Ressource hinzu oder überschreibt sie. Jede Ressource kann maximal 50 Tags haben. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Tag-Schlüssel müssen für eine Ressource eindeutig sein. Folgende Ressourcen werden unterstützt:
 - AMI
 - Instance
 - Startvorlage
 - Sicherheitsgruppe
- [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 AWS Snowcone Gerät angefügt werden kann.
 - [-Größe value] – Die Größe des Volumes in GiBs, das zwischen 1 GiB und 1 TB (1000) liegen kann GiBs.
 - [--snapshot-id value] – Der Snapshot, aus dem das Volume erstellt werden soll.
 - [--volume-type value] – Der Volume-Typ. Wenn kein Wert angegeben wird, lautet der Standardwert sbg1. Die folgenden Werte sind möglich:
 - sbg1 für magnetische Volumes
 - sbp1 für SSD-Volumes

- `[--tag-specification value]` – Eine Liste von Tags, die während der Erstellung auf das Volume angewendet werden sollen.
- [delete-launch-template](#) – Löscht eine Startvorlage. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht.

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

- `--launch-template-id string` – Die ID der Startvorlage.
- `--launch-template-name string` – Ein Name für die Startvorlage.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [delete-launch-template-version](#) – Löscht eine oder mehrere Versionen einer Startvorlage. Sie können die Standardversion einer Startvorlage erst löschen, nachdem Sie eine andere Version als Standardversion festgelegt haben. Wenn die Standardversion die einzige Version der Startvorlage ist, löschen Sie die gesamte Startvorlage, indem Sie den Befehl `delete-launch-template` verwenden.

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

- `--launch-template-id string` – Die ID der Startvorlage.
- `--launch-template-name string` – Ein Name für die Startvorlage.
- `--versions (list) "string" "string"` – Die Versionsnummern einer oder mehrerer zu löschender Startvorlagenversionen.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen 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, Rechen-Instance, Startvorlage oder Sicherheitsgruppe).

- [delete-volume](#) – Löscht das angegebene Amazon EBS-Volume. Das Volume muss den `available`-Status aufweisen (nicht an eine Instance angefügt).
 - `--volume-id value` – Die ID des Volumes.
- [describe-addresses](#) – Beschreibt eine oder mehrere Ihrer virtuellen IP-Adressen, die derselben Anzahl von Instances auf Ihrem Gerät zugeordnet 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. Bilder, die Ihnen zur Verfügung stehen, werden dem Snowcone-Gerät während 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 Instances, die auf dem Gerät gestoppt wurden.
 - `--page-size` – Die Größe jeder Seite, die in den Aufruf aufgenommen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
 - `--max-items` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
 - `--starting-token` – Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- [describe-launch-templates](#) – Beschreibt eine oder mehrere Startvorlagen. Beim Befehl `describe-launch-templates` handelt es sich um eine paginierte Operation. Sie können mehrere Aufrufe ausführen, um den gesamten Ergebnisdatensatz abzurufen.

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

- `--launch-template-ids` (Liste) `"string" "string"` – Eine Liste von IDs der Startvorlagen.
- `--launch-template-names` (Liste) `"string" "string"` – Eine Liste von Namen für die Startvorlagen.
- `--page-size` – Die Größe jeder Seite, die in den Aufruf aufgenommen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token` – Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [describe-launch-template-versions](#) – Beschreibt eine oder mehrere Versionen einer angegebenen Startvorlage. Sie können alle Versionen, einzelne Versionen oder eine Reihe von Versionen beschreiben. Beim Befehl `describe-launch-template-versions` handelt es sich um eine paginierte Operation. Sie können mehrere Aufrufe ausführen, um den gesamten Ergebnissatz abzurufen.

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

- `--launch-template-id string` – Die ID der Startvorlage.
- `--launch-template-name string` – Ein Name für die Startvorlage.
- `[--versions (list) "string" "string"]` – Die Versionsnummern einer oder mehrerer zu löschender Startvorlagenversionen.
- `[--min-version string]` – Die Versionsnummer, nach der Startvorlagenversionen beschrieben werden sollen.

- `[--max-version string]` – Die Versionsnummer, bis zu der Startvorlagenversionen beschrieben werden sollen.
- `--page-size` – Die Größe jeder Seite, die in den Aufruf aufgenommen werden soll. Dieser Wert hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen an das Gerät, wodurch bei jedem Anruf weniger Elemente abgerufen werden. Auf diese Weise kann die Zeitüberschreitung von Aufrufen verhindert werden.
- `--max-items` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
- `--starting-token` – Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Datenverarbeitungs-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [describe-security-groups](#) – Beschreibt eine oder mehrere Ihrer Sicherheitsgruppen.

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

- `[--group-name value]` – Der Name der Sicherheitsgruppe.
- `[--group-id value]` – Die ID der Sicherheitsgruppe.
- `[--page-size value]` – Die Größe jeder Seite, die im AWS Serviceaufruf abgerufen werden soll. Diese Größe hat keinerlei Auswirkung auf die Anzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben wurden. Das Festlegen einer kleineren Seitengröße führt zu mehr Aufrufen des AWS Services und zum Abrufen von weniger Elementen in jedem Aufruf. Dieser Ansatz kann dazu beitragen, ein Timeout der AWS Service-Aufrufe zu verhindern. Anwendungsbeispiele finden Sie unter [Paginierung](#) im AWS Command Line Interface - Benutzerhandbuch.
- `[--max-items value]` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-

Argument eines nachfolgenden Befehls an. Verwenden Sie das `-NextToken`Antwortelement nicht direkt außerhalb der AWS CLI. Anwendungsbeispiele finden Sie unter [Paginierung](#) im AWS Command Line Interface -Benutzerhandbuch.

- `[--starting-token value]` – Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort. Anwendungsbeispiele finden Sie unter [Paginierung](#) im AWS Command Line Interface - Benutzerhandbuch.
- [describe-tags](#) – Beschreibt ein oder mehrere Tags für die angegebene Ressource (`image`, `instance` oder Sicherheitsgruppe). Mit diesem Befehl werden die folgenden Filter unterstützt:
 - `launch-template`
 - `resource-id`
 - Ressourcentyp: `image` oder `instance`
 - `key`
 - Wert
- [describe-volumes](#) – Beschreibt die angegebenen Amazon EBS-Volumes.
 - `[--max-items value]` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an.
 - `[--starting-token value]` – Ein Token, das angibt, wo mit der Paginierung begonnen werden soll. Dieses Token ist der `NextToken`-Wert aus einer zuvor abgeschnittenen Antwort.
 - `[--volume-ids value]` – Eine oder mehrere Volume-IDs .
- [detach-volume](#) – Trennt ein Amazon-EBS-Volume von einer angehaltenen oder ausgeführten Instance.
 - `[--device value]` – Der Gerätenamen.
 - `[--instance-id]` – Die ID einer Amazon EC2-Ziel-Instance.
 - `--volume-id value` – Die ID des Volumes.
- [disassociate-address](#) – Entfernt eine virtuelle IP-Adresse von der Instance.
 - `--public-ip` – Die virtuelle IP-Adresse, die Sie von Ihrer Instance trennen möchten.
- [get-launch-template-data](#) – Ruft die Konfigurationsdaten der angegebenen Instance ab. Sie können diese Daten verwenden, um eine Startvorlage zu erstellen.
 - `--instance-id` – Die ID einer einzelnen sbe-Instance.

- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Rechen-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [modify-launch-template](#) – Ändert eine Startvorlage. Sie können angeben, welche Version der Startvorlage als Standardversion festgelegt werden soll. Wenn Sie eine Instance ohne Angabe einer Startvorlagenversion starten, wird die Standardversion der Startvorlage angewendet.

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

- `--launch-template-id string` – Die ID der Startvorlage.
- `--launch-template-name string` – Ein Name für die Startvorlage.
- `--default-version string` – Die Versionsnummer der Startvorlage, die als Standardversion festgelegt werden soll.
- `--endpoint snowballEndpoint` – Ein Wert, mit dem Sie Ihre Rechen-Instances mithilfe von Amazon EC2-API-Operationen programmgesteuert verwalten können. Weitere Informationen finden Sie unter [Angeben des AmazonEC2-compatible Endpunkts als AWS CLI Endpunkt](#).
- [modify-instance-attribute](#) – Ändert ein Attribut der angegebenen Instance. Folgende Attribute werden unterstützt:
 - `instanceInitiatedShutdownBehavior`
 - `userData`
- [revoke-security-group-egress](#) – Entfernt eine oder mehrere Ausgangsregeln aus einer Sicherheitsgruppe:
 - `[--group-id value]` – Die ID der Sicherheitsgruppe
 - `[--ip-permissions value]` – Ein oder mehrere Sätze von IP-Berechtigungen.
- [revoke-security-group-ingress](#) – Widerruft eine oder mehrere Eingangsregeln für eine Sicherheitsgruppe. Wenn Sie `revoke-security-group-ingress` aufrufen, müssen Sie entweder für `group-name` oder für `group-id` einen Wert angeben.
 - `[--group-name value]` – Der Name der Sicherheitsgruppe.
 - `[--group-id value]` – Die ID der Sicherheitsgruppe.
 - `[--ip-permissions value]` – Ein oder mehrere Sätze von IP-Berechtigungen.
 - `[--protocol value]` Das IP-Protokoll. Mögliche Werte sind `tcp`, `udp` und `icmp`. Das Argument `--port` ist erforderlich, es sei denn, es wird der Wert "alle Protokolle" (-1) angegeben.
 - `[--port value]` – Für TCP oder UDP der Bereich der zuzulassenden Ports. Eine einzelne

Ganzzahl oder ein Bereich (Minimum–Maximum).

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

- `[--cidr value]` – Der CIDR-IP-Bereich.
- [run-instances](#) – Startet eine Reihe von Datenverarbeitungs-Instances mithilfe einer Snowcone-AMI-ID für ein AMI.

Note

Je nach Größe und Typ der Instance kann es bis zu einer halben Stunde dauern, bis eine Rechen-Instance auf einem Snowcone-Gerät gestartet wird.

- `[-- --block-device-mappings (list)]` Die Blockgerät-Zuweisungseinträge. 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 Aufrufen von `describe-images` erhalten können. Um eine Instance zu starten, wird ein AMI benötigt.

- -- InstanceInitiatedShutdownBehavior – Wenn Sie ein Herunterfahren Ihrer Instance einleiten (mit einem Befehl wie Herunterfahren oder Ausschalten), wird die Instance standardmäßig angehalten. Sie können das Verhalten stattdessen ändern, sodass sie beendet wird. Die Parameter `stop` und `terminate` werden unterstützt. Der Standardwert ist `stop`. Weitere Informationen finden Sie unter [Ändern des von der Instance initiierten Herunterfahrverhaltens](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.
- --instance-type – Der sbe-Instance-Typ.
- --launch-template structure – Die Startvorlage, die zum Starten der Instances verwendet werden soll. Alle Parameter, die Sie im Befehl `run-instances` angeben, überschreiben die entsprechenden Parameter in der Startvorlage. Sie können den Namen oder die ID einer Einführungsvorlage angeben, jedoch nicht beides.

```
{
  "LaunchTemplateId": "string",
  "LaunchTemplateName": "string",
  "Version": "string"
}
```

- -- security-group-ids – Eine oder mehrere Sicherheitsgruppen-IDs. Sie können eine Sicherheitsgruppe mit erstellen [CreateSecurityGroup](#). Wenn kein Wert angegeben wird, wird die ID für die Standard-Sicherheitsgruppe den erstellten Instances zugewiesen.
- --tag-specifications – Die Tags, die während des Starts auf die Ressourcen angewendet werden sollen. Instances können nur beim Start markiert werden. Die angegebenen Tags werden auf alle Instances angewendet, die beim Start erstellt werden. Um eine Ressource mit einem Tag zu versehen, nachdem sie erstellt wurde, verwenden Sie `create-tags`.
- --user-data – Die Benutzerdaten, die der Instance zur Verfügung gestellt werden sollen. Wenn Sie die verwenden AWS CLI, wird die Base64-Codierung 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 Instance, die Sie zuvor angehalten haben. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.
 - --instance-ids – Die IDs einer oder mehrerer sbe-Instances, die auf dem Gerät gestoppt wurden.
- [stop-instances](#) – Stoppt eine ausgeführte sbe Instance. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Sie werden jedoch gelöscht, wenn die Instance beendet wird.

- `--Instance-IDs`: Die IDs einer oder mehrerer sbe-Instances, die auf dem Gerät gestoppt werden sollen.
- [terminate-instances](#) – Fahren Sie eine oder mehrere Instances herunter. Dieser Vorgang ist idempotent. Wenn Sie eine Instance mehr als einmal beenden, ist jeder Aufruf erfolgreich. Alle der Instance zugeordneten Ressourcen bleiben beim Starten und Stoppen erhalten. Die Daten werden jedoch gelöscht, wenn die Instance beendet wird.

Note

Wenn Sie einen Befehl wie `shutdown` oder `poweroff` zum Starten des Herunterfahrens über Ihre Instance verwenden, wird die Instance standardmäßig angehalten. Sie können jedoch das `InstanceInitiatedShutdownBehavior` Attribut verwenden, um dieses Verhalten so zu ändern, dass diese Befehle Ihre Instance beenden. Weitere Informationen finden Sie unter [Ändern des von der Instance initiierten Herunterfahrverhaltens](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.

- `--instance-ids` – Die IDs einer oder mehrerer sbe Instances, die auf dem Gerät beendet werden sollen. Alle für diese Instances gespeicherten Daten gehen verloren.

Unterstützte Amazon EC2-API-Operationen


Im Folgenden finden Sie Amazon EC2-API-Operationen, die Sie mit einem Snowcone-Gerät verwenden können, mit Links zu ihren Beschreibungen in der Amazon EC2-API-Referenz. Amazon EC2-API-Aufrufe erfordern Signature Version 4 (SigV4)-Signatur. Wenn Sie die AWS CLI oder ein AWS SDK verwenden, um diese API-Aufrufe durchzuführen, wird die SigV4-Signatur für Sie übernommen. 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 für die 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 Aufruf `AuthorizeSecurityGroupIngress` müssen Sie einen Wert für `GroupName` oder `groupName` angeben.
- [CreateVolume](#) – Die folgenden Anforderungsparameter werden unterstützt:
 - `SnapshotId`
 - `Size`
 - `VolumeType`
 - `TagSpecification.N`
- [CreateLaunchTemplate](#) – Die folgenden Anforderungsparameter werden unterstützt:
 - `ImageId`
 - `InstanceType`
 - `SecurityGroupIds`
 - `TagSpecifications`
 - `UserData`
- [CreateLaunchTemplateVersion](#)
- [CreateTags](#) – Die folgenden Anforderungsparameter werden unterstützt:
 - `AMI`
 - `Instance`
 - `Launch template`
 - `Security group`
- [CreateSecurityGroup](#) – Erstellt eine Sicherheitsgruppe in 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 Ergebnissatz abzurufen.
- [DescribeTags](#) – Mit diesem Befehl werden die folgenden Filter unterstützt:
 - resource-id
 - resource-type – Nur AMI oder Rechen-Instance
 - key
 - value
- [DescribeVolume](#) – Die folgenden Anforderungsparameter werden unterstützt:
 - MaxResults
 - NextToken
 - VolumeId.N
- [DetachVolume](#) – Die folgenden Anforderungsparameter werden unterstützt:
 - Device
 - InstanceId
 - VolumeId
- [DisassociateAddress](#)

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

 Note

Je nach Größe und Typ der Instance kann es bis zu einer halben Stunde dauern, bis eine Rechen-Instance auf einem Snowcone gestartet wird.

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


Automatisches Starten von Amazon EC2-compatible Instances mit Startvorlagen

Sie können Ihre AmazonEC2-compatible Instances automatisch auf Ihrem AWS Snowcone Gerät mithilfe von Startvorlagen und Snowball-Edge-Client-Startkonfigurationsbefehlen starten. Wenn eine Instance beendet wird, startet der Autostart sie. Wenn Sie 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 AmazonEC2-compatible 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-compatible Instance auf Snowcone starten.

Wenn Sie Autostart-Konfigurationen auf Ihrem Snowcone verwenden, konfigurieren Sie die Parameter, mit denen Ihre AmazonEC2-compatible Instance beginnen soll. Nachdem Ihr Snowcone

konfiguriert wurde, verwendet es beim Neustart und Entsperren Ihre Autostart-Konfiguration, um eine Instance mit den von Ihnen angegebenen Parametern zu starten. Wenn eine von Ihnen mithilfe einer Autostart-Konfiguration gestartete Instance angehalten wird, wird die Instance ab dem Moment ausgeführt, in dem Sie Ihr Gerät entsperren.


 Note

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

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

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


1. Wenn Sie Ihr AWS Snowcone Gerät bestellen, erstellen Sie einen Auftrag, um ein Snow Family-Gerät mit Rechen-Instances zu bestellen. Weitere Informationen finden Sie unter [Anlegen eines Auftrags mit Datenverarbeitungs-Instances](#).
2. Nachdem Sie Ihr Snowcone erhalten haben, entsperren Sie es.
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-compatible AWS CLI Befehle auf einem Snowcone](#).

 Note

Der Amazon EC2-Endpunkt ist der Geräteendpunkt.

4. Verwenden Sie den Snowball Edge-Client-Befehl `snowballEdge create-autostart-configuration`, um Ihre EC2-compatible Startvorlage an Ihre Netzwerkkonfiguration zu binden. Weitere Informationen finden Sie unter [Erstellen einer Startkonfiguration zum automatischen Starten von Amazon EC2-compatible Instances](#).
5. Starten Sie Ihr AWS Snowcone Gerät neu und entsperren Sie es dann. Ihre EC2-compatible Instances werden automatisch mit den Attributen gestartet, die in Ihrer Startvorlage und Ihrem Snowcone-Clientbefehl angegeben sind `create-autostart-configuration`.

Um den Status Ihrer ausgeführten Instances anzuzeigen, verwenden Sie den EC2-API-Befehl `describe-autostart-configurations`.


 Note

Es gibt keine Konsolen- oder Auftragsverwaltungs-API zur AWS Snowball Unterstützung für das Starten von Vorlagen. Sie verwenden EC2- und Snowball Edge-Client-CLI-Befehle, um EC2-compatible Instances automatisch auf Ihrem AWS Snowcone Gerät zu starten.

Verwenden von Block Storage mit Ihren Amazon EC2-compatible Instances

Mit Blockspeicher auf Snowcone können Sie Blockspeicher je nach den Anforderungen Ihrer Anwendungen hinzufügen oder entfernen. Volumes, die an eine Amazon EC2-compatible Instance angefügt sind, werden als Speicher-Volumes bereitgestellt, die unabhängig von der Lebensdauer der Instance bestehen bleiben. Sie können den Blockspeicher mit der vertrauten Amazon EBS-API verwalten.

Bestimmte Amazon-EBS-Befehle werden mithilfe des EC2-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-compatible AWS CLI Befehle auf einem Snowcone](#).

 Important

Stellen Sie sicher, dass Sie das Mounting aller Dateisysteme auf dem Gerät in Ihrem Betriebssystem aufheben, bevor Sie das Volume trennen. Andernfalls kann es zu Datenverlusten kommen.

Im Folgenden finden Sie Amazon-EBS-Volume-Kontingente und Unterschiede zwischen Amazon-EBS-Volumes auf Ihrem AWS Snowcone Gerät und Amazon-EBS-Volumes in der Cloud:

- Amazon EBS-Volumes sind nur für EC2-compatible Instances verfügbar, die auf dem AWS Snowcone Gerät ausgeführt werden, auf dem die Volumes gehostet werden.
- Volume-Typen sind entweder auf kapazitätsoptimierte HDD (sbg1) oder leistungsoptimierte SSD (sbp1) beschränkt. Der Standard-Volume-Typ ist sbg1.

- Amazon 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.
- Es können bis zu 10 Amazon EBS-Volumes an eine einzelne EC2-compatible Instance angefügt werden.
- Es gibt keine formelle Begrenzung für die Anzahl der Amazon-EBS-Volumes, die Sie auf Ihrem AWS Snowcone Gerät haben können. Die Gesamtkapazität des Amazon-EBS-Volumes ist jedoch durch den verfügbaren Speicherplatz auf Ihrem AWS Snowcone Gerät begrenzt.

Sicherheitsgruppen in Snow Devices

Eine Sicherheitsgruppe agiert als virtuelle Firewall, die den Datenverkehr für eine oder mehrere Instances steuert. Beim Start einer Instance verknüpfen Sie diese mit mindestens einer Sicherheitsgruppe. Sie können jeder Sicherheitsgruppe Regeln hinzufügen, um den Datenaustausch mit den ihr zugeordneten Instances zu ermöglichen. Weitere Informationen finden Sie unter [Amazon EC2-Sicherheitsgruppen für Linux-Instances](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Sicherheitsgruppen in Snowcone-Geräten ähneln Sicherheitsgruppen in der AWS Cloud. Virtual Private Clouds (VPCs) werden auf Snowcone-Geräten nicht unterstützt.

Im Folgenden finden Sie die anderen Unterschiede zwischen Snowcone-Sicherheitsgruppen und EC2-VPC-Sicherheitsgruppen:

- Jedes 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.

- Es werden nur die Parameter unterstützt, die für AWS CLI Aktionen und API-Aufrufe aufgeführt sind. 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-compatible AWS CLI Befehle auf einem Snowcone](#). Weitere Informationen zu unterstützten API-Operationen finden Sie unter [Unterstützte Amazon 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 Instance-Metadatenkategorien für Ihre Datenverarbeitungs-Instances. Weitere Informationen dazu finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Die folgenden Kategorien werden unterstützt. Bei Verwendung anderer Kategorien wird eine 404 Fehlermeldung zurückgegeben.

Unterstützte Instance-Metadatenkategorien auf einem Snowcone

Daten	Beschreibung
<code>ami-id</code>	Die für den Start der Instance verwendete AMI-ID
<code>hostname</code>	Der private IPv4-DNS-Hostname der Instance.
<code>instance-id</code>	Die ID dieser Instance
<code>instance-type</code>	Der Typ der Instance.
<code>local-hostname</code>	Der private IPv4-DNS-Hostname der Instance.
<code>local-ipv4</code>	Die private IPv4-Adresse der Instance.
<code>mac</code>	Die Media Access Control-Adresse (MAC) der Instance.

Daten	Beschreibung
<code>network/interfaces/macs/</code> <i>mac</i> / <code>local-hostname</code>	Der lokale Hostname der Schnittstelle
<code>network/interfaces/macs/</code> <i>mac</i> / <code>local-ipv4s</code>	Die privaten IPv4-Adressen, die mit der Netzwerkschnittstelle verknüpft sind
<code>network/interfaces/macs/</code> <i>mac</i> / <code>mac</code>	Die MAC-Adresse der Instance
<code>network/interfaces/macs/</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 Instance-Datenkategorien 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 Instance-Identitätsdokumente im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Ändern von Benutzerdaten in Snowcone Compute Instances

Benutzerdaten werden für die Verwendung mit Shell-Skripten für Rechen-Instances 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. Halten Sie Ihre Rechen-Instance mit dem `stop-instances` AWS CLI Befehl an.
2. Ändern Sie das `userData` Attribut mit dem `modify-instance-attribute` AWS CLI Befehl .
3. Starten Sie Ihre Computing-Instance mit dem `start-instances` AWS CLI Befehl neu.

Es werden nur Shell-Skripts mit Datenverarbeitungs-Instances unterstützt. Es gibt keine Unterstützung für `cloud-init` Paketdirektiven auf Datenverarbeitungs-Instances, die auf einem Snowcone ausgeführt werden. Weitere Informationen zum Arbeiten mit AWS CLI Befehlen finden Sie in der [AWS CLI -Befehlsreferenz](#).

Fehlerbehebung bei Datenverarbeitungs-Instances auf Snowcone-Geräten

Im Folgenden finden Sie Tipps zur Fehlerbehebung für Snowcone-Aufträge mit Datenverarbeitungs-Instances.

Themen

- [Die virtuelle Netzwerkschnittstelle hat die IP-Adresse 0.0.0.0](#)
- [Snowcone hängt beim Starten einer großen Datenverarbeitungs-Instance ab](#)
- [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 verfügt über zwei RJ45-Schnittstellen. Möglicherweise geben Sie die falsche physische Schnittstelle an.

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 Datenverarbeitungs-Instance ab

Es kann so aussehen, als ob Ihr Snowcone das Starten einer Instance beendet hat. Dies ist im Allgemeinen nicht der Fall. Es kann jedoch eine Stunde oder länger dauern, bis große Datenverarbeitungs-Instances gestartet werden. Sie können den Status Ihrer Instances überprüfen, indem Sie den AWS CLI Befehl verwenden, der für den HTTP- oder HTTPS-Amazon EC2-Endpunkt auf Snowcone `aws ec2 describe-instances` ausgeführt wird.

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. Der DataSync 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 [Automatisches Konfigurieren der NFS-Schnittstelle](#) und [Starten von NFS und Einschränken des Zugriffs](#).

Der DataSync Agent ist während der Snowcone-Auftragsvorbereitung als AMI auf Ihrem Snowcone-Gerät vorinstalliert. Um Daten online zu übertragen, 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 Geräte-neustart 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 DataSyncAufgabenkontingente](#) 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.

Verwalten der NFS-Schnittstelle

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

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

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

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

Note

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

Sie können die NFS-Schnittstelle auch mit [AWS OpsHub](#), einem GUI-Tool, konfigurieren und verwalten. Weitere Informationen finden Sie unter [mit NFS für Offline-Dateiübertragung](#).

NFS-Konfiguration für Snow Family-Geräte

Die NFS-Schnittstelle wird standardmäßig nicht auf dem Snow Family-Gerät ausgeführt, daher müssen Sie sie starten, um die Datenübertragung auf das Gerät zu aktivieren. Sie können die NFS-Schnittstelle konfigurieren, indem Sie die IP-Adresse einer Virtual Network Interface (VNI) angeben, die auf dem Snow Family-Gerät ausgeführt wird, und den Zugriff auf Ihre Dateifreigabe

bei Bedarf einschränken. Bevor Sie die NFS-Schnittstelle konfigurieren, richten Sie eine virtuelle Netzwerkschnittstelle (VNI) auf Ihrem Snow Family-Gerät ein. Weitere Informationen finden Sie unter [Netzwerkconfiguration für Datenverarbeitungs-Instances](#).

Konfigurieren von Snow Family-Geräten für die NFS-Schnittstelle

- Verwenden Sie den `describe-service` Befehl, um festzustellen, ob die NFS-Schnittstelle aktiv ist.

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

Der Befehl gibt den Status des NFS-Service `ACTIVE` oder zurück `INACTIVE`.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  }
}
```

Wenn der Wert des `State` Namens lautet `ACTIVE`, ist der NFS-Schnittstellenservice aktiv und Sie können das NFS-Volume des Snow-Family-Geräts mounten. Weitere Informationen finden Sie unter

[Nachdem die NFS-Schnittstelle gestartet wurde, mounten Sie den Endpunkt als lokalen Speicher auf Client-Computern.](#)

[Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und macOS-Betriebssysteme aufgeführt.](#)

- **Windows:**

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

- Linux:

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

- macOS:

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

. Wenn der Wert ist INACTIVE, müssen Sie den Service starten.

Starten des NFS-Service auf dem Snow Family-Gerät

Starten Sie bei Bedarf eine virtuelle Netzwerkschnittstelle (VNI) und starten Sie dann den NFS-Service auf dem Snow Family-Gerät. Geben Sie bei Bedarf beim Starten des NFS-Service einen Block zulässiger Netzwerkadressen an. Wenn Sie keine Adressen angeben, ist der Zugriff auf die NFS-Endpunkte uneingeschränkt.

1. Verwenden Sie den `describe-virtual-network-interface` Befehl, um die auf dem Snow Family-Gerät verfügbaren VNIs anzuzeigen.

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

Wenn eine oder mehrere VNIs auf dem Snow Family-Gerät aktiv sind, gibt der Befehl Folgendes zurück.

```
snowballEdge describe-virtual-network-interfaces  
[  
  {  
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/  
s.ni-8EXAMPLE8EXAMPLE8",  
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
```

```

    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45"
  },{
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/
s.ni-1EXAMPLE1EXAMPLE1",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.2",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "12:34:5E:XA:MP:LE"
  }
]

```

Notieren Sie sich den Wert des `VirtualNetworkInterfaceArn` Namens der VNI, die mit der NFS-Schnittstelle verwendet werden soll.

2. Wenn keine VNIs verfügbar sind, verwenden Sie den `create-virtual-network-interface` Befehl , um eine VNI für die NFS-Schnittstelle zu erstellen. Weitere Informationen finden Sie unter [Einrichten einer virtuellen Netzwerkschnittstelle \(VNI\)](#).
3. Verwenden Sie den `start-service` Befehl , um den NFS-Service zu starten und ihn der VNI zuzuordnen. Um den Zugriff auf die NFS-Schnittstelle einzuschränken, fügen Sie die `AllowedHosts` Parameter `service-configuration` und in den Befehl ein.

```

snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id
nfs --service-configuration AllowedHosts=CIDR-address-range

```

4. Verwenden Sie den `describe-service` Befehl , um den Servicestatus zu überprüfen. Es wird ausgeführt, wenn der Wert des State Namens ist `ACTIVE`.

```

snowballEdge describe-service --service-id nfs

```


Der Befehl gibt den Servicestatus sowie die IP-Adresse und Portnummer des NFS-Endpunkts und der CIDR-Bereiche zurück, die auf den Endpunkt zugreifen dürfen.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Endpoints" : [ {
    "Protocol" : "nfs",
    "Port" : 2049,
    "Host" : "192.0.2.0"
  } ],
  "ServiceConfiguration" : {
    "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]
  }
}
```

Mounten von NFS-Endpunkten auf Client-Computern

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

Im Folgenden sind die Standard-Mount-Befehle für Windows-, Linux- und macOS-Betriebssysteme aufgeführt.

- Windows:

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

- Linux:

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

- macOS:

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

Anhalten der NFS-Schnittstelle

Wenn Sie mit der Übertragung von Dateien über die NFS-Schnittstelle fertig sind und bevor Sie das Snow Family-Gerät ausschalten, verwenden Sie den `stop-service` Befehl, um den NFS-Service zu beenden.

```
snowballEdge stop-service --service-id nfs
```

Benutzen AWS IoT Greengrassum vorinstallierte Software auf Amazon EC2-kompatiblen Instances auszuführen

AWS IoT Greengrass ist ein Open-Source-Edge-Runtime- und Cloud-Service für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können. Sie können Folgendes verwenden AWS IoT Greengrassum Software zu entwickeln, die es Ihren Geräten ermöglicht, lokal auf die von ihnen generierten Daten zu reagieren, Vorhersagen auf der Grundlage von Modellen für maschinelles Lernen durchzuführen und Gerätedaten zu filtern und zu aggregieren. Für detaillierte Informationen über AWS IoT Greengrass, siehe [Was ist AWS IoT Greengrass?](#) in der AWS IoT Greengrass Version 2 Leitfaden für Entwickler.

Durch die Verwendung von 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.

Richten Sie Ihre Amazon EC2-kompatible Instance ein

Note

Um zu installieren AWS IoT Greengrass Version 2 Stellen Sie auf einem Snow Family-Gerät sicher, dass Ihr Gerät mit dem Internet verbunden ist. Nach der Installation ist kein Internet erforderlich, damit ein Snow Family-Gerät verwendet werden kann AWS IoT Greengrass.

Um eine EC2-kompatible Instanz einzurichten für AWS IoT Greengrass V2

1. Starten Sie den AWS IoT Greengrass validiertes AMI mit einer öffentlichen IP-Adresse und einem SSH-Schlüssel:
 - a. Unter Verwendung des AWS CLI: [Instanzen ausführen](#).
 - b. Verwenden AWS OpsHub: [Starten einer Amazon EC2-kompatiblen Instance](#).

Note

Notieren Sie sich die öffentliche IP-Adresse und den Namen des SSH-Schlüssels, die der Instanz zugeordnet sind.

2. Stellen Sie mithilfe von SSH eine Verbindung zur EC2-kompatiblen Instance her. Führen Sie dazu den folgenden Befehl auf dem Computer aus, der mit Ihrem Gerät verbunden ist. Ersetzen *SSH-Schlüssel* mit dem Schlüssel, mit dem Sie die EC2-kompatible Instance gestartet haben. Ersetzen *public-ip-address* durch die öffentliche IP-Adresse der EC2-kompatiblen Instance.

```
ssh -i ssh-key ec2-user@ public-ip-address
```

Important

Wenn Ihr Computer eine frühere Version von Microsoft Windows verwendet, verfügen Sie möglicherweise nicht über den SSH-Befehl, oder Sie haben SSH, können aber keine Verbindung zu Ihrer EC2-kompatiblen Instance herstellen. Um eine Verbindung zu Ihrer EC2-kompatiblen Instance herzustellen, können Sie PuTTY installieren und konfigurieren. Dabei handelt es sich um einen kostenlosen Open-Source-SSH-Client.

Sie müssen den SSH-Schlüssel konvertieren von .pem-formatieren Sie in das PuTTY-Format und stellen Sie eine Verbindung zu Ihrer EC2-Instance her. Für Anweisungen zur Konvertierung von .pem in das PuTTY-Format finden Sie unter [Konvertieren Sie Ihren privaten Schlüssel mit PuTTYgen](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Installieren von AWS IoT Greengrass

Als Nächstes richten Sie Ihre EC2-kompatible Instance als AWS IoT Greengrass Kerngerät, das Sie für die lokale Entwicklung verwenden können.

So installieren Sie AWS IoT Greengrass

1. Verwenden Sie den folgenden Befehl, um die erforderliche Software für zu installieren AWS IoT Greengrass. Dieser Befehl installiert den 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 Erlaubnis, das auszuführen AWS IoT Greengrass Software und ändern Sie die Root-Rechte von `root ALL=(ALL) ALL` zu `root ALL=(ALL:ALL) ALL` in der Sudoers-Konfigurationsdatei.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Verwenden Sie den folgenden Befehl, um das herunterzuladen AWS IoT Greengrass Kernsoftware.

```
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 bereitzustellen AWS IoT Greengrass Kernsoftware. 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 im AWS-Region, nicht das Snow Family-Gerät.

5. Verwenden Sie den folgenden Befehl, um das zu installieren AWS IoT Greengrass Kernsoftware. 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`: Das AWS-Region, in der Ressourcen gesucht oder erstellt werden sollen.
- `MyGreengrassCore`: Der Name des AWS IoT Ding für dein AWS IoT Greengrass Kerngerät.
- `MyGreengrassCoreGroup`: Der Name des AWS IoT Dinggruppe für deine 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 Sie das AWS IoT Greengrass Kernsoftware](#).

Wenn du fertig bist, wirst du eine haben AWS IoT Greengrass Core läuft auf Ihrem Snow Family-Gerät für Ihren lokalen Gebrauch.

Für die Nutzung der AWS Dienste auf einem AWS Snowcone Gerät erforderliche Ports

Damit AWS Dienste auf einem AWS Snowcone Gerät ordnungsgemäß funktionieren, müssen Sie die Netzwerkports für den Dienst zulassen.

Im Folgenden finden Sie eine Liste der Netzwerkports, die für jeden AWS Dienst erforderlich sind.

Port	Protocol (Protokoll)	Kommentar
22	SSH	Gerätezustandsprüfung und für EC2 SSH
2049	NFS	NFS-Endpunkt
808	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. 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 [Versandüberlegungen für AWS Snowcone](#).

Auftragstypbezogene Überlegung

Important

Wenn Sie Daten importieren, löschen Sie Ihre lokalen Kopien der übertragenen Daten erst nach dem Import in AWS, wenn am Ende des Vorgangs erfolgreich und Sie können die Ergebnisse der Datenübertragung überprüfen.

Note

Sobald Sie das Snow-Gerät für den Import in Amazon S3 zurückgegeben haben, beginnt AWS 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 auf sichere Weise. 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 [Versandüberlegungen für AWS Snowcone](#).

Schutz von Daten auf Ihrem Gerät

Berücksichtigen Sie die folgenden Empfehlungen, um die Daten auf Ihrem AWS Snowcone Gerät zu schützen.

Themen

- [Sichern Ihres AWS Snowcone](#)
- [Validieren von NFC-Tags](#)

Sichern Ihres AWS Snowcone

Im Folgenden finden Sie einige Sicherheitspunkte, die Sie bei der Verwendung von Snowcone berücksichtigen 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 Schutzausrüstung aufweist, kann das Wetter die stärkste Hardware beschädigen. Melden Sie gestohlene, vermisste oder defekte Geräte so schnell wie möglich. Je schneller ein Problem mit einer Appliance gemeldet wird, umso zügiger kann ein Ersatz versendet werden, um Ihren Auftrag abzuschließen.

Note

Das Snowcone-Gerät ist die Eigenschaft von AWS. Die Überschreitung eines Geräts stellt einen Verstoß gegen die Richtlinie AWS für zulässige Nutzung dar. Weitere Informationen finden Sie unter <http://aws.amazon.com/aup/>.

Wir führen die folgenden Sicherheitsschritte durch:

- Beim Übertragen von Daten über die Dateischnittstelle bleiben Objektmetadaten erhalten.
- Wenn ein Gerät bei eintrittAWS, untersuchen wir es auf Anzeichen von Manipulationen und stellen sicher, dass vom Trusted Platform Module (TPM) keine Änderungen erkannt wurden. Snowcone verwendet mehrere Sicherheitsebenen, die zum Schutz Ihrer Daten entwickelt wurden, darunter manipulationsichere Umschließungen, 256-Bit-Verschlüsselung und ein branchenübliches TPM, das sowohl Sicherheit als auch vollständige Schutzkette für Ihre Daten bietet.
- Nachdem der Datenübertragungsauftrag verarbeitet und verifiziert wurde, AWS führt eine Softwarelöschung des Snowcone-Geräts gemäß den Richtlinien des National Institute of Standards and Technology (NIST) für die Medienbereinigung durch.

Validieren von NFC-Tags

AWS Snowcone -Geräte verfügen über in sie integrierte microSD-Tags. 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 microSD-Tags umfasst die Verwendung des Snowball Edge-Clients zum Generieren eines gerätespezifischen QR-Codes, um zu überprüfen, ob die von Ihnen gescannten Tags für das richtige Gerät bestimmt sind. Weitere Informationen finden Sie unter [Anfordern Ihres QR-Codes für die NFC-Validierung](#).

Im folgenden Verfahren wird beschrieben, wie Sie die microSD-Tags auf einem Snowcone-Gerät validieren. Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden ersten Schritte der Übung „Erste Schritte“ ausgeführt haben:

1. Erstellen des ersten Auftrags Weitere Informationen finden Sie unter [Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts](#).
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 [Verwenden des AWS Snowball Edge Clients](#).

So validieren Sie die microSD-Tags in einem -AWS SnowconeGerät

1. Führen Sie den `snowballEdge get-app-qr-code` Snowball Edge-Clientbefehl 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 microSD-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 Probleme weiterhin bestehen, wenden Sie sich an [AWS Support](#).

VerständnisAWS SnowconeJobstatus

Wenn Sie eine erstellenAWS SnowconeDer Job durchläuft den Jobstatus und der Status wird auf derManagementkonsole für die AWS Snow-Familie.

Um den Status eines Jobs zu sehen

1. Loggen Sie sich in [Managementkonsole für die AWS Snow-Familie](#).
2. Auf derJob-Dashboard, wähle 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 IhreAWS Snow Familybeauftragen und Daten vom Gerät löschen.

AWS SnowconeStatus der Geräte-Jobs

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	AWSbereitet ein Gerät für Ihren Job vor.
Preparing shipment	AWSbereitet 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 nachAWS	Sie haben das Gerät zurückgeschickt anAWS.
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.
BeiAWS	Ihre Sendung ist eingetroffen amAWS. Wenn Sie Daten importieren, beginnt der Import in der Regel innerhalb eines Tages nach Ankunft der Sendung.
Importing	AWSimportiert 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 zur Ausführung von Aktionen hat. Decrypt GenerateDataKey Darüber hinaus können die Richtlinien von AWS -verwalteten KMS-Schlüsseln nicht bearbeitet werden.

So aktivieren Sie die serverseitige Verschlüsselung für ein SNS-Thema mithilfe der Amazon SNS SNS-Managementkonsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Wählen Sie im Navigationsbereich Topics (Themen) aus.
3. Wählen Sie auf der Themenseite das Thema aus, das für Benachrichtigungen zur Änderung des Jobstatus verwendet wird, und klicken Sie dann auf Bearbeiten.
4. Erweitern Sie den Abschnitt Encryption (Verschlüsselung) und gehen Sie wie folgt vor:
 - a. Wählen Sie Enable encryption (Verschlüsselung aktivieren) aus.
 - b. Geben Sie den AWS KMS-Schlüssel an. Siehe
 - c. Für jeden KMS-Typ werden die Beschreibung, das Konto und der KMS-ARN angezeigt.
5. Um einen benutzerdefinierten Schlüssel aus Ihrem AWS Konto zu verwenden, wählen Sie das Feld AWSKMS-Schlüssel und dann den benutzerdefinierten KMS-KMS aus der Liste aus. Anweisungen zum Erstellen eines benutzerdefinierten KMS finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Um einen benutzerdefinierten KMS-ARN von Ihrem AWS Konto oder einem anderen AWS Konto zu verwenden, geben Sie den KMS-Schlüssel-ARN in das Feld AWSKMS-Schlüssel ein.

6. Wählen Sie Änderungen speichern aus. Die serverseitige Verschlüsselung ist für Ihr Thema aktiviert und die Themenseite wird angezeigt.

Einrichtung einer vom Kunden verwalteten KMS-Schlüsselrichtlinie

Nachdem Sie die Verschlüsselung für SNS-Themen aktiviert haben, die Benachrichtigungen über Änderungen des Snow-Auftragsstatus erhalten, aktualisieren Sie die KMS-Richtlinie für die SNS-Themenverschlüsselung und lassen Sie dem Snow-Serviceprinzipal Aktionen "importexport.amazonaws.com" zu. "mks:Decrypt" "mks:GenerateDataKey*"

Um die Dienstrolche Import und Export in der KMS-Schlüsselrichtlinie zuzulassen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Key Management Service (AWS KMS)-Konsole unter <https://console.aws.amazon.com/kms>.
2. Wenn Sie die AWS-Region ändern möchten, verwenden Sie die Regionauswahl in der oberen rechten Ecke der Seite.

3. Ändern Sie in der oberen rechten Ecke der Konsole den Namen AWS-Region der Konsole auf dieselbe Region, in der das Snow-Gerät bestellt wurde.
4. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
5. Wählen Sie in der Liste der KMS-Schlüssel den Alias oder die Schlüssel-ID des KMS-Schlüssels aus, der aktualisiert werden soll.
6. Wählen Sie die Registerkarte Schlüsselrichtlinie. In den wichtigsten Richtlinienanweisungen können Sie die Prinzipale sehen, denen durch die Schlüsselrichtlinie Zugriff auf den KMS-Schlüssel gewährt wurde, und Sie können sehen, welche Aktionen sie ausführen können.
7. Fügen Sie für den Snow Service Principal "importexport.amazonaws.com" die folgenden Richtlinien "kms:Decrypt" und "kms:GenerateDataKey*" Aktionen hinzu:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "service.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:service:region:customer-account-id:resource-type/
customer-resource-id"
    }
  },
  "StringEquals": {
    "kms:EncryptionContext:aws:sns:topicArn": "arn:aws:sns:your_region:customer-
account-id:your_sns_topic_name"
  }
}
```

8. Wählen Sie Änderungen speichern, um die Änderungen zu übernehmen und den Policy-Editor zu beenden.

SNS-Benachrichtigungsbeispiele

Amazon SNS SNS-Benachrichtigungen erzeugen die folgenden E-Mail-Nachrichten, wenn sich Ihr Jobstatus ändert. Diese Nachrichten sind Beispiele für das Email-JSON SNS-Themenprotokoll.

Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können.

SNS-Benachrichtigung (JSON)

Job created

```
{
  "Type" : "Notification",
  "MessageId" : "dc1e94d9-56c5-5e9
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" : "dc1e94d9-56c5-5e9
6-808d-cc7f68faa162",
  "TopicArn" : "arn:aws:sns:us-ea
st-2:111122223333:ExampleTopic1",
  "Message" : "Your job Job-name
(JID8bca334a-6c2f-4cd0-97e2
-3f5a4dc9bd6d) is being prepared.
More info - https://console.aw
s.amazon.com/importexport",
  "Timestamp" : "2023-02-23T00:27:
58.831Z",
  "SignatureVersion" : "1",
  "Signature" : "FMG5t1ZhJNHLHUXvZ
gtZz1k24FzVa7oX0T4P03neeXw8
ZEXZx6z35j2F0TuNYShn2h0bKNC/
zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ
F+4uWHEE73yDVR4SyYAIkP9jstZzDRm
+bcVs8+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)

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
+1bZkLd0ZdtdRJIiYPRP44eyq78sU0Eo/
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 Managementkonsole für die AWS Snow-Familie oder die Job Management API (JMAPI) bestellen.

Verstehen der Ablaufverfolgung.

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 für den Import oder Export von Daten innerhalb der AWS Region verwendet werden, in der die Geräte bestellt wurden.

Rückgabe eines Snowcone-Geräts

Die Prepaid-Versandinformationen auf dem E-Ink-Display enthalten die korrekte Adresse für die Rücksendung des Geräts. Informationen dazu, wie Sie Ihr Snowcone-Gerät zurückgeben, 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

Sofern nicht persönlich anders angewiesen AWS, kleben Sie kein separates Versandetikett auf dem Snowcone-Gerät. Verwenden Sie immer das Versandetikett, das auf dem E-Ink-Display des Geräts angezeigt wird.

Verwendung der AWS Management Console

Sie können ein Snowcone-Gerät mit der Managementkonsole für die AWS Snow-Familie aus.

Den Snowcone von der Konsole aus bestellen

Eine Schritt-für-Schritt-Anleitung zur Bestellung eines Snowcone finden Sie unter [AWS Snowball-Konsole](#) finden Sie unter [Erste Schritte](#) aus.

Verwenden der Job Management-API

Die API zur Auftragsverwaltung (JMAPI) bietet programmgesteuerten Zugriff auf dieselbe Funktionalität, die in der Managementkonsole für die AWS Snow-Familie aus. Auf diese Weise können Sie die Job-Funktionalität automatisieren. Mithilfe des JMAPI können Sie den Auftragsstatus sehen, Jobs erstellen, die Manifestdatei herunterladen, den Code entsperren und Berichte zum Auftragsabschluss anzeigen. Da die Aufrufe über die API getätigt werden, können Sie diese Aufrufe in eine benutzerdefinierte Anwendung oder ein Web-Frontend integrieren.

Themen

- [Häufige Verwendungen von JMAPI](#)
- [JMAPI Erforderliche Strings](#)
- [JMAPI-Endpoints](#)
- [JMAPI-CLI-Befehle](#)
- [Beispiele](#)

Häufige Verwendungen von JMAPI

- Automatisieren der Bestellung von Snowcone-Geräten
- Herunterladen der Manifestdatei
- Herunterladen der Entsperrdatei
- Auflisten der aktuellen Snowcone-Jobs
- Herunterladen des Snowcone-Auftragsabschlusses

JMAPI Erforderliche Strings

Wenn Sie eine Bestellung über die Job-Management-API aufgeben, verwenden Sie die folgenden erforderlichen Parameter, die in Beispielen dargestellt werden.

```
--job-type
--resources
--address-id
--region
--role-arn
--kms-key-arn
--shipping-option
--device-type
--description
```

JMAPI-Endpoints

API-Endpoint

Um Anrufe an jeden Endpunkt zu tätigen, ist das FormatsnowballEdge.*region*.amazonaws.comaus. Im Folgenden finden Sie einige Beispiele, die Ihnen helfen, die Aufschlüsselung des Endpunkts zu verstehen.

Example

Region	Endpoint
USA Ost (Nord-Virginia)	snowball.us-east-1.amazonaws.com
USA West (Oregon)	snowball.us-west-2.amazonaws.com

JMAPI-CLI-Befehle

Job Management-CLI

Im Folgenden sind die CLI-Aufrufe, die Sie gegen die Job-Management-API tätigen 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 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>
Stornieren von Aufträgen	<code>aws snowball cancel-job --job-id [JOB ID]</code>

Beispiele

Im Folgenden finden Sie Beispiele für Befehle, die Job Management-API verwenden.

Beispiel für KMS JSON-Beispiel

Das folgende JSON-Beispiel ist eine ordnungsgemäß formatierte JSON-Datei für die Verwendung des 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 Adresse erstellen

Die folgenden Beispiele zeigen Ihnen, wie Sie den Befehl zum Erstellen Ihrer Adresse formatieren würden und wie die Antwort lautet, wenn sie 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

```

Das `create-job`-Kommando erstellt einen Importauftrag in der Region US-Ost-1 mit einem Snowcone-Gerät vom Typ `SNC1_SSD`, das eine `T14`-Kapazitätspräferenz mit einer Versandoption `SECOND_DAY` hat.

Exportieren eines AMI zur Verwendung mit Amazon EC2-Aufträgen

Dieser Abschnitt bietet einen Überblick darüber, wie Sie Ihr Amazon Machine Image (AMI) zur Verwendung mit Amazon EC2-compatibles Rechen-Instances auf einem AWS Snowcone-Gerät exportieren.

Themen

- [Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden](#)
- [Erstellen Ihres Auftrags mit der Konsole](#)
- [Erstellen Ihres Auftrags mit der -AWSCLI](#)

Konfigurieren eines AMI für die Verwendung von SSH zum Herstellen einer Verbindung mit Compute-Instances, die auf dem Gerät gestartet werden

Um Secure Shell (SSH) zum Herstellen einer Verbindung mit Ihren Datenverarbeitungs-Instances auf 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 keine Verbindung zu Ihren Instances mit SSH herstellen, wenn Sie Ihr Snowcone-Gerät erhalten.

So fügen Sie einen SSH-Schlüssel einem AMI hinzu

1. Starten Sie eine neue Instance in der AWS Cloud mit einem kompatiblen AMI-Image (siehe <https://docs.aws.amazon.com/snowball/latest/developer-guide/using-ami.html>).

Stellen Sie beim Starten Ihrer Instance sicher, dass die Speichergröße, die Sie der Instance zuweisen, für Ihre spätere Verwendung auf dem Snowcone-Gerät geeignet ist. In der Amazon EC2-Konsole tun Sie dies in Schritt 4: Hinzufügen von Speicher . Eine Liste der unterstützten Größen für Rechen-Instance-Speicher-Volumes auf einem Snowcone finden Sie unter „[ec2-snowcone-limits](#)“.

2. Installieren und konfigurieren Sie die Anwendungen, die Sie auf Snowcone ausführen möchten, und testen Sie, ob sie wie erwartet funktionieren.
3. Erstellen Sie eine Kopie der PEM/PPK-Datei, die Sie für das SSH-Schlüsselpaar zur Erstellung dieser Instance verwendet haben. Speichern Sie diese Datei auf dem Server, den Sie für die Kommunikation mit 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 Ihres Auftrags mit der Konsole

Ihr nächster Schritt besteht darin, einen Auftrag zum Bestellen eines Snow Family-Geräts zu erstellen. Ihr Auftrag kann ein beliebiger Auftragstyp sein, einschließlich eines Clusters. Befolgen Sie mithilfe der [Managementkonsole für die AWS Snow-Familie](#) die Anweisungen unter [Erstellen eines Auftrags zum Bestellen eines Snow-Family-Geräts](#). Wenn Sie die Seite Schritt 3: Geben Sie Auftragsdetails im Assistenten zur Auftragserstellung aufrufen, 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 Auftrag insgesamt bis zu 20 AMIs hinzu, je nach Gerätetyp.
5. Legen Sie Ihren Auftrag wie gewohnt an.

Erstellen Ihres Auftrags mit der -AWSCLI

Sie können Ihren Auftrag auch über die 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 eintrifft und Sie Ihr Gerät entsperren, verwenden Sie den Snowball Edge-Client, um Ihre lokalen Anmeldeinformationen zu erhalten. Weitere Informationen finden Sie unter [Abrufen von Anmeldeinformationen](#).

Versandüberlegungen für AWS Snowcone

Im Folgenden finden Sie Informationen darüber, wie der Versand für ein AWS Snowcone Gerät erfolgt, sowie eine Liste, in der jedes aufgeführt ist, AWS-Region das unterstützt wird. Die Versandrate, die Sie für einen Auftrag wählen, gilt sowohl für das Senden als auch für den Empfang des für diesen Auftrag verwendeten AWS Snowcone Geräts. Weitere Informationen zu Versandgebühren finden Sie unter [AWS Snowcone – Preise](#).

Themen

- [Vorbereiten eines -AWS SnowconeGeräts für den Versand](#)
- [Versandeinschränkungen nach Regionen](#)
- [Versand eines -AWS SnowconeGeräts](#)

Wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen, geben Sie eine Lieferadresse und eine Versandgeschwindigkeit an. Diese Versandgeschwindigkeit gibt nicht an, wie schnell Sie erwarten können, dass das AWS Snowcone Gerät an dem Tag empfangen wird, an dem Sie den Auftrag erstellt haben. Es zeigt nur die Zeit an, zu der das Gerät zwischen AWS und Ihrer Lieferadresse unterwegs ist. Diese Zeit beinhaltet keine Zeit für die Verarbeitung, die von Faktoren wie dem Auftragsstyp abhängt (Exporte dauern in der Regel länger als Importe). Außerdem holen Mobilfunkanbieter ausgehende AWS Snowcone Geräte im Allgemeinen nur einmal täglich ab. Daher kann die Bearbeitungszeit vor dem Versand auch länger dauern als einen Tag.

Note

Geräte der Snow Family können nur an denselben zurückgegeben werdenAWS-Region, in dem die Geräte bestellt wurden. Einige AWS Regionen unterstützen das Senden von Snow Family-Geräten in ein anderes Land als das, aus dem das Gerät bestellt wurde. Weitere Informationen finden Sie unter [Versandeinschränkungen nach Regionen](#).

Vorbereiten eines -AWS SnowconeGeräts für den Versand

Im Folgenden wird erläutert, wie Sie einen Snowcone vorbereiten und an zurücksendenAWS.

So bereiten Sie ein AWS Snowcone Gerät für den Versand vor

1. Stellen Sie sicher, dass Sie alle Daten für diesen Auftrag auf oder vom AWS Snowcone Gerät übertragen haben. [Entsperren Sie das Gerät.](#)
2. Drücken Sie die Einschalttaste auf der Gerätevorderseite, die sich neben den Indikatoren befindet, gegenüber den Netzwerkports. Das Herunterfahren des Geräts dauert ca. 20 Sekunden.

Wenn Sie Ihr Snowcone-Gerät ausgeschaltet und getrennt haben und die Versandinformationen nach etwa einer Minute nicht auf dem Bildschirm E-Ink angezeigt werden, finden Sie weitere Informationen unter [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten.](#)

Versandeinschränkungen nach Regionen

Bevor Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen, sollten Sie sich über das , in dem sich Ihre Daten befindenAWS-Region, bei der Konsole anmelden. Geräte der Snow Family werden nicht zwischen internationalen Ländern versendet, z. B. von Asien-Pazifik (Indien) nach Asien-Pazifik (Australien).

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

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

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

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

Note

AWS sendet keine Snow Family-Geräte an Postfächer.

Versand eines -AWS SnowconeGeräts

Die vorab angezeigten Versandinformationen auf der E-Ink-Anzeige enthalten die richtige Adresse für die Rückgabe des AWS Snowcone Geräts. Informationen zum Zurückgeben Ihres AWS Snowcone Geräts finden Sie unter [the section called “Versandanbieter”](#). Das AWS Snowcone Gerät wird an eine AWS Sortiereinrichtung 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.

Wenn Sie Ihr Snowcone-Gerät ausgeschaltet und getrennt haben und die Versandinformationen nach etwa einer Minute nicht auf dem Bildschirm E-Ink angezeigt werden, finden Sie weitere Informationen unter [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten](#).

Versandanbieter

Wenn Sie einen Auftrag zum Bestellen eines Snow Family-Geräts erstellen, geben Sie die Adresse an, an die das AWS Snowcone Gerät versendet werden soll. Der Transporteur, der Ihre Region unterstützt, übernimmt den Versand von AWS Snowcone Geräten von AWS an Sie und zurück an AWS. Wenn ein AWS Snowcone Gerät versendet wird, erhalten Sie eine Nachverfolgungsnummer. Sie finden die Nachverfolgungsnummer jedes Auftrags und einen Link zur Nachverfolgungswebsite im [Managementkonsole für die AWS Snow-Familie](#) Auftrags-Dashboard oder mithilfe von API-Aufrufen an die Auftragsverwaltungs-API.

Im Folgenden finden Sie die Liste der unterstützten Mobilfunkanbieter für AWS Snowcone Geräte nach Regionen:

- In Indien erfolgt der Versand durch Blue Dart.
- Für Korea, Japan, Australien, Indonesien, Israel und Singapur ist Kuehne + der Fluggesellschaft.
- Für China ist S.F. Express der Mobilfunkanbieter.
- 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 Bol ein AWS Snowcone Gerät aufnehmen kann:

- Ordnen Sie für microSD an, das AWS Snowcone Gerät zu übernehmen, indem Sie direkt eine Annahme mit microSD planen, oder bringen Sie das Gerät in eine microSD-Paket-Dropoff-Einrichtung, um an gesendet zu werden AWS.
- Das microSD-Versandetikett auf der E-Ink-Anzeige enthält die richtige Adresse für die Rückgabe des AWS Snowcone Geräts.
- Das AWS Snowcone Gerät wird an eine AWS Sortiereinrichtung geliefert und an das AWS Rechenzentrum weitergeleitet. microSD stellt automatisch eine Nachverfolgungsnummer für Ihre Sendung bereit.

Die microSD-Services für Snow Family-Geräte befinden sich nur in einem Land.

AWS Snowcone-Abholungen in Brasilien

Beachten Sie in Brasilien die folgenden Informationen, damit microSD ein Snowcone- aufnehmen kann:

- Wenn Sie bereit sind, eine Snowcone- zurückzugeben, rufen Sie 0800-770-9035 auf, um eine Annahme mit Bol zu planen.
- Snowcone ist in Brasilien verfügbar, das 26 Bundesstaaten und das Distrito Federal umfasst.
- Halten Sie, sofern vorhanden, Ihre Betriebszulassungsnummer (Cadastro Nacional de Pessoa Juridica, CNPJ) bereit, bevor Sie einen Auftrag erstellen.
- Sie sollten das entsprechende Dokument ausgeben, um das Snowcone-Gerät zurückzugeben. Bestätigen Sie mit Ihrer Steuerabteilung, welche der folgenden Dokumente in Ihrem Staat gemäß Ihrer ICMS-Anmeldung erforderlich sind:
 - Innerhalb von São Paulo – In der Regel sind eine Nicht-ICMS-Deklaration und eine Rechnung für die elektronische Steuer (NF-e) erforderlich.
 - Außerhalb von São Paulo – In der Regel ist Folgendes erforderlich:
 - Eine Erklärung zur Befreiung von der Warenumlaufsteuer
 - Eine Nota Fiscal
 - Elektronische Steuerrechnung (NF-e)

Note

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 -Aufnahmen in Isreal

Ordnen Sie in Israel die Annahme an, indem Sie AWS sich per E-Mail unter snowball-shipping@amazon.com an den wenden. Geben Sie Snowcone-Abholanforderung in den Betreff ein und geben Sie diese Informationen an:

- Auftrags-ID – Die Auftrags-ID, die dem von Ihnen zurückgegebenen Snow-Gerät zugeordnet ist. Sie finden die Auftrags-ID im [Managementkonsole für die AWS Snow-Familie](#).
- Aufnahmeadresse – Die Adresse, an der das Gerät abgeholt wird.
- Aufnahmedatum – Das früheste Datum, an dem das Gerät abgeholt werden soll.
- Kontaktdatenpunkt – Der Name, die E-Mail-Adresse und die lokale Telefonnummer, die der Versanddienst, Kuehne +, bei Bedarf für Informationen zur Annahme verwenden kann.

In Kürze erhalten Sie eine Follow-up-E-Mail von AWS Support mit Informationen zur Annahme Ihres Geräts unter der von Ihnen angegebenen Adresse. Bereiten Sie das Gerät für den Versand vor und bereiten Sie es vor 12:00 Uhr Ortszeit ab. Siehe [Vorbereiten eines -AWS SnowconeGeräts für den Versand](#).

AWS Snowcone -Abholungen in Großbritannien

Beachten Sie in Großbritannien die folgenden Informationen, damit Bol ein AWS Snowcone Gerät aufnehmen kann.

- Sie ordnen an, dass microSD das AWS Snowcone Gerät abholt, indem Sie direkt eine Annahme mit microSD planen, oder das Gerät in eine microSD-Paket-Dropoff-Einrichtung bringen, um an gesendet zu werdenAWS.
- Das Telefonie-Versandetikett auf der E-Ink-Anzeige enthält die richtige Adresse, um das AWS Snowcone Gerät zurückzugeben.
- Das AWS Snowcone Gerät wird an eine AWS Sortiereinrichtung geliefert und an das AWS Rechenzentrum weitergeleitet. UPS übermittelt Ihnen automatisch eine Sendungsverfolgungsnummer zu Ihrem Auftrag.

⚠ Important

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

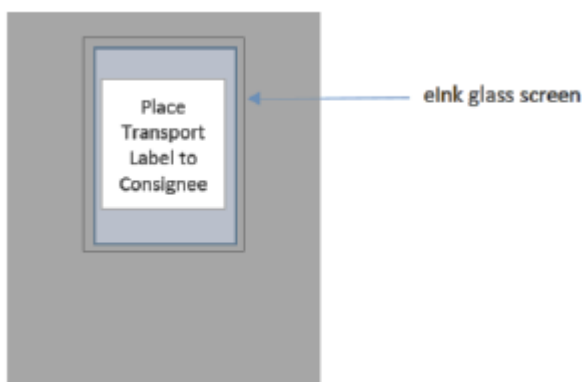
Die -Services für die Snow-Produktfamilie sind nur innerhalb eines Landes regional.

ℹ Note

Seit Januar 2021 ist Großbritannien nicht mehr Teil der EU. Bei Bestellungen zwischen Großbritannien und anderen EU-Ländern handelt es sich um internationale Bestellungen. Dabei handelt es sich um einen nicht allgemeinen Verfügbarkeitsprozess, der nur durch einen speziellen internationalen Prozess genehmigt wurde. Wenn ein Kunde eine Genehmigung erhalten hat und ein Gerät aus einem EU-Land zurück an LHR oder aus Großbritannien zurück an ein EU-Land zurückgibt, muss er zunächst eine Rückgabe an <snowball-shipping@amazon.com> beantragen, damit eine Handelsrechnung ausgestellt werden kann, bevor er die Annahme/Ablegen mit Bol anfordert.

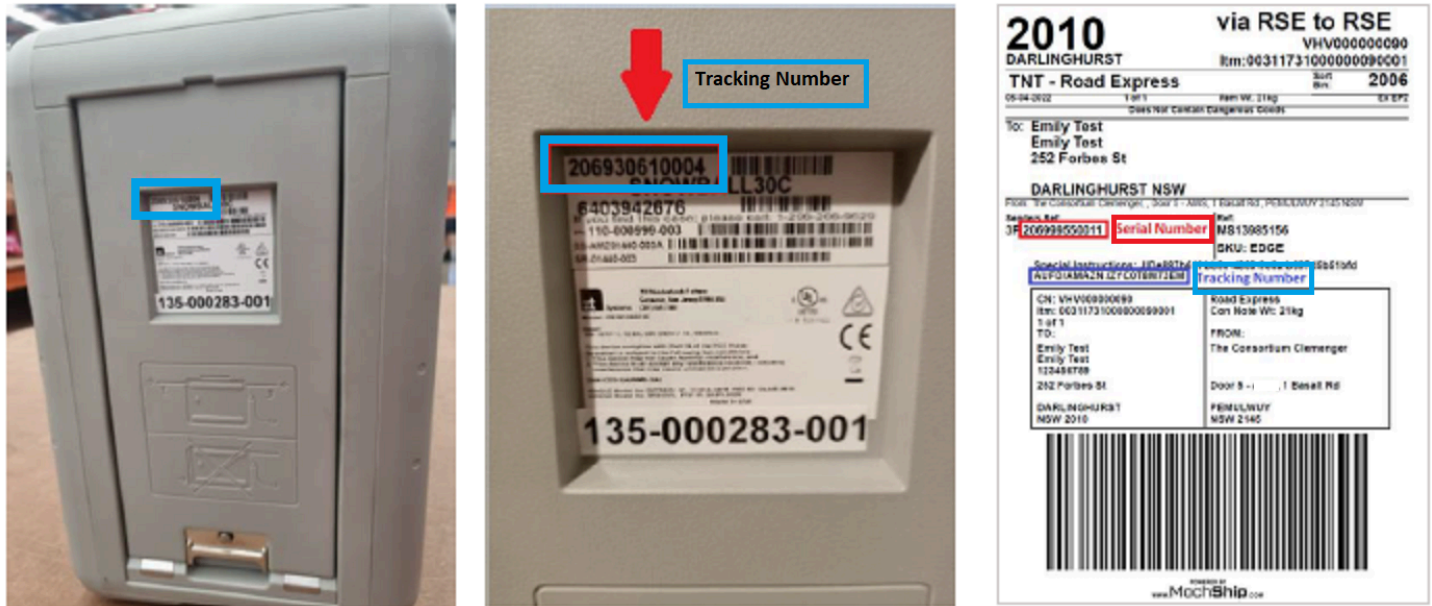
AWS Snowcone-Abholungen in Australien

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



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

Example where to locate tracking number and serial number



Um die Rückgabe des Snow-Geräts anzuordnen, senden Sie bitte eine E-Mail an knau.snowball_return@kuehne-nagel.com mit den folgenden Informationen:

- Ihr Name
- Tracking-Nummer (wie blau dargestellt)
- Geräteseriennummer (wie rot dargestellt)
- Vollständige Sammlungsadresse
- Kontaktperson bei der Annahme
- Kontakttelefonnummer bei der Annahme
- Sammlungsdatum
- Erfassungsfenster (mindestens 3 Stunden innerhalb der Geschäftszeiten)

Note

Tag und Uhrzeit der Sammlung müssen ein Werktag innerhalb der Geschäftszeiten sein

Das Team von Kuehne + antwortet, um den Empfang der Anfrage zur Annahme zu bestätigen.

AWS Snowcone-Abholungen in Indien

In Indien übernimmt Blue Dart das Snowcone-Gerät. Wenn Sie bereit sind, Ihr Snowcone-Gerät zurückzugeben, schalten Sie es aus und bereiten Sie es für den Rücksende vor. Senden Sie eine E-Mail an snowball-pickup@amazon.com mit der Snowcone-Abholanfrage in der Betreffzeile, um die Aufnahme zu planen. Geben Sie in der E-Mail folgende Informationen an:

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

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

Important

Wenn Sie einen Snowcone in Indien verwenden, denken Sie daran, alle relevanten Steuerelemente bei Ihrem Bundesstaat einzureichen.

AWS Snowcone -Abholungen in Korea

In Südafrika übernimmt Kuehne + Ihre Annahme. Wenn Sie bereit sind, Ihr Gerät zurückzugeben, senden Sie eine E-Mail mit Snowcone-Abholanfrage in der Betreffzeile an snowball-shipping@amazon.com, damit wir die Aufnahme für Sie planen können. Geben Sie im Text der E-Mail folgende Informationen an:

- Auftrags-ID – Die Auftrags-ID, die dem Snowcone zugeordnet ist, den Sie an zurückgeben möchten AWS.
- Aufnahmeadresse – Die Adresse, an der das Gerät abgeholt wird.
- Aufnahmedatum – Der früheste Tag, an dem das Gerät abgeholt werden soll.
- Kontaktdaten für einen Ansprechpartner – Name, E-Mail-Adresse und Telefonnummer, damit Kühne+Nagel Kontakt aufnehmen kann, wenn notwendig.

In Kürze erhalten Sie eine Follow-up-E-Mail vom AWS Support mit Informationen zur Annahme Ihres Geräts unter der von Ihnen angegebenen Adresse. Bereiten Sie das Gerät für den Versand vor (siehe [Vorbereiten eines -AWS Snowcone Geräts für den Versand](#)) und sind Sie für die Annahme bereit, normalerweise zwischen 1300 und 1500 Stunden Ortszeit.

AWS Snowcone-Abholungen in Hongkong

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

- Auftrags-ID
- AWS-Konto-ID
- Name des Ansprechpartners
- Telefonnummer des Ansprechpartners
- E-Mail-Adresse des Ansprechpartners
- Der Tag, an dem das Gerät abgeholt werden soll.
- Früheste bevorzugte Aufnahmezeit
- Letzte bevorzugte Aufnahmezeit
- 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 an geliefert. Verwenden Sie die S.F. Express-Nachverfolgungsnummer der Rücksendesendung, um zu erfahren, wann die Lieferung abgeschlossen wurde.

AWS Snowcone Transporte in Indonesien, Japan und Singapur

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

RETURN

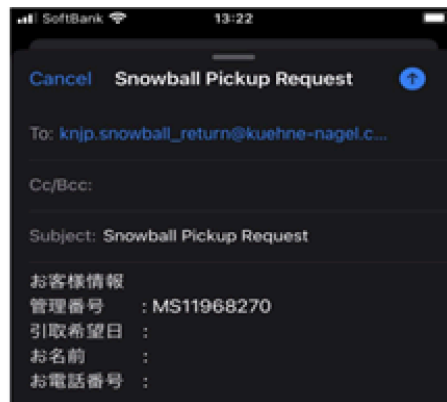
AWS Jobs ID QF6LNZGKTZPF
 シリアル番号 2R 207138750022
 管理番号 MS14003547



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 basieren auf dem Land, in dem Sie ein AWS Snowcone Gerät versenden. Von folgenden Versandzeiten können Sie ausgehen:

- Australien, Indonesien, Japan, Singapur, Korea – Wenn Sie innerhalb dieser Länder versenden, haben Sie Zugriff auf die Standard-Versandgeschwindigkeit von 1 bis 3 Tagen.
- Brasilien – Wenn Sie innerhalb Brasiliens versenden, haben Sie Zugriff auf den Express- Saver-Versand von Bol microSD, der innerhalb von zwei Werktagen zu Geschäftszeiten geliefert wird. Die Transportdauer kann durch Verspätungen an den zwischenstaatlichen Grenzen verlängert werden.

- Europa (EU) – Wenn Sie in eines der Länder innerhalb der EU versenden, haben Sie Zugriff auf Express-Versand. In der Regel werden Snowcone-Geräte, die Express geliefert werden, in etwa einem Tag geliefert. Außerdem ist in den meisten EU-Ländern der Standardversand möglich. In der Regel dauert dieser für einen Weg weniger als eine Woche.
- Indien – Beim Versand innerhalb Indiens werden AWS Snowcone Geräte innerhalb von 7 Tagen nach AWS Erhalt aller zugehörigen Steuerdokumente versendet.
- Israel – Beim Versand in Israel haben Sie Zugriff auf den Versand am selben Tag.
- USA (USA) und Kanada – Wenn Sie in den USA und Kanada versenden, haben Sie Zugriff auf einen eintägigen Versand und einen zweitägigen Versand.
- Großbritannien (UK) – Wenn Sie innerhalb Großbritanniens versenden, haben Sie Zugriff auf Express-Versand. In der Regel werden Snowcone-Geräte, die Express geliefert werden, in etwa einem Tag geliefert. Darüber hinaus haben Sie Zugriff auf den Standard-Versand, der in der Regel weniger als eine Woche dauert.

Aktualisieren von Software auf Snowcone-Geräten

AWS benachrichtigt Sie, wenn neue Software für Ihre Snow-Family-Geräte verfügbar ist. Die Benachrichtigung wird per E-Mail AWS Health Dashboard und als CloudWatch Ereignis bereitgestellt. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die dem AWS Konto zugeordnet ist, das zum Bestellen des Snow Family-Geräts verwendet wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und laden Sie das Update so schnell wie möglich herunter und installieren Sie es, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Weitere Informationen zu AWS Health Dashboard finden Sie im [AWS Health -Benutzerhandbuch](#). Weitere Informationen zu - CloudWatch Ereignissen finden Sie im [Amazon CloudWatch Events-Benutzerhandbuch](#).

Sie können Software-Updates von heruntergeladen AWS und auf Snowcone-Geräten in Ihren On-Premises-Umgebungen installieren. Diese Aktualisierungen erfolgen im Hintergrund. Sie können Ihre Geräte weiterhin wie gewohnt verwenden, während die neueste Software sicher von AWS auf Ihr Gerät heruntergeladen wird. Um heruntergeladene Updates anzuwenden, müssen Sie jedoch die auf dem Gerät ausgeführten Services beenden und 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 Software-Updates werden ausschließlich für die Installation der Software-Updates auf der entsprechenden Appliance im Namen von bereitgestellt AWS. Sie werden (oder versuchen, dies zu tun) und werden Dritten nicht erlauben oder autorisieren, (i) andere Kopien der Software-Updates als die für die Installation der Software-Updates auf der entsprechenden Appliance erforderlichen zu erstellen oder (ii) Features oder Maßnahmen in den Software-Updates zu umgehen oder zu deaktivieren, einschließlich, aber nicht beschränkt auf jegliche Verschlüsselung, die auf das Software-Update angewendet wird. Sobald die Softwareupdates auf der entsprechenden Appliance installiert wurden, erklären Sie sich damit einverstanden, die Softwareupdates von allen Medien zu löschen, die bei der Installation der Softwareupdates auf der Appliance verwendet werden.

Warning

Wir empfehlen dringend, alle Aktivitäten auf Ihrem Gerät auszusetzen, bevor Sie das Update installieren. Wenn Sie das Gerät aktualisieren und neu starten, werden keine Instances mehr ausgeführt und alle Schreibvorgänge in lokale Amazon S3-Buckets werden unterbrochen.

Themen

- [Voraussetzungen](#)
- [Herunterladen von Updates](#)
- [Installieren von Updates](#)
- [Aktualisieren des SSL-Zertifikats](#)
- [Aktualisieren Ihrer Amazon Linux 2-AMIs auf Snow Family-Geräten](#)

Voraussetzungen

Bevor Sie Ihr Gerät aktualisieren können, müssen folgende Voraussetzungen umgesetzt werden:

- Sie haben den Auftrag erstellt, haben das Gerät zur Hand und haben es entsperrt. Weitere Informationen finden Sie unter [Erste Schritte](#).
- Das Aktualisieren von 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 mit dem Gerät verfügt, das Sie aktualisieren möchten. Weitere Informationen finden Sie unter [Verwenden des AWS Snowball Edge Clients](#).
- (Optional) Wir empfehlen Ihnen, ein Profil für den Snowball-Edge-Client zu konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren eines Profils für den Snowball Edge Client](#).

Nachdem Sie diese Aufgaben abgeschlossen haben, können Sie Updates für Snowcone-Geräte herunterladen und installieren.

Herunterladen von Updates

Es gibt zwei primäre Möglichkeiten, ein Update für Snow Family-Geräte herunterzuladen:

- Sie können manuelle Updates jederzeit mit bestimmten Snowball Edge-Clientbefehlen auslösen.
- Sie können programmgesteuert einen Zeitpunkt für die automatische Aktualisierung des Geräts bestimmen.

Das folgende Verfahren beschreibt den Vorgang zum manuellen Herunterladen von Aktualisierungen. Informationen zum automatischen Aktualisieren Ihres Snowcone-Geräts finden Sie `configure-auto-update-strategy` unter [Aktualisieren eines Snowcone](#).

Note

Wenn Ihr Gerät keinen Zugriff auf das Internet hat, können Sie eine Aktualisierungsdatei mit der [GetSoftwareUpdates](#)-API herunterladen. Verweisen Sie dann auf einen lokalen Dateispeicherort, wenn Sie `download-updates` mit dem `uri` Parameter aufrufen, wie im folgenden Beispiel.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Formatieren Sie für Windows-Betriebssysteme den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file://C:/path/to/local-update
```

So suchen Sie nach Snowcone-Softwareupdates und laden sie herunter

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 aktuelle Version zurück, die auf dem Gerät installiert ist.
3. Wenn Ihre Gerätesoftware nicht mehr auf dem neuesten Stand ist, führen Sie den Befehl `snowballEdge download-updates` aus.

Note

Wenn Ihr Gerät nicht mit dem Internet verbunden ist, laden Sie zunächst eine Aktualisierungsdatei über die [GetSoftwareUpdates](#) API herunter. Führen Sie dann den `snowballEdge download-updates` Befehl mit dem `uri` Parameter mit einem lokalen Pfad zu der heruntergeladenen Datei aus, wie im folgenden Beispiel.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Formatieren Sie für Windows-Betriebssysteme den Wert des `uri` Parameters wie folgt:

```
snowballEdge download-updates --uri file://C:/path/to/local-update
```

4. Sie können den Status dieses Downloads mit dem Befehl `snowballEdge describe-device-software` überprüfen. Während ein Update heruntergeladen wird, zeigen Sie den Status mit diesem Befehl an.

Example Ausgabe des **describe-device-software** Befehls

```
Install State: Downloading
```

Installieren von Updates

Nach dem Herunterladen von Updates müssen Sie sie installieren und Ihr Gerät neu starten, damit die Updates wirksam werden. Das folgende Verfahren führt Sie durch die manuelle Installation von Updates.

Note

Halten Sie alle Aktivitäten auf dem Gerät an, bevor Sie Softwareupdates installieren. Durch die Installation von Updates werden keine Instances mehr ausgeführt und alle Schreibvorgänge in Amazon S3-Buckets auf dem Gerät unterbrochen. Dies kann zu Datenverlust führen

So installieren Sie Softwareupdates, die bereits auf eigenständige Snow-Family-Geräte heruntergeladen wurden

1. Öffnen Sie ein Terminalfenster und stellen Sie sicher, dass das 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 eines Snow-Family-Geräts](#).
2. Führen Sie den `list-services` Befehl aus, um die auf dem Gerät verfügbaren Services anzuzeigen. Der Befehl gibt die Service-IDs jedes auf dem Gerät verfügbaren Services zurück.

```
snowballEdge list-services
```

Example der Ausgabe des **list-services** Befehls

```
{  
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]  
}
```

3. Führen Sie für jede durch den `list-services` Befehl identifizierte Service-ID den `describe-service` Befehl aus, um den Status anzuzeigen. Verwenden Sie diese Informationen, um Services zu identifizieren, die angehalten werden sollen.

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

Example der Ausgabe des **describe-service** Befehls

```
{  
  "ServiceId" : "s3",  
  "Status" : {  
    "State" : "ACTIVE"  
  },  
  "Storage" : {  
    "TotalSpaceBytes" : 99608745492480,  
    "FreeSpaceBytes" : 99608744468480  
  },  
  "Endpoints" : [ {  
    "Protocol" : "http",  
    "Port" : 8080,  
    "Host" : "192.0.2.0"  
  }, {  
    "Protocol" : "https",  
    "Port" : 8443,  
    "Host" : "192.0.2.0",  
  }  
]
```

```
"CertificateAssociation" : {
  "CertificateArn" : "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}
```

Diese Ausgabe zeigt, dass der s3 Service aktiv ist und mit dem `stop-service` Befehl gestoppt werden muss.

4. Verwenden Sie den `stop-service` Befehl , um jeden Service zu beenden, bei dem sich der Wert des State Namens ACTIVE in der Ausgabe des `list-services` Befehls befindet. Wenn mehr als ein Service ausgeführt wird, beenden Sie jeden Service, bevor Sie fortfahren.

Note

Der Amazon S3-Adapter AWS STS, Amazon EC2 und die IAM-Services können nicht gestoppt werden. Wenn Amazon S3-kompatibler Speicher auf Snow-Family-Geräten ausgeführt wird, halten Sie ihn an, bevor Sie Updates installieren. Amazon S3-kompatibler Speicher auf Snow-Family-Geräten hat `s3-snow` als `serviceId`.

```
snowballEdge stop-service --service-id service-id --device-ip-addresses snow-
device-1-ip-address snow-device-device-2-ip-address snow-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code 29-character-unlock-code --
endpoint https://snow-device-ip-address
```

Example der Ausgabe des **stop-service** Befehls

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

5. Führen Sie den Befehl `snowballEdge install-updates` aus.

6. Sie können den Status dieser Installation mit dem Befehl `snowballEdge describe-device-software` überprüfen. Während ein Update installiert wird, zeigen Sie den Status mit diesem Befehl an.

Beispielausgabe

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Sie haben erfolgreich ein Software-Update für Ihr 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

Ein Neustart Ihres Snow Family-Geräts, ohne alle Aktivitäten auf dem Gerät zu beenden, kann zu Datenverlust führen.

7. Wenn alle Services auf dem Gerät angehalten wurden, starten Sie das Gerät neu, entsperren Sie das Gerät und starten Sie es erneut. Damit ist die Installation der heruntergeladenen Softwareupdates abgeschlossen. Weitere Informationen zum Neustarten des Geräts finden Sie unter [Neustarten des Snow-Family-Geräts](#). Weitere Informationen zum Entsperren des Geräts finden Sie unter [Entsperren des Snow Family-Geräts](#).
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 nun das Snow Family-Gerät oder den Gerätecluster erfolgreich aktualisiert und bestätigt, dass das Update auf die neueste Snow Family-Software durchgeführt wurde.

Aktualisieren des SSL-Zertifikats

Wenn Sie planen, Ihr Snow Family-Gerät länger als 360 Tage aufzubewahren, müssen Sie das Secure Sockets Layer (SSL)-Zertifikat auf dem Gerät aktualisieren, um eine Unterbrechung Ihrer Gerätenutzung zu vermeiden. Wenn das Zertifikat abläuft, können Sie das Gerät nicht verwenden und müssen es an zurückgeben AWS.

AWS benachrichtigt Sie 30 Tage, bevor das SSL-Zertifikat für Ihre Snow-Family-Geräte abläuft. Die Benachrichtigung wird per E-Mail AWS Health Dashboard und als CloudWatch Ereignis bereitgestellt. Die E-Mail-Benachrichtigung wird von Amazon Web Services, Inc. an die E-Mail-Adresse gesendet, die dem AWS Konto zugeordnet ist, das zum Bestellen des Snow Family-Geräts verwendet wurde. Wenn Sie die Benachrichtigung erhalten, folgen Sie den Anweisungen in diesem Thema und fordern Sie so schnell wie möglich ein Update an, um eine Unterbrechung Ihrer Nutzung des Geräts zu vermeiden. Weitere Informationen zu finden Sie AWS Health Dashboard im [AWS Health - Benutzerhandbuch](#). Weitere Informationen zu - CloudWatch Ereignissen finden Sie im [Amazon CloudWatch Events-Benutzerhandbuch](#).

In diesem Thema wird erläutert, wie Sie bestimmen, wann das Zertifikat abläuft und wie Sie Ihr Gerät aktualisieren.

1. Verwenden Sie den `snowballEdge describe-device-software` Befehl, um zu bestimmen, wann das Zertifikat abläuft. In der Ausgabe des Befehls `CertificateExpiry` enthält der Wert von das Datum und die Uhrzeit, zu der das Zertifikat abläuft.

Example der **describe-device-software** Ausgabe

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

2. Wenden Sie sich an AWS Support und fordern Sie ein SSL-Zertifikatsupdate an.
3. AWS Support stellt eine Aktualisierungsdatei bereit. [Laden Sie](#) die Aktualisierungsdatei herunter und [install](#) ieren Siesie.
4. Verwenden Sie den neuen Entsperrcode und die Manifestdatei, wenn Sie <https://docs.aws.amazon.com/snowball/latest/snowcone-guide/connect-unlock-device.html>.

Aktualisieren Ihrer Amazon Linux 2-AMIs auf Snow Family-Geräten

Als bewährte Methode für die Sicherheit sollten Sie Ihre Amazon Linux 2-AMIs up-to-date auf Geräten der Snow Family aufbewahren. Überprüfen Sie regelmäßig das [Amazon Linux 2 AMI \(HVM\), SSD-Volume-Typ \(64-Bit x86\)](#) in der AWS Marketplace auf Updates. Wenn Sie feststellen, dass Sie Ihr AMI aktualisieren müssen, importieren Sie das neueste Amazon Linux 2-Image auf das Snow-

Gerät. Weitere Informationen finden Sie unter [Importieren eines Images auf Ihr Gerät als Amazon EC2-compatible AMI](#).

Sie können die neueste Amazon Linux 2-Image-ID auch mit dem `ssm get-parameters` Befehl in der abrufen AWS CLI.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Der Befehl gibt die neueste Image-ID des AMI zurück. Beispielsweise:

```
ami-0ccb473bada910e74
```

Bewährte Methoden für das AWS Snowcone Gerät

Um den größtmöglichen Nutzen aus Ihrem Gerät zu ziehen und mit Ihrem AWS Snowcone Gerät zufrieden zu sein, 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. Wenden Sie [AWS Support](#) sich stattdessen an uns und ein neues AWS Snowcone Gerät wird Ihnen zugestellt.
- 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-Clientbefehl `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 passen nicht zu dem AWS-Konto oder zu anderen AWS-Konto. 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 Ihrem Job zugeordnet sind.
- Sie können den Zugriff auf NFS-Shares einschränken. Details hierzu finden Sie unter [Beschränken des Zugriffs auf NFS-Anteile, wenn NFS ausgeführt wird](#).
- Wenn Sie ein Snowcone-Gerät ausschalten oder aus- und wieder einschalten, wechselt es in einen gesperrten Zustand.

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. Mit beiden

Wenn NFS Mount und gleichzeitig DataSync auf demselben S3-Bucket sind, kann es zu Lese-/Schreibkonflikten kommen.

- Um zu verhindern, dass Ihre Daten beschädigt werden, trennen Sie AWS Snowcone das Gerät nicht vom Computer und ändern Sie nicht die Netzwerkeinstellungen, während Sie Daten übertragen.
- 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 [Snowcone-Leistung](#).

Ressourcenmanagement

- Die fünf freien Tage für die Durchführung Ihrer lokalen Datenübertragung beginnen am Tag, nachdem das AWS Snowcone Gerät in Ihrem Rechenzentrum eingetroffen ist.

Verwaltung von EC2-kompatiblen Instances

Um zu vermeiden, dass versehentlich die Amazon EC2-kompatiblen Instances gelöscht werden, die Sie auf Ihrem AWS Snowcone Gerät erstellen, sollten Sie Ihre Instances nicht vom Betriebssystem aus 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, die Sie beibehalten möchten, auszusetzen.

Snowcone-Leistung

Die folgende Tabelle beschreibt, wie sich die Übertragungsrates Ihres Netzwerks darauf auswirkt, wie sich eine AWS Snowcone mit Daten.

Geschwindigkeit (MB/s)	8 TB Übertragungsdauer	4 TB Übertragungsdauer
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 Amazon Elastic Block Store (Amazon EBS) -Volume-Präsentation verwenden können. Sie können diesen Speicher entweder für NFS oder Amazon EBS verwenden, aber nicht für beide. Sie können Ihren Speicherplatz je nach Anwendungsfall zuweisen. Beachten Sie, dass der Speicherplatz vorab zugewiesen ist, wenn Sie Ihre Snowcone-Bestellung aufgeben.

Speicher für Rechenaufträge

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 das Root-Volume allein. Da es sich nur um lokalen Speicher handelt, gehen auf die Amazon EBS-Volumes geschriebene Daten verloren, wenn das Gerät anAWS weil es nicht in Amazon S3 importiert werden kann.

Themen

- [Ressourcenkontingente berechnen](#)
- [Einschränkungen für den Versand eines Snowcone-Geräts](#)
- [Einschränkungen bei der Verarbeitung Ihres zurückgegebenen Snowcone-Geräts für den Import](#)
- [VerfügbarAWS-Regionen](#)

Ressourcenkontingente berechnen

Verfügbare Rechenressourcen für Snowcone-Geräte, Kontingente für Speicher

In der folgenden Tabelle sind die verfügbaren Rechenressourcen für Snowcone-Geräte und deren Speicherkontingente aufgeführt.

Instance-Typ	vCPU-Kerne	Arbeitsspeicher (GiB)	Kontingent
snc1.micro	1	1	2
snc1.small	1	2	2
snc1.medium	2	4	1

Amazon Machine Image (AMI) und Amazon EC2-Kapazitätskontingente 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 kombinierte Größe aller AMIs, die im Auftrag eines Kunden verwendet werden)
Amazon EC2-kompatible Instances	150 GB (steht für den verfügbaren Speicherplatz für die Backing-Speichervolumen der Instances)

Einschränkungen für den Versand eines Snowcone-Geräts

Im Folgenden sind die Einschränkungen für den Versand eines Snowcone-Geräts aufgeführt:

- AWSversendet 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 verstößt gegen dieAWSServicebedingungen.

Weitere Informationen zum Versand finden Sie unter [Versandüberlegungen für AWS Snowcone](#).

Einschränkungen bei der Verarbeitung Ihres zurückgegebenen Snowcone-Geräts für den Import

Um Ihre Daten in den zu importierenAWS Cloud, das Snowcone-Gerät muss 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 erzeugen.
- Sofern kein Versandetikett bereitgestellt wird vonAWS, das E-Ink-Display auf dem Snowcone-Gerät muss sichtbar sein und es muss das Rücksendetikett zeigen, das automatisch generiert wurde, als Sie die Übertragung Ihrer Daten auf das Snowcone-Gerät abgeschlossen haben.

Note

Alle zurückgegebenen Snowcone-Geräte, die diese Anforderungen nicht erfüllen, werden gelöscht, ohne dass daran gearbeitet wurde.

VerfügbarAWS-Regionen

Für Informationen über die unterstütztenAWS-Regionenund Endpunkte, siehe [AWSEndpunkte und Kontingente von Snow Family](#) in derAllgemeine AWS-Referenz.

Behebung von Snowcone-Problemen

Dieser Abschnitt bietet Anleitungen und Einblicke in die AWS Snowcone-Gerät/Dienst zur Behebung einiger der aufgetretenen Probleme.

Themen

- [Problembehandlung bei Compute-Instances](#)
- [Behebung von Netzwerkproblemen](#)
- [Fehlerbehebung bei Amazon EC2-kompatiblen Instances auf Datasync](#)
- [Behebung von Problemen mit der Datenübertragung](#)
- [Behebung von Problemen bei der Rückgabe von Snow Family-Geräten](#)

Problembehandlung bei Compute-Instances

Die Fehlerbehebung von Compute-Instances ist dokumentiert [hier](#).

Behebung von Netzwerkproblemen

Die IP-Adresse ist 0.0.0.0

Sie sind an das Netzwerk und die Stromkabel angeschlossen, 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 eine statische IP auf dem Gerät einrichten, indem Sie die STATIC-Option auf dem Snowcone-Display verwenden und das Gerät mit der entsprechenden statischen IP-Adresse programmieren.

Gerät kann nicht entsperrt werden

Sie können das Gerät nicht entsperren mit OpsHub oder dem Snowball Edge-Client.

Maßnahme

Stellen Sie sicher, dass sich der Client im selben Subnetz und im selben Netzwerk befindet wie das AWS Snowcone-Gerät.

Wenn der Snowcone mehrere IP-Adresszuweisungen hat (z. B. Wi-Fi und Ethernet), stellen Sie dann sicher, dass Sie die gleiche IP-Adresse für die Verbindung verwenden, wenn mehrere Clients versuchen, auf Snowcone zu antworten. Beachten Sie, dass Sie jeweils nur eine Schnittstelle verwenden können.

Wenn die oben genannten Schritte nicht funktionieren, engagieren Sie sich bitte bei der AWS Support-Bereitstellung der Protokolle vom Gerät. Verwenden Sie den Snowball Edge-Client und den Befehl: `snowballEdge get-support-logs`

Fehlerbehebung bei Amazon EC2-kompatiblen Instances auf Datasync

Fehler: Instanz konnte nicht gestartet werden

Snowcone hat nicht genügend Kapazität, um die Instance für diese Anfrage zu starten.

Maßnahme

Die Voraussetzungen für die Ausführung von DataSync auf einem AWS Snowcone-Gerät als Agent verwendet die Standardinstanz `snc1.medium`, die 2 CPU-Kerne und 4 GiB Speicher bereitstellt. Stellen Sie sicher, dass das Snowcone-Gerät über genügend Ressourcen verfügt, um die neue Amazon EC2-kompatible Instance-Startanfrage bereitzustellen.

Behebung von Problemen mit der Datenübertragung

Zugriff vom Server verweigert

Fehler: `mount.nfs` - 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.

Verbindungszeitüberschreitung während der Datenübertragung

Die Verbindung läuft ab, wenn versucht wird, Daten zu übertragen AWS Snowcone mithilfe der Amazon S3-Schnittstelle (über AWS CLI).

Grund für dieses erwartete Verhalten

Der AWS Snowcone-Gerät unterstützt nur Übertragungen über den NFS-Mount für Offline-Übertragungen und AWS DataSync für Online-Übertragungen; die Amazon S3-Schnittstelle wird derzeit nicht unterstützt. Dies würde erklären, warum es zu Timeouts kommt, wenn Sie eine Verbindung mit dem herstellen AWS CLI.

Spawn Showmount ENOENT

Error: Uncaught Error - spawn showmount ENOENT. 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 Arbeitsstation läuft. Wenn der NFS-Dienst vor der Konfiguration von NFS nicht gestartet wurde AWS OpsHub, möglicherweise wird 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 zwischen der Workstation eine Firewall/ein Antivirenprogramm läuft AWS OpsHub und das Gerät, das die Verbindung blockieren könnte.

Führen Sie von der Workstation aus das Telnet zum AWS Snowcone-Befehl zur Geräte-IP-Adresse an der NFS-Portnummer 2049, 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 Informationen zur Rücksendung nicht auf dem E Ink-Display angezeigt.

Maßnahme

1. Melden Sie sich bei der Managementkonsole für die AWS Snow-Familie an.
2. Sehen Sie sich den Job für das Gerät an.
3. In der Einzelheiten-Abschnitt, in der Rücksendeetikett-Abschnitt, wählen Sie Um Ihr Rücksendeetikett einzusehen und auszudrucken, folgen Sie diesem Link.
4. Drucken Sie das Etikett aus und befestigen Sie es am Gerät.
5. Senden Sie das Gerät gemäß [Rückgabe eines Snowcone-Geräts](#).

Job Management-API-Referenz

- [Job Management-API-Referenz](#)
 - [Aktionen](#)
 - [Datentypen](#)
 - [Geläufige Parameter](#)
 - [Häufige Fehler](#)

Dokumentverlauf für AWS Snowcone-Benutzerhandbuch

Die folgende Tabelle beschreibt die Dokumentation für diese Version von AWS Snowcone.

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 25. August 2023

Änderung	Beschreibung	Datum
Benutzerdefinierte AMIs bei der Bestellung von Geräten einschließen	Benutzerdefinierte Amazon Machine Images können jetzt während der Bestellung von AWS Snow Family Aufträgen vorinstalliert werden. Weitere Informationen finden Sie unter Verwenden von Amazon EC2 auf Snowcone .	15. November 2023
Neue AWS-Region unterstützte	AWS Snowcone SSD-Geräte sind jetzt in Israel (Tel Aviv) verfügbar. Die Aufnahmeinformationen für diese Region wurden hinzugefügt. Weitere Informationen finden Sie unter AWS Snow Family-Endpunkte und -Kontingente in der Allgemeinen AWS-Referenz. Informationen zum Versand finden Sie unter Überlegungen zum Versand für AWS Snowcone .	25. August 2023
Neue AWS-Region unterstützte	Snowcone-Geräte sind jetzt in Europa (Paris) verfügbar. Weitere Informationen finden Sie unter AWS	29. Juni 2022

[Snow Family-Endpunkte und -Kontingente](#) in der Allgemeine AWS-Referenz. Informationen zum Versand finden Sie unter [Überlegungen zum Versand für AWS Snowcone](#).

[Tipps zur Fehlerbehebung in Snowcone](#)

AWS Snowcone Der Abschnitt mit Tipps zur Fehlerbehebung wurde hinzugefügt, ähnlich wie bei Snowball Edge. Ein neuer Abschnitt wurde hinzugefügt, siehe [Fehlerbehebung bei Snowcone-Problemen](#).

15. April 2022

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in den Regionen Asien-Pazifik (Mumbai) und Brasilien verfügbar. Es wurden Aufnahmeinformationen für EU, Kanada, Singapur und Brasilien hinzugefügt. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeine AWS-Referenz.

23. Februar 2022

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeine AWS-Referenz.

5. Januar 2022

Unterstützung für die Network Time Protocol (NTP)-Serverkonfiguration	Snowcone-Geräte unterstützen jetzt die Konfiguration des externen Network Time Protocol (NTP)-Servers.	16. November 2021
Neue AWS-Region unterstützen	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 AWS Endpunkte und Kontingente von Snow Family im Allgemeine AWS-Referenz.	3. November 2021
Neue AWS-Region unterstützen	AWS Snowcone ist jetzt in den Regionen USA West (Nordkalifornien), USA Ost (Ohio) und Südamerika (São Paulo) verfügbar. Weitere Informationen finden Sie unter AWS Endpunkte und Kontingente von Snow Family im Allgemeine AWS-Referenz.	29. September 2021
Neue AWS-Region unterstützen	AWS Snowcone ist jetzt in den Regionen Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) verfügbar. Weitere Informationen finden Sie unter AWS Endpunkte und Kontingente von Snow Family im Allgemeine AWS-Referenz.	26. August 2021

[Unterstützung für den Offline-Datenexport aus Amazon S3 mit Snowcone-Geräten](#)

Sie können jetzt AWS den Export Ihrer Amazon S3-Daten anfordern, indem Sie sie an Snowcone-Geräte übertragen, die dann physisch an Ihren Standort geliefert werden. Weitere Informationen finden Sie unter [Funktionsweise von Import- und Exportaufträgen](#).

4. August 2021

[Einführung in AWS Snow Device Management](#)

Mit Snow Device Management können Sie Ihr AWS Snowcone Gerät und Ihre lokalen AWS Services remote verwalten. Alle Snowcone-Geräte unterstützen Snow Device Management und sind auf neuen Geräten in den meisten vorinstalliert, in AWS-Regionen denen Snowcone verfügbar ist. Weitere Informationen finden Sie unter [Verwenden von AWS Snow Device Management zur Verwaltung von Geräten](#).

4. August 2021

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeinen AWS-Referenz.

28. April 2021

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in der Region Asien-Pazifik (Sydney) verfügbar. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeinen AWS-Referenz.

24. März 2021

[Unterstützung für die direkte Netzwerkschnittstelle](#)

AWS Snowcone fügt jetzt die Direct Network Interface (DNI)-Konfiguration hinzu, ein erweitertes Netzwerkfeature, das Anwendungsfälle wie Multicast-Streams, Routing und Load Balancing ermöglicht. Weitere Informationen finden Sie unter [Netzwerkkonfiguration für Datenverarbeitungs-Instances](#).

12. Januar 2021

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in der Region Europa (Frankfurt) verfügbar. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeinen AWS-Referenz.

18. November 2020

[Neue AWS-Region unterstützte](#)

AWS Snowcone ist jetzt in der Region Europa (Irland) verfügbar. Weitere Informationen finden Sie unter [AWS Endpunkte und Kontingente von Snow Family](#) im Allgemeinen AWS-Referenz.

16. September 2020

Einführung in AWS Snowcone

AWS Snowcone ist ein portables, Telefonie- und sicheres Gerät für Edge-Computing und Datenübertragung. Sie können verwenden, AWS Snowcone um Daten zu sammeln, zu verarbeiten und nach zu verschieben AWS, entweder offline, indem Sie das Gerät ansenden AWS, 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.