



AWS Snowcone

AWS Snowcone Guia do usuário



AWS Snowcone Guia do usuário: AWS Snowcone

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

| | |
|--|----|
| O que é AWS Snowcone? | 1 |
| Casos de uso | 2 |
| Definição de preço | 3 |
| Como AWS Snowcone funciona | 4 |
| AWS Snowcone fluxo de trabalho | 5 |
| Como funcionam os trabalhos de importação | 7 |
| Transferência de dados on-line entre o Snowcone e os serviços AWS de armazenamento com DataSync | 7 |
| Transferência de dados offline entre o Snowcone e o Amazon S3 | 8 |
| Para armazenamento do trabalho de importação | 8 |
| Para armazenamento de trabalho de computação | 9 |
| Especificações do dispositivo | 10 |
| Resumo | 10 |
| Hardware e rede | 12 |
| Vista superior | 12 |
| Painel traseiro | 12 |
| Painel frontal | 13 |
| AWS Snowcone Especificações de Wi-Fi | 14 |
| Especificações de robustez | 15 |
| Fonte de alimentação e acessórios do Snowcone | 15 |
| Desempenho de disco e CPU | 16 |
| Configurar | 17 |
| Inscreva-se para AWS | 17 |
| Antes de fazer o pedido | 18 |
| Sobre o ambiente local | 18 |
| Como trabalhar com caracteres especiais | 19 |
| Amazon EC2 | 20 |
| Diferença entre instâncias compatíveis com Amazon EC2 e Amazon EC2 em dispositivos da família Snow | 21 |
| Definição de preço para instâncias de computação no Snowcone | 21 |
| Pré-requisitos | 21 |
| Verificando códigos de produto e detalhes da plataforma de AWS Marketplace AMIs | 22 |
| Criar uma AMI do Linux de uma instância | 23 |
| Criar uma AMI do Linux de um snapshot | 23 |

| | |
|---|----|
| Conceitos básicos | 28 |
| Criando um trabalho para solicitar um dispositivo Snow Family | 28 |
| Etapa 1: escolher um tipo de trabalho | 29 |
| Etapa 2: escolher as opções de computação e armazenamento | 30 |
| Etapa 3: escolha seus atributos e opções | 33 |
| Etapa 4: escolha as preferências de segurança, envio e notificação | 33 |
| Etapa 5: revise o resumo do trabalho e crie seu trabalho | 36 |
| Baixar AWS OpsHub | 37 |
| Cancelamento de um trabalho para solicitar um dispositivo Snow Family | 38 |
| Obter credenciais para acessar um dispositivo Snow Family | 38 |
| Desbloqueando o dispositivo Snow Family | 40 |
| Solução de problemas para desbloquear um dispositivo da família Snow | 41 |
| Reinicializando o dispositivo da Família Snow | 42 |
| Usando AWS OpsHub para gerenciar dispositivos | 47 |
| Baixe AWS OpsHub para dispositivos da família Snow | 48 |
| Desbloquear um dispositivo | 49 |
| Desbloquear um dispositivo localmente | 49 |
| Desbloquear um dispositivo remotamente | 52 |
| Verificando a assinatura do AWS OpsHub | 56 |
| Gerenciando AWS serviços | 59 |
| Uso de instâncias de computação localmente | 60 |
| Gerenciando a interface NFS | 68 |
| Usando AWS DataSync para transferir arquivos para AWS | 77 |
| Transferir arquivos | 78 |
| Gerenciar seus dispositivos | 79 |
| Reinicializar seu dispositivo | 79 |
| Desligando seu dispositivo | 80 |
| Editar seu alias de dispositivo | 81 |
| Recebendo atualizações | 82 |
| Como gerenciar perfis | 83 |
| Configurando os servidores de horário NTP para o seu dispositivo | 85 |
| Usando o AWS Snowball Edge cliente | 87 |
| Fazer download e instalar o Snowball Edge Client | 87 |
| Comandos para o Snowball Edge Client | 87 |
| Configurar um perfil para o Snowball Edge Client | 89 |
| Obter o código QR para validação NFC | 90 |

| | |
|---|-----|
| Desbloqueando um dispositivo AWS Snowcone | 90 |
| Atualizando um Snowcone | 91 |
| Como obter as credenciais | 94 |
| Iniciando um serviço em seu dispositivo Snowcone | 95 |
| Interrupção de um serviço em seu dispositivo Snowcone | 96 |
| Obter certificado para transferência de dados | 96 |
| AWS Snowcone Registros | 97 |
| Ver status do dispositivo | 99 |
| Ver status do serviço | 101 |
| Lançamento da AWS DataSync AMI | 102 |
| Iniciando o NFS e restringindo o acesso | 105 |
| Restringindo o acesso aos compartilhamentos NFS quando o NFS está em execução | 106 |
| Obtenção do caminho de exportação para um bucket do Amazon S3 | 107 |
| Habilitando a AWS depuração do operador local | 107 |
| Desativando a depuração AWS do operador local | 107 |
| Criando uma interface de rede direta | 108 |
| Obtendo informações sobre uma interface de rede direta | 108 |
| Atualizando uma interface de rede direta | 108 |
| Excluindo uma interface de rede direta | 109 |
| Verificação do status do atributo | 109 |
| Alterar status do atributo | 110 |
| Configurando servidores de horário | 111 |
| Verificando fontes de tempo | 112 |
| Usando o Snow Device Management para gerenciar dispositivos | 114 |
| Escolhendo o estado de gerenciamento de dispositivos Snow ao solicitar um dispositivo da família Snow | 115 |
| Ativando o gerenciamento de dispositivos Snow | 116 |
| Adicionar permissões para o Snow Device Management a uma função do IAM | 117 |
| Comandos da CLI do Snow Device Management | 118 |
| Criar uma tarefa | 119 |
| Verificar o status da tarefa | 120 |
| Verifique as informações do dispositivo | 121 |
| Verifique o estado da instância compatível com o Amazon EC2 | 123 |
| Verificar metadados de tarefas | 125 |
| Cancelar uma tarefa | 126 |
| Listar comandos e sintaxe | 127 |

| | |
|--|-----|
| Listar dispositivos gerenciáveis remotamente | 128 |
| Listar o status da tarefa em todos os dispositivos | 129 |
| Listar atributos disponíveis | 130 |
| Listar tags de dispositivo ou tarefa | 131 |
| Listar tarefas por status | 132 |
| Aplicar etiquetas | 133 |
| Remover marcações | 134 |
| Usando AWS serviços | 135 |
| Usando o Amazon EC2 para computação | 135 |
| Visão geral | 136 |
| Pré-requisitos | 137 |
| Criação de um trabalho com instâncias de computação | 138 |
| Configuração de rede para as instâncias de computação | 143 |
| Conexão à sua instância de computação em um Snowcone usando SSH | 150 |
| Comandos do Snowcone Client para instâncias de computação | 150 |
| Usando o serviço de metadados de instância para Snow com instâncias compatíveis com Amazon EC2 | 156 |
| Usar o endpoint compatível com o Amazon EC2 | 166 |
| Início automático de instâncias compatíveis com o Amazon EC2 com modelos de execução | 183 |
| Usar o Block Storage com suas instâncias compatíveis com o EC2 | 185 |
| Grupos de segurança em dispositivos Snow | 186 |
| Metadados da instância e dados do usuário compatíveis | 186 |
| Solução de problemas do Amazon EC2 | 189 |
| Usando DataSync para transferir arquivos | 190 |
| Gerenciando a interface NFS | 192 |
| Configuração NFS para dispositivos da Família Snow | 193 |
| Usando AWS IoT Greengrass em instâncias compatíveis com EC2 | 198 |
| Configurando sua instância compatível com Amazon EC2 | 198 |
| Portas necessárias para usar AWS serviços | 201 |
| Devolvendo o dispositivo Snowcone | 202 |
| Desconecte o dispositivo Snowcone | 202 |
| Proteção de dados no seu dispositivo | 203 |
| Protegendo seu AWS Snowcone | 203 |
| Validação de tags NFC | 204 |
| Noções básicas sobre status de trabalho | 206 |

| | |
|---|-----|
| Notificações | 208 |
| Como o Snow usa o Amazon SNS | 208 |
| Criptografando tópicos do SNS para alterações no status do trabalho do Snow | 208 |
| Configurando uma política de chaves KMS gerenciada pelo cliente | 209 |
| Exemplos de notificação do SNS | 210 |
| Noções básicas sobre o processo de pedido | 223 |
| Noções básicas sobre o processo de envio | 223 |
| Devolvendo um dispositivo Snowcone | 223 |
| Usando o AWS Management Console | 224 |
| Como solicitar o Snowcone a partir do console | 224 |
| Uso de APIs de gerenciamento de trabalhos | 224 |
| Usos comuns do JMAPI | 224 |
| Cadeias de caracteres obrigatórias do JMAPI | 225 |
| Endpoints JMAPI | 225 |
| Comandos da JMAPI CLI | 225 |
| Exemplos | 226 |
| Trabalhos no EC2 | 227 |
| Configurar uma AMI para usar SSH para conectar-se às instâncias de computação iniciadas no dispositivo | 228 |
| Criar seu trabalho usando o console | 229 |
| Criar seu trabalho usando a AWS CLI | 229 |
| Considerações de remessa | 231 |
| Preparando um AWS Snowcone dispositivo para envio | 231 |
| Restrições de envio conforme a região | 232 |
| Envio de um AWS Snowcone dispositivo | 233 |
| Empresas de remessa | 233 |
| Atualizar dispositivos Snowcone | 242 |
| Pré-requisitos | 243 |
| Download de atualizações | 243 |
| Instalação de atualizações | 245 |
| Atualizar o certificado SSL | 248 |
| Atualizando suas AMIs do Amazon Linux 2 em dispositivos da Família Snow | 249 |
| Práticas recomendadas | 251 |
| Segurança | 251 |
| Rede | 252 |
| Gerenciamento de recursos | 252 |

| | |
|--|-------|
| Gerenciamento de instâncias compatíveis com o EC2 | 252 |
| Performance | 253 |
| Cotas do Snowcone | 254 |
| Cotas de recursos computacionais | 254 |
| Limitações para enviar um dispositivo Snowcone | 255 |
| Limitações de processamento do Snowcone retornado para importação | 256 |
| Disponível Regiões da AWS | 256 |
| Solução de problemas | 257 |
| Solucionar problemas com instâncias de computação | 257 |
| Problemas de rede | 257 |
| O endereço IP é 0.0.0.0 | 257 |
| Não é possível desbloquear o dispositivo | 258 |
| Instância compatível com EC2 em problemas de sincronização do DataSync | 258 |
| Erro: falha ao iniciar a instância | 258 |
| Problemas de transferência de dados | 258 |
| Acesso negado pelo servidor | 258 |
| Tempo limite de conexão durante a transferência de dados | 259 |
| Spawn Showmount ENOENT | 259 |
| Solução de problemas na devolução de dispositivos da Família Snow | 260 |
| Referência da API | 261 |
| Histórico do documento | 262 |
| AWS Glossário | 269 |
| | cclxx |

O que é AWS Snowcone?

AWS Snowcone é um dispositivo portátil, robusto e seguro para computação de ponta e transferência de dados. Você pode usar um dispositivo Snowcone para coletar, processar e mover dados para o Nuvem AWS, seja off-line, enviando o dispositivo para AWS, ou on-line, usando AWS DataSync

Pode ser difícil executar aplicativos em ambientes periféricos austeros (sem datacenter) ou onde há falta de conectividade de rede consistente. Esses locais geralmente não têm o espaço, a energia e o resfriamento necessários para o equipamento de TI do datacenter.

O Snowcone está disponível em duas versões:

- Snowcone: o Snowcone tem duas vCPUs, 4 GB de memória e 8 TB de armazenamento baseado em disco rígido (HDD).
- Snowcone SSD: o Snowcone SSD tem duas vCPUs, 4 GB de memória e 14 TB de armazenamento baseado em unidade de estado sólido (SSD).

Com duas CPUs e terabytes de armazenamento, um dispositivo Snowcone pode executar workloads de computação de borda que usam instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e armazenar dados com segurança.

Os dispositivos Snowcone são pequenos (8,94" x 5,85" x 3,25" / 227 mm x 148,6 mm x 82,65 mm), portanto, podem ser colocados ao lado de máquinas em uma fábrica para coletar, formatar e transportar dados de volta para armazenamento e análise. AWS Um dispositivo Snowcone pesa cerca de 4,5 libras (2 kg), então você pode carregá-lo na mochila, usá-lo com operação baseada em bateria e usar a interface Wi-Fi para coletar dados do sensor.

Note

O Wi-Fi está disponível somente Regiões da AWS na América do Norte.

Os dispositivos Snowcone oferecem uma interface com suporte para Network File System (NFS). Os dispositivos Snowcone oferecem suporte à transferência de dados de aplicativos baseados em arquivos em servidores on-premises do Windows, Linux e macOS por meio da interface NFS.

Por exemplo AWS Snowball, AWS Snowcone tem várias camadas de recursos de criptografia de segurança. Você pode usar qualquer um desses serviços para coletar, processar, transferir dados e executar cargas de trabalho de computação de ponta que usam instâncias compatíveis com o Amazon EC2. AWS O Snowcone foi projetado para necessidades de migração de dados de até dezenas de terabytes. Ele pode ser usado em ambientes com restrição de espaço onde os dispositivos Snowball Edge não cabem.

Casos de uso

Você pode usar AWS Snowcone dispositivos para os seguintes casos de uso:

- Para aplicativos de computação de ponta, para coletar dados, processar os dados para obter uma visão imediata e, em seguida, transferir os dados on-line para a AWS.
- Transferir dados gerados continuamente por sensores ou máquinas on-line para uma fábrica ou AWS em outros locais periféricos.
- Para distribuir mídia, conteúdo científico ou outro conteúdo dos serviços de AWS armazenamento para seus parceiros e clientes.
- Para agregar conteúdo transferindo conteúdo de mídia, científico ou outro conteúdo de seus locais da borda para a AWS.
- Para cenários únicos de migração de dados em que seus dados estão prontos para serem transferidos, o Snowcone oferece uma maneira rápida e econômica de transferir até 8 TB ou 14 TB de dados para Nuvem AWS o enviando o dispositivo de volta para. AWS

Para implantações móveis, um dispositivo Snowcone pode funcionar com a energia da bateria especificada. Para uma workload leve com 25% de uso da CPU, o dispositivo pode funcionar com bateria por até aproximadamente 6 horas. Você pode usar a interface Wi-Fi em seu dispositivo Snowcone para coletar dados de sensores sem fio. Um AWS Snowcone dispositivo é de baixo consumo de energia, portátil, leve e resistente a vibrações, então você pode usá-lo em uma ampla variedade de locais remotos e austeros.

Note

O Wi-Fi está disponível somente Regiões da AWS na América do Norte.

Definição de preço

Você pode solicitar um dispositivo Snowcone pagando por uso e mantê-lo por até quatro anos. Para obter informações sobre AWS Snowcone preços e taxas, consulte [AWS Snowcone preços](#).

Como AWS Snowcone funciona

O AWS Snowcone é um dispositivo portátil usado para computação de borda e transferência de dados. Para começar, você solicita um ou mais dispositivos Snowcone no AWS Management Console com base na quantidade de dados que você precisa transferir e no desempenho computacional necessário. Os buckets e dados do Amazon Simple Storage Service (Amazon S3) e as imagens de máquina da Amazon (AMIs) do Amazon Elastic Compute Cloud (Amazon EC2) que você escolhe são automaticamente configuradas, criptografadas e pré-instaladas em seus dispositivos. O AWS DataSync agente também é pré-instalado antes de seus dispositivos serem enviados para você.

Quando seu dispositivo chegar, você o conectará à sua rede on-premises e definirá o endereço IP manual ou automaticamente com o Protocolo de Configuração Dinâmica de Host (DHCP). Você deve baixar e instalar AWS OpsHub for Snow Family um aplicativo de interface gráfica do usuário (GUI) para gerenciar seu dispositivo Snowcone. Você pode instalá-lo em qualquer computador cliente Windows ou macOS, como um laptop.

Ao abrir AWS OpsHub e desbloquear o dispositivo, você vê um painel mostrando seu dispositivo e as métricas do sistema. Em seguida, você pode iniciar instâncias para implantar seus aplicativos de borda ou migrar seus dados para o dispositivo com apenas alguns cliques no AWS OpsHub.

Quando seu trabalho de computação ou transferência de dados é concluído e o dispositivo está pronto para ser devolvido, a etiqueta de remessa E Ink atualiza automaticamente o endereço de devolução, garantindo que o dispositivo Snowcone seja entregue na AWS instalação correta. Quando o dispositivo é enviado, você pode receber o status de rastreamento por meio de mensagens enviadas pelo Amazon Simple Notification Service (Amazon SNS), textos e e-mails gerados ou diretamente do console.

Tópicos

- [AWS Snowcone fluxo de trabalho](#)
- [Como funcionam os trabalhos de importação](#)
- [Para armazenamento do trabalho de importação](#)
- [Para armazenamento de trabalho de computação](#)

AWS Snowcone fluxo de trabalho

Você pode criar três tipos de trabalho diferentes. Embora os tipos de trabalho sejam diferentes em seus casos de uso, todos eles têm o seguinte fluxo de trabalho para solicitar, receber e devolver o dispositivo.

O fluxo de trabalho

1. Crie o trabalho: você cria cada trabalho no Console de Gerenciamento da família AWS Snow ou programaticamente por meio da API de gerenciamento de trabalhos e escolhe um tipo de dispositivo, Snowcone ou Snowcone SSD, dependendo do seu caso de uso. Você pode acompanhar o status do trabalho na API Snowcone AWS Management Console ou por meio dela.
2. Um dispositivo está preparado para seu trabalho — AWS prepara um AWS Snowcone dispositivo para seu trabalho, e o status do seu trabalho muda para Preparando Snowcone.
3. Um dispositivo é enviado a você pela transportadora da região: a transportadora assume a partir daqui, e o status do trabalho muda para Em trânsito. Você pode encontrar seu número de rastreamento e um link para o site de rastreamento no Console de Gerenciamento da família AWS Snow console ou com a API de gerenciamento de tarefas. Para obter informações sobre qual é a transportadora da região, consulte [Considerações de envio para AWS Snowcone](#).
4. Adquira uma fonte de alimentação Snowcone: para diminuir a pegada, os dispositivos Snowcone não são fornecidos com uma fonte de alimentação. O Snowcone usa uma fonte de alimentação conectada USB-C de 45 watts. Também pode ser alimentado por uma bateria portátil. Para ter mais informações, consulte [AWS Snowcone Fonte de alimentação e acessórios](#).
5. Receba o dispositivo — Alguns dias depois, a transportadora da sua região entrega o AWS Snowcone dispositivo no endereço que você forneceu quando criou o trabalho. O status do seu trabalho muda para Entregue a você. O dispositivo não chega em uma caixa porque ele é seu próprio contêiner de remessa.
6. Obtenha suas credenciais e baixe o aplicativo AWS OpsHub ou cliente Snowball Edge para Snow Family — Prepare-se para começar a transferir dados obtendo suas credenciais, seu manifesto de trabalho e o código de desbloqueio do manifesto e, em seguida, baixando o cliente Snowball Edge.
 - Obtenha o manifesto para o seu dispositivo no console ou com a API de gerenciamento de trabalhos quando o dispositivo estiver on-premises na sua localização. O manifesto é usado para autenticar seu acesso ao dispositivo. O manifesto está criptografado, de forma que somente pode ser descriptografado com o código de desbloqueio.

- O código de desbloqueio é um código de 29 caracteres usado para descriptografar o manifesto. O código de desbloqueio pode ser obtido no console ou com a API de gerenciamento de trabalhos. Para evitar o acesso não autorizado ao dispositivo enquanto ele estiver em suas instalações, recomendamos que você mantenha o código de desbloqueio em um local seguro que seja diferente do local do manifesto.
- AWS OpsHub for Snow Family é um aplicativo para gerenciar dispositivos da família Snow, incluindo o Snowcone. A GUI do AWS OpsHub for Snow Family ajuda você a configurar e gerenciar dispositivos Snowcone para que você possa executar rapidamente suas workloads de computação de borda e migrar dados para a Nuvem AWS. Com apenas alguns cliques, você pode usar AWS OpsHub para desbloquear e configurar seu dispositivo Snowcone, arrastar e soltar dados, iniciar aplicativos ou monitorar métricas do dispositivo. Você pode baixá-lo e instalá-lo em máquinas clientes Windows ou macOS, como um laptop. Não há custo para usar o AWS OpsHub.

Faça o download AWS OpsHub dos [AWS Snowball recursos](#). Para obter mais informações sobre AWS OpsHub, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

- O Snowball Edge é a ferramenta que você utilizará para gerenciar o fluxo de dados do dispositivo para o destino de dados local.
7. Posicionar o hardware – mova o dispositivo para o datacenter e siga as instruções na caixa para abri-lo. Conecte o dispositivo à fonte de alimentação e à rede local.
 8. Ligar o dispositivo: ligue o dispositivo pressionando o botão de ligar/desligar acima da tela de LCD. Aguarde alguns minutos, e a tela Pronto será exibida.
 9. Obter o endereço IP para o dispositivo – a tela de LCD possui uma guia CONEXÃO. Toque nessa guia e obtenha o endereço IP do AWS Snowcone dispositivo.
 10. Use AWS OpsHub para desbloquear o dispositivo — Para desbloquear o AWS Snowcone dispositivo, você insere o endereço IP do dispositivo, carrega seu manifesto e o código de desbloqueio. AWS OpsHub descriptografa o manifesto e o usa para autenticar seu acesso ao dispositivo. Para obter mais informações sobre AWS OpsHub, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).
 11. Use o dispositivo — Use AWS OpsHub para configurar e gerenciar AWS Snowcone dispositivos para que você possa executar rapidamente suas cargas de trabalho de computação de ponta e transferir dados para a Nuvem AWS. Com apenas alguns cliques, você pode usar AWS OpsHub para desbloquear e configurar seu dispositivo Snowcone, arrastar e soltar dados, iniciar aplicativos

ou monitorar métricas do dispositivo. Para obter detalhes, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

12 Não desconecte os cabos Ethernet ou da fonte de alimentação: não desconecte o cabo Ethernet, a fonte de alimentação USB-C ou a bateria durante as operações de transferência de dados ou computação. Para desligar o dispositivo Snowcone após a conclusão da transferência de dados ou do trabalho de computação, pressione o botão liga/desliga.

13 Prepare o dispositivo para a viagem de volta — Depois de terminar de usar o dispositivo no local, pressione o botão liga/desliga acima da tela LCD para desligá-lo. Desconecte o dispositivo e guarde seus cabos de alimentação no compartimento de cabos na parte superior do dispositivo e feche as três portas do dispositivo. Agora o dispositivo está pronto para ser devolvido.

14 A operadora da sua região devolve o dispositivo para AWS — Quando a operadora tem o AWS Snowcone dispositivo, o status do trabalho muda para Em trânsito para AWS.

Como funcionam os trabalhos de importação

Você pode usar o Snowcone para transferir dados on-line entre seu dispositivo e os serviços AWS de armazenamento usando AWS DataSync. Você também pode transferir dados offline dos seus dispositivos de armazenamento on-premises para o seu dispositivo Snowcone.

Transferência de dados on-line entre o Snowcone e os serviços AWS de armazenamento com DataSync

[AWS DataSync](#) é um serviço de transferência de dados on-line que simplifica, automatiza e acelera a cópia de grandes quantidades de dados de e para serviços de AWS armazenamento pela Internet ou AWS Direct Connect. Um AWS DataSync agente está pré-instalado em seu dispositivo Snowcone e é usado para transferir dados entre o dispositivo e os buckets Amazon S3, os sistemas de arquivos Amazon Elastic File System (Amazon EFS) e o Amazon FSx for Windows File Server. DataSync lida automaticamente com a movimentação de arquivos e objetos, agendando transferências de dados, monitorando o progresso das transferências, criptografando dados, verificando transferências de dados e notificando os clientes sobre quaisquer problemas.

O DataSync agente é pré-instalado em seu dispositivo Snowcone como uma Amazon Machine Image (AMI) durante a preparação do trabalho no Snowcone. Para transferir dados on-line para AWS, conecte o dispositivo Snowcone à rede externa e use AWS OpsHub for Snow Family ou o AWS Command Line Interface (AWS CLI) para iniciar a DataSync AMI do agente. Ative o DataSync agente usando o AWS Management Console ou AWS CLI. Em seguida, configure sua tarefa de

transferência de dados on-line entre o armazenamento do AWS Snowcone Network File System (NFS) e o Amazon S3, o Amazon EFS ou o Amazon FSx.

Você pode usar a DataSync corrida no Snowcone para o seguinte:

- Para aplicativos de computação de ponta, para coletar dados, processar os dados para obter uma visão imediata e, em seguida, transferir os dados on-line para a AWS.
- Para transferir dados gerados continuamente por sensores ou máquinas on-line para a AWS em uma fábrica ou outros locais de borda.
- Para distribuir mídia, conteúdo científico ou outro conteúdo on-line dos serviços de AWS armazenamento para seus parceiros e clientes.
- Para agregar conteúdo transferindo mídia, conteúdo científico ou outro conteúdo on-line de seus locais da borda para a AWS.

Para fluxos de trabalho únicos de computação de borda ou transferência de dados ou para fluxos de trabalho Snowcone em locais periféricos sem um link de rede de longa distância (WAN) ou largura de banda de WAN inadequada, recomendamos enviar o dispositivo Snowcone de volta para concluir a transferência de dados. AWS

Transferência de dados offline entre o Snowcone e o Amazon S3

Para trabalhos de importação de dados offline, você conecta o dispositivo Snowcone à sua rede local e o usa AWS OpsHub para desbloquear o dispositivo. Faça o AWS OpsHub download na página de [AWS Snowball recursos](#). Você pode copiar dados de dispositivos de armazenamento locais para o seu dispositivo Snowcone por meio da interface NFS. Depois de copiar os dados para o seu dispositivo Snowcone, a etiqueta de remessa E Ink no dispositivo ajuda a garantir que o dispositivo seja enviado automaticamente para a instalação correta AWS. Você pode rastrear o dispositivo Snowcone usando mensagens de texto ou e-mails gerados pelo Amazon SNS e o console.

Para armazenamento do trabalho de importação

Internamente, um dispositivo Snowcone contém 8 TB ou 14 TB de armazenamento em disco que pode ser usado com o serviço interno do Network File System (NFS) ou com instâncias locais compatíveis com o Amazon EC2 por meio de uma apresentação de volume local do Amazon Elastic Block Store (Amazon EBS). Você pode usar 8 TB ou 14 TB para o volume de armazenamento NFS e 150 GB para o volume de armazenamento HDD (sbg1) Amazon EBS com capacidade otimizada.

Para armazenamento de trabalho de computação

Se o tipo de trabalho for computação local, você poderá criar um total de 8 TB ou 14 TB de volumes Amazon EBS de HDD (sbg1) local otimizado para capacidade e anexá-los a instâncias compatíveis com o Amazon EC2. O uso de volumes do Amazon EBS permite que as instâncias locais compatíveis com o Amazon EC2 acessem mais capacidade local do que apenas o volume raiz. Como esse é somente o armazenamento local, os dados gravados nos volumes do Amazon EBS são perdidos quando o dispositivo é devolvido, AWS pois não podem ser importados para o Amazon S3.

Note

O servidor NFS não está disponível para trabalhos de computação. Se você precisar importar ou exportar dados de ou para o agente Nuvem AWS ou executar um AWS DataSync agente, não escolha o tipo de tarefa de computação local ao fazer seu pedido.

AWS Snowcone Especificações do dispositivo

Esta seção fornece informações sobre especificações e requisitos de AWS Snowcone dispositivos para hardware, rede, Wi-Fi e fonte de alimentação.

Tópicos

- [Resumo de atributos e especificações](#)
- [Hardware e rede](#)
- [AWS Snowcone Especificações de Wi-Fi](#)
- [Especificações de robustez](#)
- [AWS Snowcone Fonte de alimentação e acessórios](#)
- [Desempenho de disco e CPU](#)

Resumo de atributos e especificações

A tabela a seguir resume os atributos e as especificações do dispositivo Snowcone.

| Item | Especificação |
|---------------------------------|--|
| Cenário de uso | Internet das Coisas industrial (IoT), transporte, IoT de saúde, distribuição de conteúdo, computação de borda tática, logística, veículo autônomo, migração de dados |
| Tamanho do dispositivo | 9 polegadas de comprimento, 6 polegadas de largura e 3 polegadas de altura (227 mm x 148,6 mm x 82,65 mm) |
| Peso do dispositivo | 4,5 libras (2,04 kg) para Snowcone e 4,6 libras (2,09 kg) SSD Snowcone |
| Capacidade de armazenamento | 8 TB utilizáveis para Snowcone e 14 TB utilizáveis para Snowcone SSD |
| Opções de computação integradas | Imagens de máquina da Amazon (AMIs) do Amazon EC2 |

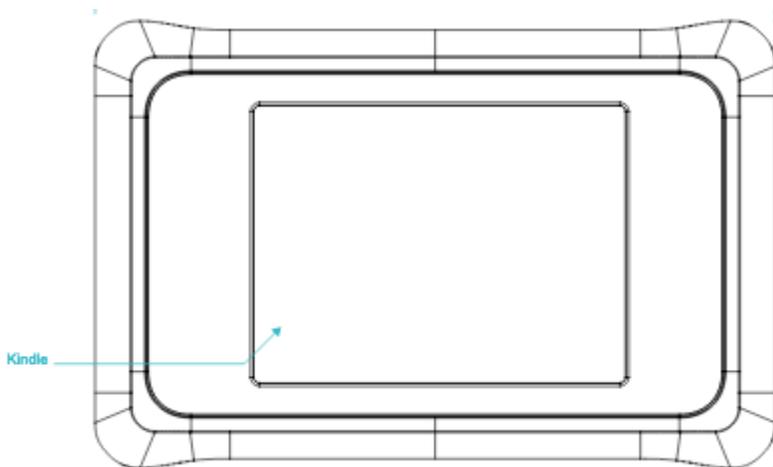
| Item | Especificação |
|--|--|
| Criptografia | Sim, 256 bits |
| Transferências através do Network File System (NFS, Sistema de arquivos de rede) | Sim |
| Transferências por meio da API do Amazon S3 | Não |
| Portabilidade | Operação baseada em bateria |
| Sem fio | Wi-Fi <div data-bbox="480 863 1507 1083"><p> Note O Wi-Fi está disponível somente Regiões da AWS na América do Norte.</p></div> |
| Número de vCPUs utilizáveis | 2 vCPUs |
| Memória disponível | 4 GB |
| Interfaces de rede | 2x 1/10 gigabit (Gb) - RJ45 |
| AWS DataSync agente pré-instalado | Sim |
| Vida útil típica | Transferência de dados offline ou online: dias a semanas Computação de borda: semanas a meses |
| Duração máxima do trabalho | Computação de borda ou transferência contínua de dados: até 360 dias |

Hardware e rede

Um dispositivo Snowcone fornece 8 TB ou 14 TB de armazenamento disponível. Ele executa instâncias específicas do Amazon Elastic Compute Cloud (Amazon EC2) com duas CPUs disponíveis e 4 GB de memória disponível para suportar seus aplicativos e funções. AWS IoT Greengrass Nesta seção, você pode encontrar informações sobre o dispositivo físico, como as interfaces, o botão liga/desliga e os requisitos de energia conforme aparecem em diferentes visualizações do dispositivo.

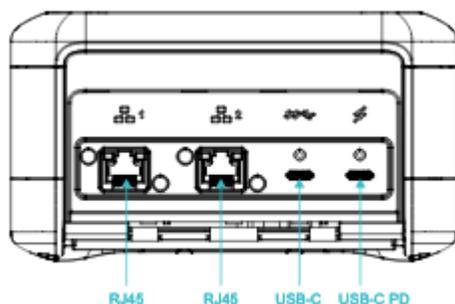
Vista superior

A superfície superior do dispositivo Snowcone inclui uma tela de toque E-Ink integrada que é usada como interface de operação para configurar redes com e sem fio. Também serve como display para uma etiqueta eletrônica de remessa. A etiqueta de remessa eletrônica é pré-programada com etiquetas de remessa de saída e de entrada que mudam automaticamente depois que o dispositivo é ligado pela primeira vez.



Painel traseiro

Você faz todas as conexões de cabos no painel traseiro. Esta seção descreve cada conector.



Alimentação

A alimentação é fornecida ao dispositivo pela conexão USB-C mais à direita, usando um adaptador de alimentação adequado que pode fornecer pelo menos 45 W.

Note

AWS Snowcone não inclui uma fonte de alimentação porque é fornecida com o menor formato possível. Para obter detalhes, consulte [AWS Snowcone Fonte de alimentação e acessórios](#).

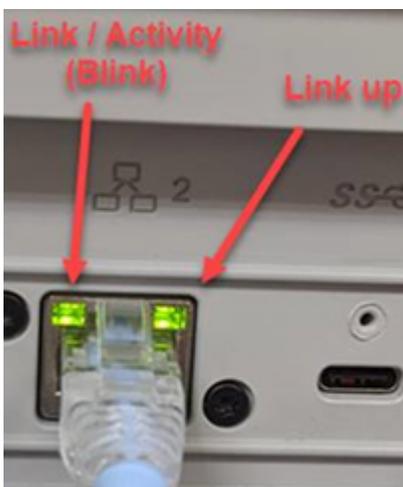
USB

A primeira conexão USB-C não está ativa.

Conectores Ethernet 1 e 2

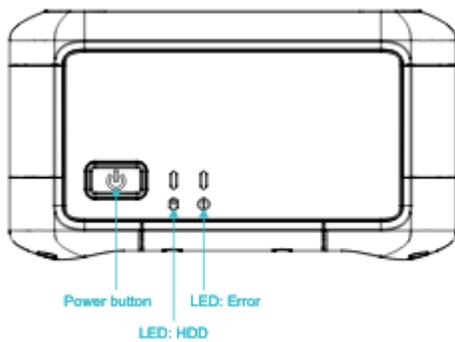
Para redes com fio, o dispositivo Snowcone fornece duas portas que negociam automaticamente redes Ethernet de 1 gigabit (Gb) ou 10 Gb.

Portas Ethernet RJ45 10/1G Base-T: essas portas negociam automaticamente entre 10 Gb e 1 Gb com base na capacidade de conexão da extremidade oposta. Eles não negociam velocidades inferiores a 1 Gb (por exemplo, 100 Mb ou 10 Mb). O LED de link está localizado à direita de cada conector e o LED de atividade está à esquerda.



Painel frontal

O painel frontal contém o botão liga/desliga e os LEDs de status.



Interruptor de alimentação

Para ligar o dispositivo, pressione momentaneamente o botão liga/desliga. O botão acende, a tela do E-Ink muda para uma barra de progresso e *Aguarde* é exibida.

Para desligar o dispositivo, segure o botão liga/desliga por dois segundos ou até que a tela do E-Ink mostre *Aguarde*.

Note

Manter pressionado o botão liga/desliga por mais de cinco segundos força o dispositivo a desligar. Fazer isso não é recomendado porque pode causar a perda de dados nos buffers. Após a perda de energia CA, o dispositivo restaura automaticamente a energia para o último estado operacional.

LEDs de status

Dois LEDs de status estão localizados ao lado do botão liga/desliga. O LED esquerdo pisca com a atividade do disco e o LED direito acende se houver uma condição de falha.

AWS Snowcone Especificações de Wi-Fi

AWS Snowcone suporta redes Wi-Fi gigabit com o padrão IEEE 802.11ac e também redes 802.11abgn. Para maximizar o throughput sem fio do Snowcone, use canais 2x2 802.11ac de 160 MHz, que podem ser até 10 vezes mais rápidos do que as redes 1x1 802.11bgn de linha de base. As especificações Wi-Fi do Snowcone são IEEE 802.11abgn+ac, 2x2, MIMO, banda dupla de 2 GHz e 5 G (160 MHz). As frequências operacionais são 2 GHz e 5 GHz.

Você pode conectar o Snowcone à sua rede on-premises usando um cabo Ethernet físico ou pode conectá-lo sem fio usando Wi-Fi. Com a conexão Wi-Fi, você pode gerenciar o dispositivo Snowcone

usando AWS OpsHub e transferir dados entre o Snowcone e os dispositivos de armazenamento locais.

Note

O Wi-Fi está disponível somente Regiões da AWS na América do Norte.

Especificações de robustez

AWS Snowcone os dispositivos são projetados para atender aos rigorosos padrões de robustez, incluindo ISTA-3A, ASTM D4169 e MIL-STD-810G para choques em queda livre, vibração operacional e muito mais. Eles são projetados para tolerar quedas de até 3,8 pés (1,15 metros). Eles também atendem ao padrão IEC da Marcação de Proteção Internacional IP65, o que significa que são à prova de poeira (não permitindo a entrada de poeira no gabinete quando selados) e resistentes à água (incluindo proteção contra jatos de água em todos os lados).

Os dispositivos têm uma ampla faixa de temperatura operacional, desde congelamento (0 graus C ou 32 graus F) até condições desérticas (Snowcone: 38 graus C ou 100 graus F; Snowcone SSD: 45 graus C ou 113 graus F). Quando armazenados ou enviados, os dispositivos Snowcone suportam temperaturas ainda mais severas (-32 graus C ou -25,6 graus F a 63 graus C ou 145,4 graus F).

AWS Snowcone Fonte de alimentação e acessórios

AWS Snowcone os dispositivos não incluem uma fonte de alimentação ou um cabo Ethernet (RJ45) porque são fornecidos com o menor formato possível. Você tem a opção de operar seu dispositivo Snowcone por meio de uma fonte de alimentação plug-in ou de uma bateria. Aqui estão os detalhes para orientá-lo ao solicitar uma fonte de alimentação e um cabo Ethernet:

Adaptador de alimentação USB-C: use um adaptador de alimentação USB-C com o dispositivo Snowcone para alimentação conectada ou para ambientes operacionais estacionários (não móveis). Para alimentar seu dispositivo Snowcone, você pode comprar um dos seguintes adaptadores de alimentação AWS USB-C testados:

- [Adaptador de alimentação USB-C de 61 W da Apple](#)
- [Adaptador AC padrão Lenovo USB-C de 65 W](#)

Ou você pode usar qualquer adaptador de alimentação USB-C com capacidade nominal de 45 W ou mais e a temperatura do ambiente.

Bateria USB-C: use uma bateria USB-C para alimentar o dispositivo Snowcone em ambientes operacionais móveis ou portáteis. Para alimentar seu dispositivo Snowcone, você pode usar um [notebook Dell Power Bank Plus — USB C, 65Wh - PW7018LC](#) ou qualquer bateria USB-C com capacidade mínima de 45 W.

Cabo Ethernet (RJ45): para conectar o dispositivo Snowcone à sua rede local, use um cabo Ethernet (RJ45). Se você não tiver, deverá comprar um.

Desempenho de disco e CPU

AWS Snowcone é um dispositivo de transferência de dados/computação de ponta desenvolvido especificamente. O desempenho do disco e da CPU variará dependendo de vários fatores. Alguns exemplos de números de desempenho para transferência estão em [Desempenho do Snowcone](#)

Configurando AWS para AWS Snowcone

Antes de criar seu primeiro AWS Snowcone trabalho, siga estas instruções para garantir que você prepare adequadamente seu ambiente.

Tópicos

- [Inscreva-se para AWS](#)

Inscreva-se para AWS

Quando você se inscreve no Amazon Web Services (AWS), sua conta é automaticamente cadastrada em todos os AWS serviços. AWS cobra apenas pelos serviços que você usa. Depois de configurar sua conta, você pode solicitar, configurar e gerenciar seu AWS Snowcone dispositivo por meio do Console de Gerenciamento da família AWS Snow. Para obter mais informações sobre definição de preços e taxas para o Snowcone, consulte [Preços do AWS Snowcone](#).

Se você já tem um Conta da AWS, anote seu Conta da AWS número. Se você não tiver um Conta da AWS, siga estas etapas:

Para criar um Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar [tarefas que requerem o acesso de usuário-raiz](#).

Anote seu Conta da AWS número, que você precisará para a próxima etapa.

Antes de encomendar um dispositivo Snowcone

AWS Snowcone é um serviço específico da região, portanto, certifique-se de que o serviço esteja disponível na sua região antes de planejar o trabalho. Certifique-se de que sua localização e o bucket do Amazon S3 estejam dentro dos mesmos, Região da AWS pois isso afetará sua capacidade de solicitar o dispositivo. Há limitações no envio do dispositivo Snowcone para fora das fronteiras do país de uma região. Para ter mais informações, consulte [Restrições de envio conforme a região](#).

Remessas internacionais para locais fora do seu Região da AWS são aceitas na Console de Gerenciamento da família AWS Snow lista de clientes autorizados para um conjunto selecionado de locais de regiões específicas (como EUA para México). Você deve discutir o destino, os custos e o prazo para atender a essas solicitações com sua equipe de contas.

Como parte do processo de pedido, você cria uma função AWS Identity and Access Management (IAM) e uma chave AWS Key Management Service (AWS KMS). O KMS protege as chaves de criptografia usadas para proteger os dados em cada dispositivo. Para obter mais informações, consulte [Criação de um trabalho para solicitar um dispositivo Snow Family](#).

Tópicos

- [Perguntas sobre o ambiente local](#)
- [Como trabalhar com arquivos com caracteres especiais](#)
- [Uso do Amazon EC2 no Snowcone](#)

Perguntas sobre o ambiente local

Compreender seu conjunto de dados e como o ambiente local está configurado ajudará você a concluir sua transferência de dados. Considere o seguinte antes de fazer seu pedido.

Os dados serão acessados durante a transferência?

Para evitar corromper os dados, não desconecte um dispositivo Snowcone ou altere as configurações de rede enquanto estiver transferindo dados. Os arquivos devem estar em um estado estático enquanto são gravados no dispositivo. Arquivos que são modificados enquanto estão sendo gravados podem resultar em conflitos de leitura/gravação.

Como trabalhar com arquivos com caracteres especiais

É importante observar que, se seus arquivos contiverem caracteres especiais, você poderá encontrar erros. Embora o Amazon S3 permita caracteres especiais, é altamente recomendável que você evite os seguintes caracteres:

- Barra invertida (“\”)
- Chave esquerda (“{”)
- Chave direita (“}”)
- Colchete esquerdo (“[”)
- Colchete direito (“]”)
- Sinal de menor (“<”)
- Sinal de maior (“>”)
- Caracteres ASCII não imprimíveis (128-255 caracteres decimais)
- Circunflexo (“^”)
- Caractere de porcentagem (“%”)
- Crase (“`”)
- Pontos de interrogação
- Til (“~”)
- Caractere de libra (“#”)
- Barra vertical (“|”)

Se seus arquivos tiverem um ou mais desses caracteres, renomeie-os antes de copiá-los para o AWS Snowcone dispositivo. Os usuários do Windows que têm espaços nos nomes dos arquivos devem ter cuidado ao copiar objetos individuais ou executar um comando recursivo. Coloque objetos individuais que contenham espaçamento no nome com aspas. Alguns exemplos dessas alterações são:

| Sistema operacional | Nome do arquivo: test file.txt |
|---------------------|---|
| Windows | “C:\Users\ <username>\desktop\test file.txt”</username> |
| Mac | /Users/<username>/test\ file.txt |

| | |
|---------------------|---------------------------------------|
| Sistema operacional | Nome do arquivo: test file.txt |
| Linux | /home/<username>/test\ file.txt |

Note

Os únicos metadados do objeto transferidos são o nome e o tamanho do objeto. No entanto, AWS DataSync preserva as listas de controle de acesso (ACLs). Para obter informações, consulte [Como DataSync manipular metadados e arquivos especiais](#) no Guia do AWS DataSync usuário.

Uso do Amazon EC2 no Snowcone

Esta seção fornece uma visão geral das instâncias de computação compatíveis com o Amazon EC2 em um dispositivo AWS Snowcone .

Você deve usar as instâncias compatíveis com o Amazon EC2 quando tiver um aplicativo em execução na borda que seja gerenciado e implantado como uma máquina virtual (uma imagem de máquina da Amazon, ou AMI). O Snowcone é compatível com o tipo de instância SNC1 com três instâncias, incluindo snc1.micro (1 CPU e 1 GB de RAM), snc1.small (1 CPU e 2 GB de RAM) e snc1.medium (2 CPUs e 4 GB de RAM). O suporte para instâncias compatíveis com EC2 no Snowcone permite que você crie e teste seu aplicativo no Amazon EC2. Você pode habilitar e provisionar AMIs compatíveis com EC2 durante a criação do AWS Snowcone trabalho usando o AWS Management Console AWS Snowball SDK ou. AWS CLI

Tipos de instância do Amazon EC2 compatíveis

Use os seguintes tipos de instância do Amazon EC2 para seus trabalhos de computação.

snc1.micro: 1 núcleo de CPU, 1 GB de RAM

snc1.small: 1 núcleo de CPU, 2 GB de RAM

snc1.medium: 2 núcleos de CPU, 4 GB de RAM

Use AWS OpsHub para gerenciar suas instâncias no Snowcone. Faça o AWS OpsHub download no site de [AWS Snowball recursos](#). Depois de desbloquear o dispositivo usando AWS OpsHub, navegue até a página do Amazon EC2. Escolha Criar instância para criar uma instância compatível com EC2

com base na AMI que você pré-carregou no dispositivo quando criou o trabalho. Em seguida, você pode se conectar às instâncias e executar seu aplicativo de borda. AWS OpsHub também fornece botões de um único clique para iniciar, parar, encerrar e reinicializar suas instâncias compatíveis com EC2. Para ter mais informações, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

Quando terminar de usar seu dispositivo, devolva-o para AWS. Se o dispositivo foi usado em um trabalho de importação, os dados transferidos usando a interface de arquivos são importados para o Amazon S3 com a interface NFS do Snowcone. Caso contrário, apagaremos completamente o dispositivo quando ele for devolvido. AWS Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Important

Os dados nas instâncias de computação em execução em um Snowcone não são importados para a AWS.

Diferença entre instâncias compatíveis com Amazon EC2 e Amazon EC2 em dispositivos da família Snow

AWS As instâncias compatíveis com o Snow Family EC2 permitem que os clientes usem e gerenciem instâncias compatíveis com o Amazon EC2 usando um subconjunto de APIs do EC2 e um subconjunto de AMIs.

Definição de preço para instâncias de computação no Snowcone

Existem custos adicionais associados ao uso de instâncias de computação. Para obter mais informações, consulte [Preços do AWS Snowcone](#).

Pré-requisitos

Antes de criar o trabalho, lembre-se das seguintes informações:

- Para poder adicionar qualquer AMI ao trabalho, é necessário ter uma AMI criada em sua Conta da AWS e deve ser do tipo de imagem compatível. Atualmente, as AMIs compatíveis se baseiam nas imagens [Amazon Linux 2](#), [CentOS 7 \(x86_64, com updates HVM\)](#) ou [Ubuntu 16.04 LTS, Xenial \(HVM\)](#). É possível obter essas imagens no [AWS Marketplace](#).

Antes de adicionar quaisquer AMI à sua solicitação de criação de trabalho, verifique se você tem uma ou mais AMIs compatíveis em sua conta da AWS. Ao escolher uma AMI no Marketplace, certifique-se de que ela tenha um código de produto e uma plataforma compatíveis. Para ter mais informações, consulte [Verificando códigos de produto e detalhes da plataforma de AWS Marketplace AMIs](#).

- Todas as AMIs devem ser baseadas no Amazon Elastic Block Store (Amazon EBS), com um único volume.
- Se estiver se conectando a uma instância de computação em execução em um Snowcone, você deverá usar Secure Shell (SSH). Para isso, primeiro você deve adicionar o par de chaves.

Verificando códigos de produto e detalhes da plataforma de AWS Marketplace AMIs

Antes de iniciar o processo de adicionar uma AMI AWS Marketplace ao seu dispositivo da família Snow, certifique-se de que o código do produto e os detalhes da plataforma da AMI sejam compatíveis com seu Região da AWS.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual iniciar suas instâncias e a partir da qual você criará o trabalho para solicitar o dispositivo da família Snow. Você pode selecionar qualquer região que esteja disponível para você, independentemente da sua localização.
3. No painel de navegação, selecione AMIs.
4. Use as opções de filtro e pesquisa para definir o escopo da lista de AMIs exibidas e ver somente as AMIs que correspondem aos seus critérios. Por exemplo, AMIs fornecidas pelo AWS Marketplace, escolha Imagens públicas. Em seguida, use as opções de pesquisa para ampliar ainda mais a lista de AMIs exibidas:
 - (Novo console) Escolha a barra de pesquisa e, no menu, escolha Alias do proprietário, depois o operador = e, em seguida, o valor amazon.
 - (Console antigo) Escolha a barra Search (Pesquisar) e, no menu, escolha Owner (Proprietário) e o valor Amazon images (Imagens da Amazon).

Note

As AMIs de AWS Marketplace incluem aws-marketplace na coluna Fonte.

5. Na coluna ID da AMI, escolha a ID da AMI.
6. No resumo da imagem da AMI, verifique se os códigos do produto são compatíveis com sua região. Para obter mais informações, consulte a tabela abaixo.

Códigos de produto AWS Marketplace AMI compatíveis

| Sistema operacional AMI | Código do produto |
|-------------------------|---------------------------|
| Ubuntu Server 14.04 LTS | b3dl4415quatdndl4qa6kcu45 |
| CentOS 7 (x86_64) | aw0evgkw8e5c1q413zgy5pjce |
| Ubuntu 16.04 LTS | csv6h7oyg29b7epjzg7qdr7no |
| Amazon Linux 2 | avyfzznywektkgl5qv5f57ska |
| Ubuntu 20.04 LTS | a8jyynf4hjutohctm41o2z18m |
| Ubuntu 22.04 LTS | 47xbqns9xujfkkjt189a13aqe |

7. Em seguida, certifique-se também de que os detalhes da plataforma contenham uma das entradas da lista abaixo.
 - Amazon Linux, Ubuntu ou Debian
 - Red Hat Linux bring-your-own-license
 - Amazon RDS for Oracle bring-your-own-license
 - Windows bring-your-own-license

Criar uma AMI do Linux de uma instância

Você pode criar uma AMI usando o console ou a linha de comando. Comece com uma AMI existente, execute uma instância, personalize-a, crie uma nova AMI a partir dela e, por fim, execute uma instância de sua nova AMI.

Para criar uma AMI de uma instância usando o console

1. Selecione a AMI baseada em EBS apropriada como ponto inicial para a nova AMI e a configure conforme o necessário antes de iniciar. Para obter mais informações, consulte [Como iniciar uma instância usando o assistente de inicialização de instância](#).
2. Escolha Executar para executar a instância da AMI com EBS que você selecionou. Aceite os valores padrão ao prosseguir no assistente. Para obter mais informações, consulte [Como iniciar uma instância usando o assistente de inicialização de instância](#).
3. Quando a instância estiver sendo executada, conecte-se a ela. É possível executar qualquer uma destas ações em sua instância para personalizá-la de acordo com suas necessidades:
 - Instalar o software e aplicações
 - Copiar dados
 - Reduzir o tempo de inicialização excluindo arquivos temporários, desfragmentando o disco rígido e liberando o espaço livre
 - Anexar volumes adicionais do Amazon EBS
4. (Opcional) Crie snapshots de todos os volumes anexados à instância. Para obter mais informações sobre como criar snapshots, consulte [Criar snapshots do Amazon EBS](#).
5. No painel de navegação, selecione Instâncias e selecione sua instância. Escolha Ações, Imagem e Criar imagem.

Tip

Se essa opção está desabilitada, sua instância não é uma instância baseada no Amazon EBS.

6. Na caixa de diálogo Criar imagem, especifique as informações a seguir e escolha Criar imagem:
 - Nome da imagem: um nome exclusivo para a imagem.
 - Descrição da imagem: uma descrição opcional da imagem, com até 255 caracteres.
 - Sem reinicialização: essa opção é selecionada por padrão. O Amazon EC2 encerra a instância, faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicializa a instância. Selecione Sem reinicialização para impedir o encerramento da sua instância.

⚠ Warning

Se você escolher Sem reinicialização, não poderemos garantir a integridade do sistema de arquivos da imagem criada.

- Volumes da instância: os campos nesta seção permitem que você modifique o volume raiz e adicione outros volumes com armazenamento de instância e com Amazon EBS. Para obter informações sobre cada campo, consulte o ícone *i* próximo a cada campo para mostrar dicas de ferramentas do campo. Alguns aspectos importantes estão listados abaixo.
 - Para alterar o tamanho do volume raiz, localize Raiz na coluna Tipo de volume. Em Tamanho (GiB), insira o valor necessário.
 - Se você selecionar Excluir ao encerrar, quando encerrar a instância criada a partir desta AMI, o volume do EBS será excluído. Se você não selecionar Excluir ao encerrar, quando encerrar a instância, o volume do EBS não será excluído. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância](#) no Guia do usuário do Amazon EC2.
 - Para adicionar o volume do EBS; escolha Adicionar novo volume (que acrescenta uma nova linha). Em Tipo de volume, escolha EBS e preencha os campos da linha. Quando você executa uma instância da nova AMI, os volumes adicionais são anexados automaticamente à instância. Os volumes vazios devem ser formatados e montados. Os volumes baseados em um snapshot devem ser montados.
 - Para adicionar um volume de armazenamento de instâncias, consulte [Adicionar volumes de armazenamento de instâncias a uma AMI](#). Quando você executa uma instância da nova AMI, os volumes adicionais são automaticamente inicializados e montados. Esses volumes não contêm dados de volumes de armazenamento de instâncias da instância em execução na qual a AMI foi baseada.
7. Para visualizar o status da AMI enquanto ela estiver sendo criada, escolha AMIs no painel de navegação. Inicialmente, o status será pendente, mas deverá mudar para após alguns minutos.
- (Opcional) Para visualizar o snapshot que foi criado para a nova AMI, escolha Snapshots. Quando você executa uma instância dessa AMI, usamos esse snapshot para criar o volume do dispositivo raiz.
8. Execute uma instância da nova AMI. Para obter mais informações, consulte [Como iniciar uma instância usando o assistente de inicialização de instância](#).

9. A nova instância em execução contém todas as personalizações que você aplicou em etapas anteriores.

Para criar uma AMI de uma instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Como acessar o Amazon EC2](#).

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

Criar uma AMI do Linux de um snapshot

Se você tiver um instantâneo do volume do dispositivo raiz de uma instância, poderá criar uma AMI a partir desse instantâneo usando a linha de comando AWS Management Console ou a linha de comando.

Como criar uma AMI de um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Elastic Block Store, escolha Snapshots.
3. Selecione o snapshot e escolha Ações, Criar imagem.
4. Na caixa de diálogo Criar imagem de snapshot do EBS, preencha os campos para criar sua AMI e, em seguida, escolha Criar. Se você estiver recriando uma instância-pai, selecione as mesmas opções que a instância-pai.
 - Arquitetura: escolha i386 para 32 bits ou x86_64 para 64 bits.
 - Nome do dispositivo raiz: insira o nome apropriado para o volume raiz. Para obter mais informações, consulte [Nomeação de dispositivos em instâncias do Linux](#).
 - Tipo de virtualização: escolha se as instâncias executadas a partir desta AMI usam virtualização paravirtual (PV) ou máquina virtual de hardware (HVM). Para obter mais informações, consulte [Tipos de virtualização de AMI no Linux](#).
 - (Somente tipo de virtualização PV) ID do kernel e ID do disco RAM: escolha AKI e ARI nas listas. Se você escolher a AKI padrão ou não escolher uma AKI, será necessário especificar uma AKI sempre que você executar uma instância usando essa AMI. Além disso, sua

instância poderá falhar nas verificações de integridade se a AKI padrão for incompatível com a instância.

- (Opcional) Mapeamentos de dispositivos de blocos: adicione volumes ou expanda o tamanho padrão do volume raiz para a AMI. Para obter mais informações sobre como redimensionar um sistema de arquivos em sua instância para um grande volume, consulte [Como estender um sistema de arquivos Linux após um redimensionamento de volume](#).

Para criar uma AMI de um snapshot usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Como acessar o Amazon EC2](#).

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

Conceitos básicos

Esta seção fornece instruções gerais para criar e concluir seu primeiro AWS Snowcone trabalho no Console de Gerenciamento da família AWS Snow. Para obter uma visão geral do AWS Snowcone dispositivo, consulte [Como AWS Snowcone funciona](#).

Esta documentação de introdução pressupõe que você use o [Console de Gerenciamento da família AWS Snow](#) para criar seu trabalho e use o cliente Snowball Edge ou AWS OpsHub for Snow Family o aplicativo para desbloquear AWS Snowcone o dispositivo. Se preferir criar o trabalho de forma programática com mais opções para os trabalhos que está criando, é possível usar a API de gerenciamento de trabalhos. Para obter mais informações, consulte [Referência de API do AWS Snowcone](#).

Antes de começar, você precisa criar um usuário administrador Conta da AWS e um usuário no AWS Identity and Access Management (IAM). Para ter mais informações, consulte [Configurando AWS para AWS Snowcone](#).

Para começar AWS Snowcone, consulte [Criação de um trabalho para solicitar um dispositivo Snow Family](#).

Tópicos

- [Criando um trabalho para solicitar um dispositivo Snow Family](#)
- [Cancelando um trabalho por meio do Console de Gerenciamento da família AWS Snow](#)
- [Obter credenciais para acessar um dispositivo Snow Family](#)
- [Desbloqueando o dispositivo Snow Family](#)
- [Reinicializando o dispositivo da Família Snow](#)

Criando um trabalho para solicitar um dispositivo Snow Family

Para solicitar um dispositivo Snow Family, você cria um trabalho para solicitar um dispositivo Snow Family no Console de Gerenciamento da família AWS Snow. Um trabalho é um termo AWS usado para descrever o ciclo de vida do uso de um dispositivo da família Snow por um cliente. Um trabalho começa quando você solicita um dispositivo, continua quando AWS prepara o dispositivo e o envia para você e você o usa, e é concluído após AWS receber e processar o dispositivo após sua devolução. Os trabalhos são categorizados por tipo: exportação, importação e computação

e armazenamento locais. Para obter mais informações, consulte [Entendendo as tarefas do AWS Snowball Edge](#).

Depois de criar o trabalho para solicitar um dispositivo, você pode usar o Console de Gerenciamento da família AWS Snow para visualizar o status do trabalho e monitorar o progresso do dispositivo que você solicitou enquanto AWS prepara o dispositivo para ser enviado a você e depois que ele for devolvido. Para obter mais informações, consulte [Job Statuses](#). Depois que o dispositivo for devolvido e processado AWS, você poderá acessar um relatório e registros de conclusão do trabalho por meio do Console de Gerenciamento da família AWS Snow. Para obter mais informações, consulte [Obter o relatório e os registros de conclusão do trabalho no console](#).

Os trabalhos também podem ser criados e gerenciados com a API de gerenciamento de trabalhos. Para obter mais informações, consulte a [AWS Snowball Referência da API do](#) .

Tópicos

- [Etapa 1: escolher um tipo de trabalho](#)
- [Etapa 2: escolher as opções de computação e armazenamento](#)
- [Etapa 3: escolha seus atributos e opções](#)
- [Etapa 4: escolha as preferências de segurança, envio e notificação](#)
- [Etapa 5: revise o resumo do trabalho e crie seu trabalho](#)
- [Baixar AWS OpsHub](#)

Etapa 1: escolher um tipo de trabalho

A primeira etapa na criação de um trabalho é determinar o tipo de trabalho de que você precisa e começar a planejá-lo usando o Console de Gerenciamento da família AWS Snow.

Para escolher seu tipo de trabalho

1. Faça login no AWS Management Console e abra [Console de Gerenciamento da família AWS Snow](#). Se esta é a primeira vez que você cria um emprego nisso Região da AWS, você verá a página da Família AWS Snow. Caso contrário, você verá a lista de trabalhos existentes.
2. Se este for seu primeiro emprego, escolha Pedir um dispositivo AWS Snow Family. Se você espera que várias tarefas migrem mais de 500 TB de dados, escolha Criar seu grande plano de migração de dados com mais de 500 TB. Caso contrário, escolha Criar trabalho na barra de navegação à esquerda. Escolha Próxima etapa para abrir a página Planejar seu trabalho.

3. Na seção Nome do trabalho, forneça um nome para seu trabalho na caixa Nome do trabalho.
4. Dependendo da sua necessidade, escolha um dos seguintes tipos de trabalho:
 - Importar para o Amazon S3: peça para a AWS enviar um dispositivo Snowcone vazio para você. Você conecta o dispositivo à sua rede local e configura o dispositivo usando OpsHub. Você copia dados para o dispositivo usando o compartilhamento NFS, os envia de volta e seus dados são enviados para o Amazon S3. AWS
 - Somente computação e armazenamento locais: execute workloads de computação e armazenamento no dispositivo sem transferir dados.

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. Escolha Próximo para continuar.

Etapa 2: escolher as opções de computação e armazenamento

Escolha as especificações de hardware do seu dispositivo da Família Snow, quais das suas instâncias compatíveis com o Amazon EC2 incluir nele, como os dados serão armazenados e os preços.

Para escolher as opções de computação e armazenamento do seu dispositivo

1. Na seção Dispositivos Snow, escolha o dispositivo da Família Snow para fazer o pedido.

Note

Alguns dispositivos da família Snow podem não estar disponíveis, dependendo do Região da AWS tipo de trabalho escolhido e do tipo de trabalho escolhido.

| 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 |

- Na seção Fonte de alimentação Snowcone, escolha Eu fornecerei minha própria fonte de alimentação e cabo Ethernet. Para obter informações sobre fontes de alimentação, consulte [Fonte de alimentação e acessórios do AWS Snowcone](#).
- Na seção Escolha sua opção de preço, no menu Escolha sua opção de preço, escolha o tipo de preço a ser aplicado a esse trabalho. Para saber os preços dos dispositivos, consulte [Definição de preços do AWS Snowcone](#).
- Na seção Selecione o tipo de armazenamento, faça uma escolha de acordo com sua necessidade:
 - Transferência de dados baseada em NFS: use a transferência de dados baseada no Network File System (NFS) para arrastar e soltar arquivos do seu computador nos buckets do Amazon S3 em dispositivos da Família Snow.

Warning

A transferência de dados baseada em NFS não é compatível com o adaptador do S3. Se você continuar com a transferência de dados baseada em NFS, deverá montar o

compartilhamento NFS para transferir objetos. O uso do AWS CLI para transferir objetos falhará.

Consulte [Usando o NFS para transferência de dados offline](#) no Guia do AWS Snowcone usuário para obter mais informações.

5. Se você selecionou a Transferência de dados baseada em NFS como o tipo de armazenamento, na seção **Selecione seus buckets do S3**, faça um ou mais dos seguintes para selecionar um ou mais buckets do S3:
 - a. Escolha o bucket do S3 que deseja usar na lista **Nome do bucket do S3**.
 - b. No campo **Pesquisar um item**, insira o nome total ou parcial de um bucket para filtrar a lista de buckets disponíveis em sua entrada e, em seguida, escolha o bucket.
 - c. Para criar um novo bucket, escolha **Criar um novo bucket do S3**. O novo nome do bucket aparece na lista **Nomes do bucket**. Escolha-o.

É possível incluir um ou mais buckets do S3. Esses buckets aparecem no seu dispositivo como buckets do S3 locais.

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. Na seção **Computar usando instâncias compatíveis com EC2 - opcional**, escolha AMIs compatíveis com Amazon EC2 em sua conta para incluir no dispositivo. Ou, no campo de pesquisa, insira todo ou parte do nome de uma AMI para filtrar a lista de AMIs disponíveis na sua entrada e escolha a AMI.

Para obter mais informações, consulte [Criação de um trabalho com instâncias de computação](#) neste guia.

Esse atributo gera cobranças adicionais. Para obter mais informações, consulte [Preços do AWS Snowball Edge](#).

7. Escolha o botão Próximo.

Etapa 3: escolha seus atributos e opções

Escolha os recursos e as opções a serem incluídos em seu trabalho de dispositivos da AWS Snow Family, incluindo o Amazon EKS Anywhere for Snow, uma AWS IoT Greengrass instância e o recurso de gerenciamento remoto de dispositivos.

Para escolher seus atributos e opções

1. Para habilitar sua rede sem fio em seu dispositivo Snowcone, selecione Ativar conexão sem fio no Snowcone.
2. Para ativar o gerenciamento remoto do seu dispositivo Snow Family pelo AWS OpsHub Snowball Edge Client, selecione Gerenciar seu dispositivo Snow remotamente com nosso cliente AWS OpsHub Snowball.
3. Selecione o botão Próximo.

Etapa 4: escolha as preferências de segurança, envio e notificação

Tópicos

- [Escolher as preferências de segurança](#)
- [Escolha suas preferências de envio](#)
- [Escolher suas preferências de notificação](#)

Escolher as preferências de segurança

A configuração de segurança adiciona as permissões e as configurações de criptografia para o trabalho dos dispositivos da Família AWS Snow para ajudar a proteger seus dados enquanto estão em trânsito.

Para definir a segurança do seu trabalho

1. Na seção Criptografia, escolha a chave KMS que você deseja usar.

- Se você quiser usar a tecla default AWS Key Management Service (AWS KMS), escolha AWS/importexport (default). Essa é a chave padrão que protege seus trabalhos de importação e exportação quando nenhuma outra chave é definida.
 - Se você quiser fornecer sua própria AWS KMS chave, escolha Inserir um ARN de chave, forneça o Amazon Resource Name (ARN) na caixa ARN da chave e escolha Use this KMS key. O ARN da chave será adicionado à lista.
2. Na seção Escolher tipo de acesso ao serviço, siga um destes procedimentos:
 - O console Choose Snow criará e usará uma função vinculada ao serviço para acessar AWS recursos em seu nome. para conceder permissões à AWS Snow Family para usar o Amazon S3 e o Amazon Simple Notification Service (Amazon SNS) em seu nome. A função AWS concede AssumeRole confiança ao Security Token Service (AWS STS) ao serviço Snow
 - Escolha Adicionar um perfil de serviço existente para usar, para especificar o ARN do perfil que você deseja, ou você pode usar o perfil padrão.
 3. Selecione Next (Próximo).

Escolha suas preferências de envio

Receber e devolver um dispositivo da Família Snow envolve enviar e receber o dispositivo, por isso é importante que você forneça informações de envio precisas.

Para fornecer detalhes de envio

1. Na seção Endereço de entrega, escolha um endereço existente ou adicione um novo endereço.
 - Se você escolher Usar endereço recente, os endereços no arquivo serão exibidos. Escolha com cuidado o endereço desejado na lista.
 - Se você escolher Adicionar um novo endereço, forneça as informações de endereço solicitadas. O Console de Gerenciamento da família AWS Snow salva suas novas informações de envio.

Note

O país que você fornece no endereço deve corresponder ao país de destino do dispositivo e deve ser válido para esse país.

2. Na seção **Prazo de envio**, escolha um prazo de entrega para o trabalho. Essa velocidade mostra a rapidez com que o dispositivo é enviado entre destinos e não reflete em quanto tempo ele chegará após a data de hoje. As velocidades de envio que você pode escolher são:
- Envio em um dia (1 dia útil)
 - Envio em dois dias (2 dias úteis)
 - Consulte [Transportadoras](#).

Escolher suas preferências de notificação

As notificações atualizam você sobre o status mais recente de seus trabalhos em dispositivos AWS Snow Family. Você cria um tópico do SNS e recebe e-mails do Amazon Simple Notification Service (Amazon SNS) à medida que o status do trabalho é alterado.

Para configurar notificações

- Na seção **Notificações**, faça o seguinte:
 - Se você quiser usar um tópico existente do SNS, escolha **Usar um tópico do SNS existente** e escolha o tópico nome do recurso da Amazon (ARN) na lista.
 - Se você quiser criar um novo tópico do SNS, escolha **Criar um novo tópico do SNS**. Insira um nome para o tópico e um endereço de e-mail.

Note

As tarefas para encomendar dispositivos Snow criados nas regiões Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon) são encaminhadas pela região Leste dos EUA (Norte da Virgínia). Por esse motivo, chamadas de serviço como o Amazon SNS também são direcionadas pelo Leste dos EUA (Norte da Virgínia). Recomendamos criar novos tópicos de SNS na região Leste dos EUA (Norte da Virgínia) para obter a melhor experiência.

As notificações serão sobre um dos seguintes estados do seu trabalho:

- Trabalho criado
- Preparação do dispositivo
- Preparação de entrega

- Em trânsito
- Entregue
- Em trânsito para AWS
- No departamento de triagem
- Em AWS
- Importação
- Concluído
- Cancelado

Para obter mais informações sobre notificações de alteração de status de trabalho e tópicos de SNS criptografados, consulte [Notificações para dispositivos da família Snow](#) neste guia.

Selecione o Próximo.

Etapa 5: revise o resumo do trabalho e crie seu trabalho

Depois de fornecer todas as informações necessárias para seu trabalho com dispositivos AWS Snow Family, revise o trabalho e crie-o. Depois de criar o trabalho, AWS começará a preparar o dispositivo Snow Family para envio para você.

Os trabalhos estão sujeitos às leis de controle de exportação em países específicos e podem exigir uma licença de exportação. As leis de exportação e reexportação dos EUA também se aplicam. O desvio das leis e regulamentos do país e dos EUA é proibido.

1. Na página de resumo do trabalho, revise todas as seções antes de criar o trabalho. Se você quiser fazer alterações, escolha Editar para a seção apropriada e edite as informações.
2. Ao terminar de revisar, selecione Criar tarefa.

Note

Depois de criar um trabalho para solicitar um dispositivo Snow Family, você pode cancelá-lo enquanto ele estiver no estado Job created sem incorrer em nenhuma cobrança. Para obter mais informações, consulte [Cancelamento de um trabalho por meio do Console de Gerenciamento da família AWS Snow](#).

Note

Os dispositivos Snowcone não são fornecidos com cabos de alimentação e um deve ser fornecido separadamente. Para obter mais informações, consulte [Fonte AWS Snowcone de alimentação e acessórios](#).

Depois que seu trabalho for criado, você poderá ver o status do trabalho na seção Status do trabalho. Para obter informações detalhadas sobre os status do trabalho, consulte [Status do trabalho](#).

Baixar AWS OpsHub

Os dispositivos da família AWS Snow oferecem uma ferramenta fácil de usar AWS OpsHub for Snow Family, que você pode usar para gerenciar seus dispositivos e dispositivos locais Serviços da AWS.

Com a AWS OpsHub instalação em seu computador cliente, você pode realizar tarefas como as seguintes:

- Desbloqueio e configuração de dispositivos únicos ou em cluster
- Transferir arquivos
- Lançamento e gerenciamento de instâncias em execução em dispositivos da Família Snow.

Para ter mais informações, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

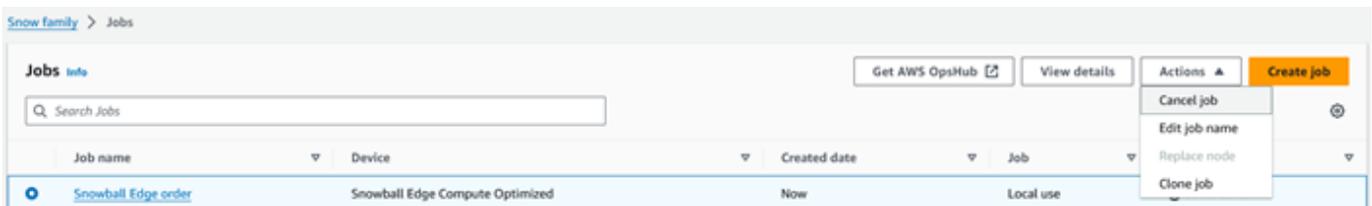
Para baixar e instalar AWS OpsHub for Snow Family

1. Nos [AWS Snowball recursos](#), clique em AWS OpsHub. Na AWS OpsHub seção com os links de download, escolha o link de download apropriado AWS OpsHub para instalar em seu sistema operacional.
2. Na seção AWS OpsHub, escolha Baixar para seu sistema operacional e siga as etapas de instalação. Quando terminar, escolha Próximo.

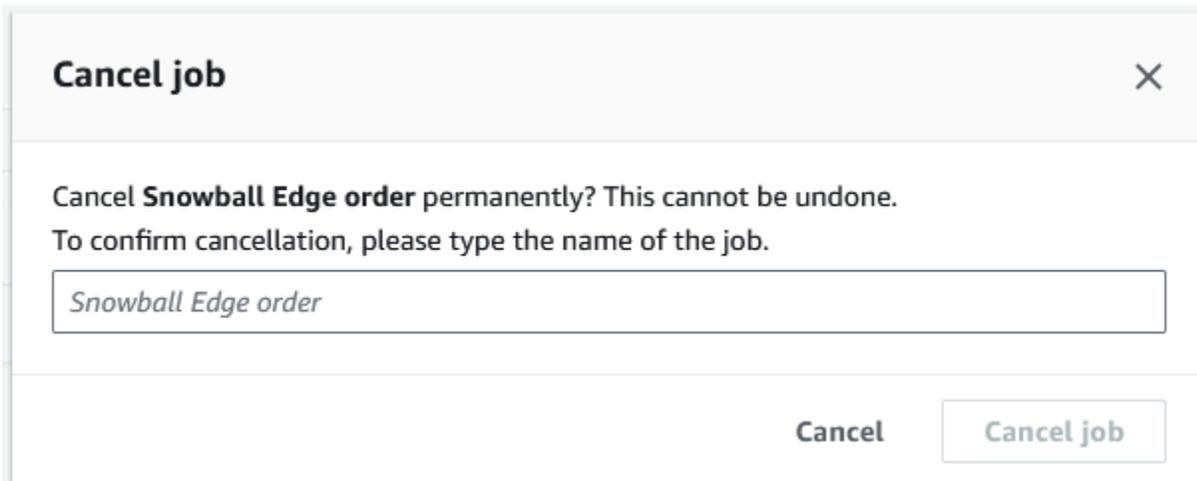
Cancelando um trabalho por meio do Console de Gerenciamento da família AWS Snow

Depois de criar um trabalho para solicitar um dispositivo Snow Family, você pode cancelar o trabalho por meio do Console de Gerenciamento da família AWS Snow. Se você cancelar o trabalho, não receberá o dispositivo que solicitou. Você só pode cancelar o trabalho enquanto o status do trabalho for Job created. Depois que o trabalho passar desse status, você não poderá cancelar o trabalho. Para obter mais informações, consulte [Job Statuses](#).

1. Faça login no [Console de Gerenciamento da família AWS Snow](#).
2. Escolha o trabalho a ser cancelado.
3. Escolha Ações. No menu exibido, escolha Cancelar trabalho.



4. A janela Cancelar trabalho é exibida. Para confirmar o cancelamento do trabalho, insira **job name** e escolha Cancelar trabalho. Na lista de trabalhos, Cancelado aparece na coluna Status.



Obter credenciais para acessar um dispositivo Snow Family

Cada trabalho tem um conjunto de credenciais que você deve obter da API de gerenciamento de tarefas Console de Gerenciamento da família AWS Snow ou da API de gerenciamento de tarefas para autenticar seu acesso ao dispositivo Snow Family. Essas credenciais são um arquivo

de manifesto criptografado e um código de desbloqueio associado. O arquivo manifesto contém informações importantes sobre o trabalho e as permissões associadas a ele.

 Note

Você vai receber as credenciais quando o dispositivo estiver a caminho. É possível ver o status do trabalho no Console de Gerenciamento da família AWS Snow. Para ter mais informações, consulte [Entendendo os status AWS Snowcone de Job](#).

Como obter credenciais usando o console

1. Faça login no AWS Management Console e abra [Console de Gerenciamento da família AWS Snowo](#).
2. No console, pesquise na tabela o trabalho específico cujo manifesto deseja baixar e, depois, selecione esse trabalho.
3. Expanda o painel Status do trabalho e escolha Exibir detalhes do trabalho.
4. No painel de detalhes que aparecer, expanda Credenciais e, em seguida, faça o seguinte:
 - Anote o código de desbloqueio (incluindo os hífen), pois você precisa fornecer todos os 29 caracteres para desbloquear o dispositivo.
 - Na caixa de diálogo, selecione Fazer download do manifesto e siga as instruções para baixar o arquivo manifesto do trabalho no computador. O nome do arquivo manifesto inclui a ID do trabalho.

 Note

Recomendamos que você não salve uma cópia do código de desbloqueio no mesmo local no computador do manifesto desse trabalho. Para ter mais informações, consulte [Melhores práticas para o AWS Snowcone dispositivo](#).

Agora que você tem suas credenciais, a próxima etapa é baixar o cliente Snowball Edge, que é usado para desbloquear AWS Snowball Edge o dispositivo.

Próximo: [Usando o AWS Snowball Edge cliente](#)

Desbloqueando o dispositivo Snow Family

Esta seção descreve o desbloqueio do dispositivo Snow Family usando a CLI do Snowball Edge. Para desbloquear o dispositivo usando AWS OpsHub uma ferramenta de interface gráfica de usuário (GUI) para dispositivos da família Snow, consulte [Desbloquear](#) um dispositivo.

Antes de usar um dispositivo da família Snow para transferir dados ou realizar tarefas de computação periférica, você precisa desbloquear o dispositivo. Ao desbloquear o dispositivo, você autentica sua capacidade de acessá-lo fornecendo duas formas de credenciais: um código de desbloqueio de 29 dígitos e um arquivo de manifesto. Depois de desbloquear o dispositivo, você pode configurá-lo ainda mais, mover dados de ou para ele, configurar e usar instâncias compatíveis com o Amazon EC2 e muito mais.

Antes de desbloquear um dispositivo, ele deve estar conectado à alimentação e à rede, ligado e ter um endereço IP atribuído. Consulte as [AWS especificações do dispositivo Snowcone](#). Você precisará das seguintes informações sobre o dispositivo Snow Family:

- Faça o download e instale o Snowball Edge Client. Para ter mais informações, consulte [Usando o AWS Snowball Edge cliente](#).
- Obtenha as credenciais do Console de Gerenciamento da família AWS Snow. Para um ou mais dispositivos autônomos, os códigos de desbloqueio e o arquivo de manifesto de cada dispositivo da família Snow. Para obter mais informações sobre como baixar credenciais, consulte [Obter credenciais para acessar um dispositivo Snow Family](#).
- Ligue cada dispositivo e conecte-o à sua rede. Para ter mais informações, consulte [AWS Snowcone Especificações do dispositivo](#).

Para desbloquear um dispositivo independente com o cliente Snowball Edge

1. Encontre o endereço IP do Snowcone na tela LCD do dispositivo. Anote esse endereço IP.
2. Use o `unlock-device` comando para autenticar seu acesso ao dispositivo Snow Family com o endereço IP do dispositivo Snow Family e suas credenciais, da seguinte forma.

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

O dispositivo indica que foi desbloqueado com sucesso com a seguinte mensagem.

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.

Se o comando retornar `connection refused`, consulte [Solução de problemas para desbloquear um dispositivo da família Snow](#).

Exemplo de **unlock-device** comando

Neste exemplo, o endereço IP do dispositivo é `192.0.2.0`, o nome do arquivo manifesto é `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` e o código de desbloqueio de 29 caracteres é `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
```

Solução de problemas para desbloquear um dispositivo da família Snow

Se o `unlock-device` comando retornar `connection refused`, você pode ter digitado incorretamente a sintaxe do comando ou a configuração do seu computador ou rede pode estar impedindo que o comando chegue ao dispositivo Snow. Execute as seguintes ações para resolver a situação:

1. Verifique se o comando foi digitado corretamente.
 - a. Use a tela LCD do dispositivo para verificar se o endereço IP usado no comando está correto.
 - b. Verifique se o caminho para o arquivo de manifesto usado no comando está correto, incluindo o nome do arquivo.
 - c. Use o [Console de Gerenciamento da família AWS Snow](#) para verificar se o código de desbloqueio usado no comando está correto.
2. Verifique se o computador que você está usando está na mesma rede e sub-rede do dispositivo Snow.

3. Verifique se o computador que você está usando e a rede estão configurados para permitir o acesso ao dispositivo Snow. Use o ping comando do seu sistema operacional para determinar se o computador pode acessar o dispositivo Snow pela rede. Verifique as configurações do software antivírus, da configuração do firewall, da rede privada virtual (VPN) ou de outras configurações do seu computador e da rede.

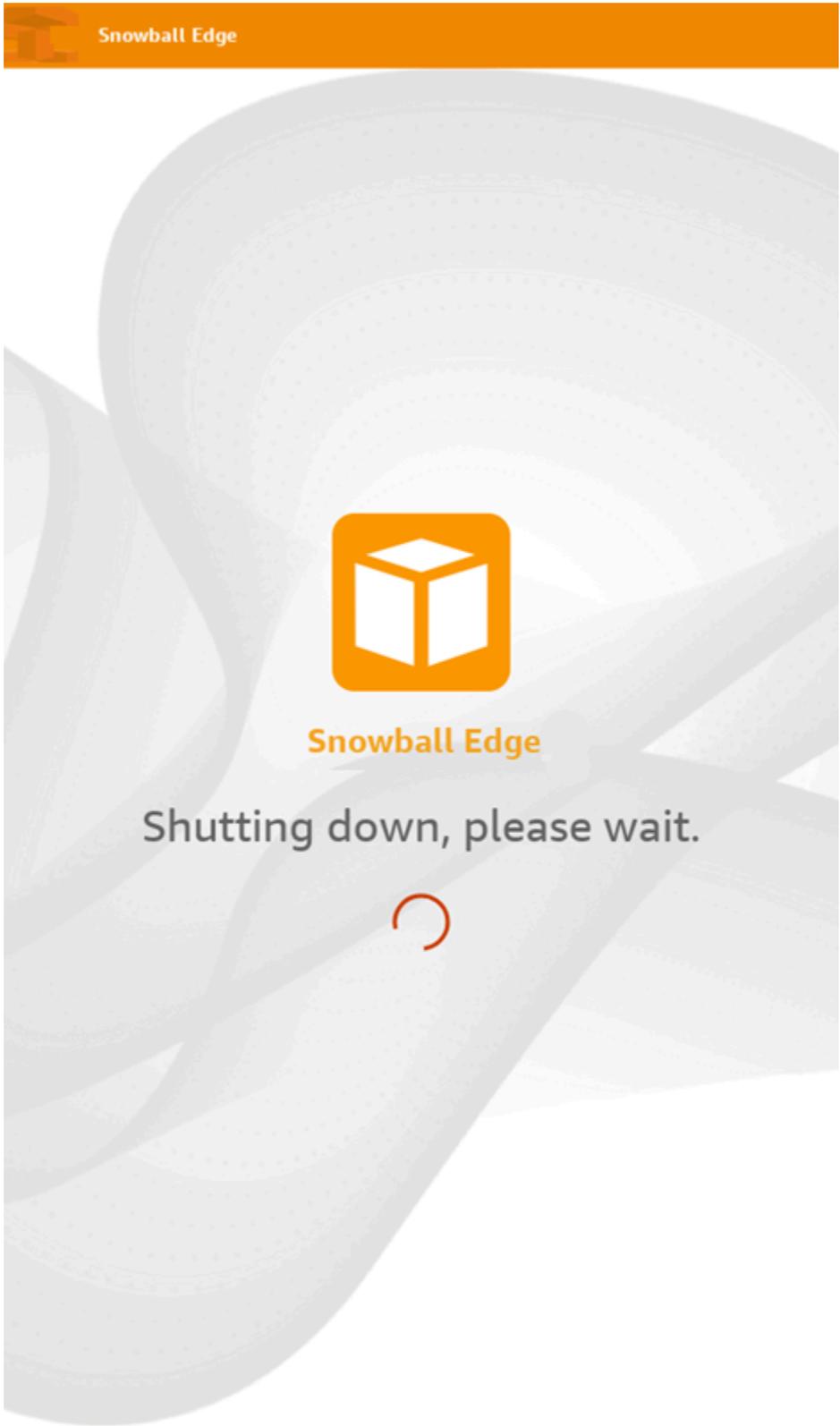
Agora você pode começar a usar o dispositivo Snow Family.

Reinicializando o dispositivo da Família Snow

Antes de reinicializar o dispositivo da Família Snow, verifique se todas as transferências de dados para o dispositivo foram interrompidas. Se você estava usando a interface NFS para transferir dados, desative-a antes de desligar o dispositivo. Para ter mais informações, consulte [Interrompendo a interface NFS](#).

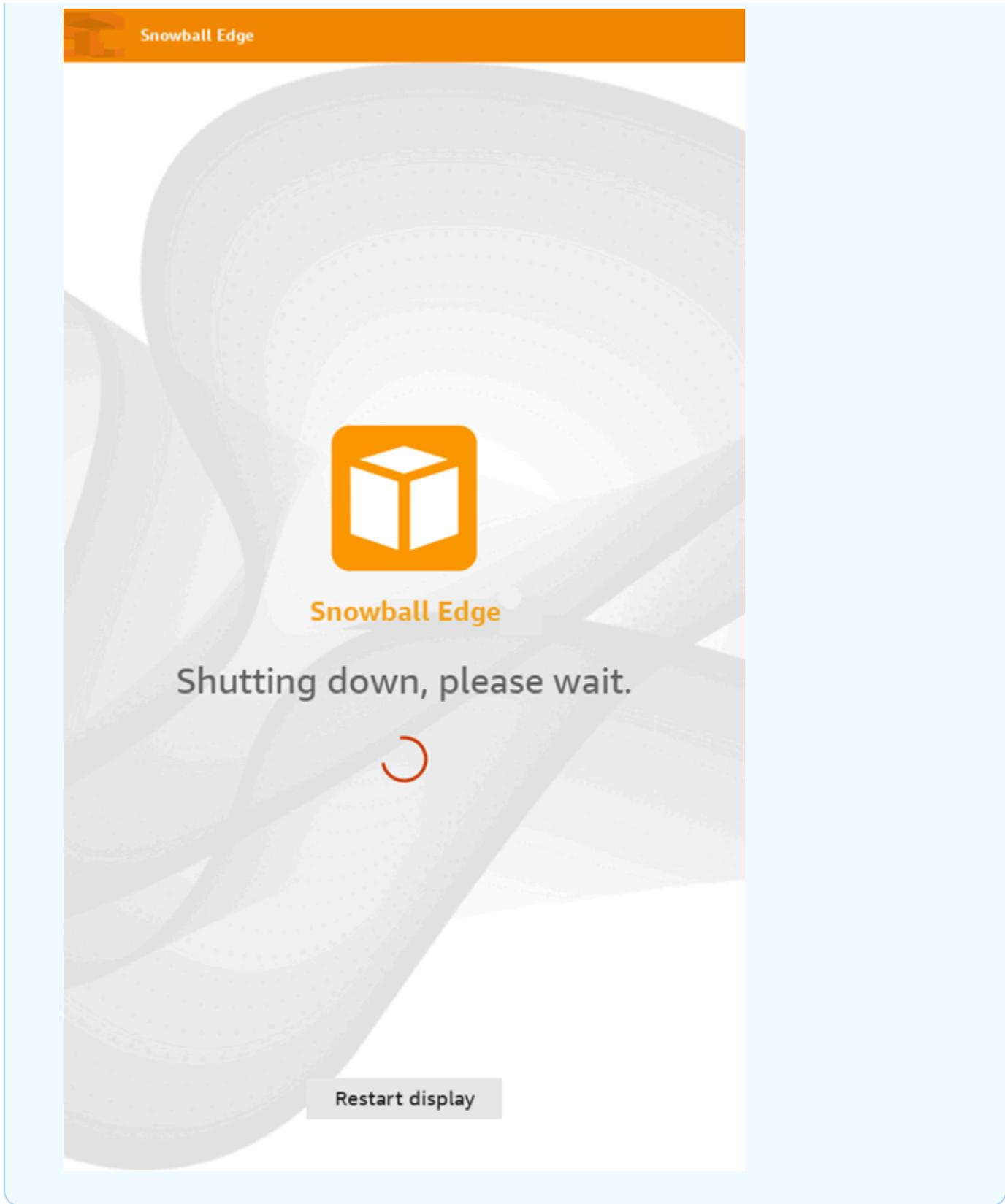
Para reinicializar o dispositivo usando o botão liga/desliga:

1. Quando todas as comunicações com o dispositivo terminarem, desligue-o pressionando o botão de ligar/desligar na frente do dispositivo. O dispositivo leva cerca de 20 segundos para desligar. Enquanto o dispositivo está sendo desligado, a tela LCD exibe uma mensagem indicando que o dispositivo está sendo desligado.



 **Note**

Se a tela LCD estiver exibindo a mensagem de desligamento quando o dispositivo não estiver realmente sendo desligado, pressione o botão Reiniciar exibição na tela para retornar a tela à operação normal.



2. Pressione o botão liga/desliga. Quando o dispositivo estiver pronto, a tela de LCD mostra um breve vídeo enquanto o dispositivo se prepara para começar. Após aproximadamente dez minutos, o dispositivo está pronto para ser desbloqueado.
3. Desbloqueie o dispositivo. Consulte [Desbloqueando um dispositivo AWS Snowcone](#).

Para reinicializar o dispositivo usando o Snowball Edge Client:

1. Quando toda a comunicação com o dispositivo terminar, use o comando `reboot-device` para reiniciá-lo. Quando o dispositivo estiver pronto, a tela de LCD mostra um breve vídeo enquanto o dispositivo se prepara para começar. Após aproximadamente dez minutos, o dispositivo está pronto para ser desbloqueado.

```
snowballEdge reboot-device
```

2. Desbloqueie o dispositivo. Consulte [Desbloqueando um dispositivo AWS Snowcone](#).

Usando AWS OpsHub for Snow Family para gerenciar dispositivos

Os dispositivos da família Snow agora oferecem uma ferramenta fácil de usar AWS OpsHub for Snow Family, que você pode usar para gerenciar seus dispositivos e AWS serviços locais. Você usa AWS OpsHub em um computador cliente para realizar tarefas como desbloquear e configurar dispositivos únicos ou em cluster, transferir arquivos e iniciar e gerenciar instâncias executadas em dispositivos da família Snow. Você pode usar AWS OpsHub para gerenciar os tipos de dispositivos Storage Optimized e Compute Optimized Snow. O AWS OpsHub aplicativo está disponível sem custo adicional para você.

AWS OpsHub pega todas as operações existentes disponíveis na API Snowball e as apresenta como uma interface gráfica de usuário. Essa interface ajuda você a migrar dados rapidamente para a Nuvem AWS e a implantar aplicativos de computação de ponta em dispositivos da família Snow.

AWS OpsHub fornece uma visão unificada dos AWS serviços que estão sendo executados nos dispositivos da família Snow e automatiza as tarefas operacionais por meio AWS Systems Manager de. Com AWS OpsHub isso, usuários com diferentes níveis de conhecimento técnico podem gerenciar um grande número de dispositivos da família Snow. Com apenas alguns cliques, você pode desbloquear dispositivos, transferir arquivos, gerenciar instâncias compatíveis com o Amazon EC2 e monitorar métricas de dispositivos.

Quando o dispositivo Snow chega ao seu site, você baixa, instala e executa o aplicativo AWS OpsHub em uma máquina cliente, como um laptop. Após a instalação, você pode desbloquear o dispositivo e começar a gerenciá-lo e usar AWS os serviços suportados localmente. AWS OpsHub fornece um painel que resume as principais métricas, como capacidade de armazenamento e instâncias ativas em seu dispositivo. Ele também fornece uma seleção dos serviços da AWS com suporte nos dispositivos da Família Snow. Em poucos minutos, você pode começar a transferir arquivos para o dispositivo.

Depois de [baixar o AWS OpsHub aplicativo](#) e instalá-lo em uma máquina cliente, AWS OpsHub pode se conectar ao AWS Snowcone dispositivo na mesma rede, independentemente de o dispositivo estar conectado via Wi-Fi ou por um cabo físico. Em seguida, você abre AWS OpsHub e desbloqueia o dispositivo. Você verá um painel que mostra o dispositivo e suas métricas do sistema. Em seguida, você pode começar a implantar seus aplicativos de ponta ou migrar seus dados para o dispositivo. AWS OpsHub simplifica as transferências de dados para seu dispositivo Snowcone, permitindo que

you insert drag-and-drop files or folders on the device. With AWS OpsHub, you can also easily see what is stored on the device.

Tópicos

- [Baixe AWS OpsHub para dispositivos da família Snow](#)
- [Desbloquear um dispositivo](#)
- [Verificando a assinatura PGP de AWS OpsHub \(opcional\)](#)
- [Gerenciando AWS serviços em seu dispositivo](#)
- [Usando DataSync para transferir arquivos para AWS](#)
- [Gerenciar seus dispositivos](#)
- [Configurando os servidores de horário NTP para o seu dispositivo](#)

Baixe AWS OpsHub para dispositivos da família Snow

Para baixar AWS OpsHub

1. Navegue até o [Site de atributos do AWS Snowball](#).

OpsHub

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

- [OpsHub documentation](#)

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

2. Na AWS OpsHub seção, escolha Baixar para seu sistema operacional e siga as etapas de instalação.

Desbloquear um dispositivo

Quando o dispositivo chega ao seu site, a primeira etapa é conectá-lo e desbloqueá-lo. O AWS OpsHub permite que você faça login, desbloqueie e gerencie dispositivos usando os seguintes métodos:

- **Localmente:** para entrar em um dispositivo localmente, você deve ligar o dispositivo e conectá-lo à sua rede local. Em seguida, forneça um código de desbloqueio e um arquivo de manifesto.
- **Remotamente:** para entrar em um dispositivo remotamente, você deve ligar o dispositivo e garantir que ele possa se conectar a *device-order-region*.amazonaws.com por meio da sua rede. Em seguida, forneça as credenciais AWS Identity and Access Management (IAM) (chave de acesso e chave secreta) do Conta da AWS que está vinculado ao seu dispositivo.

Para obter informações sobre como habilitar o gerenciamento remoto e criar uma conta associada, consulte [Ativando o gerenciamento de dispositivos Snow](#).

Tópicos

- [Desbloquear um dispositivo localmente](#)
- [Desbloquear um dispositivo remotamente](#)

Desbloquear um dispositivo localmente

Como conectar e desbloquear o dispositivo

1. Abra a aba do dispositivo, localize o cabo de alimentação e conecte o dispositivo a uma fonte de alimentação.
2. Conecte o dispositivo à sua rede usando um cabo de rede (normalmente um cabo Ethernet RJ45), depois abra o painel frontal e ligue o dispositivo.
3. Abra o AWS OpsHub aplicativo. Se você for um usuário iniciante, será solicitado a escolher um idioma e selecionar Próximo. Em seguida, escolha Próximo.
4. Na OpsHub página Começar com, escolha Entrar em dispositivos locais e, em seguida, escolha Entrar.



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. Na página Entrar em dispositivos locais, escolha o tipo de dispositivo da Família Snow e, em seguida, escolha Entrar.
6. Na página de login, insira o endereço IP do dispositivo e o código de desbloqueio. Para selecionar o manifesto do dispositivo, vá em Escolher arquivo e, em seguida, clique em Entrar.



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. Opcionalmente, você pode salvar as credenciais do dispositivo como um perfil. Nomeie o perfil e escolha Salvar nome do perfil. Para obter mais informações sobre perfis, consulte [Como gerenciar perfis](#).
8. Na guia Dispositivos locais, escolha um dispositivo para ver seus detalhes, como as interfaces de rede e AWS os serviços que estão sendo executados no dispositivo. Você também pode ver detalhes dos clusters nessa guia ou gerenciar seus dispositivos da mesma forma que faz com o AWS Command Line Interface (AWS CLI). Para ter mais informações, consulte [Gerenciando AWS serviços em seu dispositivo](#).

Note

O espaço de armazenamento disponível no dispositivo Snowcone não é preciso até que o serviço NFS seja iniciado. Consulte [Gerenciando a interface NFS](#).

Para dispositivos que foram AWS Snow Device Management instalados, você pode escolher Ativar gerenciamento remoto para ativar o recurso. Para ter mais informações, consulte [Usando AWS Snow Device Management para gerenciar dispositivos](#).

Desbloquear um dispositivo remotamente

Para desbloquear um dispositivo Snow Family, não

Como conectar e desbloquear o dispositivo remotamente

1. Abra a aba do dispositivo, localize o cabo de alimentação e conecte o dispositivo a uma fonte de alimentação.
2. Conecte o dispositivo à rede usando um cabo Ethernet (normalmente um cabo RJ45), abra o painel frontal e ligue o dispositivo.

Note

Para ser desbloqueado remotamente, seu dispositivo deve poder se conectar a *device-order-region*.amazonaws.com.

3. Abra o AWS OpsHub aplicativo. Se você for um usuário iniciante, será solicitado a escolher um idioma e selecionar Próximo. Em seguida, escolha Próximo.
4. Na OpsHub página Começar com, escolha Entrar em dispositivos remotos e, em seguida, escolha Entrar.



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. Na página Entrar em dispositivos remotos, insira as credenciais AWS Identity and Access Management (IAM) (chave de acesso e chave secreta) do Conta da AWS que está vinculado ao seu dispositivo e escolha Entrar.



Sign into remote devices

Sign in with an access key and secret key

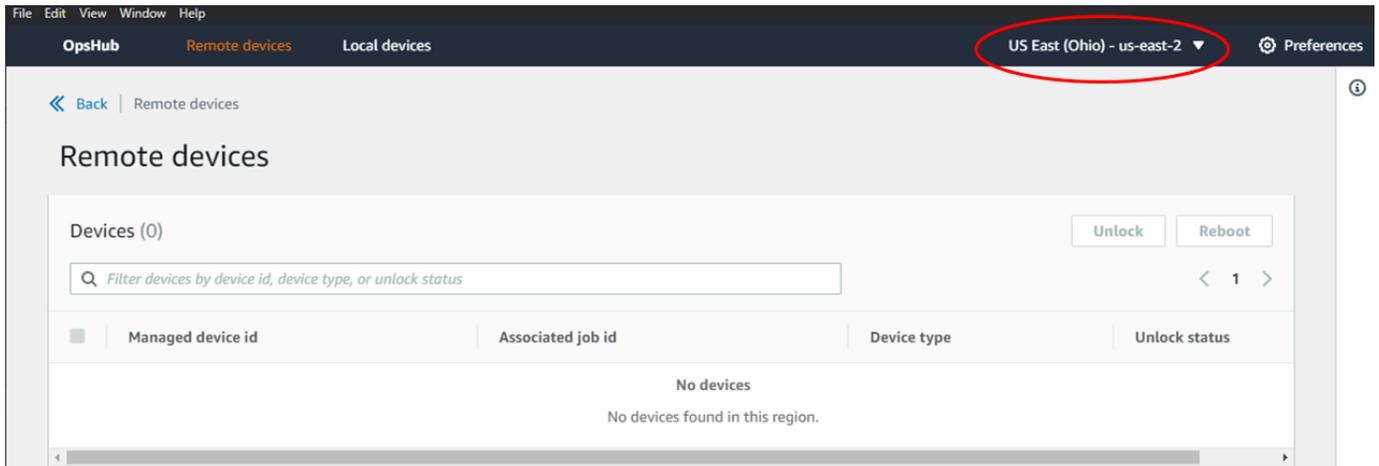
Access key

Secret key

Back

Sign in

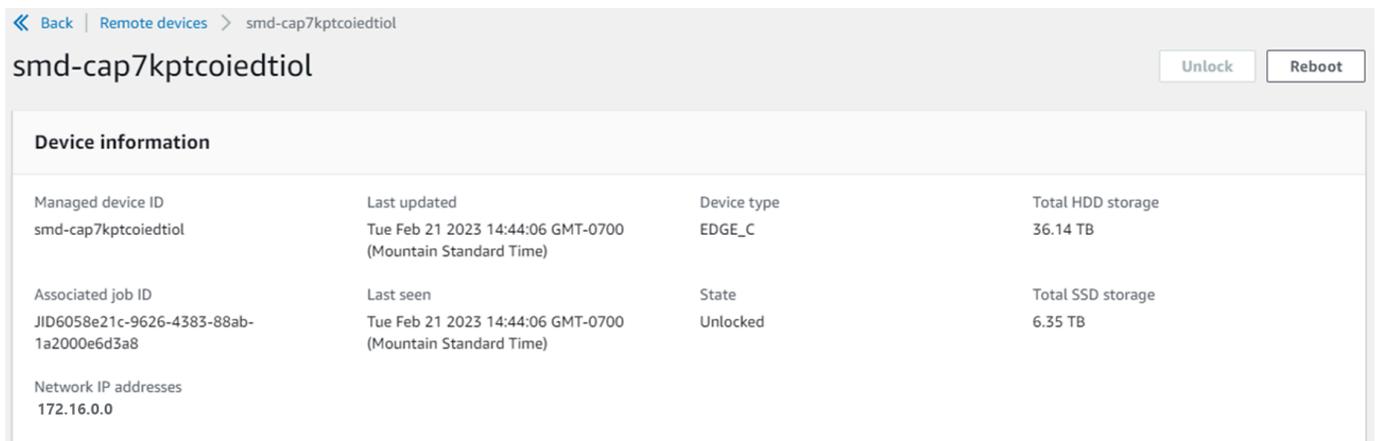
6. Na parte superior da guia Dispositivos remotos, escolha a região do dispositivo Snow para desbloquear remotamente.



7. Na guia Dispositivos remotos, escolha seu dispositivo para ver seus detalhes, como o estado e as interfaces de rede. Em seguida, escolha Desbloquear para desbloquear o dispositivo.

Note

O espaço de armazenamento disponível no dispositivo Snowcone não é preciso até que o serviço NFS seja iniciado. Consulte [Gerenciando a interface NFS](#).



Na página de detalhes do dispositivo remoto, você também pode reinicializar seus dispositivos e gerenciá-los da mesma forma que faz com o AWS Command Line Interface (AWS CLI). Para visualizar dispositivos remotos de forma diferente Regiões da AWS, escolha a região atual na barra de navegação e, em seguida, escolha a região que você deseja visualizar. Para ter mais informações, consulte [Gerenciando AWS serviços em seu dispositivo](#).

Verificando a assinatura PGP de AWS OpsHub (opcional)

O pacote do instalador do AWS OpsHub aplicativo para o sistema operacional Linux é assinado criptograficamente. Use a chave pública para verificar se o arquivo de download do atendente é original e não modificado. Se houver qualquer dano ou alteração nos arquivos, a verificação falhará. Você pode verificar a assinatura do pacote instalador usando GPG. Essa verificação é opcional. Se você optar por verificar a assinatura do aplicativo, você poderá fazer isso a qualquer momento.

Você pode baixar o arquivo SIGNATURE para o instalador do sistema operacional Linux em [AWS Snowcone Resources](#) ou [Snowball Edge Resources](#).

Para verificar o pacote de AWS OpsHub instalação no sistema operacional Linux

1. Copie a chave pública a seguir, salve-a em um arquivo e nomeie o arquivo. Por exemplo, `opshub-public-key.pgp`.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBF/hGf8BEAC9HCDV8uLjDX02Jxspi6kmPu4xqf4ZZLQsSqJcHU61oL/c
/zAN+mUqJT9aJ1rr0QFGVD1bMogecUPf1TW1DkEEpG8ZbX5P8vR+EE10/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmI07j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZXCi/+u+99YLaugJIP6ZYIEdfpxnghqyVtaappBFTAyfg67Y
N/5mea1VqJzd8liFpIFQnl+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvftb47bbv9Z28V1284
4lw2w1B1007Fo02v/Y0ukrN3VHCpmJQS1IiqZbYRa0DVK6UR5QNvUlj5fwWs
4qW9UDPhT/HDuaMrMFCejEn/7wvRUrGVtzCT9F56A1/dwRSxBejQQEb1AC8j
uuyi7gJaPdyNntR0EFTD7i02L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTp0ry/
Wvw0iKZFbo4AkiI0aLyBCk9HBXhUKA9x06g0nhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90wLRBUAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZienrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQS4NAwARAQABzTlBV1MgT3BzSHVi
IGZvciBTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFAl/hGf8GCwkHCAMCBBUICgIEFgIBAAIZAQIbAwIeAQAh
CRAHgc9adPNF8RYhBDcvpelIaY930b0vqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIawOSXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmXWwBg
cxg1g0GXNXCM4lAd68CmbA0LoLTaWSQX30ZbswzhbtX2ADAlOpV8RLBik7fm
bS9FyuubDRhfYRQq0fpjUGXFiEgwg6aMFxsrGLlv4QD7t+6ftFie/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+FOVMmPeEN5JRazEeUr1
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDW0q/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty251o8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4ED119Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEza/2upDJ1m+40HK4p
8DrEzP/3jTahT8q5ofFWSRD17d31TSU+JBmPE3mz311FNXgi08w+taY320z
```

```
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
07vxM05xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFZvzT/tDi5FiEEi+09
V+UAYN9Gnw36EVm/NP+00LnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvg0tUBxqmC0jr+8AKH00tiBWSu0
lsS8JU5rindEsKUirKTwcG2wyZFoe1z1E8xPkLRSRN5ZbbgKsTz16l1HgCCId
Do+WJdDkWGwXmtDvzjm32EI/PVBd108ga9aPwXdhLw0dKAjZ4JrJXLUQJjRI
IVDSyM0bEH0UM6a/+mWNZazNfo0LsGwqGva6Xn5WJWlwR1S78vPNf03BQYu0
YRjaVQR+kPtB9aSAZNi5sWfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7X103o/Vjb1neZ0hJK6kAKU172tnPJTJ31Jb0xX73wsMWDYZRZVcK
9X9+GFrpwKHKKPjpm0t/FRxNepvqR172TkgBPqGH2TM0FdB1f/uQprivqge
PBbS0JrmBIH9/anIqgtMdtcNQB/0erLdCDqI5af0uD10LcLwdJwG9/bSrfwT
TVEE3WbXmJ8pZgMz1HUizE6V2DSadV/YItk50I0jJR0VH0Hv1FMwGCEAIFzf
9P/pNi8hpEm1RphRi0VVcdQ30bH0M0gPHU5V9f1IhyCL1zU3LjYTHkq0yJD5
YDA1x01MYq3DcSM5130VBbLmuVS2GpcsTCYqlQA6h/zzMwz+/70wU0EX+EZ
/wEQA0AY8ULmcJIQWIr14V0jy1pJeD3qw7wd+QsBzJ+mOp0B/3ZFAhQiN01
9yCDLHeiZeAmWYX90IXrNiIdcHy+WTAp4G+NaMpqE52qhbDjz+IbvLp11yDH
bYEHpjnTHXEy21bvKAJ0Kkw/2RcQ0i4dodGnq5icyYj+9gcuHvnVwbrQ96Ia
0D7c+b5T+bzFqk90nIcztrMRuhDLJnJpi70jpvQwfq/TkkZA+mzupxfSkq/Y
N9qXNEToT/VI2gn/LS0X4Ar112KxBjzNEsQkwGSiWSYtMA5J+Tj5ED0uZ/qe
omNblA1D4bm7Na8NAoLxctAiDq/f3To9Xb18lHsnd0mfLCb/BVgP4edQKTii
C/OZH9QJ1fmN0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXM0d3I
e6NUvU7pW0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQyZe0
jXD3IJ7T+X2XA8M/BmypwMw0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcpXzehwsSVq1lzaL2ureJBL0KkBgYxUJYXpbS01ax1TsFG
091dAN0s9Ej8CND37GsNnuygjOgWXB6MNgbvPs3H3zi/AbMunQ1VB1w07JX
zdM1hBQZ6w+NeiEsK1T6wHi7IhxABEBAAHcWXYEGAEIAAKFAL/hGf8CGwwA
IQkQIYHPWntzRfEWIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PVbF
ywKvwi3GL0lpY7BXn8lQaHyunMGUavm080faRR0ynkH0ZqLHCp6bIajF0fvF
b7c0Jamzx8Hg+SIId16yRpRY+fa4RQ6PNnmT93ZgWW3EbjPyJG1m0/rt03SR
+0yn4/ldlg2KfBX4ppMoPCMKUdWxGmDETxsGihwZ0gmCZqXe81K122PYkSN
JQQ+L1fjKvCaxfPKEjXYTbIbfyyhCR6NzA0VZxCrzSz2xDrYwP/V002K1xda
0ix6r2aEHf+xYEUh0aBt80HY5nXTuRReCVU789MUVtCMqD2u6amdo4BR0kWA
QNg4yavKwV+LVtyYh2Iju9VSyv4xL1Q4xKHvcAUrSH73bHG7b7jkUJckD0f4
twhjJk/Lfwe6RdnVo2WoeTvE93w+NAq2FXmvbiG7eltl0XfQecvQU3QNbRvH
U8B96W0w8UXJdvTKg4f0NbjSw7iJ3x5naixQ+rA8hLV8x0gn2LX6wvxT/SEu
mn20KX+fPtJELK7v/NheFLX1jsKLXYo4jHrkfIXNsNUhg/x2E71kAjbET3s+
t9kCtxt2iXDDZvpIbmG04QkvLFvoR0aSmN6+8fupe3e+e2yN0e6xGTuE60gX
I2+X1p1g9IduDYTpoI20XleHyyMqGeeIb4g0iisloTp5oi3EuAYRGflXuqAT
VA19bKnpkBsJ0A==
=tD2T
-----END PGP PUBLIC KEY BLOCK-----
```

2. Importe a chave pública em seu chaveiro e observe o valor de chave retornado.

GPG

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

Exemplo de saída

```
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. Verifique a impressão digital. Substitua *key-value* pelo valor da etapa anterior. Recomendamos que você use o GPG para verificar a impressão digital.

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

Esse comando retorna uma saída semelhante à seguinte:

```
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]
```

A impressão digital deve corresponder ao seguinte:

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

Se a impressão digital não corresponder, não instale o AWS OpsHub aplicativo. Entre em contato com a AWS Support.

4. Baixe o arquivo de assinatura de acordo com a arquitetura e o sistema operacional da instância, caso ainda não tenha feito isso.
5. Verifique a assinatura do pacote do instalador. Substitua *signature-filename* e *OpsHub-download-filename* pelos valores que você especificou ao baixar o arquivo SIGNATURE e o aplicativo AWS OpsHub .

GPG

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

Esse comando retorna uma saída semelhante à seguinte:

GPG

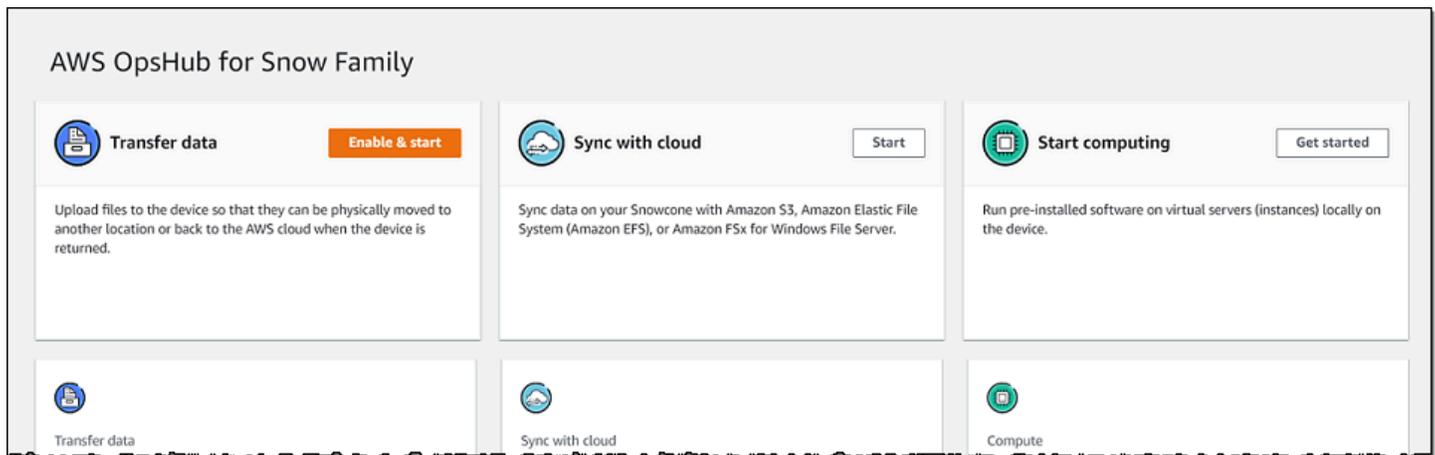
```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:          using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snow Family <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that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

Ao usar GPG, se a saída inclui a frase `BAD signature`, verifique se você executou o procedimento corretamente. Se você continuar recebendo essa resposta, entre em contato AWS Support e não instale o agente. A mensagem de aviso sobre a relação de confiança não significa que a assinatura não é válida, apenas que você não verificou a chave pública. Uma chave somente será confiável se você ou alguém em quem você confia a tiver assinado.

Gerenciando AWS serviços em seu dispositivo

Com AWS OpsHub, você pode usar e gerenciar AWS serviços em seus dispositivos Snow Family. Atualmente, AWS OpsHub oferece suporte aos seguintes recursos:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2): use instâncias compatíveis com o Amazon EC2 para executar software instalado em um servidor virtual sem enviá-lo para processamento para a Nuvem AWS .
- AWS DataSync—Transfira um grande número de arquivos entre seu armazenamento local e outros Nuvem AWS locais, como sistemas de arquivos ou Amazon S3.
- Network File System (NFS): use compartilhamentos de arquivos a fim de mover dados para o dispositivo. Você pode enviar o dispositivo AWS para transferir seus dados para o Nuvem AWS, ou usá-lo DataSync para transferir para outros Nuvem AWS locais.



Tópicos

- [Usando instâncias computacionais compatíveis com o Amazon EC2 localmente](#)
- [Gerenciando a interface NFS](#)

Usando instâncias computacionais compatíveis com o Amazon EC2 localmente

Você pode usar AWS OpsHub para executar software pré-instalado em servidores virtuais (instâncias) localmente em seu dispositivo e também para gerenciar instâncias do Amazon EC2 em seu dispositivo.

Tópicos

- [Executar uma instância compatível com o Amazon EC2](#)
- [Interrompendo uma instância compatível com o Amazon EC2](#)
- [Iniciando uma instância compatível com Amazon EC2](#)
- [Trabalhar com pares de chaves](#)
- [Encerramento de uma instância compatível com Amazon EC2](#)
- [Usar volumes de armazenamento localmente](#)

Executar uma instância compatível com o Amazon EC2

Siga estas etapas para iniciar uma instância compatível com o Amazon EC2 usando AWS OpsHub

Para executar uma instância compatível com o Amazon EC2

1. Abra o AWS OpsHub aplicativo.
2. Na seção Start computing (Iniciar computação) no painel, escolha Get started (Comece a usar). Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação). Todos os recursos de computação aparecem na seção Resources (Recursos).
3. Se você tiver instâncias compatíveis com o Amazon EC2 em execução no dispositivo, elas serão exibidas na coluna Nome da instância em Instâncias. Você pode ver os detalhes de cada instância nesta página.
4. Escolha Iniciar instância. O assistente de execução de instância é aberto.
5. Em Dispositivo, escolha o dispositivo Snow no qual você deseja executar a instância do EC2.

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. Para Imagem (AMI), escolha uma imagem de máquina da Amazon (AMI) na lista. Essa AMI é usada para executar sua instância.
7. Para Tipo de instância, escolha uma opção na lista.
8. Escolha como deseja anexar um endereço IP à instância. Você tem as seguintes opções:
 - Criar endereço IP público (VNI): escolha esta opção para criar um novo endereço IP usando uma interface de rede física. Escolha uma interface de rede física e a atribuição de endereço IP.
 - Usar endereço IP existente (VNI): escolha esta opção para usar um endereço IP existente e usar interfaces de rede virtual existentes. Escolha uma interface de rede física e uma interface de rede virtual.
 - Não anexar endereço IP: escolha esta opção se você não desejar anexar um endereço IP.
9. Escolha como deseja anexar um par de chaves à instância. Você tem as seguintes opções:

Criar par de chaves: escolha essa opção para criar um novo par de chaves e iniciar a nova instância com esse par de chaves.

Usar par de chaves existente: escolha essa opção para usar um par de chaves existente para executar a instância.

Não anexar endereço IP: escolha esta opção se você não desejar anexar um par de chaves. Você deve reconhecer que não conseguirá se conectar a essa instância a menos que já saiba a senha incorporada a essa AMI.

Para ter mais informações, consulte [Trabalhar com pares de chaves](#).
10. Escolha Executar. Você deverá ver sua instância sendo executada na seção Instâncias de computação. O Estado é Pendente e muda para Em execução ao término.

Interrompendo uma instância compatível com o Amazon EC2

Use as etapas a seguir AWS OpsHub para interromper uma instância compatível com o Amazon EC2.

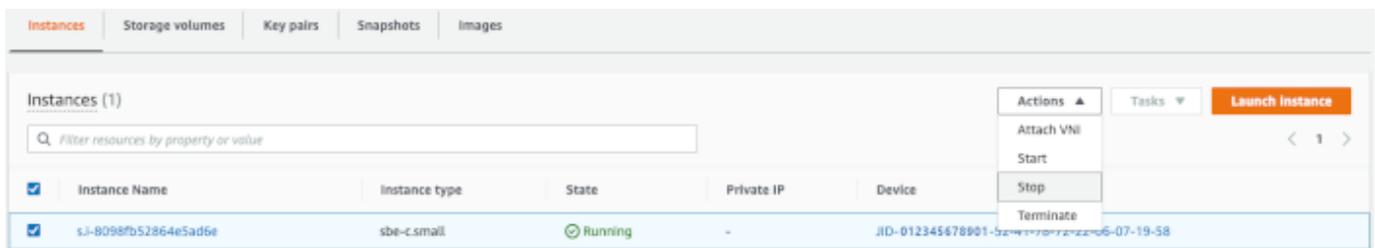
Para interromper uma instância compatível com o Amazon EC2

1. Abra o AWS OpsHub aplicativo.

2. Na seção Iniciar computação do painel, escolha Comece a usar. Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação).

Todos os recursos de computação aparecem na seção Resources (Recursos).

3. Se você tiver instâncias compatíveis com o Amazon EC2 em execução no dispositivo, elas serão exibidas na coluna Nome da instância em Instâncias.
4. Escolha a instância que você deseja interromper, escolha o menu Ações e escolha Parar. O Estado muda para Interrompendo e depois para Interrompida ao término.



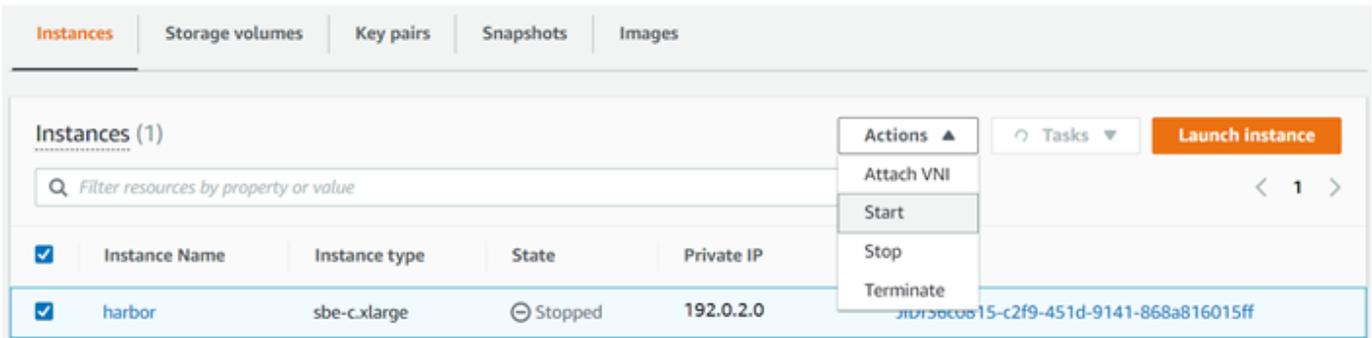
Iniciando uma instância compatível com Amazon EC2

Use essas etapas para iniciar uma instância compatível com o Amazon EC2 usando o AWS OpsHub

Para iniciar uma instância compatível com o Amazon EC2

1. Abra o AWS OpsHub aplicativo.
2. Na seção Iniciar computação do painel, escolha Comece a usar. Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação).

Seus recursos de computação aparecem na seção Resources (Recursos).
3. Na coluna Instance name (Nome da instância), em Instances (Instâncias), localize a instância que deseja iniciar.
4. Selecione a instância e escolha Start (Iniciar). O State (Estado) muda para Pending (Pendente) e depois para Running (Em execução) ao término.



Trabalhar com pares de chaves

Quando você executa uma instância compatível com o Amazon EC2 e pretende se conectar a ela usando SSH, você precisa fornecer um par de chaves. Você pode usar o Amazon EC2 para criar um novo par de chaves ou importar um par de chaves existente.

Para criar, importar ou gerenciar pares de chaves

1. Abra o Compute no AWS OpsHub painel.
2. No painel de navegação, escolha a página Computação (EC2) e, em seguida, escolha a guia Pares de chave. Você é redirecionado para o console do Amazon EC2, onde pode criar, importar ou gerenciar seus pares de chaves.
3. Para obter instruções sobre como criar e importar pares de chaves, consulte os pares de [chaves do Amazon EC2 e as instâncias Linux no Guia](#) do usuário do Amazon EC2.

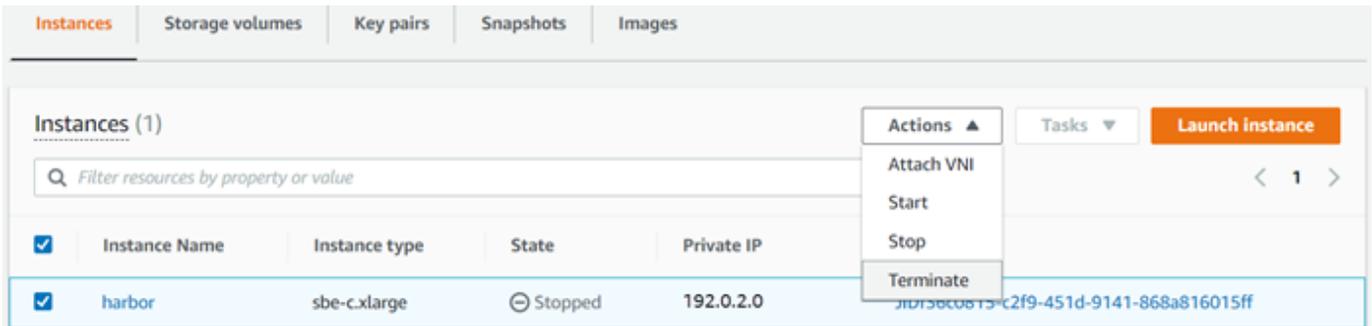
Encerramento de uma instância compatível com Amazon EC2

Depois de terminar uma instância compatível com o Amazon EC2, você não poderá reiniciar a instância.

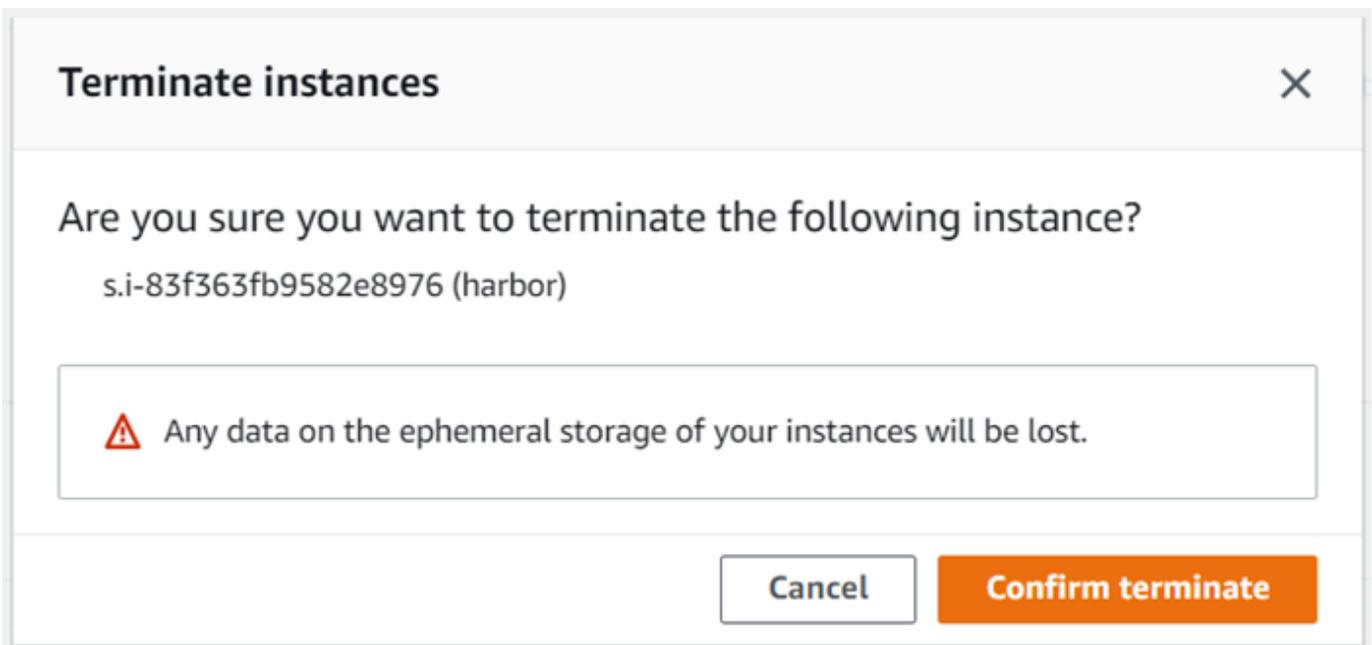
Para encerrar uma instância compatível com o Amazon EC2

1. Abra o AWS OpsHub aplicativo.
2. Na seção Start computing (Iniciar computação) no painel, escolha Get started (Comece a usar). Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação). Você pode ver todos os recursos de computação na seção Recursos.

- Na coluna Instance name (Nome da instância), em Instances (Instâncias), localize a instância que deseja encerrar.
- Escolha a instância e escolha o menu Ações. No menu Ações, escolha Encadear.



- Na janela Encerrar instâncias, escolha Confirmar encerramento.



Note

Depois que a instância for encerrada, você não poderá reiniciá-la.

O State (Estado) muda para Terminating (Encerrando) e depois para Terminated (Encerrada) ao término.

Usar volumes de armazenamento localmente

As instâncias compatíveis com o Amazon EC2 usam volumes do Amazon EBS para armazenamento. Neste procedimento, você cria um volume de armazenamento e o anexa à sua instância usando AWS OpsHub.

Como criar um volume de armazenamento

1. Abra o AWS OpsHub aplicativo.
2. Na seção Start computing (Iniciar computação) no painel, escolha Get started (Comece a usar). Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação).
3. Escolha a guia Volumes de armazenamento. Se você tiver volumes de armazenamento no seu dispositivo, os detalhes sobre os volumes serão exibidos em Volumes de armazenamento.
4. Escolha Create volume (Criar volume) para abrir a página Create volume (Criar 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

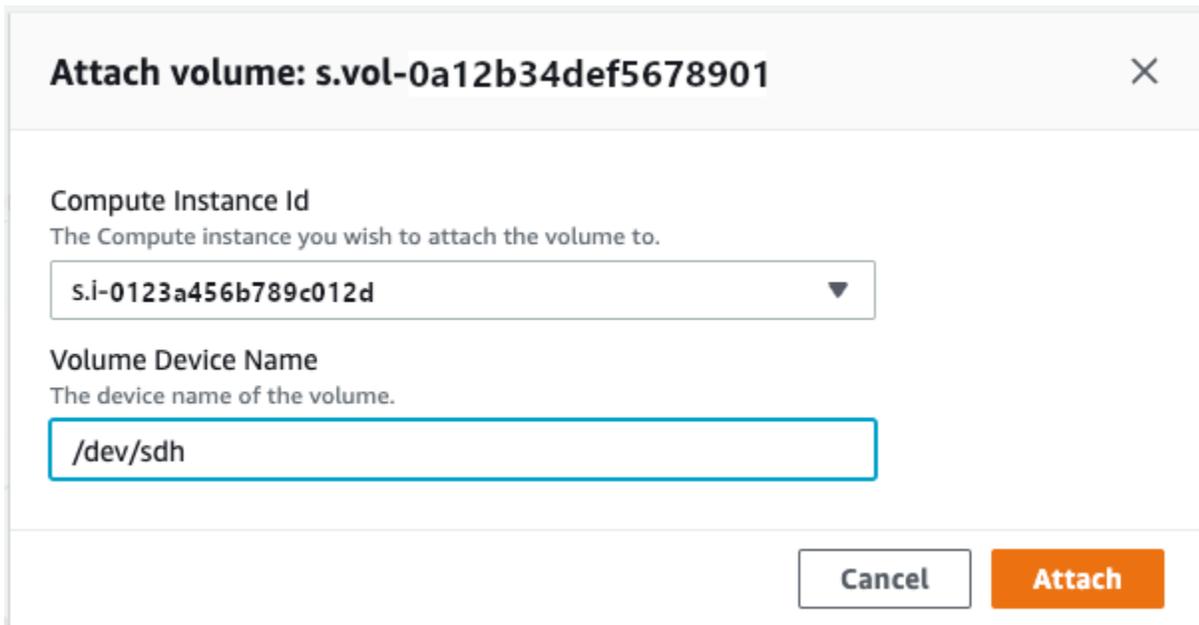
Volume Type
Select a performance type for your volume.
Capacity-optimized HDD volume (sbg1)

Cancel Submit

5. Escolha o dispositivo no qual você deseja criar o volume, insira o tamanho (em GiBs) que você deseja criar e escolha o tipo de volume.
6. Selecione Enviar. O State (Estado) é Creating (Criando) e muda para Available (Disponível) ao término. Você pode ver seu volume e os detalhes dele na guia Volumes.

Como anexar um volume de armazenamento à sua instância

1. Escolha o volume que você criou e escolha Attach volume (Anexar volume).



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

2. Em ID da instância de computação, selecione a instância à qual deseja anexar o volume.
3. Em Volume Device Name (Nome do dispositivo de volume), insira o nome do dispositivo do volume (por exemplo, **/dev/sdh** ou **xvdh**).
4. Escolha Anexar.

Se não precisar mais do volume, você poderá desanexá-lo da instância e excluí-lo.

Gerenciando a interface NFS

Use a interface Network File System (NFS) para fazer upload de arquivos para o dispositivo da família Snow como se o dispositivo fosse um armazenamento local em seu sistema operacional. Isso permite uma abordagem mais fácil de usar para transferir dados, pois você pode usar recursos do seu sistema operacional, como copiar arquivos, arrastá-los e soltá-los ou outros recursos da interface gráfica do usuário. Cada bucket S3 no dispositivo está disponível como um endpoint de interface NFS e pode ser montado para copiar dados. A interface NFS está disponível para trabalhos de importação.

Quando iniciada, a interface NFS usa 1 GB de memória e 1 CPU. Isso pode limitar o número de outros serviços em execução no dispositivo da família Snow ou o número de instâncias compatíveis com EC2 que podem ser executadas.

Os dados transferidos pela interface NFS não são criptografados em trânsito. Ao configurar a interface NFS, você pode fornecer blocos CIDR e o dispositivo da família Snow restringirá o acesso à interface NFS de computadores clientes com endereços nesses blocos.

Os arquivos no dispositivo serão transferidos para o Amazon S3 quando ele for devolvido. AWS Para obter mais informações, consulte [S3 Como funciona o AWS Snowcone](#).

Para obter mais informações sobre como usar o NFS com o sistema operacional do seu computador, consulte a documentação do sistema operacional.

Lembre-se dos seguintes detalhes ao usar a interface NFS.

- Os nomes dos arquivos são chaves de objeto em seu bucket do S3 local no dispositivo da Família Snow. O nome para uma chave é uma sequência de caracteres Unicode cuja codificação UTF-8 é de, no máximo, 1.024 bytes de comprimento. Recomendamos usar o NFSv4.1 sempre que possível e codificar os nomes dos arquivos com Unicode UTF-8 para garantir uma importação de dados bem-sucedida. Os nomes de arquivo que não estão codificados com UTF-8 podem não ser enviados para o S3 ou podem ser carregados para o S3 com um nome de arquivo diferente, dependendo da codificação NFS que você usa.
- Certifique-se de que o tamanho máximo do caminho do arquivo seja inferior a 1024 caracteres. Os dispositivos da Família Snow não oferecem suporte a caminhos de arquivo maiores que 1024 caracteres. Exceder esse tamanho de caminho de arquivo resultará em erros na importação do arquivo.
- Para obter mais informações, consulte [Chaves de objeto](#) no Guia do usuário do Amazon Simple Storage Service.
- Para transferências baseadas em NFS, metadados padrão no estilo POSIX serão adicionados aos seus objetos à medida que forem importados para o Amazon S3 a partir de dispositivos da família Snow. Além disso, você verá os metadados "x-amz-meta-user-agent aws-datasync" que usamos atualmente AWS DataSync como parte do mecanismo interno de importação para o Amazon S3 para importação de dispositivos da família Snow com a opção NFS.

 Note

Na página de detalhes do dispositivo em AWS OpsHub, o espaço de armazenamento disponível nos dispositivos Snowcone não é preciso até que a interface NFS seja iniciada.

Você também pode configurar e gerenciar a interface NFS com o cliente Snowball Edge, uma ferramenta de interface de linha de comando (CLI). Para obter mais informações, consulte [Gerenciando a interface NFS](#).

Tópicos

- [Iniciando o serviço NFS em um sistema operacional Windows](#)
- [Configurando a interface NFS automaticamente](#)
- [Configurando a interface NFS manualmente](#)
- [Gerenciando endpoints NFS no dispositivo da família Snow](#)
- [Montagem de endpoints NFS em computadores cliente](#)
- [Interrompendo a interface NFS](#)

Iniciando o serviço NFS em um sistema operacional Windows

Se o computador cliente estiver usando o sistema operacional Windows 10 Enterprise ou Windows 7 Enterprise, inicie o serviço NFS no computador cliente antes de configurar o NFS no aplicativo. AWS OpsHub

1. No computador cliente, abra Iniciar, escolha Painel de Controle e selecione Programas.
2. Escolha Ativar ou desativar recursos do Windows.

Note

Para ativar os recursos do Windows, talvez seja necessário fornecer um nome de usuário e uma senha de administrador para o seu computador.

3. Em Serviços para NFS, escolha Cliente para NFS e selecione OK.

Configurando a interface NFS automaticamente

A interface NFS não está sendo executada no dispositivo Snow Family por padrão, então você precisa iniciá-la para ativar a transferência de dados no dispositivo. Com alguns cliques, seu dispositivo Snow Family pode configurar rápida e automaticamente a interface NFS para você. Você também pode configurar a interface NFS sozinho. Para ter mais informações, consulte [Configurando a interface NFS manualmente](#).

1. Na seção Transferir dados do painel, selecione Habilitar e iniciar. Isso pode levar um minuto ou dois para ser concluído.



2. Quando o serviço NFS é iniciado, o endereço IP da interface NFS é mostrado no painel e a seção Transferir dados indica que o serviço está ativo.
3. Escolha Abrir no Explorer (se estiver usando um sistema operacional Windows ou Linux) para abrir o compartilhamento de arquivos no navegador de arquivos do seu sistema operacional e começar a transferir arquivos para o dispositivo da família Snow. Você pode copiar e colar ou arrastar e soltar arquivos do seu computador cliente no compartilhamento de arquivos. No sistema operacional Windows, seu compartilhamento de arquivos se parece com o seguinte: `\\12.123.45.679(Z:)`.

Note

Nos sistemas operacionais Linux, a montagem de endpoints NFS requer permissões de root.

Configurando a interface NFS manualmente

A interface NFS não está sendo executada no dispositivo Snow Family por padrão, então você precisa iniciá-la para ativar a transferência de dados no dispositivo. Você pode configurar manualmente a interface NFS fornecendo o endereço IP de uma Interface de Rede Virtual (VNI) em execução no dispositivo da família Snow e restringindo o acesso ao seu compartilhamento de arquivos, se necessário. Antes de configurar a interface NFS manualmente, configure uma interface de rede virtual (VNI) em seu dispositivo Snow Family. Para obter mais informações, consulte [Configuração de rede para instâncias de computação](#).

Você também pode fazer com que o dispositivo Snow Family configure a interface NFS automaticamente. Para ter mais informações, consulte [Configurando a interface NFS automaticamente](#).

1. Na parte inferior da seção Transferir dados do painel, selecione Configurar manualmente.

2. Selecione Habilitar e iniciar para abrir o assistente Iniciar o NFS. O campo Interface de rede física é preenchido.

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. Selecione Criar endereço IP (VNI) ou Usar endereço IP existente.

4. Se você escolher Criar endereço IP (VNI), escolha DHCP ou IP estático na caixa de listagem Atribuição de endereço IP.

 Important

Se você usa uma rede DHCP, é possível que o endereço IP da interface NFS possa ser reatribuído pelo servidor DHCP. Isso pode acontecer depois que o dispositivo for desconectado e os endereços IP forem reciclados. Se você definir um intervalo de hosts permitido e o endereço do cliente mudar, outro cliente poderá escolher esse endereço. Nesse caso, o novo cliente terá acesso ao compartilhamento. Para evitar isso, use reservas DHCP ou endereços IP estáticos.

Se você escolher Usar endereço IP existente, escolha uma interface de rede virtual na caixa de listagem Interface de rede virtual.

5. Escolha restringir o acesso à interface NFS e fornecer um bloco de endereços de rede permitidos ou permitir que qualquer dispositivo na rede acesse a interface NFS no dispositivo da família Snow.
 - Para restringir o acesso à interface NFS no dispositivo Snow Family, escolha Restringir NFS aos hosts permitidos. Em Hosts permitidos, insira um conjunto de blocos CIDR. Se você quiser permitir o acesso a mais de um bloco CIDR, insira outro conjunto de blocos. Para remover um conjunto de blocos, escolha X ao lado do campo que contém os blocos. Escolha Adicionar anfitriões permitidos.

 Note

Se você escolher Restringir NFS aos hosts permitidos e não fornecer blocos CIDR permitidos, o dispositivo da família Snow negará todas as solicitações para montar a interface NFS.

- Para permitir que qualquer dispositivo na rede acesse a interface NFS, escolha Permitir todos os hosts.
6. Para permitir que instâncias compatíveis com EC2 em execução no dispositivo da família Snow acessem o adaptador NFS, escolha Ativar.
 7. Escolha Iniciar NFS. Pode levar um minuto ou dois para começar.

⚠ Important

Não desligue o dispositivo Snow Family enquanto a interface NFS estiver iniciando.

Na seção Recursos do Sistema de Arquivos de Rede (NFS), o Estado da interface NFS é exibido como Ativo. Você precisará do endereço IP listado para montar a interface como armazenamento local nos computadores cliente.

Gerenciando endpoints NFS no dispositivo da família Snow

Cada bucket S3 no dispositivo da família Snow é representado como um endpoint e listado em Mount paths. Depois que a interface NFS for iniciada, monte um endpoint para transferir arquivos de ou para esse endpoint. Somente um endpoint pode ser montado por vez. Para montar um endpoint diferente, desmonte primeiro o endpoint atual.

Para montar um endpoint

1. Na seção Montar caminhos, siga um destes procedimentos para selecionar um endpoint:
 - No campo Filtrar endpoints, insira o nome total ou parcial de um bucket para filtrar a lista de endpoints disponíveis na sua entrada e escolha o endpoint.
 - Escolha o ponto final a ser montado na lista Caminhos de montagem.
2. Escolha Mount NFS endpoint. O dispositivo Snow Family monta o endpoint para uso.

Para desmontar um endpoint

1. Na seção Montar caminhos, escolha o ponto final a ser desmontado.
2. Escolha Desmontar endpoint. O dispositivo da família Snow desmonta o endpoint e ele não está mais disponível para uso.

ℹ Note

Antes de desmontar um endpoint, certifique-se de que nenhum dado esteja sendo copiado dele ou para ele.

Montagem de endpoints NFS em computadores cliente

Depois que a interface NFS for iniciada e um endpoint montado, monte o endpoint como armazenamento local nos computadores cliente.

1. Em Montar caminhos, escolha o ícone de cópia do endpoint a ser montado. Cole-o em seu sistema operacional ao montar o endpoint.
2. A seguir estão os comandos de montagem padrão para sistemas operacionais Windows, Linux e macOS.

- 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
```

Interrompendo a interface NFS

Pare a interface NFS no dispositivo Snow Family quando terminar de transferir arquivos de ou para ele.

1. No painel, selecione Serviços e Armazenamento de arquivos.
2. Na página Armazenamento de arquivos, selecione Desabilitar transferência de dados. Geralmente leva até dois minutos para que os endpoints do NFS desapareçam do painel.

Usando DataSync para transferir arquivos para AWS

Você pode usar AWS OpsHub para criar um AWS DataSync agente em seu dispositivo Snowcone. Você pode usá-lo para transferir arquivos entre seu dispositivo e o Amazon S3, o Amazon Elastic File System (Amazon EFS) ou o FSx para o Windows File Server no Nuvem AWS.

AWS DataSync é um serviço de transferência de dados on-line projetado para simplificar, automatizar e acelerar a cópia de grandes quantidades de dados de e para serviços de AWS armazenamento. DataSync copia dados pela internet ou AWS Direct Connect. Como um serviço totalmente gerenciado, DataSync elimina grande parte da necessidade de modificar aplicativos, desenvolver scripts ou gerenciar a infraestrutura.

DataSync oferece suporte à transferência de dados entre o Network File System (NFS) e o Amazon EFS, o Amazon S3 ou o Amazon FSx for Windows File Server.

Para obter informações sobre a combinação de localização de origem e destino suportada pelo AWS DataSync, consulte [Trabalhando com locais](#) no Guia AWS DataSync do Usuário.

O Snowcone é fornecido com o DataSync agente, que é uma máquina virtual (VM) usada para ler ou gravar dados de um sistema de armazenamento local. Para usar DataSync, primeiro você inicia o agente e depois acessa o DataSync console e o ativa. Para obter informações sobre DataSync, consulte [Introdução ao AWS DataSync](#).

Para iniciar o DataSync agente

1. Antes de iniciar o DataSync agente, habilite o NFS em seu dispositivo Snowcone. Consulte [Configurando a interface NFS automaticamente](#) e [Iniciando o NFS e restringindo o acesso](#).
2. No AWS OpsHub painel, escolha Iniciar na seção Sincronizar com a nuvem para abrir o assistente Iniciar DataSync agente. O formulário Iniciar DataSync agente é preenchido com os campos Endereço IP do dispositivo e Interface de rede física.
3. Escolha Criar endereço IP (VNI) para criar um endereço IP virtual ou escolha Usar endereço IP existente.
4. Se você escolher Criar endereço IP (VNI), escolha DHCP ou IP estático na caixa de listagem Atribuição de endereço IP.

Se você escolher Usar endereço IP existente, escolha uma interface virtual na caixa de listagem Interface de rede virtual.

5. Escolha Iniciar atendente. Você será redirecionado para a página do DataSync recurso. Pode levar até cinco minutos para que o endereço IP do atendente apareça.

6. Use o ícone de cópia para copiar o valor do endereço IP do agente do arquivo de endereço IP do agente e escolha Abrir DataSync console.

Isso abre o DataSync console, onde você ativa o agente e transfere seus arquivos. O resto da configuração é feito no AWS DataSync console.

Transferindo arquivos com DataSync

AWS Snowcone já criou o agente, então você só precisa ativá-lo, configurar sua localização de origem e destino, criar uma tarefa e iniciar a tarefa.

Para ativar o DataSync agente e usar o DataSync serviço

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. Na seção Ativação da página Criar atendente, cole o endereço IP copiado na caixa de texto Endereço do atendente e selecione Obter chave. O navegador se conecta a esse endereço IP para obter uma chave de ativação exclusiva do atendente.
3. Depois que o agente for ativado, você configurará o NFS em execução no seu dispositivo Snowcone como um local de origem para DataSync. Para obter instruções, consulte [Configurar um local de origem](#) no Guia do usuário do AWS DataSync .

Note

O DataSync agente em execução no seu dispositivo Snowcone pode transferir arquivos de e para um local acessível na sua rede.

4. Na página Configurar um destino, escolha e configure o destino para o qual deseja transferir arquivos. Para obter instruções, consulte [Configurar um local de destino](#) no Guia do usuário do AWS DataSync .
5. Defina a configuração da tarefa. Para obter instruções, consulte [Configuração rápida](#) no Manual do usuário do AWS DataSync .
6. Revise as configurações e crie a tarefa. Para obter instruções, consulte [Revisar as configurações e criar a tarefa](#) no Guia do usuário do AWS DataSync .
7. Inicie a tarefa e aguarde a transferência dos arquivos. Para obter instruções, consulte [Iniciar a tarefa](#) no Guia do usuário do AWS DataSync .

Gerenciar seus dispositivos

Você usa o AWS OpsHub para gerenciar seus dispositivos Snow Family. Na página de detalhes do dispositivo, você pode realizar as mesmas tarefas que você faz usando o AWS CLI, incluindo alterar o alias do seu dispositivo, reinicializar o dispositivo e verificar se há atualizações.

Tópicos

- [Reinicializar seu dispositivo](#)
- [Desligando seu dispositivo](#)
- [Editar seu alias de dispositivo](#)
- [Obter atualizações para seu dispositivo e o AWS OpsHub aplicativo](#)
- [Como gerenciar perfis](#)

Reinicializar seu dispositivo

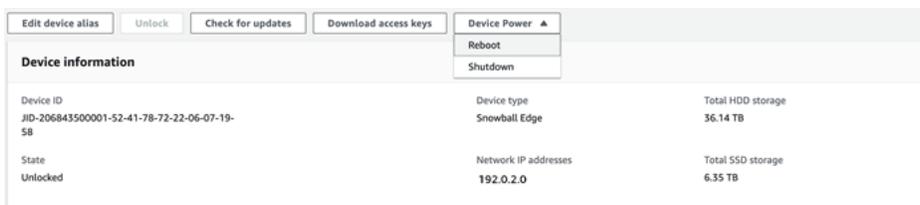
Siga estas etapas para reinicializar seu dispositivo Snow. AWS OpsHub

Important

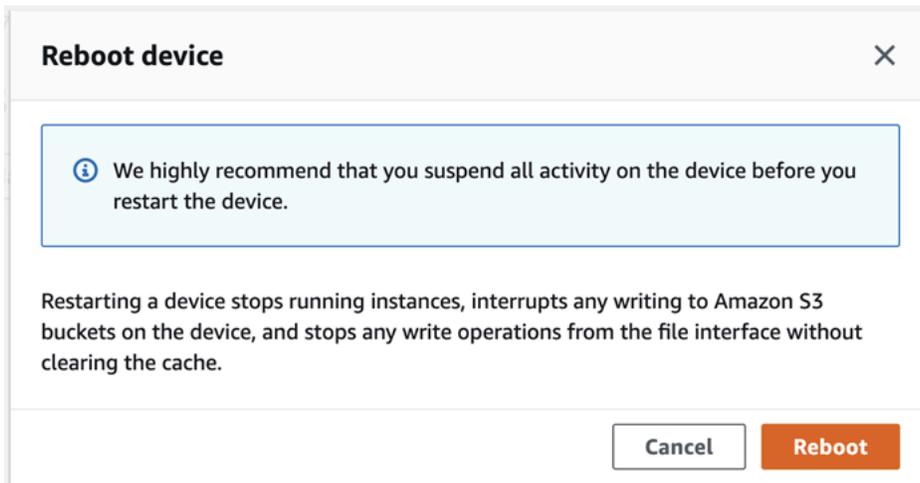
É altamente recomendável suspender todas as atividades no dispositivo antes de reinicializá-lo. A reinicialização de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo.

Como reinicializar um dispositivo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Depois escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha o menu Alimentação do dispositivo e, em seguida, escolha Reinicializar. Uma caixa de diálogo é exibida.



3. Na caixa de diálogo, escolha Reiniciar. O dispositivo começa a ser reinicializado.



Desligando seu dispositivo

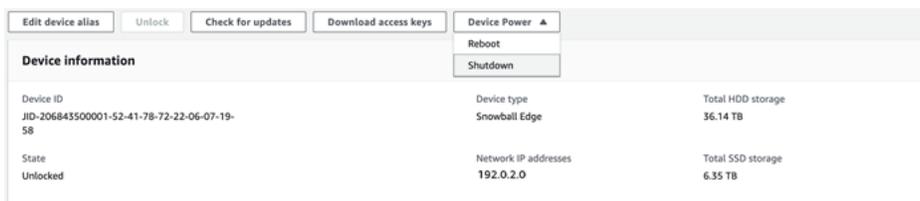
Siga estas etapas AWS OpsHub para desligar seu dispositivo Snow.

Important

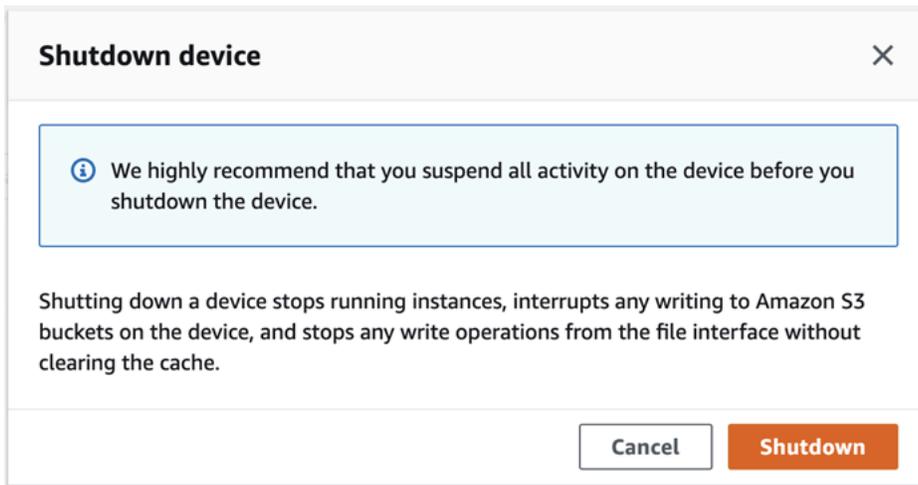
É altamente recomendável suspender todas as atividades no dispositivo antes de reiniciá-lo. O desligamento de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo.

Para desligar o dispositivo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Depois escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha o menu Alimentação do dispositivo e, em seguida, escolha Desligar. Uma caixa de diálogo é exibida.



3. Na caixa de diálogo, escolha Desligar. Seu dispositivo começa a ser desligado.

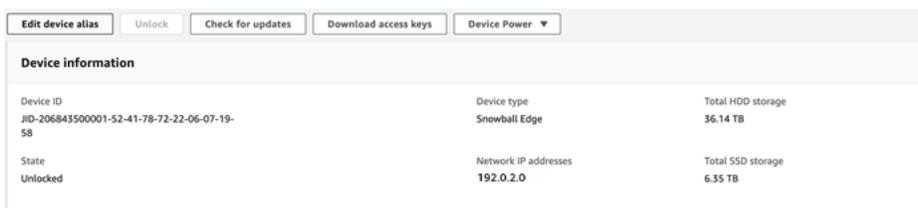


Editar seu alias de dispositivo

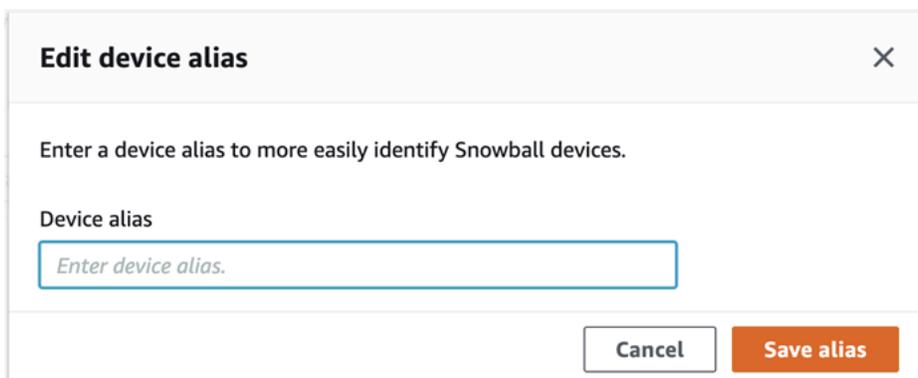
Use essas etapas para editar o alias do seu dispositivo usando AWS OpsHub.

Como editar o alias do seu dispositivo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha a guia Editar alias de dispositivo.



3. Em Alias de dispositivo , insira um novo nome e escolha Salvar alias.



Obter atualizações para seu dispositivo e o AWS OpsHub aplicativo

Você pode verificar se há atualizações para o seu dispositivo e instalá-las. Você também pode configurar AWS OpsHub para atualizar automaticamente o aplicativo para a versão mais recente.

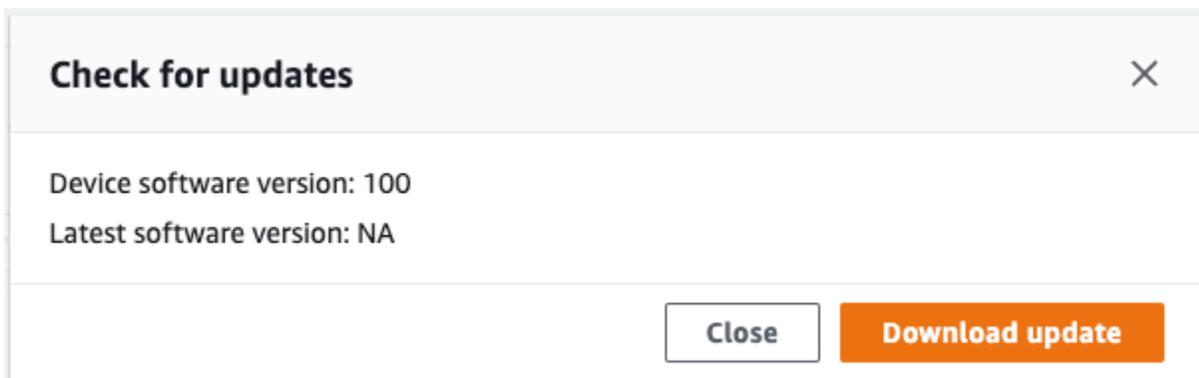
Atualizar seu dispositivo

Siga estas etapas AWS OpsHub para atualizar seu dispositivo Snow.

Como atualizar seu dispositivo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha a guia Verificar se há atualizações.

A página Verificar se há atualizações exibe a versão atual do software no seu dispositivo e a versão mais recente dele, se houver uma.



3. Se houver uma atualização, escolha Atualizar. Caso contrário, escolha Fechar.

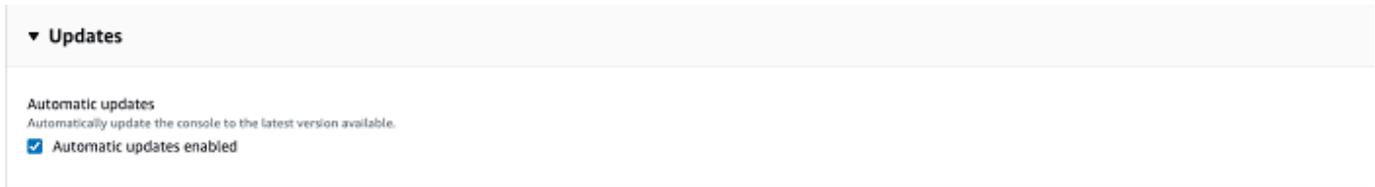
Atualizando seu AWS OpsHub aplicativo

AWS OpsHub atualiza automaticamente o aplicativo para a versão mais recente. Siga estas etapas para verificar se a atualização automática está ativada.

Para verificar se as atualizações automáticas estão habilitadas para AWS OpsHub

1. No AWS OpsHub painel, escolha Preferências.
2. Abra a guia Atualizações.

3. Verifique se a opção Atualizações automáticas ativadas está selecionada. A análise automática está habilitada por padrão.



Se as atualizações automáticas ativadas não estiverem selecionadas, você não obterá a versão mais recente do AWS OpsHub aplicativo.

Como gerenciar perfis

Você pode criar um perfil para armazenamento persistente das suas credenciais no sistema de arquivos local. Usando AWS OpsHub, você tem a opção de criar um novo perfil sempre que desbloquear o dispositivo usando o endereço IP, o código de desbloqueio e o arquivo de manifesto do dispositivo.

Você também pode usar o Snowball Edge Client para criar um perfil a qualquer momento. Consulte [Configurar um perfil para o Snowball Edge Client](#).

Para editar ou excluir perfis, edite o arquivo de perfil em um editor de texto.

Example Exemplo de arquivo **snowball-edge.config**

Este exemplo mostra um arquivo de perfil contendo três perfis:

SnowDevice1profileSnowDevice2profile e 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": []
  }
}
```

Como criar um perfil

1. Desbloqueie seu dispositivo localmente e faça login de acordo com as instruções em [Desbloquear um dispositivo](#).
2. Nomeie o perfil e escolha Salvar nome do perfil.

Como editar um perfil

1. Em um editor de texto, abra `snowball-edge.config` em `home directory\\.aws\\snowball\\config`.
2. Edite esse arquivo conforme for necessário. Por exemplo, para alterar o endereço IP de um dispositivo no perfil, altere a entrada `defaultEndpoint`.
3. Salve e feche o arquivo.

Como excluir um perfil

1. Usando um editor de texto, abra `snowball-edge.config` em `home directory\.aws\snowball\config`.
2. Exclua a linha que contém o nome do perfil, os colchetes `{ }` que seguem o nome do perfil e o conteúdo dentro desses colchetes.
3. Salve e feche o arquivo.

Configurando os servidores de horário NTP para o seu dispositivo

Siga estas etapas para visualizar e atualizar com quais servidores de horário seu dispositivo deve sincronizar o horário.

Para verificar as fontes de tempo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Você verá uma lista das fontes de tempo com as quais seu dispositivo está sincronizando a hora na tabela Fontes de tempo.

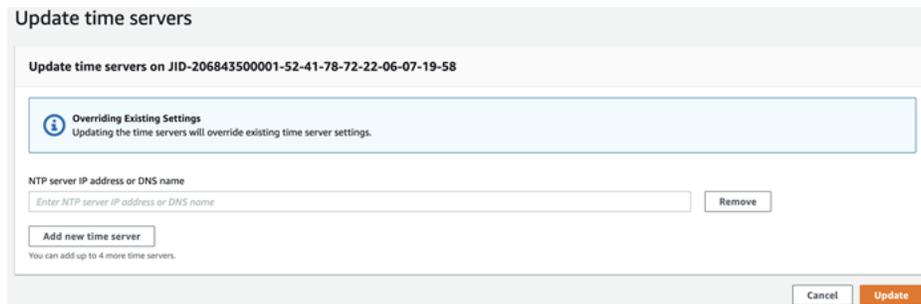
A tabela Fontes de tempo tem quatro colunas:

- **Endereço:** o nome DNS/endereço IP da fonte de horário
- **Estado:** o status atual da conexão entre o dispositivo e essa fonte de tempo, há 5 estados possíveis:
 - **ATUAL:** a fonte de tempo está sendo usada atualmente para sincronizar o tempo
 - **COMBINADO:** a fonte de tempo é combinada com a fonte atual
 - **EXCLUÍDO:** a fonte de tempo é excluída pelo algoritmo de combinação
 - **PERDIDO:** a conexão com a fonte de tempo foi perdida
 - **INDISPONIBILIDADE:** uma fonte de tempo inválida em que o algoritmo de combinação foi considerado falso ou tem muita variabilidade
- **Tipo:** as fontes do Network Time Protocol (NTP) podem ser um servidor ou um peer. Um servidor pode ser configurado pelo usuário usando o comando `update-time-server`, enquanto um peer só pode ser configurado usando outros dispositivos Snowball Edge no cluster e é configurado automaticamente quando o cluster é associado.

- **Estrato:** o estrato da fonte. O Estrato 1 indica uma fonte com um relógio de referência conectado localmente. Uma fonte sincronizada com uma fonte Estrato 1 é definida como Estrato 2. Uma fonte sincronizada com uma fonte do Estrato 2 é definida no Estrato 3 e assim por diante.

Para atualizar os servidores de tempo

1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Você verá uma lista das fontes de tempo com as quais seu dispositivo está sincronizando a hora na tabela Fontes de tempo.
3. Escolha Atualizar servidores de tempo na tabela Fontes de tempo.
4. Forneça o nome DNS ou o endereço IP dos servidores de tempo com os quais você gostaria que seu dispositivo sincronizasse o tempo e escolha Atualizar.



Update time servers

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

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

NTP server IP address or DNS name
Enter NTP server IP address or DNS name

You can add up to 4 more time servers.

Usando o AWS Snowball Edge cliente

O cliente Snowball Edge é um aplicativo de terminal independente que você executa no servidor local para desbloquear o AWS Snowcone dispositivo e obter credenciais, registros e informações de status. Ao usar o Snowball Edge Client, você pode obter informações de suporte adicionais executando o comando `snowballEdge help`.

Ao ler e gravar dados no AWS Snowcone dispositivo, você usa a interface NFS. Você também pode usar o AWS OpsHub for Snow Family aplicativo para gerenciar dispositivos da Família Snow, incluindo dispositivos Snowcone. Para ter mais informações, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

Fazer download e instalar o Snowball Edge Client

É possível fazer download e instalar o Snowball Edge Client em [Atributos do AWS Snowball](#). Nessa página, localize o pacote de instalação para o sistema operacional e siga as instruções para instalar o Snowball Edge Client. A execução do Snowball Edge Client de um terminal na estação de trabalho pode exigir o uso de um caminho específico, dependendo do sistema operacional:

- Microsoft Windows – Quando o cliente estiver instalado, ele pode ser executado a partir de qualquer diretório sem nenhuma preparação adicional.
- Linux: o Snowball Edge Client deve ser executado a partir do diretório `~/snowball-client-linux-build_number/bin/`. Observe que o Snowball Edge Client só é compatível com distribuições de 64 bits do Linux.
- macOS – o script `install.sh` copia pastas do arquivo `.tar` do Snowball Edge Client para o diretório `/usr/local/bin/snowball`. Se você executar esse script, poderá executar o cliente Snowball Edge em qualquer diretório, se `/usr/local/bin` for um caminho no seu `bash_profile`. Para verificar o caminho, use o comando `echo $PATH`.

Comandos para o Snowball Edge Client

A seguir, você encontrará informações sobre os comandos do Snowball Edge Client, incluindo exemplos de uso e exemplos de saídas.

Note

O AWS Snowcone dispositivo usa os mesmos comandos da CLI do Snowball Edge, mas não oferece suporte a comandos que se aplicam ao clustering.

Tópicos

- [Configurar um perfil para o Snowball Edge Client](#)
- [Obter o código QR para validação NFC](#)
- [Desbloqueando um dispositivo AWS Snowcone](#)
- [Atualizando um Snowcone](#)
- [Como obter as credenciais](#)
- [Iniciando um serviço em seu dispositivo Snowcone](#)
- [Interrupção de um serviço em seu dispositivo Snowcone](#)
- [Obter certificado para transferência de dados](#)
- [AWS Snowcone Registros](#)
- [Ver status do dispositivo](#)
- [Ver status do serviço](#)
- [Lançamento da AWS DataSync AMI](#)
- [Iniciando o NFS e restringindo o acesso](#)
- [Restringindo o acesso aos compartilhamentos NFS quando o NFS está em execução](#)
- [Obtenção do caminho de exportação para um bucket do Amazon S3](#)
- [Habilitando a AWS depuração do operador local](#)
- [Desativando a depuração AWS do operador local](#)
- [Criando uma interface de rede direta](#)
- [Obtendo informações sobre uma interface de rede direta](#)
- [Atualizando uma interface de rede direta](#)
- [Excluindo uma interface de rede direta](#)
- [Verificação do status do atributo](#)
- [Alterar status do atributo](#)
- [Configurando servidores de horário](#)
- [Verificando fontes de tempo](#)

Configurar um perfil para o Snowball Edge Client

Toda vez que você executar um comando para o Snowball Edge Client, forneça o arquivo manifesto, código de desbloqueio e um endereço IP. Você pode obter os dois primeiros na API de gerenciamento de tarefas Console de Gerenciamento da família AWS Snow ou na API de gerenciamento de tarefas. Para obter mais informações sobre como obter o código de manifesto e de desbloqueio, consulte [Como obter as credenciais](#).

Você tem a opção de usar o comando `snowballEdge configure` para armazenar o caminho até o manifesto, o código de desbloqueio de 29 caracteres e o endpoint como um perfil. Após a configuração, será possível usar outros comandos do Snowball Edge Client sem precisar inserir manualmente esses valores para um trabalho específico. Depois de configurar o Snowball Edge Client, as informações serão salvas em um formato JSON de texto simples em *home directory*/.aws/snowball/config/snowball-.config.

O endpoint é o endereço IP, com `https://` adicionado a ele. Você pode localizar o endereço IP do AWS Snowcone dispositivo na tela LCD do AWS Snowcone dispositivo. Quando o AWS Snowcone é conectado à rede pela primeira vez, ele recebe automaticamente um endereço IP DHCP, se um servidor DHCP estiver disponível. Se quiser usar um endereço IP diferente, é possível alterá-lo na tela LCD. Para ter mais informações, consulte [Usando AWS serviços em AWS Snowcone](#).

Important

Qualquer pessoa que possa acessar o arquivo de configuração poderá acessar os dados no seu dispositivo do Snowcone. Gerenciar o controle de acesso local a este arquivo é uma das suas responsabilidades administrativas.

Uso

Você pode usar esse comando de duas formas: em linha ou quando solicitado. Este exemplo de uso mostra o método solicitado.

```
snowballEdge configure
```

Example Exemplos de resultado

```
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
```

Você pode ter vários perfis se tiver vários trabalhos ao mesmo tempo. Para obter mais informações sobre vários AWS CLI perfis, consulte [Perfis nomeados](#) no Guia AWS Command Line Interface do usuário.

Obter o código QR para validação NFC

Você pode usar esse comando para gerar um código QR específico do dispositivo para uso com o aplicativo de verificação do AWS Snowcone . O download pode ser feito na App Store da Apple ou na loja Google Play. Para obter mais informações sobre validação de NFC, consulte [Validação de tags NFC](#).

Uso

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

Example Exemplos de resultado

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

Desbloqueando um dispositivo AWS Snowcone

Para desbloquear um AWS Snowcone dispositivo independente, execute o `snowballEdge unlock-device` comando. Esses comandos autenticam seu acesso ao AWS Snowcone dispositivo.

Ao executar um desses comandos de desbloqueio, você pode inserir manualmente o caminho para o arquivo manifesto, o código de desbloqueio de 29 caracteres e o endereço IP do seu dispositivo independente. Esse processo pode ser entediante, então recomendamos que você configure seu Snowball Edge Client em vez disso. Se você já configurou o Snowball Edge Client, só precisa inserir o comando em si sem o caminho para o manifesto, o código de desbloqueio ou o endereço IP.

Note

Para desbloquear o dispositivo associado ao seu trabalho, ele deve estar no local, ligado e conectado à rede e à alimentação. Além disso, o display LCD na parte frontal do AWS Snowcone dispositivo deve indicar que o dispositivo está pronto para uso.

Uso (Snowball Edge Client configurado)

```
snowballEdge unlock-device
```

Example

Example Desbloquear saída

```
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.
```

Atualizando um Snowcone

Use os comandos a seguir baixar e instalar atualizações em seu dispositivo Snowcone. Para obter os procedimentos que usam esses comandos, consulte [Atualizando um Snowcone](#).

`snowballEdge check-for-updates`: retorna informações sobre a versão do software Snowball disponível na nuvem e a versão atual instalada no dispositivo.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

`snowballEdge describe-device-software`: retorna a versão atual do software do dispositivo. Além disso, se a atualização estiver sendo obtida por download, o estado do download também será exibido. Se uma atualização de software estiver em andamento, o manifesto de atualização da versão e o estado da instalação também serão exibidos. Uma lista das saídas possíveis é mostrada a seguir:

- `NA`: nenhuma atualização de software está em andamento no momento.
- `Downloading`: novo software está sendo obtido por download.
- `Installing`: novo software está sendo instalado.

- **Requires Reboot:** novo software foi instalado, e o dispositivo deve ser reiniciado.

⚠ Warning

É altamente recomendável suspender todas as atividades no dispositivo antes de reiniciá-lo. A reinicialização de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo. Todos esses processos podem resultar em perda de dados.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

`snowballEdge download-updates`: inicia o download das atualizações mais recentes do Snowcone.

Uso (Snowball Edge Client configurado)

```
snowballEdge download-updates
```

Example Exemplos de resultado

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

`snowballEdge install-updates`: inicia a instalação das atualizações mais recentes do Snowcone que já foram obtidas por download.

Uso (Snowball Edge Client configurado)

```
snowballEdge install-updates
```

Example Exemplos de resultado

```
Installation started.
```

`snowballEdge reboot-device`: reinicia o dispositivo.

Warning

É altamente recomendável suspender todas as atividades no dispositivo antes de reiniciá-lo. A reinicialização de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo. Todos esses processos podem resultar em perda de dados.

Uso (Snowball Edge Client configurado)

```
snowballEdge reboot-device
```

Example Exemplos de resultado

```
Rebooting device now.
```

`snowballEdge configure-auto-update-strategies`: configura uma estratégia de atualização automática.

Uso (Snowball Edge Client configurado)

```
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 Exemplos de resultado

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

`snowballEdge describe-auto-update-strategies`: retorna qualquer estratégia de atualização automática configurada atualmente.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

```
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;
]}
```

Como obter as credenciais

Ao usar os comandos `snowballEdge list-access-keys` e `snowballEdge get-secret-access-key`, você pode obter suas credenciais locais. Você os usa para autenticar suas solicitações ao usar o AWS CLI ou com um AWS SDK. Essas credenciais só estão associadas a um trabalho individual para o Snowcone, e você pode usá-las apenas no dispositivo. O dispositivo não tem nenhuma permissão AWS Identity and Access Management (IAM) na Nuvem AWS.

Para obter mais informações, consulte [Credenciais da AWS](#) e [Uso do endpoint do Amazon EC2](#).

Note

Se você estiver usando o AWS CLI com o Snowball, deverá usar essas credenciais ao configurar a CLI. Para obter informações sobre como configurar credenciais para a CLI, consulte [Configuração rápida](#) no Manual do usuário do AWS Command Line Interface .

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Iniciando um serviço em seu dispositivo Snowcone

O Snowcone oferece suporte a vários serviços, incluindo instâncias de computação, interface de arquivos NFS, Amazon EC2 e AWS DataSync. Você pode iniciar esses serviços com o comando `snowballEdge start-service`. Para obter o ID de serviço para cada serviço, use o comando `snowballEdge list-services`.

Antes de executar esse comando, crie uma única interface de rede virtual para vincular ao serviço que está iniciando. Para ter mais informações, consulte [Criação de uma interface de rede virtual](#).

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Interrupção de um serviço em seu dispositivo Snowcone

Para interromper um serviço em execução no Snowcone, use o comando `snowballEdge stop-service`. Os serviços do Amazon EC2 não podem ser interrompidos.

Warning

A perda de dados pode ocorrer se a interface de arquivos for interrompida antes que os dados em buffer restantes sejam gravados no dispositivo.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Obter certificado para transferência de dados

Para transferir dados para um dispositivo Snowcone, use a interface NFS ou AWS DataSync. Se você desbloquear seu dispositivo Snowcone com um endereço IP diferente, um novo certificado será gerado e o certificado antigo não ficará mais válido para usar com o endpoint. Obtenha o certificado novo e atualizado do Snowcone novamente usando o comando `get-certificate`.

Você pode listar esses certificados e fazer download deles no seu dispositivo Snowcone usando os seguintes comandos:

- `list-certificates` – Lista os nomes de recursos da Amazon (ARNs) dos certificados disponíveis para uso.

Uso (Snowball Edge Client configurado)

```
snowballEdge list-certificates
```

Example Exemplos de resultado

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

- `get-certificate` – Obtém um certificado específico, com base no ARN fornecido.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

AWS Snowcone Registros

Quando você transferir dados entre o datacenter on-premises e um dispositivo Snowcone, os logs são gerados automaticamente. Se forem encontrados erros inesperados durante a transferência de dados para o dispositivo, use os comandos a seguir para salvar uma cópia dos logs no servidor local.

Há três comandos relacionados a logs:

- `list-logs`: retorna uma lista de logs no formato JSON. Esta lista relata o tamanho dos logs em bytes, além do ARN, ID de serviço e tipo dos logs.

Uso (Snowball Edge Client configurado)

```
snowballEdge list-logs
```

Example Exemplos de resultado

```
{
  "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-JIEXAMPLEf-1234-4953-
a7c4-dfEXAMPLE709",
    "LogType" : "CUSTOMER",
    "ServiceId" : "nfs",
    "EstimatedSizeBytes" : 4446
  }
]
```

- `get-log`— Faz o download de uma cópia de um registro específico do dispositivo Snowcone para o seu servidor em um caminho especificado. CUSTOMER os registros são salvos no `.zip` formato e você pode extrair esse tipo de registro para visualizar seu conteúdo. SUPPORT os registros são criptografados e só podem ser lidos por AWS Support engenheiros. Você tem a opção de especificar um nome e um caminho para o log.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

- `get-support-logs`: faz download da cópia de todos os logs de tipo SUPPORT a partir do Snowcone para o seu serviço em um caminho específico.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Important

Os logs de CUSTOMER podem conter informações confidenciais sobre seus próprios dados. Para proteger essas informações potencialmente confidenciais, sugerimos que você exclua esses logs assim que concluir o uso deles.

Ver status do dispositivo

Você pode determinar o status e a integridade geral do seu dispositivo Snowcone usando os seguintes comandos do Snowball Edge Client:

- `describe-device`

Uso (Snowball Edge Client configurado)

```
snowballEdge describe-device
```

Example Exemplos de resultado

```
{
  "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"
}
```

Ver status do serviço

Você pode determinar o status e a integridade geral dos serviços que funcionam em um dispositivo Snowcone usando o comando `describe-service`. Você pode primeiro executar o comando `list-services` para ver quais serviços estão em execução.

- `list-services`

Uso (Snowball Edge Client configurado)

```
snowballEdge list-services
```

Example Exemplos de resultado

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

- `describe-service`

Esse comando retorna um valor de status para um serviço. Ele também inclui informações de estado que podem ser úteis ao resolver problemas encontrados no serviço. Esses estados são os seguintes.

- **ACTIVE** – o serviço está em execução e disponível para o uso.
- **ACTIVATING** – o serviço está iniciando, mas ainda não está disponível para o uso.
- **DEACTIVATING** – o serviço está no processo de desligamento.
- **INACTIVE** – o serviço não está em execução e não está disponível para o uso.

Uso (Snowball Edge Client configurado)

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

Example Exemplos de resultado

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

Lançamento da AWS DataSync AMI

Inicie a AWS DataSync AMI no Snowcone.

Uso (Snowball Edge Client configurado)

AWS DataSync deve ser executado com o tipo de `snc1.medium` instância. A execução DataSync com um tipo de instância diferente pode resultar em uma operação instável e em uma possível perda de dados. Use o comando `describe-images` para encontrar a imagem a partir da qual iniciar uma instância. A saída é semelhante à seguinte.

```
{
```

```

"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 Exemplos de resultado

```

{
  "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"
],
},
}

```

Execute a instância.

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

Example Exemplos de resultado

```

{
  "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"
}
```

Iniciando o NFS e restringindo o acesso

Important

Não inicie o serviço NFS se você pretende usar o Amazon Elastic Block Store (Amazon EBS). Na primeira vez que o NFS é iniciado, todo o armazenamento é alocado ao NFS. Não é possível realocar o armazenamento NFS para o Amazon EBS, mesmo que o serviço NFS seja interrompido.

Note

O espaço de armazenamento disponível no dispositivo Snowcone não é preciso até que o serviço NFS seja iniciado.

É possível fornecer blocos CIDR para intervalos de endereços IP que têm permissão para montar os compartilhamentos do NFS expostos pelo dispositivo. Por exemplo,

10.0.0.0/16. Se você não fornecer blocos CIDR permitidos, todas as solicitações de montagem serão negadas.

Os dados transferidos por meio do NFS não são criptografados em trânsito.

Além dos hosts permitidos pelos blocos CIDR, o Snowcone não fornece nenhum mecanismo de autenticação ou de autorização para os compartilhamentos do NFS.

Inicie o NFS com o comando `snowballEdge start-service`. Para obter o ID de serviço para cada serviço, use o comando `snowballEdge list-services`.

Antes de executar esse comando, crie uma única interface de rede virtual para vincular ao serviço que está iniciando. Para ter mais informações, consulte [Criação de uma interface de rede virtual](#). Você pode restringir o acesso aos seus compartilhamentos de arquivos e dados em seus buckets do Amazon S3 e ver quais restrições estão em vigor no momento. Você faz isso alocando blocos CIDR para hosts permitidos que podem acessar seu compartilhamento de arquivos e buckets do S3 quando você inicia o serviço NFS.

Uso (Snowball Edge Client configurado)

```
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 Exemplos de resultado

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

Restringindo o acesso aos compartilhamentos NFS quando o NFS está em execução

Você pode restringir o acesso aos seus compartilhamentos de arquivos e dados em seus buckets do Amazon S3 depois de iniciar o NFS. Você pode ver quais restrições estão em vigor no momento e atribuir restrições de acesso diferentes a cada bucket. Você faz isso alocando blocos CIDR para hosts que podem acessar seu compartilhamento de arquivos e buckets S3 quando você inicia o serviço NFS. O comando a seguir é um exemplo.

Uso (Snowball Edge Client configurado)

```
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
```

Para ver as restrições atuais, use o comando `describe-service`.

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

Obtenção do caminho de exportação para um bucket do Amazon S3

Não há um comando do Snowcone específico para obter o caminho de exportação de um bucket do Amazon S3. O formato do caminho de exportação é semelhante ao seguinte.

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

Habilitando a AWS depuração do operador local

- `enable-local-aws-operator-debugging`— Ativa o dispositivo para depuração AWS do operador local abrindo a porta SSH 22.

Uso (Snowball Edge Client configurado)

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

Desativando a depuração AWS do operador local

- `disable-local-aws-operator-debugging`: desabilita o dispositivo para depuração do operador local da AWS fechando a porta SSH 22. Por padrão, a porta SSH 22 está fechada. Quando o dispositivo Snowcone é desligado ou é desligado, a depuração do AWS operador local é desativada.

Uso (Snowball Edge Client configurado)

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

Criando uma interface de rede direta

- `create-direct-network-interface` : [cria uma interface de rede direta \(DNI\)](#). Cria uma interface de rede direta para usar com instâncias computacionais do Amazon EC2 em seu dispositivo. Você pode encontrar as interfaces de rede diretas disponíveis em seu dispositivo usando o comando `describe-direct-network-interfaces`.

Uso (Snowball Edge Client configurado)

```
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]
```

Obtendo informações sobre uma interface de rede direta

- `describe-direct-network-interface` : obtém as interfaces de rede diretas em seu dispositivo. Uma interface de rede direta pode ser usada para configurar a rede para instâncias e serviços de computação do Amazon EC2 em seu dispositivo. Você pode criar uma nova interface de rede direta usando o comando `create-direct-network-interface`.

Uso (Snowball Edge Client configurado)

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

Atualizando uma interface de rede direta

- `update-direct-network-interface` : atualiza uma interface de rede direta. Use esse comando para atualizar uma interface de rede direta que será usada com as instâncias de computação do Amazon EC2 em seu dispositivo. Você pode encontrar as interfaces de rede diretas que estão disponíveis no seu dispositivo usando o comando `describe-direct-network-interfaces`. Quando você estiver modificando uma interface de rede conectada a uma instância do Amazon EC2, a interface será primeiro desanexada.

Uso (Snowball Edge Client configurado)

```
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]
```

Excluindo uma interface de rede direta

- `delete-direct-network-interface`: exclui uma interface de rede direta que não está mais em uso. Para excluir uma interface de rede direta associada à sua instância de computação do Amazon EC2, você deve primeiro desassociar a interface de rede direta da sua instância.

Uso (Snowball Edge Client configurado)

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

Verificação do status do atributo

Para listar o status dos recursos disponíveis em seu dispositivo AWS Snow Device Management, inclusive os que permitem gerenciar seu dispositivo Snowcone e AWS serviços locais remotamente, use o comando `describe-features`

`RemoteManagementState`: indica o status do Snow Device Management e retorna um dos seguintes estados:

- `INSTALLED_ONLY`: o atributo está instalado, mas não ativado.
- `INSTALLED_AUTOSTART`— O recurso está ativado e o dispositivo tentará se conectar ao mesmo Região da AWS quando estiver ligado.
- `NOT_INSTALLED`: o dispositivo não suporta o atributo ou já estava em campo antes de seu lançamento.

Uso (Snowball Edge Client configurado)

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

Exemplos de resultado

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

Alterar status do atributo

Para alterar o status dos recursos disponíveis no seu AWS Snowcone dispositivo, use o `set-features` comando. Para ativar ou desativar AWS Snow Device Management, o que permite gerenciar seu dispositivo Snowcone e AWS serviços locais remotamente, use o parâmetro. `--remote-management-state` O dispositivo deve estar desbloqueado antes de você executar esse comando.

Você pode definir o Snow Device Management para os seguintes estados:

- `INSTALLED_ONLY`: o atributo está instalado, mas não ativado.
- `INSTALLED_AUTOSTART`— O recurso está ativado e o dispositivo tenta se conectar ao mesmo Região da AWS quando está ligado.

Note

O estado `NOT_INSTALLED` existe apenas para identificar dispositivos que não suportam o Snow Device Management ou que já estavam em campo antes de seu lançamento. Não é possível instalar ou desinstalar o atributo em dispositivos que já estão implantados. Para usar o Snow Device Management, você deve solicitar um novo dispositivo com o atributo pré-instalado.

Uso (Snowball Edge Client configurado)

```
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
```

Exemplos de resultado

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

Configurando servidores de horário

Você pode configurar um servidor NTP (Network Time Protocol). Você pode usar os comandos NTP CLI quando o dispositivo está nos estados bloqueado e desbloqueado. O manifesto e o código de desbloqueio são obrigatórios. Você pode defini-las com o comando `snowballEdge configure` ou usando as opções `--unlock-code` e `--manifest-file`. Observe que você pode usar a `snowballEdge` CLI no AWS Snowcone Edge e. AWS Snowcone

É sua responsabilidade fornecer um servidor de horário NTP seguro. Para definir a quais servidores de horário NTP o dispositivo se conecta, use o comando do CLI `update-time-servers`.

Note

O comando `update-time-servers` substituirá as configurações anteriores dos servidores de horário NTP.

Uso

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

Example Exemplos de resultado

```
Updating time servers now.
```

Verificando fontes de tempo

Para ver a quais fontes de horário de NTP o dispositivo está conectado atualmente, use o comando do CLI `describe-time-sources` para o Snowball Edge.

Uso

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

Example Exemplos de resultado

```
{
  "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
  } ]
}
```

O comando `describe-time-sources` retorna uma lista dos estados da fonte de tempo. Cada estado da fonte de tempo contém os campos `Address`, `State`, `Type` e `Stratum`. A seguir estão os significados desses campos.

- `Address`: o nome DNS/endereço IP da fonte de horário.
- `State`: o status atual da conexão entre o dispositivo e essa fonte de tempo. Existem cinco estados possíveis:
 - `CURRENT`: a fonte de tempo está sendo usada atualmente para sincronizar a hora.
 - `COMBINED`: a fonte de tempo é combinada com a fonte atual.
 - `EXCLUDED`: a fonte de tempo é excluída pelo algoritmo de combinação.
 - `LOST`: a conexão com a fonte de tempo foi perdida.
 - `UNACCEPTABLE`: uma fonte de tempo inválida em que o algoritmo de combinação foi considerado falso ou tem muita variabilidade.
- `Type`: uma fonte de horário NTP pode ser um servidor ou um peer. Os servidores podem ser configurados pelo comando `update-time-servers`. Os pares só podem ser outros dispositivos Snowball Edge no cluster e são configurados automaticamente quando o cluster é associado.
- `Stratum`: esse campo mostra o estrato da fonte. O estrato 1 indica uma fonte com um relógio de referência conectado localmente. Uma fonte sincronizada com uma fonte do estrato 1 está no estrato 2. Uma fonte sincronizada com uma fonte do estrato 2 está no estrato 3 e assim por diante.

Uma fonte de horário NTP pode ser um servidor ou um peer. Um servidor pode ser configurado pelo usuário com o comando `update-time-servers`, enquanto um par só pode ser outros dispositivos Snowball Edge no cluster. No exemplo de saída, `describe-time-sources` é chamado em um Snowball Edge que está em um cluster de 5. A saída contém 4 pares e 1 servidor. Os pares têm um estrato de 10, enquanto o servidor tem um estrato de 1; portanto, o servidor é selecionado para ser a fonte de horário atual.

Usando AWS Snow Device Management para gerenciar dispositivos

AWS Snow Device Management permite que você gerencie seu dispositivo Snow Family e AWS serviços locais remotamente. Todos os dispositivos da família Snow oferecem suporte ao gerenciamento de dispositivos Snow e ele vem instalado em novos dispositivos na maioria dos Regiões da AWS locais onde os dispositivos da família Snow estão disponíveis.

Com o Snow Device Management, você pode realizar as seguintes tarefas:

- Criar uma tarefa
- Verificar o status da tarefa
- Verificar metadados de tarefas
- Cancelar uma tarefa
- Verifique as informações do dispositivo
- Verifique o estado da instância compatível com o Amazon EC2
- Listar comandos e sintaxe
- Listar dispositivos gerenciáveis remotamente
- Listar o status da tarefa em todos os dispositivos
- Listar atributos disponíveis
- Listar tarefas por status
- Listar tags de dispositivo ou tarefa
- Aplicar etiquetas
- Remover marcações

Tópicos

- [Escolhendo o estado de gerenciamento de dispositivos Snow ao solicitar um dispositivo da família Snow](#)
- [Ativando o gerenciamento de dispositivos Snow](#)
- [Adicionar permissões para o Snow Device Management a uma função do IAM](#)
- [Comandos da CLI do Snow Device Management](#)

Escolhendo o estado de gerenciamento de dispositivos Snow ao solicitar um dispositivo da família Snow

Ao criar um trabalho para solicitar um dispositivo Snow, você pode escolher em qual estado o Snow Device Management estará quando receber o dispositivo: instalado, mas não ativado, ou instalado e ativado. Se ele estiver instalado, mas não ativado, você precisará usar AWS OpsHub ou o cliente Snowball Edge para ativá-lo antes de usá-lo. Se estiver instalado e ativado, você poderá usar o Snow Device Management depois de receber o dispositivo e conectá-lo à sua rede local. Você pode escolher o estado de gerenciamento de dispositivos do Snow ao criar um trabalho para solicitar um dispositivo por meio do Console de Gerenciamento da família AWS Snow cliente Snowball Edge, do ou da API AWS CLI de gerenciamento de tarefas do Snow.

Para escolher o estado de gerenciamento de dispositivos Snow na Console de Gerenciamento da família AWS Snow

1. Para escolher que o Snow Device Management seja instalado e ativado, escolha Gerenciar seu dispositivo Snow remotamente com AWS OpsHub um cliente Snowball.
2. Para escolher que o Snow Device Management seja instalado, mas não ativado, não selecione Gerenciar seu dispositivo Snow remotamente com AWS OpsHub o cliente Snowball.

Para obter mais informações, consulte [Etapa 3: Escolha seus recursos e opções](#) neste guia.

Para escolher o estado do Snow Device Management a AWS CLI partir do cliente Snowball Edge ou da API de gerenciamento de tarefas do Snow:

- Use o `remote-management` parâmetro para especificar o estado do Snow Device Management. O `INSTALLED_ONLY` valor do parâmetro significa que o Snow Device Management está instalado, mas não ativado. O `INSTALLED_AUTOSTART` valor do parâmetro significa que o Snow Device Management está instalado e ativado. Se você não especificar um valor para esse parâmetro, `INSTALLED_ONLY` é o valor padrão.

Example da sintaxe do **remote-management** parâmetro do comando **create-job**

```
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 \

```

Para obter mais informações, consulte [Job Management API Reference](#) na AWS Snowball API Reference.

Ativando o gerenciamento de dispositivos Snow

Siga este procedimento para ativar o Snow Device Management usando o cliente Snowball Edge.

Antes de usar esse procedimento, faça o seguinte:

- Baixe e instale a versão mais recente do cliente Snowball Edge. Para obter mais informações, consulte [Baixar e instalar o Snowball Client](#).
- Baixe o arquivo de manifesto e obtenha o código de desbloqueio do dispositivo Snow Family. Para obter mais informações, consulte [Como obter suas credenciais e ferramentas](#).
- Conecte o dispositivo Snow Family à sua rede local. Para obter mais informações, consulte .
- Desbloqueie o dispositivo Snow Family. Para obter mais informações, consulte [Desbloqueando](#) um dispositivo localmente.

```

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

```

O cliente Snowball Edge retorna o seguinte quando o comando é bem-sucedido.

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

Adicionar permissões para o Snow Device Management a uma função do IAM

No local Conta da AWS do qual o dispositivo foi pedido, crie uma função AWS Identity and Access Management (IAM) e adicione a política a seguir à função. Em seguida, atribua a função ao usuário do IAM que fará login para gerenciar remotamente seu dispositivo com o Snow Device Management. Para obter mais informações, consulte [Criação de perfis do IAM](#) e [Criação de um usuário do IAM na sua Conta da AWS](#).

Política

```
{
  "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": "*"
    }
  ]
}
```

```
]
}
```

Comandos da CLI do Snow Device Management

Esta seção descreve os AWS CLI comandos que você pode usar para gerenciar seus dispositivos Snow Family remotamente com o Snow Device Management. Você também pode realizar algumas tarefas de gerenciamento remoto usando AWS OpsHub for Snow Family o. Para obter mais informações, consulte [Gerenciando AWS serviços em seu dispositivo](#) .

Note

Antes de gerenciar seu dispositivo, verifique se ele está ligado, conectado à sua rede e pode se conectar ao Região da AWS local onde foi provisionado.

Tópicos

- [Criar uma tarefa](#)
- [Verificar o status da tarefa](#)
- [Verifique as informações do dispositivo](#)
- [Verifique o estado da instância compatível com o Amazon EC2](#)
- [Verificar metadados de tarefas](#)
- [Cancelar uma tarefa](#)
- [Listar comandos e sintaxe](#)
- [Listar dispositivos gerenciáveis remotamente](#)
- [Listar o status da tarefa em todos os dispositivos](#)
- [Listar atributos disponíveis](#)
- [Listar tags de dispositivo ou tarefa](#)
- [Listar tarefas por status](#)
- [Aplicar etiquetas](#)
- [Remover marcações](#)

Criar uma tarefa

Para instruir um ou mais dispositivos de destino a realizar uma tarefa, como desbloquear ou reinicializar, use `create-task`. Você especifica os dispositivos de destino fornecendo uma lista de IDs de dispositivos gerenciados com o parâmetro `--targets` e especifica as tarefas a serem executadas com o parâmetro `--command`. Somente um único comando pode ser executado em um dispositivo por vez.

Comandos compatíveis:

- `unlock` (sem argumentos)
- `reboot` (sem argumentos)

Para criar uma tarefa a ser executada pelos dispositivos de destino, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

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

Saída

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

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

Verificar o status da tarefa

Para verificar o status de uma tarefa remota em execução em um ou mais dispositivos de destino, use o comando `describe-execution`.

Uma tarefa pode ter um dos seguintes estados:

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

Para verificar o status de uma tarefa, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

```
aws snow-device-management describe-execution \  
--taskId st-ficthmqoc2pht1ef \  
--managed-device-id smd-fictqic6gcldf111
```

Saída

```
{  
  "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"  
}
```

Verifique as informações do dispositivo

Para verificar informações específicas do dispositivo, como tipo de dispositivo, versão do software, endereços IP e status do bloqueio, use o comando `describe-device`. A saída inclui o seguinte:

- `lastReachedOutAt`: quando o dispositivo entrou em contato pela última vez com a Nuvem AWS. Indica que o dispositivo está on-line.
- `lastUpdatedAt`: quando os dados foram atualizados pela última vez no dispositivo. Indica quando o cache do dispositivo foi atualizado.

Para verificar as informações do dispositivo, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

```
{  
  "associatedWithJob": "JID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",  
  "deviceCapacities": [  
    {  
      "capacity": 100,  
      "unit": "GB"  
    }  
  ]  
}
```

```
{
  "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"
}
}
```

Verifique o estado da instância compatível com o Amazon EC2

Para verificar o estado atual da instância do Amazon EC2, use o comando `describe-ec2-instances`. A saída é semelhante à do `describe-device` comando, mas os resultados são provenientes do cache do dispositivo Nuvem AWS e incluem um subconjunto dos campos disponíveis.

Para verificar o estado da instância compatível com o Amazon EC2, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

```
{  
  "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"
}
]
```

Verificar metadados de tarefas

Para verificar os metadados de uma determinada tarefa em um dispositivo, use o comando `describe-task`. Os metadados de uma tarefa incluem os seguintes itens:

- Os dispositivos de destino
- O status da tarefa
- Quando a tarefa foi criada
- Quando os dados foram atualizados pela última vez no dispositivo
- Quando a tarefa foi concluída
- A descrição (se houver) fornecida quando a tarefa foi criada

Para verificar os metadados de uma tarefa, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

```
aws snow-device-management describe-task \
```

```
--task-id st-ficthmqoc2pht111
```

Exceções

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

```
{  
  "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"  
}
```

Cancelar uma tarefa

Para enviar uma solicitação de cancelamento para uma tarefa específica, use o comando `cancel-task`. Você pode cancelar somente tarefas no estado `QUEUED` que ainda não foram executadas. As tarefas que já estão em execução não podem ser canceladas.

Note

Uma tarefa que você está tentando cancelar ainda pode ser executada se for processada na fila antes que o comando `cancel-task` altere o estado da tarefa.

Para cancelar uma tarefa, use o seguinte comando. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

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

Listar comandos e sintaxe

Para retornar uma lista de todos os comandos compatíveis com a API Snow Device Management, use o comando `help`. Você também pode usar o comando `help` para retornar informações detalhadas e a sintaxe de um determinado comando.

Para listar todos os comandos suportados, use o comando a seguir.

Comando

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

Para retornar informações e sintaxe detalhadas de um comando, use o comando a seguir. Substitua *command* pelo nome do comando no qual você está interessado.

Comando

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

Listar dispositivos gerenciáveis remotamente

Para retornar uma lista de todos os dispositivos em sua conta que têm o Snow Device Management ativado na Região da AWS em que o comando é executado, use o comando `list-devices`. `--max-results` e `--next-token` são opcionais. Para obter mais informações, consulte [Usando as opções de AWS CLI paginação](#) no "Guia do usuário da interface de linha de AWS comando".

Para listar dispositivos gerenciáveis remotamente, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

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

Listar o status da tarefa em todos os dispositivos

Para retornar o status das tarefas de um ou mais dispositivos de destino, use o comando `list-executions`. Para filtrar a lista de retorno para mostrar as tarefas que estão atualmente em um único estado específico, use o parâmetro `--state`. `--max-results` e `--next-token` são opcionais. Para obter mais informações, consulte [Usando as opções de AWS CLI paginação](#) no "Guia do usuário da interface de linha de AWS comando".

Uma tarefa pode ter um dos seguintes estados:

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

Para listar o status da tarefa nos dispositivos, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

```
aws snow-device-management list-executions \  
--taskId st-ficthmqoc2phtlef \  
--state SUCCEEDED \  
--max-results 10
```

Exceções

```
ValidationException
InternalServerError
ThrottlingException
AccessDeniedException
```

Saída

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

Listar atributos disponíveis

Para retornar uma lista dos AWS recursos disponíveis para um dispositivo, use o `list-device-resources` comando. Para filtrar a lista por um tipo específico de recurso, use o parâmetro `--type`. Atualmente, as instâncias compatíveis com o Amazon EC2 são o único tipo de atributo compatível. `--max-results` e `--next-token` são opcionais. Para obter mais informações, consulte [Usando as opções de AWS CLI paginação](#) no "Guia do usuário da interface de linha de AWS comando".

Para listar os atributos disponíveis para um dispositivo, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

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

Exceções

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Saída

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

Listar tags de dispositivo ou tarefa

Para retornar uma lista de etiquetas de um dispositivo ou tarefa gerenciada, use o comando `list-tags-for-resource`.

Para listar as tags para um dispositivo, use o comando a seguir. Substitua o nome do recurso da Amazon (ARN) de exemplo pelo ARN de seu dispositivo.

Comando

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

Exceções

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Saída

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

Listar tarefas por status

Use o `list-tasks` comando para retornar uma lista de tarefas dos dispositivos na AWS região em que o comando é executado. Para filtrar os resultados pelos status `IN_PROGRESS`, `COMPLETED` ou `CANCELED`, use o parâmetro `--state`. `--max-results` e `--next-token` são opcionais. Para obter mais informações, consulte [Usando as opções de AWS CLI paginação](#) no "Guia do usuário da interface de linha de AWS comando".

Para listar as tarefas por status, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

```
aws snow-device-management list-tasks \
--state IN_PROGRESS \
--next-token K8VAMqKiP2Cf4xGkmH8GMyZrg0F8FUb+d10KTP9+P4pUb+8PhW+6MiXh4= \
--max-results 10
```

Exceções

```
ValidationException
InternalServerError
ThrottlingException
```

```
AccessDeniedException
```

Saída

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

Aplicar etiquetas

Para adicionar ou substituir uma tag em um dispositivo ou em uma tarefa em um dispositivo, use o comando `tag-resource`. O parâmetro `--tags` aceita uma lista de separados por vírgula `Key=Value`.

Para aplicar etiquetas a um dispositivo, use o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
```

ThrottlingException

Remover marcações

Para remover uma tag de um dispositivo ou de uma tarefa em um dispositivo, use o comando `untag-resources`.

Execute o comando a seguir para remover tags de um dispositivo. Substitua cada *user input placeholder* por suas próprias informações.

Comando

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

Exceções

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

Usando AWS serviços em AWS Snowcone

A seguir, você pode encontrar uma visão geral do AWS Snowcone dispositivo. AWS Snowcone é um dispositivo fisicamente robusto protegido por AWS Key Management Service (AWS KMS) que você pode usar para armazenamento e computação locais ou para transferir dados entre seus servidores locais e o Amazon Simple Storage Service (Amazon S3).

Para obter informações sobre como desbloquear um AWS Snowcone dispositivo, consulte. [Usando o AWS Snowball Edge cliente](#)

Assim que o dispositivo chegar, inspecione-o para ver se está danificado ou se apresenta alguma violação evidente.

Warning

Se observar qualquer coisa que pareça suspeita sobre o dispositivo, não o conecte à rede interna. Em vez disso, entre em contato com o [AWS Support](#), e você receberá um novo dispositivo.

Assim que o dispositivo chega e é ligado, você está pronto para usá-lo.

Tópicos

- [Usando instâncias computacionais compatíveis com o Amazon EC2](#)
- [Usando AWS DataSync para transferir arquivos](#)
- [Gerenciando a interface NFS](#)
- [Usando AWS IoT Greengrass para executar software pré-instalado em instâncias compatíveis com o Amazon EC2](#)
- [Portas necessárias para usar AWS serviços em um AWS Snowcone dispositivo](#)

Usando instâncias computacionais compatíveis com o Amazon EC2

Neste tópico, é possível encontrar uma visão geral do uso de instância do Amazon Elastic Compute Cloud (Amazon EC2) em um dispositivo AWS Snowcone . O tópico inclui informações conceituais, procedimentos e exemplos.

Note

Esses recursos não são suportados na Ásia-Pacífico (Mumbai) Região da AWS.

Visão geral

Você pode executar instâncias computacionais compatíveis com o Amazon EC2 hospedadas em um Snowcone usando os tipos de instância compatíveis com EC2. Assim como seus equivalentes baseados em nuvem, essas instâncias exigem imagens de máquina da Amazon (AMIs) para iniciar. Selecione a AMI a ser a imagem base para uma instância na nuvem, antes de criar o trabalho do Snowcone. Para obter mais informações sobre os tipos de instância compatíveis, consulte [Uso do Amazon EC2 no Snowcone](#).

Se o tipo de trabalho for computação local, você poderá criar um total de volumes EBS locais de 8 TiB e anexá-los a instâncias compatíveis com o Amazon EC2. Isso permite que instâncias locais compatíveis com EC2 acessem mais capacidade local do que apenas o volume raiz. Esse é somente o armazenamento local, portanto, os dados gravados nos volumes do EBS são perdidos quando o dispositivo é devolvido, AWS pois não podem ser importados para o Amazon S3.

Note

O servidor NFS não está disponível para trabalhos de computação. Se você precisar importar ou exportar dados de ou para o Nuvem AWS, não escolha o tipo de tarefa de computação local ao fazer seu pedido.

Para usar uma instância de computação em um Snowcone, crie um trabalho para solicitar um dispositivo da família Snow e especificar suas AMIs. Você pode fazer isso a partir do [Console de Gerenciamento da família AWS Snow](#), com o AWS CLI ou com um dos AWS SDKs. Normalmente, você deve realizar alguns pré-requisitos de manutenção antes da criação do trabalho para usar as instâncias.

Depois que o dispositivo chega, você pode começar a gerenciar as AMIs e as instâncias. Gerencie as instâncias de computação em um Snowcone por meio de um endpoint compatível com o Amazon EC2. Esse tipo de endpoint suporta muitos dos comandos e ações da CLI do Amazon EC2 para os SDKs. AWS Você usa a AWS OpsHub for Snow Family ferramenta para gerenciar suas AMIs,

instâncias de computação e AWS serviços. Para ter mais informações, consulte [Usando AWS OpsHub for Snow Family para gerenciar dispositivos](#).

Quando terminar de usar seu dispositivo, devolva-o para AWS. Se o dispositivo foi usado em um trabalho de importação, os dados transferidos pela interface NFS são importados para o Amazon S3. Caso contrário, realizaremos um apagamento completo do dispositivo quando ele for devolvido para a AWS. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Important

- O uso de AMIs criptografadas em dispositivos Snowcone não é suportado.
- Os dados nas instâncias de computação em execução em um Snowcone não são importados para a AWS.

Definição de preço para instâncias de computação no Snowcone

Existem custos adicionais associados ao uso de instâncias de computação. Para obter mais informações, consulte [Preços do AWS Snowcone](#).

Pré-requisitos

Antes de criar o trabalho, lembre-se das seguintes informações:

- Antes de adicionar qualquer AMIs ao seu trabalho, você deve ter uma AMI em seu Conta da AWS trabalho e ela deve ser um tipo de imagem compatível. No momento, as AMIs compatíveis são baseadas nos seguintes sistemas operacionais:

- [Amazon Linux 2](#)

Note

A versão mais recente dessa AMI será fornecida no momento em que seu dispositivo Snow Family estiver sendo preparado para envio AWS. Para determinar a versão dessa AMI no dispositivo quando você a recebe, consulte [Determinando a versão da família Amazon Linux 2 AMI for Snow](#).

- [CentOS 7 \(x86_64\): com atualizações HVM](#)

- [Ubuntu 16.04 LTS - Xenial \(HVM\), Ubuntu 20.04 LTS - Focal ou Ubuntu 22.04 LTS - Jammy](#)

 Note

Ubuntu 16.04 LTS - As imagens Xenial (HVM) não são mais suportadas no AWS Marketplace, mas ainda têm suporte para uso no dispositivo da família Snow por meio do Amazon EC2 VM Import/Export e executadas localmente em AMIs.

É possível obter essas imagens no [AWS Marketplace](#).

Antes de adicionar quaisquer AMI à sua solicitação de criação de trabalho, verifique se você tem uma ou mais AMIs compatíveis em sua Conta da AWS.

- Todas as AMIs devem ser baseadas no Amazon Elastic Block Store (Amazon EBS), com um único volume.
- Se estiver planejando conectar-se a uma instância de computação em execução em um Snowcone, você deverá usar Secure Shell (SSH). Para isso, primeiro você deve adicionar o par de chaves.

Criação de um trabalho com instâncias de computação

Nesta seção, crie o seu primeiro trabalho de instância de computação.

 Important

Lembre-se dos seguintes pontos antes de criar o trabalho:

- Se você for usar uma AMI do AWS Marketplace, verifique se ela tem um código de produto e um código de operação de uso compatíveis. Para ter mais informações, consulte [Verificando códigos de produto e opção de uso para AWS Marketplace AMIs](#).
- Verifique se os valores de vCPU, memória e armazenamento associados à AMI correspondem ao tipo de instância que deseja criar.
- Para usar SSH para conectar-se à instância depois de iniciar a instância no Snowcone, primeiro é necessário executar o procedimento a seguir.
- O uso de AMIs criptografadas ou volumes criptografados do Amazon EBS em AWS Snowcone dispositivos não é suportado.

Verificando códigos de produto e opção de uso para AWS Marketplace AMIs

Antes de iniciar o processo de adicionar uma AMI AWS Marketplace ao seu dispositivo da família Snow, certifique-se de que os códigos de produto e uso da AMI sejam compatíveis com sua Região da AWS.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual iniciar suas instâncias e a partir da qual você criará o trabalho para solicitar o dispositivo da família Snow. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel de navegação, selecione AMIs.
4. Use as opções de filtro e pesquisa para definir o escopo da lista de AMIs exibidas e ver somente as AMIs que correspondem aos seus critérios. Por exemplo, para listar todas as AMIs Linux fornecidas por AWS, escolha Imagens públicas. Em seguida, use as opções de pesquisa para aumentar o escopo da lista de AMIs exibidas.

(Novo console) Escolha a barra de pesquisa e, no menu, escolha Alias do proprietário, depois o operador = e, em seguida, o valor amazon. Escolha a barra de pesquisa novamente para escolher Platform (Plataforma) e, depois, o operador = e o sistema operacional na lista fornecida.

(Console antigo) Escolha a barra Search (Pesquisar) e, no menu, escolha Owner (Proprietário) e o valor Amazon images (Imagens da Amazon). Escolha a barra Search (Pesquisar) novamente para escolher Platform (Plataforma) e o sistema operacional na lista fornecida.

Note

As AMIs de AWS Marketplace incluem aws-marketplace na coluna Fonte.

5. Na coluna ID da AMI, escolha a ID da AMI.
6. No resumo da imagem da AMI, verifique se os códigos do produto são compatíveis com sua região. Para obter mais informações, consulte a tabela abaixo.

Note

O código do produto avyfzznywektkgl5qv5f57ska é suportado em todas as regiões.

Códigos de produto AWS Marketplace AMI compatíveis

| Sistema operacional AMI | Código do produto |
|-------------------------|---------------------------|
| Ubuntu Server 14.04 LTS | b3dl4415quatdndl4qa6kcu45 |
| CentOS 7 (x86_64) | aw0evgkw8e5c1q413zgy5pjce |
| Ubuntu 16.04 LTS | csv6h7oyg29b7epjzg7qdr7no |
| Amazon Linux 2 | avyfzznywektkgl5qv5f57ska |
| Ubuntu 20.04 LTS | a8jyynf4hjutohctm41o2z18m |
| Ubuntu 22.04 LTS | 47xbqns9xujfkkjt189a13aqe |

7. Para todas as regiões, verifique se o código de operação de uso é RunInstances.

Determinando a versão da família Amazon Linux 2 AMI for Snow

Use o procedimento a seguir para determinar a versão do Amazon Linux 2 AMI para a família Snow no dispositivo da família Snow. Instale a versão mais recente do AWS CLI antes de continuar. Para obter mais informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#) no Guia AWS Command Line Interface do Usuário.

- Use o `describe-images` AWS CLI comando para ver a descrição da AMI. A versão está contida na descrição. Forneça o certificado de chave pública da etapa anterior. Para obter mais informações, consulte [describe-images](#) na Referência de Comandos. AWS CLI

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

Exemplo da saída do `describe-images` comando

```
{  
  "Images": [  

```

```

    {
      "CreationDate": "2024-02-12T23:24:45.705Z",
      "ImageId": "s.ami-02ba84cb87224e16e",
      "Public": false,
      "ProductCodes": [
        {
          "ProductCodeId": "avyfzzywektkgl5qv5f57ska",
          "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"
    }
  ]
}

```

Neste exemplo, a versão do Amazon Linux 2 AMI para a família Snow é **2.0.20240131.0**. Ela é encontrada no valor do `Description` nome.

Configurar uma AMI para usar SSH para conectar-se às instâncias de computação iniciadas no dispositivo

Para usar o Secure Shell (SSH) para se conectar às suas instâncias de computação em dispositivos Snowcone, você deve executar o procedimento a seguir. Este procedimento adiciona a chave SSH

à AMI antes de criar o trabalho. Também recomendamos que você use esse procedimento para configurar seus aplicativos na instância que planeja usar como a AMI para o trabalho.

Para colocar uma chave SSH em uma AMI

1. Inicie uma nova instância Nuvem AWS com base na imagem [Amazon Linux 2 for Snow Family, CentOS 7 \(x86_64\) - com atualizações HVM ou Ubuntu 16.04 LTS - Xenial \(HVM\)](#).

Ao iniciar a instância, verifique se o tamanho do armazenamento atribuído à instância é adequado para uso posterior no Snowcone. No console do Amazon EC2, isso é feito na Etapa 4: Adicionar armazenamento. Para obter uma lista dos tamanhos compatíveis para volumes de armazenamento de instância de computação em um Snowcone, consulte [AWS Snowcone cotas](#).

2. Instale e configure os aplicativos que deseja executar no Snowcone e teste para verificar se funcionam conforme o esperado.
3. Faça uma cópia do arquivo PEM/PPK usado para o par de chaves SSH para criar essa instância. Salve esse arquivo no servidor que você planeja usar para se comunicar com o Snowcone. Esse arquivo é necessário para usar SSH para se conectar à instância iniciada no dispositivo, portanto anote o caminho para esse arquivo.
4. Salve a instância como uma AMI. Para obter mais informações, consulte [Criação de uma AMI Linux baseada no Amazon EBS no Guia](#) do usuário do Amazon EC2.
5. Repita esse procedimento para cada uma das instâncias às quais você deseja se conectar usando SSH. Certifique-se de copiar os diferentes pares de chaves SSH e anotar as AMIs às quais eles estão associados.

Criar seu trabalho no console

Sua próxima etapa é criar um trabalho para solicitar um dispositivo Snow Family. O trabalho pode ser de qualquer tipo, incluindo um cluster. Para usar o [Console de Gerenciamento da família AWS Snow](#), siga as instruções em [Conceitos básicos](#).

Criando seu Job no AWS CLI

Você também pode criar o trabalho usando o AWS CLI. Para isso, abra um terminal e execute o comando a seguir, substituindo o texto em vermelho pelos valores reais.

```
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
```

Depois que o dispositivo chegar e você desbloqueá-lo, use o Snowball Edge Client para obter suas credenciais locais. Para ter mais informações, consulte [Como obter as credenciais](#).

Configuração de rede para as instâncias de computação

Depois de iniciar suas instâncias de computação em um dispositivo da Família Snow, você deve fornecer a ele um endereço IP criando uma interface de rede. Os dispositivos da Família Snow suportam dois tipos de interfaces de rede, uma interface de rede virtual e uma interface de rede direta.

Interface de rede virtual (VNI)

Uma interface de rede virtual é a padrão para se conectar a uma instância compatível com o EC2 no dispositivo da Família Snow. É necessário criar uma VNI para cada uma das instâncias compatíveis com o EC2, independentemente de também usar uma interface de rede direta ou não. O tráfego que passa por uma VNI é protegido pelos grupos de segurança configurados. É possível associar VNIs somente à porta de rede física usada para controlar o dispositivo da Família Snow.

Note

A VNI usará a mesma interface física (RJ45, SFP+ ou QSFP) usada para gerenciar o dispositivo da Família Snow. Criar uma VNI em uma interface física diferente daquela usada para gerenciamento de dispositivos pode gerar resultados inesperados.

Interface de rede direta (DNI)

Uma interface de rede direta (DNI) é um atributo de rede avançado que permite casos de uso como fluxos multicast, roteamento transitivo e balanceador de carga. Ao fornecer às instâncias acesso à rede de camada 2 sem conversão ou filtragem intermediária, é possível obter maior flexibilidade na configuração de rede do dispositivo da Família Snow e melhorar a performance da rede. As DNIs são compatíveis com tags de VLAN e a personalização do endereço MAC. O tráfego nas DNIs não é protegido por grupos de segurança.

Os dispositivos Snowcone são compatíveis com oito DNIs por instância compatível com o EC2, com no máximo oito por dispositivo.

Tópicos

- [Pré-requisitos](#)
- [Configurar uma interface de rede virtual \(VNI\)](#)
- [Configurar uma interface de rede direta \(DNI\)](#)

Pré-requisitos

Antes de configurar uma VNI ou uma DNI, verifique se você cumpriu os pré-requisitos a seguir.

1. Verifique se há alimentação para o dispositivo e se uma das interfaces de rede físicas, como a porta RJ45, está conectada a um endereço IP.
2. Obtenha o endereço IP associado à interface de rede física que você está usando no dispositivo da Família Snow.
3. Configure o cliente do Snowball Edge. Para obter mais informações, consulte [Configurando um perfil para o cliente Snowcone](#).
4. Desbloqueie o dispositivo. Recomendamos usar AWS OpsHub for Snow Family para desbloquear seu dispositivo. Para obter instruções, consulte [Desbloquear um dispositivo](#).

Se você quiser usar o comando da CLI, execute o comando a seguir e forneça as informações exibidas na caixa de diálogo.

```
snowballEdge configure
```

Snowball Edge Manifest Path: `manifest.bin`

Unlock Code: `unlock code`

Default Endpoint: `https://device ip`

5. Execute o seguinte comando .

```
snowballEdge unlock-device
```

A atualização da tela do dispositivo indica que ele está desbloqueado.

6. Inicie uma instância compatível com o EC2 no dispositivo. Você associará a VNI a essa instância.
7. Execute o comando `snowballEdge describe-device` para obter a lista de IDs da interface de rede física.
8. Identifique o ID da interface de rede física que deseja usar e anote-o.

Configurar uma interface de rede virtual (VNI)

Depois de identificar o ID da interface de rede física, é possível configurar uma interface de rede virtual (VNI). Utilize o procedimento a seguir para configurar uma VNI. Assegure-se de realizar as tarefas de pré-requisito antes de criar uma VNI.

Criar uma VNI e associar o endereço IP

1. Execute o comando `snowballEdge create-virtual-network-interface`. Os exemplos a seguir mostram a execução desse comando com os dois diferentes métodos de atribuição de endereço IP, DHCP ou STATIC. O método DHCP usa Dynamic Host Configuration Protocol (DHCP — Protocolo de configuração de host dinâmico).

```
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
```

O comando retorna uma estrutura JSON que inclui o endereço IP. Anote esse endereço IP para o `ec2 associate-address` AWS CLI comando posteriormente no processo.

Sempre que precisar desse endereço IP, você pode usar o comando do cliente `snowballEdge describe-virtual-network-interfaces` Snowball Edge ou `aws ec2 describe-addresses` AWS CLI o comando para obtê-lo.

2. Para associar o endereço IP recém-criado com a instância, use o seguinte comando, substituindo o texto em vermelho pelos seus próprios valores:

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

Configurar uma interface de rede direta (DNI)

Note

O recurso de interface de rede direta está disponível em ou após 12 de janeiro de 2021 e está disponível em todos os Regiões da AWS lugares onde os dispositivos da família Snow estão disponíveis.

Pré-requisitos

Antes de configurar uma interface de rede direta (DNI), é necessário realizar as tarefas na seção de pré-requisitos.

1. Realize as tarefas de pré-requisito antes de configurar a DNI. Para obter instruções, consulte [Pré-requisitos](#).
2. Além disso, é necessário iniciar uma instância no dispositivo, criar uma VNI e associá-la à instância. Para obter instruções, consulte [Configurar uma interface de rede virtual \(VNI\)](#).

Note

Se você adicionou rede direta ao seu dispositivo existente executando uma atualização de in-the-field software, deverá reiniciar o dispositivo duas vezes para ativar totalmente o recurso.

Criar uma DNI e associar o endereço IP

1. Crie uma interface de rede direta e anexe-a à instância compatível com o Amazon EC2 executando o comando a seguir. Você precisará do endereço MAC do dispositivo para a próxima etapa.

```
create-direct-network-interface [--endpoint endpoint] [--instance-id instanceId]  
[--mac macAddress]
```

```
id physicalNetworkInterfaceId [--physical-network-interface-  
[--unlock-code unlockCode] [--vlan vlanId]
```

OPTIONS

--endpoint <endpoint> O endpoint para o qual enviar essa solicitação. O endpoint dos dispositivos será um URL que use o esquema `https` seguido por um endereço IP. Por exemplo, se o endereço IP do dispositivo for `123.0.1.2`, o endpoint do dispositivo será `https://123.0.1.2`.

--instance-id <instanceId>: o ID da instância compatível com EC2 ao qual anexar a interface (opcional).

--mac <macAddress>: define o endereço MAC da interface de rede (opcional).

--physical-network-interface-id <physicalNetworkInterfaceId> O ID da interface de rede física na qual criar uma interface de rede virtual. Você pode determinar as interfaces de rede física disponíveis no Snowball Edge usando o comando `describe-device`.

--vlan <vlanId>: defina a VLAN atribuída para a interface (opcional). Quando especificado, todo o tráfego enviado da interface é marcado com o ID de VLAN especificado. O tráfego de entrada é filtrado pelo ID de VLAN especificado e todas as tags de VLAN são removidas antes de serem transmitidas para a instância.

2. Se você não associou a DNI a uma instância na etapa 1, poderá associá-la executando o comando [Atualizando uma interface de rede direta](#).
3. Depois de criar uma DNI e associá-la à instância compatível com o EC2, é necessário fazer duas alterações na configuração na instância compatível com o Amazon EC2.
 - A primeira é garantir que os pacotes destinados à VNI associada à instância compatível com o EC2 sejam enviados por meio de `eth0`.
 - A segunda alteração configura a interface de rede direta para usar DHCP ou IP estático durante a inicialização.

Veja a seguir exemplos de script de shell para Amazon Linux 2 e CentOS Linux que fazem essas alterações na configuração.

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
```

Comandos adicionais

Para ver todos os comandos disponíveis para AWS Snowcone dispositivos, consulte [Usando o cliente Snowball Edge](#).

Conexão à sua instância de computação em um Snowcone usando SSH

Para usar SSH para conectar-se às instâncias de computação em dispositivos do Snowcone, primeiro é necessário fornecer a chave SSH à AMI antes de criar o trabalho. Para obter mais informações sobre tal procedimento, consulte [Configurar uma AMI para usar SSH para conectar-se às instâncias de computação iniciadas no dispositivo](#). Caso não tenha seguido esse procedimento, não será possível usar SSH para conectar-se a suas instâncias.

Para se conectar à instância com SSH

1. Verifique se o dispositivo está ligado, conectado à rede e desbloqueado.
2. Verifique se as configurações de rede estão configuradas para as instâncias de computação. Para ter mais informações, consulte [Configuração de rede para as instâncias de computação](#).
3. Verifique as notas para localizar o par de chaves PEM ou PPK que você usou para essa instância específica. Faça uma cópia desses arquivos em algum lugar em seu computador. Anote o caminho para o arquivo PEM.
4. Conecte-se à instância com SSH, conforme o exemplo de comando a seguir. O endereço IP é o endereço IP da interface de rede virtual (VNIC) configurada em [Configuração de rede para as instâncias de computação](#).

```
ssh -i path/to/PEM/key/file instance-user-name@192.0.2.0
```

Para obter mais informações, consulte [Conectando-se à sua instância Linux usando SSH](#) no Guia do usuário do Amazon EC2.

Comandos do Snowcone Client para instâncias de computação

O Snowball Edge é uma aplicação de terminal independente que você pode executar no servidor local. Ele permite que você execute algumas tarefas administrativas em seu dispositivo Snowcone. Para obter mais informações sobre como usar o Snowball Edge Client, incluindo como iniciar e interromper serviços com ele, consulte [Usando o AWS Snowball Edge cliente](#).

Veja a seguir informações sobre os comandos do Snowball Edge Client específicos para instâncias de computação, incluindo exemplos de uso. Para obter uma lista dos comandos compatíveis com o Amazon EC2 que você pode usar em seu AWS Snowcone dispositivo, consulte. [AWS CLI Comandos compatíveis com Amazon EC2 compatíveis em um Snowcone](#)

Note

Comandos relacionados a clusters não são suportados e retornarão um erro.

Criar uma configuração de inicialização para iniciar automaticamente instâncias compatíveis com o Amazon EC2

Para iniciar automaticamente instâncias computacionais compatíveis com o Amazon EC2 em seu AWS Snowcone dispositivo depois que ele for desbloqueado, você pode criar uma configuração de execução. Para fazer isso, use o comando `snowballEdge create-autostart-configuration`, cujo uso é mostrado a seguir.

Uso

```
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]
```

Atualizar uma configuração de inicialização para iniciar automaticamente instâncias compatíveis com o EC2

Para atualizar uma configuração de execução existente em seu Snowcone, use o comando `snowballEdge update-autostart-configuration`. Veja o seu uso a seguir. Para ativar ou desativar uma configuração de execução, especifique o parâmetro `--enabled`.

Uso

```
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]

```

Excluir uma configuração de inicialização para iniciar automaticamente instâncias compatíveis com o EC2

Para excluir uma configuração de execução que não esteja mais em uso, use o comando `snowballEdge delete-autostart-configuration`. Veja o seu uso a seguir.

Uso

```

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

```

Listar configurações de inicialização para iniciar automaticamente instâncias compatíveis com o EC2

Para listar as configurações de execução criadas em seu Snowcone, use o comando `describe-autostart-configurations`. Veja o seu uso a seguir.

Uso

```

snowballEdge describe-autostart-configurations

```

Criação de uma interface de rede virtual

Para executar uma instância de computação no Snowcone ou iniciar a interface NFS no Snowcone, primeiro você cria uma interface de rede virtual (VNIC). Cada Snowcone possui três interfaces de rede (NICs), os controladores da interface de rede física para o dispositivo. Elas são as portas RJ45 na parte de trás do dispositivo.

Cada VNIC se baseia em uma das físicas e é possível ter qualquer número de VNICs associadas a cada NIC. Para criar uma interface de rede virtual, use o comando `snowballEdge create-virtual-network-interface`.

Note

O parâmetro `--static-ip-address-configuration` é válido apenas ao usar a opção `STATIC` para o parâmetro `--ip-address-assignment`.

Uso

É possível usar esse comando de duas formas: com o cliente do Snowball Edge configurado ou sem ele. O exemplo de uso a seguir mostra o método com o cliente do Snowball Edge configurado.

```
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]
```

O exemplo de uso a seguir mostra o método sem o Snowball Edge configurado.

```
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 Exemplo: criação de VNICs (usando 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"
  }
}
```

```
}
```

Descrição das interfaces de rede virtuais

Para descrever as VNICs criadas anteriormente no dispositivo, use o comando `snowballEdge describe-virtual-network-interfaces`. Veja o seu uso a seguir.

Uso

É possível usar esse comando de duas formas: com o cliente do Snowball Edge configurado ou sem ele. O exemplo de uso a seguir mostra o método com o cliente do Snowball Edge configurado.

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

O exemplo de uso a seguir mostra o método sem o Snowball Edge configurado.

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

Example Exemplo: descrição de 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"
```

```
}
]
```

Atualização de uma interface de rede virtual

Depois de criar uma interface de rede virtual (VNIC), atualize a sua configuração usando o comando `snowballEdge update-virtual-network-interface`. Depois de fornecer o nome de recurso da Amazon (ARN) para uma VNIC específica, forneça valores somente para os elementos que estiver atualizando.

Uso

É possível usar esse comando de duas formas: com o cliente do Snowball Edge configurado ou sem ele. O exemplo de uso a seguir mostra o método com o cliente do Snowball Edge configurado.

```
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]
```

O exemplo de uso a seguir mostra o método sem o Snowball Edge configurado.

```
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 Exemplo: atualização de uma VNIC (usando DHCP)

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

Exclusão de uma interface de rede virtual

Para excluir uma interface de rede virtual, use o comando `snowballEdge delete-virtual-network-interface`.

Uso

É possível usar esse comando de duas formas: com o cliente do Snowball Edge configurado ou sem ele. O exemplo de uso a seguir mostra o método com o cliente do Snowball Edge configurado.

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

O exemplo de uso a seguir mostra o método sem o Snowball Edge configurado.

```
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 Exemplo: exclusão de uma VNIC

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

Usando o serviço de metadados de instância para Snow com instâncias compatíveis com Amazon EC2

O IMDS for Snow fornece Serviço de metadados de instância (IMDS) para instâncias compatíveis com o Amazon EC2 no Snow. Os metadados da instância são categorias de informações sobre instâncias. Inclui categorias como nome do host, eventos e grupos de segurança. Com o IMDS para Snow, você pode usar os metadados da instância para acessar os dados do usuário que você especificou ao executar sua instância compatível com Amazon EC2. Por exemplo, você pode usar o IMDS para Snow para especificar parâmetros para configurar a instância ou incluir esses parâmetros em um script simples. É possível criar AMIs genéricas e usar dados do usuário para modificar os arquivos de configuração fornecidos na hora da inicialização.

Para saber mais sobre metadados da instância e dados do usuário e instâncias compatíveis com o Snow EC2, consulte [Metadados de instâncias suportadas e dados do usuário](#) neste guia.

Important

Embora você só possa acessar os metadados de instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por autenticação ou métodos de criptografia. Qualquer usuário que tenha acesso direto à instância e, potencialmente, qualquer software em execução na instância, pode visualizar seus metadados. Portanto,

você não deve armazenar dados confidenciais, como senhas ou chaves de criptografia de longa duração, como dados de usuário.

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Não oferecemos suporte à recuperação de metadados da instância usando o endereço IPv6 local do link.

Tópicos

- [Versões do IMDS](#)
- [Exemplos de recuperação de metadados de instância usando IMDSv1 e IMDSv2](#)

Versões do IMDS

É possível acessar metadados de instância em uma instância em execução usando o IMDS versão 2 ou o IMDS versão 1:

- Serviço de metadados da instância versão 2 (IMDSv2): um método orientado a sessões
- Serviço de metadados da instância versão 1 (IMDSv1): um método de solicitação/resposta

Dependendo da versão do seu software Snow, é possível usar o IMDSv1, o IMDSv2 ou ambos. Isso também depende do tipo de AMI em execução na instância compatível com EC2. Algumas AMIs, como as que executam o Ubuntu 20.04, exigem o IMDSv2. O serviço de metadados da instância faz distinção entre as solicitações do IMDSv1 e IMDSv2 com base na presença de cabeçalhos PUT ou GET. O IMDSv2 usa esses dois cabeçalhos. O IMDSv1 usa somente o cabeçalho GET.

AWS incentiva o uso do IMDSv2 em vez do IMDSv1 porque o IMDSv2 inclui maior segurança. Para obter mais informações, consulte [Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados da instância do EC2](#).

IMDSv2

O IMDSv2 usa solicitações orientadas a sessão. Com solicitações orientadas a sessões, você cria um token de sessão que define a duração da sessão. A duração da sessão pode variar de um

segundo, no mínimo, a seis horas, no máximo. Durante o período especificado, é possível usar o mesmo token de sessão para solicitações subsequentes. Depois que a duração especificada expira, crie um novo token de sessão para uso em solicitações futuras.

O exemplo a seguir usa um script shell do Linux e o IMDSv2 para recuperar os itens de metadados de nível superior de instância. Esse exemplo:

1. Cria um token de sessão que dura seis horas (21.600 segundos) usando a solicitação PUT.
2. Armazena o cabeçalho do token da sessão em uma variável chamada TOKEN.
3. Solicita os itens de metadados de nível superior usando o token.

É possível executar dois comandos separados ou combiná-los.

Comandos separados

Primeiro, gere um token usando o comando a seguir.

 Note

`X-aws-ec2-metadata-token-ttl-seconds` é um cabeçalho obrigatório. Se esse cabeçalho não for incluído, você receberá um código de erro 400 - Parâmetros ausentes ou inválidos.

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

Em seguida, use o token para gerar itens de metadados de nível superior usando o comando a seguir.

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

Comandos combinados

É possível armazenar o token e combinar os comandos. O exemplo a seguir combina os dois comandos acima e armazena o cabeçalho do token de sessão em uma variável chamada `TOKEN`.

Note

Se houver um erro na criação do token, em vez de um token válido, uma mensagem de erro será armazenada na variável e o comando não funcionará.

Exemplo de comandos combinados

```
[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/
```

Depois de criar um token, é possível reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$TOKEN` no exemplo anterior é reutilizado.

Exemplo de reutilizar um token

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

Quando você usa o IMDSv2 para solicitar os metadados da instância, a solicitação deve incluir essas regras:

1. Use uma solicitação PUT para solicitar a inicialização de uma sessão para o serviço de metadados da instância. A solicitação PUT retorna um token que deve ser incluído em solicitações GET subsequentes para o serviço de metadados da instância. O token é exigido para acessar metadados usando o IMDSv2.
2. Inclua o token em todas as solicitações GET para o serviço de metadados da instância.

- a. O token é uma chave específica da instância. O token não é válido em outras instâncias e será rejeitado se você tentar usá-lo fora da instância na qual foi gerado.
- b. A solicitação PUT deve incluir um cabeçalho que especifique a vida útil (TTL) do token, em segundos, até um máximo de seis horas (21.600 segundos). O token representa uma sessão lógica. O TTL especifica o período de validade do token e, portanto, a duração da sessão.
- c. Depois que o token expira, para continuar a acessar os metadados da instância, crie uma nova sessão usando outra solicitação PUT.
- d. É possível optar por reutilizar um token ou criar um novo token para cada solicitação. Para um número pequeno de solicitações, pode ser mais fácil gerar e usar imediatamente um token a cada vez que você precisar acessar o serviço de metadados da instância. Mas, para obter eficiência, é possível especificar uma duração maior para o token e reutilizá-lo, em vez de precisar escrever uma solicitação PUT toda vez que precisar solicitar metadados da instância. Não há um limite prático para o número de tokens simultâneos, cada um representando sua própria sessão.

Os métodos HTTP GET e HEAD são permitidos em solicitações de metadados de instâncias do IMDSv2. As solicitações PUT serão rejeitadas se contiverem um cabeçalho X-Forwarded-For.

Por padrão, a resposta a solicitações PUT tem um limite de saltos de resposta (vida útil) de 1 no nível de protocolo IP. O IMDS for Snow não tem a capacidade de modificar o limite de salto nas respostas PUT.

IMDSv1

O IMDSv1 usa o modelo de solicitação-resposta. Para solicitar metadados da instância, envie uma solicitação GET para o serviço de metadados da instância.

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

Recuperar metadados da instância

Os metadados da sua instância estão disponíveis na sua instância em execução, então você não precisa usar o console do Amazon EC2 ou AWS CLI o para acessá-los. Isso pode ser útil quando você for elaborar scripts a serem executados a partir de sua instância. Por exemplo, é possível acessar o endereço IP local de sua instância a partir dos metadados da instância para gerenciar uma conexão com uma aplicação externa. Os metadados da instância são divididos em categorias. Para

obter uma descrição de cada categoria de metadados de instância, consulte [metadados de instância compatíveis e dados do usuário](#) neste guia.

Para visualizar todas as categorias de metadados da instância de dentro de uma instância em execução, use o seguinte URI:

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

Os endereços IP são endereços locais de link e são válidos apenas a partir da instância. Para obter mais informações, consulte [Endereço de link local](#) na Wikipedia.

Respostas e mensagens de erro

Todos os metadados de instância são retornados como texto (tipo de conteúdo HTTP `text/plain`).

Uma solicitação para um atributo de metadados específico retorna o valor apropriado, ou um código de erro de HTTP 404 - Not Found se o atributo não estiver disponível.

Uma solicitação de um recurso de metadados geral (o URI termina com `/`) retorna uma lista de atributos disponíveis, ou um código de erro de HTTP 404 - Not Found se não houver esse atributo. Os itens da lista estão em linhas separadas que são delimitadas por caracteres de alimentação de linha (ASCII 10).

Para solicitações feitas usando o IMDSv1, os seguintes códigos de erro HTTP podem ser retornados:

- 400 - parâmetros ausentes ou inválidos: a solicitação PUT não é válida.
- 401 - não autorizado: a solicitação GET usa um token inválido. A ação recomendada é gerar um novo token.
- 403 - proibido: a solicitação não é permitida ou o serviço de metadados de instância está desativado.

Exemplos de recuperação de metadados de instância usando IMDSv1 e IMDSv2

Os exemplos a seguir fornecem comandos que é possível usar em uma instância do Linux.

Exemplo de obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Cada versão indica uma compilação de metadados de instância quando novas categorias de metadados de instância foram

lançadas. As versões anteriores estarão disponíveis caso você tenha scripts que contam com a estrutura e as informações presentes em uma versão anterior.

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
```

Exemplo de obter itens de metadados de nível superior

Este exemplo obtém itens de metadados de nível superior. Para obter informações sobre itens de metadados de nível superior, consulte [Metadados de instâncias compatíveis e dados do usuário](#) neste guia.

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
```

Exemplo de obter valores de metadados de nível superior

Os exemplos a seguir obtêm os valores de alguns dos itens de metadados de nível superior que foram obtidos no exemplo anterior. As solicitações do IMDSv2 usam o token armazenado que foi criado no comando do exemplo anterior, supondo-se que ele não expirou.

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
```

Usar o endpoint compatível com o Amazon EC2

A seguir, é possível encontrar uma visão geral do endpoint compatível com o Amazon Elastic Compute Cloud (Amazon EC2). Com esse endpoint, é possível gerenciar as imagens de máquina da Amazon (AMIs) e instâncias de computação programaticamente usando operações da API compatíveis com o Amazon EC2.

Tópicos

- [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#)
- [Atributos incompatíveis do Amazon EC2 para Snowcone](#)
- [AWS CLI Comandos compatíveis com Amazon EC2 compatíveis em um Snowcone](#)
- [Operações da API do Amazon EC2 com suporte](#)

Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI

Ao usar o AWS CLI para emitir um comando para o AWS Snowcone dispositivo, você pode especificar que o endpoint é compatível com o Amazon EC2. Você tem a opção de usar o endpoint HTTPS ou um endpoint HTTP desprotegido, como mostrado a seguir.

Endpoint HTTPS protegido

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

Endpoint HTTP desprotegido

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

Se você usar o endpoint HTTPS de 8243, os dados em trânsito são criptografados. Essa criptografia é garantida com um certificado gerado pelo Snowcone sempre que for desbloqueado. Depois de receber o certificado, você poderá salvá-lo em um arquivo local `ca-bundle.pem`. Então você poderá configurar sua AWS CLI para incluir o caminho do seu certificado, conforme descrito a seguir.

Para associar o certificado ao endpoint compatível com o Amazon EC2

1. Conecte o Snowcone à alimentação e à rede e, depois, ligue-o.
2. Depois que o dispositivo terminar de desbloquear, anote o endereço IP dele na sua rede local.
3. Em um terminal na sua rede, verifique se é possível fazer teste de ping no dispositivo Snowcone.
4. Execute o comando `snowballEdge get-certificate` no seu terminal. Para obter mais informações sobre esse comando, consulte [Obter certificado para transferência de dados](#).
5. Salve a saída do comando `snowballEdge get-certificate` em um arquivo, por exemplo, `ca-bundle.pem`.
6. Execute o seguinte comando no seu terminal.

```
aws configure set profile.snowcone.ca_bundle /path/to/ca-bundle.pem
```

Depois de concluir o procedimento, execute comandos da CLI com essas credenciais locais, com o certificado e com o endpoint especificado.

Atributos incompatíveis do Amazon EC2 para Snowcone

Usando o endpoint compatível com o Amazon EC2, é possível gerenciar de forma programática as AMIs e as instâncias de computação em um Snowcone com operações da API compatível com o Amazon EC2. No entanto, nem todos os atributos e as operações da API são compatíveis para o uso com um dispositivo Snowcone.

Todos os atributos ou ações que não estão explicitamente listados como compatíveis nesse guia são incompatíveis. Por exemplo, as seguintes ações do Amazon EC2 não são compatíveis com o uso do Snowcone:

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

AWS CLI Comandos compatíveis com Amazon EC2 compatíveis em um Snowcone

É possível gerenciar as instâncias de computação em um dispositivo da Família Snow por meio de um endpoint compatível com o Amazon EC2. Esse tipo de endpoint suporta muitos dos comandos e ações da CLI do Amazon EC2 dos SDKs. AWS Para obter informações sobre como instalar e

configurar o AWS CLI, incluindo especificar para quem Regiões da AWS você deseja fazer AWS CLI chamadas, consulte o [Guia do AWS Command Line Interface usuário](#).

Lista de comandos do AWS CLI compatíveis com o Amazon EC2 em um Snowcone

A seguir, você encontrará uma descrição do subconjunto de AWS CLI comandos e opções do Amazon EC2 que são compatíveis com dispositivos Snowcone. Se um comando ou opção não estiver listado abaixo, não é compatível. É possível declarar algumas opções não compatíveis junto com um comando. No entanto, elas são ignoradas.

- [associate-address](#) – associa um endereço IP virtual a uma instância para o uso em uma das três interfaces de rede físicas no dispositivo:
 - `--instance-id` – o ID de uma única instância sbe.
 - `--public-ip` – o endereço IP virtual que deseja usar para acessar a instância.
- [attach-volume](#) — anexa um volume do Amazon EBS a uma instância parada ou em execução no AWS Snowcone seu dispositivo e o expõe à instância com o nome do dispositivo especificado.
 - `--device value`: o nome do dispositivo.
 - `-instance-id`: o ID de uma instância do Amazon EC2 de destino.
 - `-volume-id value`: o ID do volume do EBS.
- [authorize-security-group-egress](#)— Adiciona uma ou mais regras de saída a um grupo de segurança para uso com um dispositivo Snowcone. Especificamente, essa ação permite que instâncias enviem tráfego para um ou mais intervalos de endereços IPv4 CIDR de destino. Para ter mais informações, consulte [Grupos de segurança em dispositivos Snow](#).
 - `--group-id value`: o ID do grupo de segurança
 - `[-ip-permissions value]`: um ou mais conjuntos de permissões de IP.
- [authorize-security-group-ingress](#)— Adiciona uma ou mais regras de entrada a um grupo de segurança. Ao chamar `authorize-security-group-ingress`, você deve especificar um valor para `group-name` ou para `group-id`.
 - `[--group-name value]`: o nome do grupo de segurança.
 - `[--group-id value]`: o ID do grupo de segurança
 - `[-ip-permissions value]`: um ou mais conjuntos de permissões de IP.
 - `[-protocol value]` o protocolo IP. Os valores possíveis são `tcp`, `udp` e `icmp`. O argumento `--port` é obrigatório, a menos que o valor "all protocols (todos os protocolos)" seja especificado (-1).

- [--port value]: para TCP ou UDP, o intervalo de portas a ser permitido. Esse valor pode ser um único número inteiro ou um intervalo (mínimo - máximo).

Para ICMP, um único número inteiro ou um intervalo (type-code) em que type representa o número do tipo ICMP e code representa o número do código ICMP. Um valor de -1 indica todos os códigos ICMP para todos os tipos ICMP. Um valor de -1 para type indica todos os códigos ICMP para o tipo ICMP especificado.

- [--cidr value]: o intervalo de IPs CIDR.
- [create-launch-template](#)— Cria um modelo de lançamento. Um modelo de execução contém os parâmetros para executar uma instância. Ao executar uma instância usando RunInstances, é possível especificar um modelo de execução em vez de fornecer os parâmetros de execução na solicitação. Você pode criar até 100 modelos por AWS Snowcone dispositivo.
 - -- launch-template-name string — Um nome para o modelo de lançamento.
 - -- launch-template-data structure — As informações do modelo de lançamento. Há suporte para os seguintes atributos:
 - ImageId
 - InstanceType
 - SecurityGroupIds
 - TagSpecifications
 - UserData

Sintaxe do JSON:

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

```

    {
      "Key": "Stack",
      "Value": "Gamma"
    }
  ]
}
]
}

```

- `[--version-description string]`: uma descrição para a primeira versão do modelo de execução.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [create-launch-template-version](#)— Cria uma nova versão para um modelo de lançamento. Você pode especificar uma versão existente de um modelo de execução para servir como base para a nova versão. As versões de modelo de execução são numeradas na ordem em que são criadas. Não é possível especificar, alterar ou substituir a numeração das versões do modelo de execução. Você pode criar até 100 versões de cada modelo de execução.

Especifique na solicitação o ID ou o nome do modelo de execução.

- `-- launch-template-id string` — O ID do modelo de lançamento.
- `-- launch-template-name string` — Um nome para o modelo de lançamento.
- `-- launch-template-data structure` — As informações do modelo de lançamento. Há suporte para os seguintes atributos:
 - ImageId
 - InstanceType
 - SecurityGroupIds
 - TagSpecifications
 - UserData

Sintaxe do JSON:

```

'{'
  "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]`: o número de versão do modelo de execução que servirá como base para a nova versão. A nova versão herda os mesmos parâmetros de execução da versão de origem, exceto os parâmetros especificados em `launch-template-data`.
- `[-version-description string]`: uma descrição para a primeira versão do modelo de execução.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [create-tags](#) – adiciona ou substitui uma ou mais tags do atributo especificado. Cada recurso pode ter um máximo de 50 tags. Cada tag consiste em uma chave e um valor opcional. As chaves de tag devem ser exclusivas para um recurso. Há suporte para os seguintes atributos:
 - AMI
 - Instância
 - Modelo de execução
 - Grupo de segurança
- [create-security-group](#) — Cria um grupo de segurança em seu dispositivo Snowcone. Você pode criar até 50 grupos de segurança. Ao criar um grupo de segurança, você especifica um nome amigável de sua escolha:
 - `--group-name value`: o nome do grupo de segurança.
 - `--description value`: uma descrição do grupo de segurança. Isso é apenas informativo. Esse valor pode ter até 255 caracteres.
- [create-volume](#) — Cria um volume do Amazon EBS que pode ser conectado a uma instância no seu dispositivo. AWS Snowcone
 - `[-sizevalue]` — O tamanho do volume de entrada GiBs, que pode ser de 1 GiB a 1 TB (GiBs1000).
 - `[-snapshot-id value]`: o ID do snapshot a partir do qual criar o volume.
 - `[-volume-type value]`: o tipo de volume. Se nenhum valor for especificado, o padrão será `sbg1`. Os valores possíveis incluem o seguinte:
 - `sbg1` para volumes magnéticos
 - `sbp1` para volumes SSD
 - `[-tag-specification value]`: uma lista de tags a serem aplicadas ao volume durante a criação.

- [delete-launch-template](#)— Exclui um modelo de lançamento. A exclusão de um modelo de execução excluirá todas as suas versões.

Especifique na solicitação o ID ou o nome do modelo de execução.

- `-- launch-template-id string` — O ID do modelo de lançamento.
- `-- launch-template-name string` — Um nome para o modelo de lançamento.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [delete-launch-template-version](#)— Exclui uma ou mais versões de um modelo de lançamento. Não é possível excluir a versão padrão de um modelo de execução; primeiro é necessário atribuir outra versão como padrão. Se a versão padrão for a única versão para o modelo de execução, exclua todo o modelo de execução usando o comando `delete-launch-template`.

Especifique na solicitação o ID ou o nome do modelo de execução.

- `-- launch-template-id string` — O ID do modelo de lançamento.
- `-- launch-template-name string` — Um nome para o modelo de lançamento.
- `--versions (list) "string" "string"`: os números de versão de uma ou mais versões do modelo de execução a serem excluídas.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2.
- [delete-security-group](#)— Exclui um grupo de segurança.

Se você tentar excluir um grupo de segurança associado a uma instância ou referenciado por outro grupo de segurança, ocorrerá uma falha na operação com `DependencyViolation`.

- `--group-name value`: o nome do grupo de segurança.
- `--description value`: uma descrição do grupo de segurança. Isso é apenas informativo. Esse valor pode ter até 255 caracteres.
- [delete-tags](#): exclui o conjunto de tags especificado do atributo especificado (AMI, instância de computação, modelo de execução ou grupo de segurança).
- [delete-volume](#): exclui o volume do Amazon EBS especificado. O volume deve estar no estado `available` (não anexado a uma instância).
- `--volume-id value`: o ID do volume.

- [describe-address](#): descreve um ou mais endereços IP virtuais associados ao mesmo número de instâncias sbe no dispositivo.
 - `--public-ips` – um ou mais endereços IP virtuais associados às instâncias.
- [describe-images](#): descreve uma ou mais das imagens (AMIs) disponíveis para você. As imagens disponíveis são adicionadas ao dispositivo Snowcone durante a criação do trabalho.
 - `--image-id`: o ID da AMI de Snowcone da AMI.
- [describe-instance-attribute](#)— Descreve o atributo especificado da instância especificada. Você só pode pesquisar um atributo de cada vez. Há suporte para os seguintes atributos:
 - `instanceInitiatedShutdownBehavior`
 - `instanceType`
 - `userData`
- [describe-instances](#) – descreve uma ou mais instâncias. A resposta retorna todos os grupos de segurança atribuídos às instâncias.
 - `--instance-ids` – os IDs de uma ou mais instâncias sbe interrompidas no dispositivo.
 - `--page-size`: o tamanho de cada página para obtenção na chamada. Esse valor não afeta o número de itens retornados na saída do comando. Definir um tamanho de página menor resulta em mais chamadas para o dispositivo, recuperando menos itens em cada chamada. Fazer isso pode ajudar a evitar que as chamadas atinjam o tempo limite.
 - `--max-items`: o número total de itens para retornar na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente.
 - `--starting-token`: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente.
- [describe-launch-templates](#)— Descreve um ou mais modelos de lançamento. O comando `describe-launch-templates` é uma operação paginada. Você pode realizar várias chamadas para recuperar todo o conjunto de dados de resultados.

Especifique na solicitação os IDs ou os nomes de modelo de execução.

- `-- launch-template-ids (list) "string" "string"` — Uma lista de IDs dos modelos de lançamento.
- `-- launch-template-names (list) "string" "string"` — Uma lista de nomes para os modelos de lançamento.

- `--page-size`: o tamanho de cada página para obtenção na chamada. Esse valor não afeta o número de itens retornados na saída do comando. Definir um tamanho de página menor resulta em mais chamadas para o dispositivo, recuperando menos itens em cada chamada. Fazer isso pode ajudar a evitar que as chamadas atinjam o tempo limite.
- `--max-items`: o número total de itens para retornar na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente.
- `--starting-token`: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [describe-launch-template-versions](#) — Descreve uma ou mais versões de um modelo de lançamento especificado. Você pode descrever todas as versões, versões individuais ou um intervalo de versões. O comando `describe-launch-template-versions` é uma operação paginada. Você pode realizar várias chamadas para recuperar todo o conjunto de dados de resultados.

Especifique na solicitação os IDs ou os nomes de modelo de execução.

- `-- launch-template-id string` — O ID do modelo de lançamento.
- `-- launch-template-name string` — Um nome para o modelo de lançamento.
- `[--versions (list) "string" "string"]`: os números de versão de uma ou mais versões do modelo de inicialização a serem excluídas.
- `[--min-version string]`: o número da versão a partir da qual serão descritas versões do modelo de inicialização.
- `[--max-version string]`: o número da versão até a qual serão descritas versões do modelo de inicialização.
- `--page-size`: o tamanho de cada página para obtenção na chamada. Esse valor não afeta o número de itens retornados na saída do comando. Definir um tamanho de página menor resulta em mais chamadas para o dispositivo, recuperando menos itens em cada chamada. Fazer isso pode ajudar a evitar que as chamadas atinjam o tempo limite.
- `--max-items`: o número total de itens para retornar na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do

comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente.

- `--starting-token`: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente.
- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [describe-security-groups](#)— Descreve um ou mais dos seus grupos de segurança.

O comando `describe-security-groups` é uma operação paginada. É possível emitir várias chamadas da API para recuperar todo o conjunto de dados de resultados.

- `[--group-name value]`: o nome do grupo de segurança.
- `[--group-id value]`: o ID do grupo de segurança.
- `[--page-size value]` — O tamanho de cada página para entrar na chamada de serviço. AWS Esse tamanho não afeta o número de itens retornados na saída do comando. A configuração de um tamanho menor de página ocasiona mais chamadas ao serviço da AWS recuperando menos itens em cada chamada. Essa abordagem pode ajudar a evitar que as chamadas AWS de serviço atinjam o tempo limite. Para obter exemplos de uso, consulte [Pagination](#) no Guia do usuário da AWS Command Line Interface .
- `[--max-items value]`: o número total de itens a serem exibidos na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente. Não use o elemento de resposta `NextToken` diretamente fora da AWS CLI. Para obter exemplos de uso, consulte [Pagination](#) no Guia do usuário da AWS Command Line Interface .
- `[--starting-token value]`: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente. Para obter exemplos de uso, consulte [Pagination](#) no Guia do usuário da AWS Command Line Interface .
- [describe-tags](#): descreve uma ou mais das tags para o atributo especificado (`image`, `instance` ou grupo de segurança). Com esse comando, há suporte para os seguintes filtros:
 - `launch-template`
 - `resource-id`
 - `resource-type` – `image` ou `instance`
 - `chave`

- `valor`
- [describe-volumes](#): descreve os volumes do Amazon EBS especificados.
 - `[--max-items value]`: o número total de itens a serem exibidos na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente.
 - `[--starting-token value]`: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente.
 - `[--volume-ids value]`: um ou mais IDs de volume.
- [detach-volume](#): desanexa um volume do Amazon EBS de uma instância interrompida ou em execução.
 - `[--device value]`: o nome do dispositivo.
 - `[--instance-id]`: o ID de uma instância do Amazon EC2 de destino.
 - `--volume-id value`: o ID do volume.
- [disassociate-address](#) – desassocia um endereço IP virtual da instância com a qual está associado.
 - `--public-ip`: o endereço IP virtual que você deseja dissociar da instância.
- [get-launch-template-data](#)— Recupera os dados de configuração da instância especificada. Use esses dados para criar um modelo de execução.
 - `--instance-id` – o ID de uma única instância sbe.
 - `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [modify-launch-template](#)— Modifica um modelo de lançamento. Você pode especificar qual versão do modelo de execução será definida como versão padrão. Ao executar uma instância sem especificar uma versão do modelo de execução, a versão padrão do modelo de execução será aplicada.

Especifique na solicitação o ID ou o nome do modelo de execução.

- `-- launch-template-id string` — O ID do modelo de lançamento.
- `-- launch-template-name string` — Um nome para o modelo de lançamento.
- `--default-version string`: o número da versão do modelo de inicialização a ser definida como versão padrão.

- `--endpoint snowballEndpoint`: um valor que permite gerenciar suas instâncias de computação de forma programática usando operações da API do Amazon EC2. Para ter mais informações, consulte [Especificando o endpoint compatível com Amazon EC2 como o endpoint AWS CLI](#).
- [modify-instance-attribute](#)— Modifica um atributo da instância especificada. Há suporte para os seguintes atributos:
 - `instanceInitiatedShutdownBehavior`
 - `userData`
- [revoke-security-group-egress](#)— Remove uma ou mais regras de saída de um grupo de segurança:
 - `[--group-id value]`: o ID do grupo de segurança
 - `[--ip-permissions value]`: um ou mais conjuntos de permissões de IP.
- [revoke-security-group-ingress](#)— Revoga uma ou mais regras de entrada em um grupo de segurança. Ao chamar `revoke-security-group-ingress`, você deve especificar um valor para `group-name` ou `paragroup-id`.
 - `[--group-name value]`: o nome do grupo de segurança.
 - `[--group-id value]`: o ID do grupo de segurança.
 - `[--ip-permissions value]`: um ou mais conjuntos de permissões de IP.
 - `[--protocol value]` o protocolo IP. Os valores possíveis são `tcp`, `udp` e `icmp`. O argumento `--port` é obrigatório, a menos que o valor "all protocols (todos os protocolos)" seja especificado (-1).
 - `[--port value]`: para TCP ou UDP, o intervalo de portas a ser permitido. Um único número inteiro ou um intervalo (mínimo - máximo).

Para ICMP, um único número inteiro ou um intervalo (`type-code`) em que `type` representa o número do tipo ICMP e `code` representa o número do código ICMP. Um valor de -1 indica todos os códigos ICMP para todos os tipos ICMP. Um valor de -1 para `type` indica todos os códigos ICMP para o tipo ICMP especificado.
- `[--cidr value]`: o intervalo de IPs CIDR.
- [run-instances](#): inicia um número de instâncias de computação usando um ID de AMI do Snowcone para uma AMI.

Note

Pode levar até uma hora e meia para que uma instância de computação seja iniciada em um dispositivo Snowcone, dependendo do tamanho e do tipo de instância.

- `[-- block-device-mappings (list)]` — As entradas de mapeamento do dispositivo de bloqueio. Os parâmetros `DeleteOnTermination`, `VolumeSize`, e `VolumeType` têm suporte. Os volumes de devem ser do tipo `sbp1`.

A sintaxe JSON para esse comando é conforme a seguir.

```
{
  "DeviceName": "/dev/sdh",
  "Ebs":
  {
    "DeleteOnTermination": true|false,
    "VolumeSize": 100,
    "VolumeType": "sbp1"|"sbg1"
  }
}
```

- `--count`: número de instâncias a serem iniciadas. Se um único número for fornecido, é considerado como mínimo para iniciar (o padrão é 1). Se um intervalo for fornecido na forma `min:max`, o primeiro número será interpretado como o número mínimo de instâncias a serem iniciadas e o segundo será interpretado como o número máximo de instâncias a serem iniciadas.
- `--image-id`: o ID da AMI do Snowcone da AMI, que pode ser obtido chamando `describe-images`. É necessária uma AMI para executar uma instância.
- `-- InstanceInitiatedShutdownBehavior` — Por padrão, quando você inicia um desligamento da sua instância (usando um comando como `shutdown` ou `poweroff`), a instância é interrompida. É possível alterar esse comportamento para que, em vez disso, seja encerrada. Os parâmetros `stop` e `terminate` são compatíveis. O padrão é `stop`. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância](#) no Manual do usuário para instâncias do Linux do Amazon EC2.
- `--instance-type` – o tipo de instância sbe.
- `--launch-template structure`: o modelo de inicialização a ser usado para iniciar as instâncias. Os parâmetros especificados no comando `run-instances` substituem os mesmos parâmetros

no modelo de execução. Você pode especificar o nome ou o ID de um modelo de execução, mas não ambos.

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

- `-- security-group-ids` — Um ou mais IDs de grupos de segurança. Você pode criar um grupo de segurança usando [CreateSecurityGroup](#). Se nenhum valor for fornecido, o ID do grupo de segurança padrão será atribuído às instâncias criadas.
- `--tag-specifications`: as tags a serem aplicadas aos recursos durante a execução. Só é possível marcar instâncias na execução. As tags especificadas são aplicadas a todas as instâncias que são criadas durante a execução. Para marcar um recurso após sua criação, use `create-tags`.
- `--user-data`: os dados de usuário que são disponibilizados para a instância. Se você estiver usando o AWS CLI, a codificação base64 será executada para você e você poderá carregar o texto de um arquivo. Caso contrário, você deve fornecer o texto codificado em base64.
- [start-instances](#): inicia uma instância sbe interrompida anteriormente. Todos os recursos anexados à instância persistem durante inícios e interrupções, mas são apagados se a instância for encerrada.
 - `--instance-ids` – os IDs de uma ou mais instâncias sbe interrompidas no dispositivo.
- [stop-instances](#): interrompe uma instância sbe em execução. Todos os recursos anexados à instância persistem durante inícios e interrupções, mas são apagados se a instância for encerrada.
 - `--instance-ids` – os IDs de uma ou mais instâncias sbe a serem interrompidas no dispositivo.
- [terminate-instances](#): desliga uma ou mais instâncias. Essa operação é idempotente. Se você encerrar uma instância mais de uma vez, cada chamada será bem-sucedida. Todos os atributos anexados à instância persistem aos inícios e interrupções, mas os dados são apagados se a instância for encerrada.

Note

Por padrão, ao usar um comando como `shutdown` ou `poweroff` para iniciar um desligamento em sua instância, a instância será interrompida. No entanto, é possível usar o atributo `InstanceInitiatedShutdownBehavior` para alterar o comportamento para que esses comandos encerrem a instância. Para obter mais informações, consulte

[Alterar o comportamento de desligamento iniciado da instância](#) no Manual do usuário para instâncias do Linux do Amazon EC2.

- `--instance-ids`: os IDs de uma ou mais instâncias sbe a serem encerradas no dispositivo. Todos os dados associados armazenados para essas instâncias serão perdidos.

Operações da API do Amazon EC2 com suporte

A seguir, você encontrará operações de API do Amazon EC2 que podem ser usadas com um dispositivo Snowcone, com links para suas descrições na Referência de API do Amazon EC2. As chamadas de API do Amazon EC2 exigem assinatura com o Signature Version 4 (SigV4). Se você estiver usando o AWS CLI ou um AWS SDK para fazer essas chamadas de API, a assinatura SigV4 é feita para você. Caso contrário, você precisará implementar sua própria solução de assinatura do SigV4.

- [AssociateAddress](#)— Associa um endereço IP elástico a uma instância ou interface de rede.
- [AttachVolume](#)— Os seguintes parâmetros de solicitação são suportados:
 - Device
 - InstanceId
 - VolumeId
- [AuthorizeSecurityGroupEgress](#)— Adiciona uma ou mais regras de saída a um grupo de segurança para uso com um dispositivo Snowcone. Especificamente, essa ação permite que instâncias enviem tráfego para um ou mais intervalos de endereços IPv4 CIDR de destino.
- [AuthorizeSecurityGroupIngress](#)— Adiciona uma ou mais regras de entrada a um grupo de segurança. Ao chamar `AuthorizeSecurityGroupIngress`, você deve especificar um valor para `GroupName` ou `GroupId`.
- [CreateVolume](#)— Os seguintes parâmetros de solicitação são suportados:
 - SnapshotId
 - Size
 - VolumeType
 - TagSpecification.N
- [CreateLaunchTemplate](#)— Os seguintes parâmetros de solicitação são suportados:
 - ImageId

- InstanceType
- SecurityGroupIds
- TagSpecifications
- UserData
- [CreateLaunchTemplateVersion](#)
- [CreateTags](#)— Os seguintes parâmetros de solicitação são suportados:
 - AMI
 - Instance
 - Launch template
 - Security group
- [CreateSecurityGroup](#)— Cria um grupo de segurança no seu Snowcone. Você pode criar até 50 grupos de segurança. Ao criar um grupo de segurança, você especifica um nome amigável de sua escolha.
- [DeleteLaunchTemplate](#)
- [DeleteLaunchTemplateVersions](#)
- [DeleteSecurityGroup](#)— Exclui um grupo de segurança. Se você tentar excluir um grupo de segurança associado a uma instância ou referenciado por outro grupo de segurança, ocorrerá uma falha na operação com `DependencyViolation`.
- [DeleteTags](#)— Exclui o conjunto especificado de tags do conjunto especificado de recursos.
- [DeleteVolume](#)— Os seguintes parâmetros de solicitação são suportados:
 - VolumeId
- [DescribeAddresses](#)
- [DescribeImages](#)
- [DescribeInstanceAttribute](#)— Os seguintes atributos são suportados:
 - instanceType
 - userData
- [DescribeLaunchTemplates](#)
- [DescribeLaunchTemplateVersions](#)
- [DescribeInstances](#)

- [DescribeSecurityGroups](#)— Descreve um ou mais dos seus grupos de segurança. `DescribeSecurityGroups` é uma operação paginada. É possível emitir várias chamadas da API para recuperar todo o conjunto de dados de resultados.
- [DescribeTags](#)— Com esse comando, os seguintes filtros são suportados:
 - `resource-id`
 - `resource-type`: apenas AMI ou instância de computação
 - `key`
 - `value`
- [DescribeVolume](#)— Os seguintes parâmetros de solicitação são suportados:
 - `MaxResults`
 - `NextToken`
 - `VolumeId.N`
- [DetachVolume](#)— Os seguintes parâmetros de solicitação são suportados:
 - `Device`
 - `InstanceId`
 - `VolumeId`
- [DisassociateAddress](#)
- [GetLaunchTemplateData](#)
- [ModifyLaunchTemplate](#)
- [ModifyInstanceAttribute](#)— Somente o `userData` atributo é suportado.
- [RevokeSecurityGroupEgress](#)— Remove uma ou mais regras de saída de um grupo de segurança.
- [RevokeSecurityGroupIngress](#)— Revoga uma ou mais regras de entrada em um grupo de segurança. Ao chamar `RevokeSecurityGroupIngress`, você deve especificar um valor para `group-name` ou `group-id`.
- [RunInstances](#) –

 Note

Pode levar até uma hora e meia para que uma instância de computação seja iniciada em um Snowcone, dependendo do tamanho e do tipo de instância.

- [StartInstances](#)

- [StopInstances](#)— Os recursos associados a uma instância interrompida persistem. Você pode encerrar a instância para liberar esses atributos. No entanto, todos os dados associados serão excluídos.
- [TerminateInstances](#)

Início automático de instâncias compatíveis com o Amazon EC2 com modelos de execução

Você pode iniciar automaticamente suas instâncias compatíveis com o Amazon EC2 em seu AWS Snowcone dispositivo usando modelos de execução e comandos de configuração de inicialização do cliente Snowball Edge. Se uma instância sair, o início automático a iniciará, mas se você excluir a instância ou atualizar a configuração de inicialização automática da instância, a inicialização automática iniciará uma nova instância.

Um modelo de execução contém as informações de configuração necessárias para criar uma instância compatível com o Amazon EC2 em seu Snowcone. Use o modelo de execução para armazenar os parâmetros de execução de modo que não seja necessário especificá-los toda vez que iniciar uma instância compatível com o EC2 no Snowcone.

Ao usar configurações de início automático em seu Snowcone, configure os parâmetros com os quais deseja que sua instância compatível com o Amazon EC2 inicie. Assim que o Snowcone estiver configurado, ao reinicializar e desbloqueá-lo, ele usa a configuração de início automático para executar uma instância com os parâmetros especificados. Se uma instância executada usando uma configuração de início automático for interrompida, a instância inicia a execução ao desbloquear o dispositivo.

Note

Após a primeira definição de uma configuração de início automático, reinicie o dispositivo para executá-la. Todas as inicializações subsequentes da instância (após reinicializações planejadas ou não planejadas) acontecem automaticamente após o desbloqueio AWS Snowcone do dispositivo.

Um modelo de execução pode especificar o ID da imagem de máquina da Amazon (AMI), o tipo de instância, os dados do usuário, os grupos de segurança e as tags para uma instância compatível com o Amazon EC2 ao executar essa instância.

Para executar automaticamente instâncias compatíveis com o EC2 em seu Snowcone, siga as seguintes etapas:

1. Ao solicitar seu AWS Snowcone dispositivo, crie um trabalho para solicitar um dispositivo da família Snow com instâncias computacionais. Para ter mais informações, consulte [Criação de um trabalho com instâncias de computação](#).
2. Depois de receber o Snowcone, desbloqueie-o.
3. Use o comando `aws ec2 create-launch-template` da API do EC2 para criar um modelo de execução. Para ter mais informações, consulte [Lista de comandos do AWS CLI compatíveis com o Amazon EC2 em um Snowcone](#).

 Note

O endpoint do Amazon EC2 é o endpoint do dispositivo.

4. Use o comando `snowballEdge create-autostart-configuration` do Snowball Edge Client para vincular o modelo de execução compatível com o EC2 à configuração de rede. Para ter mais informações, consulte [Criar uma configuração de inicialização para iniciar automaticamente instâncias compatíveis com o Amazon EC2](#).
5. Reinicie e desbloqueie seu AWS Snowcone dispositivo. As instâncias compatíveis com o EC2 serão iniciadas automaticamente usando os atributos especificados no modelo de execução e no comando `create-autostart-configuration` do cliente Snowcone.

Para visualizar o status das instâncias em execução, use o comando `describe-autostart-configurations` da API do EC2.

 Note

Não há console ou API de gerenciamento de tarefas para AWS Snowball dar suporte ao lançamento de modelos. Use comandos da CLI do EC2 e do Snowball Edge Client para iniciar automaticamente instâncias compatíveis com o EC2 em seu dispositivo AWS Snowcone.

Usar o Block Storage com suas instâncias compatíveis com o Amazon EC2

O Block Storage no Snowcone permite que você adicione ou remova o armazenamento de blocos com base nas necessidades de seus aplicativos. Os volumes que estão anexados a uma instância compatível com o Amazon EC2 são expostos como volumes de armazenamento que persistem independentemente da vida útil da instância. É possível gerenciar o armazenamento em blocos usando a API conhecida do Amazon EBS.

Alguns comandos do Amazon EBS têm suporte usando o endpoint do EC2. Os comandos com suporte incluem `attach-volume`, `create-volume`, `delete-volume`, `detach-volume`, e `describe-volumes`. Para obter mais informações sobre esses comandos, consulte [Lista de comandos do AWS CLI compatíveis com o Amazon EC2 em um Snowcone](#).

Important

Desmonte todos os sistemas de arquivos do dispositivo no sistema operacional antes de desanexar o volume. Não fazer isso pode resultar em perda de dados.

A seguir, você encontra cotas e diferenças de volume do Amazon EBS entre os volumes do Amazon EBS no dispositivo AWS Snowcone e volumes do Amazon EBS na nuvem:

- Os volumes do Amazon EBS só estão disponíveis para instâncias compatíveis com EC2 em execução no AWS Snowcone dispositivo que hospeda os volumes.
- Os tipos de volume são limitados a HDD otimizado para capacidade (`sbg1`) ou >SSD otimizado para desempenho (`sbp1`). O tipo de volume padrão é `sbg1`.
- Os volumes raiz do Amazon EC2 sempre usam o driver IDE. Os volumes adicionais do Amazon EBS usarão preferencialmente o driver Virtio, se estiver disponível. Se o driver Virtio não estiver disponível, o SBE usará como padrão o driver IDE. O driver Virtio permite melhor desempenho e é recomendado.
- Durante a criação de volumes do Amazon EBS, não há suporte para o parâmetro `encrypted`. No entanto, todos os dados no seu dispositivo são criptografados por padrão.
- Os volumes podem ter de 1 GB a 8 TB de tamanho.
- Até dez volumes do Amazon EBS podem ser anexados a uma única instância compatível com o EC2.

- Não há um limite formal para o número de volumes do Amazon EBS que você pode ter no dispositivo AWS Snowcone . No entanto, a capacidade total do volume do Amazon EBS é limitada pelo espaço disponível em seu AWS Snowcone dispositivo.

Grupos de segurança em dispositivos Snow

Um grupo de segurança atua como um firewall virtual que controla o tráfego de uma ou mais instâncias. Ao executar uma instância, você pode associar um ou mais security groups à instância. Você pode adicionar regras a cada grupo de segurança para permitir tráfego de entrada ou de saída das instâncias associadas. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias Linux no Guia](#) do usuário do Amazon EC2.

Os grupos de segurança em dispositivos do Snowcone são semelhantes a grupos de segurança na Nuvem AWS. Nuvens privadas virtuais (VPCs) não são compatíveis em dispositivos Snowcone.

A seguir, você pode encontrar as outras diferenças entre grupos de segurança do Snowcone e grupos de segurança de EC2-VPC:

- Cada Snowcone tem um limite de 50 grupos de segurança.
- O grupo de segurança padrão permite todo o tráfego de entrada e saída.
- O tráfego entre instâncias locais pode usar o endereço IP da instância privada ou um endereço IP público. Por exemplo, suponha que você deseja se conectar usando SSH na instância A com a instância B. Nesse caso, seu endereço IP de destino pode ser o IP público ou endereço IP privado da instância B, se a regra de grupo de segurança permitir o tráfego.
- Somente os parâmetros listados para AWS CLI ações e chamadas de API são compatíveis. Normalmente, esses são um subconjunto daqueles compatíveis em instâncias de EC2-VPC.

Para obter mais informações sobre AWS CLI ações suportadas, consulte [Lista de comandos do AWS CLI compatíveis com o Amazon EC2 em um Snowcone](#) . Para obter mais informações sobre as operações da API compatíveis, consulte [Operações da API do Amazon EC2 com suporte](#).

Metadados da instância e dados do usuário compatíveis

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução. O Snowcone oferece suporte a um subconjunto de categorias de metadados da instância para as instâncias de computação. Para obter mais informações, consulte [Metadados da instância e dados do usuário](#) no Manual do usuário do Amazon EC2.

As seguintes categorias são compatíveis. O uso de qualquer outra categoria retornará uma mensagem de erro 404.

Categorias de metadados de instância compatíveis em um Snowcone

| Dados | Descrição |
|---|---|
| <code>ami-id</code> | O ID da AMI usada para executar a instância. |
| <code>hostname</code> | O nome de host DNS IPv4 privado da instância . |
| <code>instance-id</code> | O ID dessa instância. |
| <code>instance-type</code> | O tipo da instância. |
| <code>local-hostname</code> | O nome de host DNS IPv4 privado da instância . |
| <code>local-ipv4</code> | O endereço IPv4 privado da instância. |
| <code>mac</code> | O endereço Media Access Control (MAC) da instância. |
| <code>network/interfaces/macs/ <i>mac</i> / local-hostname</code> | O nome do host local da interface. |
| <code>network/interfaces/macs/ <i>mac</i> / local-ipv4s</code> | Os endereços IPv4 privados associados à interface. |
| <code>network/interfaces/macs/ <i>mac</i> / mac</code> | O endereço MAC da instância. |
| <code>network/interfaces/macs/ <i>mac</i> / public-ipv4s</code> | Os endereços IP elásticos associados à interface. |
| <code>public-ipv4</code> | O endereço IPv4 público. |
| <code>public-keys/0/openssh-key</code> | Chave pública. Disponível somente se fornecido no momento da execução da instância. |

| Dados | Descrição |
|-----------------------------|---|
| <code>reservation-id</code> | O ID da reserva. |
| <code>userData</code> | Scripts de shell para enviar instruções para uma instância na execução. |

Categorias de dados dinâmicos de instância compatíveis em um Snowcone

| Dados | Descrição |
|---|---|
| <code>instance-identity/document</code> | JSON que contém atributos de instância . Somente <code>instanceId</code> , <code>imageId</code> , <code>privateIp</code> , and <code>instanceType</code> têm valores, e os outros atributos retornados são nulos. Para obter mais informações, consulte Documentos de identidade da instância no Guia do usuário do Amazon EC2. |

Dados do usuário em instâncias de computação do Snowcone

Os dados do usuário são compatíveis para uso com scripts de shell para instâncias de computação em um dispositivo Snowcone. Usando os scripts de shell, você pode enviar instruções para uma instância na execução. Você pode alterar os dados do usuário com o `modify-instance-attribute` AWS CLI comando ou a ação `ModifyInstanceAttribute` da API.

Para alterar dados do usuário

1. Pare sua instância de computação com o `stop-instances` AWS CLI comando.
2. Usando o `modify-instance-attribute` AWS CLI comando, modifique o `userData` atributo.
3. Reinicie sua instância de computação com o `start-instances` AWS CLI comando.

Somente scripts de shell são compatíveis com instâncias de computação. Não há suporte para as diretivas de `cloud-init` do pacote nas instâncias de computação em execução em um Snowcone.

Para obter mais informações sobre como trabalhar com AWS CLI comandos, consulte a [Referência de AWS CLI comandos](#).

Solução de problemas para instâncias de computação em dispositivos Snowcone

A seguir, você pode encontrar dicas para a solução de problemas em trabalhos do Snowcone com instâncias de computação.

Tópicos

- [A interface de rede virtual tem um endereço IP de 0.0.0.0](#)
- [O Snowcone trava ao iniciar uma instância de computação grande](#)
- [Minha instância tem um volume raiz](#)
- [Erro de arquivo de chave privada desprotegido](#)

A interface de rede virtual tem um endereço IP de 0.0.0.0

Esse problema pode ocorrer se a interface de rede física (NIC) que você associou à sua interface de rede virtual (VNIC) também tiver um endereço IP 0.0.0.0. Esse efeito pode acontecer se a NIC não tiver sido configurada com um endereço IP (por exemplo, se você tiver apenas ligado o dispositivo). Isso também pode acontecer se você estiver usando a interface do RJ45 errada. O Snowcone tem duas interfaces RJ45, você pode estar especificando a interface física errada

Medida a ser tomada

Se isso acontecer, você poderá fazer o seguinte:

- Criar uma nova VNIC, associada a uma NIC que possui um endereço IP. Para ter mais informações, consulte [Configuração de rede para as instâncias de computação](#).
- Atualizar uma VNIC existente. Para ter mais informações, consulte [Atualização de uma interface de rede virtual](#).

O Snowcone trava ao iniciar uma instância de computação grande

Pode parecer que o Snowcone parou de iniciar uma instância. Normalmente, esse não é o caso. No entanto, pode demorar uma hora ou mais para que as maiores instâncias de computação sejam

executadas. Você pode verificar o status de suas instâncias usando o AWS CLI comando `aws ec2 describe-instances` executado no endpoint HTTP ou HTTPS do Amazon EC2 no Snowcone.

Minha instância tem um volume raiz

As instâncias têm um volume raiz por padrão. Todas as instâncias sbe têm um único volume raiz.

Para obter informações adicionais sobre a adição de volumes, consulte <https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-snowcone-ebs.html>

Erro de arquivo de chave privada desprotegido

Esse erro pode ocorrer se o arquivo `.pem` na instância de computação apresentar permissões de leitura/gravação insuficientes.

Medida a ser tomada

Resolva isso alterando as permissões para o arquivo com o seguinte procedimento:

1. Abra um terminal e navegue até o local onde salvou o arquivo `.pem`.
2. Insira o comando da a seguir.

```
chmod 400 filename.pem
```

Usando AWS DataSync para transferir arquivos

AWS DataSync é um serviço de transferência de dados on-line que simplifica, automatiza e acelera a cópia de grandes quantidades de dados de e para serviços de AWS armazenamento pela Internet ou. AWS Direct Connect DataSync O agente vem pré-instalado em seu dispositivo Snowcone. Ele pode transferir dados entre o dispositivo e os buckets do Amazon S3, o Amazon EFS e o Amazon FSx for Windows File Server. AWS DataSync lida automaticamente com a movimentação de arquivos e objetos, agendando transferências de dados, monitorando o progresso das transferências, criptografando, verificando as transferências de dados e notificando os clientes sobre quaisquer problemas.

Antes de iniciar o DataSync agente, habilite o Network File System (NFS) em seu dispositivo Snowcone. Consulte [Configurando a interface NFS automaticamente](#) e [Iniciando o NFS e restringindo o acesso](#).

O DataSync agente é pré-instalado em seu dispositivo Snowcone como AMI durante a preparação do trabalho no Snowcone. Para transferir dados on-line para AWS, conecte o dispositivo Snowcone à rede externa e use nossa CLI AWS OpsHub para iniciar a AMI do agente. DataSync Ative o DataSync agente no AWS Management Console ou use a CLI e configure sua tarefa de transferência de dados on-line entre a loja Snowcone NFS e o Amazon S3, o Amazon EFS ou o Amazon FSx for Windows File Server.

Você pode usar a AWS DataSync corrida no Snowcone para o seguinte:

- Aplicativos de computação de borda, para coletar dados, processar os dados para obter uma visão imediata e, em seguida, transferir os dados on-line para a AWS.
- Transfira dados gerados continuamente por sensores ou máquinas on-line para uma fábrica ou AWS em outros locais periféricos.
- Distribua mídia, conteúdo científico ou outro conteúdo on-line dos serviços de AWS armazenamento para seus parceiros e clientes.
- Agregue conteúdo transferindo mídia, conteúdo científico ou outro conteúdo on-line de seus pontos de presença para o AWS
- Certifique-se de usar um endereço IP estático para o VNI do DataSync agente. O uso do DHCP pode causar problemas porque a reinicialização de qualquer dispositivo pode significar que você está usando um endereço IP diferente, forçando a necessidade de reconfigurar o DataSync agente e DataSync a ativação na nuvem.AWS
- Para usar o agente Datasync no Snowcone, você precisa garantir que as entradas “AllowedHosts” incluam o endereço IP do DataSync agente na sua configuração de NFS no Snowcone. Isso pode exigir que você pare e reinicie o serviço NFS no Snowcone para habilitar o DataSync agente.
- Sempre que você interromper o serviço NFS, você também deve interromper o DataSync agente. Nota: Se você interromper o serviço NFS que permitiu o DataSync agente listado, ele impedirá que o agente Datasync funcione.
- Verifique as [cotas de tarefas do AWS DataSync](#) para ver o número máximo de arquivos por tarefa para um dispositivo Snowcone. Se você exceder o limite de 200.000 arquivos, a DataSync tarefa reportará um erro de alocação de memória e abortará a execução.

Para fluxos de trabalho únicos de computação de borda ou transferência de dados ou para fluxos de trabalho Snowcone em locais periféricos sem um link de rede de longa distância (WAN) ou largura de banda de WAN inadequada, você deve devolver o dispositivo Snowcone para concluir a transferência de dados. AWS

Gerenciando a interface NFS

Use a interface Network File System (NFS) para fazer upload de arquivos para o dispositivo da família Snow como se o dispositivo fosse um armazenamento local em seu sistema operacional. Isso permite uma abordagem mais fácil de usar para transferir dados, pois você pode usar recursos do seu sistema operacional, como copiar arquivos, arrastá-los e soltá-los ou outros recursos da interface gráfica do usuário. Cada bucket S3 no dispositivo está disponível como um endpoint de interface NFS e pode ser montado para copiar dados. A interface NFS está disponível para trabalhos de importação.

Quando iniciada, a interface NFS usa 1 GB de memória e 1 CPU. Isso pode limitar o número de outros serviços em execução no dispositivo da família Snow ou o número de instâncias compatíveis com EC2 que podem ser executadas.

Os dados transferidos pela interface NFS não são criptografados em trânsito. Ao configurar a interface NFS, você pode fornecer blocos CIDR e o dispositivo da família Snow restringirá o acesso à interface NFS de computadores clientes com endereços nesses blocos.

Os arquivos no dispositivo serão transferidos para o Amazon S3 quando ele for devolvido. AWS Para obter mais informações, consulte [S3 Como funciona o AWS Snowcone](#).

Para obter mais informações sobre como usar o NFS com o sistema operacional do seu computador, consulte a documentação do seu sistema operacional.

Lembre-se dos detalhes a seguir ao usar a interface NFS.

- Os nomes dos arquivos são chaves de objeto em seu bucket do S3 local no dispositivo da Família Snow. O nome para uma chave é uma sequência de caracteres Unicode cuja codificação UTF-8 é de, no máximo, 1.024 bytes de comprimento. Recomendamos usar o NFSv4.1 sempre que possível e codificar os nomes dos arquivos com Unicode UTF-8 para garantir uma importação de dados bem-sucedida. Os nomes de arquivo que não estão codificados com UTF-8 podem não ser enviados para o S3 ou podem ser carregados para o S3 com um nome de arquivo diferente, dependendo da codificação NFS que você usa.
- Certifique-se de que o tamanho máximo do caminho do arquivo seja inferior a 1024 caracteres. Os dispositivos da Família Snow não oferecem suporte a caminhos de arquivo maiores que 1024 caracteres. Exceder esse tamanho de caminho de arquivo resultará em erros na importação do arquivo.
- Para obter mais informações, consulte [Chaves de objeto](#) no Guia do usuário do Amazon Simple Storage Service.

- Para transferências baseadas em NFS, metadados padrão no estilo POSIX serão adicionados aos seus objetos à medida que forem importados para o Amazon S3 a partir de dispositivos da família Snow. Além disso, você verá os metadados "x-amz-meta-user-agent aws-datasync" que usamos atualmente AWS DataSync como parte do mecanismo interno de importação para o Amazon S3 para importação de dispositivos da família Snow com a opção NFS.

Note

O espaço de armazenamento disponível no dispositivo Snowcone não é preciso até que o serviço NFS seja iniciado.

Você também pode configurar e gerenciar a interface NFS com uma AWS OpsHub ferramenta GUI. Para obter mais informações, consulte [usando o NFS para transferência offline de arquivos](#).

Configuração NFS para dispositivos da Família Snow

A interface NFS não está sendo executada no dispositivo Snow Family por padrão, então você precisa iniciá-la para permitir a transferência de dados para o dispositivo. Você pode configurar a interface NFS fornecendo o endereço IP de uma Interface de Rede Virtual (VNI) em execução no dispositivo da família Snow e restringindo o acesso ao seu compartilhamento de arquivos, se necessário. Antes de configurar a interface NFS, configure uma interface de rede virtual (VNI) em seu dispositivo Snow Family. Para obter mais informações, consulte [Configuração de rede para instâncias de computação](#).

Configurar dispositivos da família Snow para a interface NFS

- Use o `describe-service` comando para determinar se a interface NFS está ativa.

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

O comando retornará o estado do serviço NFS ACTIVE ou INACTIVE.

```
{
  "ServiceId" : "nfs",
  "Status" : {
```

```
"State" : "ACTIVE"  
}  
}
```

Se o valor do State nome for ACTIVE, o serviço de interface NFS está ativo e você pode montar o volume NFS do dispositivo Snow Family. Para ter mais informações, consulte

[Depois que a interface NFS for iniciada, monte o endpoint como armazenamento local nos computadores cliente.](#)

[A seguir estão os comandos de montagem padrão para sistemas operacionais Windows, Linux e macOS.](#)

- 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
```

. Se o valor for INACTIVE, você precisará iniciar o serviço.

Iniciando o serviço NFS no dispositivo Snow Family

Inicie uma interface de rede virtual (VNI), se necessário, e inicie o serviço NFS no dispositivo da família Snow. Se necessário, ao iniciar o serviço NFS, forneça um bloco de endereços de rede permitidos. Se você não fornecer nenhum endereço, o acesso aos endpoints do NFS será irrestrito.

1. Use o `describe-virtual-network-interface` comando para ver os VNIs disponíveis no dispositivo Snow Family.

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

Se uma ou mais VNIs estiverem ativas no dispositivo Snow Family, o comando retornará o seguinte.

```
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"
  }
]
```

Observe o valor do `VirtualNetworkInterfaceArn` nome do VNI a ser usado com a interface NFS.

- Se nenhum VNIs estiver disponível, use o `create-virtual-network-interface` comando para criar um VNI para a interface NFS. Para obter mais informações, consulte [Configurando uma interface de rede virtual \(VNI\)](#).
- Use o `start-service` comando para iniciar o serviço NFS e associá-lo ao VNI. Para restringir o acesso à interface NFS, inclua os `AllowedHosts` parâmetros `service-configuration` e no comando.

```
snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id nfs --service-configuration AllowedHosts=CIDR-address-range
```

- Use o `describe-service` comando para verificar o status do serviço. Ele está sendo executado quando o valor do `State` nome é `ACTIVE`.

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

O comando retorna o estado do serviço, bem como o endereço IP e o número da porta do endpoint NFS e os intervalos CIDR permitidos para acessar o endpoint.

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

Montagem de endpoints NFS em computadores cliente

Depois que a interface NFS for iniciada, monte o endpoint como armazenamento local nos computadores cliente.

A seguir estão os comandos de montagem padrão para sistemas operacionais Windows, Linux e macOS.

- 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
```

Interrompendo a interface NFS

Quando você terminar de transferir arquivos pela interface NFS e antes de desligar o dispositivo Snow Family, use o `stop-service` comando para interromper o serviço NFS.

```
snowballEdge stop-service --service-id nfs
```

Usando AWS IoT Greengrass para executar software pré-instalado em instâncias compatíveis com o Amazon EC2

AWS IoT Greengrass é um serviço de nuvem e tempo de execução de ponta da Internet das Coisas (IoT) de código aberto que ajuda você a criar, implantar e gerenciar aplicativos de IoT em seus dispositivos. Você pode usar AWS IoT Greengrass para criar um software que permite que seus dispositivos atuem localmente com base nos dados que eles geram, executem previsões com base em modelos de aprendizado de máquina e filtrem e agreguem dados do dispositivo. Para obter informações detalhadas sobre AWS IoT Greengrass, consulte [O que é AWS IoT Greengrass?](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Ao usar AWS IoT Greengrass em seu dispositivo Snow Family, você permite que o dispositivo colete e analise dados mais perto de onde eles são gerados, reaja de forma autônoma aos eventos locais e se comunique com segurança com outros dispositivos na rede local.

Configurando sua instância compatível com Amazon EC2

Note

Para instalar AWS IoT Greengrass Version 2 em um dispositivo Snow Family, verifique se o dispositivo está conectado à Internet. Após a instalação, a Internet não é necessária para que um dispositivo da Snow Family funcione AWS IoT Greengrass.

Para configurar uma instância compatível com EC2 para AWS IoT Greengrass V2

1. Inicie a AMI AWS IoT Greengrass validada com um endereço IP público e uma chave SSH:
 - a. Usando AWS CLI: [run-instances](#).
 - b. Usando AWS OpsHub: [Iniciando uma instância compatível com o Amazon EC2](#).

Note

Anote o endereço IP público e o nome da chave SSH associados à instância.

2. Conecte-se à instância compatível com EC2 usando o SSH. Para fazer isso, execute o comando a seguir no computador conectado ao dispositivo. Substitua *ssh-key* pela chave que você usou

para iniciar a instância compatível com EC2. *public-ip-address* Substitua pelo endereço IP público da instância compatível com EC2.

```
ssh -i ssh-key ec2-user@ public-ip-address
```

Important

Se seu computador usa uma versão anterior do Microsoft Windows, talvez você não tenha o comando SSH ou tenha SSH, mas não consiga se conectar à sua instância compatível com EC2. Para se conectar à sua instância compatível com EC2, você pode instalar e configurar o PuTTY, que é um cliente SSH de código aberto e gratuito. Você deve converter a chave SSH do formato `.pem` para o formato PuTTY e conectar-se à sua instância do EC2. Para obter instruções sobre como converter para o formato PuTTY, consulte [Converter sua chave privada usando PuTTYgen no](#) Guia do usuário do Amazon EC2. `.pem`

Instalando AWS IoT Greengrass

Em seguida, você configura sua instância compatível com EC2 como um dispositivo AWS IoT Greengrass Core que pode ser usado para desenvolvimento local.

Para instalar AWS IoT Greengrass

1. Use o comando a seguir para instalar o software de pré-requisito para AWS IoT Greengrass. Esse comando instala o AWS Command Line Interface (AWS CLI) v2, o Python 3 e o 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. Conceda ao usuário root permissão para executar o AWS IoT Greengrass software e modificar a permissão root de `root ALL=(ALL) ALL` para `root ALL=(ALL:ALL) ALL` no arquivo de configuração `sudoers`.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Use o comando a seguir para baixar o software AWS IoT Greengrass Core.

```
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
```

- Use os comandos a seguir para fornecer credenciais para permitir a instalação do software AWS IoT Greengrass principal. Substitua os valores de exemplo pelas suas credenciais.

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE  
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

Note

Essas são credenciais do usuário do IAM na AWS região, não do dispositivo da família Snow.

- Use o comando a seguir para instalar o software AWS IoT Greengrass Core. O comando cria AWS os recursos que o software principal precisa para operar e configura o software principal como um serviço do sistema que é executado quando a AMI é inicializada.

Substitua os parâmetros a seguir no comando:

- `region`: A AWS região na qual encontrar ou criar recursos.
- `MyGreengrassCore`: O nome do AWS IoT item do seu dispositivo AWS IoT Greengrass principal.
- `MyGreengrassCoreGroup`: o nome do grupo de AWS IoT coisas do seu dispositivo AWS IoT Greengrass principal.

```
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

Esse comando é para uma instância compatível com o Amazon EC2 que executa uma AMI do Amazon Linux 2. Para uma AMI do Windows, consulte [Instalar o software AWS IoT Greengrass principal](#).

Quando terminar, você terá um AWS IoT Greengrass núcleo em execução no seu dispositivo Snow Family para uso local.

Portas necessárias para usar AWS serviços em um AWS Snowcone dispositivo

Para que AWS os serviços funcionem corretamente em um AWS Snowcone dispositivo, você deve permitir as portas de rede para o serviço.

Veja a seguir uma lista de portas de rede necessárias para cada serviço da AWS .

| Porta | Protocolo | Comentário |
|-------|-----------|--|
| 22 | SSH | Verificação de integridade do dispositivo e para EC2 SSH |
| 2049 | NFS | Endpoint de NFS |
| 8008 | HTTP | Endpoint do HTTP do EC2 |
| 8243 | HTTPS | Endpoint do HTTPS do EC2 |
| 9091 | HTTP | Endpoint para gerenciamento de dispositivos |

Devolvendo o dispositivo Snowcone

Quando terminar de transferir dados para o dispositivo Snowcone, prepare-o para sua viagem de volta para a AWS. Antes de continuar, verifique se todas as transferências de dados para o dispositivo foram interrompidas.

Quando todas as comunicações com o dispositivo terminarem, desligue-o pressionando o botão de ligar/desligar. O dispositivo leva cerca de 20 segundos para desligar.

Desconecte o dispositivo Snowcone

Desconecte os cabos do Snowcone. Quando o rótulo de remessa de devolução aparecer na tela E Ink na parte superior do dispositivo, ele está pronto para ser devolvido. Para ver qual é a empresa de remessas da região, consulte [Considerações de envio para AWS Snowcone](#).

Consideração específica do tipo de trabalho

Important

Se você estiver importando dados, não exclua suas cópias locais dos dados transferidos até que a importação AWS seja bem-sucedida no final do processo e você possa verificar os resultados da transferência de dados.

Note

Depois de devolver o dispositivo Snow para importação no Amazon S3, AWS iniciará a ingestão dos dados após garantir que o dispositivo não tenha sido adulterado e que o dispositivo esteja íntegro. Caso não queira que os dados do dispositivo sejam ingeridos no bucket do S3 de destino, é possível solicitar o cancelamento do trabalho do Snow. Se você cancelar o trabalho, vamos ignorar a transferência de dados e apagar o dispositivo com segurança seguindo os processos estabelecidos. Não podemos manter um dispositivo com seus dados em nossas instalações devido à nossa rigorosa cadeia de custódia e procedimentos operacionais.

Para obter informações sobre como enviar um dispositivo, consulte [Considerações de envio para AWS Snowcone](#).

Proteção de dados no seu dispositivo

Considere as recomendações a seguir para ajudar a proteger os dados em seu AWS Snowcone dispositivo.

Tópicos

- [Protegendo seu AWS Snowcone](#)
- [Validação de tags NFC](#)

Protegendo seu AWS Snowcone

A seguir estão alguns pontos de segurança que recomendamos que você considere ao usar o Snowcone, além de algumas informações de alto nível sobre outras precauções de segurança que tomamos quando um dispositivo chega para processamento. AWS

Recomendamos as seguintes abordagens de segurança:

- Assim que o dispositivo chegar, inspecione-o para ver se está danificado ou se apresenta alguma violação evidente. Se observar qualquer coisa que pareça suspeita sobre o dispositivo, não o conecte à rede interna. Em vez disso, entre em contato com o [AWS Support](#), e você receberá um novo dispositivo.
- Você deve fazer um esforço para proteger as credenciais de trabalho contra divulgação. Qualquer pessoa que tiver acesso a um manifesto e código de desbloqueio do trabalho pode acessar o conteúdo do dispositivo enviado para esse trabalho.
- Não deixe o dispositivo parado em uma plataforma de carregamento. Deixá-lo em uma plataforma de carregamento pode expô-lo à intempérie. Embora os dispositivos do Snowcone sejam resistentes, o clima pode danificar até o hardware mais resistente. Relate dispositivos roubados, perdidos ou quebrados o mais rápido possível. Quanto antes um problema for relatado, tanto antes será possível enviar outro para fazer o trabalho.

Note

O dispositivo Snowcone é propriedade da AWS. A adulteração de um dispositivo é uma violação da Política de Uso AWS Aceitável. Para obter mais informações, consulte <http://aws.amazon.com/aup/>.

Nós executamos as seguintes etapas de segurança:

- Ao transferir dados com a interface de arquivos, os metadados de objeto são mantidos.
- Quando um dispositivo chega AWS, nós o inspecionamos em busca de sinais de adulteração e verificamos se nenhuma alteração foi detectada pelo Trusted Platform Module (TPM). O Snowcone usa várias camadas de segurança projetadas para proteger os dados, incluindo gabinetes invioláveis, criptografia de 256 bits e um TPM padrão do setor projetado para fornecer segurança e uma rede de proteção completa dos dados.
- Depois que o trabalho de transferência de dados for processado e verificado, AWS executa uma eliminação de software do dispositivo Snowcone seguindo as diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) para higienização de mídia.

Validação de tags NFC

AWS Snowcone os dispositivos têm etiquetas NFC incorporadas. Você pode digitalizar essas tags com o aplicativo de verificação do Snowcone, disponível para Android. Digitalizar e validar essas tags NFC pode ajudar você a verificar se o dispositivo não foi adulterado antes de usá-lo.

A validação de tags NFC inclui o uso de cliente Snowball Edge Client para gerar um código QR específico do dispositivo para verificar se as tags são para o dispositivo certo. Para mais informações, consulte [Obter o código QR para validação NFC](#).

O procedimento a seguir descreve como validar as tags NFC em um dispositivo Snowcone. Antes de começar, verifique se você executou as primeiras etapas a seguir do exercício de conceitos básicos:

1. Crie seu primeiro trabalho. Para obter mais informações, consulte [Criação de um trabalho para solicitar um dispositivo Snow Family](#).
2. Receba o dispositivo.
3. Conecte-se à sua rede local.
4. Obtenha suas credenciais e ferramentas. Para ter mais informações, consulte [Como obter as credenciais](#).
5. Faça o download e instale o Snowball Edge Client. Para ter mais informações, consulte [Usando o AWS Snowball Edge cliente](#).

Para validar as etiquetas NFC em um dispositivo AWS Snowcone

1. Execute o comando do cliente Snowball Edge `snowballEdge get-app-qr-code`. Para obter mais informações sobre o uso desse comando, consulte [Obter o código QR para validação NFC](#).

O código QR é salvo em um local de sua escolha como um arquivo .png.

2. Navegue até o arquivo .png que salvou e abra-o para que você possa digitalizar o código QR com o aplicativo.
3. Para digitalizar as etiquetas NFC com o telefone, baixe e instale o aplicativo Snowcone Verification. Faça download do aplicativo na loja Google Play se estiver usando um dispositivo Android.
4. Inicie o aplicativo e siga as instruções na tela.

Agora, você digitalizou e validou as tags NFC com êxito para o dispositivo.

Se você tiver problemas durante a digitalização, tente o seguinte:

- Faça download do aplicativo em outro telefone e tente novamente.
- Mova o dispositivo para uma área isolada da sala, longe de interferência de outras tags NFC e tente novamente.
- Se os problemas persistirem, entre em contato com o [AWS Support](#).

Entendendo os status AWS Snowcone de Job

Quando você cria um AWS Snowcone trabalho, ele passa pelos status do trabalho e o status é mostrado no Console de Gerenciamento da família AWS Snow

Como ver o status de um trabalho

1. Faça login no [Console de Gerenciamento da família AWS Snow](#).
2. No painel Job, escolha o trabalho.
3. Clique no nome do seu trabalho no console.
4. O painel Status do trabalho estará localizado próximo à parte superior e refletirá o status do trabalho.

Note

Se não conseguirmos importar dados do dispositivo Snow para os nossos datacenters devido a qualquer problema com as permissões de acesso que você configurou, tentaremos enviar uma notificação, e você terá trinta dias a partir da data da notificação para resolver o problema. Se o problema não for resolvido, poderemos cancelar seu AWS Snow Family trabalho e excluir dados do dispositivo.

AWS Snowcone status de trabalho do dispositivo

| Status do trabalho | Significado |
|---------------------------|---|
| Trabalho criado | O trabalho foi criado. Esse status é o único durante o qual é possível cancelar um trabalho ou partes do trabalho, se o trabalho é um trabalho de exportação. |
| Preparação do dispositivo | AWS está preparando um dispositivo para seu trabalho. |
| Preparação de entrega | AWS está se preparando para enviar um dispositivo para você. |

| Status do trabalho | Significado |
|----------------------------|---|
| Em trânsito | O dispositivo foi enviado para o endereço fornecido durante a criação do trabalho. |
| Entregue | O dispositivo chegou ao endereço indicado durante a criação do trabalho. |
| Em trânsito para AWS | Você enviou o dispositivo de volta para o. AWS |
| No departamento de triagem | O dispositivo para este trabalho está em nosso departamento de triagem interna. Qualquer processamento adicional para trabalhos de importação para o Amazon S3 começará em breve, normalmente em até dois dias. |
| Em AWS | O envio chegou à AWS. Se estiver importando dados, a importação normalmente começa em um dia da chegada. |
| Importação | AWS está importando seus dados para o Amazon S3. |
| Concluído | O trabalho ou parte do trabalho foi concluída com êxito. |
| Cancelado | O trabalho foi cancelado. |

Notificações para dispositivos da família Snow

Como o Snow usa o Amazon SNS

O serviço Snow foi projetado para aproveitar as notificações robustas fornecidas pelo Amazon Simple Notification Service (Amazon SNS). Ao criar um trabalho para solicitar um dispositivo Snow, você pode fornecer endereços de e-mail para receber notificações sobre alterações no status do trabalho. Ao fazer isso, escolha um tópico do SNS existente ou crie um novo. Se o tópico do SNS estiver criptografado, você precisará habilitar a criptografia KMS gerenciada pelo cliente para o tópico e configurar a política de chave do KMS gerenciada pelo cliente. Consulte [Escolher suas preferências de notificação](#).

Depois de criar seu trabalho, cada endereço de e-mail que você especificou para receber notificações do Amazon SNS recebe uma mensagem de e-mail de AWS notificações solicitando a confirmação da assinatura do tópico. Para que cada endereço de e-mail receba notificações adicionais, um usuário da conta deve confirmar a assinatura, escolhendo Confirmar assinatura. Os e-mails de notificação do Amazon SNS são personalizadas para cada estado de ativação e incluem um link para a [Console de Gerenciamento da família AWS Snow](#).

O Amazon SNS pode ser configurado para enviar mensagens de texto para essas notificações de status do console do Amazon SNS. Para obter mais informações, consulte [Mensagens de texto móveis \(SMS\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

Criptografando tópicos do SNS para alterações no status do trabalho do Snow

Ative a criptografia KMS gerenciada pelo cliente para o tópico SNS para notificações de alteração do status do trabalho do Snow. Os tópicos do SNS criptografados com criptografia AWS gerenciada não podem receber alterações no status do trabalho do Snow porque a função do IAM de importação do Snow não tem acesso à chave KMS AWS gerenciada para executar e executar ações. Decrypt GenerateDataKey Além disso, as políticas AWS de chaves KMS gerenciadas não podem ser editadas.

Para habilitar a criptografia do lado do servidor para um tópico do SNS usando o console do gerenciamento do Amazon SNS

1. [Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. No painel de navegação, escolha Tópicos.
3. Na página Tópicos, escolha o tópico usado para notificações de alteração do status do trabalho e escolha Editar.
4. Expanda a seção Criptografia e faça o seguinte:
 - a. Selecione Ativar criptografia.
 - b. Especifique a chave AWS KMS. Consulte
 - c. Para cada tipo de KMS, são exibidos descrição, conta e ARN do KMS.
5. Para usar uma chave personalizada da sua AWS conta, escolha o campo Chave AWS KMS e, em seguida, escolha a chave KMS personalizada na lista. Para obter instruções sobre como criar um KMS personalizado, consulte [Criação de chaves](#) no Guia do AWS Key Management Service desenvolvedor.

Para usar um ARN KMS personalizado da AWS sua conta ou de AWS outra conta, insira o ARN AWS da chave KMS no campo Chave KMS.

6. Escolha Salvar alterações. SSE é habilitada para o seu tópico e a página do tópico é exibida.

Configurando uma política de chaves KMS gerenciada pelo cliente

Depois de habilitar a criptografia para tópicos do SNS que receberão notificações sobre alterações no status do trabalho do Snow, atualize a política do KMS para a criptografia de tópicos do SNS e permita a entidade principal do serviço do Snow "importexport.amazonaws.com" para as ações "mks:Decrypt" e "mks:GenerateDataKey*".

Para permitir o perfil de serviço de importação e exportação na política de chaves do KMS

1. Faça login AWS Management Console e abra o console AWS Key Management Service (AWS KMS) em <https://console.aws.amazon.com/kms>.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No canto superior direito do console, altere o console para a mesma região Região da AWS de onde o dispositivo Snow foi pedido.

4. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
5. Na lista de chaves do KMS, escolha o alias ou o ID de chave da chaves do KMS que você deseja examinar.
6. Nas instruções da política de chaves, é possível ver as entidades principais que receberam acesso à chave do KMS pela política de chaves e ver as ações que elas podem executar.
7. Para a entidade principal do serviço do Snow "importexport.amazonaws.com", adicione a seguinte declaração de política para as ações "kms:Decrypt" e "kms:GenerateDataKey*":

```
{
  "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. Escolha Salvar alterações para aplicar as alterações e sair do editor de políticas.

Exemplos de notificação do SNS

As notificações do Amazon SNS produzem as seguintes mensagens de e-mail quando o status do seu trabalho muda. Essas mensagens são exemplos do protocolo de tópicos do Email-JSON SNS.

| Status do trabalho | Notificações do SNS |
|--------------------|--|
| Trabalho criado | <pre> { "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+T0yaLiEGLrIIIL4esi111hIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJIYPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre> |

| Status do trabalho | Notificações do SNS |
|---------------------------|---|
| Preparação do dispositivo | <pre> { "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" } </pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|---|
| Exportação | <pre>{ "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" }</pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|--|
| Em trânsito | <pre> { "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" } </pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|---|
| Entregue | <pre>{ "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 +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" }</pre> |

| Status do trabalho | Notificações do SNS |
|----------------------|--|
| Em trânsito para AWS | <pre>{ "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" }</pre> |

| Status do trabalho | Notificações do SNS |
|----------------------------|--|
| No departamento de triagem | <pre> { "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 +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 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|---|
| Em AWS | <pre> { "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" } </pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|---|
| Importação | <pre>{ "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" }</pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|--|
| Concluído | <pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) complete.\nThanks for using AWS Snow Family.\nCan you take a quick survey on your experienc e? Survey here: http://bit.ly/1pLQ JMY. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkg ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre> |

| Status do trabalho | Notificações do SNS |
|--------------------|---------------------|
| | |

| Status do trabalho | Notificações do SNS |
|--------------------|--|
| Cancelado | <pre>{ "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 +1bZkLd0ZdtRj1IyPRP44eyq78sU0Eo/ 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" }</pre> |

Entendendo o AWS Snowcone processo de pedido

Existem duas opções ao pedir um AWS Snowcone. Você pode fazer o pedido por meio do Console de Gerenciamento da família AWS Snow ou usar a API de gerenciamento de trabalhos (JMAPI).

Noções básicas sobre o processo de envio

Nesta seção, você encontrará informações sobre como o envio de um AWS Snowcone dispositivo é tratado e uma lista de Regiões da AWS quais são compatíveis. Para obter mais informações sobre as regiões e os endpoints, consulte [Endpoints da Família AWS Snow e cotas](#) no Referência geral da AWS. A taxa de envio que for escolhida para um trabalho é aplicável tanto para enviar e receber o dispositivo Snowcone usado para esse trabalho. Para obter mais informações sobre cobranças de envio, consulte [Definição de preço do AWS Snowcone](#).

Note

Os dispositivos Snowcone somente podem ser usados para importar ou exportar dados dentro da região da AWS onde eles foram solicitados.

Devolvendo um dispositivo Snowcone

As informações de remessa de pré-pago na tela E Ink contêm o endereço correto para retornar o dispositivo. Para obter mais informações sobre como fazer a devolução do dispositivo Snowcone, consulte [Empresas de remessa](#). O dispositivo Snowcone é entregue a uma instalação de AWS triagem e encaminhado para o data center. AWS O rastreamento do pacote está disponível por meio da empresa de remessa da sua região. Para rastrear alterações de status do trabalho use o Console de Gerenciamento da família AWS Snow.

Important

A menos que seja pessoalmente instruído de outra forma AWS, não afixe uma etiqueta de remessa separada no dispositivo Snowcone. Use sempre a etiqueta de envio exibida na tela E Ink do dispositivo .

Usando o AWS Management Console

Você pode solicitar um dispositivo Snowcone usando o Console de Gerenciamento da família AWS Snow.

Como solicitar o Snowcone a partir do console

Para obter instruções passo a passo sobre como encomendar um Snowcone usando o AWS Snowball console, consulte. [Conceitos básicos](#)

Uso de APIs de gerenciamento de trabalhos

A API de gerenciamento de trabalhos (JMAPI) fornece acesso programático à mesma funcionalidade disponível no Console de Gerenciamento da família AWS Snow. Isso permite que você automatize a funcionalidade do trabalho. Usando o JMAPI, você pode ver o status do trabalho, criar trabalhos, baixar o arquivo manifesto, desbloquear o código e visualizar relatórios de conclusão do trabalho. Como as chamadas são feitas por meio da API, você pode integrá-las a um aplicativo personalizado ou front-end da Web.

Tópicos

- [Usos comuns do JMAPI](#)
- [Cadeias de caracteres obrigatórias do JMAPI](#)
- [Endpoints JMAPI](#)
- [Comandos da JMAPI CLI](#)
- [Exemplos](#)

Usos comuns do JMAPI

- Automatizando pedidos de dispositivos Snowcone
- Baixando o arquivo manifesto
- Baixando o arquivo de desbloqueio
- Listando os trabalhos atuais de Snowcone
- Baixando o relatório de conclusão de trabalhos do Snowcone

Cadeias de caracteres obrigatórias do JMAPI

Ao fazer um pedido por meio da API de gerenciamento de tarefas, você usa os seguintes parâmetros obrigatórios, que são mostrados com exemplos.

```
--job-type
--resources
--address-id
--region
--role-arn
--kms-key-arn
--shipping-option
--device-type
--description
```

Endpoints JMAPI

Endpoint de API

Para fazer chamadas para cada endpoint, o formato é `snowballEdge.region.amazonaws.com`. Aqui estão algumas sugestões para ajudar a entender a divisão do endpoint.

Example

| Região | Endpoint |
|-----------------------------------|----------------------------------|
| Leste dos EUA (Norte da Virgínia) | snowball.us-east-1.amazonaws.com |
| Oeste dos EUA (Oregon) | snowball.us-west-2.amazonaws.com |

Comandos da JMAPI CLI

CLI de gerenciamento de trabalhos

A seguir estão as chamadas de CLI que você pode fazer na API de gerenciamento de trabalhos.

| Command | Exemplo |
|---------------------|-------------------------------------|
| Listar os trabalhos | <code>aws snowball list-jobs</code> |

| Command | Exemplo |
|--------------------|--|
| Descrever trabalho | <code>aws snowball describe-job --job-id [JOB ID]</code> |
| Descrever endereço | <code>aws snowball describe-address --address-id</code> |
| Criar endereço | <code>aws snowball create-address --cli-input-json file://create-address.json</code> |
| Criar trabalho | <code>aws snowball create-job --cli-input-json file://create-job.json</code> |
| Cancelar trabalho | <code>aws snowball cancel-job --job-id [JOB ID]</code> |

Exemplos

Veja a seguir exemplos de comandos usando a API de gerenciamento de trabalhos.

Exemplo de KMS JSON

O exemplo de JSON a seguir é um arquivo JSON formatado corretamente para usar o arquivo de política do AWS KMS .

```
{
  "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"
  }
}
```

```
}  
}
```

Exemplo de criação de endereço

Os exemplos a seguir mostram como você formataria o comando para criar seu endereço e qual seria a resposta quando ele fosse bem-sucedido.

```
aws snowball create-address --address "Name=Bob,Company=AWS,Street1=1234 Fake  
St.,City=All,StateOrProvince=Any,Country=US,PostalCode=12345,PhoneNumber=1234567890"
```

Exemplos de resultado

```
{  
  "AddressId": "ADID3be640c8-1111-1111-1111-917f201ffa42"  
}
```

Exemplo de criação de trabalho

O comando a seguir mostra um exemplo de comando para executar o comando `create-job`.

```
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
```

O comando `create-job` acima criará uma tarefa de importação na região `us-east-1` com um dispositivo Snowcone do tipo `SNC1_SSD` com preferência de capacidade `T14` com uma opção de envio `SECOND_DAY`.

Exportação de uma AMI para uso com trabalhos do Amazon EC2

Esta seção fornece uma visão geral de como exportar sua Amazon Machine Image (AMI) para uso com instâncias computacionais compatíveis com Amazon EC2 em um dispositivo. AWS Snowcone

Tópicos

- [Configurar uma AMI para usar SSH para conectar-se às instâncias de computação iniciadas no dispositivo](#)
- [Criar seu trabalho usando o console](#)
- [Criar seu trabalho usando a AWS CLI](#)

Configurar uma AMI para usar SSH para conectar-se às instâncias de computação iniciadas no dispositivo

Para usar o Secure Shell (SSH) para se conectar às suas instâncias de computação em dispositivos Snowcone, você deve executar o procedimento a seguir. Este procedimento adiciona a chave SSH à AMI antes de criar o trabalho. Também recomendamos que você use esse procedimento para configurar seus aplicativos na instância que planeja usar como a AMI para o trabalho.

Important

Se você não seguir esse procedimento, não será possível conectar-se às suas instâncias com SSH ao receber o dispositivo Snowcone.

Para colocar uma chave SSH em uma AMI

1. Execute uma nova instância Nuvem AWS usando uma imagem de AMI compatível (consulte <https://docs.aws.amazon.com/snowball/latest/developer-guide/using-ami.html>).

Ao iniciar a instância, verifique se o tamanho do armazenamento atribuído à instância é adequado para uso posterior no dispositivo Snowcone. No console do Amazon EC2, isso é feito na Etapa 4: Adicionar armazenamento. Para obter uma lista dos tamanhos compatíveis para volumes de armazenamento de instância de computação em um Snowcone, consulte "[ec2-snowcone-limits](#)".

2. Instale e configure os aplicativos que deseja executar no Snowcone e teste para verificar se funcionam conforme o esperado.
3. Faça uma cópia do arquivo PEM/PPK usado para o par de chaves SSH para criar essa instância. Salve esse arquivo no servidor que você planeja usar para se comunicar com o Snowcone. Esse arquivo é necessário para usar SSH para se conectar à instância iniciada no dispositivo, portanto anote o caminho para esse arquivo.

4. Salve a instância como uma AMI. Para obter mais informações, consulte [Criar uma AMI do Linux baseada no Amazon EBS](#).
5. Repita esse procedimento para cada uma das instâncias às quais você deseja se conectar usando SSH. Certifique-se de copiar os diferentes pares de chaves SSH e anotar as AMIs às quais eles estão associados.

Criar seu trabalho usando o console

Sua próxima etapa é criar um trabalho para solicitar um dispositivo Snow Family. O trabalho pode ser de qualquer tipo, incluindo um cluster. Usando o [Console de Gerenciamento da família AWS Snow](#), siga as instruções fornecidas em [Criação de um trabalho para solicitar um dispositivo da família Snow](#). Ao chegar à página Etapa 3: Fornecer detalhes do trabalho no assistente de criação de trabalhos, adicione as seguintes etapas.

1. Selecione Habilitar a computação com o EC2.
2. Selecione Adicionar uma AMI.
3. Na caixa de diálogo aberta, selecione uma AMI e escolha Salvar.
4. Adicione até 20 AMIs no total ao seu trabalho, dependendo do tipo de dispositivo.
5. Continue a criação do trabalho normalmente.

Criar seu trabalho usando a AWS CLI

Você também pode criar seu trabalho usando o AWS Command Line Interface (AWS CLI). Para isso, abra um terminal e execute o comando a seguir, substituindo o texto em vermelho pelos valores reais.

```
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}}}'
```

Depois que o dispositivo chegar e você desbloqueá-lo, use o Snowball Edge Client para obter suas credenciais locais. Para ter mais informações, consulte [Como obter as credenciais](#).

Considerações de envio para AWS Snowcone

A seguir, você encontrará informações sobre como o envio de um AWS Snowcone dispositivo é feito e uma lista que mostra cada Região da AWS um dos dispositivos compatíveis. A taxa de frete escolhida para um trabalho se aplica tanto ao envio quanto ao recebimento do AWS Snowcone dispositivo usado para esse trabalho. Para obter mais informações sobre cobranças de envio, consulte [Definição de preço do AWS Snowcone](#).

Tópicos

- [Preparando um AWS Snowcone dispositivo para envio](#)
- [Restrições de envio conforme a região](#)
- [Envio de um AWS Snowcone dispositivo](#)

Ao criar um trabalho para solicitar um dispositivo Snow Family, você especifica um endereço e um prazo de entrega. Esse prazo de entrega não indica em quanto tempo você espera receber o AWS Snowcone dispositivo a partir do dia em que criou o trabalho. Mostra apenas o tempo em que o dispositivo está em trânsito entre AWS e seu endereço de entrega. Esse período não inclui o tempo de processamento, que depende de vários fatores, entre eles o tipo de trabalho (normalmente, as exportações levam mais tempo do que importações). Além disso, as operadoras geralmente só pegam os AWS Snowcone dispositivos de saída uma vez por dia. Desse modo, o processamento antes da entrega pode demorar um dia ou mais.

Note

Os dispositivos da família Snow só podem ser devolvidos ao mesmo Região da AWS local em que foram pedidos. Algumas AWS regiões oferecem suporte ao envio de dispositivos Snow Family para um país diferente daquele em que o dispositivo foi pedido. Consulte [Restrições de envio conforme a região](#) Para mais informações.

Preparando um AWS Snowcone dispositivo para envio

As considerações a seguir explicam como preparar um Snowcone e enviá-lo de volta para a AWS.

Para preparar um AWS Snowcone dispositivo para envio

1. Certifique-se de ter concluído a transferência de todos os dados desse trabalho para ou do AWS Snowcone dispositivo. [Desbloqueie o dispositivo.](#)
2. Pressione o botão liga/desliga na parte frontal do dispositivo, localizado próximo às luzes indicadoras, em frente às portas de rede. O dispositivo leva cerca de 20 segundos para desligar.

Se você desligou e desconectou seu dispositivo Snowcone e as informações de envio não aparecem na tela E Ink após cerca de um minuto, consulte [Solução de problemas na devolução de dispositivos da Família Snow.](#)

Restrições de envio conforme a região

Antes de criar um trabalho para solicitar um dispositivo da família Snow, você deve entrar no console a partir do Região da AWS qual seus dados residem. Os dispositivos da Família Snow não são enviados entre países, por exemplo, da Ásia-Pacífico (Índia) para a Ásia-Pacífico (Austrália).

Uma exceção ao envio entre países é entre os países membros da União Europeia (UE). Para transferências de dados AWS nas regiões europeias, enviamos dispositivos somente para os países membros da UE listados:

- Áustria, Bélgica, Bulgária, Croácia, Chipre, República Tcheca, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Irlanda, Letônia, Lituânia, Luxemburgo, Malta, Holanda, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Espanha e Suécia

Remessas domésticas dentro do mesmo país são permitidas. Exemplos:

- Para transferências de dados na região do Reino Unido, enviamos dispositivos internamente dentro do Reino Unido.
- Em caso de transferências de dados na região da Ásia-Pacífico (Mumbai), enviamos dispositivos apenas dentro da Índia.

Note

AWS não envia dispositivos da família Snow para caixas postais.

Envio de um AWS Snowcone dispositivo

As informações de remessa de pré-pago na tela E Ink contêm o endereço correto para retornar o dispositivo AWS Snowcone . Para obter informações sobre como devolver seu AWS Snowcone dispositivo, consulte [the section called “Empresas de remessa”](#). O AWS Snowcone dispositivo é entregue a uma instalação AWS de triagem e encaminhado para o AWS data center. O rastreamento do pacote está disponível por meio da empresa de remessa da sua região. Você pode acompanhar as mudanças de status do seu trabalho usando Console de Gerenciamento da família AWS Snow o.

Se você desligou e desconectou seu dispositivo Snowcone e as informações de envio não aparecem na tela E Ink após cerca de um minuto, consulte [Solução de problemas na devolução de dispositivos da Família Snow](#).

Empresas de remessa

Ao criar um trabalho para solicitar um dispositivo Snow Family, você fornece o endereço para onde deseja que o AWS Snowcone dispositivo seja enviado. A operadora que oferece suporte à sua região administra o envio de AWS Snowcone dispositivos AWS para você e de volta para AWS. Quando um AWS Snowcone dispositivo é enviado, você recebe um número de rastreamento. O número de rastreamento de trabalho e um link para o site de rastreamento podem ser encontrados no painel de trabalho do [Console de Gerenciamento da família AWS Snow](#) ou usando chamadas de API para a API de gerenciamento de trabalhos.

A seguir está a lista de operadoras compatíveis para AWS Snowcone dispositivos por região:

- Na Índia, a transportadora é a Blue Dart.
- Para a Coreia do Sul, o Japão, a Austrália, a Indonésia, Israel e Cingapura, a Kuehne + Nagel é a transportadora.
- Na China, a S.F. Express é a transportadora.
- Para todas as outras regiões, a empresa de remessa é a [UPS](#).

AWS Snowcone Recolhas no Canadá, na UE, na África do Sul e nos EUA

No Canadá, na UE, na África do Sul e nos EUA, lembre-se das seguintes informações para que a UPS pegue um AWS Snowcone dispositivo:

- Providencie para que a UPS retire o AWS Snowcone dispositivo agendando uma coleta diretamente com a UPS, ou leve o dispositivo a um centro de entrega de pacotes da UPS para o qual será enviado. AWS
- A etiqueta de remessa pré-paga da UPS na tela E Ink contém o endereço correto para devolver o AWS Snowcone dispositivo.
- O AWS Snowcone dispositivo é entregue a uma instalação AWS de triagem e encaminhado para o AWS data center. A UPS fornece automaticamente um número de rastreamento para sua remessa.

Os serviços da UPS para dispositivos da Família Snow são domésticos somente dentro de um país.

AWS Snowcone Pickups no Brasil

No Brasil, tenha as seguintes informações em mente para que a UPS colete um Snowcone:

- Quando você estiver pronto para devolver um Snowcone, ligue para 0800-770-9035 para agendar a retirada com a UPS.
- O Snowcone está disponível nacionalmente no Brasil, o que inclui 26 estados e o Distrito Federal.
- Se você tiver um, certifique-se de saber seu Cadastro Nacional de Pessoa Jurídica (CNPJ) antes de criar o trabalho.
- Você deve emitir o documento apropriado para devolver o dispositivo Snowcone. Confirme com o departamento fiscal quais dos documentos a seguir são necessários em seu estado, de acordo com o registro de ICMS:
 - Em São Paulo: geralmente são necessárias uma declaração de não recolhimento do ICMS e uma Nota fiscal eletrônica (NF-e).
 - Fora de São Paulo: geralmente são necessários os seguintes documentos:
 - Uma declaração de não recolhimento do ICMS
 - Uma nota fiscal avulsa
 - Uma Nota fiscal eletrônica (NF-e)

Note

Para declaração de não recolhimento do ICMS do contribuinte, recomendamos que você gere quatro cópias da declaração: uma para seus registros, as outras três para o transporte.

AWS Snowcone pickups em Israel

Em Israel, providencie a coleta entrando em contato AWS pelo e-mail snowball-shipping@amazon.com. Insira Snowcone Pickup Request no assunto e inclua as seguintes informações:

- Job ID: o ID do trabalho associado ao dispositivo Snow que você está devolvendo. Você pode encontrar o ID do trabalho no [Console de Gerenciamento da família AWS Snow](#).
- Endereço de retirada: o endereço no qual o dispositivo será retirado.
- Data de retirada: a data mais próxima em que você deseja que o dispositivo seja retirado.
- Detalhes do ponto de contato: o nome, endereço de e-mail e número de telefone que o serviço de remessa Kuehne + Nagel pode usar, se for necessário, para obter informações sobre a coleta.

Em breve, você receberá um e-mail de acompanhamento AWS Support com informações sobre a retirada do seu dispositivo no endereço fornecido. Prepare o dispositivo para envio e esteja pronto para retirada, geralmente antes das 12h, horário local. Consulte [Preparando um AWS Snowcone dispositivo para envio](#).

AWS Snowcone Pickups no Reino Unido

No Reino Unido, lembre-se das seguintes informações para que a UPS pegue um AWS Snowcone dispositivo.

- Você faz com que a UPS retire o AWS Snowcone dispositivo agendando uma coleta diretamente com a UPS, ou leve o dispositivo a um centro de entrega de pacotes da UPS para o qual será enviado. AWS
- A etiqueta de remessa pré-paga da UPS na tela E Ink contém o endereço correto para devolver o AWS Snowcone dispositivo.
- O AWS Snowcone dispositivo é entregue a uma instalação AWS de triagem e encaminhado para o AWS data center. A UPS informa automaticamente um número de controle para o trabalho.

Important

A menos que seja pessoalmente instruído de outra forma AWS, nunca afixe uma etiqueta de remessa separada no AWS Snowcone dispositivo. Use sempre a etiqueta de envio exibida na tela E Ink do dispositivo.

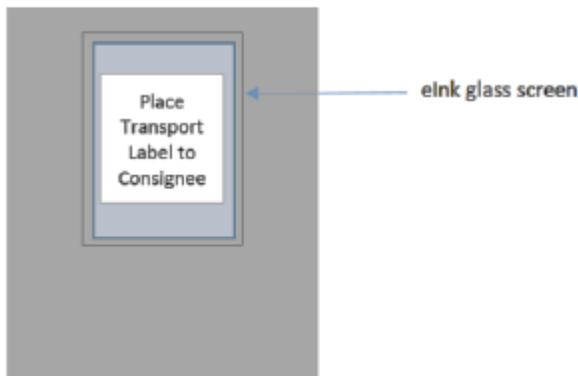
Os serviços da UPS para a família de produtos Snow são nacionais somente dentro de um país.

Note

Desde janeiro de 2021, o Reino Unido não faz mais parte da UE. Pedidos entre o Reino Unido e outros países da UE são pedidos internacionais, um processo de disponibilidade não geral aprovado apenas por meio de um processo internacional especial. Se um cliente foi aprovado e estiver devolvendo um dispositivo de um país da UE para o LHR ou do Reino Unido de volta para um país da UE, ele deverá primeiro solicitar a devolução para <snowball-shipping@amazon.com> para que uma fatura comercial possa ser fornecida antes de organizar a retirada ou entrega com a UPS.

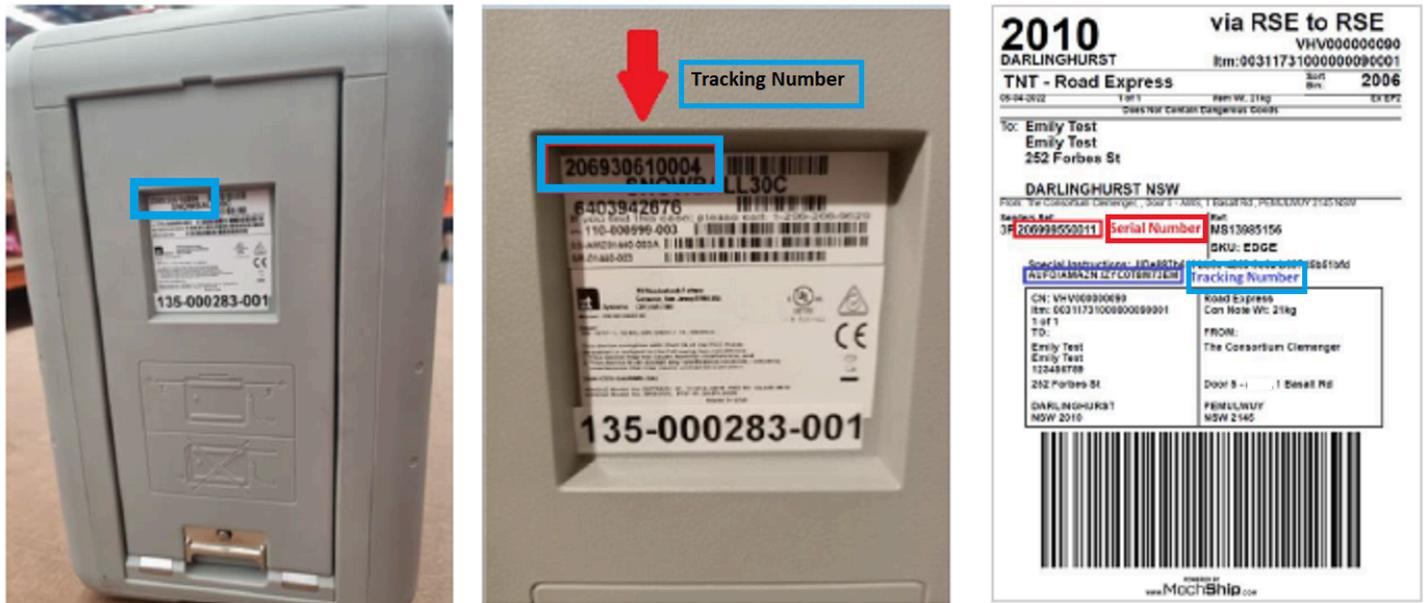
AWS Snowcone Pickups na Austrália

Na Austrália, se você estiver enviando um AWS Snowcone dispositivo de volta AWS, coloque a etiqueta de transporte de devolução (encontrada na embalagem contendo essas instruções) sobre a etiqueta eInk no dispositivo Snow.



Se você não recebeu uma etiqueta de devolução com seu dispositivo Snow, envie um e-mail para knau.snowball_return@kuehne-nagel.com com o número de série do seu dispositivo ou número de referência.

Example where to locate tracking number and serial number



Para agendar a devolução do dispositivo Snow, envie um e-mail para knau.snowball_return@kuehne-nagel.com com as informações:

- Seu nome
- Número de rastreamento (conforme mostrado em azul)
- Número de série do dispositivo (conforme mostrado em vermelho)
- Endereço completo da coleta
- Pessoa de contato na retirada
- Número de telefone de contato na retirada
- Data de coleta
- Janela de coleta (janela mínima de 3 horas dentro do horário comercial)

i Note

O dia e a hora da coleta devem ser um dia útil dentro do horário comercial

A equipe da Kuehne + Nagel responderá para confirmar o recebimento da solicitação de retirada.

AWS Snowcone Pickups na Índia

Na Índia, a Blue Dart coleta o dispositivo Snowcone. Quando você estiver pronto para devolver o dispositivo Snowcone, desligue-o e prepare-o para enviá-lo para devolução. Para programar a coleta, [envie um e-mail para snowball-pickup@amazon.com](mailto:snowball-pickup@amazon.com) com o assunto Snowcone Pickup Request. No e-mail, inclua as seguintes informações:

- ID do trabalho: o ID da tarefa associada ao Snowcone a ser retornado para a AWS.
- AWS ID da conta — A ID da AWS conta que criou o trabalho.
- Primeiro horário para coleta (seu horário local): a primeira hora do dia em que o Snowcone; deve ser coletado.
- Último horário para coleta (seu horário local): a última hora do dia em que o Snowcone deve ser coletado.
- Instruções especiais (opcional): todas as instruções especiais para coleta do Snowcone, incluindo detalhes de contato para coordenar a coleta.

A equipe do Snowcone organiza a coleta com a Blue Dart e envia um e-mail de confirmação para você. A Blue Dart fornece uma etiqueta de envio em papel e coleta o dispositivo do Snowcone.

Important

Ao usar um Snowcone na Índia, lembre-se de arquivar todos os documentos de impostos relevantes com o seu estado.

AWS Snowcone Pickups na Coreia do Sul

Na Coreia do Sul, Kuehne + Nagel processa as retiradas. Quando estiver pronto para devolver seu dispositivo, envie um e-mail para snowball-shipping@amazon.com com o Snowcone Pickup Request na linha de assunto para que possamos programar a retirada para você. No corpo do e-mail, inclua as seguintes informações:

- ID do Job — O ID do trabalho associado ao Snowcone para o qual você deseja retornar. AWS
- Endereço de retirada: o endereço no qual o dispositivo será retirado.
- Data de retirada: a data mais próxima em que você deseja que o dispositivo seja retirado.
- Detalhes do ponto de contato – o nome, o endereço de e-mail e o número de telefone local que a Kuehne + Nagel pode usar para entrar em contato com você, se necessário.

Em breve, você receberá um e-mail de acompanhamento AWS Support com informações sobre a retirada do seu dispositivo no endereço fornecido. Prepare o dispositivo para envio (consulte [Preparando um AWS Snowcone dispositivo para envio](#)) e esteja pronto para retirada, geralmente entre 13:00 e 15:00, horário local.

AWS Snowcone Pickups em Hong Kong

Em Hong Kong, a S.F. Express processa as retiradas. Quando estiver pronto para devolver seu dispositivo, envie um e-mail para snowball-shipping-ap-east-1@amazon.com com a Solicitação de coleta do Snowcone na linha de assunto para que possamos agendar a coleta para você. No corpo do e-mail, inclua as seguintes informações:

- ID do trabalho
- AWS ID da conta
- Nome de contato
- Número de telefone para contato
- Endereço de e-mail para contato
- O dia em que você quer que o dispositivo seja retirado.
- Horário de coleta preferencial mais cedo
- Último horário de coleta preferencial
- Endereço de coleta

Note

Assim que você organizar a data da retirada com a S.F. Express, não será possível reagendá-la.

O dispositivo será entregue AWS pela S.F. Express. Use o número de rastreamento S.F. Express da remessa de devolução para saber quando a entrega foi concluída.

AWS Snowcone Recolhas na Indonésia, Japão e Cingapura

Na Indonésia, no Japão e em Singapura, quando estiver pronto para devolver o dispositivo, digitalize o código QR exibido na etiqueta E Ink de devolução com o telefone celular. Isso levará você diretamente para um modelo de e-mail. Preencha a data, a hora e os detalhes de contato da coleta.

RETURN

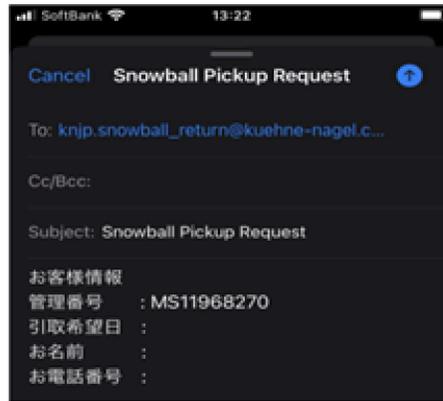
AWS Jobs ID QF6LNZGKTZPF
 シリアル番号 2R 207138750022
 管理番号 MS14003547



返送のご案内

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

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



Prazos de entrega

Cada país tem diferentes prazos de entrega disponíveis. Esses prazos de envio são baseados no país para o qual você está enviando um AWS Snowcone dispositivo. Os prazos de entrega são os seguintes:

- Austrália, Indonésia, Japão, Singapura, Coreia do Sul: ao enviar dentro desses países, você tem acesso à velocidade de envio padrão de 1 a 3 dias.
- Brasil: ao fazer envios para o Brasil, você tem acesso ao envio UPS Domestic Express Saver, que faz entregas em até dois dias úteis durante o horário comercial. Os prazos de entrega podem ser afetados por atrasos de fronteiras interestaduais.
- União Europeia (UE): as remessas para qualquer um dos países da UE também incluem remessa expressa. Normalmente, as remessas expressas do dispositivo Snowcone são entregues em aproximadamente um dia. Além disso, a maioria dos países na UE tem acesso ao envio padrão que geralmente leva menos de uma semana, só de envio.
- Índia — Ao enviar dentro da Índia, AWS Snowcone os dispositivos são enviados dentro de 7 dias úteis após o AWS recebimento de todos os documentos fiscais relacionados.
- Israel: ao enviar em Israel, você tem acesso ao envio no mesmo dia.
- Estados Unidos da América (EUA) e Canadá: ao fazer envios nos EUA ou no Canadá, você tem acesso ao envio de um e dois dias.

- Reino Unido: ao enviar dentro do Reino Unido, você tem acesso ao frete expresso. Normalmente, as remessas expressas do dispositivo Snowcone são entregues em aproximadamente um dia. Além disso, você tem acesso à remessa padrão, que geralmente leva menos de uma semana, apenas o envio.

Atualização de software em dispositivos Snowcone

AWS notificará você quando um novo software estiver disponível para os dispositivos Snow Family que você possui. A notificação é fornecida por e-mail AWS Health Dashboard e como um CloudWatch evento. A notificação por e-mail é enviada pela Amazon Web Services, Inc. para o endereço de e-mail associado à AWS conta usada para solicitar o dispositivo Snow Family. Ao receber a notificação, siga as instruções neste tópico e baixe e instale a atualização o mais rápido possível para evitar a interrupção do uso do dispositivo. Para obter mais informações sobre AWS Health Dashboard, consulte o [Guia AWS Health do usuário](#). Para obter mais informações sobre CloudWatch eventos, consulte o [Guia do usuário do Amazon CloudWatch Events](#).

Você pode baixar atualizações de software AWS e instalá-las em dispositivos Snowcone em seus ambientes locais. Essas atualizações ocorrem em segundo plano. Você pode continuar usando seus dispositivos normalmente enquanto o software mais recente é baixado com segurança AWS para o seu dispositivo. No entanto, para aplicar as atualizações baixadas, você deve interromper a execução dos serviços no dispositivo e reiniciá-lo após a conclusão da atualização.

As atualizações de software fornecidas AWS pelos dispositivos Snowball Edge/Snowcone (Eletrodomésticos) são Software de Aparelho de acordo com a Seção 9 dos Termos de Serviço.

As atualizações de software são fornecidas exclusivamente com a finalidade de instalar as atualizações de software no dispositivo aplicável em nome da AWS. Você não fará (nem tentará) e não permitirá ou autorizará terceiros a (ou tentarão) (i) fazer cópias das atualizações de software além das necessárias para instalar as atualizações de software no Dispositivo aplicável, ou (ii) contornar ou desativar quaisquer atributos ou medidas nas atualizações de software, incluindo, mas não se limitando a, qualquer criptografia aplicada à atualização de software. Depois que as atualizações de software forem instaladas no dispositivo aplicável, você concorda em excluí-las de toda e qualquer mídia utilizada na instalação das atualizações de software no aparelho.

Warning

É altamente recomendável suspender todas as atividades no dispositivo antes de reiniciá-lo. Atualizar o dispositivo e reiniciá-lo interromperá a execução de instâncias e interromperá qualquer gravação nos buckets locais do Amazon S3.

Tópicos

- [Pré-requisitos](#)
- [Download de atualizações](#)
- [Instalação de atualizações](#)
- [Atualizar o certificado SSL](#)
- [Atualizando suas AMIs do Amazon Linux 2 em dispositivos da Família Snow](#)

Pré-requisitos

Antes de atualizar o dispositivo, os seguintes pré-requisitos devem ser atendidos:

- Você criou seu trabalho, tem o dispositivo on-premises e desbloqueado. Para ter mais informações, consulte [Conceitos básicos](#).
- A atualização dos dispositivos Snowcone é feita por meio do Snowball Edge Client. A versão mais recente do cliente Snowball Edge deve ser baixada e instalada em um computador em seu ambiente local que tenha uma conexão de rede com o dispositivo que você deseja atualizar. Para obter mais informações, consulte [Usando o cliente AWS Snowball Edge](#).
- (Opcional) Recomendamos configurar um perfil para o Snowball Edge Client. Para obter mais informações, consulte [Configurando um perfil para o Snowball Edge Client](#).

Agora que concluiu essas tarefas, você pode fazer download e instalar atualizações para dispositivos Snowcone.

Download de atualizações

Há duas maneiras principais de baixar uma atualização para dispositivos da família Snow:

- Você pode acionar atualizações manuais a qualquer momento usando comandos específicos do Snowball Edge.
- Você pode determinar uma hora de forma programática para atualizar o dispositivo automaticamente.

O procedimento a seguir descreve o processo de download manual das atualizações. Para obter informações sobre como atualizar automaticamente seu dispositivo Snowcone, consulte `configure-auto-update-strategy` em [Atualizando um Snowcone](#).

Note

Se seu dispositivo não tiver acesso à Internet, você poderá baixar um arquivo de atualização usando a [GetSoftwareUpdatesAPI](#). Em seguida, aponte para um local de arquivo local ao chamar `download-updates` usando o `uri` parâmetro, como no exemplo a seguir.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Para sistemas operacionais Windows, formate o valor do `uri` parâmetro da seguinte forma:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

Para verificar e fazer download de atualizações de software do Snowcone

1. Abra uma janela de terminal e verifique se o dispositivo do Snowcone está desbloqueado com o comando `describe-device`. Se o dispositivo estiver bloqueado, use o comando `unlock-device` para desbloqueá-lo. Para obter mais informações, consulte [Desbloquear o dispositivo da família Snow](#)
2. Quando o dispositivo estiver desbloqueado, execute o comando `snowballEdge check-for-updates`. Esse comando retorna a versão mais recente disponível do software Snowball Edge, além da versão atual instalada no dispositivo.
3. Se o software do dispositivo estiver desatualizado, execute o comando `snowballEdge download-updates`.

Note

Se seu dispositivo não estiver conectado à Internet, primeiro baixe um arquivo de atualização usando a [GetSoftwareUpdatesAPI](#). Em seguida, execute o `snowballEdge download-updates` comando usando o `uri` parâmetro com um caminho local para o arquivo que você baixou, como no exemplo a seguir.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Para sistemas operacionais Windows, formate o valor do `uri` parâmetro da seguinte forma:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

4. Você pode verificar o status desse download com o comando `snowballEdge describe-device-software`. Enquanto o download de uma atualização estiver sendo feito, o status será exibido com esse comando.

Example saída do **describe-device-software** comando

```
Install State: Downloading
```

Instalação de atualizações

Depois de obter as atualizações por download, você precisa instalá-las e reiniciar o dispositivo para que as atualizações entrem em vigor. O procedimento a seguir fornece instruções para instalar atualizações manualmente.

Note

Suspenda todas as atividades no dispositivo antes de instalar as atualizações de software. A instalação de atualizações interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo. Isso pode resultar em perda de dados

Para instalar atualizações de software que já foram baixadas para dispositivos autônomos da Família Snow

1. Abra uma janela de terminal e verifique se o dispositivo do Snowcone está desbloqueado com o comando `describe-device`. Se o dispositivo estiver bloqueado, use o comando `unlock-device` para desbloqueá-lo. Para obter mais informações, consulte [Desbloquear um dispositivo da família Snow](#).
2. Execute o `list-services` comando para ver os serviços disponíveis no dispositivo. O comando retorna os IDs de cada serviço disponível no dispositivo.

```
snowballEdge list-services
```

Exemplo da saída do **list-services** comando

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

3. Para cada ID de serviço identificado pelo `list-services` comando, execute o `describe-service` comando para ver o status. Use essas informações para identificar serviços a serem interrompidos.

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

Exemplo da saída do **describe-service** comando

```
{
  "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"
```

```

    }
  } ]
}

```

Essa saída mostra que o s3 serviço está ativo e deve ser interrompido usando o `stop-service` comando.

- Use o `stop-service` comando para interromper cada serviço em que o valor do State nome esteja ACTIVE na saída do `list-services` comando. Se mais de um serviço estiver em execução, interrompa cada um antes de continuar.

Note

O adaptador Amazon S3, o Amazon EC2 e os serviços do IAM não AWS STS podem ser interrompidos. Se o armazenamento compatível com Amazon S3 em dispositivos da Família Snow estiver em execução, pare-o antes de instalar as atualizações. O armazenamento compatível com Amazon S3 em dispositivos da família Snow tem `s3-snow` como o `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

```

Exemplo da saída do **stop-service** comando

```

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

```

- Execute o comando `snowballEdge install-updates`.
- Você pode verificar o status dessa instalação com o comando `snowballEdge describe-device-software`. Enquanto uma atualização estiver sendo instalada, o status será exibido com esse comando.

Exemplo de saída

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Você instalou uma atualização de software com êxito em seu dispositivo do Snowcone. A instalação de uma atualização não a aplica automaticamente ao dispositivo. Para concluir a instalação da atualização, o dispositivo deve ser reiniciado.

Warning

A reinicialização do dispositivo da Família Snow sem interromper todas as atividades no dispositivo pode resultar em perda de dados.

7. Quando todos os serviços do dispositivo tiverem parado, reinicie o dispositivo, desbloqueie o dispositivo e reinicie-o novamente. Isso conclui a instalação das atualizações de software baixadas. [Para obter mais informações sobre a reinicialização do dispositivo, consulte Reinicializando o dispositivo da](#) . Para obter mais informações sobre como desbloquear o dispositivo, consulte [Desbloqueando o dispositivo dispositivo da família Snow](#).
8. Quando o dispositivo for ligado após a segunda reinicialização, desbloqueie o dispositivo.
9. Execute o comando `check-for-updates`. Esse comando retorna a versão mais recente disponível do software Snowcone, além da versão atual instalada no dispositivo.

Agora você atualizou com sucesso o dispositivo ou o cluster de dispositivos da Família Snow e confirmou a atualização para o software mais recente da Família Snow.

Atualizar o certificado SSL

Se você planeja manter seu dispositivo Snow Family por mais de 360 dias, precisará atualizar o certificado Secure Sockets Layer (SSL) no dispositivo para evitar a interrupção do uso do dispositivo. Se o certificado expirar, você não poderá usar o dispositivo e precisará devolvê-lo para a AWS.

AWS notificará você 30 dias antes que o certificado SSL expire para os dispositivos Snow Family que você possui. A notificação é fornecida por e-mail AWS Health Dashboard e como um CloudWatch evento. A notificação por e-mail é enviada pela Amazon Web Services, Inc. para o endereço de e-mail associado à AWS conta usada para solicitar o dispositivo Snow Family. Ao receber a notificação, siga as instruções neste tópico e solicite uma atualização o mais rápido possível

para evitar a interrupção do uso do dispositivo. Para obter mais informações sobre AWS Health Dashboard, consulte o [Guia AWS Health do usuário](#). Para obter mais informações sobre CloudWatch eventos, consulte o [Guia do usuário do Amazon CloudWatch Events](#).

Este tópico explica como determinar quando o certificado expirará e como atualizar seu dispositivo.

1. Use o comando `snowballEdge describe-device-software` para determinar quando o certificado expirará. Na saída do comando, o valor de `CertificateExpiry` inclui a data e a hora em que o certificado expirará.

Exemplo da saída `describe-device-software`

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

2. Entre em contato AWS Support e solicite uma atualização do certificado SSL.
3. AWS Support fornecerá um arquivo de atualização. [Baixe](#) e [instale](#) o arquivo de atualização.
4. [Use o novo código de desbloqueio e arquivo de manifesto ao Desbloquear um dispositivo](#).

Atualizando suas AMIs do Amazon Linux 2 em dispositivos da Família Snow

Como melhor prática de segurança, mantenha suas AMIs do Amazon Linux 2 up-to-date em dispositivos da família Snow. Verifique regularmente o [Amazon Linux 2 AMI \(HVM\) e o tipo de volume SSD \(64 bits x86\)](#) no para obter atualizações. AWS Marketplace Ao identificar a necessidade de atualizar sua AMI, importe a imagem mais recente do Amazon Linux 2 para o dispositivo Snow. Consulte [Importação de uma imagem para o seu dispositivo como uma AMI compatível com Amazon EC2](#).

Você também pode obter a ID de imagem mais recente do Amazon Linux 2 usando o comando `ssm get-parameters` no 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
```

O comando retorna a ID de imagem mais recente da AMI. Por exemplo: .

```
ami-0ccb473bada910e74
```

Melhores práticas para o AWS Snowcone dispositivo

Para ajudar a obter o máximo benefício e satisfação com seu AWS Snowcone dispositivo, recomendamos que você siga estas práticas recomendadas.

Tópicos

- [Segurança](#)
- [Rede](#)
- [Gerenciamento de recursos](#)
- [Gerenciamento de instâncias compatíveis com o EC2](#)

Segurança

- Se você notar algo que pareça suspeito no AWS Snowcone dispositivo, não o conecte à sua rede interna. Em vez disso, entre em contato com o [AWS Support](#), e você receberá um novo dispositivo AWS Snowcone .
- Recomendamos não salvar uma cópia do código de desbloqueio no mesmo local na estação de trabalho que o manifesto para esse trabalho. Salvá-los separadamente ajuda a impedir que pessoas não autorizadas tenham acesso ao AWS Snowcone dispositivo. Por exemplo, é possível salvar uma cópia do manifesto no servidor local e enviar o código que desbloqueia o dispositivo por e-mail para um usuário. Essa abordagem limita o acesso ao AWS Snowcone dispositivo a indivíduos que têm acesso aos arquivos salvos no servidor e também ao endereço de e-mail desse usuário.
- As credenciais exibidas ao executar o comando `snowballEdge list-access-keys` do Snowball Edge Client seguido por `snowballEdge get-secret-access-key` são um par de chaves: uma chave de acesso e uma chave secreta. Essas chaves são associadas apenas ao trabalho e aos recursos locais no dispositivo. Eles não são mapeados para o seu Conta da AWS ou para qualquer outro Conta da AWS. Se você tentar usar essas chaves para acessar serviços e recursos no Nuvem AWS, elas falharão, pois funcionam somente para os recursos locais associados ao seu trabalho.
- Você pode restringir o acesso a compartilhamentos do NFS. Para obter detalhes, consulte [Restringindo o acesso aos compartilhamentos NFS quando o NFS está em execução](#).
- Quando você desliga ou liga um dispositivo Snowcone, ele entra em um estado bloqueado.

Rede

- Recomendamos que você use somente um método de leitura e gravação de dados em um bucket local em um AWS Snowcone dispositivo por vez. Uso dos dois

A montagem do NFS e a montagem DataSync no mesmo bucket do S3 ao mesmo tempo podem resultar em conflitos de leitura/gravação.

- Para evitar corromper seus dados, não desconecte um AWS Snowcone dispositivo nem altere suas configurações de rede ao transferir dados.
- Os arquivos devem estar em um estado estático enquanto são gravados no dispositivo. Arquivos que são modificados enquanto estão sendo gravados podem resultar em conflitos de leitura/gravação.
- Para obter mais informações sobre como melhorar o desempenho do seu AWS Snowcone dispositivo, consulte [Desempenho do Snowcone](#).

Gerenciamento de recursos

- Os cinco dias gratuitos para realizar sua transferência de dados no local começam no dia seguinte à chegada do AWS Snowcone dispositivo ao seu data center.

Gerenciamento de instâncias compatíveis com o EC2

Para evitar a exclusão acidental das instâncias compatíveis com o Amazon EC2 criadas em seu dispositivo AWS Snowcone , não encerre as instâncias do sistema operacional. Por exemplo, não use os comandos `shutdown` ou `reboot`. Encerrar uma instância a partir do sistema operacional tem o mesmo efeito que chamar o comando [terminate-instances](#).

Em vez disso, use o comando [stop-instances](#) para suspender as instâncias compatíveis com o Amazon EC2 que você deseja preservar.

Desempenho do Snowcone

A tabela a seguir descreve como a taxa de transferência da sua rede afeta o tempo necessário para preencher uma AWS Snowcone com dados.

| Taxa (MB/s) | Tempo de transferência de 8 TB | Tempo de transferência de 4 TB |
|-------------|--------------------------------|--------------------------------|
| 100 | 21,17 horas | 10,59 horas |
| 60 | 36,57 horas | 18,29 horas |
| 30 | 68,57 horas | 34,29 horas |
| 10 | 210,29 horas | 105,15 horas |

AWS Snowcone cotas

A seguir, você encontrará informações sobre as cotas para uso do seu dispositivo Snowcone.

Armazenamento em disco Snowcone

Internamente, seu dispositivo Snowcone contém 8 TB ou 14 TB de armazenamento em disco que você pode usar com o serviço interno de Network File System (NFS) ou com instâncias locais compatíveis com o Amazon EC2 por meio de uma apresentação de volume local do Amazon Elastic Block Store (Amazon EBS). Você pode usar esse armazenamento para NFS ou Amazon EBS, mas não para ambos. Dependendo de seu caso de uso, é possível alocar o armazenamento. Esteja ciente de que o armazenamento é pré-alocado quando você faz seu pedido do Snowcone.

Armazenamento do trabalho de computação

Se o tipo de trabalho for computação local, você poderá criar um total de 8 TB ou 14 TB de volumes locais do Amazon EBS e anexá-los a instâncias compatíveis com o Amazon EC2. O uso de volumes do Amazon EBS permite que as instâncias locais do Amazon EC2 acessem mais capacidade local do que apenas o volume raiz. Como esse é somente o armazenamento local, os dados gravados nos volumes do Amazon EBS são perdidos quando o dispositivo é devolvido para a AWS, pois não podem ser importados para o Amazon S3.

Tópicos

- [Cotas de recursos computacionais](#)
- [Limitações para enviar um dispositivo Snowcone](#)
- [Limitações de processamento do Snowcone retornado para importação](#)
- [Disponível Regiões da AWS](#)

Cotas de recursos computacionais

Recursos computacionais disponíveis para cotas de dispositivos Snowcone para armazenamento

A tabela a seguir descreve os recursos computacionais disponíveis para dispositivos Snowcone e suas cotas de armazenamento.

| Tipo de instância | Núcleos de vCPU | Memória (GiB) | Cota |
|-------------------|-----------------|---------------|------|
| snc1.micro | 1 | 1 | 2 |
| snc1.small | 1 | 2 | 2 |
| snc1.medium | 2 | 4 | 1 |

Cotas de capacidade da imagem de máquina da Amazon (AMI) e do Amazon EC2 para dispositivos Snowcone

A tabela a seguir descreve as cotas de capacidade de instância compatíveis com AMI e Amazon EC2 para um dispositivo Snowcone.

| Amazon EC2 | Tamanho |
|---|--|
| AMIs compatíveis com Amazon EC2 | 125 GB (o tamanho combinado de todas as AMIs usadas no trabalho de um cliente) |
| Instâncias compatíveis com o Amazon EC2 | 150 GB (representa o espaço disponível para os volumes de armazenamento de apoio das instâncias) |

Limitações para enviar um dispositivo Snowcone

A seguir estão as limitações para o envio de um dispositivo Snowcone:

- AWS não enviará um dispositivo Snowcone para uma caixa postal.
- Mover um dispositivo Snowcone para um endereço fora do país especificado quando o trabalho foi criado não é permitido e representa uma violação dos Termos de serviço da AWS .

Para obter mais informações sobre restrições de envio, consulte [Considerações de envio para AWS Snowcone](#).

Limitações de processamento do Snowcone retornado para importação

Para importar seus dados para o Nuvem AWS, o dispositivo Snowcone deve atender aos seguintes requisitos:

- O dispositivo Snowcone não deve estar comprometido. Exceto para abrir as portas na frente e atrás, não abra o dispositivo Snowcone por nenhum motivo.
- O dispositivo não deve estar fisicamente danificado. Para evitar danos, feche as duas portas do dispositivo Snowcone e pressione até que as travas emitam um som audível de clique.
- A menos que uma etiqueta de remessa seja fornecida pela AWS, a tela E Ink no dispositivo Snowcone deve estar visível e mostrar a etiqueta de devolução que foi gerada automaticamente quando você terminou de transferir seus dados para o dispositivo Snowcone.

Note

Todos os dispositivos Snowcone retornados que não atenderem a esses requisitos são apagados sem o trabalho executado neles.

Disponível Regiões da AWS

Para obter informações sobre os endpoints suportados Regiões da AWS e os endpoints, consulte os [endpoints e cotas da família AWS Snow](#) no. Referência geral da AWS

Solução de problemas no Snowcone

Esta seção fornece orientação e informações sobre o AWS Snowcone dispositivo/serviço para solucionar alguns dos problemas encontrados.

Tópicos

- [Solucionar problemas com instâncias de computação](#)
- [Solução de problemas de rede](#)
- [Solução de problemas da instância compatível com o Amazon EC2 no DataSync](#)
- [Solução de problemas de transferência de dados](#)
- [Solução de problemas na devolução de dispositivos da Família Snow](#)

Solucionar problemas com instâncias de computação

A solução de problemas de instâncias de computação está documentada [aqui](#).

Solução de problemas de rede

O endereço IP é 0.0.0.0

Você está conectado à rede e aos cabos de alimentação, mas o endereço IP do dispositivo mostra 0.0.0.0

Medida a ser tomada

Certifique-se de que o cabeamento entre o Snowcone e os dispositivos de rede seja verificado corretamente.

Se o dispositivo ainda não mostrar um endereço IP, verifique se há problemas relacionados ao mau funcionamento ou à configuração do roteador que possam levar à falha na configuração do IP.

Se a rede não tiver o DHCP ativado, certifique-se de configurar um IP estático no dispositivo usando a opção STATIC do monitor Snowcone e programando o dispositivo com o endereço IP estático apropriado.

Não é possível desbloquear o dispositivo

Você não consegue desbloquear o dispositivo usando o OpsHub cliente Snowball edge.

Medida a ser tomada

Certifique-se de que o cliente esteja na mesma sub-rede e na mesma rede do dispositivo AWS Snowcone .

Se o Snowcone tiver várias atribuições de endereço IP (por exemplo, WiFi e Ethernet), verifique se você está usando o mesmo endereço IP para se conectar se vários clientes estiverem tentando responder ao Snowcone. Observe que é possível usar apenas uma interface de cada vez.

Se as etapas acima não funcionarem, AWS Support forneça os registros do dispositivo. Use o cliente Snowball Edge e o comando: `SnowballEdge get-support-logs`

Solução de problemas da instância compatível com o Amazon EC2 no DataSync

Erro: falha ao iniciar a instância

O Snowcone não tem capacidade suficiente para iniciar a instância para essa solicitação.

Medida a ser tomada

Os requisitos para execução DataSync em um AWS Snowcone dispositivo como agente usam a instância padrão `snc1.medium`, que fornece 2 núcleos de CPU e 4 GiB de memória. Certifique-se de ter atributos suficientes no dispositivo Snowcone para provisionar a nova solicitação de execução de instância compatível com Amazon EC2.

Solução de problemas de transferência de dados

Acesso negado pelo servidor

Erro: `mount.nfs - acesso negado pelo servidor ao montar 192.168.1.214`

Medida a ser tomada

Se você configurou o NFS usando a configuração rápida, por padrão, somente seu sistema terá acesso para transferir arquivos para esse dispositivo. Se você quiser permitir que outros hosts carreguem dados para o Snowcone, desative o serviço NFS e reative o serviço com a lista de endereços IP que você deseja permitir na configuração do NFS.

Tempo limite de conexão durante a transferência de dados

A conexão expira ao tentar transferir dados para AWS Snowcone usar a interface do Amazon S3 (AWS CLI via).

Razão para esse comportamento esperado

O AWS Snowcone dispositivo só suporta transferências por meio do suporte NFS para transferências offline e AWS DataSync transferências on-line; a interface do Amazon S3 não é suportada atualmente. Isso explicaria por que você enfrenta tempos limite ao se conectar usando o AWS CLI.

Spawn Showmount ENOENT

Error: Uncaught Error - spawn showmount ENOENT. É uma abreviatura de Error NO ENTRY (ou Error NO ENTity) e, na verdade, pode ser usado para mais do que arquivos/diretórios.

Medida a ser tomada

Este erro poderá ocorrer se o cliente NFS não estiver sendo executado na estação de trabalho. Se o serviço NFS não tiver sido iniciado antes da configuração do NFS no AWS OpsHub, você poderá ver esse erro.

Em um cliente Windows, você pode verificar se o Serviço NFS está em execução executando as seguintes etapas:

1. No computador cliente, abra Iniciar, escolha Painel de Controle e selecione Programas.
2. Escolha Ativar ou desativar atributos do Windows.
3. Em Serviços para NFS, escolha Cliente para NFS e selecione OK. Referência: [montagem do NFS em um cliente Windows](#)

Esse erro também pode ocorrer se houver um firewall/antivírus entre a estação de trabalho em execução AWS OpsHub e o dispositivo que possa bloquear a conexão.

Na estação de trabalho, execute o comando telnet to the AWS Snowcone device IP address na porta NFS número 2049 para verificar se a conexão foi estabelecida com êxito.

Solução de problemas na devolução de dispositivos da Família Snow

Às vezes, depois de desligar o dispositivo da Família Snow para se preparar para devolvê-lo, as informações do frete de devolução não aparecem na tela E Ink.

Medida a ser tomada

1. Faça login no Console de Gerenciamento da família AWS Snow.
2. Veja o trabalho do dispositivo.
3. Na seção Detalhes, na seção Etiqueta de devolução, escolha Para visualizar e imprimir sua etiqueta de devolução, siga este link.
4. Imprima a etiqueta e coloque-a no dispositivo.
5. Devolva o dispositivo de acordo com [Devolvendo um dispositivo Snowcone](#).

Referência da API de gerenciamento de trabalhos

- [Referência da API de gerenciamento de trabalhos](#)
 - [Ações](#)
 - [Tipos de dados](#)
 - [Parâmetros gerais](#)
 - [Erros comuns](#)

Histórico do documento para guia AWS Snowcone do usuário

A tabela a seguir descreve a documentação desta versão do AWS Snowcone.

- Versão da API: mais recente
- Última atualização da documentação: 25 de agosto de 2023

| Alteração | Descrição | Data |
|--|--|------------------------|
| Inclua AMIs personalizadas ao solicitar dispositivos | Agora, as imagens personalizadas da Amazon Machine podem ser pré-carregadas durante o pedido AWS Snow Family de trabalhos. Para obter mais informações, consulte Usando o Amazon EC2 no Snowcone . | 15 de novembro de 2023 |
| Novo Região da AWS suporte | AWS Snowcone Os dispositivos SSD agora estão disponíveis em Israel (Tel Aviv). Região da AWS As informações de retirada para essa região foram adicionadas. Para obter mais informações, consulte endpoints e cotas do AWS Snow Family na Referência geral da AWS. Para obter informações sobre frete, consulte Considerações de envio para o AWS Snowcone . | 25 de agosto de 2023 |

| | | |
|--|--|-------------------------|
| <u>Novo Região da AWS suporte</u> | Os dispositivos Snowcone estão agora disponíveis na Europa (Paris). Região da AWS Para obter mais informações, consulte <u>endpoints e cotas do AWS Snow Family</u> na Referência geral da AWS. Para obter informações sobre frete, consulte <u>Considerações de envio para o AWS Snowcone</u> . | 29 de junho de 2022 |
| <u>Novas dicas de solução de problemas do Snowcone</u> | AWS Snowcone seção de dicas de solução de problemas adicionada semelhante ao Snowball Edge. Para ver a nova seção adicionada, consulte <u>Solução de problemas do Snowcone</u> . | 15 de abril de 2022 |
| <u>Novo Região da AWS suporte</u> | AWS Snowcone agora está disponível nas regiões Ásia-Pacífico (Mumbai) e Brasil. Foram adicionadas informações de coleta para a UE, Canadá, Singapura e Brasil. Para obter mais informações, consulte <u>Endpoints e cotas da Família AWS Snow</u> na Referência geral da AWS. | 23 de fevereiro de 2022 |

| | | |
|---|---|------------------------|
| Novo Região da AWS suporte | AWS Snowcone agora está disponível na região Europa (Londres). Para obter mais informações, consulte Endpoints e cotas da Família AWS Snow na Referência geral da AWS. | 5 de janeiro de 2022 |
| Suporte para configuração do servidor NTP (Network Time Protocol) | Os dispositivos Snowcone agora oferecem suporte externo de configuração de servidor NTP (Network Time Protocol). | 16 de novembro de 2021 |
| Novo Região da AWS suporte | AWS Snowcone O SSD agora está disponível nas regiões Oeste dos EUA (Norte da Califórnia), Leste dos EUA (Ohio), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Sydney). Para obter mais informações, consulte Endpoints e cotas da Família AWS Snow na Referência geral da AWS. | 3 de novembro de 2021 |
| Novo Região da AWS suporte | AWS Snowcone agora está disponível nas regiões Oeste dos EUA (Norte da Califórnia), Leste dos EUA (Ohio) e América do Sul (São Paulo). Para obter mais informações, consulte Endpoints e cotas da Família AWS Snow na Referência geral da AWS. | 29 de setembro de 2021 |

[Novo Região da AWS suporte](#)

AWS Snowcone agora está disponível nas regiões Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio). Para obter mais informações, consulte [Endpoints e cotas da Família AWS Snow](#) na Referência geral da AWS.

26 de agosto de 2021

[Suporte para exportação de dados off-line do Amazon S3 usando dispositivos Snowcone](#)

Agora você pode solicitar AWS a exportação de seus dados do Amazon S3 transferindo-os para dispositivos Snowcone, que são então enviados fisicamente para sua localização. Para obter mais informações, consulte [Como funcionam os trabalhos de importação e exportação](#).

4 de agosto de 2021

[Apresentando AWS Snow Device Management](#)

O Snow Device Management permite que você gerencie seu AWS Snowcone dispositivo e AWS serviços locais remotamente. Todos os dispositivos Snowcone oferecem suporte ao Snow Device Management e ele vem pré-instalado em novos dispositivos na maioria dos lugares em que o Regiões da AWS Snowcone está disponível. Para obter mais informações, consulte [Usando AWS Snow Device Management para gerenciar dispositivos](#).

4 de agosto de 2021

[Novo Região da AWS suporte](#)

AWS Snowcone agora está disponível na região do Canadá (Central). Para obter mais informações, consulte [Endpoints e cotas da Família AWS Snow](#) na Referência geral da AWS.

28 de abril de 2021

[Novo Região da AWS suporte](#)

AWS Snowcone agora está disponível na região Ásia-Pacífico (Sydney). Para obter mais informações, consulte [Endpoints e cotas da Família AWS Snow](#) na Referência geral da AWS.

24 de março de 2021

[Suporte para interface de rede direta](#)

AWS Snowcone agora adiciona a configuração de interface de rede direta (DNI), um recurso de rede avançado que permite casos de uso como fluxos multicast, roteamento e balanceamento de carga. Para obter mais informações, consulte [Configuração de rede para instâncias de computação.](#)

12 de janeiro de 2021

[Novo Região da AWS suporte](#)

AWS Snowcone agora está disponível na região da Europa (Frankfurt). Para obter mais informações, consulte [Endpoints e cotas da Família AWS Snow](#) na Referência geral da AWS.

18 de novembro de 2020

[Novo Região da AWS suporte](#)

AWS Snowcone agora está disponível na região Europa (Irlanda). Para obter mais informações, consulte [Endpoints e cotas da Família AWS Snow](#) na Referência geral da AWS.

16 de setembro de 2020

[Apresentando AWS Snowcone](#)

AWS Snowcone é um dispositivo portátil, robusto e seguro para computação de ponta e transferência de dados. Você pode usar AWS Snowcone para coletar, processar e mover dados para AWS, seja offline, enviando o dispositivo para AWS, ou usando on-line AWS DataSync. Para obter mais informações, consulte [O que é o AWS Snowcone?](#)

17 de junho de 2020

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o [AWS glossário](#) na Glossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.