Unable to locate subtitle

AWS Snowball Edge Guia do desenvolvedor

AWS Snowball Edge Guia do desenvolvedor: ***Unable to locate subtitle***

Table of Contents

O que é AWS Snowball Edge?

AWS Snowball O Edge é um tipo de dispositivo Snowball com armazenamento integrado e capacidade de computação para recursos selecionados. AWS O Snowball Edge pode assumir workloads de computação de borda e processamento locais além de transferir dados entre o ambiente local e a Nuvem AWS.

Cada dispositivo Snowball Edge pode transportar dados em velocidades mais rápidas do que a internet. Esse transporte é feito enviando os dados nos dispositivos através de uma empresa de remessa regional. Os dispositivos são resistentes, complementados com etiquetas de envio E Ink.

Os dispositivos Snowball Edge têm quatro opções para configurações de dispositivos: armazenamento otimizado, otimizado para computação e otimizado para computação com GPU. Quando este guia faz referência a dispositivos Snowball Edge, ele se refere a todas as opções do dispositivo. Quando informações específicas se aplicam apenas a uma ou mais configurações opcionais de dispositivos (como o Snowball Edge com GPU ter uma GPU integrada), elas são mencionadas de forma específica. Para ter mais informações, consulte Opções do dispositivo Snowball Edge.

Tópicos

AWS Snowball Características do Edge

O dispositivos Snowball Edge têm os seguintes recursos:

- Grandes quantidades de capacidade de armazenamento ou funcionalidade de computação para dispositivos. Isso depende das opções selecionadas ao criar o trabalho.

- Adaptadores de rede com velocidades de transferência de até 100 Gbit/segundo.
- A criptografia é aplicada protegendo os dados ociosos e em trânsito físico.
- É possível importar ou exportar dados entre os ambientes locais e o Amazon S3 e transportar fisicamente os dados com um ou mais dispositivos, sem necessidade de utilizar a internet.
- Os dispositivos Snowball Edge são sua própria caixa resistente. A tela E link incorporada é alterada para mostrar a etiqueta de remessa quando o dispositivo está pronto para ser enviado.
- Os dispositivos Snowball Edge são fornecidos com um monitor LCD integrado que pode ser usado para gerenciar conexões de rede e obter informações de status do serviço.
- É possível agrupar dispositivos Snowball Edge para trabalhos de armazenamento e computação locais, a fim de atingir durabilidade de dados em 3 a 16 dispositivos e aumentar e diminuir localmente o armazenamento sob demanda.
- É possível usar o Amazon EKS Anywhere em dispositivos Snowball Edge para workloads do Kubernetes.
- Os dispositivos Snowball Edge têm endpoints compatíveis com o Amazon S3 e o Amazon EC2 disponíveis, permitindo casos de uso programáticos.
- Os dispositivos Snowball Edge são compatíveis com os novos tipos de instância `sbe1`, `sbe-c` e `sbe-g`, que podem ser usados para executar instâncias de computação no dispositivo utilizando imagens de máquina da Amazon (AMIs).
- O Snowball Edge é compatível com os seguintes protocolos de transferência de dados para migração de dados:
  - NFSv3
  - NFSv4
  - NFSv4.1
  - Amazon S3 via HTTP ou HTTPS (via API compatível com a AWS CLI versão 1.16.14 e anteriores)

Pré-requisitos para usar dispositivos da Família Snow

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

   Durante a criação da conta, você vai receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e utilize somente o usuário raiz para executar as tarefas que exigem acesso do usuário raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Login como usuário administrativo

- Para fazer login com o usuário do Centro de Identidade do IAM, utilize o URL de login enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Pré-requisitos para usar o adaptador do Amazon S3 em dispositivos da Família Snow para trabalhos de importação e exportação

Você usará o adaptador do S3 em dispositivos da Família Snow quando estiver usando os dispositivos para mover dados de fontes de dados on-premises para a nuvem ou da nuvem para o armazenamento de dados on-premises.

> **Note**
>
> É necessário selecionar o adaptador do S3 no Snow ao solicitar dispositivos. Consulte Etapa 2: Selecionar as opções de computação e armazenamento neste guia.

O bucket do Amazon S3 associado ao trabalho deve usar a classe de armazenamento do Amazon S3 Standard. Antes de criar o primeiro trabalho, lembre-se do seguinte.

Para trabalhos que importam dados para o Amazon S3, siga estas etapas:

- Confirme se os arquivos e as pastas a serem transferidos têm nomes que seguem as diretrizes de nomeação de chave de objeto do Amazon S3. Os arquivos ou as pastas com nomes que não estiverem de acordo com essas diretrizes não serão importados para o Amazon S3.

- Planeje os dados que você deseja importar para o Amazon S3. Para ter mais informações, consulte Planejar transferências de grande porte.

Antes de exportar dados do Amazon S3, siga estas etapas:

- Entenda quais dados serão exportados ao criar o trabalho. Para ter mais informações, consulte Utilização de intervalos de exportação.
- Para todos os arquivos com dois-pontos (`:`) no nome, altere os nomes no Amazon S3 antes de criar o trabalho de exportação para obter esses arquivos. Arquivos com dois pontos no nome não são exportados para o Microsoft Windows Server.

Pré-requisitos para usar armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

Você usará o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow quando estiver armazenando dados no dispositivo no local da borda e usando os dados para operações computacionais locais. Para migrar dados de ou para AWS, configure um trabalho de exportação ou importação e use o adaptador Amazon S3.

Ao solicitar um dispositivo Snow para computação e armazenamento locais com armazenamento compatível com o Amazon S3, lembre-se do seguinte:

- Você provisionará a capacidade de armazenamento do Amazon S3 ao pedir o dispositivo. Portanto, pense na necessidade de armazenamento antes de pedir um dispositivo.
- É possível criar buckets do Amazon S3 no dispositivo depois de recebê-lo em vez de ao fazer o pedido de um dispositivo da Família Snow.
- Você precisará baixar a versão mais recente do cliente Snowball Edge AWS CLI (v2.11.15 ou superior) ou AWS OpsHub instalá-la em seu computador para usar o armazenamento compatível com Amazon S3 em dispositivos da família Snow.
- Depois de receber o dispositivo, configure, inicie e use o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, de acordo com Usar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow neste guia.

Pré-requisitos para usar instância de computação em dispositivos da Família Snow

Em trabalhos que usem instâncias de computação, para adicionar qualquer AMI ao trabalho, é necessário ter uma AMI na Conta da AWS e ela deve ser de um tipo de imagem compatível. No momento, as AMIs compatíveis são baseadas nos seguintes sistemas operacionais:

- Amazon Linux 2
- CentOS 7 (x86_64): com atualizações HVM
- Ubuntu 16.04 LTS: Xenial (HVM)
- Ubuntu 20.04 LTS: Focal
- Ubuntu 22.04 LTS: Jammy
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

> **Note**
>
> Ubuntu 16.04 LTS - As imagens Xenial (HVM) não são mais suportadas no AWS Marketplace, mas ainda têm suporte para uso em dispositivos Snowball Edge por meio do Amazon EC2 VM Import/Export e executadas localmente em AMIs.

É possível obter essas imagens no AWS Marketplace.

Se você estiver usando SSH para se conectar às instâncias em execução em um Snowball Edge, poderá usar o próprio par de chaves ou criar um no Snowball Edge. Para usar AWS OpsHub para criar um par de chaves no dispositivo, consulteTrabalhar com pares de chaves. Para usar o AWS CLI para criar um par de chaves no dispositivo, consulte `create-key-pair` emLista de comandos da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge. Para obter mais informações sobre pares de chave e o Amazon Linux 2, consulte Pares de chaves do Amazon EC2 e instâncias do Linux no Manual do usuário para instâncias do Linux do Amazon EC2.

Para obter informações específicas sobre o uso de instâncias de computação em um dispositivo, consulte Usar instâncias de computação compatíveis com o Amazon EC2.

Serviços relacionados ao AWS Snowball Edge

Você pode usar um AWS Snowball Edge dispositivo com os seguintes AWS serviços relacionados:

- Adaptador Amazon S3 — Use para transferência programática de dados para dentro e para fora do AWS uso da API Amazon S3 para Snowball Edge, que suporta um subconjunto de operações de API do Amazon S3. Nessa função, os dados são transferidos para o dispositivo Snow AWS em seu nome e o dispositivo é enviado para você (para um trabalho de exportação), ou AWS envia um dispositivo Snow vazio para você e você transfere dados de suas fontes locais para o dispositivo e os envia de volta para AWS (para um trabalho de importação)”
- Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow: use para atender às necessidades de dados de serviços computacionais, como o Amazon EC2, o Amazon EKS Anywhere no Snow, entre outros. Esse recurso está disponível nos dispositivos Snowball Edge e fornece um conjunto expandido de APIs do Amazon S3 e recursos como maior resiliência com configuração flexível de cluster para 3 a 16 nós, gerenciamento local de buckets e notificações locais.
- Amazon EC2: execute instâncias computacionais em um dispositivo Snowball Edge usando o endpoint compatível com o Amazon EC2, que aceita um subconjunto das operações da API do Amazon EC2. Para obter mais informações sobre como usar o Amazon EC2 na AWS, consulte Conceitos básicos de instâncias do Amazon EC2 para Linux.
- Amazon EKS Anywhere no Snow: cria e opera clusters do Kubernetes em dispositivos da Família Snow. Consulte Usando o Amazon EKS Anywhere on AWS Snow.
- AWS Lambda desenvolvido por AWS IoT Greengrass — Invoque as funções do Lambda com base no armazenamento compatível com Amazon S3 em dispositivos da família Snow, ações de armazenamento feitas em um dispositivo. AWS Snowball Edge Para obter mais informações sobre o uso do Lambda, consulte Usando AWS Lambda com um AWS Snowball Edge e o Guia do desenvolvedor do AWS Lambda.
- Amazon Elastic Block Store (Amazon EBS): oferece volumes de armazenamento ao nível do bloco para usar com instâncias compatíveis com o EC2. Para obter mais informações, consulte Amazon Elastic Block Store (Amazon EBS).
- AWS Identity and Access Management (IAM) — Use esse serviço para controlar com segurança o acesso aos AWS recursos. Para obter mais informações, consulte O que é IAM?
- AWS Security Token Service (AWS STS) — Solicite credenciais temporárias com privilégios limitados para usuários do IAM ou para usuários que você autentica (usuários federados). Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

- Amazon EC2 Systems Manager: use esse serviço para visualizar e controlar a infraestrutura na AWS. Para obter mais informações, consulte O que é o AWS Systems Manager?

Acessar o serviço

Você pode usar o Console de Gerenciamento da família AWS Snow ou a API de gerenciamento de trabalhos para criar e gerenciar trabalhos. Para obter informações sobre a API de gerenciamento de trabalhos, consulte Referência da API de gerenciamento de trabalhos do AWS Snowball.

Acessar um dispositivo AWS Snowball Edge

Depois que o dispositivo Snowball Edge estiver no local, você poderá configurá-lo com um endereço IP usando a tela LCD e, em seguida, desbloqueá-lo usando o cliente do Snowball Edge ou o AWS OpsHub for Snow Family. Depois, é possível executar tarefas de transferência de dados ou computação de borda. Para ter mais informações, consulte Usando um dispositivo AWS Snowball Edge.

Preços do AWS Snowball Edge

Para obter informações sobre a definição de preço e as taxas associadas ao serviço e os dispositivos, consulte .Preços do AWS Snowball Edge .

Monitoramento de dispositivos

AWS monitorará o dispositivo Snow e poderá coletar métricas e informações de uso quando o dispositivo Snow estiver conectado a um Região da AWS. Se o dispositivo Snow não estiver conectado ao Região da AWS, então não AWS monitorará o dispositivo Snow.

Se AWS detectar um problema irreparável, e houver necessidade de substituir o equipamento físico, AWS notificará você. Em seguida, você pode fazer um trabalho de substituição que enviaremos para o seu site. Não há cobrança adicional por isso, pois o monitoramento do dispositivo Snow está incluído como parte da taxa de serviço do dispositivo Snow.

Você é um AWS Snowball usuário iniciante?

Se você é um usuário iniciante do serviço AWS Snow Family, recomendamos que você leia as seguintes seções na ordem:

1. Para obter informações sobre os tipos e as opções de dispositivos, consulte AWS Snowball Diferenças do dispositivo Edge.
2. Para saber mais sobre os tipos de trabalho, consulte Noções básicas sobre trabalhos do AWS Snowball Edge.
3. Para obter uma end-to-end visão geral de como usar um AWS Snowball Edge dispositivo, consulteComo o AWS Snowball Edge funciona.
4. Quando estiver pronto para começar, consulte Conceitos básicos.
5. Para obter informações sobre o uso de instâncias de computação em um dispositivo, consulte Usar instâncias de computação compatíveis com o Amazon EC2.

AWS Snowball Diferenças do dispositivo Edge

Este guia contém documentação para dispositivos Snowball Edge. Você pode usar esses dispositivos para mover terabytes de dados enviados e recebidos do Amazon S3. Você pode solicitá-los usando a API de gerenciamento de trabalhos ou o console da Família AWS Snow. Para obter as perguntas frequentes e informações sobre preços, consulte AWS Snowball.

Tópicos

- Opções do dispositivo Snowball Edge
- AWS Snow Family diferenças de casos de uso
- AWS Diferenças de ferramentas da família Snow

Opções do dispositivo Snowball Edge

Os dispositivos Snowball Edge têm as seguintes opções para configurações de dispositivo:

- Snowball Edge otimizado para armazenamento (para transferência de dados) — Essa opção de dispositivo Snowball Edge tem 80 TB de capacidade de armazenamento utilizável.
- 210 TB otimizado para armazenamento do Snowball Edge — Essa opção de dispositivo Snowball Edge tem 210 TB de capacidade de armazenamento utilizável.
- Snowball Edge otimizado para armazenamento (com funcionalidade computacional compatível com EC2) — Essa opção de dispositivo Snowball Edge tem até 80 TB de capacidade de armazenamento utilizável, 40 vCPUs e 80 GB de memória para funcionalidade computacional. Ele também vem com 1 TB de capacidade adicional de armazenamento SSD para volumes de blocos conectados a AMIs compatíveis com Amazon EC2.

- Snowball Edge otimizado para computação: esse dispositivo Snowball Edge (com AMD EPYC 2ª geração) tem a maior funcionalidade computacional, com até 104 vCPUs, 416 GB de memória e 28 TB de SSD NVMe dedicado para instâncias de computação.

  O Snowball Edge otimizado para computação (com AMD EPYC Gen1) tem até 52 vCPUs, 208 GB de memória, 39,5 TB de capacidade de armazenamento utilizável e 7,68 TB de SSD NVMe dedicado para instâncias de computação.
- Snowball Edge otimizado para computação com GPU: essa opção de dispositivo Snowball Edge é idêntica à opção otimizada para computação (com AMD EPYC 1ª geração) e inclui uma unidade de processamento gráfico (GPU) instalada. A GPU é equivalente à disponível no tipo de instância P3 compatível com o Amazon EC2.

> **Note**
>
> Ao usar o armazenamento compatível com o Amazon S3 em dispositivos da família Snow nesses dispositivos, o armazenamento utilizável variará. Consulte Uso do armazenamento compatível com o Amazon S3 em dispositivos da família Snow em dispositivos da família Snow para obter capacidade de armazenamento com armazenamento compatível com o Amazon S3 em dispositivos da família Snow.

Para obter mais informações sobre a funcionalidade de computação dessas três opções, consulte Usar instâncias de computação compatíveis com o Amazon EC2. A criação de trabalhos e as diferenças de capacidade de disco em terabytes são descritas aqui.

> **Note**
>
> Quando nos referimos aos dispositivos Snowball Edge, isso inclui todas as variantes opcionais do dispositivo. Quando as informações se aplicarem apenas a uma ou mais configurações opcionais (como no caso de a opção Snowball Edge otimizado para computação com GPU ter uma GPU periférica integrada), mencionaremos explicitamente.

A tabela a seguir resume as diferenças entre as várias opções de dispositivo. Para obter informações sobre especificação de hardware, consulte Especificações do dispositivo AWS Snowball Edge.

	Snowball Edge otimizado para armazenamento (para transferência de dados)	Snowball Edge de 210 TB otimizado para armazenamento	Snowball Edge otimizado para armazenamento (com funcionalidade de computação do EC2)	Snowball Edge otimizado para computação com AMD EPYC 2ª geração e NVME	Snowball Edge otimizado para computação com AMD EPYC 1ª geração, HDD e GPU opcional
CPU	AMD Naples, 32 núcleos, 3,4 Ghz	AMD Rome, 64 núcleos, 2 GHz	AMD Naples, 32 núcleos, 3,4 Ghz	AMD Rome, 64 núcleos, 2 GHz	AMD Naples, 32 núcleos, 3,4 Ghz
vCPUs	40	104	40	104	52
Memória utilizável	80 GB	416 GB	80 GB	416 GB	208 GB
Cartão de segurança	Sim	Sim	Sim	Sim	Sim
GPU (opcional)	Nenhum	Nenhum	Nenhum	Nenhum	NVidia V100
SSD	SATA de 1 TB	NVMe de 210 TB	SATA de 1 TB	NVMe de 210 TB	NVMe de 7,68 TB
HDD utilizável	80 TB	Não aplicável	80 TB	Não aplicável	39,5 TB utilizáveis
Interfaces de rede	• 2x 10 Gbit — RJ45 (um utilizável) • 1x 25 Gbit – SFP28	• 2x 10 Gbit — RJ45 (um utilizável) • 1x 25 Gbit – SFP28	• 2x 10 Gbit — RJ45 (um utilizável) • 1x 25 Gbit – SFP28	• 2x 10 Gbit — RJ45 (um utilizável) • 1x 25 Gbit – SFP28	• 2x 10 Gbit — RJ45 (um utilizável) • 1x 25 Gbit – SFP28

	Snowball Edge otimizado para armazenamento (para transferência de dados)	Snowball Edge de 210 TB otimizado para armazenamento	Snowball Edge otimizado para armazenamento (com funcionalidade de computação do EC2)	Snowball Edge otimizado para computação com AMD EPYC 2ª geração e NVME	Snowball Edge otimizado para computação com AMD EPYC 1ª geração, HDD e GPU opcional
	• 1x 100 Gbit: QSFP28	• 1x 100 Gbit: QSFP28	• 1x 100 Gbit: QSFP28	• 1x 100 Gbit: QSFP28	• 1x 100 Gbit: QSFP28

	Snowball Edge otimizado para armazenamento (para transferência de dados)	Snowball Edge de 210 TB otimizado para armazenamento	Snowball Edge otimizado para armazenamento (com funcionalidade de computação do EC2)	Snowball Edge otimizado para computação com AMD EPYC 2ª geração e NVME	Snowball Edge otimizado para computação com AMD EPYC 1ª geração, HDD e GPU opcional
Recursos de segurança física	• Parafusos magnéticos ocultos • Interruptores de intrusão • Tags NFC • Dispositivos anti-adulteração • Aplicativo Android para detecção de adulteração • GPS e celular • Revestimento isolante	• Parafusos magnéticos ocultos • Interruptores de intrusão • Tags NFC • Dispositivos anti-adulteração • Aplicativo Android para detecção de adulteração • Revestimento isolante	• Parafusos magnéticos ocultos • Interruptores de intrusão • Tags NFC • Dispositivos anti-adulteração • Aplicativo Android para detecção de adulteração • GPS e celular • Revestimento isolante	• Parafusos magnéticos ocultos • Interruptores de intrusão • Tags NFC • Dispositivos anti-adulteração • Aplicativo Android para detecção de adulteração • Revestimento isolante	• Parafusos magnéticos ocultos • Interruptores de intrusão • Tags NFC • Dispositivos anti-adulteração • Aplicativo Android para detecção de adulteração • Revestimento isolante

AWS Snow Family diferenças de casos de uso

A tabela a seguir mostra os casos de uso de diferentes AWS Snow Family devices.

Caso de uso	Snowball Edge	AWS Snowcone	
Importar dados para o Amazon S3	✓	✓	
Exportar do Amazon S3	✓		
Armazenamento local durável	✓		
Computação local com AWS Lambda	✓	✓	
Instâncias de computação locais	✓	✓	
Armazenamento durável do Amazon S3 em um cluster de dispositivos	✓		
Use com AWS IoT Greengrass (IoT)	✓	✓	
Transferir arquivos por meio de NFS com uma interface gráfica	✓	✓	
Workloads da GPU	✓		

> **Note**
>
> As workloads que precisam de suporte da GPU exigem a opção Snowball Edge otimizado para computação com GPU.

O Snowball Edge de 210 TB otimizado para armazenamento suporta transferência de dados via NFS, adaptador S3 e armazenamento compatível com Amazon S3 em dispositivos da família Snow.

AWS Diferenças de ferramentas da família Snow

A seguir você encontra uma descrição das diferentes ferramentas usadas com os dispositivos da Família Snow e de como elas são usadas.

Ferramentas do Snowball Edge

AWS OpsHub for Snow Family

- Os dispositivos da família Snow agora oferecem uma ferramenta fácil de usar chamada AWS OpsHub for Snow Family, que você pode usar para gerenciar seus dispositivos e AWS serviços locais. Você pode usar 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. Para obter mais informações, consulte Using AWS OpsHub for Snow Family to Manage Snowball Devices.

Cliente Snowball Edge com Snowball Edge

- Baixe o cliente Snowball Edge na página AWS Snowball Edge Recursos e instale-o em seu próprio computador.
- Use o cliente Snowball Edge para desbloquear o Snowball Edge ou o cluster de dispositivos Snowball Edge. Para ter mais informações, consulte Utilização do Snowball Edge Client.
- Não é possível usar o cliente Snowball Edge para transferir dados de ou para dispositivos da Família Snow.

Adaptador Amazon S3 com Snowball Edge

- Use o adaptador Amazon S3 para transferência de dados de ou para. AWS
- Já vem instalado no Snowball Edge por padrão para exportar ou importar trabalhos. Não precisa ser baixado nem instalado.
- É possível transferir dados para ou do Snowball Edge. Para ter mais informações, consulte Transferência de arquivos usando o adaptador do Amazon S3 para migração de dados.

- Criptografa dados no Snowball Edge enquanto os dados são transferidos para o dispositivo.

Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

- Use armazenamento compatível com Amazon S3 em dispositivos da família Snow para operações de computação e armazenamento de ponta.
- O serviço de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow é instalado em um dispositivo Snowball Edge quando escolhido durante a criação do trabalho. Para configurar, iniciar e usar o serviço, consulte Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow neste guia.

AWS IoT Greengrass console com Snowball Edge

- Com o Snowball Edge, você pode usar o AWS IoT Greengrass console para atualizar seu AWS IoT Greengrass grupo e o núcleo em execução no Snowball Edge.

Itens fornecidos para Snowball Edge

Veja a seguir as diferenças entre adaptadores de rede, cabos usados e cabos fornecidos para o dispositivo Snowball Edge.

Interface de rede	Suporte do Snowball Edge	Cabos fornecidos com o dispositivo	
RJ45	✓	Não fornecido.	
SFP28	✓	Não fornecido.	
SFP28 (com conector óptico)	✓	Não há cabos fornecidos. Não há conectores ópticos fornecidos com os dispositivos Snowball Edge.	
QSFP	✓	Não há cabos ou ópticos fornecidos.	

Para obter mais informações sobre interfaces de rede, cabos e conectores, consulte Hardware de rede suportado.

Como o AWS Snowball Edge funciona

AWS Snowball Os dispositivos Edge são AWS de propriedade e residem em sua localização local enquanto estão em uso.

Há quatro tipos de trabalho que você pode usar com um AWS Snowball Edge dispositivo. Embora os tipos de trabalho sejam diferentes quanto aos seus casos de uso, cada tipo de trabalho tem o mesmo fluxo de trabalho para como solicitar, receber e devolver os dispositivos. Independentemente do tipo de trabalho, após a conclusão de cada um, é realizado o apagamento dos dados de acordo com o padrão 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

O fluxo de trabalho compartilhado

1. Crie o trabalho: cada trabalho é criado no Console de Gerenciamento da família AWS Snow ou de modo programático por meio da API de gerenciamento de trabalhos. O status de um trabalho pode ser monitorado no console ou por meio da API.
2. Um dispositivo é preparado para o trabalho: preparamos um dispositivo AWS Snowball Edge para o trabalho e o status do trabalho agora é Preparando o Snowball.
3. Um dispositivo é enviado a você pela transportadora da região: a transportadora assume o processo a partir daqui, e o status do trabalho agora é Em trânsito. Você pode localizar o número de rastreamento e um link para o site de rastreamento no console ou com a API de gerenciamento de trabalhos. Para obter informações sobre qual é a transportadora da região, consulte Considerações de envio para dispositivos da Família Snow.
4. Receba o dispositivo — Alguns dias depois, a operadora da sua região entrega o AWS Snowball Edge dispositivo no endereço que você forneceu quando criou o trabalho, e o status do seu trabalho muda para Entregue a você. Quando chegar, você verá que ele não veio em uma caixa, porque o dispositivo é seu próprio contêiner de envio.
5. Obter as credenciais e baixar o cliente do Snowball Edge: prepare-se para iniciar a transferência de dados. Para isso, obtenha as credenciais, o manifesto do trabalho e o código de desbloqueio do manifesto e, depois, baixe o cliente do Snowball Edge.
   - O cliente do Snowball Edge é a ferramenta que você utilizará para gerenciar o fluxo de dados do dispositivo para o destino de dados on-premises.

     É possível baixar e instalar o cliente do Snowball Edge pela página Recursos do AWS Snowball.

     É necessário baixar o cliente do Snowball Edge pela página Recursos do AWS Snowball Edge e instalá-lo em uma estação de trabalho potente.

- O manifesto é usado para autenticar o acesso ao dispositivo e está criptografado, de forma que somente pode ser descriptografado pelo código de desbloqueio. Você pode obter o manifesto no console ou com a API de gerenciamento de trabalhos quando o dispositivo estiver no local na sua localização.
- 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. Recomendamos manter o código de desbloqueio salvo em algum lugar separado do manifesto para impedir o acesso não autorizado ao dispositivo enquanto estiver nas suas instalações.

6. Posicionar o hardware: mova o dispositivo para o datacenter e siga as instruções na caixa para abri-lo. Conecte o dispositivo à energia elétrica e à rede local.
7. Ligar o dispositivo: depois, ligue o dispositivo pressionando o botão liga/desliga acima da tela LCD. Aguarde alguns minutos, e a tela Pronto será exibida.
8. 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 Snowball Edge dispositivo.
9. Use o cliente Snowball Edge para desbloquear o dispositivo — Ao usar o cliente Snowball Edge para desbloquear o AWS Snowball Edge dispositivo, insira o endereço IP do dispositivo, o caminho para seu manifesto e o código de desbloqueio. O cliente do Snowball Edge descriptografa o manifesto e o utiliza para autenticar o acesso ao dispositivo.
10. Usar o dispositivo: o dispositivo está ativo e funcionando. É possível usá-lo para transferir dados com o adaptador do Amazon S3 ou o ponto de montagem do Network File System (NFS) ou para computação e armazenamento locais com armazenamento compatível com o Amazon S3 em dispositivos da Família Snow.
11. 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. O dispositivo leva cerca de 20 segundos para desligar. Desconecte o dispositivo e 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.
12. A operadora da sua região devolve o dispositivo para AWS — Quando a operadora tem o AWS Snowball Edge dispositivo, o status do trabalho passa a ser Em trânsito para AWS.

> **Note**
>
> Para trabalhos de cluster e exportação, há etapas adicionais. Para ter mais informações, consulte Como funcionam os trabalhos de exportação e Como funciona um trabalho de computação e armazenamento local em cluster.

Tópicos

Como funcionam os trabalhos de importação

Cada trabalho de importação usa um único dispositivo Snowball. Depois de criar um trabalho para solicitar um dispositivo da família Snow na API de gerenciamento de tarefas Console de Gerenciamento da família AWS Snow ou na API de gerenciamento de tarefas, enviamos um Snowball para você. Quando ele chegar após alguns dias, conecte o dispositivo Snowball Edge à rede e transfira para o dispositivo os dados a serem importados ao Amazon S3. Quando você terminar de transferir os dados, envie o Snowball de volta AWS para, e nós importaremos seus dados para o Amazon S3.

Como funcionam os trabalhos de exportação

Cada tarefa de exportação pode usar qualquer número de dispositivos AWS Snowball Edge. Se a listagem contiver mais dados do que cabem em um único dispositivo, vários dispositivos serão fornecidos a você. Cada parte do trabalho tem exatamente um dispositivo associado a ela. Depois da criação das partes do trabalho, a primeira parte assume o status Preparando o Snowball.

> **Note**
>
> A operação de listagem usada para dividir o trabalho em partes é uma função do Amazon S3, e ela é cobrada do mesmo modo que qualquer operação do Amazon S3.

Logo após, começaremos a exportar os dados para um dispositivo. O tempo necessário para exportar os dados variará de acordo com a natureza do conjunto de dados. Por exemplo, exportar muitos arquivos pequenos (menos de 10 MB) leva muito mais tempo. Quando a exportação estiver concluída, AWS o dispositivo estará pronto para ser retirado pela operadora da sua região. Quando ele chega, você conecta o AWS AWS Snowball Edge dispositivo à sua rede e transfere os dados do dispositivo para o armazenamento na sua rede.

Quando terminar de transferir os dados, envie o dispositivo de volta para o. AWS Assim que recebermos o dispositivo para a parte do trabalho de exportação, faremos um apagamento completo dele. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST). Esta etapa indica a conclusão de determinada parte do trabalho.

- Para listagem de chaves

  Antes de exportar os objetos no bucket do S3, examinamos o bucket. Se o bucket for alterado após a verificação, o trabalho poderá sofrer atrasos, pois examinaremos objetos ausentes ou alterados.
- Para o S3 Glacier Flexible Retrieval

  É importante observar que AWS Snowball não é possível exportar objetos que estejam na classe de armazenamento S3 Glacier. Esses objetos devem ser restaurados para que o AWS Snowball possa exportar os objetos com êxito no bucket.

Como funcionam trabalhos de computação e armazenamento locais

Você pode usar a funcionalidade local de computação e armazenamento de um AWS Snowball Edge dispositivo executando instâncias de computação AWS compatíveis com EC2 ou contêineres Kubernetes no Amazon EKS Anywhere on Snow. Para funcionalidade de computação, o armazenamento de dados é fornecido pelo armazenamento compatível com o Amazon S3 em dispositivos da Família Snow.

Você pode criar buckets do Amazon S3 nos dispositivos Snowball Edge para armazenar e recuperar objetos no local para aplicativos que exigem acesso e processamento de dados locais e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos Snowball Edge. É

possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação. Quando o dispositivo ou dispositivos são devolvidos AWS, todos os dados criados ou armazenados no armazenamento compatível com o Amazon S3 nos dispositivos da família Snow são apagados. Para obter mais informações, consulte Trabalhos somente de computação e armazenamento locais.

Para ter mais informações, consulte Somente trabalhos de computação e armazenamento local.

Como funciona um trabalho de computação e armazenamento local em cluster

Um trabalho de cluster é um tipo especial de trabalho somente para armazenamento e computação locais. Ele é destinado àquelas workloads que exigem maior durabilidade de dados e capacidade de armazenamento. Para ter mais informações, consulte Opção de cluster local.

> **Note**
>
> Assim como ocorre com trabalhos de computação e armazenamento locais autônomos, os dados armazenados em um cluster não podem ser importados para o Amazon S3 sem a solicitação de dispositivos adicionais como parte de trabalhos de importação separados. Caso solicite esses dispositivos, será possível transferir os dados do cluster para os dispositivos e importá-los ao devolver os dispositivos para os trabalhos de importação.

Os clusters têm de 3 a 16 dispositivos AWS Snowball Edge, chamados de nós. Quando você receber os nós da transportadora local, conecte todos os nós à alimentação e à rede para obter os endereços IP deles. Você vai usar esses endereços IP para desbloquear todos os nós do cluster de uma só vez com um único comando de desbloqueio, utilizando o endereço IP de um dos nós. Para ter mais informações, consulte Utilização do Snowball Edge Client.

É possível gravar dados em um cluster desbloqueado usando o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow e os dados distribuídos entre os outros nós.

Quando você terminar de usar seu cluster, envie todos os nós de volta para AWS o. Quando recebermos um nó do cluster, realizamos um apagamento completo do Snowball. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Vídeos e blogs do Snowball Edge

- Migração de tamanhos de arquivo mistos com os dispositivos do snow-transfer-tool AWS Snowball Edge
- AWS Snowball Migração de dados Edge
- AWS OpsHub for Snow Family
- Novetta delivers IoT and Machine Learning to the edge for disaster response
- Permita migrações de banco de dados em grande escala com DMS e AWS Snowball
- Melhores práticas de migração de dados com AWS Snowball Edge
- AWS Snowball recursos
- Armazenamento compatível com Amazon S3 em dispositivos otimizados para computação AWS Snowball Edge agora disponível ao público em geral
- Introdução ao armazenamento compatível com o Amazon S3 em dispositivos da família Snow em dispositivos Snowball AWS Edge

Especificações do dispositivo AWS Snowball Edge

Nesta seção, é possível encontrar especificações para tipos de dispositivos AWS Snowball Edge e o hardware.

Tópicos

Especificações do Snowball Edge otimizado para armazenamento (para transferência de dados)

A tabela a seguir contém as especificações de hardware dos dispositivos Snowball Edge otimizado para armazenamento.

Item	Especificações do Snowball Edge otimizado para armazenamento (para transferência de dados)
Especificações de armazenamento	
Capacidade de armazenamento HDD	80 TB de capacidade utilizável
Especificações da fonte de alimentação	
Alimentação	Nas Regiões da AWS nos EUA: 5-15 p 100-220 volts NEMA. Em todas as regiões da AWS, é incluído um cabo de alimentação
Consumo de energia	304 watts para um caso de uso médio, embora a fonte de alimentação seja classificada para 1200 watts.

Item	Especificações do Snowball Edge otimizado para armazenamento (para transferência de dados)
Voltagem	100–240 VCA
Frequência	47/63 Hz
Conexões de dados e de rede	2x 10 Gbit — RJ45 (um utilizável) 1x 25 Gbit: SFP28 1x 100 Gbit – QSFP28
Cabos	Cada dispositivo AWS Snowball Edge é enviado com cabos de alimentação específicos do país. Nenhum outro cabo ou fibra ótica são fornecidos. Para ter mais informações, consulte Hardware de rede suportado.
Requisitos térmicos	Os dispositivos do AWS Snowball Edge são projetados para operações de escritório e são ideais para operações de datacenter.
Saída de decibéis	Em média, um dispositivo AWS Snowball Edge produz 68 decibéis de som, geralmente mais silencioso que um aspirador de pó ou música em uma sala de estar.
Especificações de dimensões e peso	
Weight	49.7 libras (22,54 kg)
Altura	15,5 polegadas (394 mm)
Largura	10,6 polegadas (265 mm)
Comprimento	28,3 polegadas (718 mm)
Especificações do ambiente	

Item	Especificações do Snowball Edge otimizado para armazenamento (para transferência de dados)
Vibração	Uso não operacional equivalente ao nível I do caminhão ASTM D4169 0,73 GRMS
Choque	Uso operacional equivalente a 70G (MIL-S-90 1) Uso não operacional equivalente a 50G (ISTA-3A)
Altitude	Uso operacional equivalente a 0—3.000 metros (0—10.000 pés) Uso não operacional equivalente a 0—12.000 metros
Faixa de temperatura	0°–45°C (operacional)

Especificações de 210 TB do Snowball Edge otimizado para armazenamento

A tabela a seguir contém as especificações de hardware dos dispositivos do Snowball Edge otimizado para armazenamento com 210 TB.

Item	Especificações de 210 TB do Snowball Edge otimizado para armazenamento
Especificações de computação e memória	
CPU	104 vCPUs
RAM	416 GB

Item	Especificações de 210 TB do Snowball Edge otimizado para armazenamento
Especificações de armazenamento	
Capacidade de armazenamento NVME	210 TB utilizáveis (para transferência de dados de objetos e NFS)
Capacidade de armazenamento SSD	Nenhum
Especificações da fonte de alimentação	
Alimentação	Nas Regiões da AWS nos EUA: 5-15 p 100-220 volts NEMA. Em todas as regiões da AWS, é incluído um cabo de alimentação
Consumo de energia	304 watts para um caso de uso médio, embora a fonte de alimentação seja classificada para 1200 watts
Voltagem	100–240 VCA
Frequência	47/63 Hz
Conexões de dados e de rede	2x 10 Gbit — RJ45 (um utilizável) 1x 25 Gbit: SFP28 1x 100 Gbit – QSFP28
Cabos	Cada dispositivo AWS Snowball Edge é enviado com cabos de alimentação específicos do país. Nenhum outro cabo ou fibra ótica são fornecidos. Para ter mais informações, consulte Hardware de rede suportado.
Requisitos térmicos	Os dispositivos AWS Snowball Edge são projetados para as operações de escritório e são ideais para operações de datacenter.

Item	Especificações de 210 TB do Snowball Edge otimizado para armazenamento
Saída de decibéis	Em média, um dispositivo AWS Snowball Edge produz 68 decibéis de som, geralmente mais silencioso que um aspirador de pó ou música em uma sala de estar.
Especificações de dimensões e peso	
Weight	49.7 libras (22,54 kg)
Altura	15,5 polegadas (394 mm)
Largura	10,6 polegadas (265 mm)
Comprimento	28,3 polegadas (718 mm)
Especificações do ambiente	
Vibração	Uso não operacional equivalente ao nível I do caminhão ASTM D4169 0,73 GRMS
Choque	Uso operacional equivalente a 70G (MIL-S-901) Uso não operacional equivalente a 50G (ISTA-3A)
Altitude	Uso operacional equivalente a 0—3.000 metros (0—10.000 pés) Uso não operacional equivalente a 0—12.000 metros
Faixa de temperatura	0°–30°C (operacional)

Especificações do Snowball Edge otimizado para armazenamento (com EC2)

A tabela a seguir contém as especificações de hardware dos dispositivos Snowball Edge otimizado para armazenamento (com EC2).

Item	Especificações do Snowball Edge otimizado para armazenamento (com EC2)
Especificações de computação e memória	
CPU	40 vCPUs
RAM	80 GiB
Especificações de armazenamento	
Capacidade de armazenamento HDD	80 TB utilizáveis (para armazenamento de objetos e blocos)
Capacidade de armazenamento SSD	Armazenamento SSD SATA utilizável de 1 TB (para armazenamento em bloco)
Especificações da fonte de alimentação	
Alimentação	Nas Regiões da AWS nos EUA: 5-15 p 100-220 volts NEMA. Em todas as regiões da AWS, é incluído um cabo de alimentação
Consumo de energia	304 watts para um caso de uso médio, embora a fonte de alimentação seja classificada para 1200 watts
Voltagem	100–240 VCA
Frequência	47/63 Hz
Conexões de dados e de rede	2x 10 Gbit — RJ45 (um utilizável) 1x 25 Gbit: SFP28 1x 100 Gbit – QSFP28

Item	Especificações do Snowball Edge otimizado para armazenamento (com EC2)
Cabos	Cada dispositivo AWS Snowball Edge é enviado com cabos de alimentação específicos do país. Nenhum outro cabo ou fibra ótica são fornecidos. Para ter mais informações, consulte Hardware de rede suportado.
Requisitos térmicos	Os dispositivos AWS Snowball Edge são projetados para as operações de escritório e são ideais para operações de datacenter.
Saída de decibéis	Em média, um dispositivo AWS Snowball Edge produz 68 decibéis de som, geralmente mais silencioso que um aspirador de pó ou música em uma sala de estar.
Especificações de dimensões e peso	
Weight	49.7 libras (22,54 kg)
Altura	15,5 polegadas (394 mm)
Largura	10,6 polegadas (265 mm)
Comprimento	28,3 polegadas (718 mm)
Especificações do ambiente	
Vibração	Uso não operacional equivalente ao nível I do caminhão ASTM D4169 0,73 GRMS
Choque	Uso operacional equivalente a 70G (MIL-S-901) Uso não operacional equivalente a 50G (ISTA-3A)
Altitude	Uso operacional equivalente a 0—3.000 metros (0—10.000 pés) Uso não operacional equivalente a 0—12.000 metros

Item	Especificações do Snowball Edge otimizado para armazenamento (com EC2)
Faixa de temperatura	0°–45°C (operacional)

Especificações do dispositivo Snowball Edge otimizado para computação

Item	Especificações do Snowball Edge otimizado para computação
Especificações de computação e memória	
CPU	Até 104 vCPUs (disponível em configurações de 52 ou 104 vCPUs)
RAM	512 GB de RAM (até 416 GB de RAM - utilizável pelo cliente)
GPU	nVidia V100 (disponível em configuração otimizada para computação com GPU, oferecida somente com 52 vCPUs)
Especificações de armazenamento	
Capacidade de armazenamento SSD	SSD NVMe de 28 TB ou HDD de 42 TB (39,5 TB utilizáveis)
Especificações da fonte de alimentação	
Alimentação	Nas Regiões da AWS nos EUA: 5-15 p 100-220 volts NEMA. Em todas as regiões da AWS, é incluído um cabo de alimentação

Item	Especificações do Snowball Edge otimizado para computação
Consumo de energia	304 watts para um caso de uso médio, embora a fonte de alimentação seja classificada para 1200 watts
Voltagem	100–240 VCA
Frequência	47/63 Hz
Conexões de dados e de rede	2x 10 Gbit — RJ45 (um utilizável) 1x 25 Gbit: SFP28 1x 100 Gbit – QSFP28
Cabos	Cada dispositivo AWS Snowball Edge é enviado com cabos de alimentação específicos do país. Nenhum outro cabo ou fibra ótica são fornecidos. Para ter mais informações, consulte Hardware de rede suportado.
Requisitos térmicos	Os dispositivos AWS Snowball Edge são projetados para as operações de escritório e são ideais para operações de datacenter.
Saída de decibéis	Em média, um dispositivo AWS Snowball Edge produz 68 decibéis de som, geralmente mais silencioso que um aspirador de pó ou música em uma sala de estar.
Especificações de dimensões e peso	
Weight	49.7 libras (22,54 kg)
Altura	15,5 polegadas (394 mm)
Largura	10,6 polegadas (265 mm)
Comprimento	28,3 polegadas (718 mm)
Especificações do ambiente	

Item	Especificações do Snowball Edge otimizado para computação
Vibração	Uso não operacional equivalente ao nível I do caminhão ASTM D4169 0,73 GRMS
Choque	Uso operacional equivalente a 70G (MIL-S-901) Uso não operacional equivalente a 50G (ISTA-3A)
Altitude	Uso operacional equivalente a 0—3.000 metros (0—10.000 pés) Uso não operacional equivalente a 0—12.000 metros
Faixa de temperatura	0°–45°C (operacional)

Hardware de rede suportado

Para usar o dispositivo AWS Snowball Edge, você precisa ter cabos de rede. Para cabos RJ45 , não há recomendações específicas. Os cabos e módulos SFP+ e QSFP+ da Mellanox e Finisar foram verificados quanto à compatibilidade com o dispositivo.

Depois de abrir o painel traseiro do dispositivo AWS Snowball Edge, será possível ver as portas de rede semelhantes às portas exibidas na captura de tela a seguir.

Somente uma interface de rede no dispositivo AWS Snowball Edge pode ser usada por vez. Portanto, use qualquer uma das portas para suportar o seguinte hardware de rede.

SFP

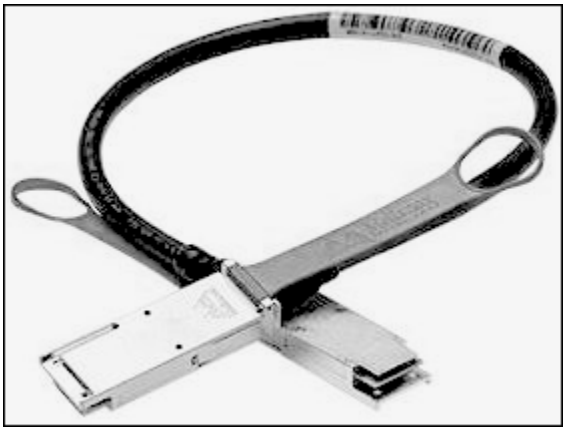
Essa porta fornece uma interface SFP28 de 10 G/25 G+compatível com os módulos transceptores SFP28 e SFP+ e os cabos de cobre de conexão direta (DAC). Você precisa fornecer seus próprios transceptores ou cabos DAC.

- Para operação de 10G, você pode usar qualquer opção SFP+. Os exemplos incluem:
  - Transceptor de 10 Gbase-LR (fibra de modo único)
  - Transceptor de 10 Gbase-DR (fibra de modo único)
  - Cabo DAC SFP+
- Para operação de 25 G, você pode usar qualquer opção SFP28. Os exemplos incluem:
  - Transceptor de 25 Gbase-LR (fibra de modo único)
  - Transceptor de 25 Gbase-SR (fibra de modo múltiplo)
  - Cabo DAC SFP28

QSFP

Essa porta fornece uma interface QSFP+ de 40 G em dispositivos otimizados para armazenamento e uma interface QSFP+ de 40/50/100 G em dispositivos otimizados para computação. Os dois são compatíveis com módulos transceptores QSFP+ e cabos DAC. Você precisa fornecer seus próprios transceptores ou cabos DAC. Os exemplos incluem:

- Transceptor de 40 Gbase-LR4 (fibra de modo único)
- Transceptor de 40 Gbase-SR4 (fibra de modo múltiplo)
- DAC QSFP+

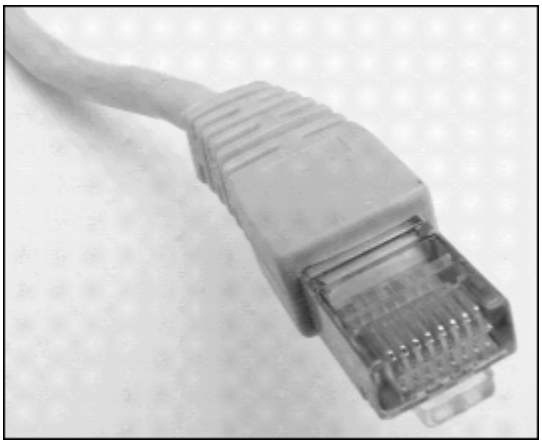


RJ45

Essa porta oferece uma operação de 1 Gbase-TX/10 Gbase-TX. Ela é conectada por cabo UTP com conector RJ45 na ponta. Os dispositivos Snowball Edge têm duas portas RJ45. Escolha uma porta para usar.

A operação de 1 G é indicada por luz âmbar piscante. A operação de 1 GB não é recomendada para transferências de dados em grande escala para o dispositivo Snowball Edge, visto que isso aumenta significativamente o tempo necessário para transferir os dados.

A operação de 10 G é indicada por luz verde piscante. É necessário usar um cabo Cat6A UTP com distância operacional máxima de 180 pés (55 metros).



Preços de longo prazo para dispositivos Snowball Edge

Ao comprar um dispositivo Snowball Edge, você pode escolher a opção de preço mais adequada ao seu caso de uso. Os preços estão disponíveis de duas formas: sob demanda, para cada dia em que você tem o dispositivo ou pré-pago, preços de longo prazo em períodos mensais, de um ou três anos, com base no tipo de dispositivo. Você pode optar por renovar automaticamente sua opção de preço de longo prazo por períodos de um ou três anos, de modo que um novo período pré-pago comece quando o período anterior terminar, para evitar a interrupção do uso do dispositivo. A opção de preço de longo prazo mensal será renovada automaticamente enquanto o dispositivo estiver em sua posse. Para obter mais informações sobre como solicitar um dispositivo, consulte Criação de um trabalho para solicitar um dispositivo da família Snow neste guia.

Além da conveniência orçamentária, os preços de longo prazo permitem que você troque de dispositivo Snowball Edge durante o período de preços quando seus requisitos operacionais mudarem. Por exemplo, você pode solicitar a troca de dispositivos para que o novo inclua uma nova AMI ou novos dados do Amazon S3 ou para substituir um dispositivo com defeito. Consulte Troca de dispositivos durante o período de preços de longo prazo.

> **Note**
>
> Se você solicitar a troca ou substituição de um dispositivo Snowball Edge antes do compromisso de 1 ou 3 anos do plano de preços por qualquer motivo que não seja um problema de hardware ou software atribuído ao serviço do AWS Snow, será cobrada uma taxa de troca do dispositivo. Essa taxa de troca de dispositivos é determinada como a taxa mensal (para o Snowball Edge otimizado para computação) ou a taxa de trabalho sob demanda para sua configuração.

Para obter mais informações sobre preços de longo prazo, consulte Otimização de custos com opções de preços de longo prazo para AWS Snowball. Para saber os preços do AWS Snowball para sua Região da AWS, consulte Definição de preços do AWS Snowball.

Troca de dispositivos durante o período de preços de longo prazo

A troca de dispositivos Snowball Edge durante o período de preços de longo prazo envolve o pedido de um novo dispositivo e a devolução imediata do dispositivo atual.

1. Crie um novo trabalho para o dispositivo substituto do Snowball Edge. O dispositivo de substituição deve ser do mesmo tipo de trabalho e ter as mesmas opções de computação e armazenamento do dispositivo que você tem. Consulte Criação de um trabalho para solicitar um dispositivo Snow Family neste guia.
2. Devolva imediatamente o dispositivo que você tem. Veja Desligar o Snowball Edge e Devolver o dispositivo Snowball Edge. A AWS gerenciará a logística de substituição do dispositivo e haverá uma taxa de troca do dispositivo cobrada para esse fim.

Configurando seu AWS acesso ao AWS Snowball Edge

> **Note**
>
> Na Ásia-Pacífico (Mumbai), o Região da AWS serviço é fornecido pela Amazon na Internet Services Private Limited (AISPL). Para obter informações sobre como se inscrever na Amazon Web Services na Ásia-Pacífico (Mumbai) Região da AWS, consulte Inscrever-se no AISPL.

Quando você se inscreve no Amazon Web Services (AWS), você se inscreve automaticamente em todos os serviços AWS, incluindo o AWS Snow Family. Conta da AWS Você será cobrado apenas pelos serviços que usar. Para obter mais informações sobre preços e taxas, consulte AWS Snowball Edge Preços. AWS Snowball O uso do Edge não é gratuito. Para obter mais informações sobre quais serviços da AWS são gratuitos, consulte Nível de uso gratuito da AWS.

Anote seu Conta da AWS número, pois você precisará dele para criar um trabalho e pedir um Snowball Edge.

Os serviços em AWS, como o AWS Snowball Edge, exigem que você forneça credenciais ao acessá-los, para que o serviço possa determinar se você tem permissão para acessar seus recursos. AWS recomenda não usar suas credenciais raiz Conta da AWS para fazer solicitações. Em vez disso, crie um usuário AWS Identity and Access Management (IAM) e conceda a esse usuário acesso total. Chamamos esses usuários de usuários do IAM com credenciais a nível de administrador.

Você pode usar as credenciais de usuário administrador, em vez das credenciais raiz da sua conta, para interagir AWS e realizar tarefas, como criar um bucket do Amazon S3, criar usuários e conceder permissões a eles. Para obter mais informações, consulte Comparando as credenciais do usuário raiz da AWS conta e as credenciais do usuário do IAM na Referência AWS geral e nas melhores práticas do IAM no Guia do usuário do IAM.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Acesse https://portal.aws.amazon.com/billing/signup.

2. Siga as instruções on-line.

   Durante a criação da conta, você vai receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e utilize somente o usuário raiz para executar as tarefas que exigem acesso do usuário raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .

2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Login como usuário administrativo

- Para fazer login com o usuário do Centro de Identidade do IAM, utilize o URL de login enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Antes de solicitar um dispositivo Snowball Edge

AWS Snowball O Edge é um serviço específico da região. Portanto, antes de planejar seu trabalho, confira se o serviço está disponível na sua Região da AWS. Certifique-se de que sua localização e o bucket do Amazon S3 estejam no mesmo país Região da AWS ou no mesmo país, pois isso afetará sua capacidade de solicitar o dispositivo.

Para usar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow com dispositivos otimizados para trabalhos de armazenamento e computação de borda locais, você precisará provisionar a capacidade do S3 no dispositivo ou nos dispositivos ao fazer o pedido. O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow comporta o gerenciamento local de buckets, para que você possa criar buckets do S3 no dispositivo ou cluster depois de receber o dispositivo ou os dispositivos.

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). Essa chave do KMS é usada para criptografar o código de desbloqueio do trabalho. Para obter mais informações sobre a criação de funções do IAM e chaves KMS, consulte Criação de um trabalho para solicitar um dispositivo da família Snow.

Tópicos

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.

Quais dados você está transferindo?

A transferência de um grande número de arquivos pequenos não funciona bem com o AWS Snowball Edge. Isso ocorre porque o Snowball Edge criptografa cada objeto. Arquivos pequenos incluem arquivos com menos de 1 MB. Recomendamos que você feche o zíper antes de transferi-

los para o dispositivo AWS Snowball Edge. Também recomendamos que você não tenha mais de 500 mil ou diretórios em cada diretório.

Os dados serão acessados durante a transferência?

É importante ter um conjunto de dados estático (ou seja, nenhum usuário ou sistema deverá estar acessando os dados durante a transferência). Caso contrário, a transferência de arquivos pode falhar devido a uma incompatibilidade na soma de verificação. Os arquivos não serão transferidos e serão marcados como `Failed`.

Para evitar corromper seus dados, não desconecte um dispositivo AWS Snowball Edge nem altere suas configurações de rede ao transferir dados. Os arquivos devem estar em um estado estático enquanto são gravados no dispositivo. Arquivos modificados enquanto estão sendo gravados podem resultar em conflitos de leitura/gravação.

A rede suportará a transferência de AWS Snowball dados?

O Snowball Edge é compatível com os adaptadores de rede RJ45, SFP+ ou QSFP+. Verifique se o switch é um switch de gigabit. Dependendo da marca do switch, pode ser gigabit ou 10/100/1.000. Os dispositivos Snowball Edge não são compatíveis com switch de megabit ou switch 10/100.

Trabalhar com nomes de arquivos contendo 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 nos nomes dos objetos, renomeie os objetos antes de copiá-los para o dispositivo AWS Snowball Edge. Os usuários do Windows que têm espaços nos nomes dos arquivos devem ter cuidado ao copiar objetos individuais ou executar um comando recursivo. Nos comandos, coloque os nomes dos objetos que incluem espaços nos nomes entre aspas. Veja exemplos desses arquivos a seguir.

Sistema operacional	Nome do arquivo: arquivo teste.txt
Windows	`“C:\Users\<username>\desktop\test file.txt”`
iOS	`/Users/<username>/test\ file.txt`
Linux	`/home/<username>/test\ file.txt`

> **Note**
>
> Os únicos metadados do objeto transferidos são o nome e o tamanho do objeto.

Usar o Amazon EC2 em dispositivos da Família Snow

Esta seção fornece uma visão geral do uso de instâncias computacionais compatíveis com o Amazon EC2 em um AWS Snowball dispositivo Edge. Ela inclui informações conceituais, procedimentos e exemplos.

> **Note**
>
> Esses recursos do Amazon EC2 AWS Snowball ativados não são suportados na Ásia-Pacífico (Mumbai) e na Europa (Paris). Regiões da AWS

Você pode executar instâncias computacionais compatíveis com o Amazon EC2 hospedadas em um AWS Snowball Edge com os tipos de instâncias`sbe1`,`sbe-c`, `esbe-g`:

- O tipo de instância `sbe1` funciona em dispositivos com a opção Snowball Edge otimizado para armazenamento.
- O tipo de instância `sbe-c` funciona em dispositivos com a opção Snowball Edge otimizado para computação.
- Os dois tipos de instância `sbe-c` e `sbe-g` funcionam em dispositivos com a opção Snowball Edge otimizado para computação com GPU.

Todos os três tipos de instância de computação compatíveis nas opções de dispositivo Snowball Edge são exclusivos para dispositivos AWS Snowball Edge. Assim como seus equivalentes baseados em nuvem, essas instâncias exigem imagens de máquina da Amazon (AMIs) para iniciar. Selecione a AMI para uma instância, antes de criar o trabalho do Snowball Edge.

Para usar uma instância de computação em um Snowball Edge, crie um trabalho para solicitar um dispositivo da família Snow e especificar suas AMIs. Você pode fazer isso usando o AWS Snowball Management Console, o AWS Command Line Interface (AWS CLI) ou um dos AWS SDKs. Normalmente, para usar as instâncias, há alguns pré-requisitos de manutenção que devem ser executados antes da criação do trabalho.

Depois que o dispositivo chega, você pode começar a gerenciar as AMIs e as instâncias. Gerencie as instâncias de computação em um Snowball Edge por meio de um endpoint do Amazon EC2. Esse tipo de endpoint suporta muitos dos comandos e ações da CLI do Amazon EC2 para os SDKs. AWS Você não pode usar o AWS Management Console on the Snowball Edge para gerenciar suas AMIs e instâncias de computação.

Quando terminar de usar seu dispositivo, devolva-o para AWS. Se o dispositivo tiver sido usado em um trabalho de importação, os dados transferidos usando o adaptador do Amazon S3 ou a interface NFS serão importados para o Amazon S3. 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 Snowball Edge não são importados para a AWS.

Diferença entre o Amazon EC2 e instâncias compatíveis com o 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.

Preços de instâncias de computação no Snowball Edge

Existem custos adicionais associados ao uso de instâncias de computação. Para obter mais informações, consulte Preços do AWS Snowball Edge.

Pré-requisitos

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

- Antes de adicionar quaisquer AMIs à solicitação de trabalho, verifique se você criou uma AMI compatível com sua Conta da AWS. Atualmente, as AMIs compatíveis se baseiam nas imagens CentOS 7 (x86_64) com atualizações HVM e Ubuntu 16.04 LTS, Xenial (HVM). É possível obter essas imagens no site AWS Marketplace.
- 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 Snowball Edge, você deverá usar Secure Shell (SSH). Para isso, primeiro você deve adicionar o par de chaves. Para ter mais informações, consulte Configurar uma AMI para usar SSH a fim de conectar-se às instâncias de computação iniciadas no dispositivo.

Criar uma AMI do Linux de uma instância

Você pode criar uma AMI usando a linha de comando AWS Management Console ou. Comece com uma AMI existente, execute uma instância, personalize-a, crie uma AMI com base nela e, por fim, execute uma instância da 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 necessário antes de iniciar. Para obter mais informações, consulte Inicie uma instância

usando o assistente de inicialização de instância no Manual do usuário para instâncias do Linux do Amazon EC2.

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 as seguintes ações na instância para personalizá-la de acordo com suas necessidades:
   - Instalar o software e as 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 Como criar snapshots de Amazon EBS no Manual do usuário para instâncias do Linux do Amazon EC2.
5. No painel de navegação, selecione Instâncias e escolha sua instância. Escolha Ações, Imagem e, em seguida, Criar imagem.

   > **Tip**
   >
   > Se essa opção estiver disponível, isso significa que 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 Não reinicializar para impedir o encerramento da instância.

> **Warning**
>
> Se você selecionar Não reinicializar, não poderemos garantir a integridade do sistema de arquivos da imagem criada.

- Volumes de instâncias: os campos nesta seção permitem que você modifique o volume raiz e adicione mais 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 Manual do usuário para instâncias do Linux 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 instância, consulte Adicionar volumes de armazenamento de instâncias a uma AMI no Manual do usuário para instâncias Linux do Amazon EC2. 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 instância 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 Inicie uma instância usando o assistente de inicialização de instância no Manual do usuário para instâncias do Linux do Amazon EC2.

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 comandos, consulte Acessar o Amazon EC2 no Manual do usuário para instâncias do Linux do Amazon EC2.

- create-image (AWS CLI)
- New-EC2Image (Ferramentas para Windows)AWS 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; em seguida, escolha Criar imagem.
4. Na caixa de diálogo Criar imagem de snapshot do EBS, preencha os campos para criar a AMI. Em seguida, selecione Criar. Se você estiver recriando uma instância principal, selecione as mesmas opções escolhidas para a instância principal.
   - 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 Nomes de dispositivos em instâncias do Linux no Manual do usuário para instâncias do Linux do Amazon EC2.
   - Tipo de virtualização: escolha se as instâncias executadas com essa AMI usam virtualização paravirtual (PV) ou máquina virtual de hardware (HVM). Para obter mais informações, consulte Tipos de virtualização da AMI em 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, a 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 na instância para um volume maior, consulte Estender um sistema de arquivos Linux após um redimensionamento de volume no Manual do usuário para instâncias do Linux do Amazon EC2.

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

Para criar uma AMI com base em um snapshot, você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comandos, consulte Acessar o Amazon EC2 no Manual do usuário para instâncias do Linux do Amazon EC2.

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

Usar o Amazon S3 no Snowball Edge

Como parte do processo de pedido, você deve criar uma função AWS Identity and Access Management (IAM) e uma chave AWS Key Management Service (AWS KMS). A chave do KMS é usada para criptografar os dados em repouso no dispositivo Snowball Edge. Para obter mais informações sobre a criação de funções do IAM e chaves KMS, consulte Criação de um trabalho para solicitar um dispositivo da família Snow.

> **Important**
>
> Se os dados importados precisarem ser criptografados no bucket do S3 usando criptografia do lado do servidor com chaves armazenadas em AWS KMS (SSE-KMS), consulte. Criptografia Amazon S3 com AWS KMS
> Se os dados importados precisarem ser criptografados no bucket do S3 usando criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), consulte Criptografia do Amazon S3 com criptografia do lado do servidor.

Como a importação funciona

Cada trabalho de importação usa um único dispositivo Snowball Edge. Depois de criar um trabalho para solicitar um dispositivo da família Snow, enviamos um dispositivo Snowball Edge para você. Quando ele chegar, conecte o dispositivo Snowball Edge à sua rede e transfira os dados que deseja importar para o Amazon S3 para esse Snowball Edge. Quando concluir a transferência de dados, envie o Snowball de volta para a AWS. Em seguida, importamos seus dados para o Amazon S3.

> **Important**
>
> O Snowball Edge não poderá gravar em buckets se você tiver ativado o Bloqueio de Objetos do S3. Também não poderemos gravar no bucket se as políticas do IAM no bucket impedirem a gravação no bucket.

Como a exportação funciona

Cada tarefa de exportação pode usar qualquer número de dispositivos AWS Snowball Edge. Depois que você cria um trabalho, é iniciada uma operação de listagem no Amazon S3. Essa operação de listagem divide o trabalho em partes. Cada parte do trabalho tem exatamente um dispositivo associado a ela. Após a criação das partes do trabalho, a primeira parte assume o status Preparando o Snowball.

> **Note**
>
> A operação de listagem para dividir o trabalho em partes é uma função do Amazon S3, e ela é cobrada do mesmo modo que qualquer operação do Amazon S3.

Em seguida, começamos a exportar os dados para um dispositivo. Normalmente, a exportação de dados leva um dia útil. Mas esse processo pode demorar mais. Quando a exportação estiver concluída, o dispositivo estará pronto para ser AWS retirado pela operadora regional.

Quando o dispositivo chegar, conecte-o à rede e transfira os dados que deseja importar para o Amazon S3 no dispositivo. Quando terminar de transferir os dados, envie o dispositivo de volta para o. AWS Quando recebemos o dispositivo devolvido, nós o apagamos completamente. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Esta etapa indica a conclusão de determinada parte do trabalho. Se houver mais partes do trabalho, a próxima parte do trabalho será preparada para entrega.

> **Important**
>
> O Snowball Edge não consegue exportar arquivos na classe de armazenamento do S3 Glacier. Esses objetos devem ser restaurados para que possamos exportar os arquivos. Se encontrarmos arquivos na classe de armazenamento do S3 Glacier, entraremos em contato para informar você, mas isso pode atrasar seu trabalho de exportação.

Usar armazenamento compatível com o Amazon S3 em dispositivos da Família Snow para trabalhos de armazenamento e computação de borda

O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow oferece armazenamento seguro de objetos com maior resiliência, escala e um conjunto expandido de recursos de API do Amazon S3 para ambientes robustos, móveis e desconectados. O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow permite que os clientes armazenem dados e executem aplicações altamente disponíveis em dispositivos da Família Snow para casos de uso de computação de borda.

Você pode criar buckets do Amazon S3 nos dispositivos Snowball Edge para armazenar e recuperar objetos no local para aplicativos que exigem acesso e processamento de dados locais e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos Snowball Edge. É possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação. Quando o dispositivo ou dispositivos são devolvidos AWS, todos os dados criados ou armazenados no armazenamento compatível com o Amazon S3 nos dispositivos da família Snow são apagados. Para obter mais informações, consulte Trabalhos somente de computação e armazenamento locais.

O armazenamento compatível com Amazon S3 em dispositivos da Família Snow pode ser implantado em configuração autônoma ou configuração de cluster. Na configuração autônoma, você pode provisionar a capacidade do S3 no dispositivo e o balanceamento está disponível como armazenamento em bloco. Na configuração de cluster, toda a capacidade do disco de dados será utilizada para armazenamento do S3. Dependendo do tamanho do cluster, o serviço S3 foi projetado

para manter a tolerância a falhas de um ou dois dispositivos. Para obter mais informações sobre tolerância a falhas de cluster, consulte Visão geral de clustering.

Para configurar e usar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, consulte Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow neste guia.

Criptografia Amazon S3 com AWS KMS

Você pode usar as chaves de criptografia padrão AWS gerenciadas ou gerenciadas pelo cliente para proteger seus dados ao importar ou exportar dados.

Usando a criptografia de bucket padrão do Amazon S3 com chaves gerenciadas AWS KMS

Para habilitar a criptografia AWS gerenciada com AWS KMS

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o bucket do Amazon S3 que deseja criptografar.
3. No assistente que aparece no lado direito, escolha Propriedades.
4. Na caixa Criptografia padrão, escolha Desabilitada (essa opção está esmaecida) para habilitar a criptografia padrão.
5. Escolha AWS-KMS como método de criptografia e selecione a chave do KMS que você deseja usar. Essa chave é usada para criptografar objetos que são colocados no bucket.
6. Escolha Salvar.

Depois que o trabalho do Snowball Edge for criado e antes da importação dos dados, adicione uma instrução à política de perfil do IAM já existente. Esse é o perfil que você criou durante o processo de pedido. Dependendo do tipo de trabalho, o nome do perfil padrão é semelhante a `Snowball-import-s3-only-role` ou `Snowball-export-s3-only-role`.

Veja a seguir exemplos do uso de uma instrução.

Para importar dados

Se você usa criptografia do lado do servidor com chaves AWS KMS gerenciadas (SSE-KMS) para criptografar os buckets do Amazon S3 associados ao seu trabalho de importação, você também precisa adicionar a seguinte declaração à sua função do IAM.

Example Exemplo de perfil do IAM de importação do Snowball

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

Para exportar dados

Se você usa criptografia do lado do servidor com chaves AWS KMS gerenciadas para criptografar os buckets do Amazon S3 associados ao seu trabalho de exportação, você também deve adicionar a seguinte declaração à sua função do IAM.

Example Perfil do IAM para exportação do Snowball

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

Usando a criptografia de bucket padrão do S3 com chaves de AWS KMS cliente

Você pode usar a criptografia padrão de bucket do Amazon S3 com suas próprias chaves do KMS para proteger os dados que você está importando e exportando.

Para importar dados

Para habilitar a criptografia gerenciada pelo cliente com AWS KMS

1. Faça login no console AWS Management Console e abra o 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 painel de navegação esquerdo, escolha Chaves gerenciadas pelo cliente e depois selecione a chave do KMS associada aos buckets que você deseja usar.
4. Expanda a Política de chave se ela ainda não estiver expandida.
5. Na seção Usuários de chaves, escolha Adicionar e pesquise o perfil do IAM. Escolha o perfil do IAM e selecione Adicionar.
6. Como alternativa, você pode escolher Mudar para visualização da política para exibir o documento de política de chave e adicionar uma instrução à política de chave. Veja a seguir um exemplo da política.

Example de uma política para a chave gerenciada pelo AWS KMS cliente

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

Depois que essa política for adicionada à chave gerenciada pelo AWS KMS cliente, também será necessário atualizar a função do IAM associada ao trabalho do Snowball. Por padrão, o perfil é `snowball-import-s3-only-role`.

Example Exemplo do perfil do IAM de importação do Snowball

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

```
}
```

Para ter mais informações, consulte Usar políticas baseadas em identidade (políticas do IAM) para o AWS Snowball.

A chave do KMS que está sendo usada tem a seguinte aparência:

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

Para exportar dados

Example de uma política para a chave gerenciada pelo AWS KMS cliente

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

Depois que essa política for adicionada à chave gerenciada pelo AWS KMS cliente, também será necessário atualizar a função do IAM associada ao trabalho do Snowball. Por padrão, o perfil se parece com o seguinte:

`snowball-export-s3-only-role`

Example Exemplo do perfil do IAM de exportação do Snowball

```
{
  "Effect": "Allow",
  "Action": [
    "kms: GenerateDataKey",
    "kms: Decrypt"
  ],
```

```
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-
efgh-111111111111"
}
```

Depois que essa política for adicionada à chave gerenciada pelo AWS KMS cliente, também será necessário atualizar a função do IAM associada ao trabalho do Snowball. Por padrão, o perfil é `snowball-export-s3-only-role`.

Criptografia do Amazon S3 com criptografia do lado do servidor

AWS Snowball suporta criptografia do lado do servidor com chaves de criptografia gerenciadas do Amazon S3 (SSE-S3). A criptografia do lado do servidor tem a ver com proteção de dados em repouso, e o SSE-S3 tem criptografia multifator, forte, para proteger os dados em repouso no Amazon S3. Para obter mais informações sobre o SSE-S3, consulte Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Atualmente, AWS Snowball não oferece suporte à criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). No entanto, você pode usar esse tipo de SSE para proteger dados que foram importados, ou talvez você já a esteja usando nos dados que deseja exportar. Nesses casos, tenha em mente o seguinte:
>
> - Importar: se quiser usar SSE-C para criptografar os objetos que importou para o S3, copie esses objetos em outro bucket que tenha a criptografia SSE-KMS ou SSE-S3 estabelecida como parte da política desse bucket.
> - Exportar: se deseja exportar objetos criptografados com SSE-C, copie esses objetos para outro bucket que não tenha criptografia do lado do servidor ou que tenha SSE-KMS ou SSE-S3 especificado na política desse bucket.

Clusters do Snowball Edge

Para o AWS Snowball serviço, um cluster é um coletivo de dispositivos Snowball Edge, usados como uma única unidade lógica, para fins de armazenamento e computação locais.

Um cluster é um agrupamento lógico de dispositivos AWS Snowball Edge, em grupos de 3 a 16 dispositivos. Um cluster é criado com um único trabalho. Um cluster oferece maior durabilidade e

capacidade de armazenamento. Esta seção fornece informações sobre clusters do Snowball Edge com armazenamento compatível do Amazon S3 em dispositivos da Família Snow.

Considerações sobre trabalhos de cluster do AWS Snowball Edge

Lembre-se das seguintes considerações quando estiver pensando em usar um cluster de dispositivos Snowball Edge:

- Recomendamos que você tenha uma fonte de alimentação redundante para reduzir possíveis problemas de desempenho e estabilidade do cluster.
- Assim como ocorre com trabalhos de computação e armazenamento locais autônomos, os dados armazenados em um cluster não podem ser importados para o Amazon S3 sem a solicitação de dispositivos adicionais como parte de trabalhos de importação separados. Caso solicite esses dispositivos, será possível transferir os dados do cluster para os dispositivos e importá-los ao devolver os dispositivos para os trabalhos de importação.
- Para inserir dados em um cluster do Amazon S3, crie um trabalho de exportação separado e copie os dados dos dispositivos do trabalho de exportação para o cluster.
- Você pode usar o console AWS CLI, o ou o AWS SDK para criar um trabalho de cluster.
- Os nós de cluster têm IDs de nó. A ID do nó é igual à ID do trabalho de um dispositivo que você pode obter do console AWS CLI, do AWS SDKs ou do cliente Snowball Edge. Você pode usar IDs de nó para remover nós de cluster antigos. Para obter uma lista de IDs de nós, use o comando `snowballEdge describe-device` em um dispositivo desbloqueado ou o `describe-cluster` em um cluster desbloqueado.
- A duração de um cluster é limitada pelo certificado de segurança concedido a dispositivos do cluster quando o cluster é provisionado.
- Ao AWS receber um dispositivo devolvido que fazia parte de um cluster, realizamos uma eliminação completa do dispositivo. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Considerações de envio para dispositivos da Família Snow

Ao criar um trabalho para solicitar um dispositivo Snow Family, você fornece um endereço de entrega e escolhe a velocidade de envio. Observe que a velocidade de remessa não indica em quanto tempo você pode esperar receber o dispositivo a partir da data em que criou o trabalho foi criado. Em vez disso, indica o tempo em que o dispositivo está em trânsito entre a AWS e seu endereço de entrega. Antes de o dispositivo ser enviado, AWS processa o dispositivo para o trabalho. O tempo necessário para processar seu trabalho depende de fatores como tipo e tamanho do trabalho. Além disso, as transportadoras geralmente só retiram os dispositivos Snow Family de saída uma vez por dia e as transportadoras não retiram os dispositivos de saída nos fins de semana. Desse modo, o processamento antes da entrega pode demorar um dia ou mais. Enquanto AWS prepara seu dispositivo para envio e depois de receber o dispositivo após sua devolução, você pode monitorar o status do seu trabalho por meio doConsole de Gerenciamento da família AWS Snow. Para ter mais informações, consulte Status dos trabalhos.

> **Note**
>
> A velocidade de envio que você escolhe se aplica quando a AWS envia o dispositivo para você e quando você devolve o dispositivo para a AWS.
> Os dispositivos Snowball Edge somente podem ser usados para importar ou exportar dados dentro da região da AWS onde eles foram solicitados.

Para obter mais informações sobre como escolher a velocidade de envio e inserir seu endereço de entrega ao criar um trabalho para solicitar um dispositivo Snow Family, consulteEtapa 4: escolha as preferências de segurança, envio e notificação. Para obter mais informações sobre como devolver um dispositivo Snow FamilyAWS, consulteDevolver o dispositivo Snowball Edge.

Para obter mais informações sobre cobranças de envio, consulte Definição de preço do AWS Snowball Edge.

Restrições de envio conforme a região

Antes de criar um trabalho para solicitar um dispositivo da família Snow, você deve fazer login no console usando os Região da AWS mesmos dados do Amazon S3. AWSnão envia dispositivos da família Snow entre países dentro do mesmo país Região da AWS — 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

Os dispositivos da Família Snow só podem ser devolvidos para a mesma região da AWS em que os dispositivos foram pedidos.

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**
>
> A AWS não envia dispositivos da Família Snow para caixas postais.

Conceitos básicos

Com um AWS Snowball Edge dispositivo, você pode acessar o armazenamento e o poder computacional do Nuvem AWS local de forma econômica em locais onde a conexão à Internet pode não ser uma opção. Também é possível transferir centenas de terabytes ou petabytes de dados entre os datacenters on-premises e o Amazon Simple Storage Service (Amazon S3).

A seguir, você encontrará instruções gerais para criar e concluir o primeiro trabalho no dispositivo AWS Snowball Edge no Console de Gerenciamento da família AWS Snow. O console apresenta os fluxos de trabalho mais comuns, separados em tipos de trabalho. Há mais informações sobre componentes específicos do dispositivo AWS Snowball Edge disponíveis nesta documentação. Para obter uma visão geral do serviço como um todo, consulte Como o AWS Snowball Edge funciona.

Os exercícios de introdução pressupõem que você use o Console de Gerenciamento da família AWS Snow para criar seu trabalho, o AWS OpsHub for Snow Family para desbloquear e gerenciar o AWS Snowball Edge dispositivo e a interface do Amazon S3 para ler e gravar dados. 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 Snowball.

Antes de começar, você deve criar um usuário administrador Conta da AWS e um usuário no AWS Identity and Access Management (IAM). Para obter mais informações, consulte Configurando seu AWS acesso ao AWS Snowball Edge.

Tópicos

- Desligar o Snowball Edge
- Devolver o dispositivo Snowball Edge
- Envio para devolução de dispositivos da Família Snow
- Monitorar o status da importação
- Obter o relatório e logs de conclusão de trabalho no console

Criando um trabalho para solicitar um dispositivo da família Snow

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.

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

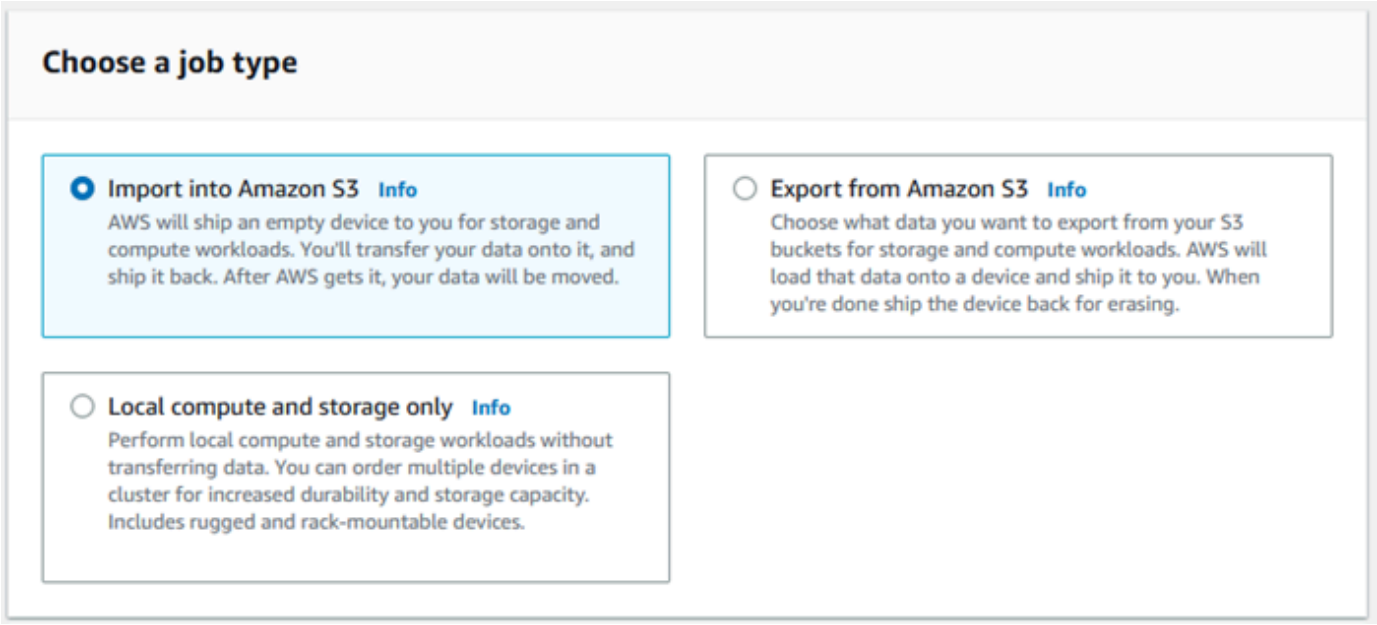
Etapa 1: escolher um tipo de trabalho

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 Snowo. 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 — Escolha essa opção para AWS enviar um dispositivo Snowball Edge vazio para você. Você conecta o dispositivo à sua rede local e executa o Snowball Edge Client. Você copia os dados para o dispositivo usando o compartilhamento NFS ou o adaptador S3, os envia de volta e seus dados são enviados para AWS. AWS
   - Exportar do Amazon S3: escolha essa opção para exportar dados do seu bucket do Amazon S3 para o seu dispositivo. A AWS carrega seus dados no dispositivo e os envia para você. Você conecta o dispositivo à sua rede local e executa o Snowball Edge Client. Você copia dados do seu dispositivo para seus servidores. Quando terminar, envie o dispositivo para AWS, e seus dados serão apagados do dispositivo.
   - Somente computação e armazenamento locais: execute workloads de computação e armazenamento no dispositivo sem transferir dados.



5. Escolha Próximo para continuar.

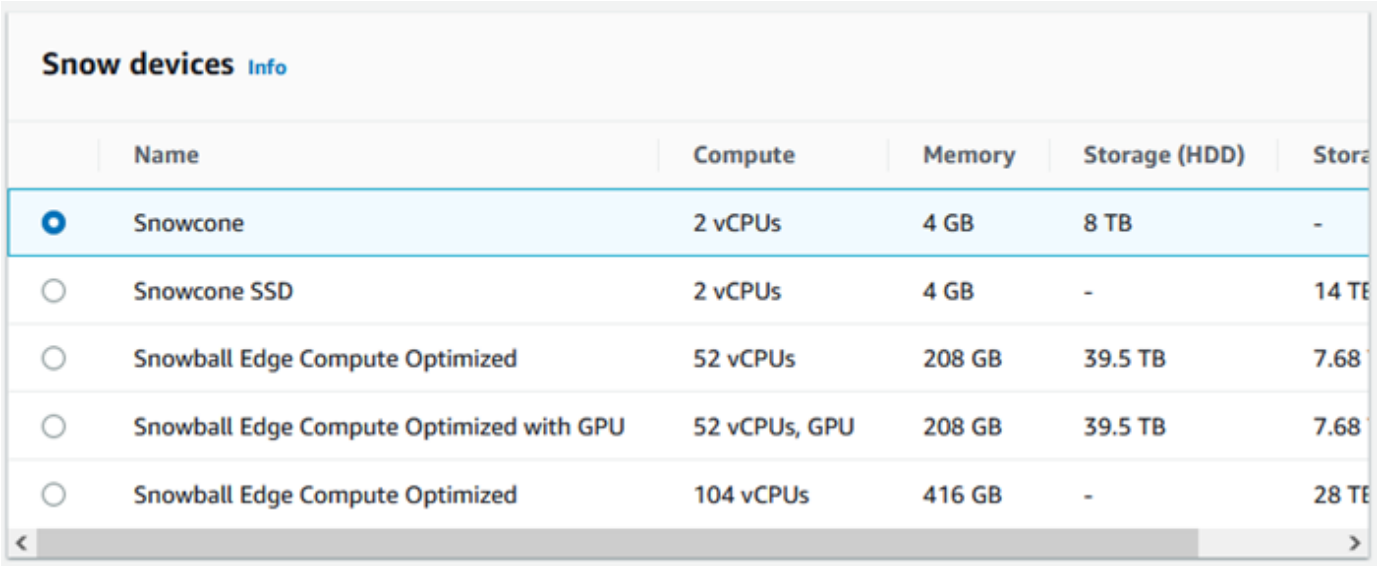
Etapa 2: escolher as opções de computação e armazenamento

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.



2. 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. Se você escolher estabelecer preços antecipados de 1 ou 3 anos, em Renovação automática, escolha Ativado para renovar automaticamente o preço quando o período atual terminar ou Desativado para não renovar automaticamente o preço quando o período atual terminar. Para obter mais informações sobre as opções de preços de longo prazo para dispositivos Snowball Edge, consulte Preços de longo prazo para dispositivos Snowball Edge neste guia. Para saber os preços dos dispositivos para você Região da AWS, consulte AWS Snowball Preços.
3. Na seção Selecione o tipo de armazenamento, faça uma escolha de acordo com sua necessidade:

   - Adaptador S3: use o adaptador do S3 para transferir dados programaticamente de e para dispositivos da Família Snow usando ações da API REST do Amazon S3.
   - Armazenamento compatível com o Amazon S3: use o armazenamento compatível com o Amazon S3 para implantar armazenamento de objetos durável e escalável compatível com o S3 em um único dispositivo Snowball Edge ou em um cluster com vários dispositivos.
   - 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 Desenvolvedor do AWS Snowball Edge para obter mais informações.

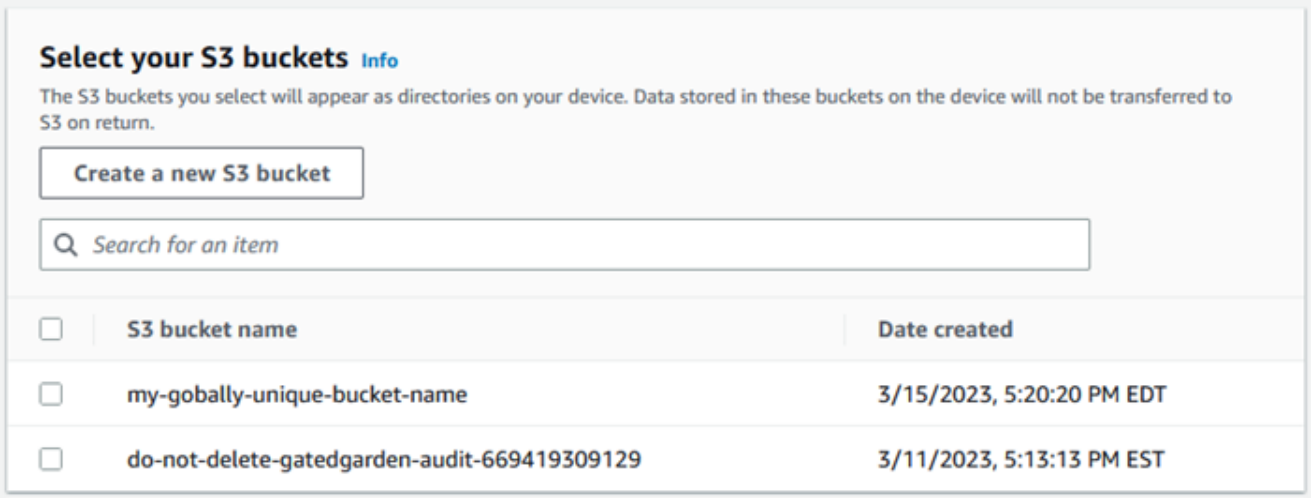
> **Note**
>
> As opções de tipo de armazenamento disponíveis dependem do tipo de trabalho e do dispositivo Snow escolhido.

4. Se você selecionou Adaptador do S3 como o tipo de armazenamento ou se selecionou um dispositivo que suporte armazenamento em bloco, faça o seguinte para selecionar um ou mais buckets do S3 para incluir no dispositivo:

   - Na seção Selecione seus buckets do S3, siga um ou mais dos procedimentos a seguir para selecionar um ou mais buckets do S3:

     1. Escolha o bucket do S3 que deseja usar na lista Nome do bucket do S3.
     2. 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.
     3. 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.

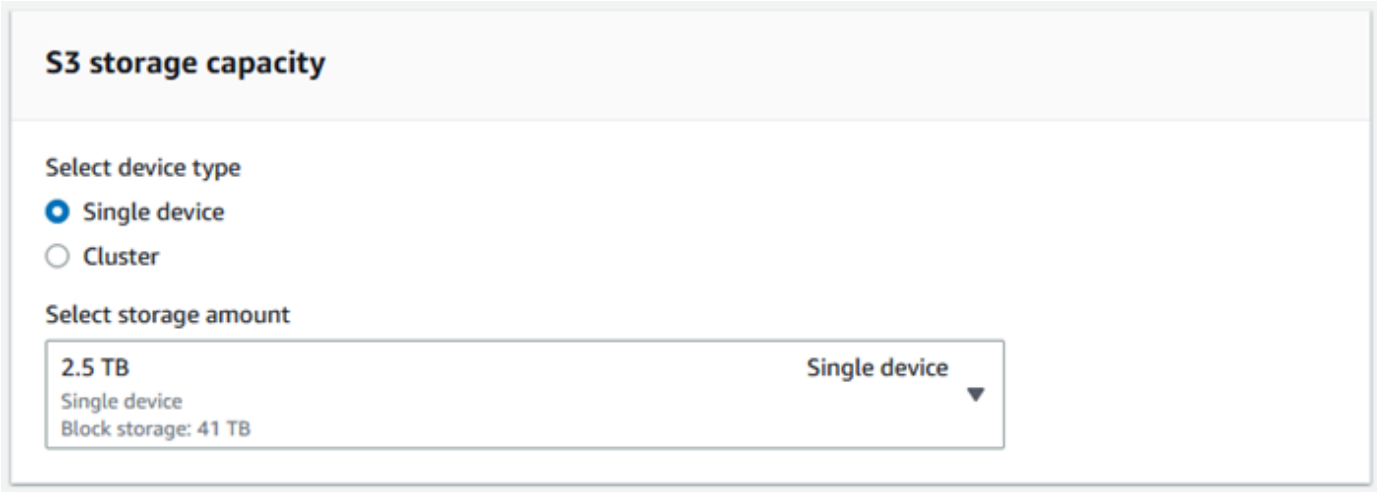


5. Se você selecionou Armazenamento compatível com Amazon S3 como o tipo de armazenamento, na seção Capacidade de armazenamento do S3, faça o seguinte:

   a. Selecione usar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow em um único dispositivo ou em um cluster de dispositivos. Consulte Como usar um AWS Snowball Edge cluster neste guia.

   b. Selecione a quantidade de armazenamento do dispositivo a ser usada para armazenamento compatível com Amazon S3 em dispositivos da Família Snow.

> **Note**
>
> Ao usar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, você pode gerenciar e criar buckets do Amazon S3 depois de receber o dispositivo, para que você não precise escolhê-los ao fazer o pedido. Consulte o Armazenamento compatível com Amazon S3 em dispositivos da família Snow neste guia.



6. 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:

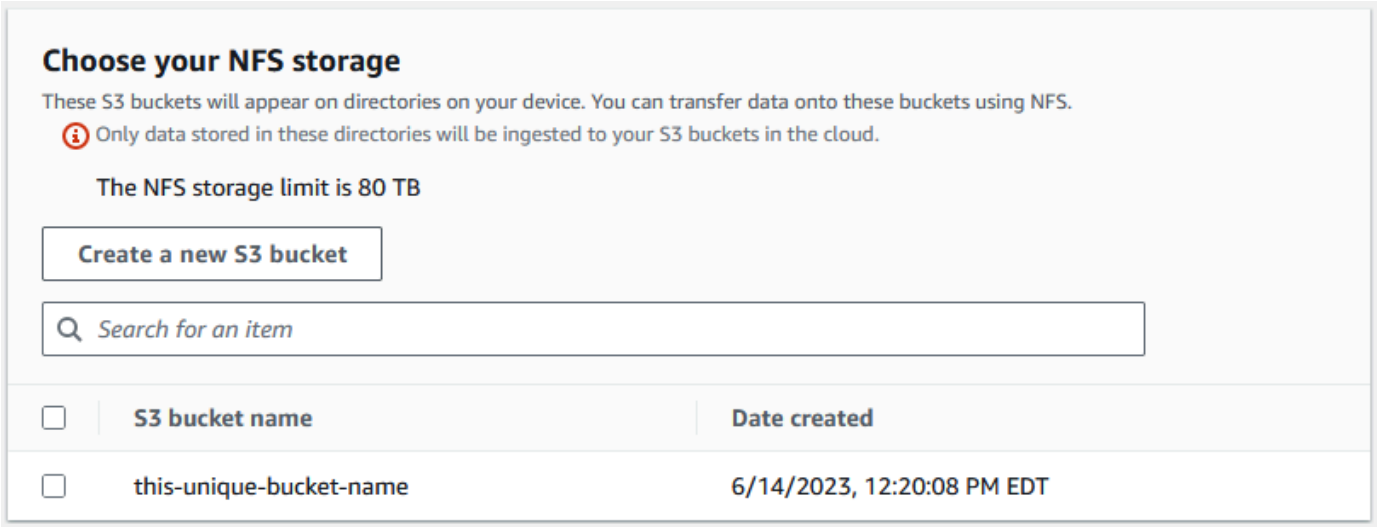
   a. Escolha o bucket do S3 que deseja usar na lista Nome do bucket do S3.

   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.

   d. Depois de escolher buckets do S3 para usar com transferência de dados NFS, escolha também um bucket S3 para usar como armazenamento em bloco para AMIs. Veja as etapas para escolher um bucket do S3.

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



7. 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 Adicionar uma AMI ao fazer o pedido do seu dispositivo neste guia.

   Esse atributo gera cobranças adicionais. Para obter mais informações, consulte Preços do AWS Snowball Edge.
8. 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. Na seção Amazon EKS Anywhere on AWS Snow, para incluir o Amazon EKS Anywhere on AWS Snow, selecione Include Amazon EKS Anywhere on Snow e faça o seguinte.

> **Note**
>
> Recomendamos que você crie seu cluster Kubernetes com a versão mais recente disponível do Kubernetes suportada pelo Amazon EKS Anywhere. Para obter mais informações, consulte Controle de versão do Amazon EKS-Anywhere. Se seu aplicativo exigir uma versão específica do Kubernetes, use qualquer versão do Kubernetes oferecida no suporte padrão ou estendido pelo Amazon EKS. Considere as datas de lançamento e suporte das versões do Kubernetes ao planejar o ciclo de vida de sua implantação. Isso ajudará você a evitar a possível perda de suporte para a versão do Kubernetes que você pretende usar. Para obter mais informações, consulte o calendário de lançamento do Amazon EKS Kubernetes.

   a. Na seção Crie sua própria AMI, escolha as AMIs que você criou para o Amazon EKS Anywhere. Consulte Ações a serem concluídas antes de comprar um dispositivo Snowball Edge para o Amazon EKS Anywhere on Snow AWS.

   b. Na seção Alta disponibilidade, para operar clusters do Amazon EKS Anywhere em vários dispositivos Snowball Edge, escolha o número de dispositivos a serem incluídos em seu pedido.

2. Na seção AWS IoT Greengrass on Snow, para incluir uma AMI validada para cargas de trabalho de IoT, selecione AWS IoT Greengrass Instalar AMI validada no meu dispositivo Snow.
3. 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.
4. 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. Escolha 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.

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.

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

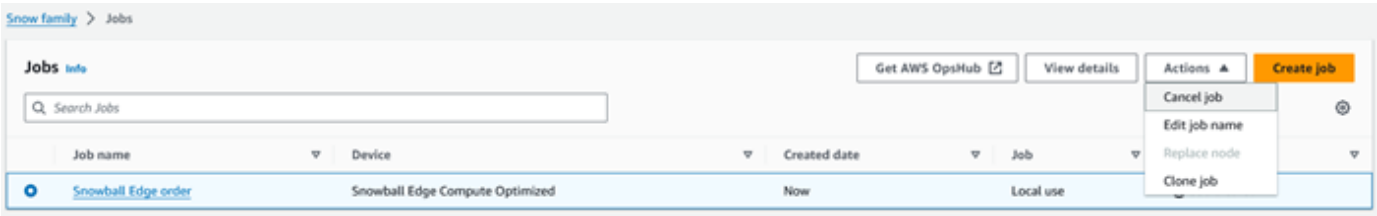
1. Nos AWS Snowball recursos, clique em AWS OpsHub. Na AWS OpsHub seção com os links de download, escolha o link de download apropriado AWS OpsHub para instalar em seu sistema operacional.
2. Na seção AWS OpsHub, escolha Baixar para seu sistema operacional e siga as etapas de instalação. Quando terminar,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

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

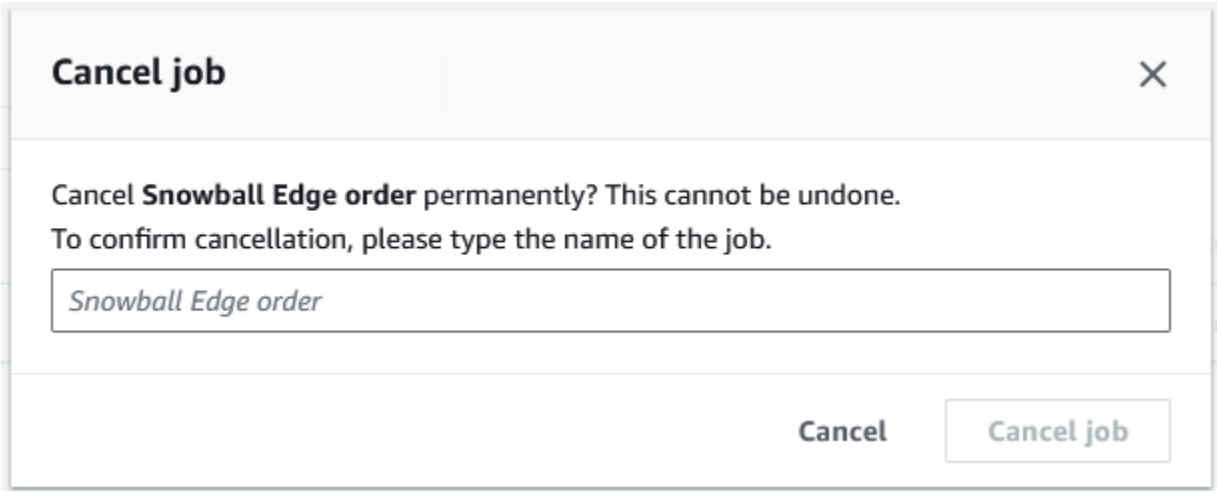
Depois de criar um trabalho para solicitar um dispositivo Snow Family, você pode cancelar o trabalho por meio doConsole de Gerenciamento da família AWS Snow. Se você cancelar o trabalho, não receberá o dispositivo que solicitou. Você só pode cancelar o trabalho enquanto o status do trabalho for Job created. 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.



Receber o Snowball Edge

Ao receber o AWS Snowball Edge dispositivo, você pode perceber que ele não vem em uma caixa. O dispositivo é seu próprio contêiner de envio, fisicamente resistente. 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 informe o problema para que seja possível enviar um novo dispositivo.

> **Important**
>
> O AWS Snowball Edge dispositivo é propriedade de AWS. A adulteração de um AWS Snowball Edge dispositivo é uma violação da Política de Uso AWS Aceitável. Para obter mais informações, consulte Política de uso aceitável da AWS.

O dispositivo é semelhante à imagem a seguir.

Se estiver pronto para conectar o dispositivo à rede interna, consulte a próxima seção.

Próximo: Conectar-se à rede local

Conectar-se à rede local

Usando o procedimento a seguir, você conecta o AWS Snowball Edge dispositivo à sua rede local. O dispositivo não precisa estar conectado à Internet. O dispositivo tem três portas, uma frontal, uma traseira e outra na parte superior.

Para conectar o dispositivo à rede

1. Abra as portas da frente e de trás deslizando-as dentro das ranhuras das portas do dispositivo. Isso oferece acesso à tela de toque no LCD incorporado na parte da frente do dispositivo, à alimentação elétrica e às entradas de rede na parte de trás.

   > **Note**
   >
   > Não feche as portas frontal e traseira enquanto estiver usando o dispositivo Snowball Edge. As portas abertas permitem que o ar resfrie o dispositivo. Fechar as portas durante o uso do dispositivo pode fazer com que o dispositivo seja desligado para evitar superaquecimento.

2. Abra a porta superior e remova o cabo de alimentação fornecido do compartimento para cabos, e conecte o dispositivo na alimentação.
3. Escolha um dos cabos de rede RJ45, SFP+ ou QSFP+ e conecte o dispositivo à rede. As portas de rede estão na parte de trás do dispositivo.
4. Ligue o AWS Snowball Edge dispositivo pressionando o botão liga/desliga acima da tela LCD.
5. 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.
6. (Opcional) Altere as configurações de rede padrão na tela de LCD, escolhendo CONEXÃO.

   É possível alterar o endereço IP para um endereço estático diferente que é fornecido usando o procedimento a seguir.

Para solucionar problemas de inicialização, consulte Solução de problemas de inicialização.

Para alterar o endereço IP de um AWS Snowball Edge dispositivo

1. No monitor LCD, escolha CONNECTION (CONEXÃO).

   Será exibida uma tela que mostrará as configurações de rede atuais do dispositivo AWS Snowball Edge . O endereço IP abaixo da caixa suspensa é atualizado automaticamente para refletir o endereço DHCP solicitado pelo AWS Snowball Edge dispositivo.
2. (Opcional) Altere o endereço IP para um endereço IP estático. Você também pode mantê-lo como está.

O dispositivo está conectado à rede.

> **Important**
>
> Para evitar corromper seus dados, não desconecte o AWS Snowball Edge dispositivo nem altere suas configurações de conexão enquanto ele estiver em uso.

Próximo: Obter credenciais para acessar um dispositivo Snow Family

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 Status dos trabalhos.

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 hífens), 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 em que está o manifesto desse trabalho. Para ter mais informações, consulte Práticas recomendadas para usar o dispositivo Snowball Edge.

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: Baixar e instalar o cliente do Snowball Edge

Baixar e instalar o cliente do Snowball Edge

O cliente Snowball Edge é a ferramenta que você usa para desbloquear o AWS Snowball Edge dispositivo. Recomendamos que você use o AWS OpsHub for Snow Family aplicativo. Para obter instruções, consulte Usando AWS OpsHub for Snow Family para gerenciar dispositivos.

É possível baixar e instalar o cliente do Snowball Edge pela página Recursos do AWS Snowball em uma estação de trabalho potente.

Próximo: Desbloqueando o dispositivo Snow Family

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 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 Conectar-se à rede local Você precisará das seguintes informações sobre o dispositivo Snow Family:

- Faça o download e instale o Snowball Edge Client. Para ter mais informações, consulte Utilização do Snowball Edge Client.
- 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 um cluster de dispositivos Snowball Edge, um código de desbloqueio e um arquivo de manifesto para o cluster. Para obter mais informações sobre como baixar credenciais, consulteObter credenciais para acessar um dispositivo Snow Family.
- Ligue cada dispositivo e conecte-o à sua rede. Para ter mais informações, consulte Conectar-se à rede local.

Para desbloquear um dispositivo independente com o cliente Snowball Edge

1. Encontre o endereço IP do AWS Snowball Edge dispositivo na tela LCD do AWS Snowball Edge dispositivo, na guia Conexões. 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`, consulteSolução de problemas para desbloquear um dispositivo da família Snow.

Example 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
```

Para desbloquear um cluster de dispositivos Snowball Edge com o cliente Snowball Edge

1. Encontre o endereço IP de cada um dos dispositivos no cluster na tela LCD de cada AWS Snowball Edge dispositivo, na guia Conexões. Anote o endereço IP.
2. Use o `snowballEdge unlock-cluster` comando para autenticar seu acesso ao cluster de AWS Snowball Edge dispositivos com o endereço IP de um dos dispositivos no cluster, suas credenciais e os endereços IP de todos os dispositivos no cluster da seguinte forma.

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

O cluster de dispositivos indica que foi desbloqueado com sucesso com a seguinte mensagem.

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

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

Example de **`unlock-cluster`** comando

Neste exemplo, para um cluster de cinco dispositivos, o endereço IP de um dos dispositivos no cluster é`192.0.2.0`, o nome do arquivo de 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-cluster --endpoint https://192.0.2.0 --manifest-file /
Downloads/JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin /

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

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.

Próximo: Configurar usuários locais

Configurar usuários locais

A seguir estão as etapas para configurar um administrador local em seu AWS Snowball Edge dispositivo.

1. Recuperar as credenciais do usuário raiz

   Use `snowballEdge list-access-keys` e `snowballEdge get-secret-access-key` para obter as credenciais locais. Para ter mais informações, consulte Como obter as credenciais.

2. (Configurar as credenciais do usuário raiz usando **`aws configure`**)

   Forneça `AWS Access Key ID`, `AWS Secret Access Key` e `Default region name`. O nome da região deve ser `snow`. Opcionalmente, forneça um `Default output format`. Para obter mais informações sobre como configurar o AWS CLI, consulte Configurando o AWS CLI no Guia do AWS Command Line Interface Usuário.

3. Criar um ou mais usuários locais no dispositivo

   Use o comando `create-user` para adicionar usuários ao dispositivo.

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

   Depois de adicionar os usuários de acordo com as necessidades empresariais, é possível armazenar as credenciais raiz da AWS em um local seguro e usá-las somente para tarefas de gerenciamento de conta e serviço. Para obter mais informações sobre como criar usuários do IAM, consulte Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.

4. Criar uma chave de acesso para o usuário

> **Warning**
>
> Este cenário precisa de usuários do IAM com acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização de chaves de acesso no Guia de usuário do IAM.

Use o comando `create-access-key` para criar uma chave de acesso para o usuário.

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

Salve as informações da chave de acesso em um arquivo e distribua-o aos usuários.

5. Criar uma política de acesso

Talvez você queira atribuir diferentes níveis de acesso às funcionalidades no dispositivo para usuários diferentes. O exemplo a seguir cria um documento de política chamado de `s3-only-policy` e o anexa a um usuário.

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

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

6. Anexar a política ao usuário

   Use `attach-user-policy` para anexar o s3-only-policy a um usuário.

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

Para obter mais informações sobre como usar o IAM localmente, consulte Usar o IAM localmente.

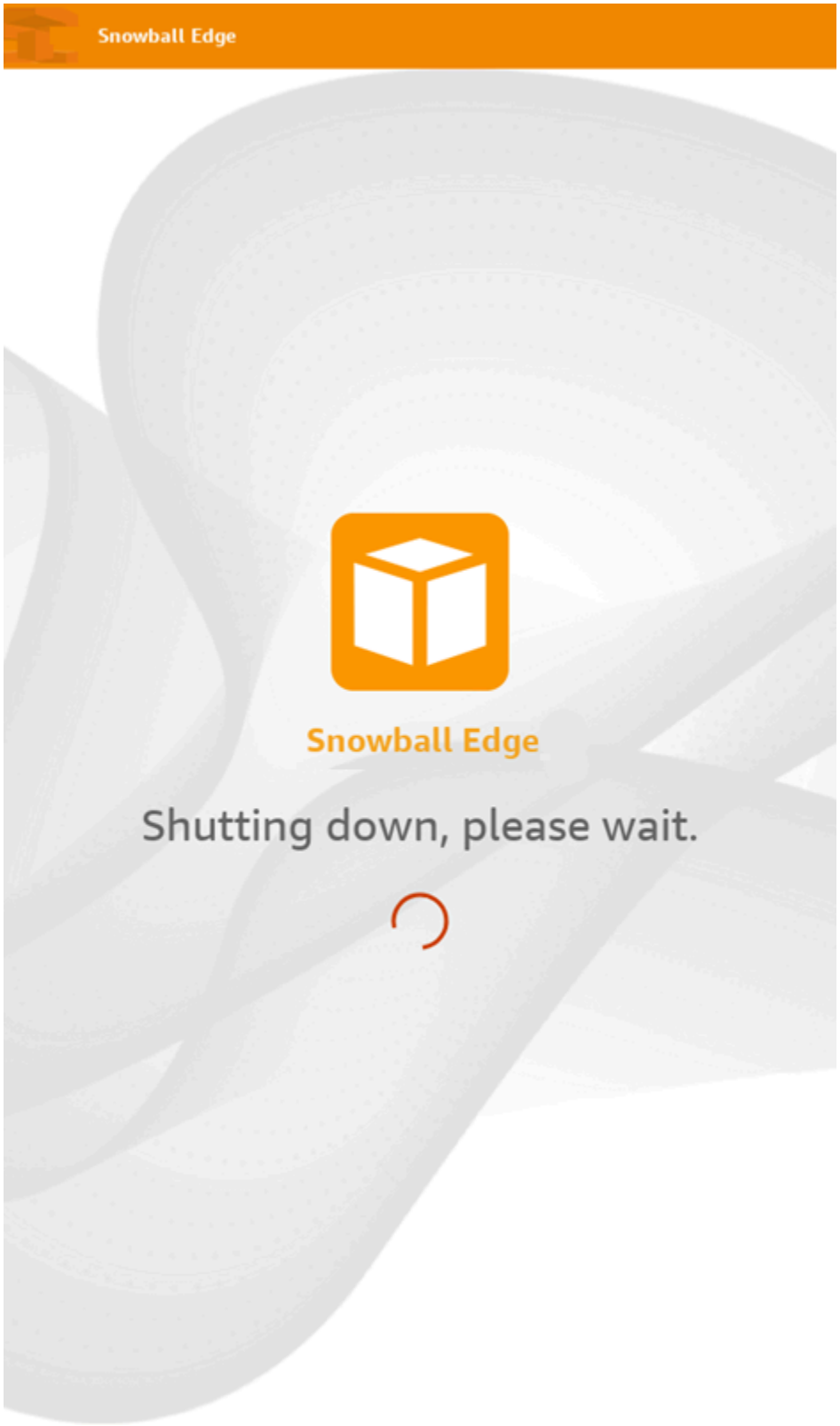
Próximo: Usando um dispositivo AWS Snowball Edge

Reinicializando o dispositivo da Família Snow

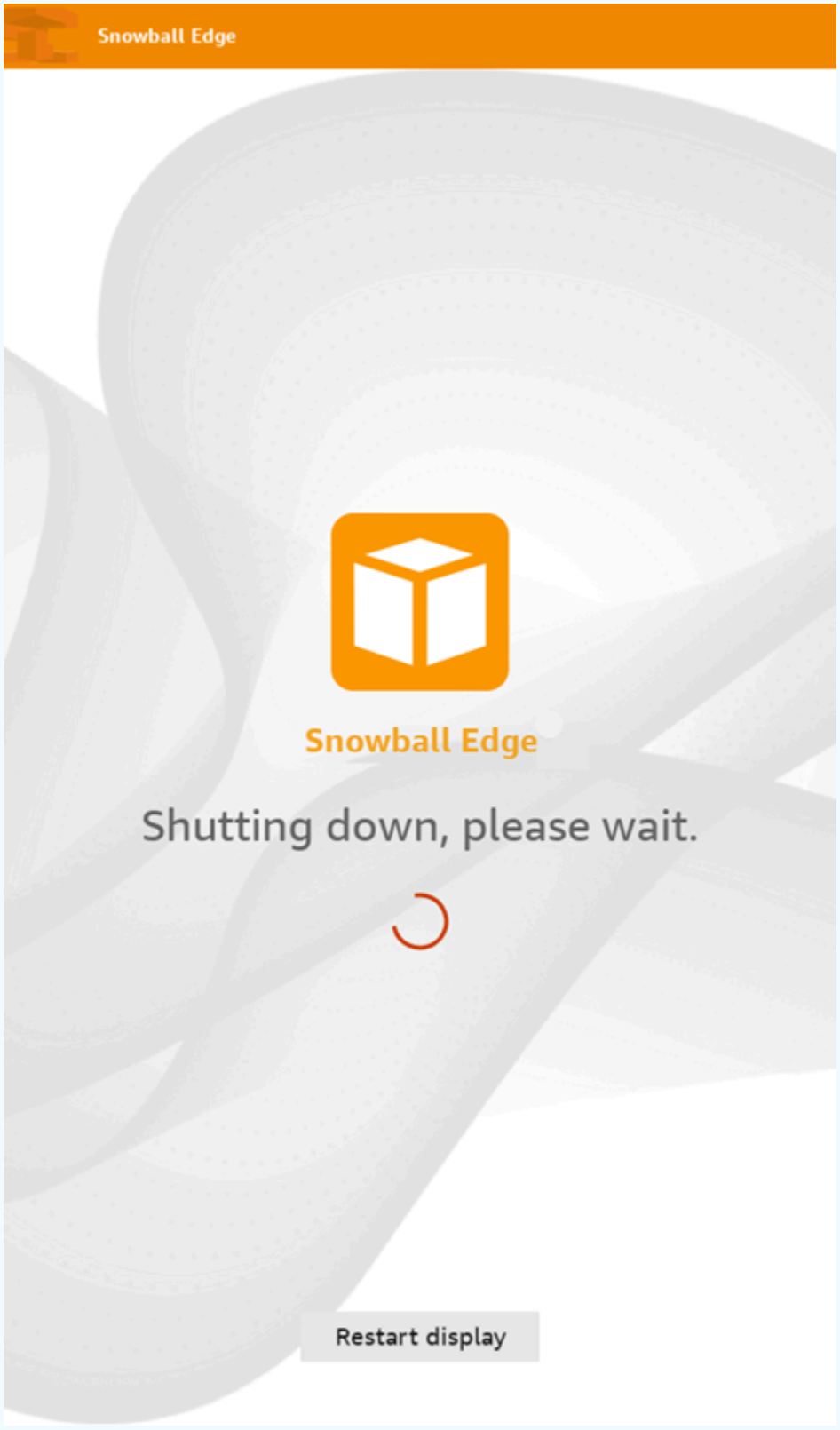
Antes de reinicializar o dispositivo da Família Snow, verifique se todas as transferências de dados para o dispositivo foram interrompidas.

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 acima da tela de LCD. 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.


Snowball Edge
Snowball Edge
Shutting down, please wait.

> **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.


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

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 o dispositivo Snow Family.

Para reinicializar o dispositivo usando o Snowball Edge Client:

1. Quando toda a comunicação com o dispositivo terminar, use o comando `reboot-device` para reinicializá-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.

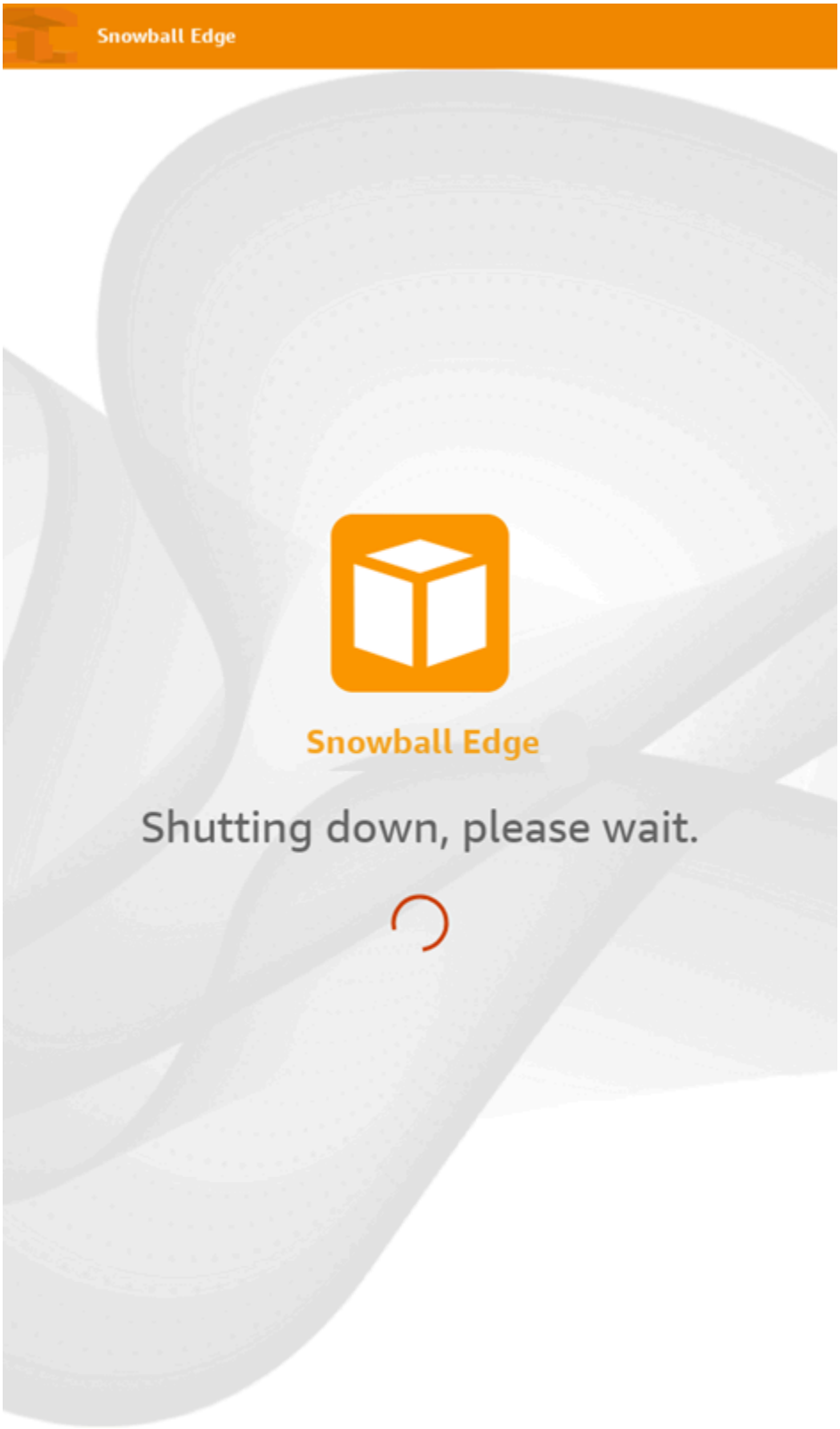
```
snowballEdge reboot-device
```

2. Desbloqueie o dispositivo. Consulte Desbloqueando o dispositivo Snow Family.

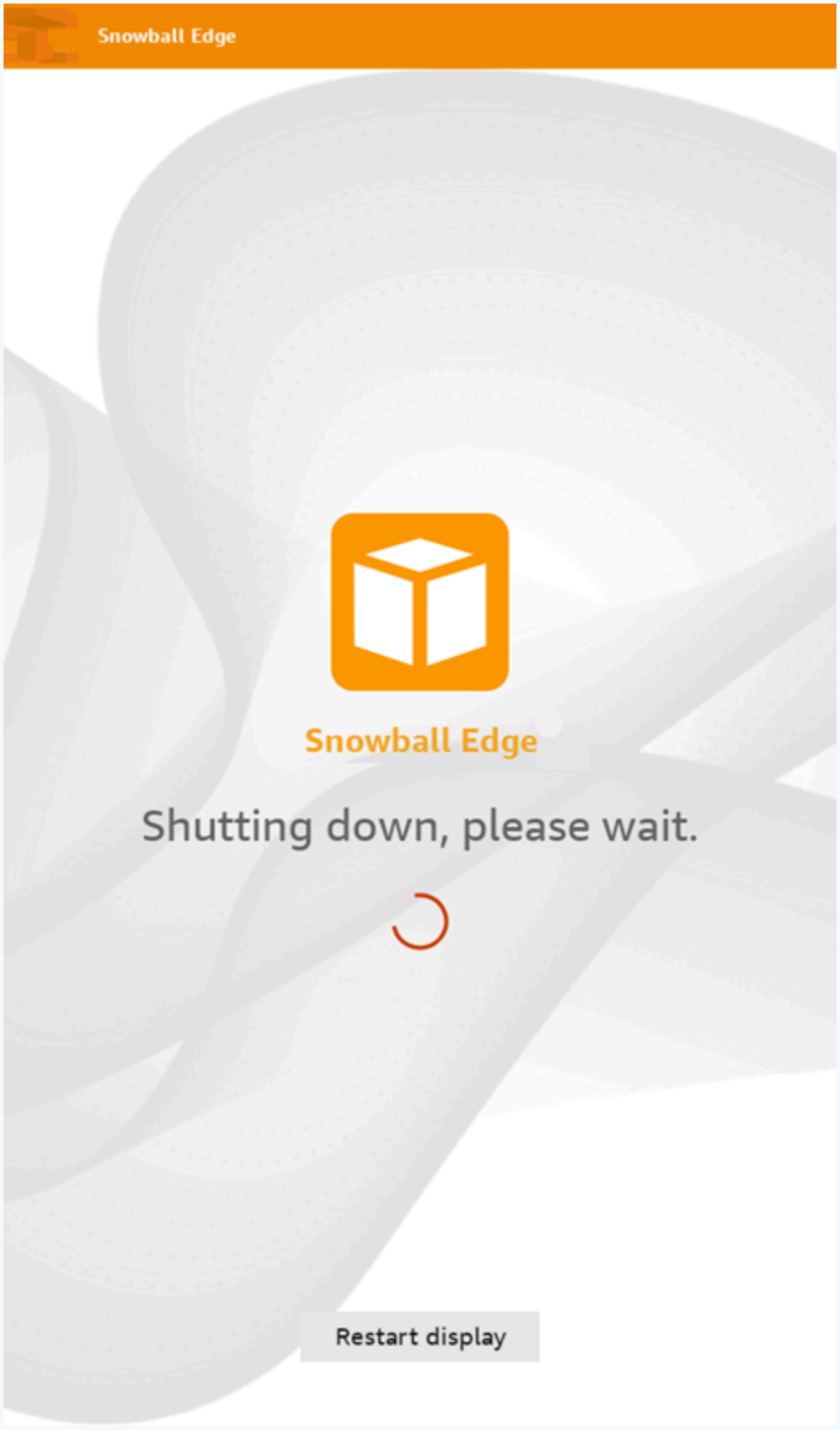
Desligar o Snowball Edge

Quando terminar de transferir os dados para o AWS Snowball Edge dispositivo, prepare-o para a viagem de volta para o. AWS Antes de continuar, 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 obter mais informações, consulte Gerenciando a interface NFS.

Quando todas as comunicações com o dispositivo terminarem, desligue-o pressionando o botão de ligar/desligar acima da tela de LCD. 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.


Snowball Edge
Snowball Edge
Shutting down, please wait.

> **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.



Depois que o dispositivo é desligado, as informações de envio aparecem na tela E Ink.

Próximo: Devolver o dispositivo Snowball Edge

Devolver o dispositivo Snowball Edge

As informações de envio pré-pago na tela E Ink contêm o endereço para devolução do AWS Snowball Edge dispositivo. Para obter informações sobre qual transportadora usar para devolver o dispositivo, consulte Transportadoras.

> **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.

O dispositivo é entregue a uma instalação AWS de triagem e encaminhado para o AWS data center. A empresa de envio informará automaticamente ao Console de Gerenciamento da família AWS Snow um número de rastreamento do trabalho. É possível acessar o número de rastreamento e um link para o site de rastreamento da transportadora visualizando os detalhes do status do trabalho no console ou por meio de chamadas para a API de gerenciamento de trabalhos.

Você pode acompanhar as mudanças de status do seu trabalho por meio dos Console de Gerenciamento da família AWS Snow AWS processos do dispositivo. É possível usar as notificações do Amazon SNS se tiver selecionado essa opção durante a criação do trabalho, ou fazer chamadas para a API de gerenciamento de trabalhos. Para obter mais informações sobre essa API, consulte a Referência da API do AWS Snowball.

Os valores de status final incluem quando o AWS Snowball Edge dispositivo foi recebido AWS, quando a importação de dados começa e quando o trabalho é concluído.

Preparando um dispositivo AWS Snowball Edge para envio

A seguir, explicamos como preparar um AWS Snowball Edge dispositivo e enviá-lo de volta para AWS.

Para preparar um AWS Snowball Edge dispositivo para envio

1. Desconecte e guarde o cabo de alimentação no compartimento para cabos na parte superior do dispositivo AWS Snowball Edge .
2. Feche as portas na parte traseira, superior e frontal do AWS Snowball Edge dispositivo. Pressione-as até ouvir um clique.

Você não precisa embalar o AWS Snowball Edge dispositivo em um contêiner, porque o dispositivo em si é seu próprio contêiner de transporte fisicamente resistente. A tela E Ink na parte superior do dispositivo AWS Snowball Edge exibe as informações do envio para devolução quando o dispositivo é desligado.

Consideração específica do tipo de trabalho

> **Important**
>
> Em caso de importação de dados, não exclua as cópias locais dos dados transferidos até que a importação para o Amazon S3 seja bem-sucedida no final do processo e os resultados da transferência de dados possam ser verificados.

Envio para devolução de dispositivos da Família Snow

O AWS Snowball Edge dispositivo é enviado e entregue a um AWS data center. As informações de envio pré-pago na tela E Ink do dispositivo incluem o endereço para devolução do AWS Snowball Edge dispositivo. A velocidade de envio da devolução corresponde à velocidade de envio original quando você recebeu o dispositivo. É possível acompanhar as alterações de status usando o Console de Gerenciamento da família AWS Snow e acompanhar o andamento do pacote pela transportadora da região.

Para obter mais informações sobre como devolver seu AWS Snowball Edge dispositivo, consulteTransportadoras.

> **Important**
>
> A menos que seja instruído de outra forma AWS, nunca afixe uma etiqueta de remessa separada no AWS Snowball Edge dispositivo. Sempre use as informações de envio exibidas na tela E Ink do AWS Snowball Edge dispositivo.

Transportadoras

Ao criar um trabalho para solicitar um dispositivo Snow Family, você fornece o endereço para o qual enviar o AWS Snowball Edge dispositivo. A operadora que oferece suporte à sua região administra o envio de dispositivos AWS para você e de você de volta para AWS. Será possível ver as informações de envio de saída quando o trabalho atingir o status Preparando remessa.

Há um número de rastreamento para cada AWS Snowball Edge dispositivo enviado. É possível encontrar o número de rastreamento e um link para o site de rastreamento usando o painel de trabalhos do Console de Gerenciamento da família AWS Snow ou a API de gerenciamento de trabalhos.

Essas operadoras são compatíveis com dispositivos AWS Snowball Edge:

- Na Índia, a transportadora é a Blue Dart.
- Na Coreia, no Japão, na Austrália, na Indonésia, em Israel e em Singapura, a transportadora é a Kuehne + Nagel.
- Na China e em Hong Kong, a S.F. Express é a transportadora.
- Para todas as outras regiões, a empresa de remessa é a UPS.

Tópicos

AWS Snowball Edge Recolhas da UPS na UE, EUA, Reino Unido, África do Sul e Canadá

Em geral, a UPS pode retirar o dispositivo na UE, nos EUA, no Reino Unido, na África do Sul e no Canadá. Veja algumas instruções úteis:

- Agende uma coleta diretamente com a UPS ou leve o AWS Snowball Edge dispositivo a uma instalação de entrega de pacotes da UPS para onde será enviado. AWS
- A etiqueta de remessa pré-paga da UPS na tela E Ink contém o endereço de devolução do AWS Snowball Edge dispositivo.
- O AWS Snowball Edge dispositivo é entregue a uma instalação AWS de triagem e encaminhado para um AWS data center. A UPS fornece um número de rastreamento.

> **Important**
>
> A menos que seja instruído de outra forma AWS, nunca afixe uma etiqueta de remessa separada no AWS Snowball Edge dispositivo. Use sempre as informações de envio exibidas na tela E Ink do dispositivo.

A UPS envia dispositivos Snowball Edge aos seguintes países da UE: Áustria, Bélgica, Bulgária, Croácia, República de Chipre, República Tcheca, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Holanda, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Espanha e Suécia.

> **Note**
>
> Os pedidos entre o Reino Unido e os países da União Europeia agora são considerados internacionais e exigem aprovação por meio de um processo internacional especial.
> Se você precisar enviar o dispositivo entre o Reino Unido e a UE, envie um e-mail para `<snowball-shipping@amazon.com>` para solicitar uma fatura comercial antes de organizar a coleta ou a entrega com a UPS.

Os serviços da UPS para a família de produtos Snow são nacionais somente dentro de um país.

AWS Snowball Pickups no Reino Unido

No Reino Unido, lembre-se das seguintes informações para que a UPS colete um dispositivo Snowball Edge:

- Você faz com que a UPS retire o AWS Snowball Edge dispositivo agendando uma coleta diretamente com a UPS, ou leve o AWS Snowball Edge 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 Snowball Edge dispositivo.
- O AWS Snowball Edge 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 Snowball Edge dispositivo. Use sempre as informações de envio exibidas 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 Snowball pickups no Brasil

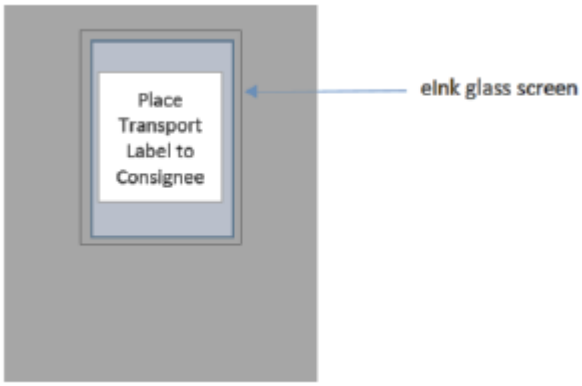
Veja algumas diretrizes para a UPS retirar um dispositivo Snowball Edge no Brasil:

- Quando você estiver pronto para devolver um dispositivo Snowball Edge, ligue para 0800-770-9035 e agende a retirada com a UPS.
- O Snowball Edge 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 Juridica (CNPJ) antes de criar o trabalho.
- É necessário emitir o documento apropriado para devolver o dispositivo Snowball Edge. Confirme com o departamento fiscal quais dos seguintes documentos são necessários em seu estado, de acordo com o registro de Imposto sobre Circulação de Mercadorias e Serviços (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 gerar quatro cópias da declaração: uma para seus registros, as outras três para o transporte.

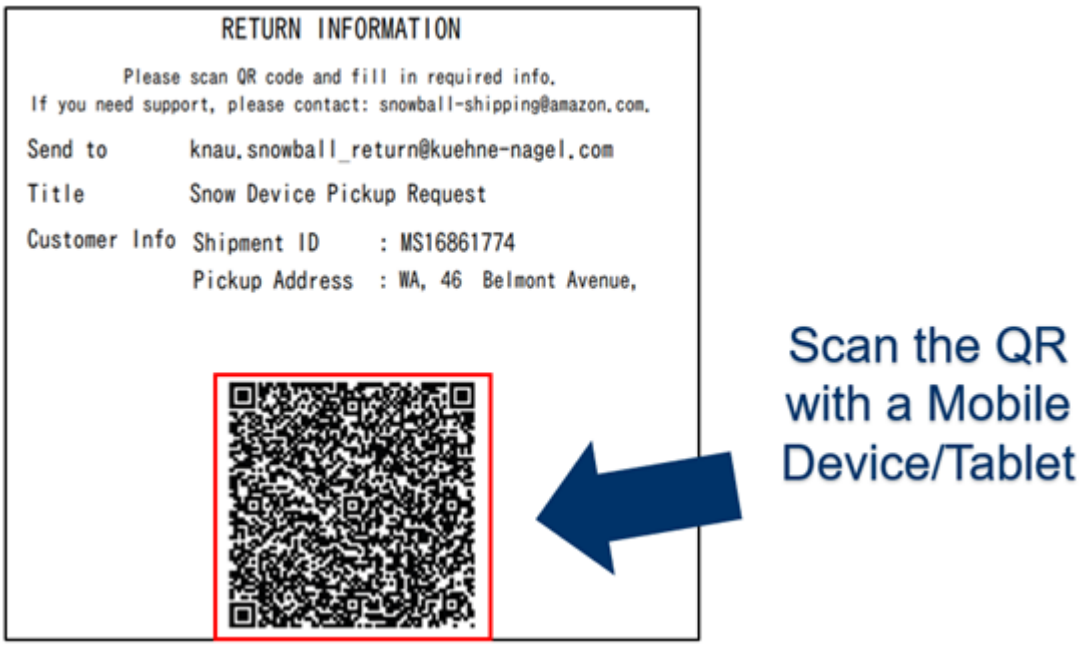
AWS Snowball pickups na Austrália

Na Austrália, se você estiver enviando um AWS Snowball Edge dispositivo de volta AWS, coloque a etiqueta de transporte de devolução (encontrada na embalagem contendo essas instruções) sobre a etiqueta E Ink no dispositivo Snow.



> **Note**
>
> Se você não recebeu uma etiqueta de devolução com o dispositivo, envie um e-mail para knau.snowball_return@kuehne-nagel.com com o número de série do dispositivo ou o número de referência.

Para organizar a devolução do dispositivo da Família Snow, digitalize o código QR nas instruções de devolução do dispositivo móvel. No dispositivo, é exibido um hiperlink para uma mensagem de e-mail. A mensagem contém informações, como endereço de e-mail, assunto e número de controle ou número da remessa. Preencha a data da retirada, o nome e os detalhes de contato ou forneça um novo endereço de retirada se houver alguma alteração.



AWS Snowball pickups na Índia

Na Índia, a Blue Dart retira o dispositivo Snowball. Quando estiver tudo pronto para devolver o dispositivo Snowball, desligue-o e prepare-o para enviá-lo. Para programar a retirada, envie um e-mail para snowball-pickup@amazon.com com o assunto Snowball Pickup Request. No e-mail, inclua as seguintes informações:

- ID do Job — O ID do trabalho associado ao Snowball para o qual você deseja retornar. AWS
- Conta da AWS ID — A ID da AWS conta que criou o trabalho.
- Primeiro horário para retirada (seu horário local): a primeira hora do dia em que o Snowball deve ser retirado.
- Último horário para retirada (seu horário local): a última hora do dia em que o Snowball deve ser retirado.
- Instruções especiais (opcional): todas as instruções especiais para coleta do Snowball, incluindo detalhes de contato para coordenar a coleta.

A equipe do Snowball organiza a retirada com a Blue Dart e envia um e-mail de confirmação para você. A Blue Dart fornece uma etiqueta de envio impressa e retira o dispositivo Snowball.

> **Important**
>
> Ao usar um Snowball na Índia, lembre-se de arquivar todos os documentos de impostos relevantes para o seu estado.

AWS Snowball Captadores Edge na Coreia

Na Coreia, Kuehne + Nagel processa as retiradas. Quando estiver pronto para devolver seu dispositivo, envie um e-mail para snowball-shipping@amazon.com com Snowball 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 Snowball 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 da equipe do Snowball com informações sobre a retirada no endereço fornecido. Reinicie o dispositivo e prepare-se para a retirada, que geralmente ocorre entre 13h e 15h.

AWS Snowball Captadores Edge 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 Snowball na linha de assunto para que possamos agendar a coleta para você. No corpo do e-mail, inclua as seguintes informações:

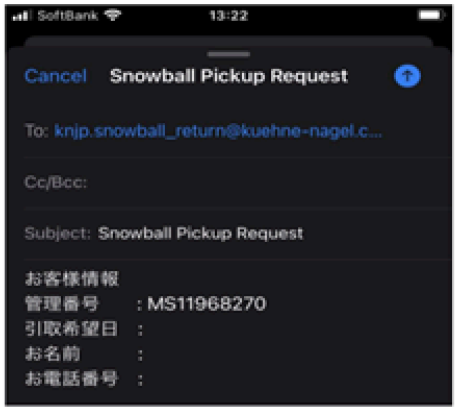
- ID do trabalho
- Conta da AWS ID
- Nome de contato
- Número de telefone para contato
- Endereço de e-mail para contato
- O dia em que você quer que o(s) dispositivo(s) seja(m) retirado(s)
- Horário inicial da retirada
- Último horário de retirada
- Endereço de coleta

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. O número de controle da S.F. Express para a devolução informa quando ele foi entregue.

AWS Snowball Recolhas em Cingapura, Japão e Indonésia

Em Singapura, no Japão e na Indonésia, quando estiver tudo pronto para devolução do dispositivo, digitalize o código QR exibido na etiqueta E Ink de devolução com o dispositivo móvel. Isso levará você diretamente para um modelo de e-mail. Preencha a data/hora e os detalhes de contato da retirada.



> **Note**
>
> Se o endereço de retirada for diferente do endereço em que o dispositivo foi entregue, adicione o novo endereço ao corpo do e-mail para que a transportadora indicada possa ser informada.

> **Note**
>
> No Japão, a transportadora cobra uma taxa de envio de USD 120,00. A descrição da taxa indica Snowball, mas ela se aplica ao envio de todos os dispositivos da Família Snow.

AWS Snowball recebendo e devolvendo em Dubai, Emirados Árabes Unidos

Veja algumas diretrizes que você deve seguir ao receber ou devolver um dispositivo AWS Snowball Edge em Dubai.

Receber um dispositivo Snowball Edge

Ao receber um dispositivo Snowball Edge em uma zona franca, quando você for notificado pela UPS de que o pacote está pronto para entrega, solicite, obtenha e compartilhe a passagem da zona franca.

Se você estiver em uma zona franca ou no continente, assine o comprovante de entrega (POD) ao receber o dispositivo.

Devolver um dispositivo Snowball Edge

Ao devolver um dispositivo Snowball Edge, solicite que a UPS retire o dispositivo agendando a retirada com a UPS diretamente pelo telefone 600 544 743 ou pelo site da UPS. Assegure-se de que as informações de envio para devolução sejam exibidas na tela E Ink antes que o dispositivo seja retirado. Consulte Devolver o dispositivo Snowball Edge. Em uma zona franca, quando receber a notificação de que um motorista da UPS foi designado para retirar o dispositivo, solicite, obtenha e compartilhe a passagem para a zona franca.

As informações de envio pré-pago da UPS na tela E Ink contêm o endereço correto para devolução do dispositivo Snowball Edge.

O dispositivo Snowball Edge é entregue a uma instalação de AWS triagem e encaminhado para o data center. AWS A UPS fornece automaticamente um número de rastreamento para o trabalho.

> **Important**
>
> A menos que seja pessoalmente instruído de outra forma AWS, nunca afixe uma etiqueta de remessa separada no dispositivo Snowball Edge. 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.

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 Snowball Edge dispositivo. Os prazos de entrega são os seguintes:

- Austrália, Indonésia, Japão, Singapura, Coreia do Sul: o prazo de entrega padrão nesses países é de um a três dias.
- Brasil: no 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): os envios para qualquer um dos países da UE também incluem remessa expressa. Normalmente, AWS Snowball Edge os dispositivos enviados por correio expresso são

entregues em cerca de 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.

- Hong Kong: em caso de entregas em Hong Kong, você tem acesso à entrega expressa.
- Índia: na Índia, os dispositivos Snowball Edge são enviados em até sete dias úteis após a AWS receber todos os documentos fiscais correspondentes.
- Dubai, Emirados Árabes Unidos: você tem acesso ao envio Courier Express Saver.
- Reino Unido: no Reino Unido, você tem acesso à remessa expressa. Normalmente, os dispositivos Snowball Edge enviados de forma expressa são entregues em cerca de um dia. Além disso, você tem acesso à remessa padrão, que geralmente leva menos de uma semana, apenas o envio.
- 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.

Monitorar o status da importação

Para monitorar o status do seu trabalho de importação no console, entre no local Console de Gerenciamento da família AWS Snowem Região da AWS que o trabalho foi criado. Na tabela, escolha o trabalho a ser rastreado ou procure-o pelos parâmetros escolhidos na barra de pesquisa acima da tabela. Depois de selecionar o trabalho, as informações detalhadas dele aparecem na tabela, incluindo uma barra que mostra o status do trabalho em tempo real.

> **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.

Depois que seu dispositivo chega AWS, seu status de trabalho muda de Em trânsito AWS para Em AWS. Em média, é necessário um dia para a importação de dados para o Amazon S3 ser iniciada. Quando chegar a hora, o status do trabalho mudará para Importando. Levará aproximadamente o mesmo tempo AWS para importar seus dados do dispositivo Snow Family e para movê-los para o dispositivo Snow Family. Depois que seus dados são importados, o status do trabalho muda para o status Concluído.

Agora, seu primeiro trabalho de importação de dados para o Amazon S3 usando AWS Snowball está concluído. O relatório sobre a transferência de dados pode ser obtido no console. Para acessar esse relatório a partir do console, selecione o trabalho na tabela e expanda-o para mostrar informações detalhadas do trabalho. Selecione Obter relatório para fazer download do relatório de conclusão do trabalho como um arquivo PDF. Para ter mais informações, consulte Obter o relatório e logs de conclusão de trabalho no console.

Próximo: Obter o relatório e logs de conclusão de trabalho no console

Obter o relatório e logs de conclusão de trabalho no console

Quando os dados forem importados ou exportados do Amazon S3, será disponibilizado um relatório de trabalho em PDF para download. Para trabalhos de importação, esse relatório se torna disponível no final do processo de importação. Para trabalhos de exportação, seu relatório de trabalho normalmente fica disponível para você enquanto o AWS Snowball Edge dispositivo da sua peça de trabalho é entregue a você. Não há relatórios de conclusão de trabalho disponíveis para o tipo de trabalho de Uso local.

O relatório do trabalho fornece informações sobre o estado da transferência de dados do seu Amazon S3. O relatório inclui detalhes sobre o trabalho ou parte do trabalho para os registros. O relatório de trabalho também inclui uma tabela que fornece uma visão geral de alto nível do número total de objetos e bytes transferidos entre o dispositivo e o Amazon S3.

Para mais visibilidade do status dos objetos transferidos, é possível observar os dois logs associados: um log de sucessos e um log de falhas. Os logs são salvos no formato de valores separados por vírgulas (CSV) e o nome de cada log inclui o ID do trabalho ou parte de trabalho que o log descreve.

O download do relatório e dos logs pode ser feito no Console de Gerenciamento da família AWS Snow. Veja abaixo um exemplo de relatório.

Snow Family Job Completion Report

Region: us-gov-east-1(OSU)
Job ID: JIDd6d95004-fe1a-42d3-895d-684f357ef840
Snow Device Serial ID: 207117851234
Job type: IMPORT
Device type: Snowball Edge Storage Optimized
Storage type: S3
Job creation date: 2022-06-02 19:32:27.831 GMT
Job state: Completed
Customer address:

123 Any Street
Any Town, USA

Transfer details:

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

Job state transition details:

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

Please review your job's status from the console.
For Snow job details, please see: https://docs.aws.amazon.com/snowball/

Para obter o relatório e os logs do trabalho

1. Faça login no AWS Management Console e abra Console de Gerenciamento da família AWS Snowo.
2. Selecione o trabalho ou a parte do trabalho na tabela e expanda o painel de status.

Há três opções para obter seu relatório de trabalho e os logs: Obter relatório do trabalho, Fazer download do log de êxito e Fazer download do log de falha.

3. Escolha o registro para download.

A lista a seguir descreve os valores possíveis para o relatório:

- Concluído: a transferência foi realizada com êxito. Para obter mais informações detalhadas, consulte o log de sucesso.
- Concluído com erros: nenhum ou alguns dados não foram transferidos. Para obter mais informações detalhadas, consulte o log de falhas.

Próximo: Usando um dispositivo AWS Snowball Edge

Grande migração de dados com AWS Snow Family devices

A migração de grandes volumes de dados de locais on-premises exige planejamento, orquestração e execução cuidadosos para garantir que os dados sejam migrados com sucesso para a AWS.

Recomendamos que você tenha uma estratégia de migração de dados em vigor antes de iniciar a migração para evitar a possibilidade de perda de prazos, excesso de orçamentos e falhas na migração. AWS Os serviços da Snow ajudam você a colocar, solicitar e rastrear seus grandes projetos de migração de dados por meio do recurso Snow Family Large Data Migration Manager (LDMM) no Console de Gerenciamento da família AWS Snow.

Os tópicos Planejar transferências de grande porte e Calibrar uma transferência de grande porte descrevem um processo manual de migração de dados. É possível simplificar as etapas manuais usando o plano de migração do LDMM da Família Snow.

Tópicos

Planejar transferências de grande porte

Recomendamos que você planeje e calibre transferências de grandes volumes dados entre os dispositivos AWS Snowball Edge existentes no local e os servidores usando as diretrizes nas seções a seguir.

Tópicos

Etapa 1: Entender o que você está migrando para a nuvem

Antes de criar seu primeiro trabalho usando o Console de Gerenciamento da família AWS Snow, certifique-se de avaliar o volume de dados que você precisa transferir, onde eles estão armazenados atualmente e o destino para o qual você deseja transferi-los. Em caso de transferências de dados que tenham um petabyte de escala ou mais, fazer essa organização administrativa torna o processo muito mais fácil quando os dispositivos da Família Snow são recebidos.

Se você estiver migrando dados Nuvem AWS para o pela primeira vez, recomendamos que você crie um modelo de migração para a nuvem. A migração para a nuvem não acontece da noite para o dia. Ela requer um processo de planejamento cuidadoso a fim de garantir que todos os sistemas funcionem conforme o esperado.

Ao terminar essa etapa, você saberá a quantidade total de dados que moverá para a nuvem.

Etapa 2: Calcular a taxa de transferência de destino

É importante estimar a rapidez com que os dados podem ser transferidos para os dispositivos da Família Snow conectados a cada servidor. Essa velocidade estimada em MB/s determina a rapidez com que é possível transferir os dados da fonte para os dispositivos Snowball Edge usando a infraestrutura de rede local.

> **Note**
>
> Para transferências de grandes volumes de dados, recomendamos usar o método de transferência de dados do Amazon S3. É necessário selecionar essa opção ao solicitar dispositivos no Console de Gerenciamento da família AWS Snow.

Para determinar uma taxa de transferência básica, transfira um pequeno subconjunto de dados para o dispositivo Snowball Edge ou transfira um arquivo de amostra de 10 GB e observe o throughput.

Ao determinar a velocidade de transferência de destino, lembre-se de que é possível melhorar o throughput. Para isso, ajuste o ambiente, incluindo a configuração da rede, altere a velocidade da rede, o tamanho dos arquivos que serão transferidos e a velocidade com que os dados podem ser lidos nos servidores locais. O adaptador do Amazon S3 copia dados em dispositivos da Família Snow com a rapidez pertinente às condições.

Etapa 3: Determinar quantos dispositivos da Família Snow são necessários

Usando a quantidade total de dados que você planeja mover para a nuvem, a velocidade de transferência estimada e o número de dias para os quais você deseja permitir a movimentação dos dados AWS, determine quantos dispositivos da família Snow você precisa para sua migração de dados em grande escala. Dependendo do tipo de dispositivo, os dispositivos Snowball Edge têm cerca de 39,5 TB, 80 TB ou 210 TB de espaço de armazenamento utilizável. Por exemplo, se você quiser mover 300 TB de dados para AWS mais de 10 dias e tiver uma velocidade de transferência de 250 MB/s, precisará de 4 dispositivos Snowball Edge. Com menos de 40 TB de dados restantes para transferir, AWS Snowcone dispositivos (com 14 TB de espaço utilizável) serão recomendados.

> **Note**
>
> O AWS Snow Family devices LDMM fornece um assistente para estimar o número AWS Snow Family devices que pode ser suportado simultaneamente. Para ter mais informações, consulte Criar um plano de migração de grandes volumes de dados.

Etapa 4: Criar os trabalhos

Depois de saber quantos dispositivos da Família Snow são necessários, você precisa criar um trabalho de importação para cada dispositivo. A criação de vários trabalhos é simplificada pelo LDMM da Família Snow. Para ter mais informações, consulte Implementar a próxima ordem de trabalho.

> **Note**
>
> É possível implementar a próxima ordem de trabalho e adicioná-la automaticamente ao plano diretamente pela Programação recomendada de ordenação de trabalhos. Para ter mais informações, consulte Programação recomendada de ordenação de trabalhos.

Etapa 5: Separar os dados em segmentos de transferência

Como prática recomendada para transferências de grandes volumes de dados que envolvam vários trabalhos, recomendamos separar os dados em vários conjuntos menores e mais gerenciáveis. Isso permite transferir cada partição por vez ou várias partições em paralelo. Ao planejar as

partições, assegure-se de que os dados das partições combinadas correspondam à capacidade dos dispositivos da Família Snow para o trabalho. Por exemplo, é possível separar a transferência em partições de qualquer uma das seguintes formas:

- É possível criar dez partições de 8 TB cada para um Snowball Edge.
- Para arquivos grandes, cada um pode ser uma partição individual de até 5 TB de tamanho para objetos no Amazon S3.
- Cada partição pode ter um tamanho diferente e o mesmo tipo de dados, por exemplo, arquivos pequenos em uma, arquivos compactados em outra, arquivos grandes em outra partição etc. Essa abordagem ajuda você a determinar a taxa de transferência média para diferentes tipos de arquivos.

> **Note**
>
> Operações de metadados são realizadas para cada arquivo transferido. Essa sobrecarga permanece a mesma, independentemente do tamanho de um arquivo. Portanto, é possível obter uma performance mais rápida compactando pequenos arquivos em um pacote maior, colocando os arquivos em lote ou transferindo grandes arquivos individuais.

A criação de segmentos de transferência de dados ajuda a resolver rapidamente qualquer problema na transferência, pois pode ser complexo tentar solucionar problemas em uma transferência heterogênea de grandes volumes após um dia ou mais de andamento.

Ao terminar de planejar a transferência de dados em escala de petabytes, recomendamos transferir alguns segmentos do servidor para o dispositivo da Família Snow com o objetivo de calibrar a velocidade e o tempo total de transferência.

Calibrar uma transferência de grande porte

É possível calibrar a performance da transferência movendo um conjunto representativo das partições de dados. Selecione várias partições definidas e transfira-as a um dispositivo da Família Snow. Faça um registro da velocidade de transferência e do tempo total de transferência para cada operação. Se os resultados da calibração forem inferiores à taxa de transferência de destino, será possível copiar várias partes da transferência de dados ao mesmo tempo. Nesse caso, repita a calibração com as partições adicionais do conjunto de dados.

Continue adicionando operações de cópia paralelas durante a calibração até ver menos retornos na soma da velocidade de transferência de todas as instâncias que estiverem transferindo dados no momento. Finalize a última instância ativa e anote a nova taxa de transferência de destino.

É possível transferir dados mais rapidamente para os dispositivos da Família Snow transferindo dados paralelamente usando um dos seguintes cenários:

- Usando várias sessões do adaptador do S3 em uma estação de trabalho em um único dispositivo da Família Snow.
- Usando várias sessões do adaptador do S3 em várias estações de trabalho em um único dispositivo da Família Snow.
- Usando várias sessões da interface do S3 (utilizando uma ou várias estações de trabalho) para vários dispositivos da Família Snow.

Ao concluir essas etapas, você saberá a rapidez com que pode transferir dados para um dispositivo da Família Snow.

Criar um plano de migração de grandes volumes de dados

O recurso de AWS Snow Family grande plano de migração de dados permite que você planeje, acompanhe, monitore e gerencie grandes migrações de dados de 500 TB para vários petabytes usando vários produtos de serviços da família Snow.

Use o recurso de grande plano de migração de dados para coletar informações sobre as metas de migração de dados, como o tamanho dos dados para os quais migrar AWS e o número de dispositivos da família Snow necessários para migrar os dados simultaneamente. Use o plano para criar um cronograma projetado para o projeto de migração de dados e a programação recomendada de ordenação de trabalhos para concretizar as metas.

> **Note**
>
> No momento, o plano de migração de dados está disponível para trabalhos de importação maiores que 500 TB.

Tópicos

- Etapa 1: Selecionar os detalhes da migração

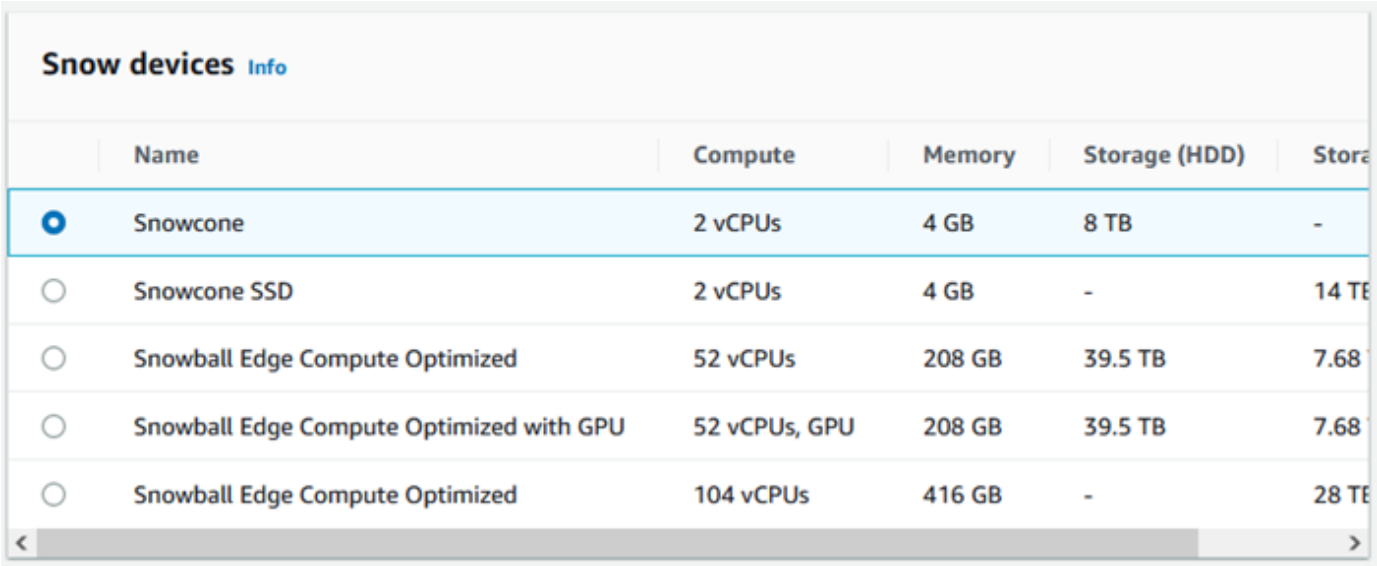
- Etapa 2: Selecionar as preferências de segurança, envio e notificação
- Etapa 3: Revisar e criar o plano

Etapa 1: Selecionar os detalhes da migração

> **Note**
>
> Um plano de migração de grandes volumes de dados está disponível para migrações maiores que 500 TB. Crie ordens de trabalho individualmente nos dispositivos da Família Snow para os projetos de transferência de dados com menos de 500 TB. Para obter mais informações, consulte Criação de um trabalho para solicitar um dispositivo Snow Family neste guia.

1. Faça login no Console de Gerenciamento da família AWS Snow. Se esta é a primeira vez que você usa o Console de Gerenciamento da família AWS Snow in this Região da AWS, você vê a AWS Snow Family página. Caso contrário, você verá a lista de trabalhos existentes.
2. Se esse for seu primeiro plano de migração de dados, selecione Criar seu plano de migração de grandes volumes de dados na página principal. Caso contrário, selecione Plano de migração de grandes volumes de dados. Selecione Criar plano de migração de dados para abrir o assistente de criação de planos.
3. Em Nomeie seu plano de migração de dados, forneça um Nome do plano de migração de dados. O nome do plano pode ter até 64 caracteres. Os caracteres válidos A-Z, a-z, 0-9 e . _ - (hífen). O nome do plano não deve começar com **`aws:`**.
4. Em Total de dados a serem migrados AWS, insira a quantidade de dados para a qual você deseja migrar. AWS
5. Em Dispositivos Snow, selecione um dispositivo da Família Snow.

   > **Note**
   >
   > As opções de dispositivos compatíveis podem variar de acordo com a disponibilidade dos dispositivos em determinadas Regiões da AWS.



6. Em Dispositivos simultâneos, insira o número de dispositivos da Família Snow para os quais você pode copiar dados simultaneamente em sua localização. Se não tiver certeza, vá para a próxima seção e obtenha informações sobre como usar o assistente de estimativa de dispositivos simultâneos.
7. Escolha Próximo.

Usar o assistente de estimativa de dispositivos simultâneos

O assistente de estimativa de dispositivos simultâneos ajuda você a determinar o número de dispositivos simultâneos que você pode usar durante migrações de grandes volumes de dados.

Pré-requisitos:

- Você realizou uma prova de conceito para testar a metodologia de transferência de dados e mediu a performance com um dispositivo da Família Snow no ambiente.
- Você conhece a rede e a conexão com o armazenamento de back-end.

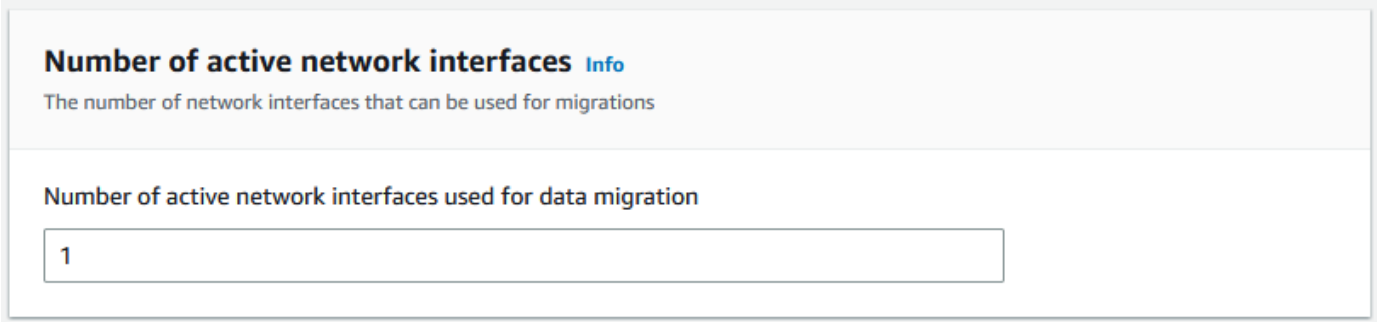
Etapa 1: Inserir as informações da fonte de dados

Primeiro, descubra o throughput teórico máximo para copiar dados da fonte de armazenamento.

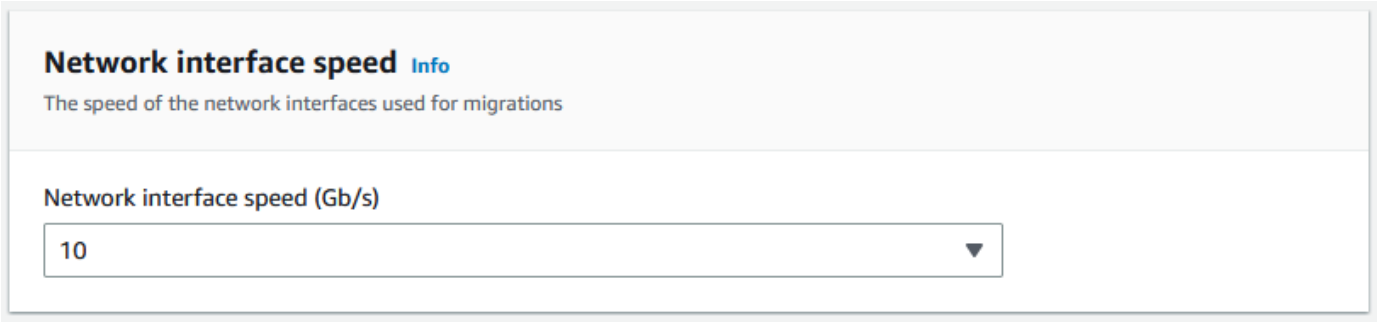
1. Em Total de dados a serem migrados, insira a quantidade de dados que pretende migrar.

Em Unidade, selecione a unidade de medida (GB ou TB) para a quantidade de dados a serem migrados.

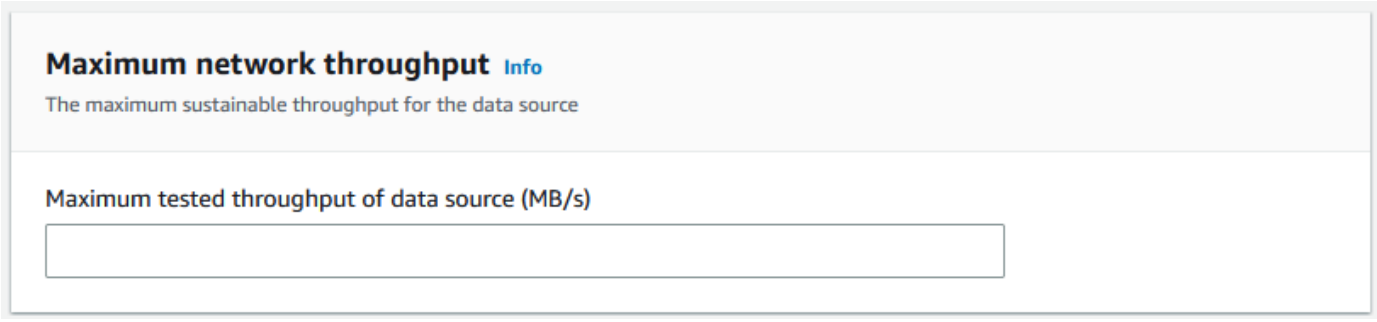
2. Em Número de interfaces de rede ativas, insira o número de interfaces de rede ativas disponíveis para migração de dados da fonte de armazenamento.



3. Em Velocidade da interface de rede, selecione a velocidade da interface de rede para a fonte de armazenamento. As velocidades da rede estão em Gb/s.



4. Em Throughput máximo de rede, insira o throughput máximo da rede testada para a fonte de armazenamento que você determinou durante a prova de conceito. O throughput é definido em MB/S.

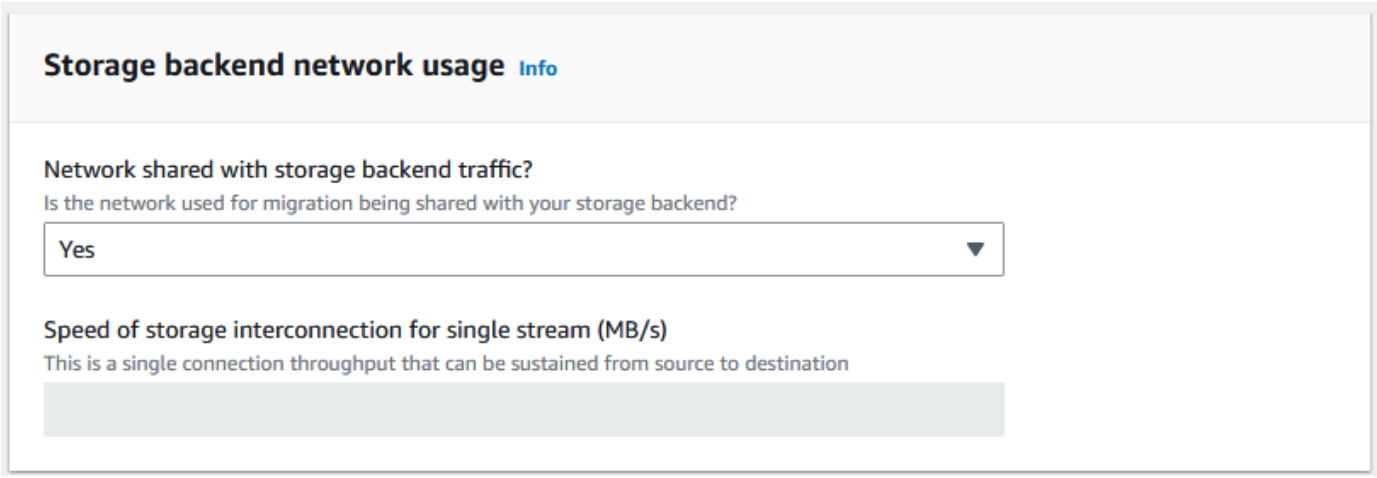


5. Em Uso de rede de back-end de armazenamento, indique se a fonte de armazenamento compartilha uma rede com o armazenamento de back-end.

   - Selecione Sim se a rede não for compartilhada. Não é necessário inserir a velocidade da interconexão de armazenamento para um único fluxo.

- Selecione Não se a rede for compartilhada. Insira a velocidade da interconexão de armazenamento para um único fluxo em MB/s.

Com base na escolha, o assistente atualiza o valor Throughput máxima de migração para a fonte de dados (MB/s) na parte inferior da página.



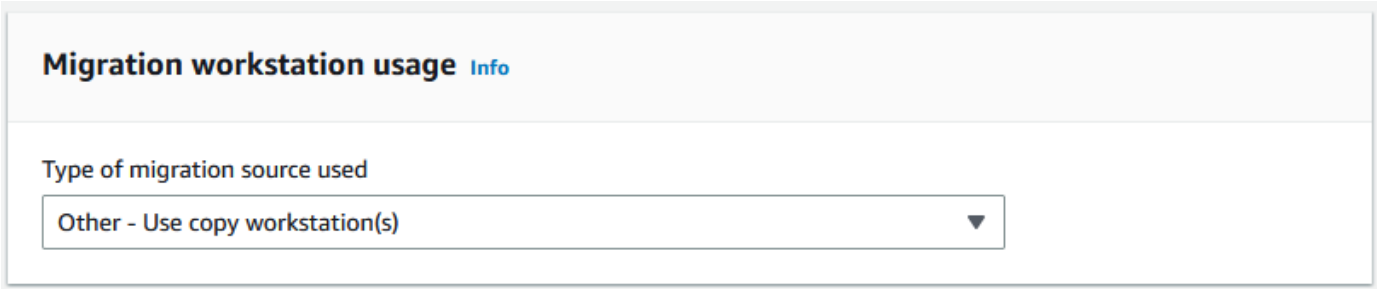
6. Escolha Próximo.

Etapa 2: Inserir os parâmetros da estação de trabalho da migração

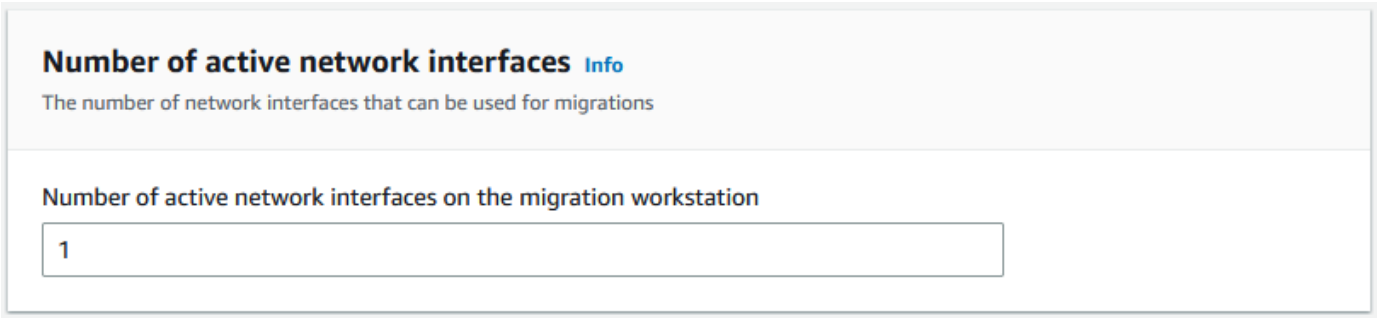
É possível conectar os dispositivos da Família Snow diretamente à fonte de armazenamento (um servidor Microsoft Windows, por exemplo). Em vez disso, é possível optar por conectar os dispositivos da Família Snow a uma ou mais estações de trabalho para copiar dados da fonte de armazenamento.

1. Em Uso da estação de trabalho de migração, indique a opção de uso da estação de trabalho.

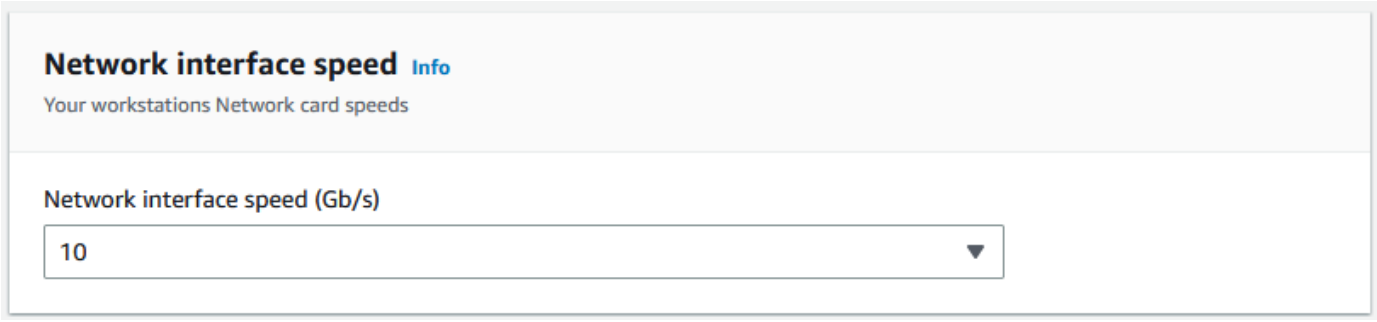
   - Selecione Nenhum: Use a fonte de dados diretamente para transferir dados diretamente de uma fonte de dados sem usar uma estação de trabalho e, depois, selecione Próximo.
   - Selecione Outros - Usar estações de trabalho de cópia para usar uma ou mais estações de trabalho para transferir dados.



2. Em Número de interfaces de rede ativas, insira o número de portas a serem usadas para migração de dados.

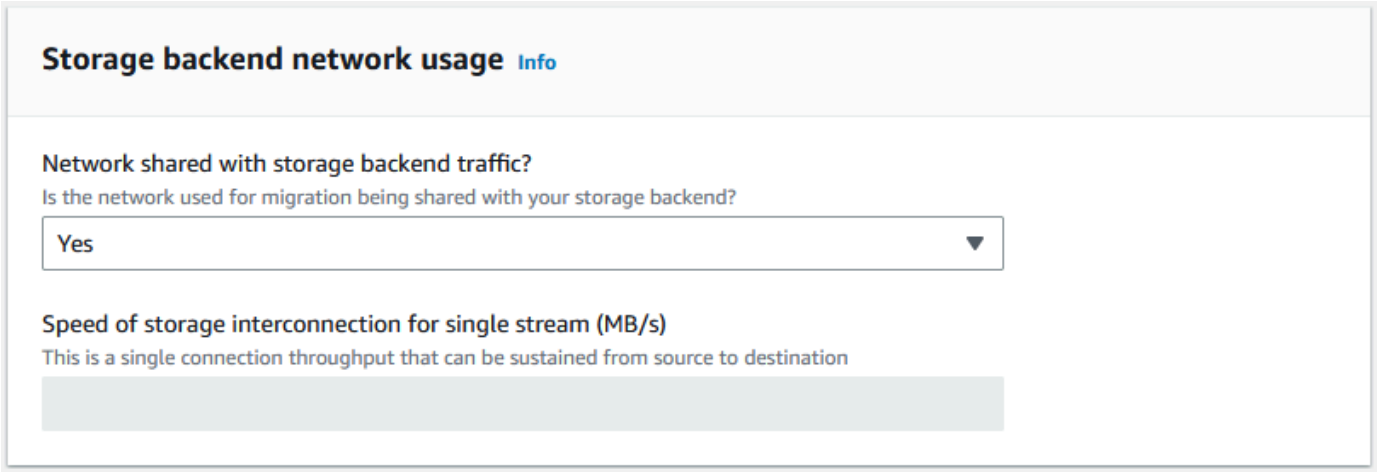


3. Em Velocidade da interface de rede, selecione a velocidade em Gb/s das interfaces de rede.

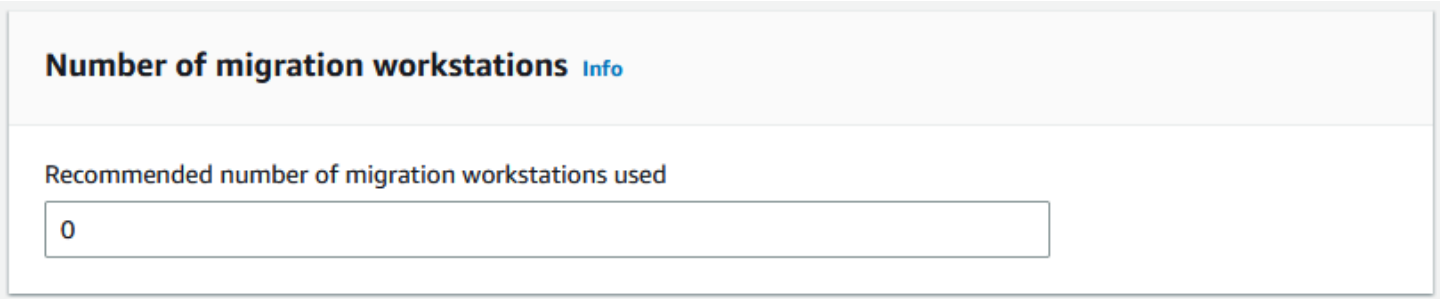


4. Em Uso de rede de back-end de armazenamento, indique se a rede na qual estão as estações de trabalho é compartilhada com o armazenamento de back-end.

   - Selecione Sim se for compartilhada.
   - Selecione Não se não for compartilhada. Insira a velocidade da interconexão de armazenamento para um único fluxo em MB/s.

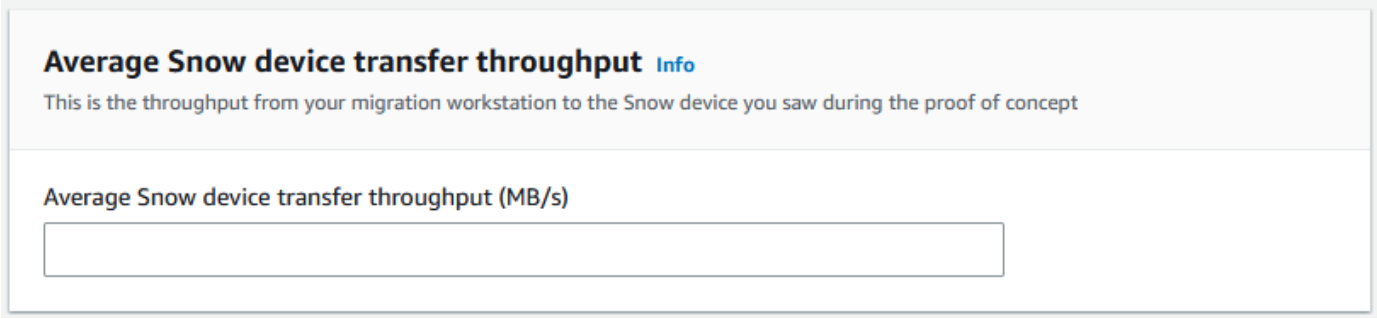


Com base na entrada, o assistente exibe uma recomendação em Número de estações de trabalho de migração. É possível alterar manualmente o número caso não concorde com a recomendação. Esse número será exibido em Dispositivos simultâneos no plano de migração de grandes volumes de dados.



Etapa 3: Inserir o throughput médio de transferência dos dispositivos da Família Snow

1. No campo Throughput de transferência média do dispositivo Snow, insira o throughput em MB/s observado durante a prova de conceito.



Com base no throughput médio, o assistente atualiza o Número recomendado de dispositivos Snow simultâneos e o Número máximo de dispositivos simultâneos nos detalhes do plano de migração.

2. Selecione Use este número para continuar e volte para escolher os detalhes da migração. Selecione Próximo para passar para a próxima etapa (Etapa 2: Selecionar as preferências de segurança, envio e notificação).

> **Note**
>
> É possível usar até cinco dispositivos Snow simultâneos.

Etapa 2: Selecionar as preferências de segurança, envio e notificação

1. Na seção Endereço de entrega, selecione um endereço existente ou adicione outro.

   - > **Note**
     >
     > O país indicado no endereço deve corresponder ao país de destino do dispositivo e deve ser válido para esse país.

2. Em Escolha o tipo de acesso de serviço, siga um destes procedimentos:

   - Permita que a Snow Family crie uma nova função vinculada ao serviço para você com todas as permissões necessárias para publicar CloudWatch métricas e notificações do Amazon SNS para seus trabalhos na Snow Family.
   - Adicione um perfil de serviço existente que tenha as permissões necessárias. Para obter um exemplo de como configurar esse perfil, consulte Exemplo 4: Permissões de perfil esperadas e política de confiança.

3. Em Enviar notificações, decida se deseja enviar notificações. Observe que, se selecionar Não enviar notificação sobre planos de migração de dados, não receberá notificações desse plano, mas ainda receberá notificações de trabalho.

4. Em Definir notificações,

   - Selecione Usar um tópico do SNS existente.
   - ou Criar um novo tópico do SNS.

Etapa 3: Revisar e criar o plano

1. Revise as informações em Detalhes do plano e em Preferências de envio, segurança e notificação e edite, se necessário.
2. Selecione Criar plano de migração de dados para criar o plano.

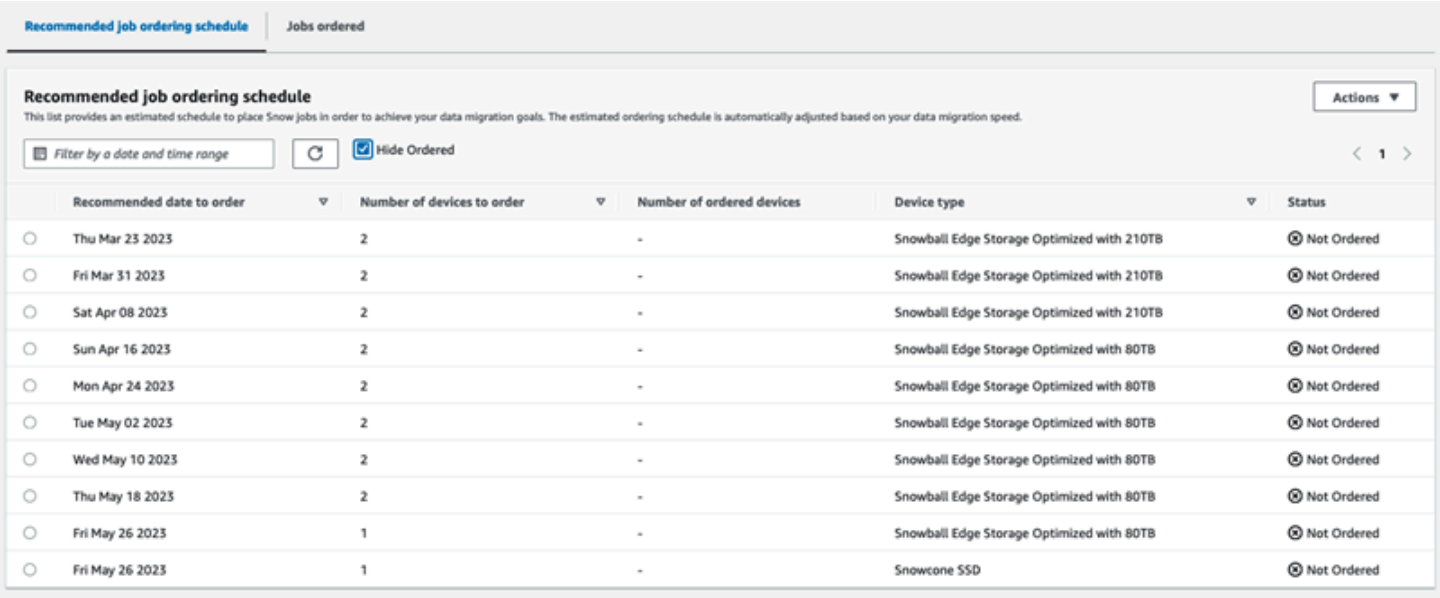
Usar o plano de migração de grandes volumes de dados

Depois de criar o plano de migração de grandes volumes de dados, é possível usar a programação e o painel resultantes para guiá-lo pelo restante do processo de migração.

Programação recomendada de ordenação de trabalhos

Depois de criar um AWS Snow Family devices grande plano de migração, você pode usar o cronograma de pedidos de trabalho recomendado para criar novos trabalhos.

> **Note**
>
> As atualizações manuais feitas no tamanho do volume de dados ou no número de dispositivos simultâneos ajustam a programação. A programação será ajustada automaticamente se um trabalho não tiver sido ordenado até a data da ordem recomendada ou tiver sido ordenado antes da data da ordem recomendada. Se um trabalho for devolvido antes da data da ordem recomendada, a programação será ajustada automaticamente.



Implementar a próxima ordem de trabalho

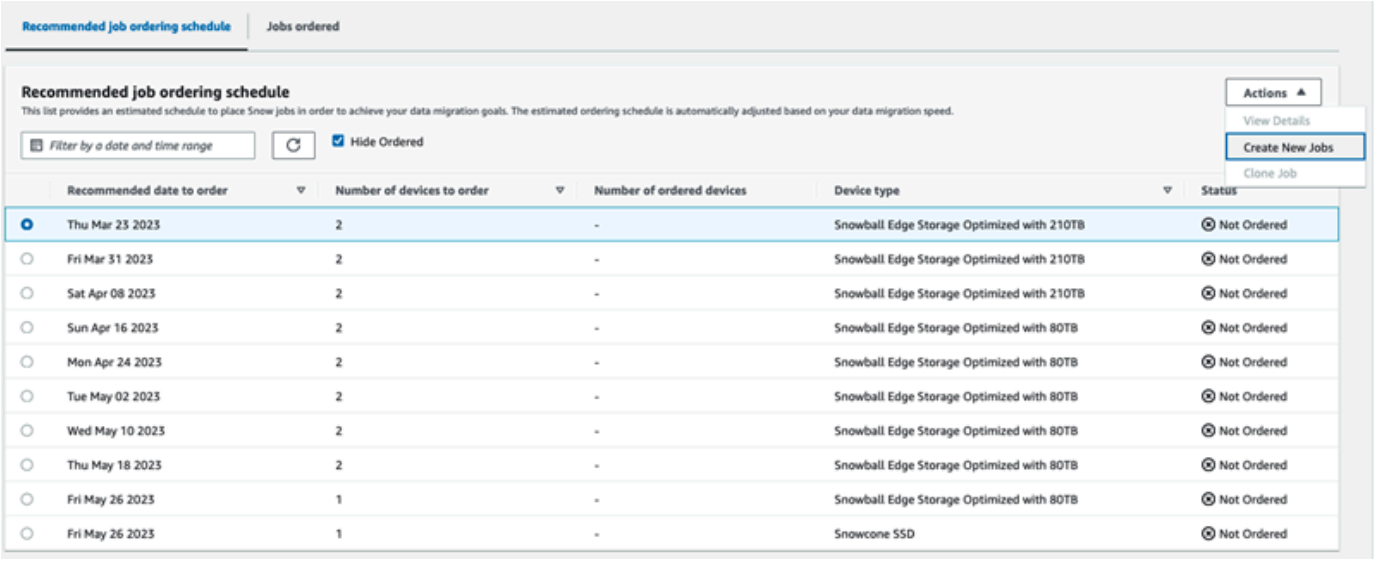
Para implementar a próxima ordem, em vez de criar manualmente um trabalho e depois adicioná-lo ao plano, há a opção de clonar um trabalho ordenado anteriormente ou criar um trabalho pré-preenchido.

Como clonar um trabalho:

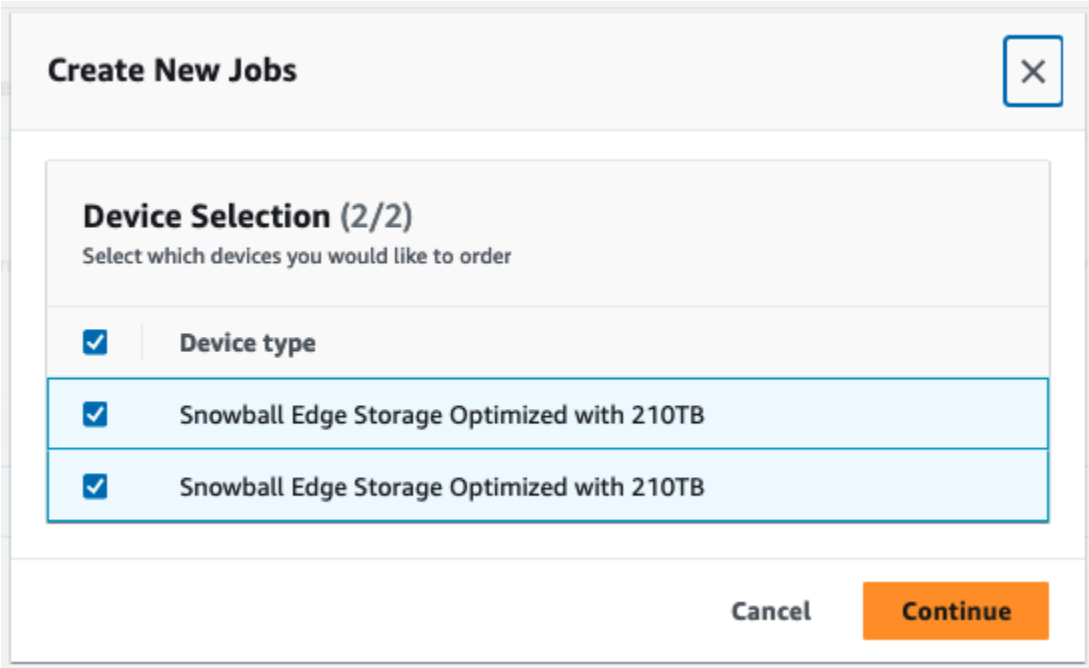
1. Selecione a próxima ordem (a primeira recomendação com o status Não solicitado) na Programação recomendada de ordenação de trabalhos e, depois, selecione Clonar trabalho no menu Ações. A janela Clonar trabalho é exibida.
2. Na janela Clonar trabalho, na seção Trabalhos ordenados, selecione o trabalho a ser clonado.
3. Na seção Detalhes dos novos trabalhos, selecione os dispositivos que você deseja solicitar. Para cada dispositivo selecionado, o Nome do trabalho será preenchido automaticamente com base no trabalho selecionado. É possível substituir o nome do trabalho.
4. Selecione Confirmar para implementar a ordem de trabalhos para os dispositivos selecionados. O sistema vai clonar o trabalho para cada dispositivo.

Como criar trabalhos:

1. Selecione a próxima ordem (a primeira recomendação com o status Não solicitado) na Programação recomendada de ordenação de trabalhos e, depois, selecione Criar novos trabalhos no menu Ações. A janela Criar novos trabalhos é exibida.



2. Na seção Seleção de dispositivo, selecione os dispositivos que você deseja solicitar. Escolha Continuar.



3. A página Criar novo é exibida. A maioria dos parâmetros, como tipo de trabalho, endereço de entrega e tipo de dispositivo, é definida com base no plano. O sistema vai criar o trabalho para cada dispositivo.

É possível ver se o trabalho ou os trabalhos foram criados com êxito ou não. Os trabalhos criados com êxito são automaticamente adicionados ao plano.

Lista de trabalhos ordenados

Cada plano exibe uma lista de trabalhos ordenados. No início, está vazio. Ao começar a ordenar trabalhos, é possível adicionar trabalhos ao plano selecionando Adicionar trabalho no menu Ações. Os trabalhos adicionados aqui são controlados no painel de monitoramento.

Da mesma forma, é possível remover o trabalho da lista de trabalhos ordenados selecionando Remover trabalho no menu Ações.

Recomendamos usar a programação de ordenação de trabalhos fornecida no plano para realizar uma migração de dados tranquila.

Painel de monitoramento

Depois de adicionar trabalhos ao seu plano, você pode ver as métricas no painel à medida que os trabalhos retornam AWS para ingestão. Estas métricas podem ajudar você a acompanhar o andamento:

- Dados migrados para AWS — A quantidade de dados para os quais foram migrados AWS até o momento.
- Média de dados migrados por trabalho: a quantidade média de dados por trabalho em terabytes.
- Total de trabalhos do Snow: o número de trabalhos do Snowball Edge ordenados em comparação com os trabalhos restantes a serem ordenados.
- Duração média de um trabalho de migração: a duração média de um trabalho em dias.
- Status do trabalho do Snow: o número de trabalhos em cada status.

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 o 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.

Tópicos

- Automatizar suas tarefas de gerenciamento
- 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.

2. Na seção AWS OpsHub, 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.

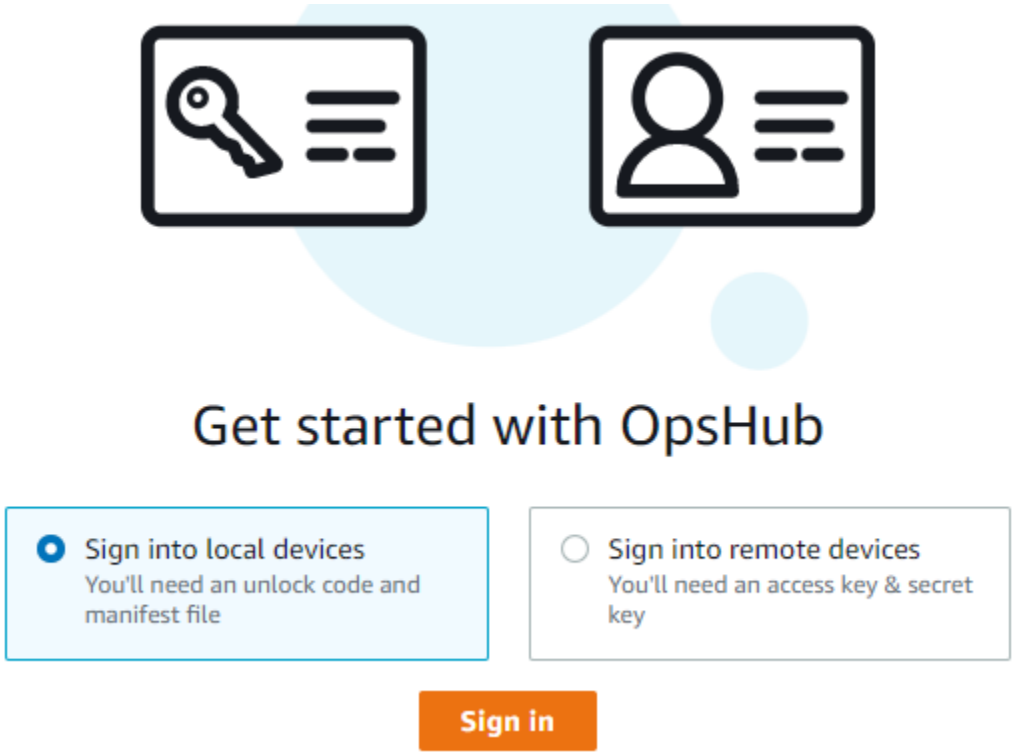
Para obter informações sobre como habilitar o gerenciamento remoto e criar uma conta associada, consulte Ativando o gerenciamento de dispositivos Snow.

Tópicos

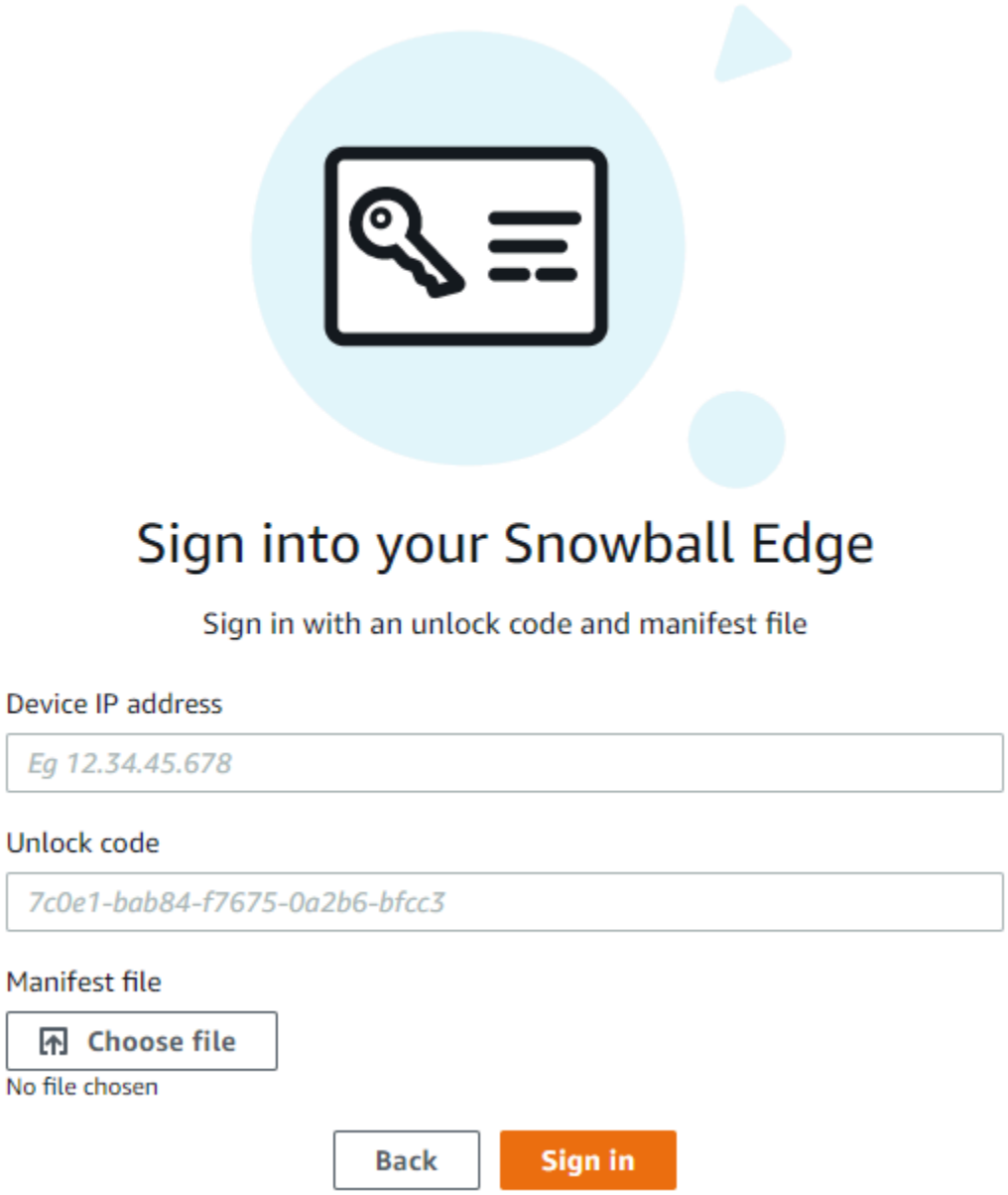
Desbloquear um dispositivo localmente

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.



5. Na página Entrar em dispositivos locais, escolha o tipo de dispositivo da Família Snow e, em seguida, escola 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.



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.

Para dispositivos que foram AWS Snow Device Management instalados, você pode escolher Ativar gerenciamento remoto para ativar o recurso. Para ter mais informações, consulte Usar o AWS Snow Device Management para gerenciar dispositivos.

Desbloquear um dispositivo remotamente

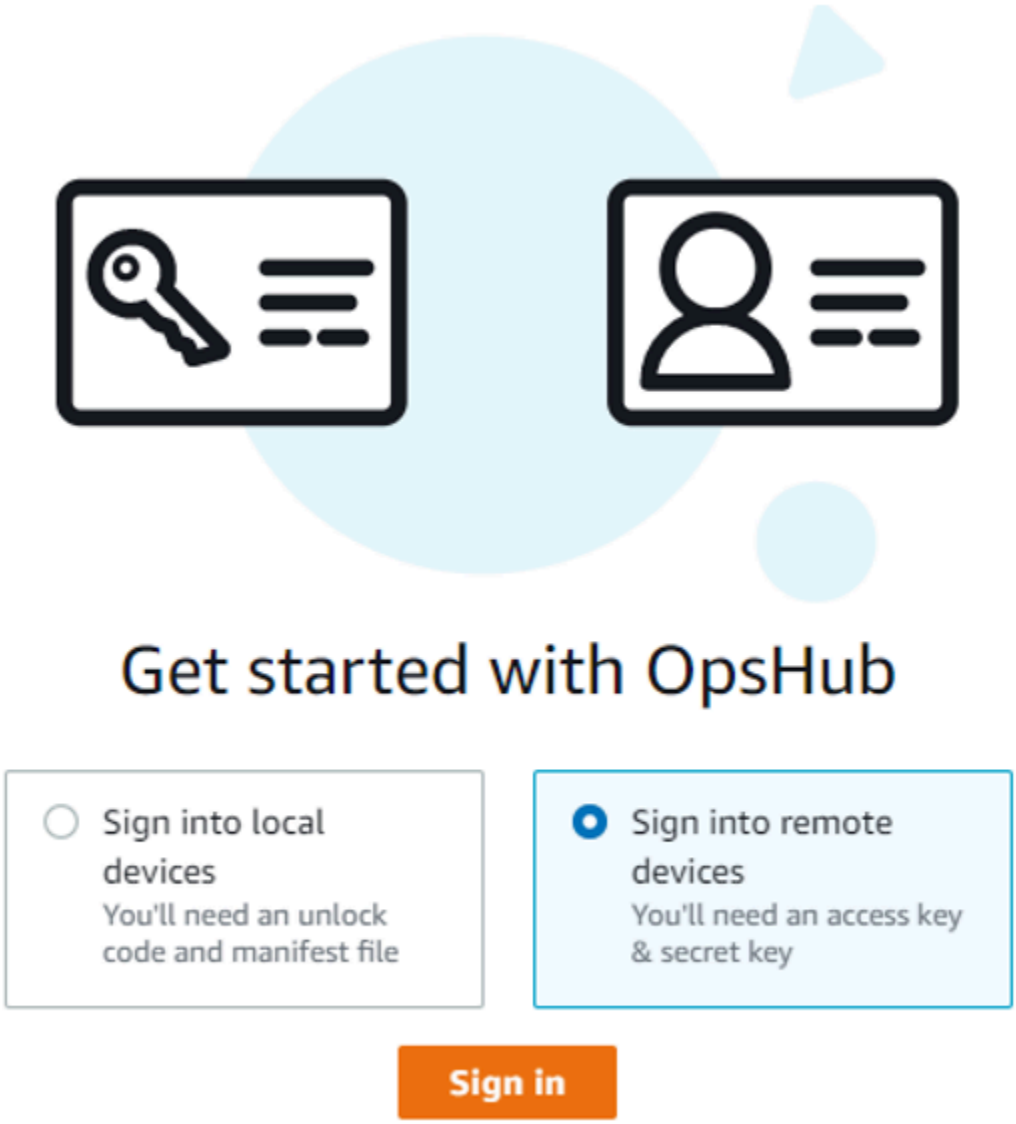
Para desbloquear um dispositivo Snow Family, não

Como conectar e desbloquear o dispositivo remotamente

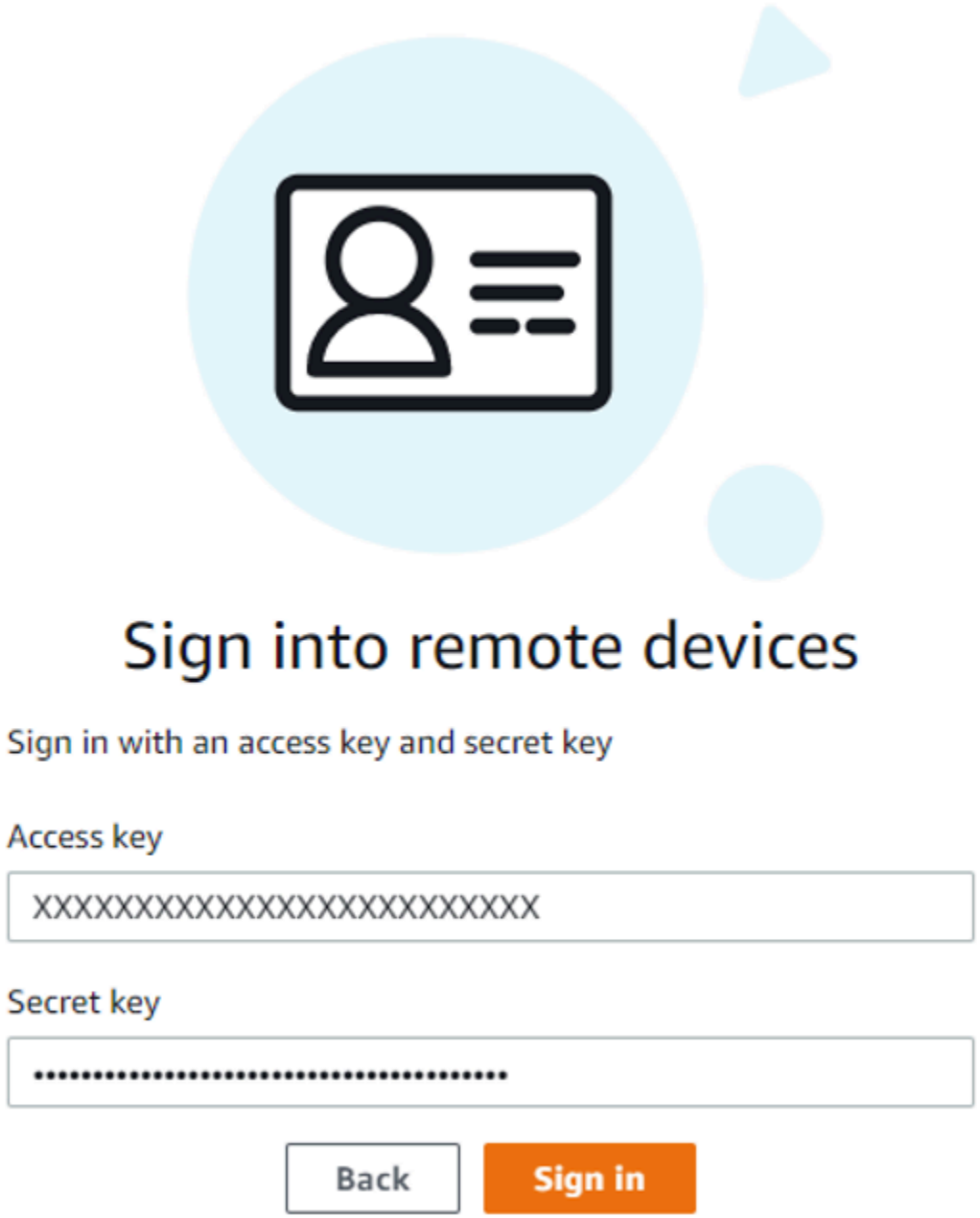
1. Abra a aba do dispositivo, localize o cabo de alimentação e conecte o dispositivo a uma fonte de alimentação.
2. Conecte o dispositivo à rede usando um cabo Ethernet (normalmente um cabo RJ45), abra o painel frontal e ligue o dispositivo.

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

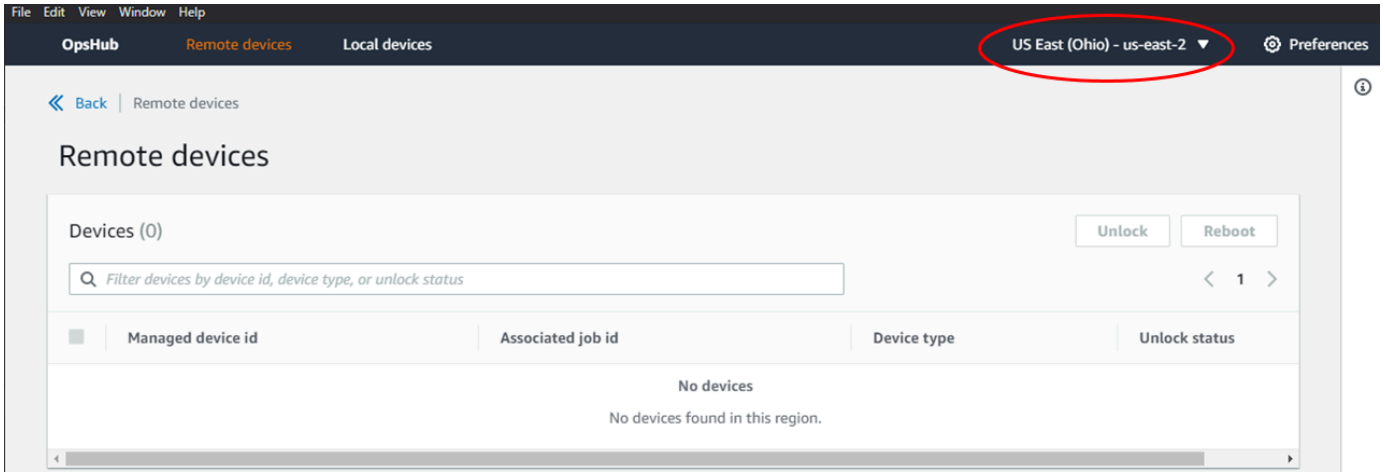
3. Abra o AWS OpsHub aplicativo. Se você for um usuário iniciante, será solicitado a escolher um idioma e selecionar Próximo. Em seguida, escolha Próximo.
4. Na OpsHub página Começar com, escolha Entrar em dispositivos remotos e, em seguida, escolha Entrar.



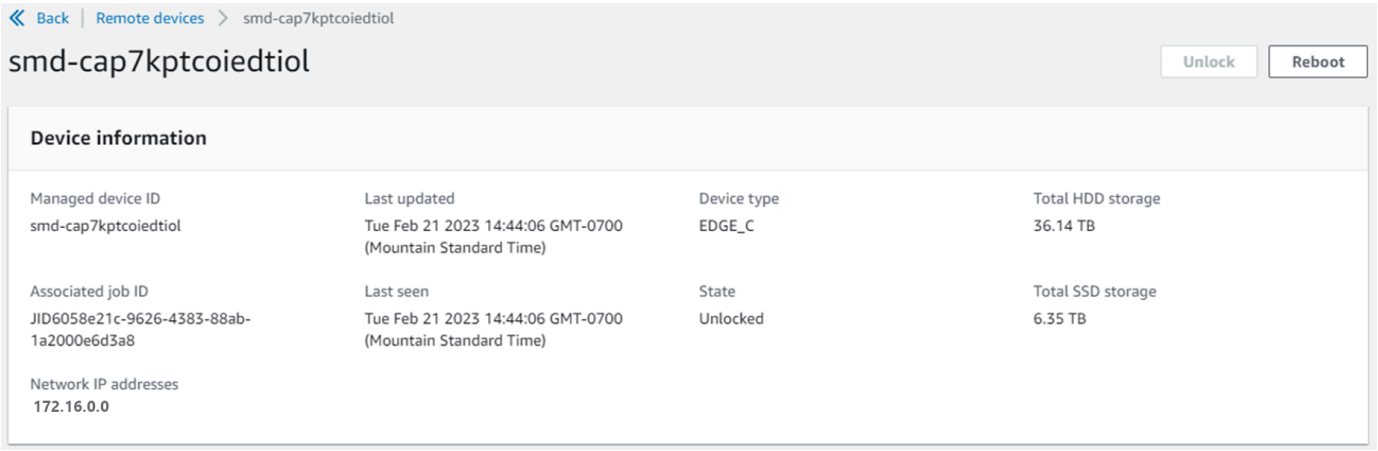
5. Na página Entrar em dispositivos remotos, insira as credenciais AWS Identity and Access Management (IAM) (chave de acesso e chave secreta) do Conta da AWS que está vinculado ao seu dispositivo e escolha Entrar.



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.



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+mUqJT9aJ1rr0QFGVD1bMogecUPflTWlDkEEpG8ZbX5P8vR+EElO/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmIO7j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZXcI/+u+99YLaugJIP6ZYIeDfpxnghqyVtaappBFTAyfG67Y
N/5mea1VqJzd8liFpIFQnl+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvfTb47bbv9Z28Vl284
4lw2w1Bl007FoO2v/Y0ukrN3VHCpmJQS1IiqZbYRa0DVK6UR5QNvUlj5fwWs
4qW9UDPhT/HDuaMrMFCejEn/7wvRUrGVtzCT9F56Al/dwRSxBejQQEb1AC8j
uuyi7gJaPdyNntROEFTD7iO2L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTpOry/
Wvw0iKZFbo4AkiI0aLyBCk9HBXhUKa9x06gOnhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90wlRBUAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZIenrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQS4NAwARAQABzTlBV1MgT3BzSHVi
IGZvciBTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFAl/hGf8GCwkHCAMCBBUICgIEFgIBAAIZAQIbAwIeAQAh
CRAhgc9adPNF8RYhBDcvpelIaY930bOvqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIawOSXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmxWWbg
cxg1g0GXNXCM4lAd68CmbAOLoLTaWSQX30ZbswzhbtX2ADAlopV8RLBik7fm
bS9FyuubDRhfYRQq0fpjUGXFiEgwg6aMFxsrGLlv4QD7t+6ftFIe/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+FOVMmPeEN5JRazEeUrl
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDWOq/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty25lo8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4EDl19Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEZa/2upDJ1m+4OHK4p
8DrEzP/3jTahT8q5ofFWSRDL17d3lTSU+JBmPE3mz311FNXgiO8w+taY320z
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
O7vxMO5xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFZvzT/tDi5FiEEi+O9
V+UAYN9Gnw36EVm/NP+0OLnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvgOtUBxqmCOjr+8AKH0OtiBWSuO
lsS8JU5rindEsKUrKTwcG2wyZFoe1zlE8xPkLRSRN5ZbbgKsTz16l1HgCCId
Do+WJdDkWGWxmtDvzjM32EI/PVBd108ga9aPwXdhLwOdKAjZ4JrJXLUQJjRI
IVDSyMObEHOUM6a/+mWNZazNfo0LsGWqGVa6Xn5WJWlwR1S78vPNfO3BQYuO
YRjaVQR+kPtB9aSAZNi5sWfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7Xl03o/VjblneZOhJK6kAKU172tnPJTJ31JbOxX73wsMWDYZRZVcK
```

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

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

   GPG

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

   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]
   ```

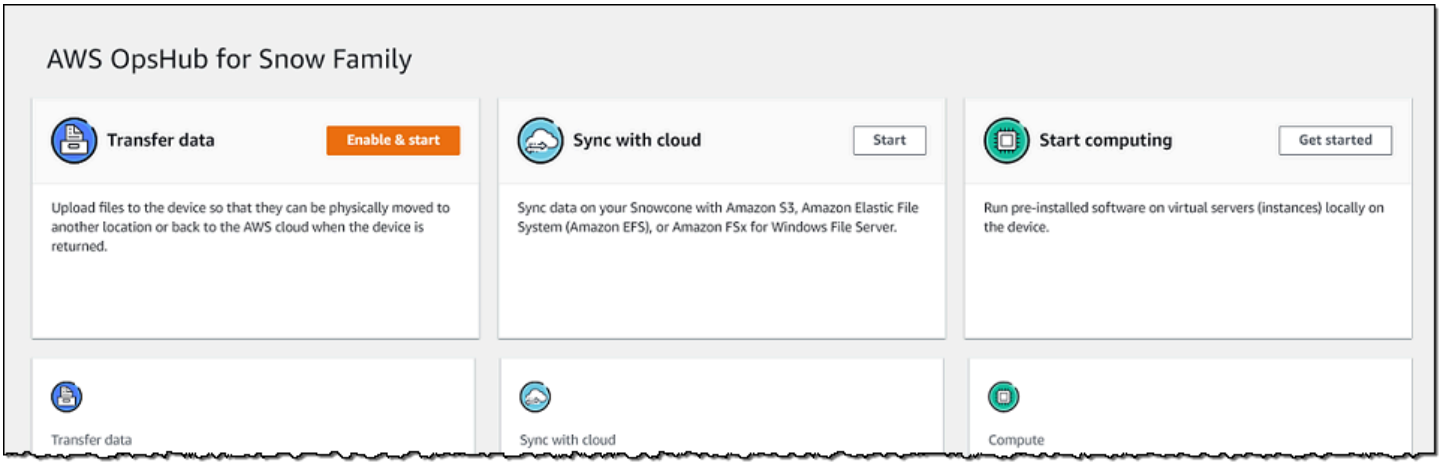
```
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9C93 4C3B 61F8 C434 9F94  5CA0 1655 BBDE 2B77 0256
```

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 .
- 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.
- Armazenamento compatível com o Amazon S3 em dispositivos da família Snow — Oferece armazenamento seguro de objetos com maior resiliência, escala e um conjunto expandido de recursos de API do Amazon S3 para ambientes robustos, móveis periféricos e desconectados. Usando o armazenamento compatível com o Amazon S3 em dispositivos da família Snow, você pode armazenar dados e executar aplicativos altamente disponíveis no dispositivo da família Snow para computação de ponta.



Tópicos

- Usando instâncias computacionais compatíveis com o Amazon EC2 localmente
- Gerenciar um cluster do Amazon EC2
- Configure o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow
- Gerenciar o armazenamento do adaptador do Amazon S3
- 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
- Importar uma imagem para o seu dispositivo como uma AMI compatível com Amazon EC2
- Excluir um snapshot

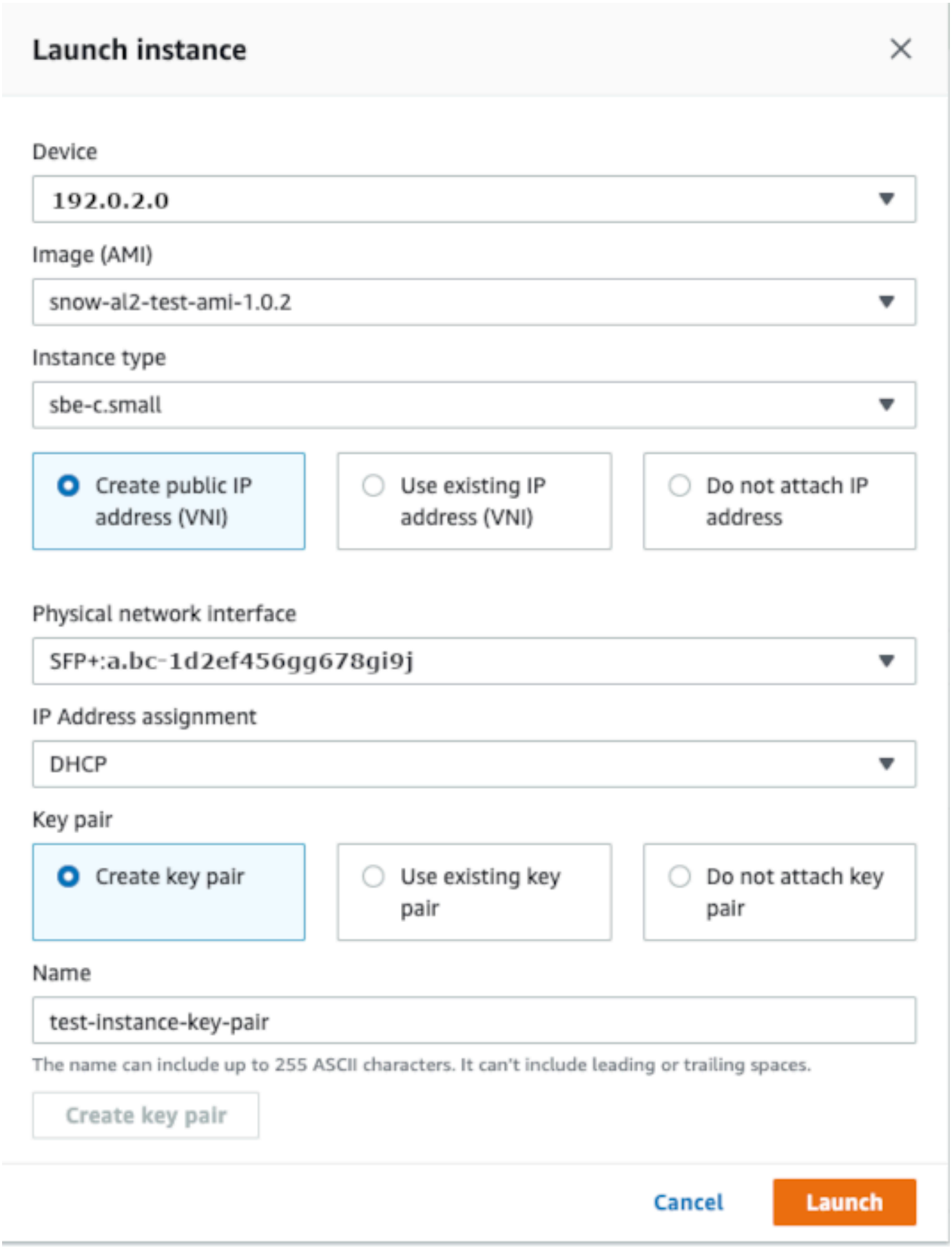
- Cancelar o registro da AMI

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

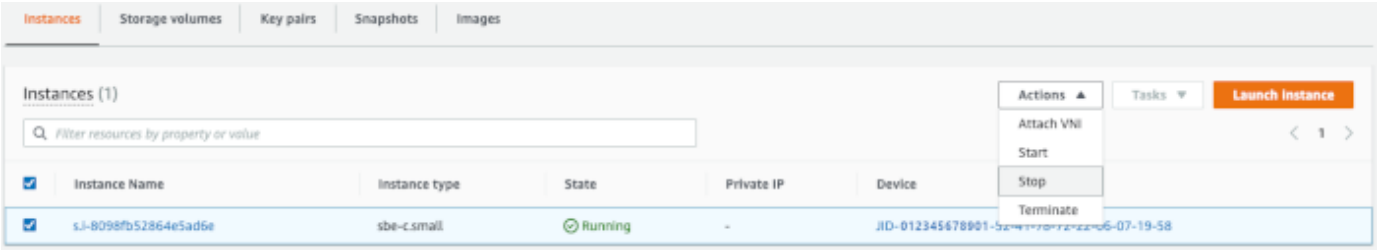
1. Abra o AWS OpsHub aplicativo.

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. AWS OpsHub

Para iniciar uma instância compatível com o Amazon EC2

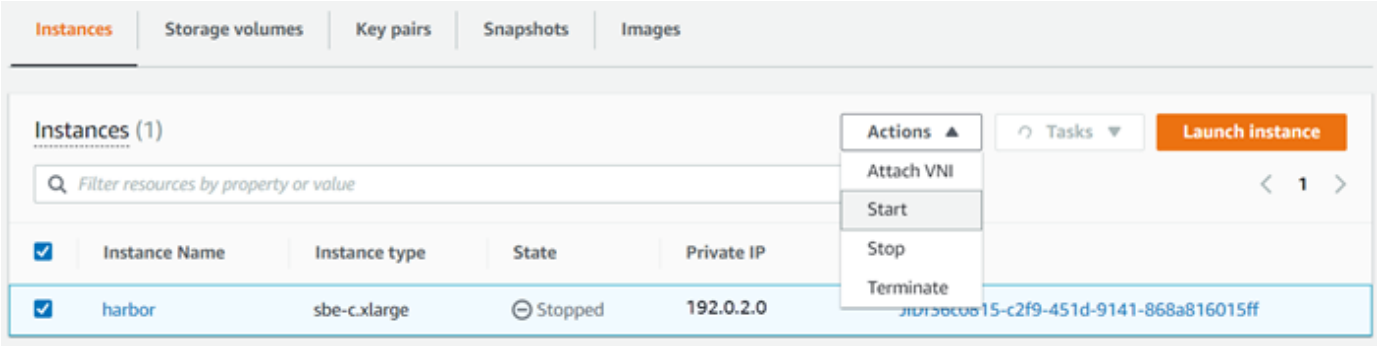
1. Abra o AWS OpsHub aplicativo.

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 informações sobre como criar um par de chaves, consulte Pares de chaves do Amazon EC2 e instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

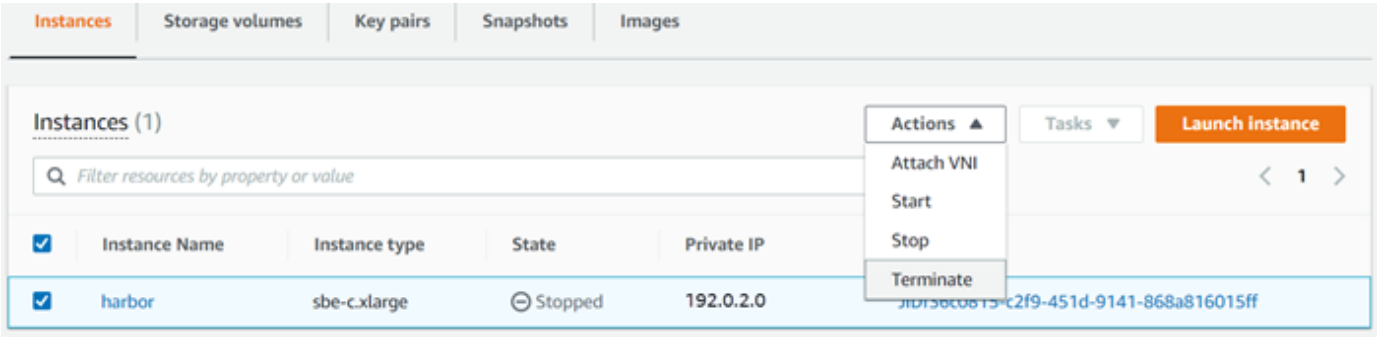
Encerramento de uma instância compatível com Amazon EC2

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

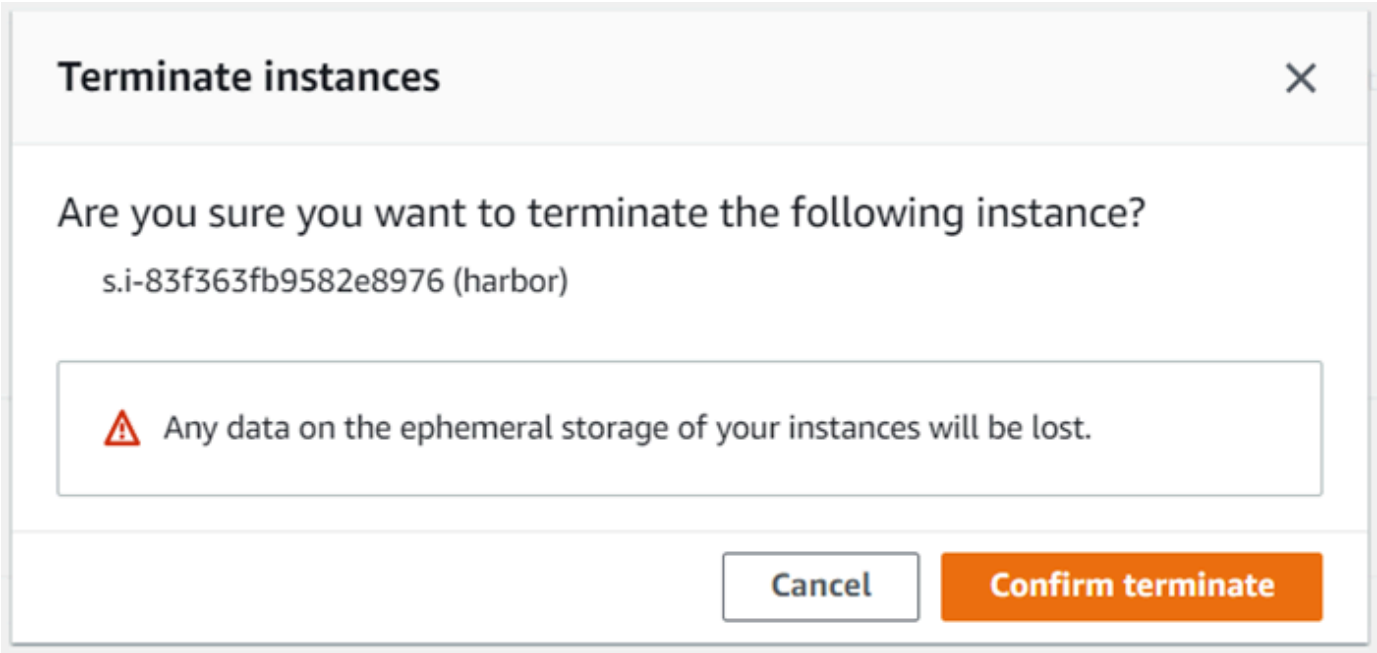
Para encerrar uma instância compatível com o Amazon EC2

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.

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



5. Na janela Encerrar instâncias, escolha Confirmar encerramento.



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

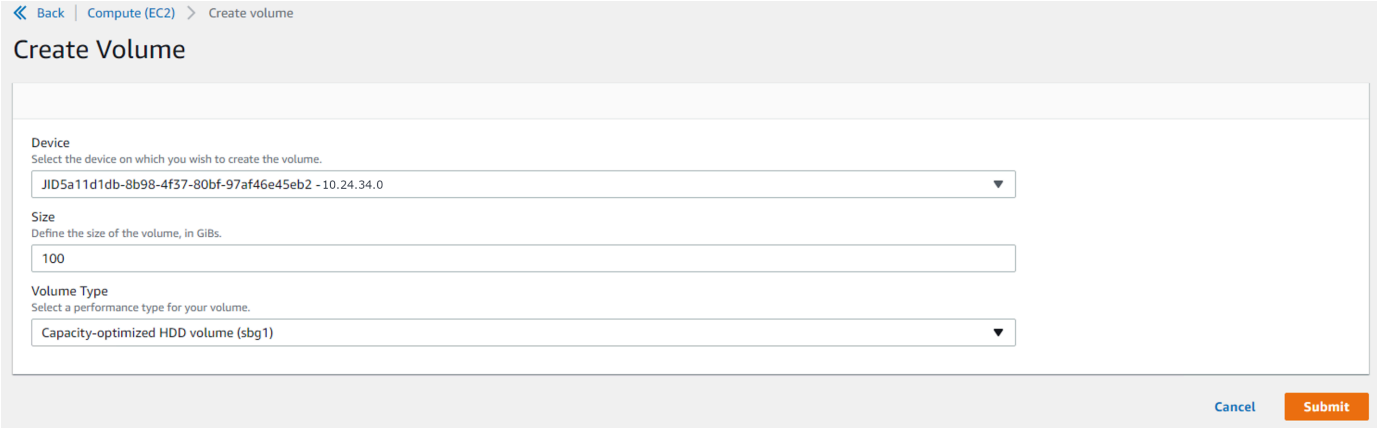
O State (Estado) muda para Terminating (Encerrando) e depois para Terminated (Encerrada) ao término.

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

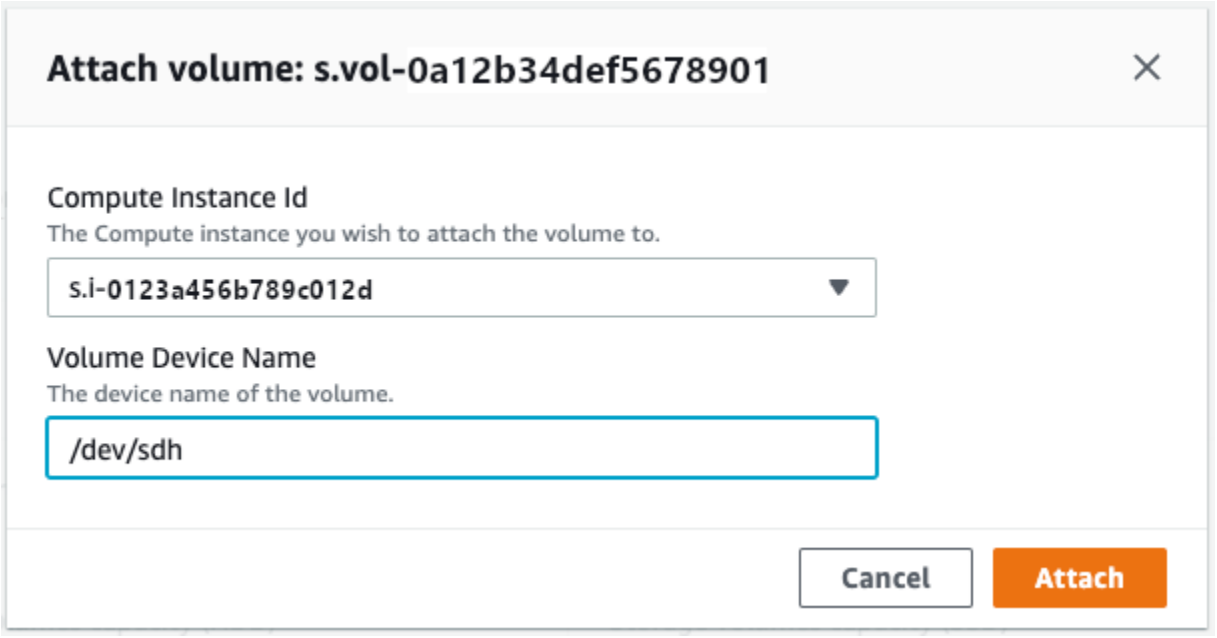
1. Abra o AWS OpsHub aplicativo.
2. Na seção Start computing (Iniciar computação) no painel, escolha Get started (Comece a usar). Ou escolha o menu Services (Serviços) na parte superior e selecione Compute (EC2) (Computação (EC2)) para abrir a página Compute (Computação).
3. Escolha a guia Volumes de 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).



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).



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.

Importar uma imagem para o seu dispositivo como uma AMI compatível com Amazon EC2

Você pode importar um snapshot da sua imagem para o seu dispositivo Snowball Edge e registrá-lo como uma imagem de máquina da Amazon (AMI) compatível com Amazon EC2. Um snapshot é basicamente uma cópia do seu volume de armazenamento que você pode usar para criar uma AMI ou outro volume de armazenamento. Ao fazer isso, você pode trazer sua própria imagem de uma fonte externa para o seu dispositivo e iniciá-la como uma instância compatível com o Amazon EC2.

Siga estas etapas para concluir a importação da sua imagem.

1. Faça upload do snapshot em um bucket do Amazon S3 em seu dispositivo.
2. Configure as permissões necessárias para conceder acesso ao Amazon S3, Amazon EC2 e VM Import/Export, o atributo usado para importar e exportar snapshots.
3. Importe o instantâneo do bucket do S3 para o seu dispositivo como uma imagem.
4. Registre a imagem como uma AMI compatível com Amazon EC2.

5. Inicie a AMI como uma instância compatível com o Amazon EC2.

> **Note**
>
> Esteja ciente das seguintes limitações ao fazer o upload de instantâneos para os dispositivos da Família Snow.
>
> - No momento, os dispositivos da Família Snow são compatíveis apenas com a importação de snapshots no formato de imagem RAW.
> - No momento, os dispositivos da Família Snow são compatíveis apenas com a importação de snapshots de 1 GB a 1 TB.

Etapa 1: fazer upload de um snapshot em um bucket do S3 no seu dispositivo

Você deve fazer o upload do seu snapshot para o Amazon S3 em seu dispositivo antes de importá-lo. Isso ocorre porque os snapshots só podem ser importados do Amazon S3 disponível em seu dispositivo ou cluster. Durante o processo de importação, você escolhe o bucket do S3 em seu dispositivo para armazenar a imagem.

Para obter um snapshot e fazer upload no Amazon S3

- Para criar um bucket do S3, consulte Criação do armazenamento do Amazon S3.

  Para fazer upload de um snapshot em um bucket do S3, consulte Upload de arquivos para o Amazon S3 Storage.

Etapa 2: importar o snapshot de um bucket do S3

Quando seu snapshot é carregado no Amazon S3, você pode importá-lo para o seu dispositivo. Todos os instantâneos que foram importados ou estão em processo de importação são mostrados na guia Instantâneos.

Para importar o instantâneo para o seu dispositivo

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. Escolha a guia Instantâneos para ver todos os instantâneos que foram importados para o seu dispositivo. O arquivo de imagem no Amazon S3 é um arquivo .raw que é importado para o seu dispositivo como um snapshot. Você pode filtrar por ID do instantâneo ou pelo estado do instantâneo para encontrar instantâneos específicos. Você pode escolher uma ID de instantâneo para ver os detalhes desse instantâneo.
4. Escolha o snapshot que você deseja importar e escolha Importar snapshot para abrir a página Importar snapshot.
5. Em Dispositivo, escolha o endereço IP do dispositivo da Família Snow para o qual você deseja importar.
6. Em Descrição da importação e Descrição do instantâneo, insira uma descrição para cada uma.
7. Na lista Perfil, escolha um perfil para usar na importação. Os dispositivos da família Snow usam o VM Import/Export para importar instantâneos. AWS assume essa função e a usa para importar o snapshot em seu nome. Se você não tiver uma função configurada no seu AWS Snowball Edge, abra o AWS Identity and Access Management (IAM) AWS OpsHub onde você pode criar uma função local do IAM. A função também precisa de uma política que tenha as permissões de VM Import/Export necessárias para realizar a importação. Você também deve anexar a política ao perfil. Para obter mais detalhes sobre isso, consulte Como usar o IAM localmente.

   Veja a seguir um exemplo da política.

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

   Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

O perfil que você cria deve ter permissões mínimas para acessar o Amazon S3. A seguir está um exemplo de uma política mínima.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:GetMetadata"
         ],
         "Resource":[
            "arn:aws:s3:::import-snapshot-bucket-name",
            "arn:aws:s3:::import-snapshot-bucket-name/*"
         ]
      }
   ]
}
```

8. Escolha Procurar S3 e escolha o bucket do S3 que contém o snapshot que você deseja importar. Escolha o snapshot e escolha Enviar. O snapshot começa a ser baixado para o seu dispositivo. Você pode escolher o ID do snapshot para ver os detalhes. Você pode cancelar o processo de importação nesta página.

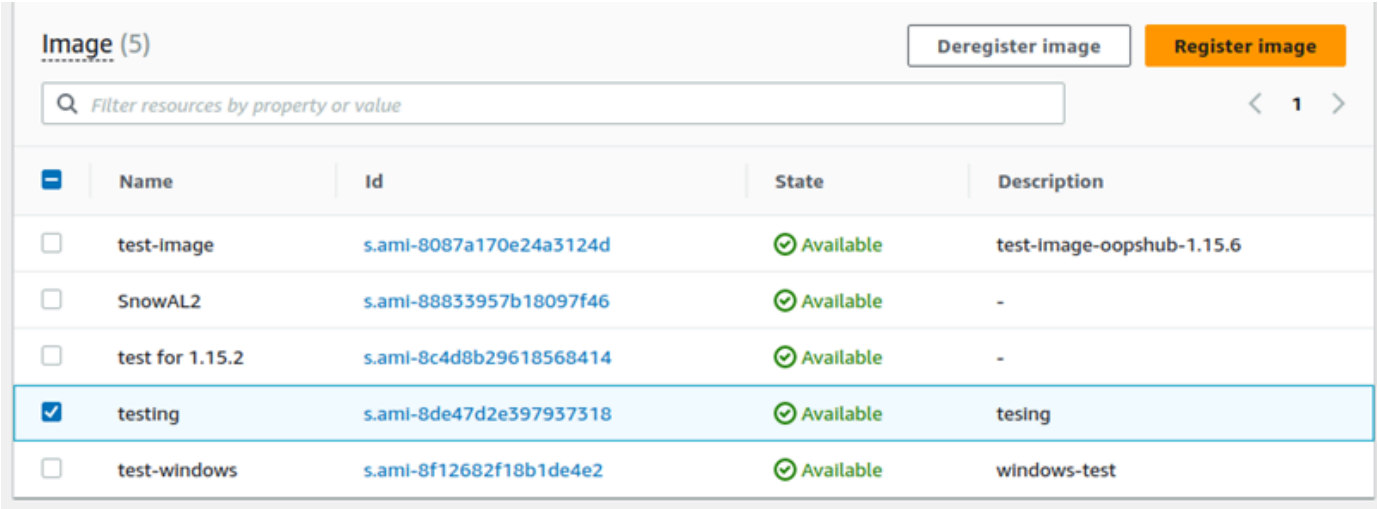
Etapa 3: registrar o snapshot como uma AMI compatível com Amazon EC2

O processo de criação de uma AMI compatível com Amazon EC2 a partir de uma imagem importada como um snapshot é conhecido como registro. As imagens importadas para o seu dispositivo devem ser registradas antes de serem executadas como instâncias compatíveis com o Amazon EC2.

Para registrar uma imagem importada como um instantâneo

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. Selecione a guia Images (Imagens). Você pode filtrar as imagens por nome, ID ou estado para encontrar uma imagem específica.
4. Escolha a imagem que você deseja registrar e escolha Registrar imagem.



5. Na página Registrar imagem, forneça um Nome e uma Descrição.
6. Em Volume raiz, especifique o nome do dispositivo raiz.

   Na seção Dispositivo de blocos, você pode alterar o tamanho do volume e o tipo de volume.
7. Se você quiser que o volume seja excluído quando a instância for encerrada, selecione Excluir ao encerrar.
8. Se você deseja adicionar mais volumes, escolha Adicionar novo volume.
9. Quando estiver pronto, escolha Enviar.

Etapa 4: iniciar a AMI compatível com Amazon EC2

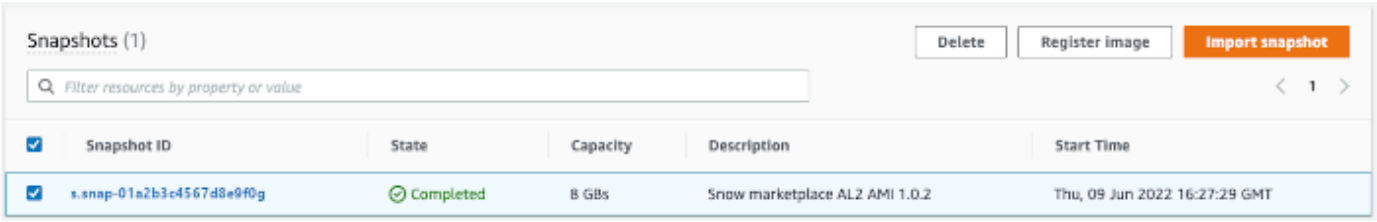
- Para obter mais informações, consulte Como iniciar uma instância compatível com o Amazon EC2.

Excluir um snapshot

Se você não precisar mais de um snapshot, é possível excluí-lo do dispositivo. O arquivo de imagem no Amazon S3 é um arquivo .raw que é importado para o seu dispositivo como um snapshot. Se o snapshot que você está excluindo for usado por uma imagem, ele não poderá ser excluído. Depois que a importação for concluída, você também poderá excluir o arquivo .raw que você carregou no Amazon S3 em seu dispositivo.

Para excluir um snapshot

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. Escolha a guia Snapshot para ver todos os snapshots que foram importados. Você pode filtrar por ID do snapshot ou estado do snapshot para encontrar snapshots específicos.
4. Escolha os snapshots que você deseja excluir e selecione Excluir. Você pode escolher vários snapshots.

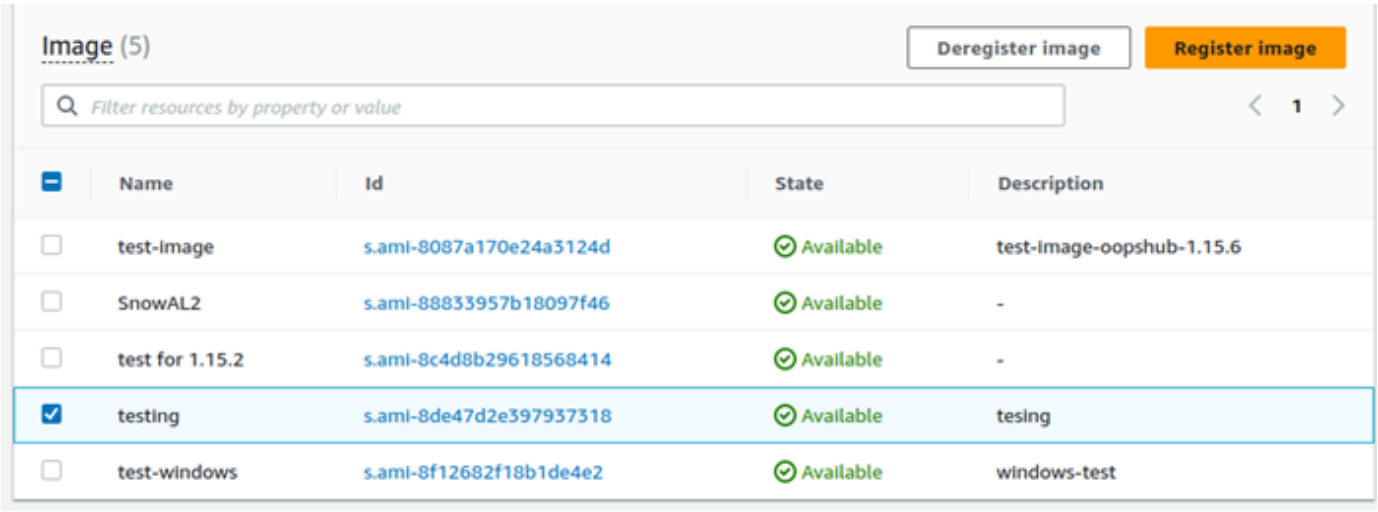


5. Na caixa de confirmação Excluir snapshot, escolha Excluir snapshot. Se a ação de excluir com sucesso, o snapshot será removido da lista na guia Snapshot.

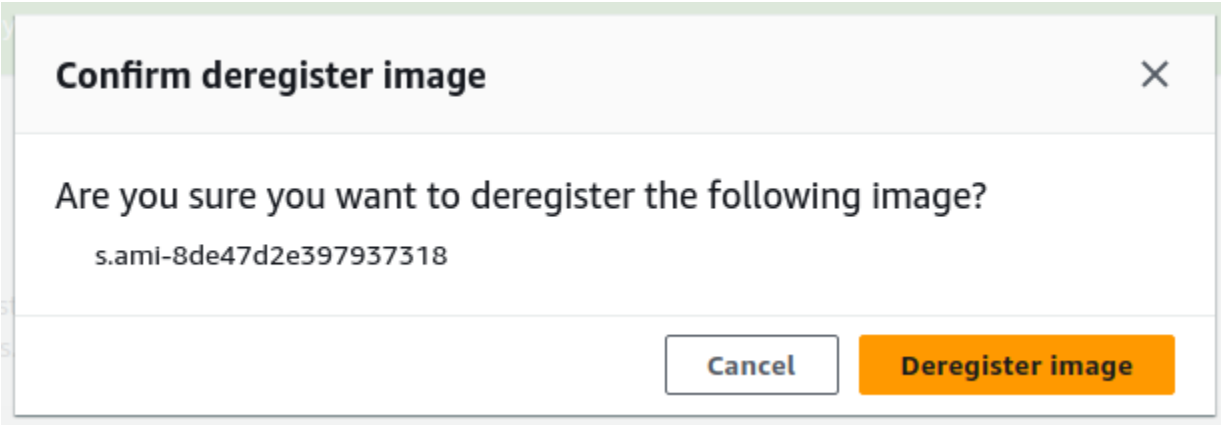
Cancelar o registro da AMI

Para cancelar o registro de uma AMI

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. Selecione a guia Images (Imagens). Todas as imagens estão listadas. Você pode filtrar as imagens por nome, ID ou estado para encontrar uma imagem específica.
4. Escolha a imagem cujo registro você deseja cancelar e escolha Cancelar registro.



5. Na janela Confirmar cancelamento do registro da imagem, confirme a ID da imagem e escolha Cancelar registro da imagem. Quando o cancelamento do registro é bem-sucedido, a imagem é removida da lista de imagens.



Gerenciar um cluster do Amazon EC2

Um cluster do Amazon EC2 é um grupo de dispositivos que são provisionados juntos como um cluster de dispositivos. Para usar um cluster, os AWS serviços em seu dispositivo devem estar em execução no seu endpoint padrão. Você também precisa escolher o dispositivo específico no cluster com o qual deseja se comunicar. Você usa um cluster com base em cada dispositivo.

Para criar um cluster do Amazon EC2

1. Conecte-se e faça login no seu dispositivo Snow. Para obter instruções sobre como fazer login no seu dispositivo, consulte Desbloquear um dispositivo.
2. Na página Escolher dispositivo, escolha Cluster do Snowball Edge e selecione Próximo.

3. Na página Conectar ao dispositivo, forneça o endereço IP do dispositivo e os endereços IP de outros dispositivos do cluster.
4. Escolha Add another (Adicionar outro) dispositivo para adicionar mais dispositivos e selecione Next (Próximo).
5. Na página Fornecer as chaves, insira o código de desbloqueio do cliente do dispositivo, faça upload do manifesto do dispositivo e escolha Desbloquear dispositivo.

   Os dispositivos Snowball Edge usam criptografia de 256 bits para ajudar a garantir a segurança e a integridade de seus dados. chain-of-custody
6. Opcionalmente, você pode inserir um nome para criar um perfil e escolher Salvar nome de perfil. Você é direcionado para o painel, onde vê todos os seus clusters.

   Agora você pode começar a usar AWS serviços e gerenciar seu cluster. Você gerencia instâncias no cluster da mesma maneira que gerencia instâncias individuais. Para obter instruções, consulte Gerenciando AWS serviços em seu dispositivo ou Gerenciar seus dispositivos.

Configure o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

O serviço de armazenamento compatível com Amazon S3 em dispositivos da Família Snow não está ativo por padrão. Para iniciar o serviço em um dispositivo ou cluster, você deve criar duas interfaces de rede virtual (vNICs) em cada dispositivo para se conectar aos endpoints `s3control` e `s3api`.

Tópicos

- Remova arquivos e pastas do armazenamento compatível com Amazon S3 em buckets de dispositivos da Família Snow
- Exclua buckets do armazenamento compatível com Amazon S3 em dispositivos da Família Snow

Pré-requisitos

Antes de configurar seu dispositivo ou cluster usando AWS OpsHub for Snow Family, faça o seguinte:

- Ligue seu dispositivo Snowball Edge e conecte-o à sua rede.
- Na sua máquina local, baixe e instale a última versão do AWS OpsHub. Conecte-se ao dispositivo ou cluster para desbloqueá-lo com um arquivo de manifesto. Para obter mais informações, consulte como desbloquear um dispositivo.

Usando a opção de configuração simples

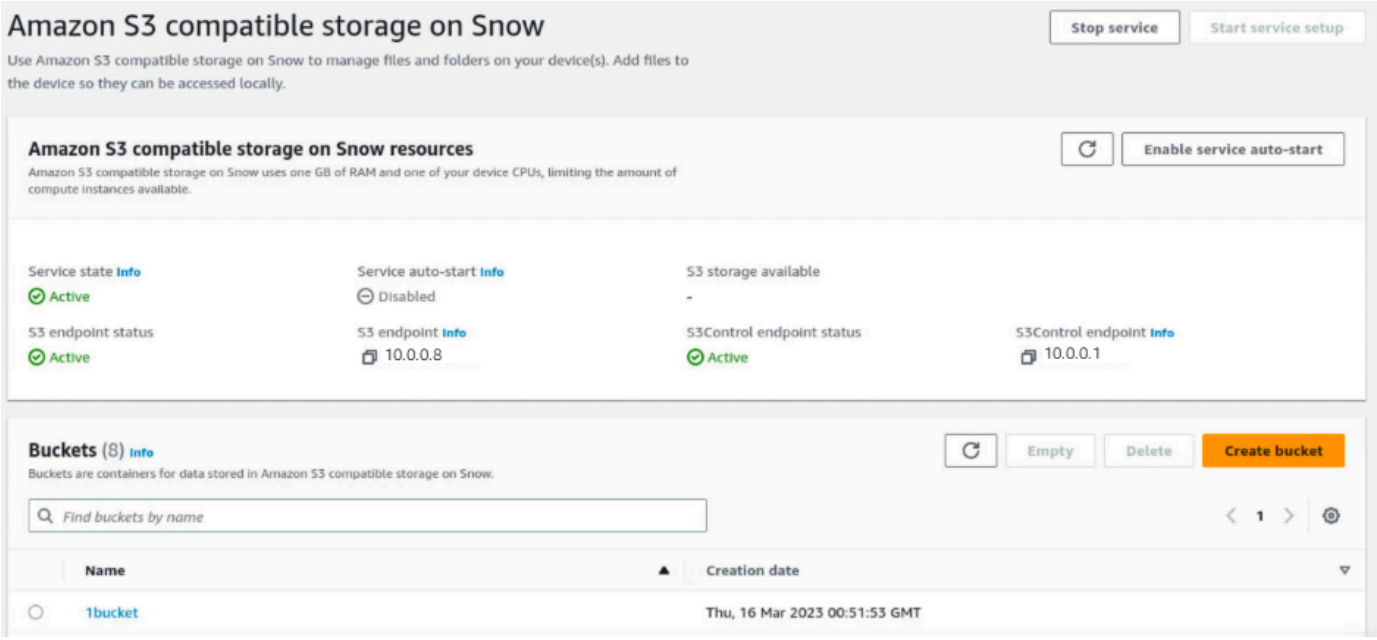
Use a opção de configuração simples se sua rede usar DHCP. Com essa opção, os vNICs são criados automaticamente em cada dispositivo quando você inicia o serviço.

1. Faça login AWS OpsHub e escolha Gerenciar armazenamento.

   Isso leva você à página inicial de armazenamento compatível com Amazon S3 em dispositivos da Família Snow.
2. Em Iniciar o tipo de configuração do serviço, escolha Simples.
3. Escolha Iniciar serviço.

   > **Note**
   >
   > Isso leva alguns minutos para ser concluído e depende do número de dispositivos que você está usando.

   Depois que o serviço é iniciado, o estado do serviço fica ativo e há endpoints.



Usando a opção de configuração avançada

Use a opção de configuração avançada se sua rede usar endereços IP estáticos ou se você quiser reutilizar VNIs existentes. Com essa opção, você cria vNICs para cada dispositivo manualmente.

1. Faça login AWS OpsHub e escolha Gerenciar armazenamento.

   Isso leva você à página inicial de armazenamento compatível com Amazon S3 em dispositivos da Família Snow.
2. Em Iniciar o tipo de configuração do serviço, escolha Avançado.
3. Selecione os dispositivos para os quais você precisa criar vNICs.

   Para clusters, você precisa de um quórum mínimo de dispositivos para iniciar o serviço de armazenamento compatível com Amazon S3 em dispositivos da Família Snow. O quorum é dois para um cluster de três nós.

> **Note**
>
> Para o início do serviço em uma configuração de cluster, você deve ter todos os dispositivos no cluster configurados e disponíveis para que o serviço seja iniciado. Para inicializações subsequentes, você pode usar um subconjunto dos dispositivos se atingir o quórum, mas o serviço será iniciado em um estado degradado.

4. Para cada dispositivo, escolha uma VNIC existente ou selecione Criar VNI.

   Cada dispositivo precisa de uma VNIC para o endpoint S3 para operações de objetos e outra para o endpoint S3Control para operações de bucket.
5. Se você estiver criando uma VNIC, escolha uma interface de rede física e insira o endereço IP de status e a máscara de sub-rede e, em seguida, escolha Criar interface de rede virtual.
6. Depois de criar seu VNICS, escolha Iniciar serviço.

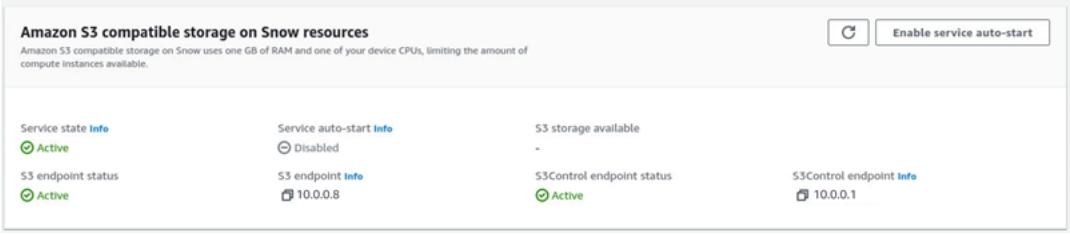
   > **Note**
   >
   > Isso leva alguns minutos para ser concluído e depende do número de dispositivos que você está usando.

   Depois que o serviço é iniciado, o estado do serviço fica ativo e há endpoints.

Configurando o armazenamento compatível com o Amazon S3 no serviço de dispositivos da família Snow para inicialização automática

1. Faça login AWS OpsHub e escolha Gerenciar armazenamento.

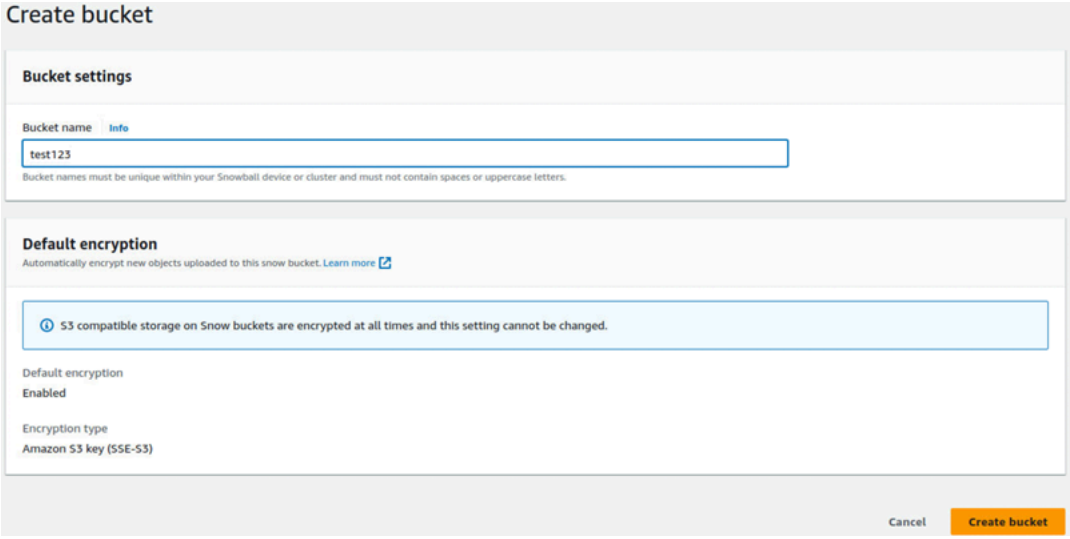
   Isso leva você à página inicial de armazenamento compatível com Amazon S3 em dispositivos da Família Snow.
2. Em Armazenamento compatível com Amazon S3 em atributos do Snow, escolha Ativar início automático do serviço. O sistema configura o serviço para ser iniciado automaticamente no futuro.



Criação de um bucket no armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

Use a AWS OpsHub interface para criar um bucket Amazon S3 em seu dispositivo Snow Family.

1. Aberto AWS OpsHub.
2. Em Gerenciar armazenamento, escolha Começar. A página Armazenamento compatível com Amazon S3 no Snow é exibida.
3. Em Buckets, escolha Criar bucket. A tela Criar bucket é exibida.



4. Para Nome do bucket, digite um nome para o bucket.

> **Note**
>
> Os nomes dos buckets devem ser exclusivos em seu dispositivo ou cluster Snowball e não devem conter espaços ou letras maiúsculas.

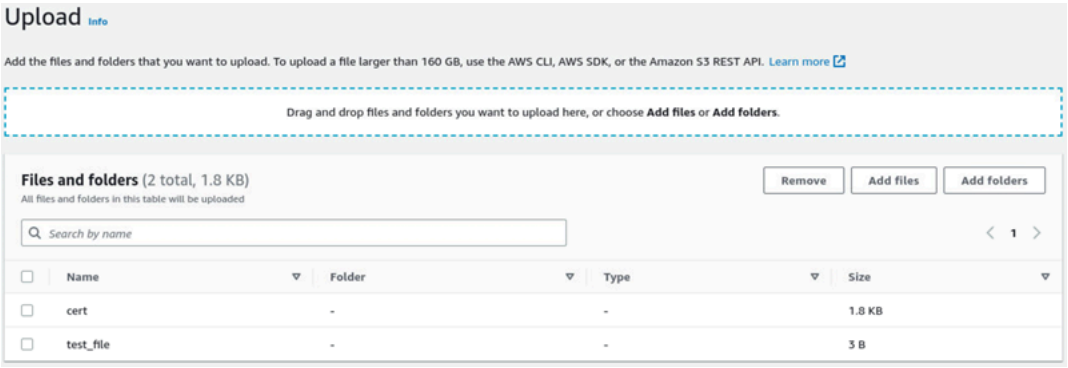
5. Selecione Criar bucket. O sistema cria o bucket e ele aparece em Buckets na página Armazenamento compatível com Amazon S3 no Snow.

Faça upload de arquivos e pastas para o armazenamento compatível com Amazon S3 em buckets de dispositivos da Família Snow

Use a AWS OpsHub interface para fazer upload de arquivos e pastas para o armazenamento compatível com Amazon S3 em buckets de dispositivos da família Snow. Arquivos e pastas podem ser carregados separadamente ou juntos.

1. Abra o AWS OpsHub
2. Em Gerenciar armazenamento, em Buckets, escolha um bucket no qual fazer upload de arquivos. A página do bucket é exibida.

3. Na página do bucket, escolha Carregar. A página de upload é exibida.



4. Faça upload de arquivos ou pastas arrastando-os de um gerenciador de arquivos do sistema operacional para a AWS OpsHub janela ou faça o seguinte:

   a. Selecione Adicionar arquivos ou Adicionar pastas.

   b. Selecione os arquivos ou as pastas para upload. Selecione Abrir.

   O sistema carrega os arquivos e pastas selecionados para o bucket no dispositivo. Depois que o upload for concluído, os nomes dos arquivos e pastas aparecerão na lista Arquivos e pastas.

Remova arquivos e pastas do armazenamento compatível com Amazon S3 em buckets de dispositivos da Família Snow

Use a AWS OpsHub interface para remover e excluir permanentemente arquivos e pastas dos buckets no dispositivo Snow Family.

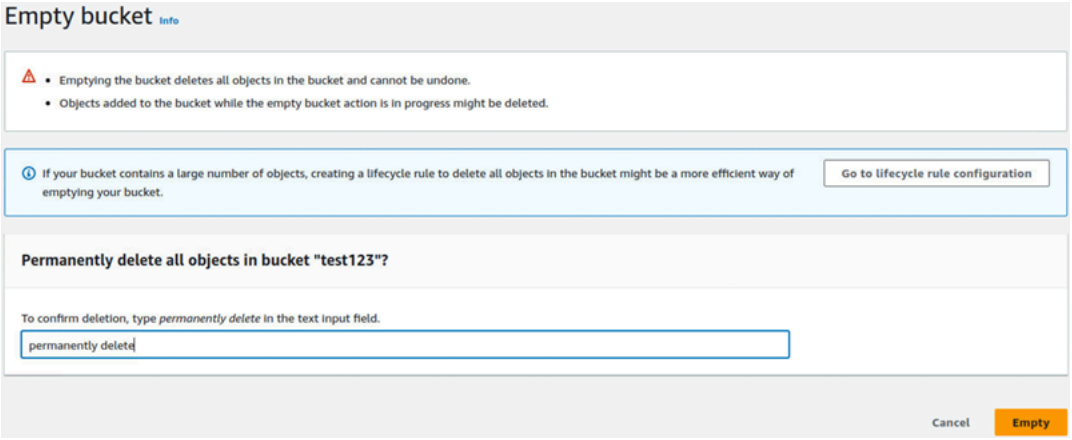
1. Aberto AWS OpsHub.
2. Em Gerenciar armazenamento, em Buckets, selecione o nome de um bucket do qual excluir arquivos e pastas. A página do bucket é exibida.
3. Em Arquivos e pastas, marque as caixas de seleção dos arquivos e pastas a serem excluídos permanentemente.
4. Selecione Remover. O sistema remove os arquivos ou pastas do bucket no dispositivo.

Exclua buckets do armazenamento compatível com Amazon S3 em dispositivos da Família Snow

Antes de excluir um bucket de um dispositivo, ele deve estar vazio. Remova arquivos e pastas do bucket ou use a ferramenta bucket vazio. Para remover arquivos e pastas, consulte Remova arquivos e pastas do armazenamento compatível com Amazon S3 em buckets de dispositivos da Família Snow.

Para usar a ferramenta de bucket vazio

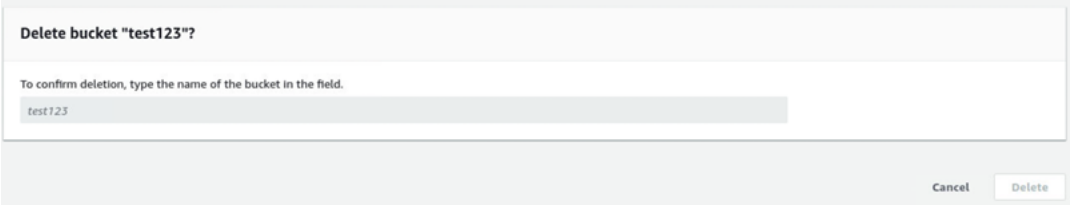
1. Aberto AWS OpsHub.
2. Em Gerenciar armazenamento, em Buckets, selecione o botão de rádio do bucket para esvaziar.
3. Selecione Esvaziar. A página Esvaziar bucket é exibida.



4. Na caixa de texto na página do Esvaziar bucket, digite **`permanently delete`**.
5. Selecione Esvaziar. O sistema esvazia o bucket.

Excluir um bucket vazio

1. Em Gerenciar armazenamento, em Buckets, selecione o botão de rádio do bucket a ser excluído.
2. Selecione Excluir. A página Excluir bucket é exibida.



3. Na caixa de texto na página Excluir bucket, digite o nome do bucket.

4. Selecione Excluir. O sistema exclui o bucket do dispositivo.

Gerenciar o armazenamento do adaptador do Amazon S3

Você pode usar AWS OpsHub para criar e gerenciar o armazenamento do Amazon Simple Storage Service (Amazon S3) em seus dispositivos da família Snow usando o adaptador S3 para trabalhos de importação e exportação.

Tópicos

Acessar o armazenamento do Amazon S3

É possível fazer upload de arquivos no seu dispositivo e acessar os arquivos localmente. Você pode movê-los fisicamente para outro local no dispositivo ou importá-los de volta para o Nuvem AWS quando o dispositivo for devolvido.

Os dispositivos da Família Snow usam buckets do Amazon S3 para armazenar e gerenciar arquivos em seu dispositivo.

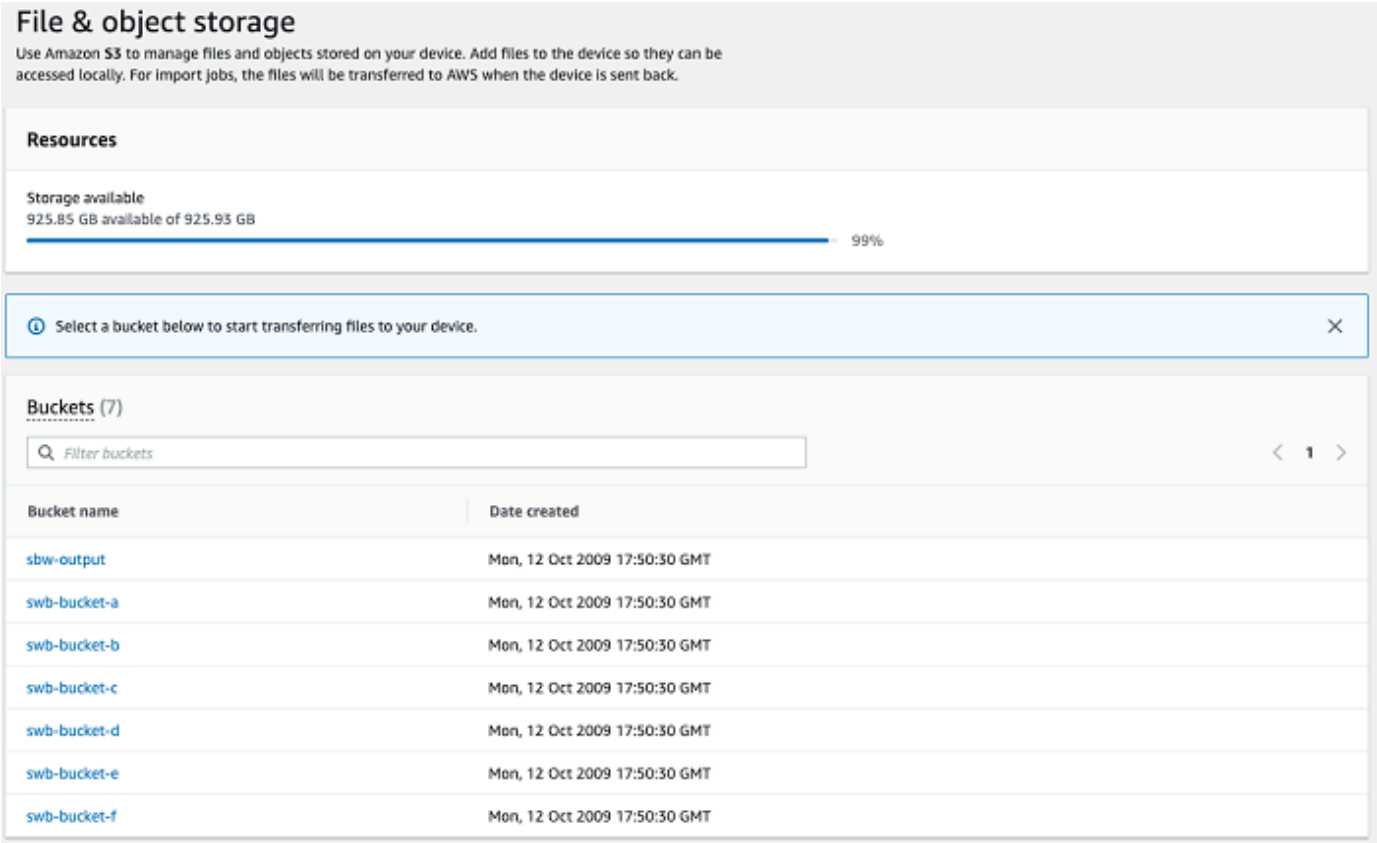
Para acessar um bucket do S3

1. Abra o AWS OpsHub aplicativo.
2. Na seção Gerenciar armazenamento de arquivos do painel, escolha Comece a usar.

   Se o seu dispositivo tiver sido encomendado com o mecanismo de transferência Amazon S3, eles aparecerão na seção Buckets da página Armazenamento de arquivos e objetos. Na página Armazenamento de arquivos e objetos, você pode ver os detalhes de cada bucket.

   > **Note**
   >
   > Se o dispositivo foi pedido com o mecanismo de transferência NFS, o nome do bucket aparecerá na seção de pontos de montagem após a configuração e ativação do serviço

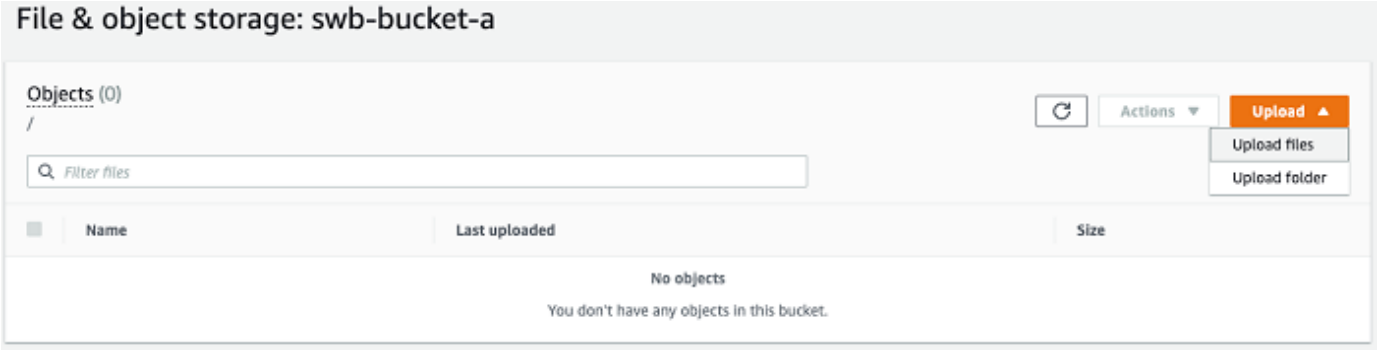
NFS. Para obter mais informações sobre como usar a interface de arquivos, consulte Gerenciando a interface NFS.



Carregar arquivos para o armazenamento do Amazon S3

Como fazer upload de um arquivo

1. Na seção Gerenciar armazenamento de arquivos no painel, escolha Comece a usar. Se você tiver buckets do S3 no seu dispositivo, eles serão exibidos na seção Buckets na página Armazenamento de arquivos. Você pode ver os detalhes de cada bucket na página.
2. Escolha o bucket no qual você deseja fazer upload dos arquivos.
3. Escolha Fazer upload e Fazer upload de arquivos ou arraste e solte os arquivos no bucket e escolha OK.

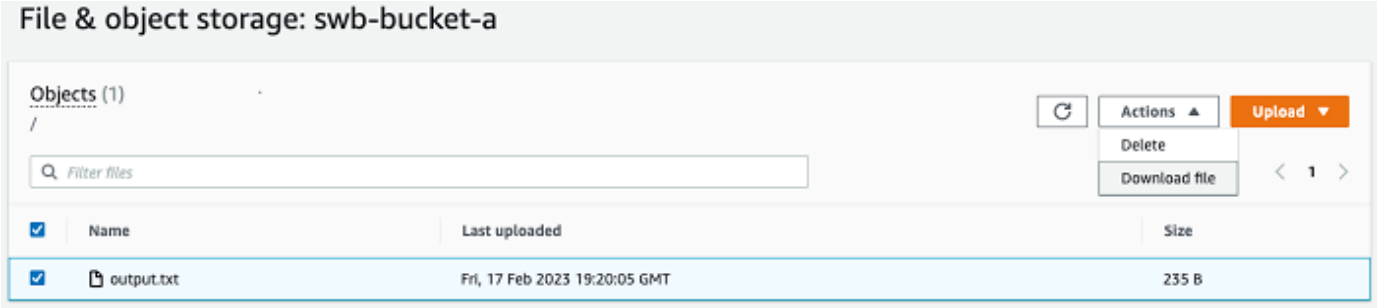


> **Note**
>
> Para fazer upload de arquivos maiores, você pode usar o atributo multipart upload no Amazon S3 usando o AWS CLI. Para obter mais informações sobre como definir as configurações da CLI do S3, consulte Configuração do CLI S3. Para obter mais informações sobre o upload de várias partes, consulte Visão geral do upload de várias partes no Guia do usuário do Amazon Simple Storage Service
> Há suporte para o upload de uma pasta de uma máquina local para o Snowball Edge usando AWS OpsHub o. Se o tamanho da pasta for muito grande, levará algum tempo para ler OpsHub a seleção do arquivo/pasta. Durante OpsHub a leitura dos arquivos e pastas, ele não exibe um rastreador de progresso. No entanto, ele exibe um rastreador de progresso quando o processo de upload é iniciado.

Fazer download de arquivos do armazenamento do Amazon S3

Para baixar um arquivo

1. Na seção Gerenciar armazenamento de arquivos do painel, escolha Comece a usar. Se você tiver buckets do S3 no seu dispositivo, eles serão exibidos na seção Buckets na página Armazenamento de arquivos. Você pode ver os detalhes de cada bucket na página.
2. Escolha o bucket do qual deseja fazer download de arquivos e navegue até o arquivo dos quais deseja fazer download. Escolha um ou mais arquivos.



3. No menu Ações, escolha Fazer download.
4. Escolha um local para o qual fazer download do arquivo e escolha OK.

Excluir arquivos do armazenamento do Amazon S3

Se não precisar mais de um arquivo, você poderá excluí-lo do bucket do Amazon S3.

Para excluir um arquivo

1. Na seção Gerenciar armazenamento de arquivos do painel, escolha Comece a usar. Se você tiver buckets do S3 no seu dispositivo, eles serão exibidos na seção Buckets na página Armazenamento de arquivos. Você pode ver os detalhes de cada bucket na página.
2. Escolha o bucket do qual deseja excluir arquivos e navegue até o arquivo que deseja excluir.
3. No menu Ações, escolha Excluir.
4. Na caixa de diálogo exibida, escolha Confirmar exclusão.

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.

Você pode usar a interface NFS se o dispositivo Snowball Edge tiver sido configurado para incluí-la quando a tarefa de solicitar o dispositivo foi criada. Se o dispositivo não estiver configurado para incluir a interface NFS, use o adaptador S3 ou o armazenamento compatível com Amazon S3 nos

dispositivos da família Snow para transferir dados. Para obter mais informações sobre o adaptador S3, consulteGerenciar o armazenamento do adaptador do Amazon S3. Para obter mais informações sobre o armazenamento compatível com o Amazon S3 em dispositivos da família Snow, consulte. Configure o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

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 Importação de trabalhos para o Amazon .

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 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.

- Você pode transferir até 40 milhões de arquivos usando um único dispositivo Snowball Edge. Se você precisar transferir mais de 40 milhões de arquivos em um único trabalho, agrupe os arquivos para reduzir o número de arquivos por cada transferência. Arquivos individuais podem ser de qualquer tamanho, com um tamanho máximo de arquivo de 5 TB para dispositivos Snowball Edge com a interface NFS aprimorada ou a interface S3.

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

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.

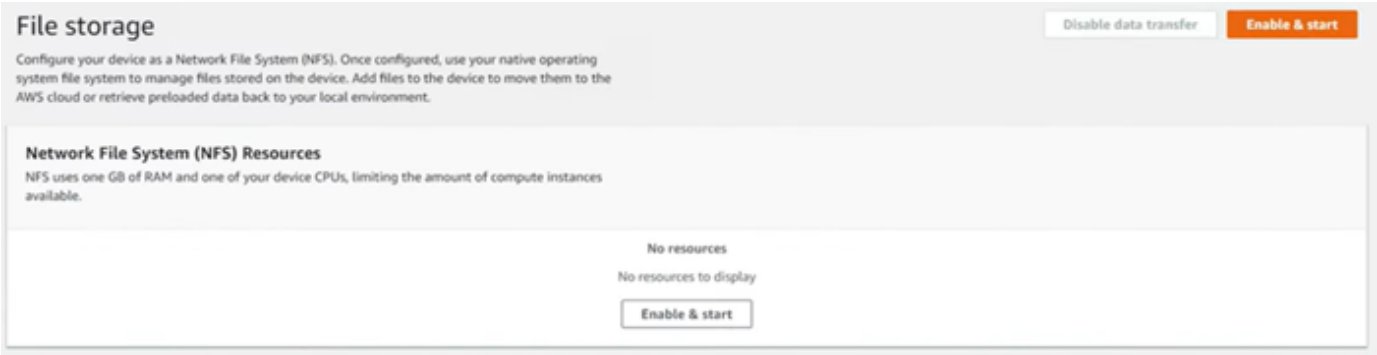
> **Note**
>
> Para ativar os recursos do Windows, talvez seja necessário fornecer um nome de usuário e uma senha de administrador para o seu computador.

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 por conta própria. 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`buckets(\\12.123.45.679)(Z:)`.

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

Configurando a interface NFS manualmente

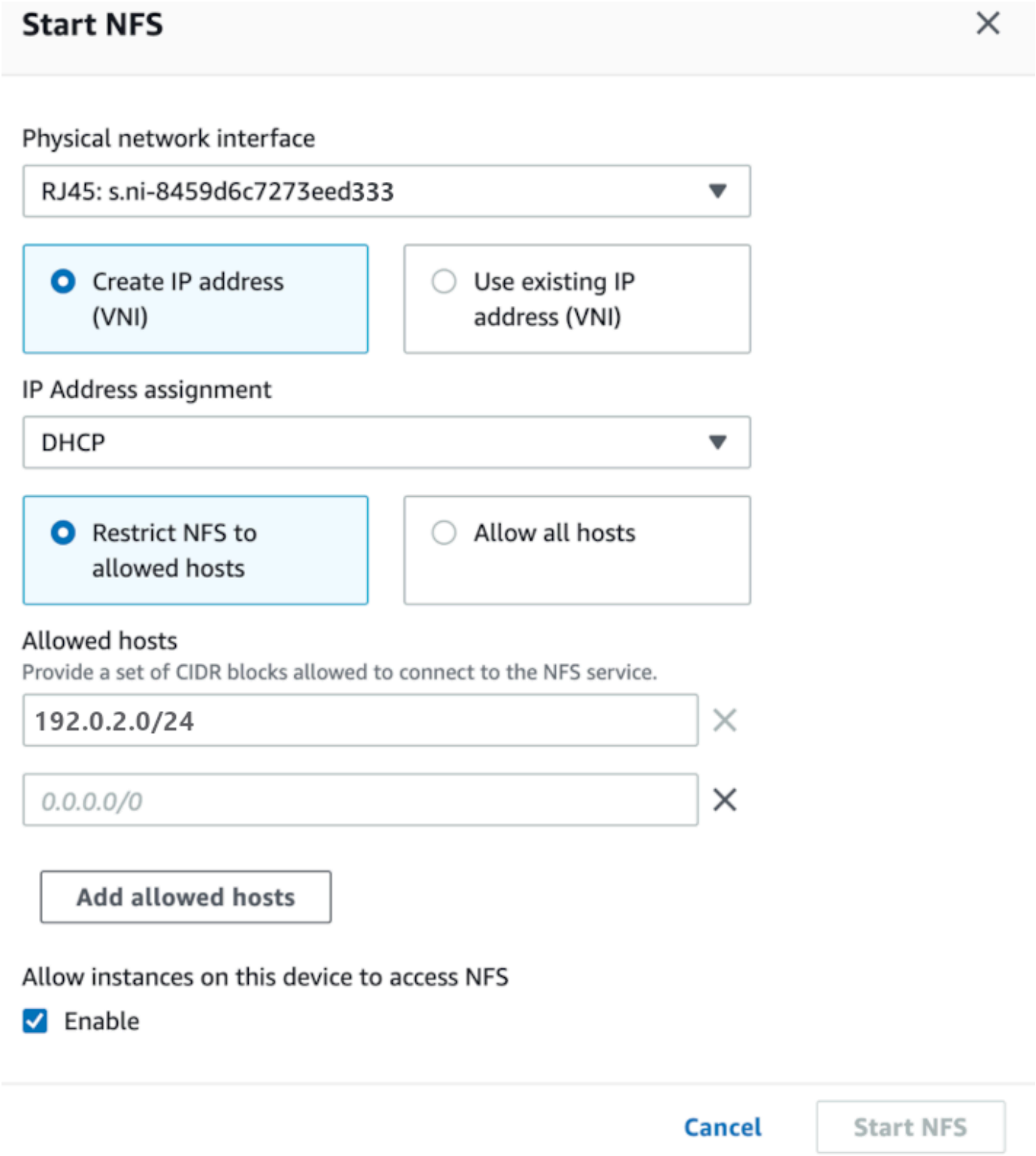
A interface NFS não está sendo executada no dispositivo Snow Family por padrão, então você precisa iniciá-la para ativar a transferência de dados no dispositivo. Você pode configurar

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.



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 DCHP. 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.

> **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.

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

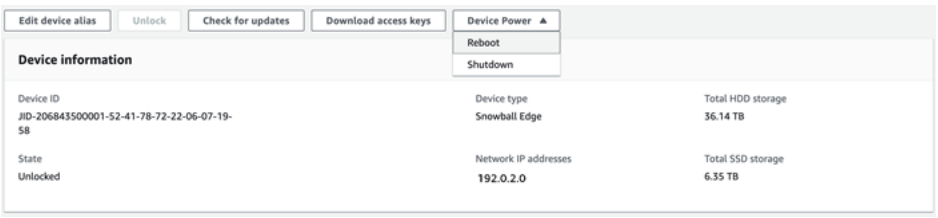
Reinicializar seu dispositivo

Siga estas etapas para reinicializar seu dispositivo Snow. AWS OpsHub

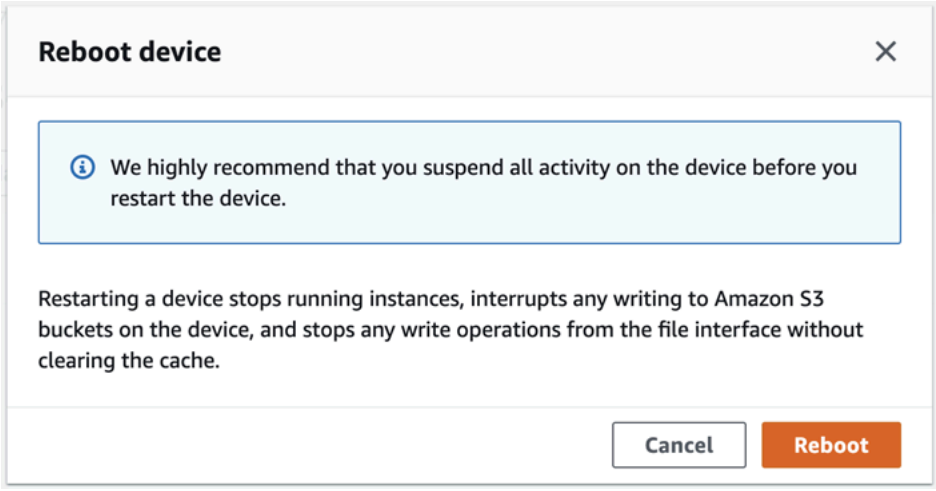
> **Important**
>
> É altamente recomendável suspender todas as atividades no dispositivo antes de reinicializá-lo. A reinicialização de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo.

Como reinicializar um dispositivo

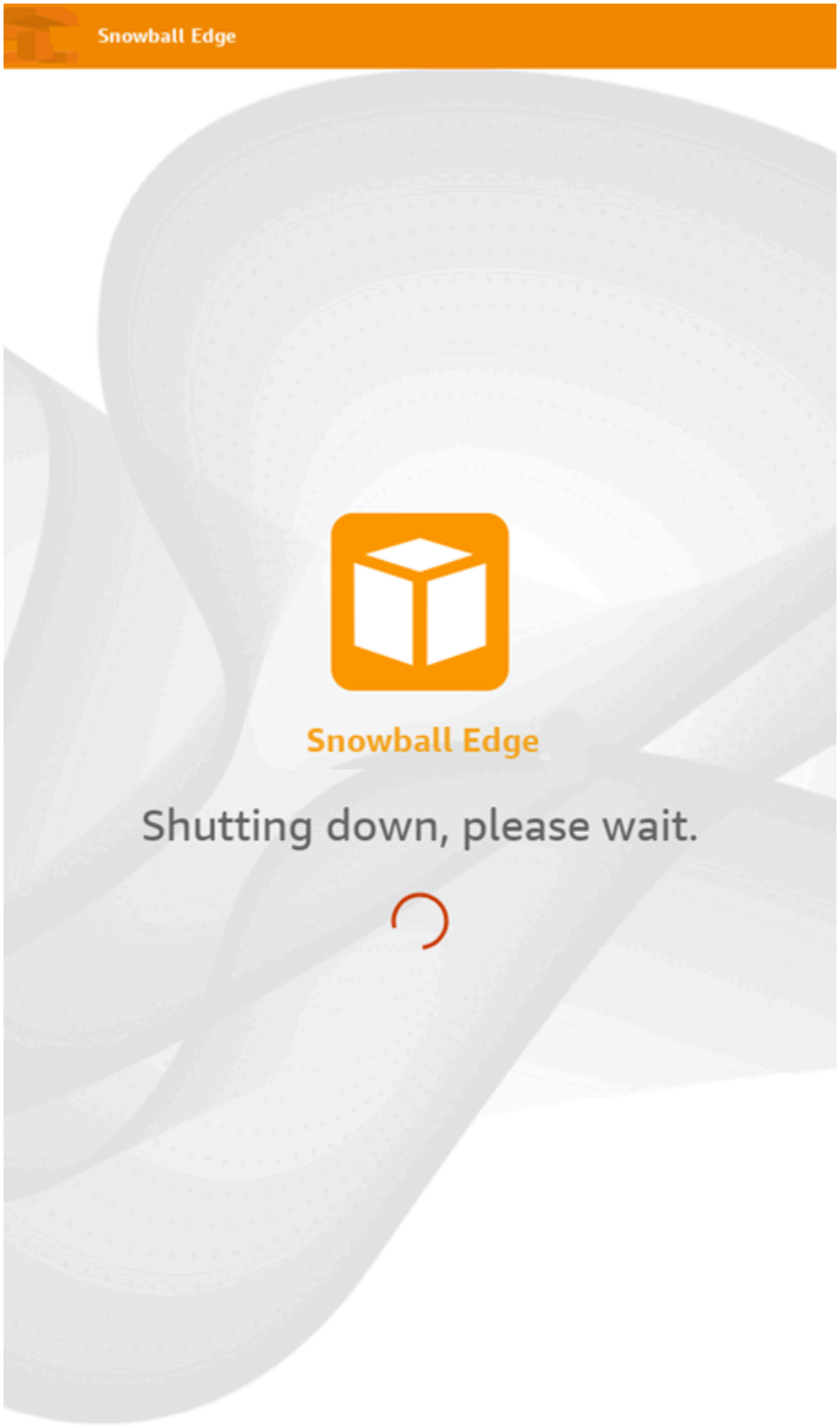
1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Depois escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha o menu Alimentação do dispositivo e, em seguida, escolha Reinicializar. Uma caixa de diálogo é exibida.



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



Enquanto o dispositivo é desligado, a tela LCD exibe uma mensagem indicando que o dispositivo está sendo desligado.


Snowball Edge
Snowball Edge
Shutting down, please wait.

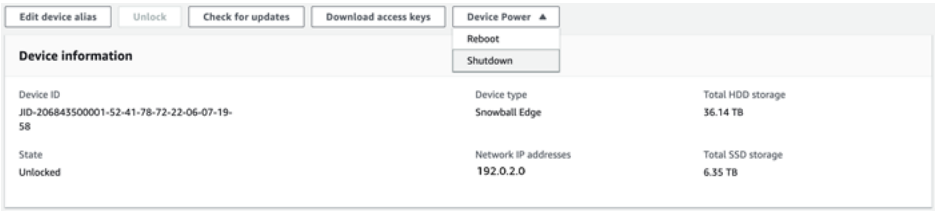
Desligando seu dispositivo

Siga estas etapas AWS OpsHub para desligar seu dispositivo Snow.

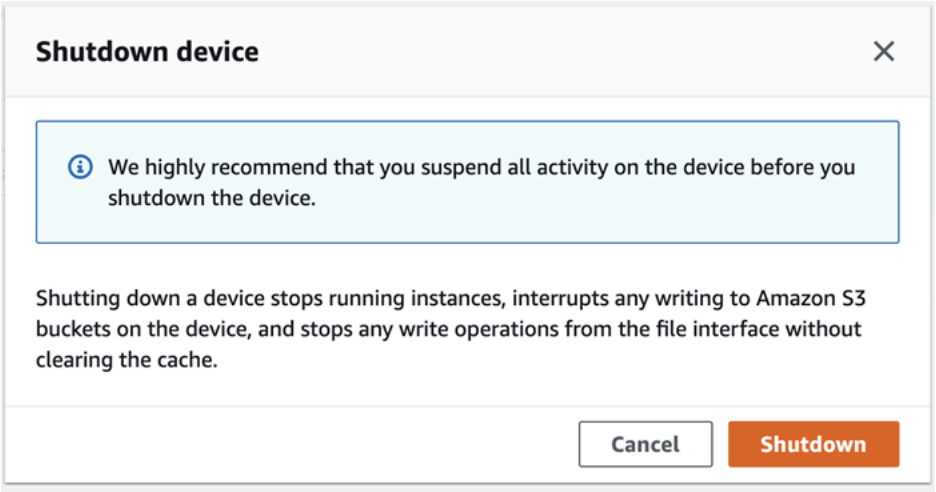
> **Important**
>
> É altamente recomendável suspender todas as atividades no dispositivo antes de reinicializá-lo. O desligamento de um dispositivo interrompe a execução de instâncias e interrompe qualquer gravação nos buckets do Amazon S3 no dispositivo.

Para desligar o dispositivo

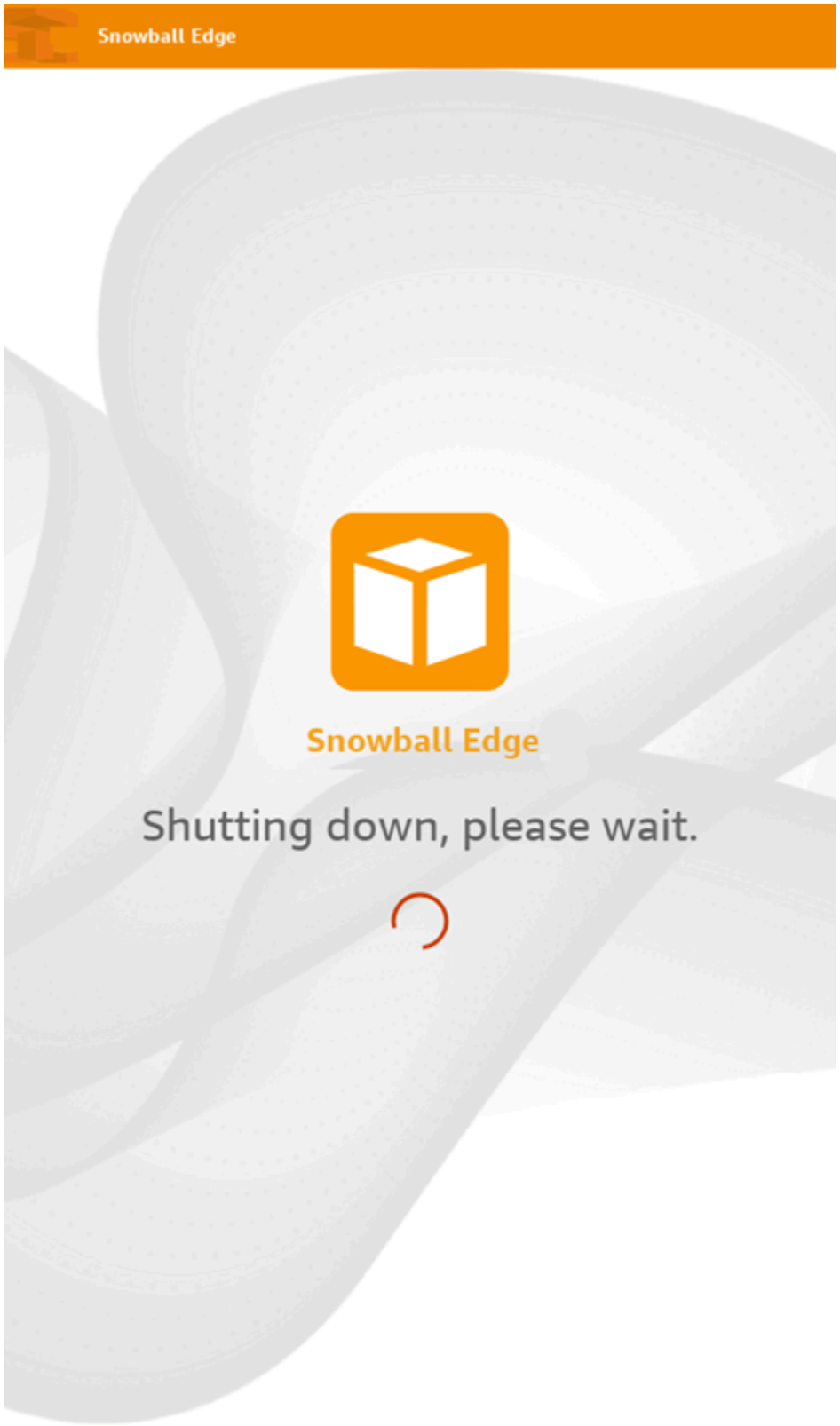
1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Depois escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Escolha o menu Alimentação do dispositivo e, em seguida, escolha Desligar. Uma caixa de diálogo é exibida.



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



Enquanto o dispositivo é desligado, a tela LCD exibe uma mensagem indicando que o dispositivo está sendo desligado.

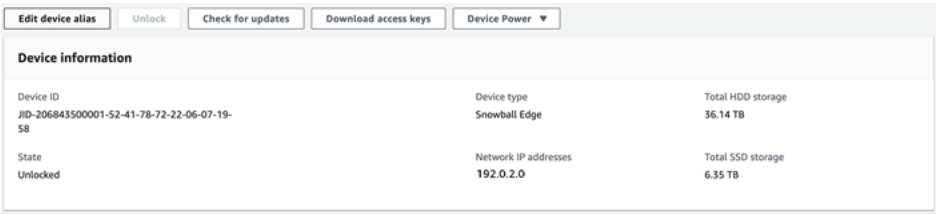

Snowball Edge
Snowball Edge
Shutting down, please wait.

Editar seu alias de dispositivo

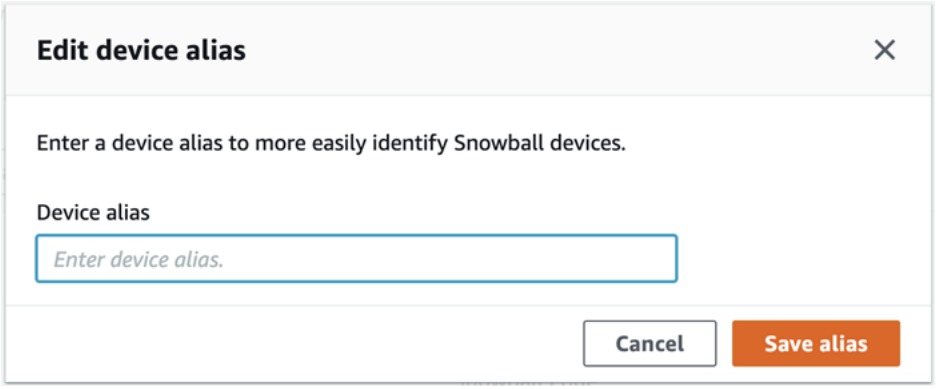
Use essas etapas para editar o alias do seu dispositivo usando AWS OpsHub.

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.



Gerenciando certificados de chave pública usando OpsHub

Você pode interagir com segurança com AWS serviços executados em um dispositivo Snowball Edge ou em um cluster de dispositivos Snowball Edge por meio do protocolo HTTPS fornecendo um certificado de chave pública. Você pode usar o protocolo HTTPS para interagir com AWS serviços como IAM, Amazon EC2, adaptador S3, armazenamento compatível com Amazon S3 em dispositivos da família Snow, Amazon EC2 Systems Manager e dispositivos Snowball Edge. AWS STS No caso de um cluster de dispositivos, um único certificado é necessário, e ele pode ser gerado por qualquer dispositivo no cluster. Depois que um dispositivo Snowball Edge gera o certificado e você desbloqueia o dispositivo, é possível usar os comandos do cliente do Snowball Edge para listar, obter e excluir o certificado.

Um dispositivo Snowball Edge gera um certificado quando ocorrem os seguintes eventos:

- O dispositivo ou o cluster Snowball Edge é desbloqueado pela primeira vez.
- O dispositivo ou cluster Snowball Edge é desbloqueado após a exclusão do certificado (usando o `delete-certificate` comando Renovar certificado em). AWS OpsHub
- O dispositivo ou o cluster Snowball Edge é reinicializado e desbloqueado após a expiração do certificado.

Sempre que um novo certificado é gerado, o certificado antigo deixa de ser válido. Um certificado é válido por um período de um ano a partir do dia em que foi gerado.

Você também pode usar o cliente Snowball Edge para gerenciar certificados de chave pública. Para obter mais informações, consulte Gerenciar certificados de chave pública.

Tópicos

Baixe o certificado de chave pública usando OpsHub

Você pode baixar o certificado de chave pública ativo para o seu computador.

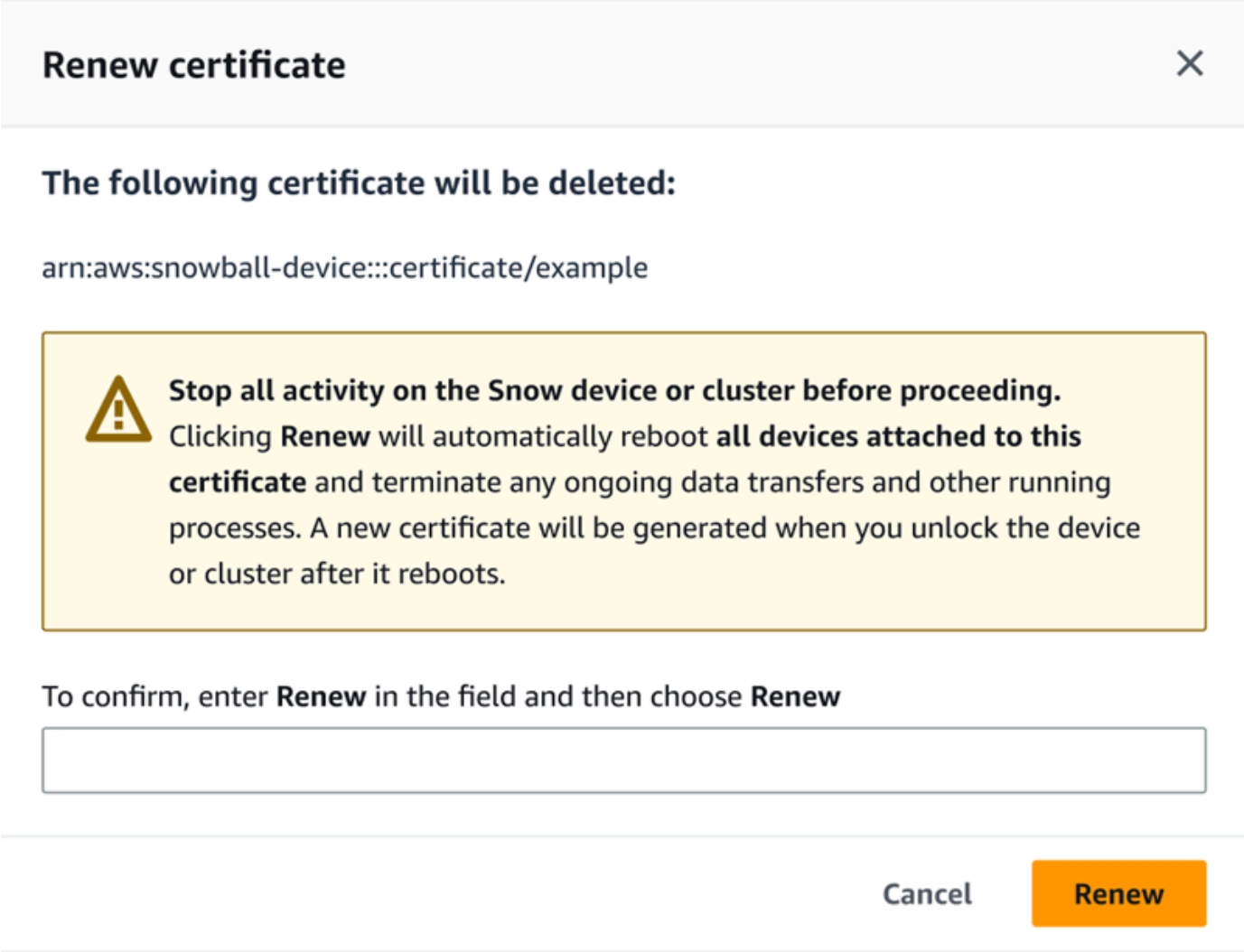
1. No AWS OpsHub painel, encontre seu dispositivo em Dispositivos. Escolha o dispositivo a ser aberto a página de detalhes de dispositivos.
2. Na página de detalhes do dispositivo, escolha o menu Gerenciar certificado. No menu, escolha Baixar certificado.
3. É exibida uma janela na qual você pode nomear o arquivo de certificado a ser baixado e escolher o local em seu computador onde ele será baixado. Escolha Salvar.

Renovando o certificado de chave pública usando OpsHub

Antes de renovar o certificado de chave pública, interrompa todas as transferências de dados de ou para o dispositivo da família Snow e interrompa qualquer compatível com EC2 que esteja em execução. Para obter mais informações, consulte Como interromper uma instância compatível com o Amazon EC2 neste guia.

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

2. Na página de detalhes do dispositivo, escolha o menu Gerenciar certificado. No menu, escolha Renovar certificado.
3. Na janela Renovar certificado, insira o **`Renew`** campo e escolha Renovar. O dispositivo da Família Snow exclui o certificado de chave pública existente e reinicializa o dispositivo ou cluster.



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.

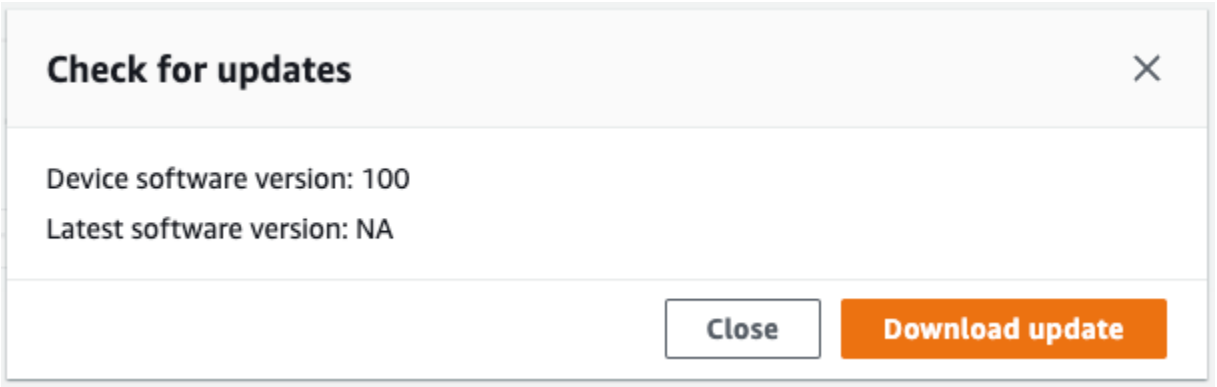
Atualizar seu dispositivo

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.



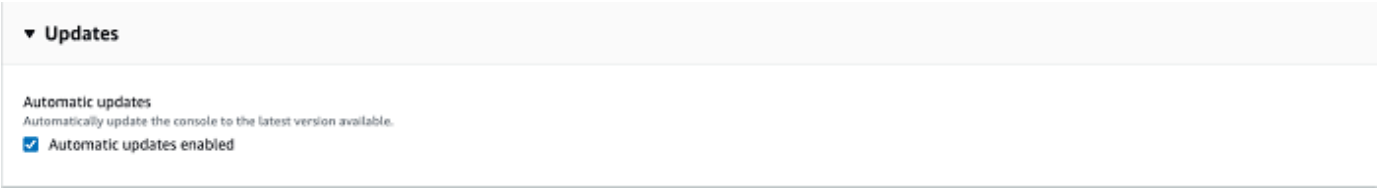
3. Se houver uma atualização, escolha Atualizar. Caso contrário, escolha Fechar.

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.

Automatizar suas tarefas de gerenciamento

Você pode usar AWS OpsHub para automatizar tarefas operacionais que você executa com frequência nos dispositivos da família Snow. Você poderá criar uma tarefa para as ações recorrentes que talvez queira executar em atributos, como reiniciar servidores virtuais, interromper instâncias compatíveis com Amazon EC2 e assim por diante. Você fornece um documento de automação que executa tarefas operacionais com segurança e executa a operação em AWS recursos em massa. Você também pode agendar fluxos de trabalho comuns de TI.

> **Note**
>
> Não há suporte para a automação de tarefas em clusters.
> Para usar tarefas, o serviço Amazon EC2 Systems Manager deve ser iniciado primeiro. Para iniciar um serviço em seu Snowball Edge, consulte Iniciando um serviço em seu Snowball Edge.

Tópicos

Criar e iniciar uma tarefa

Ao criar uma tarefa, você especifica os tipos de recursos em que a tarefa deve ser executada e fornece um documento da tarefa que contém as instruções que executam a tarefa. O documento da tarefa está no formato YAML ou JSON. Depois você fornece os parâmetros necessários para a tarefa e inicia a tarefa.

Para criar uma tarefa

1. Na seção Executar tarefas do painel, escolha Comece a usar para abrir a página Tarefas. Se você tiver criado tarefas, elas serão exibidas em Tarefas.
2. Escolha Criar tarefa e forneça detalhes para a tarefa.
3. Em Nome, insira um nome exclusivo para a tabela.

> **Tip**
>
> O nome deve ter entre 3 e 128 caracteres. Os caracteres válidos são: `a-z`, `A-Z`, `0-9`, `.`, `_` e `-`.

4. Opcionalmente, você poderá escolher um tipo de destino na lista Tipo de destino - opcional. Esse é o tipo de atributo no qual você deseja que a tarefa seja executada.

   Por exemplo, você pode especificar **`/AWS::EC2::Instance`** para as tarefas serem executadas em uma instância compatível com Amazon EC2 ou **`/`** para serem executadas em todos os tipos de atributos.
5. Na seção Conteúdo, escolha YAML ou JSON e forneça o script que executa a tarefa. Você tem duas opções de formato: YAML ou JSON. Para ver exemplos, consulte Exemplos de tarefas.
6. Escolha Criar. A tarefa criada é exibida na página Tarefas.

Como iniciar uma tarefa

1. Na seção Executar tarefas do painel, escolha Comece a usar para abrir a página Tarefas. Suas tarefas são exibidas em Tarefas.
2. Escolha sua tarefa para abrir a página Iniciar tarefa.
3. Escolha Execução simples para executar em destinos.

   Escolha Controle de taxa para executar com segurança em vários destinos e definir limites de simultaneidade e erro. Para essa opção, você fornece as informações adicionais de limite de erro e destino na seção Controle de taxa.
4. Forneça os parâmetros de entrada necessários e escolha Iniciar tarefa.

   O status da tarefa é Pendente e muda para Êxito quando a tarefa é executada com êxito.

Exemplos de tarefas

O exemplo a seguir reinicia uma instância compatível com o Amazon EC2. Ele requer dois parâmetros de entrada: `endpoint` e `instance ID`.

Exemplo de YAML

```
description: Restart EC2 instance
schemaVersion: '0.3'
parameters:
  Endpoint:
    type: String
    description: (Required) EC2 Service Endpoint URL
  Id:
    type: String
    description: (Required) Instance Id
mainSteps:
  - name: restartInstance
    action: aws:executeScript
    description: Restart EC2 instance step
    inputs:
      Runtime: python3.7
      Handler: restart_instance
      InputPayload:
        Endpoint: "{{ Endpoint }}"
        Id: "{{ Id }}"
      TimeoutSeconds: 30
      Script: |-
        import boto3
        import time
        def restart_instance(payload, context):
            ec2_endpoint = payload['Endpoint']
            instance_id = payload['Id']
            ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)
            instance = ec2.Instance(instance_id)
            if instance.state['Name'] != 'stopped':
                instance.stop()
                instance.wait_until_stopped()
            instance.start()
            instance.wait_until_running()
            return {'InstanceState': instance.state}
```

Exemplo de JSON

```
{
  "description" : "Restart EC2 instance",
  "schemaVersion" : "0.3",
  "parameters" : {
    "Endpoint" : {
```

```
      "type" : "String",
      "description" : "(Required) EC2 Service Endpoint URL"
    },
    "Id" : {
      "type" : "String",
      "description" : "(Required) Instance Id"
    }
  },
  "mainSteps" : [ {
    "name" : "restartInstance",
    "action" : "aws:executeScript",
    "description" : "Restart EC2 instance step",
    "inputs" : {
      "Runtime" : "python3.7",
      "Handler" : "restart_instance",
      "InputPayload" : {
        "Endpoint" : "{{ Endpoint }}",
        "Id" : "{{ Id }}"
      },
      "TimeoutSeconds" : 30,
      "Script" : "import boto3\nimport time\ndef restart_instance(payload, context):\n

            ec2_endpoint = payload['Endpoint']\n    instance_id = payload['Id']\n
            ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)\n
            instance = ec2.Instance(instance_id)\n
            if instance.state['Name'] != 'stopped':\n
            instance.stop()\n
            instance.wait_until_stopped()\n
            instance.start()\n
            instance.wait_until_running()\n
            return {'InstanceState': instance.state}"
    }
  } ]
}
```

Visualizar detalhes de uma tarefa

Você pode visualizar os detalhes de uma tarefa de gerenciamento, como a descrição e os parâmetros necessários para executar a tarefa.

Como visualizar os detalhes de uma tarefa

1. Na seção Executar tarefas do painel, escolha Comece a usar para abrir a página Tarefas.

2. Na página Tarefas, localize e escolha a tarefa da qual você deseja ver os detalhes.
3. Escolha Exibir detalhes e selecione uma das guias para ver os detalhes. Por exemplo, a guia Parâmetros mostra os parâmetros de entrada no script.

Exclusão de uma tarefa

Siga estas etapas para excluir uma tarefa de gerenciamento.

Para excluir uma tarefa

1. Na seção Executar tarefas do painel, escolha Comece a usar para abrir a página Tarefas.
2. Localize a tarefa que você deseja excluir. Selecione a tarefa e escolha Excluir.

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.

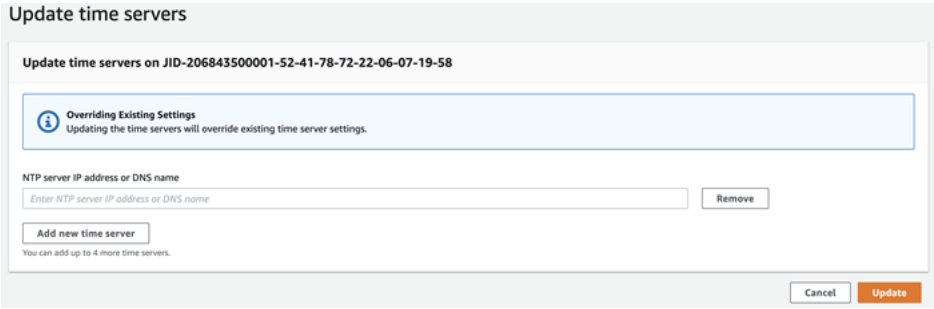
   A tabela Fontes de tempo tem quatro colunas:

   - 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.



Tipos de dispositivos NTP e versões de software compatíveis

O NTP não está disponível em nenhum tipo de dispositivo de armazenamento e computação da versão 2. No entanto, os tipos de dispositivos de armazenamento e computação do Snowball Edge versão 3 com software versão 77 ou posterior oferecem suporte a NTP. Para verificar se o NTP está ativado, use o comando `describe-time-sources` da CLI do Snowball Edge.

Usando um dispositivo AWS Snowball Edge

A seguir, você pode encontrar uma visão geral do AWS Snowball Edge dispositivo. O Snowball Edge é um dispositivo fisicamente robusto protegido por AWS Key Management Service (AWS KMS) que você usa 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 Snowball Edge dispositivo, consulte. Utilização do Snowball Edge Client

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. Você receberá um novo dispositivo.

A imagem a seguir mostra a aparência do AWS Snowball Edge dispositivo.

Ele tem três portas, uma frontal, uma traseira e uma na parte superior que podem ser abertas por travas. O cabo de alimentação do dispositivo encontra-se na porta superior. As outras duas portas podem ser abertas e deslizadas para dentro do dispositivo, de forma que não funcionem enquanto ele estiver sendo usado. Abrindo as portas, você obtém acesso ao monitor LCD E Ink integrado na parte frontal do dispositivo, e às portas de energia e de rede na parte traseira.

Assim que o dispositivo chegar e for ligado, estará tudo pronto para usá-lo.

Tópicos

- Utilização do Snowball Edge Client
- Transferência de arquivos usando o adaptador do Amazon S3 para migração de dados
- Gerenciando a interface NFS
- Usando AWS IoT Greengrass para executar software pré-instalado em instâncias compatíveis com o Amazon EC2

- Usando AWS Lambda com um AWS Snowball Edge
- Usar instâncias de computação compatíveis com o Amazon EC2
- Usando armazenamento compatível com Amazon S3 em dispositivos da Família Snow
- Usando o Amazon EKS Anywhere on AWS Snow
- Usar o IAM localmente
- Usar o AWS Security Token Service
- Gerenciar certificados de chave pública
- Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge

Utilização do Snowball Edge Client

A seguir, você encontrará informações sobre como obter e usar o cliente Snowball Edge com seu AWS Snowball Edge dispositivo. O Snowball Edge Client é uma aplicação terminal autônoma executada no servidor local para desbloquear o dispositivo e obter credenciais, logs e informações de status. Você também pode usar o cliente para tarefas administrativas para um cluster. 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 Snowball Edge dispositivo, você usa o adaptador Amazon S3 ou a interface de arquivos.

Fazer download e instalar o Snowball Edge Client

É possível fazer download e instalar o Snowball Edge Client em Atributos do AWS Snowball Edge. Nessa página, você pode encontrar o pacote de instalação para o sistema operacional. 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/`. O Snowball Edge Client só é compatível com distribuições Linux de 64 bits.
- 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.

Tópicos

- 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 deles 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 Obter credenciais para acessar um dispositivo Snow Family.

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-edge.config`.

O endpoint é o endereço IP, com `https://` adicionado a ele. Você pode localizar o endereço IP do AWS Snowball Edge dispositivo na tela LCD do AWS Snowball Edge dispositivo. Quando o AWS Snowball Edge dispositivo é conectado à sua rede pela primeira vez, ele obtém 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 um dispositivo AWS Snowball Edge.

> **Important**
>
> Qualquer pessoa que possa acessar o arquivo de configuração poderá acessar os dados nos seus dispositivos ou clusters do Snowball Edge. 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 Saída

```
Configuration will stored at home directory\.aws\snowball\config\snowball-edge.config
Snowball Edge Manifest Path: /Path/to/manifest/file
Unlock Code: 29 character unlock code
Default Endpoint: https://192.0.2.0
```

Você pode ter múltiplos perfis se tiver vários trabalhos ao mesmo tempo ou se quiser a opção de gerenciar um cluster a partir de diferentes endpoints. 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 Snowball Edge. 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 Saída

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

Versão do Snowball Edge Client

Use o comando `version` para ver a versão do cliente da interface de linha de comando (CLI) do Snowball Edge.

Uso

```
    snowballEdge version
```

Exemplo de saída

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

Desbloquear dispositivos do Snowball Edge

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

> **Note**
>
> Para desbloquear os dispositivos associados ao seu trabalho, eles devem estar no local, ligados e conectados à rede e à alimentação. Além disso, o display LCD na parte frontal do AWS Snowball Edge dispositivo deve indicar que o dispositivo está pronto para uso.

Uso

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

Example Entrada de desbloqueio de dispositivo individual

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

Example Saída de desbloqueio de dispositivo individual

```
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.
```

Uso do cluster

Ao desbloquear um cluster, forneça o endpoint para um dos seus nós, além de todos os endereços IP para os outros dispositivos no seu cluster.

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

Example Saída de desbloqueio de cluster

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

Atualização de um Snowball Edge

Use os comandos a seguir para fazer download e instalar atualizações para seu dispositivo Snowball Edge. Para obter os procedimentos que usam esses comandos, consulte Atualização de software em dispositivos Snowball Edge.

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

Uso (Snowball Edge Client configurado)

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

Example Saída

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

`snowballEdge describe-device-software`: retorna a versão atual do software e a data de validade do certificado SSL do dispositivo. Além disso, se a atualização do software estiver sendo baixada ou instalada, o estado do download também será exibido. 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 precisa 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 Saída

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

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

Uso (Snowball Edge Client configurado)

```
snowballEdge download-updates
```

Example Saída

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

`snowballEdge install-updates`: inicia a instalação das atualizações mais recentes do Snowball Edge que já foram baixadas.

Uso (Snowball Edge Client configurado)

```
snowballEdge install-updates
```

Example Saída

```
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 Saída

```
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 Saída

```
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 Saída

```
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

Usando os `snowballEdge get-secret-access-key` comandos `snowballEdge list-access-keys` e, você pode obter as credenciais do usuário administrador do seu Conta da AWS no Snowball Edge. Você pode usar essas credenciais para criar AWS Identity and Access Management (usuários do IAM) e funções, além de autenticar suas solicitações ao usar o AWS CLI ou com um AWS SDK. Essas credenciais só estão associadas a um trabalho individual para o Snowball Edge, e você pode usá-las apenas no dispositivo ou cluster de dispositivos. Os dispositivos não têm permissões do IAM na Nuvem AWS.

> **Note**
>
> Se você estiver usando o AWS CLI com o Snowball Edge, deverá usar essas credenciais ao configurar a CLI. Para obter informações sobre como configurar credenciais para o AWS CLI, consulte Configurando o AWS CLI no Guia doAWS Command Line Interface Usuário.

Uso (Snowball Edge Client configurado)

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

Example Saída

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

Uso (Snowball Edge Client configurado)

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

Example Saída

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

Inicialização de um serviço no Snowball Edge

Os dispositivos Snowball Edge oferecem suporte a vários serviços, além do Amazon S3. Isso inclui instâncias de computação, a interface de arquivos e. AWS IoT Greengrass O Amazon S3 e o Amazon EC2 sempre estão ativados por padrão e não podem ser interrompidos ou reiniciados com o Snowball Edge Client. No entanto, a interface do arquivo AWS IoT Greengrass pode ser iniciada com o `snowballEdge start-service` comando. 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 Saída

```
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 no Snowball Edge

Para interromper um serviço em execução no Snowball Edge, use o comando `snowballEdge stop-service`.

O adaptador Amazon S3, o Amazon EC2 e os serviços do IAM não AWS STS 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. Para obter mais informações sobre como usar a interface de arquivos, consulte Gerenciando a interface NFS.

> **Note**
>
> A interrupção do serviço de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow desativa o acesso aos dados armazenados em seus buckets do S3 no dispositivo ou cluster. O acesso é restaurado quando o armazenamento compatível com o Amazon S3 nos dispositivos da Família Snow é reiniciado. Para dispositivos habilitados com armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, é recomendável iniciar o serviço depois que o dispositivo Snowball Edge for ligado. Consulte Configuração do Snowball Edge neste guia.

Uso (Snowball Edge Client configurado)

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

Example Saída

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

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**
>
> É possível fornecer blocos CIDR para intervalos de 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. Lembre-se de que 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 obter mais informações, consulte Como criar 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
```

AWS Snowball Edge Registros

Ao transferir dados entre o datacenter local e um Snowball Edge, 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 Saída

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

- `get-log`— Faz o download de uma cópia de um registro específico do Snowball Edge 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-
  JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709
  ```

  Example Saída

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

- `get-support-logs`: baixa a cópia de todos os logs de tipo `SUPPORT` a partir do Snowball Edge para o seu serviço em um caminho específico.

  Uso (Snowball Edge Client configurado)

  Snowball Edge Client

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

Example Saída

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

> **Important**
>
> O tipo CUSTOMER pode 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 Snowball Edge usando os seguintes comandos do Snowball Edge Client:

- `describe-device`

  Uso (Snowball Edge Client configurado)

  ```
  snowballEdge describe-device
  ```

  Example Saída

  ```
  {
    "DeviceId" : "JID-EXAMPLE12345-123-456-7-890",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.0.2.0"
    },
    "PhysicalNetworkInterfaces" : [ {
      "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLEd9ecbf03e3",
      "PhysicalConnectorType" : "RJ45",
      "IpAddressAssignment" : "STATIC",
  ```

```
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLE4c3840068f",
    "PhysicalConnectorType" : "QSFP",
    "IpAddressAssignment" : "STATIC",
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.0.2.2",
    "MacAddress" : "EX:AM:PL:E0:56:78"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLE0a3a6499fd",
    "PhysicalConnectorType" : "SFP_PLUS",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.168.1.231",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.3",
    "MacAddress" : "EX:AM:PL:E0:90:12"
  } ]
}
```

- `describe-cluster`

  Uso (Snowball Edge Client configurado)

  ```
  snowballEdge describe-cluster
  ```

  Example Saída

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

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

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

Ver status do serviço

Você pode determinar o status e a integridade geral dos serviços que funcionam nos dispositivos Snowball Edge 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 Saída

  ```
  {
    "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
  }
  ```

- `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.
  - `DEGRADED`: para armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, esse status indica que um ou mais discos ou dispositivos no cluster estão inativos. O serviço de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow está funcionando sem interrupções, mas você deve recuperar ou substituir o dispositivo afetado antes que o quorum do cluster seja perdido para minimizar o risco de perda de dados. Consulte a Visão geral do cluster neste guia.
  - `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 Saída

```
{
"ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
"Storage" : {
"TotalSpaceBytes" : 99608745492480,
"FreeSpaceBytes" : 99608744468480
},
"Endpoints" : [ {
"Protocol" : "http",
"Port" : 8080,
"Host" : "192.0.2.0"
}, {
"Protocol" : "https",
"Port" : 8443,
"Host" : "192.0.2.0",
```

```
"CertificateAssociation" : {
"CertificateArn" : "arn:aws:snowball-
device:::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}
```

Example Saída de serviço de armazenamento compatível com Amazon S3 em dispositivos da Família Snow

O comando `describe-service` fornece a seguinte saída para o valor **`s3-snow`** do parâmetro `service-id`.

```
{
  "ServiceId" : "s3-snow",
  "Autostart" : false,
  "Status" : {
    "State" : "ACTIVE"
  },
  "ServiceCapacities" : [ {
    "Name" : "S3 Storage",
    "Unit" : "Byte",
    "Used" : 640303104,
    "Available" : 219571981512
  } ],
  "Endpoints" : [ {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.123",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.202",
```

```
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.63",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.243",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.220",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
```

```
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.55",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.213",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.144",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
```

```
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.143",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.224",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  } ]
}
```

Remoção de um nó a partir de um cluster

O comando `disassociate-device` remove um nó de um cluster Snowball Edge. Se você quiser substituir um nó não íntegro, use este comando. Para obter mais informações sobre clusters, consulte Visão geral do cluster neste guia.

> **Important**
>
> Use o comando `disassociate-device` somente quando você estiver removendo um nó não íntegro. Este comando falhará e retornará um erro se você tentar remover um nó íntegro.

Não use esse comando para remover um nó que foi desligado acidentalmente ou desconectado da rede e, portanto, está temporariamente indisponível para o resto do cluster. Os nós removidos com este comando não podem ser adicionados a nenhum cluster e devem ser retornados à AWS.

Se um nó foi acidentalmente desligado ou desconectado da rede, conecte o nó de volta à alimentação e à rede e usar o comando `associate-device`. Não é possível usar o comando `disassociate-device` para desassociar um nó se ele estiver ligado e for íntegro.

Uso (Snowball Edge Client configurado)

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

Example Saída

```
Disassociating your Snowball Edge device from the cluster. Your Snowball Edge device
 will be disassociated from the cluster when it is in the "DISASSOCIATED" state. You
 can use the describe-cluster command to determine the state of your cluster.
```

Como adicionar um nó a um cluster

O comando `associate-device` adiciona um nó a um cluster de dispositivos Snowball Edge. Se você desligar um nó, ele reverterá seu estado de desbloqueado para bloqueado. Para desbloquear esse nó, você pode usar este comando. Use esse comando para substituir um nó indisponível por um novo nó que você tenha solicitado como substituto. Para obter mais informações sobre clusters, consulte Visão geral do cluster neste guia.

Uso (Snowball Edge Client configurado)

```
snowballEdge associate-device --device-ip-address IP Address
```

Example Saída

```
Associating your Snowball Edge device with the cluster. Your Snowball Edge device will
 be associated with the cluster when it is in the ASSOCIATED state. You can use the
 describe-cluster command to determine the state of your cluster.
```

Criar tags para o dispositivo

Adiciona ou substitui as tags especificadas no dispositivo. É possível criar no máximo 50 tags. Cada tag consiste em um par de chave-valor. O valor é opcional.

> **Note**
>
> Não coloque dados confidenciais nas tags.

Uso (Snowball Edge Client configurado)

```
snowballEdge create-tags --tag Key=Name,Value=user-test --tag Key=Stage,Value=beta
```

Para obter mais informações, execute o comando `describe-tags`.

Example Saída

```
Tag(s) [Key=Name,Value=test, Key=Stage,Value=beta] created.
```

Excluir tags do dispositivo

O comando `delete-tags` exclui as tags especificadas do dispositivo Snowball Edge.

Uso (Snowball Edge Client configurado)

```
snowballEdge delete-tags --tag Key=Stage,Value=beta
    Tag(s) [Key=Stage,Value=beta] deleted.
```

Para obter mais informações, execute o comando `describe-tags`.

> **Note**
>
> Se você quiser excluir várias tags ao mesmo tempo, poderá especificar vários pares de chave-valor, como o seguinte:
> `delete-tags --tag Key=Name,Value=test --tag Key=Stage,Value=Beta`
> Se você especificar uma chave de tag sem um valor de tag, qualquer tag com essa chave, independentemente de seu valor, será excluída. Se você especificar uma chave de tag com uma string vazia como o valor da tag, somente as tags que têm uma string vazia como valor serão excluídas.

Descrever tags no dispositivo

O comando `describe-tags` descreve as tags no dispositivo Snowball Edge.

Uso (Snowball Edge Client configurado)

```
snowballEdge describe-tags
```

Para obter mais informações, execute o comando `describe-tags`.

Example Saída

```
{
  "Tags" : [ {
    "Key" : "Name",
    "Value" : "user-test"
  }, {
    "Key" : "Stage",
    "Value" : "beta"
  } ]
}
```

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 compatíveis com 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)

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

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 computacionais compatíveis com o 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)

```
snowballEdge 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 instâncias computacionais compatíveis com Amazon EC2 no 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 compatível com o Amazon EC2, a interface será primeiro desanexada.

Uso (Snowball Edge Client configurado)

```
snowballEdge update-direct-network-interface [--direct-network-interface-
arn directNetworkInterfaceArn] [--endpoint endpoint]
                                [--mac macAddress]
                                [--manifest-file manifestFile] [--profile profile] [--
unlock-code unlockCode]
                                [--vlan vlanId] [--attach-instance-id instanceId | --
detach]
```

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 computacional compatível com Amazon EC2, você deve primeiro desassociar a interface de rede direta da sua instância.

Uso (Snowball Edge Client configurado)

```
snowballEdge 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 no seu dispositivo, use o `describe-features` comando.

`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
}
```

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.

Tipos de dispositivos NTP e versões de software compatíveis

O NTP não está disponível em nenhum tipo de dispositivo de armazenamento e computação da versão 2. No entanto, os tipos de dispositivos de armazenamento e computação do Snowball Edge versão 3 com software versão 77 ou posterior oferecem suporte a NTP. Para verificar se o NTP está ativado, use o comando `describe-time-sources` da CLI do Snowball Edge.

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.

Transferência de arquivos usando o adaptador do Amazon S3 para migração de dados

Veja a seguir uma visão geral do adaptador Amazon S3, que você pode usar para transferir dados programaticamente de e para buckets do S3 que já estão no dispositivo usando as ações da API REST do AWS Snowball Edge Amazon S3. Esse suporte da API REST do Amazon S3 é limitado a um subconjunto de ações. Esse subconjunto de ações pode ser usado com um dos SDKs da AWS para transferir dados de forma programática. O subconjunto de comandos AWS Command Line Interface (AWS CLI) compatíveis com o Amazon S3 também pode ser usado para transferir dados de forma programática.

Se a solução usar o AWS SDK for Java versão 1.11.0 ou mais recente, será necessário empregar o seguinte `S3ClientOptions`:

- `disableChunkedEncoding()`: indica que a codificação em partes não é compatível com a interface.
- `setPathStyleAccess(true)`: configura a interface para usar o acesso no estilo de caminho para todas as solicitações.

Para obter mais informações, consulte Class S3 ClientOptions .Builder no Amazon AppStream SDK for Java.

> **Important**
>
> Recomendamos usar apenas um método de leitura e gravação de dados num bucket local em um dispositivo AWS Snowball Edge por vez. Usar a interface de arquivos e o adaptador

do Amazon S3 no mesmo bucket ao mesmo tempo pode resultar em conflitos de leitura/gravação.
AWS Snowball Cotas Edge detalha os limites.
Para que os serviços da AWS funcionem corretamente em um Snowball Edge, é necessário ativar as portas dos serviços. Para obter detalhes, consulte Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge.

Tópicos

Baixando e instalando a versão 1.16.14 do AWS CLI para uso com o adaptador do Amazon S3

No momento, os dispositivos Snowball Edge dão suporte apenas à versão 1.16.14 e anteriores do AWS CLI para uso com o adaptador do Amazon S3. As versões mais recentes do AWS CLI não são compatíveis com o adaptador do Amazon S3 porque não oferecem suporte a todas as funcionalidades.

Note

Se você estiver usando armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, pode usar a versão mais recente do AWS CLI. Para baixar e usar a versão mais recente, consulte o Manual do usuário do AWS Command Line Interface.

Instalação do AWS CLI em sistemas operacionais Linux

Execute este comando em cadeia:

```
curl "https://s3.amazonaws.com/aws-cli/awscli-bundle-1.16.14.zip" -o "awscli-
bundle.zip";unzip awscli-bundle.zip;sudo ./awscli-bundle/install -i /usr/local/aws -b /
usr/local/bin/aws;/usr/local/bin/aws --version;
```

Instale o AWS CLI em sistemas operacionais Windows

Faça o download e execute o arquivo do instalador para o seu sistema operacional:

- 32 bits
- 64 bits

Usar o AWS CLI e as operações de API em dispositivos Snowball Edge

Ao usar o AWS CLI ou as operações de API para emitir comandos do IAM, Amazon S3 e Amazon EC2 no Snowball Edge, você deve especificar a região como "`snow`". Você pode fazer isso usando `AWS configure` ou dentro do próprio comando, como nos exemplos a seguir.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Ou

```
aws s3 ls --profile snowballEdge --endpoint http://192.0.2.0:8080 --region snow
```

Autorização com a interface de API do Amazon S3 para AWS Snowball

Quando você usa o adaptador do Amazon S3, todas as interações são assinadas por padrão com o algoritmo do AWS Signature versão 4. Essa autorização é usada apenas para verificar os dados que estão trafegando da origem para a interface. Toda a criptografia e descriptografia acontecem no dispositivo. Os dados não criptografados nunca são armazenados no dispositivo.

Ao usar a interface, tenha em mente o seguinte:

- Para obter as credenciais locais do Amazon S3 e assinar as solicitações para o dispositivo AWS Snowball Edge, execute os comandos `snowballEdge list-access-keys` e `snowballEdge get-secret-access-keys` do Snowball Edge Client. Para ter mais informações, consulte Utilização do Snowball Edge Client. Essas credenciais locais do Amazon S3 incluem um par de chaves: uma chave de acesso e uma chave secreta. Essas chaves são válidas apenas para os dispositivos associados ao trabalho. Eles não podem ser usados na Nuvem AWS porque não têm equivalente do AWS Identity and Access Management (IAM).
- A chave de criptografia não é alterada pelas credenciais da AWS usadas. A assinatura com o algoritmo do Signature versão 4 é usada somente para verificar os dados que estão trafegando da origem para a interface. Assim, essa assinatura nunca é fatorada nas chaves de criptografia usadas para criptografar seus dados no Snowball.

Obtenção e utilização de credenciais do Amazon S3 locais

Cada interação com o Snowball Edge é assinada com o algoritmo Signature versão 4 da AWS. Para obter mais informações sobre o algoritmo, consulte Processo de assinatura do Signature versão 4 na Referência geral da AWS.

Você pode obter as credenciais locais do Amazon S3 para assinar suas solicitações do dispositivo Edge do Snowball Edge Client executando `snowballEdge list-access-keys` e `snowballEdge get-secret-access-key`. Consulte Como obter as credenciais. Essas credenciais locais do Amazon S3 incluem um par de chaves: um ID de chave de acesso e uma chave secreta. Essas credenciais são válidas apenas para os dispositivos que estão associados ao trabalho. Eles não podem ser usados na Nuvem AWS porque não têm equivalente do IAM.

Essas credenciais podem ser adicionadas ao arquivo de credenciais da AWS no servidor. O arquivo de perfis de credenciais padrão normalmente está localizado em `~/.aws/credentials`, mas a localização pode variar conforme a plataforma. Este arquivo é compartilhado por muitos SDKs da AWS e pelo AWS CLI. As credenciais locais podem ser salvas com um nome de perfil, como no exemplo a seguir.

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

Especificação do adaptador do S3 como endpoint do AWS CLI

Quando a AWS CLI for usado para emitir um comando para o dispositivo AWS Snowball Edge, especifique que o endpoint é o adaptador do Amazon S3. Você tem a opção de usar o endpoint HTTPS ou um endpoint HTTP desprotegido, como mostrado a seguir.

Endpoint HTTPS protegido

```
aws s3 ls --profile snowballEdge --endpoint https://192.0.2.0:8443 --ca-bundle path/to/certificate
```

Endpoint HTTP desprotegido

```
aws s3 ls --profile snowballEdge --endpoint http://192.0.2.0:8080
```

Se você usar o endpoint HTTPS `8443`, os dados serão transferidos com segurança a partir do seu servidor para o Snowball Edge. A criptografia é garantida com um certificado que é gerado pelo Snowball Edge sempre que ele recebe um novo endereço IP. 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 da interface

1. Conecte o Snowball Edge à alimentação e à rede. Em seguida, ligue-o.
2. Depois que o dispositivo tiver sido inicializado, 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 Snowball Edge.
4. Execute o comando `snowballEdge get-certificate` no seu terminal. Para obter mais informações sobre este comando, consulte Gerenciar certificados de chave pública.
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.snowballEdge.ca_bundle /path/to/ca-bundle.pem
   ```

Depois de concluir o procedimento, você poderá executar os comandos da CLI com essas credenciais locais, além do seu certificado e endpoint especificado, como no exemplo a seguir.

```
aws s3 ls --profile snowballEdge --endpoint https://192.0.2.0:8443
```

Atributos não compatíveis do Amazon S3 para o adaptador do Amazon S3

Usando o Amazon S3, você pode transferir, de forma programática, dados de e para um Snowball Edge com ações da API do Amazon S3. No entanto, nem todas as ações de API e atributos de transferência do Amazon S3 podem ser usados com um dispositivo Snowball Edge ao usar o adaptador do Amazon S3. Por exemplo, os seguintes atributos e ações não são compatíveis com o uso do Snowball Edge:

- TransferManager— Esse utilitário transfere arquivos de um ambiente local para o Amazon S3 com o SDK for Java. Em vez disso, considere o uso de ações de API com suporte ou comandos da AWS CLI com a interface.
- GET Bucket (listagem de objetos) versão 2: essa implementação da ação GET retorna alguns ou todos (até 1.000) dos objetos de um bucket. Considere o uso da ação GET Bucket (listagem de objetos) versão 1 ou do comando ls da AWS CLI.
- ListBuckets— O ListBuckets com o endpoint do objeto não é suportado. O comando a seguir não funciona com armazenamento compatível com o Amazon S3 em dispositivos da Família Snow:

  ```
  aws s3 ls --endpoint https://192.0.2.0 --profile profile
  ```

Agrupar arquivos pequenos em lote

Cada operação de cópia tem certa sobrecarga por causa da criptografia. Para acelerar o processo de transferência de arquivos pequenos para o dispositivo AWS Snowball Edge, você pode agrupá-los em um único arquivo. Quando você agrupa os arquivos em lote, eles podem ser extraídos automaticamente quando são importados para o Amazon S3, se eles foram armazenados em lote em um dos formatos de arquivo compatíveis.

Normalmente, os arquivos de 1 MB ou menos devem ser incluídos em lotes. Não há limite rígido para o número de arquivos que é possível ter em um lote. Entretanto, recomendamos que você limite os lotes para 10.000 arquivos aproximadamente. Ter mais de 100.000 arquivos em um lote pode afetar a rapidez com que os arquivos são importados para o Amazon S3 depois que você devolver o dispositivo. Recomendamos que o tamanho total de cada lote não seja maior que 100 GB.

Agrupar os arquivos em lote é um processo manual que você gerencia. Depois de agrupar os arquivos em lote, transfira-os para um dispositivo Snowball Edge usando o comando `cp` do AWS CLI com a opção `--metadata snowball-auto-extract=true`. A especificação `snowball-auto-extract=true` extrai automaticamente o conteúdo dos arquivos compactados quando os dados são importados para o Amazon S3, desde que o tamanho do arquivo em lote não seja maior que 100 GB.

> **Note**
>
> Todos os lotes com mais de 100 GB não são extraídos quando importados para o Amazon S3.

Para agrupar arquivos pequenos em lote

1. Decida em qual formato você deseja agrupar seus arquivos pequenos em lote. O recurso de extração automática é compatível com os formatos `TAR`, `ZIP` e `tar.gz`.
2. Identifique quais arquivos pequenos você deseja agrupar em lote, incluindo o tamanho e o número total de arquivos.
3. Faça um lote de seus arquivos na linha de comando da seguinte forma.

   - Para Linux, é possível agrupar os arquivos em lote na mesma linha de comando usada para transferir os arquivos para o dispositivo.

     ```
     tar -cf - /Logs/April | aws s3 cp - s3://mybucket/batch01.tar --metadata
      snowball-auto-extract=true --endpoint http://192.0.2.0:8080
     ```

     > **Note**
     >
     > Você também pode usar o utilitário de arquivamento de sua escolha para agrupar os arquivos em lote em um ou mais arquivos grandes. No entanto, essa abordagem exige mais armazenamento local para salvar os arquivos antes de transferi-los para o Snowball.

   - Para Windows, use o comando de exemplo a seguir para agrupar os arquivos em lote quando todos os arquivos estiverem no mesmo diretório a partir do qual o comando é executado:

```
7z a -tzip -so "test" | aws s3 cp - s3://mybucket/batch01.zip --metadata
 snowball-auto-extract=true --endpoint http://192.0.2.0:8080
```

Para agrupar arquivos em lote de um diretório diferente a partir do qual o comando é executado, use o seguinte comando de exemplo:

```
7z a -tzip -so "test" "c:\temp" | aws s3 cp - s3://mybucket/batch01.zip --
metadata snowball-auto-extract=true --endpoint http://10.x.x.x:8080
```

> **Note**
>
> Para o Microsoft Windows 2016, o tar não está disponível, mas você pode baixá-lo no site do Tar for Windows.
> Você pode baixar o 7 ZIP no site do 7ZIP.

4. Repita até que você arquive todos os arquivos pequenos que deseja transferir para o Amazon S3 usando um Snowball Edge.
5. Transfira os arquivos armazenados para o Snowball. Se você deseja que os dados sejam extraídos automaticamente, e usou um dos formatos de arquivo compatíveis mencionados anteriormente na etapa 1, use o comando `cp` da AWS CLI com a opção `--metadata snowball-auto-extract=true`.

> **Note**
>
> Se houver arquivos que não são de arquivamento, não use esse comando.

Ao criar os arquivos de arquivamento, a extração manterá a estrutura de dados atual. Isso significa que, se você criar um arquivo que contenha arquivos e pastas, o Snowball Edge o recriará durante o processo de ingestão no Amazon S3.

O arquivo será extraído no mesmo diretório em que está armazenado e as estruturas de pastas serão criadas de acordo. Lembre-se de que, ao copiar arquivos compactados, é importante definir o sinalizador `--metadata snowball-auto-extract=true`. Caso contrário, o Snowball Edge não extrairá os dados quando forem importados para o Amazon S3.

Usando o exemplo na etapa 3, se você tiver a estrutura de pastas /Logs/April/ que contém arquivos `a.txt`, `b.txt` e `c.txt`. Se esse arquivo de arquivamento fosse colocado na raiz de /mybucket/, os dados teriam a seguinte aparência após a extração:

```
/mybucket/Logs/April/a.txt
/mybucket/Logs/April/b.txt
/mybucket/Logs/April/c.txt
```

Se o arquivo de arquivamento fosse colocado em /mybucket/Test/, a extração teria a seguinte aparência:

```
/mybucket/Test/Logs/April/a.txt
/mybucket/Test/Logs/April/b.txt
/mybucket/Test/Logs/April/c.txt
```

Comandos AWS CLI compatíveis

A seguir, você pode encontrar informações sobre como especificar o adaptador Amazon S3 ou o armazenamento compatível com Amazon S3 em dispositivos da Família Snow como o endpoint para os comandos AWS Command Line Interface aplicáveis (AWS CLI). Você também pode encontrar a lista de comandos AWS CLI do Amazon S3 que são compatíveis com a transferência de dados para o dispositivo AWS Snowball Edge com o adaptador ou armazenamento compatível com o Amazon S3 em dispositivos da Família Snow.

> **Note**
>
> Para obter informações sobre como instalar e configurar o AWS CLI, incluindo especificar em quais regiões você deseja fazer chamadas à AWS CLI, consulte o Manual do usuário do AWS Command Line Interface.

Atualmente, os dispositivos Snowball Edge oferecem suporte somente às versões 1.16.14 e anteriores do AWS CLI ao usar o adaptador do Amazon S3. Consulte Versão do Snowball Edge Client. Se você estiver usando armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, pode usar a versão mais recente do AWS CLI. Para baixar e usar a versão mais recente, consulte o Manual do usuário do AWS Command Line Interface.

> **Note**
>
> Instale a versão 2.6.5+ ou 3.4+ do Python antes de instalar a versão 1.16.14 da AWS CLI.

Comandos AWS CLI compatíveis com o Amazon S3

Veja a seguir uma descrição do subconjunto de comandos AWS CLI e opções para o Amazon S3 que são compatíveis com dispositivos AWS Snowball Edge. Se um comando ou opção não estiver listado, não é compatível. É possível declarar algumas opções não compatíveis, como `--sse` ou `--storage-class`, juntamente com um comando. No entanto, elas são ignoradas e não têm impacto sobre a forma como os dados são importados.

- cp: copia um arquivo ou objeto para ou do dispositivo AWS Snowball Edge. Veja a seguir as opções de comando:
  - `--dryrun` (booleano): as operações que seriam executadas utilizando o comando especificado são exibidas sem serem executadas.
  - `--quiet` (booleano): operações executadas pelo comando especificado não são exibidas.
  - `--include` (string): não excluir arquivos ou objetos no comando que corresponda ao padrão especificado. Para obter detalhes, consulte Uso de filtros de exclusão e inclusão na Referência de comando do AWS CLI.
  - `--exclude` (string): excluir todos os arquivos ou objetos do comando que corresponda ao padrão especificado.
  - `--follow-symlinks | --no-follow-symlinks` (booleano): links simbólicos (symlinks) são seguidos apenas ao carregar no Amazon S3 a partir do sistema local de arquivos. O Amazon S3 não é compatível com links simbólicos, portanto, o conteúdo do link alvo é carregado com o nome do link. Quando nenhuma das opções é especificada, o padrão é seguir symlinks.
  - `--only-show-errors` (booleano): são exibidos apenas erros e avisos. Todas as outras saídas são suprimidas.
  - `--recursive` (booleano): o comando é executado em todos os arquivos ou objetos no diretório ou prefixo especificado.
  - `--page-size` (inteiro): o número de resultados a ser retornado em cada resposta a uma operação em lista. O valor padrão é 1000 (o valor máximo permitido). A utilização de um valor menor pode ajudar se uma operação expirar.

  - `--metadata` (mapear): um mapa de metadados a ser armazenado com os objetos no Amazon S3. Esse mapa é aplicado a cada objeto que faz parte desta solicitação. Em uma sincronização, essa funcionalidade significa que os arquivos que não foram alterados não receberão os novos metadados. Ao copiar entre dois locais do Amazon S3, o argumento `metadata-directive` é padronizado como `REPLACE`, exceto se especificado de outra forma.
- ls: lista objetos no dispositivo AWS Snowball Edge. Veja a seguir as opções de comando:
  - `--human-readable` (booleano): tamanhos de arquivos são exibidos em formato legível.
  - `--summarize` (booleano): a informação de resumo é exibida. Esta informação é o número de objetos e seu tamanho total.
  - `--recursive` (booleano): o comando é executado em todos os arquivos ou objetos no diretório ou prefixo especificado.
  - `--page-size` (inteiro): o número de resultados a ser retornado em cada resposta a uma operação em lista. O valor padrão é 1000 (o valor máximo permitido). A utilização de um valor menor pode ajudar se uma operação expirar.
- rm: exclui um objeto no dispositivo AWS Snowball Edge. Veja a seguir as opções de comando:
  - `--dryrun` (booleano): as operações que seriam executadas utilizando o comando especificado são exibidas sem serem executadas.
  - `--include` (string): não excluir arquivos ou objetos no comando que corresponda ao padrão especificado. Para obter detalhes, consulte Uso de filtros de exclusão e inclusão na Referência de comando do AWS CLI.
  - `--exclude` (string): excluir todos os arquivos ou objetos do comando que corresponda ao padrão especificado.
  - `--recursive` (booleano): o comando é executado em todos os arquivos ou objetos no diretório ou prefixo especificado.
  - `--page-size` (inteiro): o número de resultados a ser retornado em cada resposta a uma operação em lista. O valor padrão é 1000 (o valor máximo permitido). A utilização de um valor menor pode ajudar se uma operação expirar.
  - `--only-show-errors` (booleano): são exibidos apenas erros e avisos. Todas as outras saídas são suprimidas.
  - `--quiet` (booleano): operações executadas pelo comando especificado não são exibidas.
- sync: sincroniza diretórios e prefixos. Esse comando copia os arquivos novos e atualizados a partir do diretório de origem para o destino. Este comando cria diretórios no destino apenas se elas contêm um ou mais arquivos.

> **Important**
>
> A sincronização de um diretório para outro diretório no mesmo Snowball Edge não tem suporte.
> A sincronização de um dispositivo AWS Snowball para outro dispositivo AWS Snowball não é compatível.
> Você só pode usar essa opção para sincronizar o conteúdo entre o armazenamento de dados on-premises e um Snowball Edge.

- `--dryrun` (booleano): as operações que seriam executadas utilizando o comando especificado são exibidas sem serem executadas.
- `--quiet` (booleano): operações executadas pelo comando especificado não são exibidas.
- `--include` (string): não excluir arquivos ou objetos no comando que corresponda ao padrão especificado. Para obter detalhes, consulte Uso de filtros de exclusão e inclusão na Referência de comando do AWS CLI.
- `--exclude` (string): excluir todos os arquivos ou objetos do comando que corresponda ao padrão especificado.
- `--follow-symlinks` ou `--no-follow-symlinks` (booleano): links simbólicos (symlinks) são seguidos apenas ao carregar no Amazon S3 a partir do sistema local de arquivos. O Amazon S3 não é compatível com links simbólicos, portanto, o conteúdo do link alvo é carregado com o nome do link. Quando nenhuma das opções é especificada, o padrão é seguir symlinks.
- `--only-show-errors` (booleano): são exibidos apenas erros e avisos. Todas as outras saídas são suprimidas.
- `--no-progress` (booleano): o progresso de transferência de arquivos não é exibido. Essa opção só é aplicada quando as opções `--quiet` e `--only-show-errors` não são fornecidas.
- `--page-size` (inteiro): o número de resultados a ser retornado em cada resposta a uma operação em lista. O valor padrão é 1000 (o valor máximo permitido). A utilização de um valor menor pode ajudar se uma operação expirar.
- `--metadata` (mapear): um mapa de metadados a ser armazenado com os objetos no Amazon S3. Esse mapa é aplicado a cada objeto que faz parte desta solicitação. Em uma sincronização, essa funcionalidade significa que os arquivos que não foram alterados não receberão os novos

metadados. Ao copiar entre dois locais do Amazon S3, o argumento `metadata-directive` é padronizado como `REPLACE`, exceto se especificado de outra forma.

> **Important**
>
> A sincronização de um diretório para outro diretório no mesmo Snowball Edge não tem suporte.
> A sincronização de um dispositivo AWS Snowball para outro dispositivo AWS Snowball não é compatível.
> Você só pode usar essa opção para sincronizar o conteúdo entre o armazenamento de dados on-premises e um Snowball Edge.

- `--size-only` (booleano): com essa opção, o tamanho de cada chave é o único critério usado para decidir se fazer a sincronização da origem para o destino.
- `--exact-timestamps` (booleano): durante a sincronização do Amazon S3 para um armazenamento local, os itens locais do mesmo tamanho são ignorados apenas quando as marcas de data/hora coincidirem exatamente. O comportamento padrão é ignorar itens de mesmo tamanho, a menos que a versão local seja mais recente do que a versão do Amazon S3.
- `--delete` (booleano): arquivos que existem no destino, mas não na origem, são excluídos durante a sincronização.

Você pode trabalhar com arquivos ou pastas com espaços nos nomes, como `my photo.jpg` ou `My Documents`. No entanto, certifique-se de que você lida com os espaços corretamente nos comandos AWS CLI. Para obter mais informações, consulte Especificar valores de parâmetros para o AWS CLI no Guia do usuário do AWS Command Line Interface.

Ações de API REST compatíveis

Veja a seguir ações de API REST que você pode usar com o dispositivo AWS Snowball Edge e o Amazon S3.

Tópicos

- Ações de API REST compatíveis com o Snowball Edge
- Ações de API REST suportadas para o adaptador Amazon S3

Ações de API REST compatíveis com o Snowball Edge

HEAD Snowball Edge

Descrição

No momento, há apenas uma operação da API REST do Snowball Edge, que pode ser usada para retornar informações de status de um dispositivo específico. Essa operação retorna o status de um Snowball Edge. Esse status inclui informações que podem ser usadas pelo AWS Support para fins de solução de problemas.

Não é possível usar essa operação com os SDKs da AWS nem com o AWS CLI. Recomendamos que você use o `curl` ou um cliente HTTP. A solicitação não precisa ser assinada para essa operação.

Solicitação

No exemplo a seguir, o endereço IP para o Snowball Edge é *`192.0.2.0`*. Substitua esse valor pelo endereço IP de seu dispositivo real.

```
curl -X HEAD http://192.0.2.0:8080
```

Resposta

```
<Status xsi:schemaLocation="http://s3.amazonaws.com/doc/2006-03-01/" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <snowballIp>127.0.0.1</snowballIp>
    <snowballPort>8080</snowballPort>
    <snowballId>device-id</snowballId>
    <totalSpaceInBytes>499055067136</totalSpaceInBytes>
    <freeSpaceInBytes>108367699968</freeSpaceInBytes>
    <jobId>job-id</jobId>
    <snowballServerVersion>1.0.1</snowballServerVersion>
    <snowballServerBuild>DevBuild</snowballServerBuild>
    <snowballClientVersion>Version 1.0</snowballClientVersion>
    <snowballRoundTripLatencyInMillis>33</snowballRoundTripLatencyInMillis>
</Status>
```

Ações de API REST suportadas para o adaptador Amazon S3

Veja a seguir a lista de ações da API REST do Amazon S3 que são compatíveis para usar o adaptador do Amazon S3. A lista inclui links para informações sobre como as ações da API

funcionam com o Amazon S3. A lista também abrange as diferenças de comportamento entre a ação da API do Amazon S3 e o equivalente do dispositivo AWS Snowball Edge. Todas as respostas retornadas de um dispositivo AWS Snowball Edge declaram `Server` como `AWSSnowball`, como no exemplo a seguir.

```
HTTP/1.1 201 OK
x-amz-id-2: JuKZqmXuiwFeDQxhD7M8KtsKobSzWA1QEjLbTMTagkKdBX2z7Il/jGhDeJ3j6s80
x-amz-request-id: 32FE2CEB32F5EE25
Date: Fri, 08 2016 21:34:56 GMT
Server: AWSSnowball
```

As chamadas de API REST do Amazon S3 exigem assinatura do SigV4. Se você estiver usando a AWS CLI ou um AWS SDK para fazer essas chamadas da API, a assinatura do SigV4 será fornecida para você. Caso contrário, você precisará implementar sua própria solução de assinatura do SigV4. Para obter mais informações, consulte Autenticação de solicitações (AWS Signature Version 4) no Guia do usuário do Amazon Simple Storage Service.

- GET Bucket (listagem de objetos) versão 1: compatível. No entanto, nessa implementação da operação GET, o seguinte não é suportado:
  - Paginação
  - Marcadores
  - Delimitadores
  - A lista não é classificada quando é retornada.

  Há suporte apenas para a versão 1. Não há suporte a GET Bucket (listar objetos) versão 2.
- GET serviço
- Bucket do HEAD
- Objeto HEAD
- GET Object: é um DOWNLOAD de um objeto do bucket do S3 do dispositivo Snow.
- Objeto PUT: quando um objeto é carregado em um dispositivo AWS Snowball Edge usando PUT `Object`, uma ETag é gerada.

  O ETag é um hash do objeto. O ETag reflete as alterações apenas no conteúdo de um objeto, não em seus metadados. O ETag pode ou não ser um digest MD5 do objeto de dados. Para ter mais informações sobre ETags, consulte Cabeçalhos de respostas comuns na Referência da API do Amazon Simple Storage Service.

- Objeto DELETE
- Iniciar multipart upload: nesta implementação, iniciar uma solicitação de multipart upload para um objeto já no dispositivo AWS Snowball Edge, primeiro exclui esse objeto. Em seguida, ele copia em partes no dispositivo AWS Snowball Edge.
- Listar carregamentos fracionados
- Carregar parte
- Concluir carregamento fracionado
- Anular carregamento fracionado

> **Note**
>
> Qualquer ação da API REST do adaptador do Amazon S3 não listada aqui não é compatível. Se você usar uma ação da API REST incompatível com seu Snowball Edge, receberá uma mensagem de erro informando que a ação não é compatível.

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.

Você pode usar a interface NFS se o dispositivo Snowball Edge tiver sido configurado para incluí-la quando a tarefa de solicitar o dispositivo foi criada. Se o dispositivo não estiver configurado para incluir a interface NFS, use o adaptador S3 ou o armazenamento compatível com Amazon S3 nos dispositivos da família Snow para transferir dados. Para obter mais informações sobre o adaptador S3, consulteGerenciar o armazenamento do adaptador do Amazon S3. Para obter mais informações sobre o armazenamento compatível com o Amazon S3 em dispositivos da família Snow, consulte. Configure o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

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 Importação de trabalhos para o Amazon .

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.
- Você pode transferir até 40 milhões de arquivos usando um único dispositivo Snowball Edge. Se você precisar transferir mais de 40 milhões de arquivos em um único trabalho, agrupe os arquivos para reduzir o número de arquivos por cada transferência. Arquivos individuais podem ser de

qualquer tamanho, com um tamanho máximo de arquivo de 5 TB para dispositivos Snowball Edge com a interface NFS aprimorada ou a interface S3.

Você também pode configurar e gerenciar a interface NFS com uma AWS OpsHub ferramenta GUI. Para obter mais informações, consulte Gerenciando a interface NFS .

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.

2. 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).
3. 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
```

4. 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 runtime de borda da Internet das Coisas (IoT) de código aberto que ajuda você a criar, implantar e gerenciar aplicações 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 machine learning e filtrem e agreguem dados do dispositivo. Para obter mais informações sobre o AWS IoT Greengrass, consulte O que é o AWS IoT Greengrass? no Guia do desenvolvedor do AWS IoT Greengrass Version 2.

Ao usar AWS IoT Greengrass em seu dispositivo da Família Snow, 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 o AWS IoT Greengrass Version 2 em um dispositivo da Família Snow, verifique se o dispositivo está conectado à Internet. Após a instalação, a Internet não é necessária para que um dispositivo da Família Snow funcione com o AWS IoT Greengrass.

Para configurar uma instância compatível com EC2 para o AWS IoT Greengrass V2

1. Inicie a AMI do AWS IoT Greengrass validada com um endereço IP público e uma chave SSH:

   a. Usando o AWS CLI: run-instances.

   b. Uso do AWS OpsHub: Iniciar 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. Substitua *public-ip-address* 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 de `.pem` para o

formato PuTTY, consulte Converter a chave privada com PuTTYgen no Guia do usuário do Amazon EC2 para instâncias do Linux.

Instalação do 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 o 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 raiz permissão para executar o software AWS IoT Greengrass e modificar a permissão raiz 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. Execute o comando a seguir para baixar o software do 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
```

4. Use os comandos a seguir para fornecer credenciais para permitir a instalação do software AWS IoT Greengrass Core. 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 região da AWS, não do dispositivo da Família Snow.

5. Execute o comando a seguir para iniciar o software AWS IoT Greengrass Core. O comando cria os atributos da AWS para o software principal 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 região da AWS na qual encontrar ou criar atributos.
   - `MyGreengrassCore`: o nome da coisa da AWS IoT para seu dispositivo de núcleo do AWS IoT Greengrass.
   - `MyGreengrassCoreGroup`: o nome da coisa da AWS IoT para seu dispositivo de núcleo do AWS IoT Greengrass.

```
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 núcleo do AWS IoT Greengrass em execução no seu dispositivo da Família Snow para uso local.

Usando AWS Lambda com um AWS Snowball Edge

AWS Lambda com a tecnologia do AWS IoT Greengrass é um serviço de computação que permite executar código sem servidor (funções do Lambda) localmente em dispositivos Snowball Edge. Você pode usar o Lambda para invocar funções do Lambda em um dispositivo Snowball Edge com mensagens do Message Queuing Telemetry Transport (MQTT), executar código Python em funções do Lambda e usá-las para chamar endpoints de serviço público da AWS na nuvem. Para usar funções do Lambda com dispositivos do Snowball Edge, você deve criar seus trabalhos do Snowball Edge em uma região da Região da AWS compatível com AWS IoT Greengrass. Para obter uma lista de Regiões da AWS válidas, consulte AWS IoT Greengrass no Referência geral da AWS. O Lambda no Snowball Edge está disponível em regiões onde os dispositivos Lambda e Snowball Edge estão disponíveis.

> **Note**
>
> Se você alocar a recomendação mínima de 128 MB de memória para cada uma das funções, será possível ter até sete funções do Lambda em um único trabalho.

Tópicos

Antes de começar

Antes de criar uma função do Lambda em linguagem Python para executar no Snowball Edge, recomendamos que você se familiarize com os serviços, conceitos e tópicos relacionados a seguir.

Pré-requisitos para o AWS IoT Greengrass

O AWS IoT Greengrass é um software que estende os atributos da Nuvem AWS aos dispositivos locais. O AWS IoT Greengrass possibilita que os dispositivos locais coletem e analisem os dados que estão mais próximos da origem das informações, além de proporcionar uma comunicação segura entre eles nas redes locais. Mais especificamente, os desenvolvedores que usam o AWS

IoT Greengrass podem autorizar códigos sem servidor (funções do Lambda) na Nuvem AWS. Eles podem implantar esse código de forma conveniente em dispositivos para execução local de aplicativos.

Os seguintes conceitos do AWS IoT Greengrass são importantes de se compreender ao usar o AWS IoT Greengrass com um Snowball Edge:

- Requisitos do AWS IoT Greengrass: para obter uma lista completa de requisitos do AWS IoT Greengrass, consulte Requisitos no Guia do desenvolvedor do AWS IoT Greengrass Version 2.
- Núcleo do AWS IoT Greengrass: faça o download do software do núcleo do AWS IoT Greengrass e instale-o em uma instância do EC2 em execução no dispositivo. Consulte Uso de AWS IoT Greengrass em instâncias do Amazon EC2 neste guia.

  Para usar as funções do Lambda em um dispositivo Snowball Edge, você deve primeiro instalar o software do núcleo do AWS IoT Greengrass em uma instância do Amazon EC2 no dispositivo. As funções do Lambda que você planeja usar no dispositivo Snowball Edge devem ser criadas pela mesma conta que você usará para instalar o AWS IoT Greengrass no dispositivo Snowball Edge. Para obter informações sobre a instalação do AWS IoT Greengrass em seu dispositivo Snowball Edge, consulte Usando AWS IoT Greengrass para executar software pré-instalado em instâncias compatíveis com o Amazon EC2.
- Grupo do AWS IoT Greengrass: um dispositivo Snowball Edge faz parte de um grupo do AWS IoT Greengrass como o dispositivo principal do grupo. Para obter mais informações sobre grupos, consulte Grupos do AWS Greengrass IoT no Guia do desenvolvedor do AWS IoT Greengrass.
- MQTT: o AWS IoT Greengrass usa o protocolo MQTT leve e padrão do setor para se comunicar dentro de um grupo. Qualquer dispositivo ou software compatível com o MQTT em seu grupo do AWS IoT Greengrass pode invocar mensagens do MQTT. Essas mensagens podem invocar funções do Lambda, se você definir a mensagem MQTT relacionada para fazer isso.

Pré-requisitos para o AWS Lambda

O AWS Lambda é um serviço de computação que permite executar código sem o provisionamento ou gerenciamento de servidores. Os seguintes conceitos do Lambda são importantes de se compreender ao usar o Lambda com um Snowball Edge:

- Funções do Lambda: seu código personalizado, enviado e publicado no Lambda e usado em um Snowball Edge. Para obter mais informações, consulte Invocar funções do Lambda no Guia do desenvolvedor do AWS Lambda.

- Console do Lambda: o console no qual você faz o upload, atualiza e publica as funções do Lambda em linguagem Python para uso em um Snowball Edge. Para obter mais informações sobre o console do Lambda, consulte console do Lambda no Guia do desenvolvedor do AWS Lambda.
- Python: a linguagem de programação de alto nível usada para as funções do Lambda oferecidas pelo AWS IoT Greengrass em um Snowball Edge. O AWS IoT Greengrass é compatível com o Python versão 3.8x.

Implantar uma função do Lambda em um dispositivo Snowball Edge

Para executar uma função do Lambda em um dispositivo Snowball Edge em um grupo do AWS IoT Greengrass, importe a função como um componente. Para obter informações completas sobre a importação de uma função como componente usando o console do AWS IoT Greengrass, consulte Importar uma função do Lambda como componente (console) no Guia do desenvolvedor do AWS IoT Greengrass Version 2.

1. No console de AWS IoT, na página de componentes do Greengrass, escolha Criar componente.
2. Em Fonte do componente, escolha Importar função do Lambda. Em Função do Lambda, escolha o nome da função. Na versão da função do Lambda, escolha a versão da sua função.
3. Para inscrever a função em mensagens nas quais ela pode atuar, escolha Adicionar fonte do evento e escolha o evento. Em Tempo limite (segundos), forneça um período de tempo limite em segundos.
4. Em Fixado, escolha se deseja ou não fixar sua função.
5. Escolha Criar componente
6. Escolha Implantar.
7. Em Implantação, escolha Adicionar à implantação existente e, em seguida, escolha seu grupo do Greengrass. Escolha Próximo.
8. Em Componentes públicos, escolha estes componentes:
   - aws.greengrass.Cli
   - aws.greengrass.LambdaLauncher
   - aws.greengrass.LambdaManager
   - aws.greengrass.LambdaRuntimes
   - aws.greengrass.Nucleus

9. Escolha Implantar.

Usar instâncias de computação compatíveis com o Amazon EC2

Esta seção oferece uma visão geral do uso de instâncias de computação compatíveis com o Amazon EC2 em um dispositivo AWS Snowball Edge, incluindo informações conceituais, procedimentos e exemplos.

Tópicos

Visão geral

É possível executar instâncias de computação compatíveis com o Amazon EC2 hospedadas em um Snowball Edge com os tipos de instância `sbe1`, `sbe-c` e `sbe-g`. O tipo de instância `sbe1` funciona em dispositivos com a opção Snowball Edge otimizado para armazenamento. O tipo de instância `sbe-c` funciona em dispositivos com a opção Snowball Edge otimizado para computação. Os dois tipos de instância `sbe-c` e `sbe-g` funcionam em dispositivos com a opção Snowball Edge otimizado para computação com GPU. Para obter uma lista dos tipos de instâncias compatíveis, consulte Cotas para instâncias de computação em um dispositivo Snowball Edge.

Todos os três tipos de instância de computação compatíveis para uso em um dispositivo Snowball Edge são exclusivos para dispositivos Snowball Edge. Assim como seus equivalentes baseados em nuvem, essas instâncias exigem imagens de máquina da Amazon (AMIs) para iniciar. Selecione a AMI para ser a imagem base para uma instância na nuvem, antes de criar o trabalho do Snowball Edge.

Para usar uma instância de computação em um Snowball Edge, crie um trabalho para solicitar um dispositivo da família Snow e especificar suas AMIs. Para isso, use o Console de Gerenciamento da família AWS Snow, a AWS CLI ou um dos SDKs da AWS. Normalmente, há alguns pré-requisitos de manutenção que devem ser executados antes da criação do trabalho para usar as instâncias.

Depois que o dispositivo chega, você pode começar a gerenciar as AMIs e as instâncias. É possível gerenciar as instâncias de computação em um Snowball Edge por meio de um endpoint compatível com o Amazon EC2. Esse tipo de endpoint é aceito por muitos dos comandos da CLI compatíveis com o Amazon EC2 e ações dos SDKs da AWS. Não é possível usar o AWS Management Console no Snowball Edge para gerenciar as AMIs e instâncias de computação.

Ao terminar de usar o dispositivo, devolva-o para a AWS. Se o dispositivo tiver sido usado em um trabalho de importação, os dados transferidos usando o adaptador do Amazon S3 ou a interface NFS serão 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 Snowball não é compatível.
- Os dados nas instâncias de computação em execução em um Snowball Edge não são importados para a AWS.

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

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

Preços de instâncias de computação no Snowball Edge

Existem custos adicionais associados ao uso de instâncias de computação. Para obter mais informações, consulte Preços do AWS Snowball Edge.

Usar uma AMI compatível com o Amazon EC2 em dispositivos da Família Snow

Para usar uma Amazon Machine Image (AMI) em seu dispositivo AWS Snow Family, você deve primeiro adicioná-la ao dispositivo. É possível adicionar uma AMI das seguintes maneiras:

- Faça upload da AMI ao fazer o pedido do dispositivo.
- Adicione a AMI quando o dispositivo chegar ao local.

As instâncias de computação do Amazon EC2 que vêm com os dispositivos da Família Snow são lançadas com base nas AMIs do Amazon EC2 adicionadas ao dispositivo. As AMIs compatíveis com o Amazon EC2 são compatíveis com os sistemas operacionais Linux e Microsoft Windows.

Linux

Os seguintes sistemas operacionais Linux são compatíveis:

- Amazon Linux 2 para a Família Snow

  > **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, consulteDeterminando a versão da família Amazon Linux 2 AMI for Snow.

- CentOS 7 (x86_64): com atualizações HVM

- Ubuntu 16.04 LTS: Xenial (HVM)

> **Note**
>
> Ubuntu 16.04 LTS - As imagens Xenial (HVM) não são mais suportadas no AWS Marketplace, mas ainda têm suporte para uso em dispositivos Snowball Edge por meio do Amazon EC2 VM Import/Export e executadas localmente em AMIs.

- Ubuntu 20.04 LTS: Focal
- Ubuntu 22.04 LTS: Jammy

Como melhor prática de segurança, mantenha suas AMIs do Amazon Linux 2 nos dispositivos da família Snow up-to-date à medida que novas AMIs do Amazon Linux 2 forem lançadas. Consulte Atualizando suas AMIs do Amazon Linux 2 em dispositivos da Família Snow.

Windows

Os seguintes sistemas operacionais Windows são compatíveis:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Você pode adicionar AMIs do Windows ao seu dispositivo importando a imagem da máquina virtual (VM) do Windows para AWS usar o VM Import/Export. Também é possível importar a imagem para o dispositivo logo após a implantação dele no local. Para ter mais informações, consulte Adicionar uma AMI do Microsoft Windows.

> **Note**
>
> As AMIs do Windows originadas em não AWS podem ser adicionadas ao seu dispositivo. As AMIs importadas localmente devem estar no modo de inicialização do BIOS, pois o UEFI não é compatível.

A Família Snow é compatível com o modelo traga a sua própria licença (BYOL). Para ter mais informações, consulte Adicionar uma AMI do Microsoft Windows.

> **Note**
>
> 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.

Tópicos

Adicionar uma AMI ao fazer o pedido do dispositivo

Ao fazer o pedido do dispositivo, é possível adicionar AMIs ao dispositivo escolhendo-as na seção Computação usando instâncias do EC2 - opcional no Console de Gerenciamento da família AWS Snow. A opção Computação usando instâncias do EC2 - opcional indica todas as AMIs que podem ser carregadas no dispositivo. As AMIs se encaixam nas seguintes categorias:

- AMIs do AWS Marketplace — Essas são AMIs criadas a partir da lista de AMIs compatíveis. Para obter informações sobre como criar uma AMI a partir das AMIs compatíveis do AWS Marketplace, consulteAdicionando uma AMI de AWS Marketplace.
- AMIs carregadas usando o VM Import/Export: ao pedir o dispositivo, as AMIs que foram carregadas usando o VM Import/Export são listadas no console. Para obter mais informações, consulte Como importar uma VM como uma imagem usando o VM Import/Export no Guia do usuário de VM Import/Export. Para obter informações sobre ambientes de virtualização compatíveis, consulte VM Import/Export Requirements.

Adicionando uma AMI de AWS Marketplace

Você pode adicionar várias AMIs AWS Marketplace ao seu dispositivo da família Snow iniciando a AWS Marketplace instância, criando uma AMI a partir dela e configurando a AMI na mesma

região na qual você solicitará o dispositivo Snow. Em seguida, você pode optar por incluir a AMI no dispositivo ao criar um trabalho para solicitar o dispositivo. Ao escolher uma AMI no Marketplace, certifique-se de que ela tenha um código de produto e uma plataforma compatíveis.

Tópicos

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
   - Janelas bring-your-own-license

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
```

Example da saída do **`describe-images`** comando

```
{
    "Images": [
        {
            "CreationDate": "2024-02-12T23:24:45.705Z",
            "ImageId": "s.ami-02ba84cb87224e16e",
            "Public": false,
            "ProductCodes": [
                {
                    "ProductCodeId": "avyfzznywektkgl5qv5f57ska",
                    "ProductCodeType": "marketplace"
                }
            ],
            "State": "AVAILABLE",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/xvda",
                    "Ebs": {
                        "DeleteOnTermination": true,
                        "Iops": 0,
                        "SnapshotId": "s.snap-0efb49f2f726fde63",
                        "VolumeSize": 8,
                        "VolumeType": "sbp1"
                    }
                }
            ],
            "Description": "Snow Family Amazon Linux 2 AMI 2.0.20240131.0 x86_64
 HVM gp2",
            "EnaSupport": false,
            "Name": "amzn2-ami-snow-family-hvm-2.0.20240131.0-x86_64-gp2-
b7e7f8d2-1b9e-4774-a374-120e0cd85d5a",
            "RootDeviceName": "/dev/xvda"
        }
    ]
}
```

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 a AMI para o dispositivo da família Snow

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Execute uma nova instância de uma AMI compatível em AWS Marketplace.

   > **Note**
   >
   > Ao iniciar a instância, verifique se o tamanho do armazenamento atribuído à instância é adequado para o caso de uso. No console do Amazon EC2, isso é feito na etapa Adicionar armazenamento.

3. Instale e configure as aplicações que deseja executar no Snowball Edge e teste para verificar se funcionam conforme o esperado.

   > **Important**
   >
   > - Somente AMIs de volume único são compatíveis.
   > - O volume do EBS na AMI deve ter 10 TB ou menos. Recomendamos que você provisione o tamanho do volume do EBS necessário para os dados na AMI. Isso ajudará a diminuir o tempo necessário para exportar a AMI e carregá-la no dispositivo. É possível redimensionar ou adicionar mais volumes à instância após a implantação do dispositivo.
   > - O snapshot do EBS na AMI não deve ser criptografado.

4. Faça uma cópia do arquivo PEM ou PPK utilizado para o par de chaves SSH quando você criou essa instância. Salve esse arquivo no servidor que você planeja usar para se comunicar com o dispositivo Snowball Edge. Anote o caminho desse arquivo, pois ele será necessário ao usar o SSH para se conectar à instância compatível com EC2 no dispositivo.

> **Important**
>
> Se você não seguir esse procedimento, não poderá se conectar às instâncias com SSH ao receber o dispositivo Snowball Edge.

5. Salve a instância como uma AMI. Para obter mais informações, consulte o Guia do usuário do Amazon EC2 para instâncias Linux no Guia do usuário do Amazon EC2 para instâncias Linux.
6. Repita as etapas 1 a 4 para cada uma das instâncias às quais você deseja se conectar usando SSH. Assegure-se de fazer cópias de todos os pares de chaves SSH e acompanhar as AMIs às quais eles estão associados.
7. Agora, ao pedir o dispositivo, essas AMIs estão disponíveis para serem adicionadas a ele.

Adicionar uma AMI localmente

Quando o dispositivo chegar ao local, você poderá adicionar novas AMIs a ele. Para obter instruções, consulte Importando uma imagem de máquina virtual para um dispositivo da família Snow. Lembre-se de que, embora todas as VMs sejam aceitas, somente as AMIs compatíveis foram testadas quanto à funcionalidade completa.

> **Note**
>
> Ao usar o VM Import/Export para adicionar AMIs ao dispositivo ou importar uma VM após a implantação do dispositivo, será possível adicionar VMs que usam qualquer sistema operacional. No entanto, somente os sistemas operacionais compatíveis foram testados e validados nos dispositivos da Família Snow. Você é responsável por cumprir os termos e condições de qualquer sistema operacional ou software que esteja na imagem virtual importada para o dispositivo.
>
> > **Important**
> >
> > Para que AWS os serviços funcionem adequadamente em um Snowball Edge, você deve permitir as portas dos serviços. Para obter detalhes, consulte Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge.

Adicionar uma AMI do Microsoft Windows

Para máquinas virtuais (VMs) que usam um sistema operacional Windows compatível, você pode adicionar a AMI importando sua imagem de VM do Windows para AWS usar o VM Import/Export ou importando-a para seu dispositivo diretamente após a implantação em seu site.

Traga a sua própria licença (BYOL)

O Snowball Edge é compatível com a importação de AMIs do Microsoft Windows para o dispositivo com sua própria licença. Traga sua própria licença (BYOL) é o processo de trazer uma AMI que você possui com sua licença local. AWS AWS fornece opções de implantação compartilhadas e dedicadas para a opção BYOL.

Você pode adicionar sua imagem de VM do Windows ao seu dispositivo importando-a AWS usando o VM Import/Export ou importando-a para o seu dispositivo diretamente após a implantação no seu site. Você não pode adicionar AMIs do Windows que se originaram em. AWS Portanto, é necessário criar e importar a própria imagem de VM do Windows e trazer a sua própria licença se quiser usar a AMI no dispositivo da Família Snow. Para obter mais informações sobre o licenciamento do Windows e a opção BYOL, consulte Amazon Web Services e Microsoft: Perguntas frequentes.

Criar uma imagem de VM do Windows para importar para o dispositivo

Para criar uma imagem de VM do Windows, você precisa de um ambiente de virtualização, como VirtualBox, que seja compatível com os sistemas operacionais Windows e macOS. Ao criar uma VM para dispositivos Snow, recomendamos alocar pelo menos dois núcleos com 4 GB de RAM, no mínimo. Quando a VM estiver em execução, você deverá instalar o sistema operacional (Windows Server 2012, 2016 ou 2019). Para instalar os drivers necessários para o dispositivo da Família Snow, siga as instruções descritas nesta seção.

Para que uma AMI do Windows seja executada em um dispositivo Snow, você deve adicionar o VirtIO, o FLR, o NetVCM, o Vioinput, o Viorng, o Vioscsi, o Vioserial e os drivers. VioStor Você pode baixar um Microsoft Software Installer (virtio-win-guest-tools-installer) para instalar esses drivers em imagens do Windows a partir do virtio-win-pkg-scripts repositório em. GitHub

> **Note**
>
> Se você planeja importar a imagem da VM diretamente para o dispositivo Snow implantado, o arquivo de imagem da VM deve estar no formato RAW.

Como criar uma imagem do Windows

1. No computador com Microsoft Windows, selecione Iniciar e insira **`devmgmt.msc`** para abrir o Gerenciador de Dispositivos.
2. No menu principal, selecione Ações e, depois, Adicionar hardware herdado.
3. No assistente, selecione Próximo.
4. Selecione Instalar o hardware que eu seleciono manualmente em uma lista (avançado) e escolha Próximo.
5. Selecione Mostrar todos os dispositivos e Próximo.
6. Selecione Tenho disco, abra a lista Copiar arquivos do fabricante de e navegue até o arquivo ISO.
7. No arquivo ISO, acesse o diretório `Driver\W2K8R2\amd64` e localize o arquivo `.INF`.
8. Selecione o arquivo .INF, selecione Abrir e, depois, OK.
9. Ao ver o nome do driver, selecione Próximo e, depois, Próximo mais duas vezes. Em seguida, escolha Finish (Concluir).

   Um dispositivo será instalado usando o novo driver. O hardware real não existe, então você verá um ponto de exclamação amarelo que indica um problema no dispositivo. É necessário corrigir esse problema.

Como corrigir o problema de hardware

1. Abra o menu de contexto (com botão direito do mouse) do dispositivo que tem o ponto de exclamação.
2. Selecione Desinstalar, desmarque Excluir o software do driver para este dispositivo e selecione OK.

   O driver é instalado e estará tudo pronto para iniciar a AMI no dispositivo.

Importar uma imagem de VM para o dispositivo

Depois de preparar a imagem da VM, é possível usar uma das opções para importar a imagem para o dispositivo.

- Na nuvem usando o VM Import/Export — Quando você importa sua imagem de VM AWS e a registra como uma AMI, você pode adicioná-la ao seu dispositivo ao fazer um pedido no. Console

de Gerenciamento da família AWS Snow Para obter mais informações, consulte Como importar uma VM como uma imagem usando o VM Import/Export no Guia do usuário de VM Import/Export.

- Localmente em seu dispositivo que está implantado em seu site — Você pode importar sua imagem de VM diretamente para o seu dispositivo usando AWS OpsHub for Snow Family ou o AWS Command Line Interface ()AWS CLI.

  Para obter informações sobre o uso AWS OpsHub, consulte Como usar localmente instâncias computacionais compatíveis com o Amazon EC2.

  Para obter informações sobre como usar o AWS CLI, consulteImportando uma imagem de máquina virtual para um dispositivo da família Snow.

Exportação da AMI mais recente do Amazon Linux 2

Para atualizar suas AMIs do Amazon Linux 2 para a versão mais recente, primeiro exporte a imagem mais recente da VM do Amazon Linux 2 e, em seguida AWS Marketplace, importe essa imagem da VM para o dispositivo Snow.

1. Use o `ssm get-parameters` AWS CLI comando para encontrar o ID de imagem mais recente do Amazon Linux 2 AMI no AWS Marketplace.

   ```
   aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
   ```

   O comando retorna a ID de imagem mais recente da AMI. Por exemplo, `ami-0ccb473bada910e74`.

2. Exporte a imagem mais recente do Amazon Linux 2. Consulte Exportação de uma VM diretamente de uma imagem de máquina da Amazon (AMI) no Guia do usuário do Amazon EC2 para instâncias Linux. Use o ID de imagem mais recente do Amazon Linux 2 AMI como o valor do `image-id` parâmetro do `ec2 export-image` comando.
3. Importe a imagem da VM para o dispositivo Snow usando o AWS CLI ou AWS OpsHub.

   - Para obter informações sobre o uso AWS CLI, consulteImportando uma imagem de máquina virtual para um dispositivo da família Snow.

- Para obter informações sobre o uso AWS OpsHub, consulteImportar uma imagem para o seu dispositivo como uma AMI compatível com Amazon EC2 .

Importando uma imagem de máquina virtual para um dispositivo da família Snow

Você pode usar o AWS CLI e o serviço VM Import/Export para importar uma imagem de máquina virtual (VM) para o dispositivo da família Snow como uma Amazon Machine Image (AMI). Depois de importar uma imagem de VM, registre a imagem como uma AMI e inicie-a como uma instância compatível com Amazon EC2.

Você pode adicionar AMIs do Amazon EC2 ao dispositivo ao criar um trabalho para solicitar um dispositivo da família Snow. Use esse procedimento depois de receber o dispositivo Snow Family. Para ter mais informações, consulte Etapa 2: escolher as opções de computação e armazenamento.

Você também pode usar AWS OpsHub para carregar o arquivo de imagem da VM. Para obter mais informações, consulte Importar uma imagem em seu dispositivo como uma AMI compatível com Amazon EC2 neste guia.

Tópicos

- Etapa 1: Prepare a imagem da VM e faça o upload para o dispositivo da família Snow
- Etapa 2: configurar as permissões necessárias
- Etapa 3: importar a imagem da VM como um instantâneo no dispositivo
- Etapa 4: registrar o snapshot como uma AMI
- Etapa 5: Iniciar uma instância usando a AMI
- Ações adicionais da AMI

Etapa 1: Prepare a imagem da VM e faça o upload para o dispositivo da família Snow

Prepare a imagem da VM exportando uma imagem da VM de uma AMI ou instância do Amazon EC2 usando o VM Import/Export ou gerando a imagem da VM localmente Nuvem AWS usando a plataforma de virtualização de sua escolha.

Para exportar uma instância do Amazon EC2 como uma imagem de VM usando o VM Import/Export, consulte Exportar uma instância como uma VM usando o VM Import/Export no Guia do usuário do

VM Import/Export. Para exportar uma AMI do Amazon EC2 como uma imagem de VM usando o VM Import/Export, consulte Exportar uma VM diretamente de uma Amazon Machine Image (AMI) no Guia do usuário do VM Import/Export.

Se estiver gerando uma imagem de VM do seu ambiente local, certifique-se de que a imagem esteja configurada para uso como AMI no dispositivo da família Snow. Talvez seja necessário configurar os itens a seguir, dependendo do seu ambiente.

- Configure e atualize o sistema operacional.
- Defina um nome de host.
- Certifique-se de que o protocolo de horário de rede (NTP) esteja configurado.
- Inclua chaves públicas SSH, se necessário. Faça cópias locais dos pares de chaves. Para obter mais informações, consulte Como usar o SSH para se conectar às suas instâncias de computação em um Snowball Edge.
- Instale e configure qualquer software que você usará no dispositivo Snow Family.

> **Note**
>
> Esteja ciente das seguintes limitações ao preparar um instantâneo de disco para um dispositivo da família Snow.
>
> - No momento, os dispositivos da Família Snow são compatíveis apenas com a importação de snapshots no formato de imagem RAW.
> - No momento, os dispositivos da Família Snow são compatíveis apenas com a importação de snapshots de 1 GB a 1 TB.

Fazer upload de uma imagem de VM para um bucket Amazon S3 no dispositivo da família Snow

Depois de preparar uma imagem de VM, carregue-a em um bucket S3 no dispositivo ou cluster da família Snow. Você pode usar o adaptador S3 ou o armazenamento compatível com Amazon S3 nos dispositivos da família Snow para fazer o upload do snapshot.

Para carregar a imagem da máquina virtual usando o adaptador S3

- Use o `cp` comando para copiar o arquivo de imagem da VM em um bucket no dispositivo.

```
aws s3 cp image-path s3://S3-bucket-name --endpoint http://S3-object-API-
endpoint:443 --profile profile-name
```

Para obter mais informações, consulte AWS CLIComandos compatíveis neste guia.

Para carregar a imagem da VM usando armazenamento compatível com Amazon S3 em dispositivos da família Snow

- Use o `put-object` comando para copiar o arquivo de snapshot em um bucket no dispositivo.

```
aws s3api put-object --bucket bucket-name --key path-to-snapshot-file --
body snapshot-file --profile your-profile --endpoint-url s3api-endpoint-ip
```

Para obter mais informações, consulte Trabalho com objetos do S3 em um dispositivo Snowball Edge.

Etapa 2: configurar as permissões necessárias

Para que a importação seja bem-sucedida, você deve configurar permissões para o VM Import/Export no dispositivo da família Snow, no Amazon EC2 e no usuário.

> **Note**
>
> Os perfis de serviço e as políticas de serviço que concedem essas permissões estão localizados no dispositivo da Família Snow.

Permissões necessárias para o VM Import/Export

Antes de iniciar o processo de importação, você deve criar uma função do IAM com uma política de confiança que permita que o VM Import/Export no dispositivo da família Snow assuma a função. Permissões adicionais são concedidas à função para permitir que o VM Import/Export no dispositivo acesse a imagem armazenada no bucket do S3 no dispositivo.

Criar um arquivo json de política de confiança

Veja a seguir um exemplo de política de confiança que deve ser anexada ao perfil para que o VM Import/Export possa acessar o snapshot que precisa ser importado do bucket do S3.

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

Criar um perfil com o arquivo json da política de confiança

O nome do perfil pode ser vmimport. É possível alterá-lo usando a opção --role-name no comando:

```
aws iam create-role --role-name role-name --assume-role-policy-document file:///trust-policy-json-path --profile profile-name --endpoint http://snowball-ip:6078 --region
 snow
```

Veja um exemplo de saída do comando `create-role`.

```
{
   "Role":{
      "AssumeRolePolicyDocument":{
         "Version":"2012-10-17",
         "Statement":[
            {
               "Action":"sts:AssumeRole",
               "Effect":"Allow",
               "Principal":{
                  "Service":"vmie.amazonaws.com"
               }
            }
         ]
      },
      "MaxSessionDuration":3600,
      "RoleId":"AROACEMGEZDGNBVGY3TQOJQGEZAAAABQBB6NSGNAAAABPSVLTREPY3FPAFOLKJ3",
      "CreateDate":"2022-04-19T22:17:19.823Z",
```

```
      "RoleName":"vmimport",
      "Path":"/",
      "Arn":"arn:aws:iam::123456789012:role/vmimport"
   }
}
```

Criar uma política para a função

O exemplo de política a seguir tem as permissões mínimas necessárias para acessar o Amazon S3. Altere o nome do bucket do Amazon S3 para aquele que tem as imagens. Em um dispositivo Snowball Edge independente, altere *snow-id* para o ID de trabalho. Em um cluster de dispositivos, altere *snow-id* para o ID do cluster. Também é possível usar prefixos para restringir ainda mais o local de onde o VM Import/Export pode importar snapshots. Crie um arquivo json de política como este.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:GetMetadata"
         ],
         "Resource":[
            "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-bucket-
name",
            "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-bucket-
name/*"
            ]
      }
   ]
}
```

Crie uma política com o arquivo de política:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-
file-path --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Veja a seguir um exemplo de saída do comando create-policy.

```
{
   "Policy":{
      "PolicyName":"vmimport-resource-policy",
      "PolicyId":"ANPACEMGEZDGNBVGY3TQOJQGEZAAAABOOEE3IIHAAAABWZJPI2VW4UUTFEDBC2R",
      "Arn":"arn:aws:iam::123456789012:policy/vmimport-resource-policy",
      "Path":"/",
      "DefaultVersionId":"v1",
      "AttachmentCount":0,
      "IsAttachable":true,
      "CreateDate":"2020-07-25T23:27:35.690000+00:00",
      "UpdateDate":"2020-07-25T23:27:35.690000+00:00"
   }
}
```

Anexar a política ao perfil

Anexe uma política ao perfil anterior e conceda permissões para acessar os recursos necessários. Isso permite que o serviço local VM Import/Export baixe o snapshot do Amazon S3 no dispositivo.

```
aws iam attach-role-policy --role-name role-name --policy-arn
 arn:aws:iam::123456789012:policy/policy-name --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Permissões exigidas pelo chamador

Além do perfil a ser assumido pelo Snowball Edge VM Import/Export, também é necessário garantir que o usuário tenha as permissões que autorizem a transmissão da função para o VMIE. Se você usar o usuário raiz padrão para realizar a importação, o qual já tem todas as permissões necessárias, poderá ignorar esta etapa e ir para a 3.

Anexe as duas permissões do IAM a seguir ao usuário que está fazendo a importação.

- `pass-role`
- `get-role`

Criar uma política para a função

Veja um exemplo de política que permite ao usuário realizar as ações `get-role` e `pass-role` para o perfil do IAM.

```
{
   "Version":"2012-10-17",
   "Statement":[
        {
            "Effect":"Allow",
            "Action": "iam:GetRole",
            "Resource":"*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "importexport.amazonaws.com"
                }
            }
        }
   ]
}
```

Crie uma política com o arquivo de política:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-file-path --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Veja a seguir um exemplo de saída do comando create-policy.

```
{
   "Policy":{
      "PolicyName":"caller-policy",
      "PolicyId":"ANPACEMGEZDGNBVGY3TQOJQGEZAAAABOOOTUOE3AAAAAAPPBEUM7Q7ARPUE53C6R",
      "Arn":"arn:aws:iam::123456789012:policy/caller-policy",
      "Path":"/",
      "DefaultVersionId":"v1",
      "AttachmentCount":0,
      "IsAttachable":true,
      "CreateDate":"2020-07-30T00:58:25.309000+00:00",
      "UpdateDate":"2020-07-30T00:58:25.309000+00:00"
   }
}
```

Depois que a política for gerada, anexe a política aos usuários do IAM que chamarão a operação de API ou a CLI do Amazon EC2 para importar o snapshot.

```
aws iam attach-user-policy --user-name your-user-name --policy-arn
 arn:aws:iam::123456789012:policy/policy-name --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Permissões necessárias para chamar as APIs do Amazon EC2 em seu dispositivo

Para importar um snapshot, o usuário do IAM precisa ter as permissões `ec2:ImportSnapshot`. Se não for necessário restringir o acesso ao usuário, você poderá usar as permissões `ec2:*` para conceder acesso total ao Amazon EC2. Veja as permissões que podem ser concedidas ou restringidas para o Amazon EC2 no dispositivo. Crie um arquivo de política com o conteúdo mostrado:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ec2:ImportSnapshot",
            "ec2:DescribeImportSnapshotTasks",
            "ec2:CancelImportTask",
            "ec2:DescribeSnapshots",
            "ec2:DeleteSnapshot",
            "ec2:RegisterImage",
            "ec2:DescribeImages",
            "ec2:DeregisterImage"
         ],
         "Resource":"*"
      }
   ]
}
```

Crie uma política com o arquivo de política:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-
file-path --profile profile-name --endpoint http://snowball-ip:6078 --region snow
```

Veja a seguir um exemplo de saída do comando create-policy.

```
{
    "Policy":
        {
            "PolicyName": "ec2-import.json",
            "PolicyId":
 "ANPACEMGEZDGNBVGY3TQOJQGEZAAAABQBGPDQC5AAAAATYN62UNBFYTF5WVCSCZS",
            "Arn": "arn:aws:iam::123456789012:policy/ec2-import.json",
            "Path": "/",
            "DefaultVersionId": "v1",
            "AttachmentCount": 0,
            "IsAttachable": true,
            "CreateDate": "2022-04-21T16:25:53.504000+00:00",
            "UpdateDate": "2022-04-21T16:25:53.504000+00:00"
        }
}
```

Depois que a política for gerada, anexe a política aos usuários do IAM que chamarão a operação de API ou a CLI do Amazon EC2 para importar o snapshot.

```
aws iam attach-user-policy --user-name your-user-name --policy-arn
 arn:aws:iam::123456789012:policy/policy-name --profile profile-name --endpoint
 http://snowball-ip:6078 --region snow
```

Etapa 3: importar a imagem da VM como um instantâneo no dispositivo

A próxima etapa é importar a imagem da VM como um instantâneo no dispositivo. O valor do `S3Bucket` parâmetro é o nome do bucket que contém a imagem da VM. O valor do `S3Key` parâmetro é o caminho para o arquivo de imagem da VM nesse bucket.

```
aws ec2 import-snapshot --disk-container "Format=RAW,UserBucket={S3Bucket=bucket-
name,S3Key=image-file}" --profile profile-name --endpoint http://snowball-ip:8008 --
region snow
```

Para obter mais informações, consulte import-snapshot na Referência de Comandos. AWS CLI

Esse comando não é compatível com as opções a seguir.

- [--client-data `value`]
- [--client-token `value`]
- [--dry-run]

- [--no-dry-run]
- [--encrypted]
- [--no-encrypted]
- [--kms-key-id `value`]
- [--tag-specifications `value`]

Example saída do **`import-snapshot`** comando

```
{
   "ImportTaskId":"s.import-snap-1234567890abc",
   "SnapshotTaskDetail":{
      "DiskImageSize":2.0,
      "Encrypted":false,
      "Format":"RAW",
      "Progress":"3",
      "Status":"active",
      "StatusMessage":"pending",
      "UserBucket":{
         "S3Bucket":"bucket",
         "S3Key":"vmimport/image01"
      }
   }
}
```

Note

Atualmente, os dispositivos da família Snow permitem que apenas um trabalho de importação ativo seja executado por vez, por dispositivo. Para iniciar uma nova tarefa de importação, aguarde a conclusão da tarefa atual ou selecione outro nó disponível em um cluster. Também é possível optar por cancelar a importação atual, se desejar. Para evitar atrasos, não reinicie o dispositivo Snow Family enquanto a importação estiver em andamento. Se você reinicializar o dispositivo, a importação falhará e o andamento será excluído quando o dispositivo estiver acessível. Para conferir o status de importação do snapshot, use o seguinte comando:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --endpoint http://snowball-ip:8008 --region snow
```

Etapa 4: registrar o snapshot como uma AMI

Quando a importação do snapshot para o dispositivo for bem-sucedida, você poderá registrá-lo com o comando `register-image`.

> **Note**
>
> Você só pode registrar uma AMI quando todos os snapshots estiverem disponíveis.

Para obter mais informações, consulte register-image na Referência de AWS CLI Comandos.

Example do **`register-image`** comando

```
aws ec2 register-image \
--name ami-01 \
--description my-ami-01 \
--block-device-mappings "[{\"DeviceName\": \"/dev/sda1\",\"Ebs\":{\"Encrypted\":false,
\"DeleteOnTermination\":true,\"SnapshotId\":\"snapshot-id\",\"VolumeSize\":30}}]" \
--root-device-name /dev/sda1 \
--profile profile-name \
--endpoint http://snowball-ip:8008 \
--region snow
```

Veja a seguir um exemplo de mapeamento de dispositivos de blocos JSON. Para obter mais informações, consulte o block-device-mapping parâmetro de register-image na Referência de AWS CLI Comandos.

```
[
    {
        "DeviceName": "/dev/sda",
        "Ebs":
            {
                "Encrypted": false,
                "DeleteOnTermination": true,
                "SnapshotId": "snapshot-id",
                "VolumeSize": 30
            }
    }
]
```

Example do **`register-image`** comando

```
{
    "ImageId": "s.ami-8de47d2e397937318"
 }
```

Etapa 5: Iniciar uma instância usando a AMI

Para iniciar uma instância, consulte run-instances na Referência de AWS CLI comandos.

O valor do `image-id` parâmetro é o valor do `ImageId` nome como saída do `register-image` comando.

```
aws ec2 run-instances --image-id image-id --instance-type instance-type --
profile profile-name --endpoint http://snowball-ip:8008 --region snow
```

```
{
   "Instances":[
      {
         "SourceDestCheck":false,
         "CpuOptions":{
            "CoreCount":1,
            "ThreadsPerCore":2
         },
         "InstanceId":"s.i-12345a73123456d1",
         "EnaSupport":false,
         "ImageId":"s.ami-1234567890abcdefg",
         "State":{
            "Code":0,
            "Name":"pending"
         },
         "EbsOptimized":false,
         "SecurityGroups":[
            {
               "GroupName":"default",
               "GroupId":"s.sg-1234567890abc"
            }
         ],
         "RootDeviceName":"/dev/sda1",
         "AmiLaunchIndex":0,
         "InstanceType":"sbe-c.large"
      }
```

```
   ],
   "ReservationId":"s.r-1234567890abc"
}
```

> **Note**
>
> Você também pode usar AWS OpsHub para iniciar a instância. Para obter mais informações, consulte Lançamento de uma instância compatível com Amazon EC2 neste guia.

Ações adicionais da AMI

Você pode usar AWS CLI comandos adicionais para monitorar o status de importação de instantâneos, obter detalhes sobre instantâneos que foram importados, cancelar a importação de um instantâneo e excluir ou cancelar o registro de instantâneos após a importação.

Monitorando o status de importação de instantâneos

Para ver o estado atual do andamento da importação, é possível executar o comando `describe-import-snapshot-tasks` do Amazon EC2. Esse comando suporta paginação e filtragem no. `task-state`

Example do **`describe-import-snapshot-tasks`** comando

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

Example da saída **`describe-import-snapshot-tasks`** do comando

```
{
        "ImportSnapshotTasks": [
            {
                "ImportTaskId": "s.import-snap-8f6bfd7fc9ead9aca",
                "SnapshotTaskDetail": {
                    "Description": "Created by AWS-Snowball-VMImport service for
 s.import-snap-8f6bfd7fc9ead9aca",
                    "DiskImageSize": 8.0,
                    "Encrypted": false,
                    "Format": "RAW",
                    "Progress": "3",
```

```
                    "SnapshotId": "s.snap-848a22d7518ad442b",
                    "Status": "active",
                    "StatusMessage": "pending",
                    "UserBucket": {
                        "S3Bucket": "bucket1",
                        "S3Key": "image1"
                    }
                }
            }
        ]
}
```

> **Note**
>
> Esse comando mostra somente a saída de tarefas que foram concluídas com êxito ou que foram marcadas como excluídas nos últimos 7 dias. A filtragem é compatível apenas com `Name=task-state` e `Values=active | deleting | deleted | completed`.

Esse comando não oferece suporte aos seguintes parâmetros.

- [--dry-run]
- [--no-dry-run]

Cancelamento de uma tarefa de importação

Para cancelar uma tarefa de importação, execute o comando `cancel-import-task`.

Example do **`cancel-import-task`** comando

```
aws ec2 cancel-import-task --import-task-id import-task-id --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

Example da saída **`cancel-import-task`** do comando

```
{
        "ImportTaskId": "s.import-snap-8234ef2a01cc3b0c6",
        "PreviousState": "active",
        "State": "deleting"
}
```

> **Note**
>
> Somente tarefas não concluídas podem ser canceladas.

Esse comando não oferece suporte aos seguintes parâmetros.

- [--dry-run]
- [--no-dry-run]

Descrição de snapshots

Após a importação de um snapshot, é possível usar esse comando para descrevê-lo. Para filtrar os snapshots, é possível transmiti-los em `snapshot-ids` com o ID do snapshot da resposta da tarefa de importação anterior. Esse comando suporta paginação e filtro em `volume-id`status, e. `start-time`

Example de **`describe-snapshots`** comando

```
aws ec2 describe-snapshots --snapshot-ids snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

Example da saída **`describe-snapshots`** do comando

```
{
    "Snapshots": [
        {
            "Description": "Created by AWS-Snowball-VMImport service for s.import-
snap-8f6bfd7fc9ead9aca",
            "Encrypted": false,
            "OwnerId": "123456789012",
            "SnapshotId": "s.snap-848a22d7518ad442b",
            "StartTime": "2020-07-30T04:31:05.032000+00:00",
            "State": "completed",
            "VolumeSize": 8
        }
    ]
 }
```

Esse comando não oferece suporte aos seguintes parâmetros.

- [--restorable-by-user-ids `value`]
- [--dry-run]
- [--no-dry-run]

Excluindo um instantâneo de um dispositivo da família Snow

Para remover snapshots desnecessários, é possível usar o comando `delete-snapshot`.

Example do **`delete-snapshot`** comando

```
aws ec2 delete-snapshot --snapshot-id snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

> **Note**
>
> O Snowball Edge não é compatível com a exclusão de snapshots que estejam em estado PENDENTE ou que tenham sido designados como dispositivo raiz para uma AMI.

Esse comando não oferece suporte aos seguintes parâmetros.

- [--dry-run]
- [--no-dry-run]

Cancelar o registro da AMI

Para cancelar o registro de AMIs desnecessárias, é possível executar o comando `deregister-image`. O cancelamento do registro de uma AMI no estado Pendente não é aceito no momento.

Example do **`deregister-image`** comando

```
aws ec2 deregister-image --image-id image-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

Esse comando não oferece suporte aos seguintes parâmetros.

- [--dry-run]

- [--no-dry-run]

Usar a AWS CLI e as operações da API no Snowball Edge

Ao usar a AWS Command Line Interface (AWS CLI) ou as operações da API para emitir comandos do IAM, do Amazon S3 e do Amazon EC2 no Snowball Edge, é necessário especificar a `region` como “`snow`”. Para isso, use `AWS configure` ou no próprio comando, como nos exemplos a seguir.

```
aws configure --profile ProfileName
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Ou

```
aws s3 ls --profile ProfileName --endpoint http://192.0.2.0:8080 --region snow
```

Cotas para instâncias de computação em um dispositivo Snowball Edge

Veja as cotas de armazenamento e as limitações de recursos de computação compartilhados em um dispositivo AWS Snowball Edge.

Cotas de armazenamento

O armazenamento disponível para recursos de computação é um recurso separado do armazenamento dedicado do Amazon S3 em um dispositivo Snowball Edge. As cotas de armazenamento são as seguintes:

- Cotas de armazenamento para a opção Snowball Edge otimizado para armazenamento: o total de armazenamento disponível para o Amazon S3 é entre 60 TB e 80 TB, dependendo de você estar usando ou não instâncias de computação no dispositivo. Se estiver usando instâncias de computação, o armazenamento dedicado total disponível para instâncias de computação `sbe1` para a opção Snowball Edge otimizado para armazenamento será de 1.000 GB.
- Cotas de armazenamento para as opções GPU e otimizada para computação do Snowball Edge: o total de armazenamento dedicado disponível para as instâncias `sbe-c` e `sbe-g` é 7,68 TB. O total de armazenamento disponível restante é de 42 TB.

As tabelas a seguir descrevem os recursos de computação disponíveis para dispositivos Snowball Edge.

Atributo	Limitação
Número de AMIs em uma única opção Snowball Edge otimizado para armazenamento	10
Número de AMIs em uma única opção Snowball Edge otimizado para computação	20
Número de AMIs em uma única opção Snowball Edge otimizado para computação com GPU	20
Número de volumes por instância	10
Instâncias em execução (ou interrompidas) simultaneamente	Varia de acordo com os recursos disponíveis

Tipo de instância	Núcleos de vCPU	Memória (GiB)	GPUs	Opção de dispositivo compatível
`sbe1.small`	1	1	0	otimizado para armazenamento
`sbe1.medium`	1	2	0	otimizado para armazenamento
`sbe1.large`	2	4	0	otimizado para armazenamento
`sbe1.xlarge`	4	8	0	otimizado para armazenamento
`sbe1.2xlarge`	8	16	0	otimizado para armazenamento

Tipo de instância	Núcleos de vCPU	Memória (GiB)	GPUs	Opção de dispositivo compatível
sbe1.4xlarge	16	32	0	otimizado para armazenamento
sbe1.6xlarge	24	32	0	otimizado para armazenamento
sbe-c.small	1	2	0	otimizado para computação
sbe-c.medium	1	4	0	otimizado para computação
sbe-c.large	2	8	0	otimizado para computação
sbe-c.xlarge	4	16	0	otimizado para computação
sbe-c.2xlarge	8	32	0	otimizado para computação
sbe-c.4xlarge	16	64	0	otimizado para computação
sbe-c.8xlarge	32	128	0	otimizado para computação
sbe-c.12xlarge	48	192	0	otimizado para computação
sbe-c.16xlarge	64	256	0	otimizado para computação
sbe-c.24xlarge	96	384	0	otimizado para computação

Tipo de instância	Núcleos de vCPU	Memória (GiB)	GPUs	Opção de dispositivo compatível
`sbe-g.small`	1	2	1	com GPU
`sbe-g.medium`	1	4	1	com GPU
`sbe-g.large`	2	8	1	com GPU
`sbe-g.xlarge`	4	16	1	com GPU
`sbe-g.2xlarge`	8	32	1	com GPU
`sbe-g.4xlarge`	16	64	1	com GPU
`sbe-g.8xlarge`	32	128	1	com GPU
`sbe-g.12xlarge`	48	192	1	com GPU

Limitações de recursos de computação compartilhada

Todos os serviços em um dispositivo Snowball Edge usam alguns dos recursos finitos no dispositivo. Um dispositivo Snowball Edge com os recursos de computação disponíveis maximizados não pode iniciar novos recursos de computação. Por exemplo, se você tentar iniciar a interface NFS enquanto executa uma instância de computação `sbe1.4xlarge` em um dispositivo otimizado para armazenamento, o serviço da interface NFS não será iniciado. A tabela a seguir descreve os recursos disponíveis nas diferentes opções de dispositivo, bem como os requisitos dos recursos para cada serviço.

- Se nenhum serviço de computação estiver `ACTIVE`:
  - Em uma opção otimizado para armazenamento, você tem 24 vCPUs e 32 GiB de memória para suas instâncias de computação.
  - Em uma opção otimizado para computação, você tem 52 vCPUs e 208 GiB de memória para suas instâncias de computação. Isso também é verdadeiro para a opção com GPU.
- Enquanto o AWS IoT Greengrass e o AWS Lambda habilitados pelo AWS IoT Greengrass estão `ACTIVE`:

- Em uma opção otimizada para armazenamento, esses serviços usam 4 núcleos de vCPU e 8 GiB de memória.
- Em uma opção otimizada para computação, esses serviços usam 1 núcleo de vCPU e 1 GiB de memória. Isso também vale para a opção com GPU.
- Se a interface NFS estiver `ACTIVE`, ela usará oito núcleos de vCPU e 16 GiB de memória em um dispositivo Snowball Edge.
- Enquanto o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow está ATIVO:
  - Em um Snowball Edge otimizado para computação com AMD EPYC 2ª geração e NVME, para um único nó com a configuração mínima de 3 TB de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, ele usa oito núcleos de vCPU e 16 GB de memória. Para um único nó com mais de 3 TB de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, ele usa vinte núcleos de vCPU e 40 GB de memória. Para um cluster, ele usa vinte núcleos de vCPU e 40 GB de memória.
  - Em um Snowball Edge otimizado para computação com AMD EPYC 1ª geração, HDD e GPU opcional, para um único nó ele usa oito núcleos de vCPU e 16 GB de memória. Para um cluster, ele usa vinte núcleos de vCPU e 40 GB de memória.

É possível determinar se um serviço está `ACTIVE` em um Snowball Edge usando o comando `snowballEdge describe-service` no cliente do Snowball Edge. Para ter mais informações, consulte Ver status do serviço.

Criar um trabalho de computação

Nesta seção, você vai criar o primeiro trabalho de instância de computação compatível com o Amazon EC2 para um dispositivo AWS Snowball Edge.

> **Important**
>
> Lembre-se dos seguintes pontos antes de criar o trabalho:
>
> - Verifique se os valores de vCPU, memória e armazenamento associados à AMI correspondem ao tipo de instância que deseja criar.
> - Se estiver usando Secure Shell (SSH) para conectar-se à instância depois de iniciar a instância no Snowball Edge, primeiro é necessário executar o procedimento a seguir. Não

é possível atualizar as AMIs no Snowball Edge após o fato. É necessário realizar esta etapa antes de criar o trabalho.

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

Para usar o Secure Shell (SSH) para se conectar às instâncias de computação em dispositivos Snowball Edge, é necessário 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 poderá se conectar às instâncias com SSH ao receber o dispositivo Snowball Edge.

Para colocar uma chave SSH em uma AMI

1. Inicie uma nova instância na Nuvem AWS com base na imagem CentOS 7 (x86_64), com atualizações HVM, Ubuntu 16.04 LTS, Xenial (HVM) e AMI do Amazon Linux 2 ou Windows.

   Ao iniciar a instância, verifique se o tamanho do armazenamento atribuído à instância é adequado para uso posterior no Snowball Edge. No console do Amazon EC2, isso é feito em Etapa 4: Adicionar armazenamento. Para obter uma lista dos tamanhos compatíveis de volumes de armazenamento de instância de computação em um Snowball Edge, consulte Cotas para instâncias de computação em um dispositivo Snowball Edge.
2. Instale e configure as aplicações que deseja executar no Snowball Edge 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 Snowball Edge. 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 no Manual do usuário para instâncias do Linux 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. 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 acessar a página Etapa 3: Fornecer detalhes do trabalho no assistente de criação de trabalhos, adicione as etapas a seguir.

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 o trabalho na 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 snowball create-job --job-type IMPORT --resources '{"S3Resources":
[{"BucketArn":"arn:aws:s3:::bucket-name"}],"Ec2AmiResources":
[{"AmiId":"ami-12345678"}]}' --description Example --address-
id ADIEXAMPLE60-1234-1234-5678-41fEXAMPLE57  --kms-key-arn arn:aws:kms:us-
west-2:012345678901:key/eEXAMPLE-1234-1234-5678-5b4EXAMPLE8e --role-
arn arn:aws:iam::012345678901:role/snowball-local-s3-lambda-us-west-2-role --snowball-
capacity-preference T100 --shipping-option SECOND_DAY --snowball-type EDGE
```

Depois que ele chegar e você o desbloquear, use o cliente do Snowball Edge para obter as credenciais locais. Para ter mais informações, consulte Como obter as credenciais.

Configuração de rede para as instâncias de computação

Depois de iniciar as instâncias de computação em um dispositivo da Família Snow, é necessário fornecer a ele um endereço IP criando uma interface de rede. Os dispositivos da Família Snow são compatíveis com dois tipos de interface de rede, uma virtual e uma 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)

Interface de rede direta (DNI) é um recurso de rede avançado que permite casos de uso, como fluxos multicast, roteamento transitivo e balanceamento 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.

Nos dispositivos Snowball Edge, as DNIs podem ser associadas às portas RJ45, SFP ou QSFP. Cada porta física suporta no máximo 63 DNIs. Os DNIs não precisam estar associados à mesma porta de rede física que você usa para gerenciar o dispositivo da família Snow.

> **Note**
>
> Dispositivos otimizados para armazenamento do Snowball Edge (com funcionalidade de computação do EC2) não são compatíveis com DNIs.

Tópicos

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 Configuring a Profile for the Snowball Edge Client.
4. Desbloqueie o dispositivo. Recomendamos usar o AWS OpsHub for Snow Family para desbloquear o dispositivo. Para obter instruções, consulte .

   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 usá-lo com o comando `ec2 associate-address` da AWS CLI posteriormente no processo.

   Sempre que precisar desse endereço IP, use o comando `snowballEdge describe-virtual-network-interfaces` do cliente do Snowball Edge ou o comando `aws ec2 describe-addresses` da AWS CLI 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 desde 12 de janeiro de 2021 e está acessível em todas as Regiões da AWS 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]
```

```
                                    [--physical-network-interface-
id physicalNetworkInterfaceId]
                                    [--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 o 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. É possível determinar as interfaces de rede físicas 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 DCHP 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
```

Usando SSH para se conectar a instâncias de computação em um dispositivo da família Snow

Para usar o Secure Shell (SSH) para se conectar a instâncias de computação em um dispositivo da família Snow, você tem as seguintes opções para fornecer ou criar uma chave SSH.

- Você pode fornecer a chave SSH para a Amazon Machine Image (AMI) ao criar um trabalho para solicitar um dispositivo. Para ter mais informações, consulte Configurar uma AMI para usar SSH a fim de conectar-se às instâncias de computação iniciadas no dispositivo.
- Você pode fornecer a chave SSH para a AMI ao criar uma imagem de máquina virtual para importar para um dispositivo da família Snow. Para ter mais informações, consulte Importando uma imagem de máquina virtual para um dispositivo da família Snow.
- Você pode criar um par de chaves no dispositivo Snow Family e optar por iniciar uma instância com essa chave pública gerada localmente. Para obter mais informações, consulte Criar um par de chaves usando o Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

Para se conectar a uma instância por meio de SSH

1. Verifique se o dispositivo está ligado, conectado à rede e desbloqueado. Para ter mais informações, consulte Conectar-se à rede local.
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 do Linux usando SSH no Manual do usuário para instâncias do Linux do Amazon EC2.

Transferir dados de instâncias de computação compatíveis com o EC2 para buckets do S3 no mesmo Snowball Edge

É possível transferir dados entre instâncias de computação e buckets do Amazon S3 no mesmo dispositivo Snowball Edge. Isso é feito usando os comandos da AWS CLI compatíveis e os endpoints apropriados. Por exemplo, suponha que deseja mover dados de um diretório na minha instância

`sbe1.xlarge` para o bucket do Amazon S3, `myBucket` no mesmo dispositivo. Suponha que você esteja usando o armazenamento compatível com o Amazon S3 no endpoint de dispositivos da Família Snow `https://S3-object-API-endpoint:443`. Use o procedimento a seguir:

> **Note**
>
> Este procedimento só funcionará se você tiver seguido as instruções em Configurar uma AMI para usar SSH a fim de conectar-se às instâncias de computação iniciadas no dispositivo.

Como transferir dados entre uma instância de computação e um bucket no mesmo Snowball Edge

1. Use SSH para se conectar à instância de computação.
2. Faça download e instale o AWS CLI. Se a instância ainda não tiver a AWS CLI, faça download e instale-a. Para obter mais informações, consulte Instalar a AWS Command Line Interface.
3. Configure a AWS CLI na instância de computação para trabalhar com o endpoint do Amazon S3 no Snowball Edge. Para ter mais informações, consulte Obtenção e utilização de credenciais do Amazon S3 locais.
4. Use o armazenamento compatível com o Amazon S3 compatível com os comandos dos dispositivos da família Snow para transferir dados. Por exemplo: .

```
aws s3 cp ~/june2018/results s3://myBucket/june2018/results --recursive --endpoint
 https://S3-object-API-endpoint:443
```

Comandos do cliente do Snowball Edge para instâncias de computação

O Snowball Edge é uma aplicação de terminal independente que você pode executar no servidor local. É possível usá-lo para realizar algumas tarefas administrativas no dispositivo Snowball Edge ou um cluster de dispositivos. Para obter mais informações sobre como usar o cliente do Snowball Edge, incluindo como iniciar e interromper serviços com ele, consulte Utilização do Snowball Edge Client.

Veja a seguir informações sobre os comandos do cliente do Snowball Edge específicos de instâncias de computação, incluindo exemplos de uso.

Para obter uma lista dos comandos compatíveis com o Amazon EC2 que podem ser usados no dispositivo AWS Snowball Edge, consulte Comandos aceitos da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge.

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

Para iniciar automaticamente instâncias de computação compatíveis com o Amazon EC2 no dispositivo AWS Snowball Edge depois de desbloqueado, é possível criar uma configuração de inicialização. Para isso, use o comando `snowballEdge create-autostart-configuration`, conforme mostrado a seguir.

Uso

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

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

Para atualizar uma configuração de inicialização existente no Snowball Edge, 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 or QSFP]] [--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 inicialização que não esteja mais em uso, utilize o comando `snowballEdge delete-autostart-configuration` da forma 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 inicialização criadas no Snowball Edge, use o comando `describe-autostart-configurations` da forma a seguir.

Uso

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

Criação de uma interface de rede virtual

Para executar uma instância de computação ou iniciar a interface NFS no Snowball Edge, primeiro você criará uma interface de rede virtual (VNIC). Cada Snowball Edge tem três interfaces de rede (NICs), os controladores da interface de rede física para o dispositivo. Elas são as portas RJ45, SFP e QSFP 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
```

Usar o endpoint compatível com o Amazon EC2

Veja a seguir uma visão geral do endpoint compatível com o 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.

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

Ao usar a AWS CLI para emitir um comando para o dispositivo AWS Snowball Edge, é possível especificar que o endpoint é o 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 Snowball Edge quando é 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.

Como associar o certificado ao endpoint compatível com o Amazon EC2

1. Conecte o Snowball Edge à alimentação e à rede e, depois, ative-o.
2. Depois que o dispositivo terminar de desbloquear, anote o endereço IP dele na sua rede local.
3. Em um terminal na rede, verifique se é possível fazer ping no Snowball Edge.
4. Execute o comando `snowballEdge get-certificate` no seu terminal. Para obter mais informações sobre este comando, consulte Gerenciar certificados de chave pública.
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.snowballEdge.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.

Comandos aceitos da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge

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 é compatível com muitos dos comandos da CLI do Amazon EC2 e ações dos SDKs da AWS. Para obter informações sobre como instalar e configurar a AWS CLI, incluindo como especificar as Regiões da AWS nas quais você deseja fazer chamadas à AWS CLI, consulte o Guia do usuário da AWS Command Line Interface.

Lista de comandos da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge

Veja a seguir uma descrição do subconjunto de comandos e opções da AWS CLI para o Amazon EC2 que são compatíveis com dispositivos Snowball Edge. 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 em execução ou interrompida no dispositivo e o expõe para a instância com o nome de dispositivo especificado.
  - --device `value`: o nome do dispositivo.
  - --instance-id: o ID de uma instância compatível com o 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 Snowball Edge. 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 Snowball Edge.
  - --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. É possível criar até cem modelos por 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"}]}],
    "UserData":"this is my user data"
}
```

- [--version-description `string`]: uma descrição para a primeira versão do modelo de inicialização.
- --endpoint `snowballEndpoint`: um valor que permite gerenciar as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 inicialização 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 inicialização.
  - --endpoint `snowballEndpoint`: um valor que permite gerenciar as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o Amazon EC2 como o endpoint AWS CLI.
- create-tags: adiciona ou substitui uma ou mais tags do recurso 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
  - Par de chaves
- create-security-group— Cria um grupo de segurança no seu Snowball Edge. 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 EBS que pode ser anexado a uma instância no dispositivo.
  - [--size`value`] — O tamanho do volume de entrada GiBs, que pode ser de 1 GiB a 1 TB (GiBs1000).
  - [--snapshot-id `value`]: o 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 as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 inicialização a serem excluídas.
  - --endpoint `snowballEndpoint`: um valor que permite gerenciar as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o Amazon EC2 como o endpoint AWS CLI.
- 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 recurso determinado (AMI, instância de computação, modelo de inicialização 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-addresses: 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 Snowball Edge durante a criação do trabalho.
  - --image-id: o ID do Snowball 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 a ser obtida 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 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: um token para especificar onde iniciar a paginação. Esse token é o valor `NextToken` de uma resposta truncada anteriormente.
- describe-instance-status— Descreve o status das instâncias especificadas ou de todas as suas instâncias. Por padrão, somente as instâncias em execução são descritas, a menos que você

indique especificamente para exibir o status de todas as instâncias. O status da instância inclui os seguintes componentes:

- Verificações de status: o dispositivo Snow realiza verificações de status na execução de instâncias compatíveis com o Amazon EC2 para identificar problemas de hardware e software.
- Estado da instância: é possível gerenciar as instâncias desde o momento em que as inicia até o encerramento.

Com esse comando, os filtros a seguir são compatíveis.

- `[--filters]` (lista)

  Os filtros.

  - `instance-state-code`: o código do estado da instância, como um valor inteiro não assinado de 16 bits. O byte alto é usado para fins de geração de relatórios de serviços internos e deve ser ignorado. O byte baixo é definido com base no estado representado. Os valores válidos são 0 (pendente), 16 (em execução), 32 (desligando), 48 (encerrado), 64 (interrompendo) e 80 (interrompido).
  - `instance-state-name`: o estado da instância (`pending` | `running` | `shutting-down` | `terminated` | `stopping` | `stopped`).
  - `instance-status.reachability`: filtra o status da instância em que o nome é `reachability` (`passed` | `failed` | `initializing` | `insufficient-data`).
  - `instance-status.status`: o status da instância (ok | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
  - `system-status.reachability`: filtra o status do sistema em que o nome é acessibilidade (`passed` | `failed` | `initializing` | `insufficient-data`).
  - `system-status.status`: o status do sistema da instância (ok | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
- Sintaxe do JSON:

```
[
  {
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
]
```

- `[--instance-ids]` (lista)

Os IDs de instâncias.

Padrão: descreve todas as instâncias.

- `[--dry-run|--no-dry-run]` (booliano)

  Confere se você tem as permissões necessárias para a ação, sem realmente fazer a solicitação, e fornece uma resposta de erro. Se você tiver as permissões necessárias, a resposta do erro será`DryRunOperation`.

  Caso contrário, ele será `UnauthorizedOperation`.

- `[--include-all-instances | --no-include-all-instances]` (booliano)

  Quando `true`, inclui o status de integridade de todas as instâncias. Quando `false`, inclui o status de integridade somente das instâncias em execução.

  Padrão: `false`

- `[--page-size]` (valor inteiro): o tamanho de cada página a ser obtida 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]` (valor inteiro): o número total de itens a serem gerados 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]` (string): 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 a ser obtida 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 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: 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 as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 a ser obtida 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 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: 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 as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 a ser obtida na chamada aos serviços da 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 aos serviços da AWS esgotem 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 recurso 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 as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 as instâncias de computação de forma programática usando operações da API compatíveis com o Amazon EC2. Para ter mais informações, consulte Especificar o endpoint compatível com o 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 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. 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 várias instâncias de computação usando um ID do Snowball de uma AMI.

> **Note**
>
> Pode levar até uma hora e meia para iniciar uma instância de computação em um Snowball Edge, 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 `sbg1`.

  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 do Snowball 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 CreateSecurityGroupo. 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 inicialização. 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 do usuário disponibilizados para a instância. Se estiver usando a AWS CLI, a codificação em Base64 será realizada para você, e você poderá carregar o texto a partir de um arquivo. Caso contrário, você deve fornecer o texto codificado em base64.
- --key-name (string): o nome do par de chaves. É possível criar um par de chaves usando `CreateKeyPair` ou `ImportKeyPair`.

> **Warning**
>
> Se você não especificar um par de chaves, não conseguirá se conectar à instância a menos que selecione uma AMI configurada para permitir aos usuários uma maneira de fazer login.

- 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.
- create-key-pair— Cria um par de chaves RSA de 2048 bits com o nome especificado. O Amazon EC2 armazena a chave pública e exibe a chave privada para que você salve em um arquivo. A chave privada é gerada como uma chave privada PKCS#1 codificada por PEM descriptografada. Se uma chave com o nome especificado já existir, o Amazon EC2 vai gerar um erro.
  - --key-name (string): um nome exclusivo para o par de chaves.

    Restrições: até 255 caracteres ASCII.
  - [--tag-specifications] (list): as tags a serem aplicadas ao novo par de chaves.

```
{
    "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
      ...
    ]
  }
  ...
```

- import-key-pair –
  - --key-name (string): um nome exclusivo para o par de chaves.

Restrições: até 255 caracteres ASCII.

- -- public-key-material (blob) — A chave pública. Para chamadas da API, o texto deve ser codificado em base64. Para ferramentas de linha de comando, a codificação base64 é realizada para você.
- [--tag-specifications] (list): as tags a serem aplicadas ao novo par de chaves.

```
{
    "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
      ...
    ]
  }
```

- describe-key-pairs –

  [--filters] (list): os filtros.

  - key-pair-id — O ID do par de chaves.
  - key-name: o nome do par de chaves.
  - tag-key: a chave de uma tag atribuída ao recurso. Use esse filtro para encontrar todos os recursos atribuídos a uma tag com uma chave específica, independentemente do valor da tag.
  - [--tag-specifications] (list): as tags a serem aplicadas ao novo par de chaves.
  - tag :key: a combinação de chave/valor de uma tag atribuída ao recurso. Use a chave de etiqueta no nome do filtro e o valor da etiqueta como o valor do filtro. Por exemplo, para encontrar todos os recursos que têm uma etiqueta com a chave `Owner` e o valor `Team A`, especifique `tag:Owner` para o nome do filtro e `Team A` no valor do filtro.

```
{
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
```

- [--key-names] (list): os nomes dos pares de chaves.

Padrão: descreve todos os pares de chaves.

- [--key-pair-ids] (list) — Os IDs dos pares de chaves.
- delete-key-pair –
  - [--key-name] (string): o nome do par de chaves.
  - [--key-pair-id] (string) — O ID do par de chaves.

Operações da API compatíveis com o Amazon EC2 aceitas

Veja a seguir operações da API compatíveis com o Amazon EC2 que podem ser usadas com um Snowball Edge, com links para as descrições na Referência da API do Amazon EC2. As chamadas da API compatíveis com o Amazon EC2 exigem assinatura com o Signature Version 4 (SigV4). Se você estiver usando a AWS CLI ou um AWS SDK para fazer essas chamadas da API, a assinatura do SigV4 será fornecida para você. Caso contrário, você precisará implementar sua própria solução de assinatura do SigV4. Para ter mais informações, consulte Obtenção e utilização de credenciais do Amazon S3 locais.

- 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 Snowball Edge. 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 Snowball Edge. 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`
- DescribeInstanceStatus
- 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 iniciar uma instância de computação em um Snowball Edge, dependendo do tamanho e do tipo de instância.

- StartInstances

- StopInstances— Os recursos associados a uma instância parada persistem. Você pode encerrar a instância para liberar esses atributos. No entanto, todos os dados associados serão excluídos.
- TerminateInstances

Iniciar automaticamente instâncias compatíveis com o Amazon EC2 com modelos de inicialização

É possível iniciar automaticamente as instâncias compatíveis com o Amazon EC2 no dispositivo AWS Snowball Edge usando modelos de inicialização e comandos de configuração de inicialização do cliente do Snowball Edge.

Um modelo de inicialização contém as informações de configuração necessárias para criar uma instância compatível com o Amazon EC2 no Snowball Edge. É possível usar um modelo de inicialização para armazenar os parâmetros de inicialização para que não seja necessário especificá-los toda vez que iniciar uma instância compatível com o EC2 no Snowball Edge.

Ao usar configurações de início automático no Snowball Edge, você vai configurar os parâmetros com os quais deseja que a instância compatível com o Amazon EC2 inicie. Assim que o Snowball Edge estiver configurado, ao reinicializá-lo e desbloqueá-lo, ele usará a configuração de início automático para iniciar 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 de instâncias subsequentes (após reinicializações planejadas ou não) acontecerão automaticamente após o dispositivo ser desbloqueado.

Um modelo de inicialização 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 iniciar essa instância. Para obter uma lista dos tipos de instâncias compatíveis, consulte Cotas para instâncias de computação em um dispositivo Snowball Edge.

Para iniciar automaticamente instâncias compatíveis com o EC2 no Snowball Edge, realize as seguintes etapas:

1. Ao solicitar seu AWS Snowball Edge dispositivo, crie um trabalho para solicitar um dispositivo da família Snow com instâncias computacionais. Para ter mais informações, consulte Criar um trabalho de computação.
2. Depois de receber o Snowball Edge, desbloqueie-o.
3. Use o comando `aws ec2 create-launch-template` da API compatível com o EC2 para criar um modelo de inicialização.
4. Use o comando `snowballEdge create-autostart-configuration` do cliente do Snowball Edge para vincular o modelo de inicialização 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, depois, desbloqueie o dispositivo. As instâncias compatíveis com o EC2 serão iniciadas automaticamente usando os atributos especificados no modelo de inicialização e o comando `create-autostart-configuration` do cliente do Snowball Edge.

Para visualizar o status das instâncias em execução, use o comando `describe-autostart-configurations` da API compatível com o EC2.

> **Note**
>
> Não há suporte do console nem da API de gerenciamento de trabalhos do AWS Snowball para modelos de inicialização. Use comandos da CLI compatíveis com o EC2 e do cliente do Snowball Edge para iniciar automaticamente instâncias compatíveis com o EC2 no dispositivo AWS Snowball Edge.

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

O IMDS para Snow oferece o serviço de metadados de instância (IMDS) para instâncias compatíveis com o Amazon EC2 no Snow. Os metadados de instância são categorias de informações sobre instâncias. Incluem categorias, como nome do host, eventos e grupos de segurança. Usando o IMDS para Snow, também é possível usar os metadados de instância para acessar os dados do usuário que você especificou ao iniciar a instância compatível com o Amazon EC2. Por exemplo, é possível usar o IMDS para Snow para especificar parâmetros e configurar a instância ou incluí-los 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 e dados do usuário compatíveis 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 compatibilidade com a recuperação de metadados da instância usando o endereço IPv6 local do link.

Tópicos

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

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

A 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 sessão, 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 esse período, é possível usar o mesmo token de sessão para solicitações subsequentes. Depois que essa duração expirar, será necessário criar um token de sessão para solicitações futuras.

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

Depois, 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.

Example 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. O exemplo de comando a seguir obtém o ID da AMI utilizada para iniciar a instância e o armazena no `$TOKEN` criado no exemplo anterior.

Example 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 de instância, a solicitação deve seguir estas 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 compatíveis com o EC2 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 para 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 de instância, envie uma solicitação GETpara o serviço de metadados de instância.

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

Recuperar metadados da instância

Como os metadados de instância estão disponíveis na instância em execução, não é necessário usar o console do Amazon EC2 nem a AWS CLI para acessá-la. 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 e dados do usuário compatíveis neste guia.

Para visualizar todas as categorias de metadados de instância de dentro de uma instância em execução, use o seguinte URI de IPv4.

```
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 recurso de metadados específico gera o valor apropriado, ou um código de erro de HTTP 404: Não encontrado se o recurso não estiver disponível.

Uma solicitação de um recurso de metadados geral (o URI termina com o caractere `/`) gera uma lista de recursos disponíveis, ou um código de erro de HTTP 404: Não encontrado se não houver esse recurso. Os itens da lista estão em linhas separadas, encerradas por caracteres de alimentação de linha (código de caractere ASCII 10).

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

- 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.

Example Exemplo de obtenção das versões disponíveis dos metadados de 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
```

Example Exemplo de obtenção de 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 da instância e dados do usuário compatíveis 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
```

Example Exemplo de obtenção de 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 armazenamento em blocos com instâncias compatíveis com o Amazon EC2

Com armazenamento em blocos no Snowball Edge, é possível adicionar ou remover o armazenamento em blocos com base nas necessidades das aplicações. Os volumes anexados a uma instância compatível com o Amazon EC2 são expostos como volumes de armazenamento que são mantidos independentemente da vida útil da instância. É possível gerenciar o armazenamento em blocos usando a API conhecida do Amazon EBS.

Determinados comandos do Amazon EBS são aceitos por meio do uso do endpoint compatível com o EC2. Os comandos com 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 da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge.

> **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.

Veja a seguir cotas e diferenças entre os volumes do Amazon EBS no dispositivo e na nuvem:

- Os volumes do Amazon EBS estão disponíveis apenas para instâncias compatíveis com o EC2 em execução no dispositivo que hospeda os volumes.
- Os tipos de volume são limitados a HDD otimizado para capacidade (`sbg1`) ou SSD otimizado para performance (`sbp1`). O tipo de volume padrão é `sbg1`.
- O Snowball Edge compartilha memória de HDD entre objetos do Amazon S3 e o Amazon EBS. Se você usar armazenamento em blocos baseado em HDD no AWS Snowball Edge, isso reduzirá a quantidade de memória disponível para objetos do Amazon S3. Da mesma forma, os objetos do Amazon S3 reduzem a quantidade de memória disponível para armazenamento em blocos do Amazon EBS em volumes de HDD.
- Os volumes raiz compatíveis com o 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, o parâmetro `encrypted` não é compatível. No entanto, todos os dados no seu dispositivo são criptografados por padrão.
- Os volumes podem ter de 1 GB a 10 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 Snowball Edge. No entanto, a capacidade total do volume do Amazon EBS é limitada pelo espaço disponível no dispositivo.

Grupos de segurança em dispositivos Snowball Edge

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 do Linux no Manual do usuário para instâncias do Linux do Amazon EC2.

Os grupos de segurança em dispositivos Snowball Edge são semelhantes a grupos de segurança na Nuvem AWS. Nuvens privadas virtuais (VPCs) não são compatíveis com dispositivos Snowball Edge.

Veja a seguir as outras diferenças entre grupos de segurança do Snowball Edge e grupos de segurança de EC2-VPC:

- Cada Snowball Edge tem um limite de cinquenta 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 ações da AWS CLI e chamadas à API são compatíveis. Normalmente, esses são um subconjunto daqueles compatíveis em instâncias de EC2-VPC.

Para obter mais informações sobre ações compatíveis da AWS CLI, consulte Lista de comandos da AWS CLI compatíveis com o Amazon EC2 em um Snowball Edge. Para obter mais informações sobre as operações da API compatíveis, consulte Operações da API compatíveis com o Amazon EC2 aceitas.

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 Snowball Edge é compatível com um subconjunto de categorias de metadados das instâncias de computação. Para obter mais informações, consulte Metadados de instância e dados do usuário no Manual do usuário para instâncias do Linux 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 Snowball Edge

Dados	Descrição
`ami-id`	O ID da AMI usada para executar a instância.
`hostname`	O nome de host DNS IPv4 privado da instância .
`instance-id`	O ID dessa instância.
`instance-type`	O tipo da instância.

Dados	Descrição
`local-hostname`	O nome de host DNS IPv4 privado da instância .
`local-ipv4`	O endereço IPv4 privado da instância.
`mac`	O endereço Media Access Control (MAC) da instância.
`network/interfaces/macs/ mac/ local-hostname`	O nome do host local da interface.
`network/interfaces/macs/ mac/ local-ipv4s`	Os endereços IPv4 privados associados à interface.
`network/interfaces/macs/ mac/mac`	O endereço MAC da instância.
`network/interfaces/macs/ mac/ public-ipv4s`	Os endereços IP elásticos associados à interface.
`public-ipv4`	O endereço IPv4 público.
`public-keys/0/openssh-key`	Chave pública. Disponível somente se fornecido no momento da execução da instância.
`reservation-id`	O ID da reserva.
userData	Scripts de shell para enviar instruções para uma instância na execução.

Categorias de dados dinâmicos de instância compatíveis em um Snowball Edge

Dados	Descrição
instance-identity/document	JSON que contém atributos de instância . Somente `instanceId` , `imageId`, `privateIp` , and `instanceType` têm

Dados	Descrição
	valores, e os outros atributos retornados são nulos. Para obter mais informações, consulte Documentos de identidade da instância no Manual do usuário para instâncias do Linux do Amazon EC2.

Dados do usuário em instâncias de computação do Snowball

Os dados do usuário são compatíveis para uso com scripts de shell para instâncias de computação em um Snowball Edge. Usando os scripts de shell, você pode enviar instruções para uma instância na execução. Você pode alterar os dados do usuário com o comando `modify-instance-attribute` da AWS CLI ou a ação `ModifyInstanceAttribute` da API.

Para alterar dados do usuário

1. Pare a instância de computação com o comando `stop-instances` da AWS CLI.
2. Usando o comando `modify-instance-attribute` da AWS CLI, modifique o atributo `userData`.
3. Reinicie a instância de computação com o comando `start-instances` da AWS CLI.

Somente scripts de shell são compatíveis com instâncias de computação. Não há suporte para as diretivas de pacote `cloud-init` nas instâncias de computação em execução em um Snowball Edge. Para obter mais informações sobre como trabalhar com comandos da AWS CLI, consulte a Referência de comandos da AWS CLI.

Interromper uma instância compatível com o EC2

Para evitar a exclusão acidental das instâncias compatíveis com o Amazon EC2 criadas no dispositivo, 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.

Solucionar problemas com instâncias de computação em dispositivos Snowball Edge

Veja a seguir dicas para a solução de problemas em trabalhos do Snowball Edge com instâncias de computação.

Tópicos

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 errada. Por exemplo, você pode estar tentando obter o endereço IP da interface SFP+, mas é a interface RJ45 que está conectada à rede.

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 Snowball Edge trava ao iniciar uma instância de computação grande.

Pode parecer que o Snowball Edge 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.

Para conferir o status das instâncias, use o comando `aws ec2 describe-instances` da AWS CLI no endpoint compatível com o Amazon EC2 HTTP ou HTTPS no Snowball Edge.

Minha instância tem um volume raiz

As instâncias têm um volume raiz por padrão. Todas as instâncias `sbe` têm um único volume raiz, mas com o Snowball Edge, é possível adicionar ou remover o armazenamento em blocos com base nas necessidades das aplicações. Para ter mais informações, consulte Usar armazenamento em blocos com instâncias compatíveis com o Amazon EC2.

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 a seguir.

```
chmod 400 filename.pem
```

Usando armazenamento compatível com Amazon S3 em dispositivos da Família Snow

O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow oferece armazenamento seguro de objetos com maior resiliência, escala e um conjunto expandido de atributos de API do Amazon S3 para ambientes robustos, móveis de borda e desconectados. Usando o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, você pode armazenar dados e executar aplicativos altamente disponíveis em dispositivos da Família Snow para computação de borda.

Você pode criar buckets do Amazon S3 nos dispositivos Snowball Edge para armazenar e recuperar objetos no local para aplicativos que exigem acesso e processamento de dados locais e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para

armazenar dados de forma duradoura e redundante em vários dispositivos Snowball Edge. É possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação. Quando o dispositivo ou dispositivos são devolvidos AWS, todos os dados criados ou armazenados no armazenamento compatível com o Amazon S3 nos dispositivos da família Snow são apagados. Para obter mais informações, consulte Trabalhos somente de computação e armazenamento locais.

Você pode implantar armazenamento compatível com o Amazon S3 em dispositivos da Família Snow em configuração independente ou em configuração de cluster. Na configuração autônoma, você pode provisionar a capacidade do S3 no dispositivo e o balanceamento está disponível como armazenamento em bloco. Na configuração do cluster, toda a capacidade do disco de dados é usada para armazenamento do S3. Um cluster pode consistir em um mínimo de 3 dispositivos até um máximo de 16 dispositivos. Dependendo do tamanho do cluster, o serviço S3 foi projetado para manter a tolerância a falhas de 1 ou 2 dispositivos.

Com AWS DataSync, você pode transferir objetos entre o armazenamento compatível com o Amazon S3 em dispositivos da família Snow em um dispositivo Snowball Edge e serviços de armazenamento. AWS Para obter mais informações, consulte Configurando transferências com armazenamento compatível com S3 no Snowball Edge no Guia do Usuário. AWS DataSync

A seguir está a capacidade de armazenamento compatível com o Amazon S3 em dispositivos da Família Snow e a capacidade de armazenamento em blocos para um dispositivo autônomo usando armazenamento compatível com o Amazon S3 em dispositivos da Família Snow. Para tolerância a falhas e capacidade de armazenamento de clusters, consulte this table.

Snowball Edge Compute Optimized and Compute Optimized with GPU

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow e armazenamento em blocos de dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen1, HDD e GPU opcional)

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow (em TB)	Capacidade de armazenamento em blocos (em TB)
2,5	41
5.5	37

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow (em TB)	Capacidade de armazenamento em blocos (em TB)
8.5	33
11	29
14	25
17	21
19,5	17
22,5	13
25.5	9
28,5	5
31	1

Snowball Edge Compute Optimized with NVMe storage

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow e armazenamento em blocos de dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen2 e NVMe)

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow (em TB)	Capacidade de armazenamento em blocos (em TB)
3	17,5
5.5	14,5
10.5	8.5
12	6.5

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow (em TB)	Capacidade de armazenamento em blocos (em TB)
13	5.5
16,5	1.5

Snowball Edge storage optimized 210 TB

Capacidade de armazenamento do armazenamento compatível com Amazon S3 em dispositivos da família Snow e armazenamento em bloco de dispositivos de 210 TB otimizados para armazenamento do Snowball Edge

Capacidade de armazenamento compatível com Amazon S3 em dispositivos da Família Snow (em TB)	Capacidade de armazenamento em blocos (em TB)
20	206
40	182
60	158
80	134
100	110
120	86
140	62
160	38
180	14
190	2

Especificações de armazenamento compatível com Amazon S3 em dispositivos da Família Snow:

- O número máximo de buckets de dispositivos da Família Snow é 100 por dispositivo ou por cluster.
- A conta do proprietário do bucket do dispositivo do S3 na Família Snow é o proprietário de todos os objetos no bucket.
- Somente a conta de proprietário do bucket do S3 na Família Snow pode executar operações no bucket.
- As limitações de tamanho do objeto são consistentes com as do Amazon S3.
- Todos os objetos armazenados no S3 no dispositivo da Família Snow têm o SNOW como classe de armazenamento.
- Por padrão, todos os objetos armazenados na classe de armazenamento SNOW são armazenados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Você também pode optar explicitamente por armazenar objetos usando a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C).
- Se não houver espaço suficiente para armazenar um objeto em seu dispositivo da Família Snow, a API retornará uma exceção de capacidade insuficiente (ICE).

Tópicos

Solicite armazenamento compatível com Amazon S3 em dispositivos da Família Snow

Pedir um dispositivo para armazenamento compatível com o Amazon S3 em dispositivos da Família Snow é muito semelhante ao processo de pedido de um Snowball Edge. Para fazer o pedido, consulte Criando um trabalho para solicitar um dispositivo da família Snow neste guia e lembre-se desses itens durante o processo de pedido:

- Em Escolher um tipo de trabalho, escolha Somente computação e armazenamento locais.
- Em Dispositivos Snow, escolha Snowball Edge otimizado para computação
- Em Selecionar o tipo de armazenamento, selecione Armazenamento compatível com Amazon S3 em dispositivos da Família Snow.
- Para um dispositivo autônomo, em Capacidade de armazenamento, escolha Dispositivo único e selecione a quantidade de armazenamento desejada.
- Para um cluster, em Capacidade de armazenamento, selecione Cluster e, em seguida, selecione a capacidade de armazenamento e a tolerância a falhas desejadas.

Configurando o armazenamento compatível com o Amazon S3 em dispositivos da família Snow

Instale e configure ferramentas de AWS software em seu ambiente local para interagir com o dispositivo ou cluster de dispositivos Snowball Edge e o armazenamento compatível com Amazon S3 em dispositivos da família Snow. Em seguida, use essas ferramentas para configurar o dispositivo ou cluster Snowball Edge e iniciar o armazenamento compatível com o Amazon S3 em dispositivos da família Snow.

Pré-requisitos

O armazenamento compatível com o Amazon S3 em dispositivos da família Snow exige que você tenha o cliente Snowball Edge e o AWS CLI instalado em seu ambiente local. Você também pode usar o AWS SDK for .NET AWS Tools for Windows PowerShell para trabalhar com armazenamento compatível com Amazon S3 em dispositivos da família Snow. AWS recomenda o uso das seguintes versões dessas ferramentas:

- Cliente Snowball Edge — Use a versão mais recente. Para obter mais informações, consulte Baixar e instalar o cliente Snowball Edge neste guia.

- AWS CLI— Versão 2.11.15 ou mais recente. Para obter mais informações, consulte Instalando, atualizando e desinstalando o AWS CLI no Guia do AWS Command Line Interface Usuário.
- AWS SDK for .NET— AWSSDK .S3Control 3.7.304.8 ou mais recente. Para ter mais informações, consulte AWS SDK for .NET.
- AWS Ferramentas para Windows PowerShell — Versão 4.1.476 ou mais recente. Para obter mais informações, consulte o Guia do usuário do AWS Tools for Windows PowerShell.

Configurando seu ambiente local

Esta seção descreve como instalar e configurar o cliente Snowball Edge e seu ambiente local para uso com armazenamento compatível com Amazon S3 em dispositivos da família Snow.

Para configurar seu ambiente

1. Baixe e instale a versão mais recente do Snowball Edge Client. Para obter mais informações, consulte Baixar e instalar o cliente Snowball Edge neste guia.
2. Execute os comandos a seguir para configurar suas pastas.

```
chmod u+x new_cli/bin/snowballEdge
chmod u+x new_cli/jre/bin/java
```

3. Adicione `new_cli/bin` ao seu `$PATH`.
4. Execute o comando `snowballEdge configure`. Você receberá uma resposta semelhante ao seguinte:

```
Configuration will be stored at /home/user/.aws/snowball/config/snowball-
edge.config
```

5. Insira as seguintes informações:
   - O caminho do manifesto.
   - Um código de desbloqueio.
   - O endpoint padrão. Para dispositivos autônomos do Snowball Edge, use o endereço IP do dispositivo. Para um cluster de dispositivos, especifique o endereço IP de qualquer dispositivo no cluster. Para testar se os endpoints padrão estão disponíveis no cliente, use um comando

semelhante ao seguinte. Para o número da porta, use 9091 (porta de ativação), 22 (SSH) e 8080 (endpoint HTTP para s3).

```
telnet snowball_ip port_number
```

6. Se você estiver usando AWS SDK for .NET, defina o valor do `clientConfig.AuthenticationRegion` parâmetro da seguinte forma:

```
clientConfig.AuthenticationRegion = "snow"
```

Configuração de seu dispositivo Snowball Edge

Configure seu dispositivo Snowball Edge de acordo com Como receber o Snowball Edge neste guia.

Depois que seu dispositivo estiver configurado e em execução, configure e inicie o armazenamento compatível com o Amazon S3 nos dispositivos da Família Snow. Consulte Configurando o armazenamento compatível com o Amazon S3 em dispositivos da família Snow.

Configurando o IAM no Snowball Edge

AWS Identity and Access Management (IAM) ajuda você a habilitar o acesso granular aos AWS recursos que são executados em seus dispositivos Snowball Edge. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.

O IAM é suportado localmente no Snowball Edge. É possível usar o serviço local do IAM para criar perfis e anexar políticas do IAM a eles. É possível usar essas políticas para permitir o acesso necessário para realizar as tarefas atribuídas.

O exemplo a seguir permite acesso total à API do Amazon S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
```

```
            "Resource": "*"

        }
    ]
}
```

Para obter exemplos de políticas do IAM, consulte o Guia do desenvolvedor da AWS Snowball Edge.

Iniciando o serviço de armazenamento compatível com Amazon S3 em dispositivos da Família Snow

Use as instruções a seguir para iniciar o serviço de armazenamento compatível com Amazon S3 em dispositivos da família Snow em um dispositivo ou cluster Snowball Edge.

> **Note**
>
> Se você preferir uma experiência mais fácil de usar, você pode iniciar o serviço de armazenamento compatível com Amazon S3 em dispositivos da família Snow para um dispositivo autônomo ou um cluster de dispositivos usando. AWS OpsHub Consulte Configure o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow.

1. Desbloqueie seu dispositivo Snowball Edge ou cluster de dispositivos executando o seguinte comando:

   - Para um único dispositivo:

     ```
     snowballEdge unlock-device --endpoint https://snow-device-ip
     ```

   - Para um cluster:

     ```
     snowballEdge unlock-cluster
     ```

2. Execute o comando a seguir e certifique-se de que o dispositivo ou o cluster de dispositivos do Snowball Edge esteja desbloqueado:

   - Para um único dispositivo:

```
snowballEdge describe-device --endpoint https://snow-device-ip
```

- Para um cluster:

```
snowballEdge describe-cluster --device-ip-addresses [snow-device-1-ip] [snow-device-2-ip] /
    [snow-device-3-ip] [snow-device-4-ip] [snow-device-5-ip] /
    [snow-device-6-ip]
```

3. Para cada dispositivo (se você tem um ou um cluster), para iniciar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, faça o seguinte:

   a. Obtenha os `PhysicalNetworkInterfaceId` dos dispositivos executando o comando `describe-device` a seguir:

   ```
   snowballEdge describe-device --endpoint https://snow-device-ip
   ```

   b. Execute o comando `create-virtual-network-interface` a seguir duas vezes para criar as interfaces de rede virtual (VNIs) para os endpoints `s3control` (para operações de bucket) e `s3api` (para operações de objetos).

   ```
   snowballEdge create-virtual-network-interface --ip-address-assignment
   dhcp --manifest-file manifest --physical-network-interface-id
   "PhysicalNetworkInterfaceId" --unlock-code unlockcode --endpoint https://snow-device-ip
   ```

   Para obter detalhes sobre esses comandos, consulte Criação de uma interface de rede virtual.

   > **Note**
   >
   > Iniciar o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow consome atributos do dispositivo.

4. Inicie o serviço de armazenamento compatível com o Amazon S3 em dispositivos da família Snow executando o seguinte `start-service` comando, que inclui os endereços IP dos seus

dispositivos e os Amazon Resource Names (ARNs) das VNIs que você criou para os endpoints e. `s3control` `s3api`

Para iniciar o serviço em um único dispositivo:

```
  snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-device-1-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2
```

Para iniciar o serviço em um cluster:

```
  snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2 vni-arn-3  vni-arn-4 vni-arn-5 vni-arn-6
```

Para `--virtual-network-interface-arns`, inclua ARNs para todas as VNIs que você criou na etapa anterior. Separe cada ARN usando um espaço.

5. Execute o comando `describe-service` a seguir para um único dispositivo:

```
  snowballEdge describe-service --service-id s3-snow
```

Espere até que o status do serviço seja `Active`.

Execute o comando `describe-service` a seguir para um cluster:

```
  snowballEdge describe-service --service-id s3-snow \
    --device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip
```

Como trabalhar com buckets do S3 em um dispositivo Snowball Edge

Você pode criar buckets do Amazon S3 em seus dispositivos Snowball Edge para poder armazenar e recuperar objetos on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos

Snowball Edge. É possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação.

Usando o AWS CLI

Siga estas instruções para trabalhar com buckets do Amazon S3 no seu dispositivo usando o AWS CLI.

Para configurar o AWS CLI

1. Crie um perfil para endpoints de objetos em `~/.aws/config`.

   ```
   [profile your-profile]
   aws_access_key_id = your-access-id
   aws_secret_access_key = your-access-key
   region = snow
   ca_bundle = dev/apps/ca-certs/your-ca_bundle
   ```

2. Obtenha um certificado do seu dispositivo. Para obter informações, consulte o Guia do desenvolvedor do Snowball Edge.
3. Se você tiver instalado o SDK em um ambiente virtual, ative-o usando o seguinte comando:

   ```
   source your-virtual-environment-name/bin/activate
   ```

Depois de configurar suas operações, você pode acessá-las usando chamadas de API com o AWS CLI. Nos exemplos a seguir, *cert* é o certificado de dispositivo que você acabou de obter usando o IAM.

Acessar operações de objeto

```
aws s3api --profile your-profile list-objects-v2 --endpoint-url
https://s3api-endpoint-ip
```

Acessar operações de bucket

```
aws s3control --profile your-profile list-regional-buckets --account-id
bucket-owner --endpoint-url https://s3ctrlapi-endpoint-ip
```

Uso do Java SDK

Use o exemplo a seguir para trabalhar com objetos do Amazon S3 usando o Java SDK.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.auth.credentials.StaticCredentialsProvider;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.regions.Region;

import java.net.URI;

AwsBasicCredentials creds = AwsBasicCredentials.create(accessKey, secretKey); // set
 creds by getting Access Key and Secret Key from snowball edge
SdkHttpClient httpClient =
 ApacheHttpClient.builder().tlsTrustManagersProvider(trustManagersProvider).build(); //
 set trust managers provider with client certificate from snowball edge
String s3SnowEndpoint = "10.0.0.0"; // set s3-snow object api endpoint from describe
 service

S3Client s3Client =
 S3Client.builder().httpClient(httpClient).region(Region.of("snow")).endpointOverride(new
 URI(s3SnowEndpoint)).credentialsProvider(StaticCredentialsProvider.create(creds)).build();
```

Formato do ARN do bucket

Você pode usar o formato do nome do recurso da Amazon (ARN) listado aqui para identificar um bucket do Amazon S3 em um dispositivo Snowball Edge:

```
arn:partition:s3:snow:account-id:device/device-id/bucket/bucket-name
```

Onde *partição* é a partição da região em que você solicitou seu dispositivo Snowball Edge. *device-id* é o job_id se for um dispositivo autônomo do Snowball Edge, ou o *cluster_id* se você tiver um cluster do Snowball Edge.

Criação de um bucket do S3 em um dispositivo Snowball Edge

Você pode criar buckets do Amazon S3 em seus dispositivos Snowball Edge para armazenar e recuperar objetos na borda para aplicações que exigem acesso a dados locais, processamento de

dados local e residência de dados. O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow é uma nova classe de armazenamento, `SNOW`, que usa o Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos. É possível usar os mesmos atributos e APIs nos buckets da mesma maneira que em buckets do Amazon S3, incluindo políticas de ciclo de vida de bucket, criptografia e marcação.

O exemplo a seguir cria um bucket do Amazon S3 para um dispositivo Snowball Edge usando o AWS CLI. Para executar esse comando, substitua os espaços reservados de entrada por suas próprias informações.

```
aws s3control --profile your-profile create-bucket --bucket your-snow-bucket --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Criando e gerenciando uma configuração do ciclo de vida do objeto usando o AWS CLI

Você pode usar o ciclo de vida do Amazon S3 para otimizar a capacidade de armazenamento para armazenamento compatível com Amazon S3 em dispositivos da Família Snow. Você pode criar regras de ciclo de vida para expirar objetos à medida que envelhecem ou quando são substituídos por versões mais recentes. Você pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida. Para obter mais informações sobre o ciclo de vida do Amazon S3, consulte Gerenciar ciclo de vida de armazenamento.

> **Note**
>
> Quem Conta da AWS cria o bucket é dono dele e é o único que pode criar, habilitar, desabilitar ou excluir uma regra de ciclo de vida.

Para criar e gerenciar uma configuração de ciclo de vida de um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow usando o AWS Command Line Interface (AWS CLI), consulte os exemplos a seguir.

Coloque uma configuração de ciclo de vida em um bucket do Snowball Edge

O AWS CLI exemplo a seguir coloca uma política de configuração de ciclo de vida em um bucket do Snowball Edge. Essa política especifica que todos os objetos que têm o prefixo sinalizado (*myprefix*) e tags expiram após dez dias. Para usar esse exemplo, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

Primeiro, salve a política da configuração do ciclo de vida em um arquivo JSON. Neste exemplo, o nome do arquivo é **`lifecycle-example.json`**.

```
{
    "Rules": [{
        "ID": "id-1",
        "Filter": {
            "And": {
                "Prefix": "myprefix",
                "Tags": [{
                        "Value": "mytagvalue1",
                        "Key": "mytagkey1"
                    },
                    {
                        "Value": "mytagvalue2",
                        "Key": "mytagkey2"
                    }
                ],
            }
        },
        "Status": "Enabled",
        "Expiration": {
            "Days": 10
        }
    }]
}
```

Depois de salvar o arquivo, envie o arquivo JSON como parte do comando `put-bucket-lifecycle-configuration`. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3control put-bucket-lifecycle-configuration --bucket
                example-snow-bucket --profile your-profile
                --lifecycle-configuration file://lifecycle-example.json --endpoint-url
 https://s3ctrlapi-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte put-bucket-lifecycle-configurationna Referência de AWS CLI Comandos.

Como trabalhar com buckets do S3 em um dispositivo Snowball Edge

Com o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, você pode criar buckets do Amazon S3 nos dispositivos Snowball Edge para armazenar e recuperar objetos on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos Snowball Edge. É possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação. Você pode usar o armazenamento compatível com o Amazon S3 em dispositivos da família Snow usando o AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Determine se você pode acessar um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow

O exemplo a seguir usa o comando `head-bucket` para determinar se existe um bucket do Amazon S3 e se você tem permissão para acessá-lo usando o AWS CLI. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3api head-bucket --bucket sample-bucket --profile your-profile --endpoint-url
 https://s3api-endpoint-ip
```

Recupere uma lista de compartimentos ou compartimentos regionais

Use o `list-regional-buckets` ou `list buckets` para listar o armazenamento compatível com o Amazon S3 em buckets de dispositivos da família Snow usando o. AWS CLI

```
aws s3control list-regional-buckets --account-id 123456789012 --profile your-profile --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obter mais informações sobre o comando `list-regional-buckets`, consulte list-regional-buckets na Referência de comandos da AWS CLI .

```
 aws s3 list-buckets --account-id 123456789012 --endpoint-url https://s3api-endpoint-ip
```

Para obter mais informações sobre o *`list-buckets`* comando, consulte list-buckets na Referência de comandos AWS CLI

O exemplo do SDK para Java a seguir obtém uma lista de buckets nos dispositivos Snowball Edge. Para obter mais informações, consulte ListBucketsa Referência de API do Amazon Simple Storage Service.

```
  import com.amazonaws.services.s3.model.*;
  public void listBuckets() {
    ListBucketsRequest reqListBuckets = new ListBucketsRequest()
    .withAccountId(AccountId)
    ListBucketsResult respListBuckets = s3APIClient.RegionalBuckets(reqListBuckets);
    System.out.printf("ListBuckets Response: %s%n", respListBuckets.toString());
  }
```

O PowerShell exemplo a seguir obtém uma lista de buckets nos dispositivos Snowball Edge.

```
   Get-S3CRegionalBucketList -AccountId 012345678910 -Endpoint "https://snowball_ip" -
Region snow
```

O exemplo do.NET a seguir obtém uma lista de buckets em dispositivos Snowball Edge.

```
using Amazon.S3Control;
using Amazon.S3Control.Model;

namespace SnowTest;

internal class Program
{
    static async Task Main(string[] args)
    {
        var config = new AmazonS3ControlConfig
        {
            ServiceURL = "https://snowball_ip",
            AuthenticationRegion = "snow" // Note that this is not RegionEndpoint
        };

        var client = new AmazonS3ControlClient(config);

        var response = await client.ListRegionalBucketsAsync(new
 ListRegionalBucketsRequest()
```

```
        {
            AccountId = "012345678910"
        });
    }
}
```

Obter um bucket

O exemplo a seguir obtém um armazenamento compatível com o Amazon S3 no bucket de dispositivos da Família Snow usando o AWS CLI. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3control get-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte get-bucket na Referência de comandos do AWS CLI .

O exemplo a seguir do armazenamento compatível com Amazon S3 em dispositivos da Família Snow obtém um bucket usando o SDK para Java. Para obter mais informações, consulte GetBucket na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucket(String bucketName) {

    GetBucketRequest reqGetBucket = new GetBucketRequest()
            .withBucket(bucketName)
            .withAccountId(AccountId);

    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);
    System.out.printf("GetBucket Response: %s%n", respGetBucket.toString());
}
```

Excluir um bucket

> **Important**
>
> - Aquele Conta da AWS que cria o bucket o possui e é o único que pode excluí-lo.
> - Os buckets de dispositivos da Família Snow devem estar vazios antes de serem excluídos.
> - Você não pode recuperar um bucket depois que ele foi excluído.

O exemplo a seguir exclui um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow usando o AWS CLI. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3control delete-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte delete-bucket na Referência de comandos do AWS CLI .

Como trabalhar com objetos do S3 em um dispositivo Snowball Edge

Esta seção descreve várias operações que você pode realizar com objetos no armazenamento compatível com Amazon S3 em dispositivos da Família Snow.

Copie um objeto para um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow

O exemplo a seguir carrega um arquivo chamado *sample-object.xml* em um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow para o qual você tem permissões de gravação para usar o AWS CLI. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3api put-object --bucket sample-bucket --key sample-object.xml --body sample-
object.xml --profile your-profile --endpoint-url s3api-endpoint-ip
```

O exemplo a seguir do armazenamento compatível com Amazon S3 em dispositivos da Família Snow copia um objeto para um novo objeto no mesmo bucket usando o SDK para Java. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
add : import java.io.IOException;

public class CopyObject {
    public static void main(String[] args) {
        String bucketName = "*** Bucket name ***";
        String sourceKey = "*** Source object key ***";
        String destinationKey = "*** Destination object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(sourceKey,
 destinationKey);
            s3Client.copyObject(copyObjectRequest);
            CopyObjectRequest copyObjectRequest = CopyObjectRequest.builder()
                    .sourceKey(sourceKey)
                    .destinationKey(destKey)
                    .build();
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Obter um objeto de um bucket

O exemplo a seguir obtém um objeto chamado *sample-object.xml* de um armazenamento compatível com Amazon S3 no bucket de dispositivos da família Snow usando o AWS CLI. O comando do SDK é `s3-snow:GetObject`. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3api get-object --bucket sample-bucket --key sample-object.xml --profile your-
profile --endpoint-url s3api-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte get-object na Referência de comandos da AWS CLI .

O exemplo a seguir do armazenamento compatível com Amazon S3 em dispositivos da Família Snow obtém um objeto usando o SDK para Java. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações. Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String bucketName = "*** Bucket name ***";
        String key = "*** Object key ***";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
```

```
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();
            GetObjectRequest getObjectRequest = GetObjectRequest.builder()
                    .bucket(bucketName)
                    .key(key)
                    .build());

s3Client.getObject(getObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        } finally {
            // To ensure that the network connection doesn't remain open, close any
 open input streams.
            if (fullObject != null) {
                fullObject.close();
            }
            if (objectPortion != null) {
                objectPortion.close();
            }
            if (headerOverrideObject != null) {
                headerOverrideObject.close();
            }
        }
    }

    private static void displayTextInputStream(InputStream input) throws IOException {
        // Read the text input stream one line at a time and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line = null;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

Listar objetos em um bucket

O exemplo a seguir lista objetos em um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow usando o AWS CLI. O comando do SDK é `s3-snow:ListObjectsV2`. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3api list-objects-v2 --bucket sample-bucket --profile your-profile --endpoint-
url s3api-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte list-objects-v2 na Referência de AWS CLI comandos.

O exemplo a seguir do armazenamento compatível com Amazon S3 em dispositivos da Família Snow lista objetos em um bucket usando o SDK para Java. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

Este exemplo usa a ListObjectsV2, que é a revisão mais recente da operação da ListObjects API. Recomendamos que você use essa operação de API revisada para o desenvolvimento de aplicações. Para compatibilidade com versões anteriores, o Amazon S3 continua a oferecer suporte à versão anterior desta operação de API.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {

    public static void main(String[] args) {
        String bucketName = "*** Bucket name ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
```

```
                    .build();

            System.out.println("Listing objects");

            // maxKeys is set to 2 to demonstrate the use of
            // ListObjectsV2Result.getNextContinuationToken()
            ListObjectsV2Request req = new
 ListObjectsV2Request().withBucketName(bucketName).withMaxKeys(2);
            ListObjectsV2Result result;

            do {
                result = s3Client.listObjectsV2(req);

                for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
                    System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
 objectSummary.getSize());
                }
                // If there are more than maxKeys keys in the bucket, get a
 continuation token
                // and list the next objects.
                String token = result.getNextContinuationToken();
                System.out.println("Next Continuation Token: " + token);
                req.setContinuationToken(token);
            } while (result.isTruncated());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Excluir objetos em um bucket

É possível excluir um ou mais objetos de um armazenamento compatível com Amazon S3 no bucket de dispositivos da Família Snow. O exemplo a seguir exclui um objeto chamado *`sample-object.xml`* usando o AWS CLI. Para usar este comando, substitua cada espaço reservado para entrada do usuário por suas próprias informações.

```
aws s3api delete-object --bucket sample-bucket --key key --profile your-profile --
endpoint-url s3api-endpoint-ip
```

Para obter mais informações sobre esse comando, consulte delete-object na Referência de comandos do AWS CLI .

O exemplo a seguir do armazenamento compatível com o Amazon S3 em dispositivos da Família Snow exclui um objeto de um bucket usando o SDK para Java. Para usar este exemplo, especifique o nome principal para o objeto que você deseja excluir. Para obter mais informações, consulte DeleteObjecta Referência de API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String bucketName = "*** Bucket name ***";
        String keyName = "*** key name ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            DeleteObjectRequest deleteObjectRequest = DeleteObjectRequest.builder()
                    .bucket(bucketName)
                    .key(keyName)
                    .build()));
            s3Client.deleteObject(deleteObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
```

```
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Ações de API REST suportadas para armazenamento compatível com o Amazon S3 em dispositivos da Família Snow

As listas a seguir mostram as operações de API suportadas pelo armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, incluindo links para as operações relacionadas do Amazon S3 em Regiões da AWS.

Operações de API de bucket compatíveis

- CreateBucket
- DeleteBucket
- DeleteBucketLifecycle
- GetBucket
- GetBucketLifecycleConfiguration
- ListBuckets
- PutBucketLifecycleConfiguration

Operações de API de objeto compatíveis

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetObject
- GetObjectTagging

- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListParts
- PutObject
- PutObjectTagging
- UploadPart
- UploadPartCopy

Visão geral de clustering

Para o AWS Snowball serviço, um cluster é um coletivo de dispositivos Snowball Edge usados como uma única unidade lógica para fins de armazenamento e computação locais.

Um cluster oferece dois benefícios principais em comparação com um dispositivo Snowball Edge independente para fins de armazenamento e computação locais:

- Maior durabilidade: os dados armazenados em um cluster de dispositivos Snowball Edge têm maior durabilidade em comparação com um único dispositivo. Além disso, os dados no cluster permanecem tão seguros e viáveis quanto anteriormente, apesar de possíveis interrupções do Snowball Edge no cluster. Os clusters podem suportar a perda de um dispositivo em clusters de 3 e 4 dispositivos e até dois dispositivos em clusters de 5 a 16 dispositivos antes que os dados estejam em perigo. Você também pode adicionar ou substituir nós.
- Maior armazenamento — Com os dispositivos otimizados de armazenamento do Snowball Edge, você pode criar um único cluster de 16 nós com até 2,6 PB de capacidade de armazenamento utilizável compatível com S3. Com os dispositivos otimizados para computação do Snowball Edge, você pode criar um único cluster de 16 nós de até 501 TB de capacidade de armazenamento utilizável compatível com S3.

Armazenamento compatível com Amazon S3 em dispositivos da Família Snow, tolerância a falhas de cluster e capacidade de armazenamento

Tamanho do cluster	Tolerância a falhas	Capacidade de armazenamento dos dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen1, HDD e GPU opcional)	Capacidade de armazenamento dos dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen2 e NVMe)	Capacidade de armazenamento dos dispositivos de 210 TB otimizados para armazenamento do Snowball Edge
3	Perda de até 1 nó	83	38	438
4	Perda de até 1 nó	125	57	657
5	Perda de até 2 nós	125	57	657
6	Perda de até 2 nós	167	76	904
7	Perda de até 2 nós	209	95	1096
8	Perda de até 2 nós	250	114	1315
9	Perda de até 2 nós	292	133	1534
10	Perda de até 2 nós	334	152	1754

Tamanho do cluster	Tolerância a falhas	Capacidade de armazenamento dos dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen1, HDD e GPU opcional)	Capacidade de armazenamento dos dispositivos Snowball Edge otimizado para computação (com AMD EPYC Gen2 e NVMe)	Capacidade de armazenamento dos dispositivos de 210 TB otimizados para armazenamento do Snowball Edge
11	Perda de até 2 nós	370	165	1970
12	Perda de até 2 nós	376	171	1973
13	Perda de até 2 nós	418	190	2192
14	Perda de até 2 nós	459	209	2411
15	Perda de até 2 nós	495	225	2625
16	Perda de até 2 nós	501	228	2631

Um cluster de dispositivos Snowball Edge é composto de nós sem líderes. Qualquer nó pode gravar e ler dados de todo o cluster, e todos os nós são capazes de realizar o behind-the-scenes gerenciamento do cluster.

Quoruns de clusters do Snowball Edge

Um quorum representa o número mínimo de dispositivos Snowball Edge em um cluster que devem se comunicar entre si para manter um quorum de leitura/gravação.

Vamos supor que você fez upload de seus dados em um cluster de dispositivos Snowball Edge. Com todos os dispositivos saudáveis, você tem um quorum de leitura/gravação para seu cluster. Se um ou dois desses nós ficar offline, você reduzirá a capacidade operacional do cluster. No entanto, você ainda pode ler e gravar no cluster. Por isso, com o cluster operando todos os nós com exceção de um ou dois, ele ainda tem um quorum de leitura/gravação. O número de nós que podem ficar off-line antes que a capacidade operacional do cluster seja afetada é encontrado em this table.

Finalmente, o quorom pode ser violado se um cluster perder mais do que o número de nós indicado em this table. Se isso acontecer, o cluster fica off-line, e os dados no cluster se tornam indisponíveis. Você pode corrigir isso, ou os dados podem ser permanentemente perdidos, dependendo da gravidade do evento. Se for um evento temporário de alimentação externa e você conseguir ligar os três dispositivos Snowball Edge novamente e desbloquear todos os nós do cluster, seus dados ficarão disponíveis novamente.

> **Important**
>
> Se não existir um quorum mínimo de nós saudáveis, entre em contato com o AWS Support.

É possível determinar o estado de quórum do cluster. Para isso, basta determinar o estado de bloqueio do nó e a acessibilidade da rede. O comando `snowballEdge describe-cluster` informa o estado de bloqueio e de acessibilidade da rede para cada nó de um cluster desbloqueado. Garantir que os dispositivos no cluster estejam íntegros e conectados é uma responsabilidade administrativa que você assume ao criar o trabalho de cluster. Para obter mais informações sobre os diversos comandos de cliente, consulte Comandos para o Snowball Edge Client.

Considerações sobre trabalhos de cluster para dispositivos Snowball Edge

Lembre-se das seguintes considerações ao planejar usar um cluster de Snowball Edge:

- Recomendamos que você tenha uma fonte de alimentação redundante para reduzir possíveis problemas de desempenho e estabilidade do cluster.
- Assim como ocorre com trabalhos de computação e armazenamento locais autônomos, os dados armazenados em um cluster não podem ser importados para o Amazon S3 sem solicitar dispositivos adicionais como parte de trabalhos de importação separados. Se você solicitar dispositivos adicionais como trabalhos de importação, poderá transferir os dados do cluster para os dispositivos de trabalho de importação.

- Para inserir dados em um cluster do Amazon S3, crie um trabalho de exportação separado e copie os dados dos dispositivos do trabalho de exportação para o cluster.
- Você pode criar um trabalho de cluster a partir do console AWS CLI, do ou de um dos AWS SDKs. Para obter uma descrição guiada da criação de um trabalho, consulte Conceitos básicos.
- Os nós de cluster têm IDs de nó. A ID do nó é igual à ID do trabalho de um dispositivo que você pode obter do console, do AWS CLI, dos AWS SDKs e do cliente Snowball Edge. Você pode usar IDs de nó para remover nós de cluster antigos. Para obter uma lista de IDs de nós, use o comando `snowballEdge describe-device` em um dispositivo desbloqueado ou o `describe-cluster` em um cluster desbloqueado.
- A duração de um cluster é limitada pelo certificado de segurança concedido a dispositivos do cluster quando o cluster é provisionado. Por padrão, os dispositivos Snowball Edge podem ser usados por até 360 dias antes de serem retornados. Ao final desse tempo, os dispositivos param de responder às solicitações de leitura/gravação. Se você precisar manter um ou mais dispositivos por mais de 360 dias, entre em contato AWS Support.
- Ao AWS receber um dispositivo devolvido que fazia parte de um cluster, realizamos uma eliminação completa do dispositivo. Esse apagamento segue as normas 800-88 do National Institute of Standards and Technology (NIST - Instituto Nacional de Normas e Tecnologias).

Administração de um cluster

Leitura e gravação de dados em um cluster

Depois de desbloquear um cluster, você estará pronto para armazenar e acessar dados nesse cluster. Você pode usar o endpoint compatível com Amazon S3 para ler e gravar dados em um cluster.

Para ler e gravar dados em um cluster, você deve ter um quorum de leitura/gravação com, no máximo, o número de nós indisponíveis permitidos no cluster de dispositivos.

Reconexão de um nó de cluster indisponível

Um nó, ou dispositivo dentro de um cluster, pode se tornar temporariamente indisponível devido a um problema, como perda de energia ou de rede, sem danificar os dados no nó. Quando isso acontece, o status de seu cluster é afetado. O status de bloqueio e acessibilidade da rede de um nó é informado no Snowball Edge com o comando `snowballEdge describe-cluster`.

Recomendamos que você posicione fisicamente seu cluster para que tenha acesso às partes frontal, traseira e superior de todos os nós. Dessa forma, você pode acessar os cabos de alimentação e de

rede na parte traseira, as etiquetas de envio na parte superior para obter as IDs do nó e as telas LCD na parte frontal dos dispositivos para obter os endereços IP e outras informações administrativas.

Quando você detectar que um nó está indisponível, recomendamos tentar um dos seguintes procedimentos, dependendo do cenário que causou a indisponibilidade do nó.

Para reconectar um nó indisponível

1. Verifique se o nó está ligado.
2. Certifique-se de que o nó esteja conectado à mesma rede interna que o restante do cluster ao qual ele está conectado.
3. Se você precisar ligar o nó, espere até 20 minutos para que ele termine.
4. Execute o comando `snowballEdge unlock-cluster` ou o comando `snowballEdge associate-device`. Por exemplo, consulte Desbloqueio de dispositivos Snowball Edge.

Para reconectar um nó indisponível que perdeu a conectividade da rede, mas não foi desligado

1. Certifique-se de que o nó esteja conectado à mesma rede interna que o resto do cluster.
2. Execute o comando `snowballEdge describe-device` para ver quando o nó indisponível anteriormente é readicionado ao cluster. Por exemplo, consulte Como obter o status do dispositivo.

Depois de você executar os procedimentos anteriores, seus nós deverão funcionar normalmente. Você também deve ter um quorum de leitura/gravação. Se esse não for o caso, um ou mais dos seus nós podem ter um problema mais sério e talvez seja necessário removê-los do cluster.

Como adicionar ou substituir um nó em um cluster

Você pode adicionar um novo nó depois remover um nó não íntegro de um cluster. Você também pode adicionar um novo nó para aumentar o armazenamento local.

Para adicionar um novo nó, primeiro você precisa solicitar uma substituição. Você pode solicitar um nó de substituição no console AWS CLI, no ou em um dos AWS SDKs. Se estiver solicitando um nó de substituição do console, poderá solicitar substituições para qualquer trabalho que ainda não tenha sido cancelado nem concluído.

Para solicitar um nó de substituição no console

1. Faça login no Console de Gerenciamento da família AWS Snow.

2. Encontre e escolha um trabalho para um nó que pertença ao cluster que você criou no painel de trabalho.
3. Em Ações, escolha Substituir nó.

   Ao fazer isso, é aberta a etapa final do assistente de criação de trabalho, com todas as configurações idênticas à forma como o cluster foi criado originalmente.
4. Escolha Criar trabalho.

Seu Snowball Edge de substituição agora está a caminho. Quando ele chegar, use o procedimento a seguir para adicioná-lo ao seu cluster.

Para adicionar um nó de substituição

1. Posicione o novo nó do cluster, de forma que você tenha acesso às partes frontal, traseira e superior de todos os nós.
2. Certifique-se de que o nó tenha energia.
3. Certifique-se de que o nó esteja conectado à mesma rede interna que o resto do cluster.
4. Aguarde até que o nó seja ligado (se for necessário ligá-lo).
5. Execute o comando `snowballEdge associate-device`. Para ver um exemplo, consulte Como adicionar um nó a um cluster.

Configuração do armazenamento compatível com o Amazon S3 em dispositivos da Família Snow: notificações de eventos

O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow oferece suporte às notificações de eventos do Amazon S3 para chamadas de API de objetos com base no protocolo MQTT.

Você pode usar armazenamento compatível com Amazon S3 em dispositivos da Família Snow para receber notificações quando determinados eventos acontecerem no bucket do S3. Para habilitar notificações, adicione uma configuração de notificação que identifique os eventos que deseja que o serviço publique.

O armazenamento compatível com Amazon S3 em dispositivos da Família Snow suporta os seguintes tipos de notificação:

- Eventos de criação de novos objetos

- Eventos de remoção de objetos
- Eventos de marcação de objetos

Configurar notificações de eventos do Amazon S3

1. Antes de começar, é necessário ter uma infraestrutura do MQTT na sua rede.
2. No seu Snowball Edge Client, execute o comando `snowballEdge configure` para configurar o dispositivo Snowball Edge.

   Quando solicitado, forneça as seguintes informações:

   - O caminho até o seu arquivo manifesto.
   - O código de desbloqueio do dispositivo.
   - O endpoint do dispositivo (por exemplo, **`https://10.0.0.1`**).
3. Execute o comando `put-notification-configuration` a seguir para enviar notificações a um atendente externo.

   ```
   snowballEdge put-notification-configuration --broker-endpoint ssl://mqtt-broker-ip-address:8883 --enabled true --service-id s3-snow --ca-certificate file:path-to-mqtt-broker-ca-cert
   ```
4. Execute o comando `get-notification-configuration` a seguir para verificar se tudo está configurado corretamente:

   ```
   snowballEdge get-notification-configuration --service-id s3-snow
   ```

   Isso retorna o endpoint do atendente e o campo ativado.

Depois de configurar todo o cluster para enviar notificações ao atendente MQTT na rede, cada chamada de API de objeto resultará em uma notificação de evento.

> **Note**
>
> Você precisa se inscrever no tópico s3SnowEvents/ID do *`dispositivo (ou ID`* do *`cluster`*, se for um cluster) /bucketName. Você também pode usar curingas, por exemplo, o nome do tópico pode ser *`#`* ou *`s3 SnowEvents /#`*.

A seguir está um exemplo de registro de eventos de armazenamento compatível com Amazon S3 em dispositivos da Família Snow:


```
{
"eventDetails": {
"additionalEventData": {
"AuthenticationMethod": "AuthHeader",
"CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"SignatureVersion": "SigV4",
"bytesTransferredIn": 1205,
"bytesTransferredOut": 0,
"x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg=="
},
"eventName": "PutObject",
"eventTime": "2023-01-30T14:13:24.772Z",
"requestAuthLatencyMillis": 40,
"requestBandwidthKBs": 35,
"requestID": "140CD93455CB62B4",
"requestLatencyMillis": 77,
"requestLockLatencyNanos": 1169953,
"requestParameters": {
"Content-Length": "1205",
"Content-MD5": "GZdTUOhYHvHgQgmaw2gl4w==",
"Host": "10.0.2.251",
"bucketName": "buckett",
"key": "file-key"
},
"requestTTFBLatencyMillis": 77,
"responseElements": {
"ETag": ""19975350e8581ef1e042099ac36825e3"",
"Server": "AmazonS3",
"x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg==",
"x-amz-request-id": "140CD93455CB62B4"
},
"responseStatusCode": 200,
"sourceIPAddress": "172.31.37.21",
"userAgent": "aws-cli/1.27.23 Python/3.7.16 Linux/4.14.301-224.520.amzn2.x86_64
 botocore/1.29.23",
"userIdentity": {
"identityType": "IAMUser",
"principalId": "531520547609",
"arn": "arn:aws:iam::531520547609:root",
```

```
"userName": "root"
}
}
}
```

Para obter mais informações sobre notificações de eventos do Amazon S3, consulte Notificações de eventos do Amazon S3.

Configuração de notificações SMTP locais

Você pode configurar notificações locais para seus dispositivos Snowball Edge com Simple Mail Transfer Protocol (SMTP). As notificações locais enviam e-mails aos servidores configurados quando o estado do serviço (ativo, degradado, inativo) muda ou se você ultrapassa os limites de utilização da capacidade de 80%, 90% ou 100%.

Pré-requisitos

Antes de começar, confirme se:

- Você tem acesso ao cliente mais recente do Snowball Edge.
- Seu dispositivo está desbloqueado e pronto para uso.
- Seu dispositivo pode se conectar à Internet (se estiver usando o Amazon Simple Email Service ou um servidor SMTP externo) ou a um servidor SMTP local.

Configuração do dispositivo

Configure seu dispositivo para enviar notificações por e-mail.

Para configurar o dispositivo para notificações SMTP

1. Execute o comando a seguir para adicionar uma configuração SMTP ao seu dispositivo:

```
# If you don't specify a port, port 587 is the default.
SMTP_ENDPOINT=your-local-smtp-server-endpoint:port

# For multiple email recepients, separate with commas
RECIPIENTS_LIST=your-email-address

snowballEdge put-notification-configuration \
```

```
  --service-id local-monitoring \
  --enabled true \
  --type smtp \
  --broker-endpoint "$SMTP_ENDPOINT" \
  --sender example-sender@domain.com \
  --recipients "$RECIPIENTS_LIST"
```

Você receberá um e-mail de teste de example-sender@domain.com se for bem-sucedido.

2. Teste a configuração executando o comando `get-notification-configuration` a seguir:

```
snowballEdge get-notification-configuration \
  --service-id local-monitoring
```

A resposta não inclui uma senha ou certificado, mesmo que você os forneça.

Monitoramento remoto para armazenamento compatível com Amazon S3 em dispositivos da Família Snow

O monitoramento remoto permite AWS monitorar o armazenamento compatível com o Amazon S3 em dispositivos da família Snow em dispositivos Snowball Edge conectados a um. Região da AWS Quando o monitoramento remoto está ativado, ele aciona carregamentos periódicos de registros de serviços para o. Região da AWS AWS monitora essas informações e pode notificá-lo proativamente quando detectamos problemas com o serviço. Quando o monitoramento remoto não estiver ativado ou se o dispositivo ou cluster do Snowball Edge não estiver conectado a um Região da AWS, o serviço de monitoramento remoto não tentará publicar a telemetria interna do dispositivo ou do serviço na nuvem. O monitoramento remoto está disponível para dispositivos Snowball Edge autônomos e clusters de dispositivos Snowball Edge.

> **Note**
>
> O monitoramento remoto só permite o monitoramento do armazenamento compatível com Amazon S3 no serviço de dispositivos da família Snow no momento.

Você pode usar o `describe-features` comando para ver se o serviço de monitoramento remoto está em execução ou não. Para obter mais informações, consulte Verificando o status do recurso neste guia.

Para habilitar o monitoramento remoto para um dispositivo autônomo

- Use o `set-features` comando e defina o valor do `remote-monitoring-state` parâmetro como`INSTALLED_AUTOSTART`.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-local-ip
```

> **Note**
>
> Para obter mais informações sobre o arquivo de manifesto e o código de desbloqueio do dispositivo Snow Family, consulte Como obter suas credenciais e ferramentas neste guia.

O comando retorna o seguinte:

```
{
    "RemoteMonitoringState" : INSTALLED_AUTOSTART
}
```

Para habilitar o monitoramento remoto para um cluster de dispositivos

- Use o `set-features` comando e defina o valor do `remote-monitoring-state` parâmetro `INSTALLED_AUTOSTART` para cada dispositivo da família Snow no cluster.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-1-local-ip
```

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-2-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_AUTOSTART
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-3-local-ip
```

> **Note**
>
> Para obter mais informações sobre o arquivo de manifesto e o código de desbloqueio do dispositivo Snow Family, consulte Como obter suas credenciais e ferramentas neste guia.

Cada vez que você executa o comando, ele retorna o seguinte.

```
{
    "RemoteMonitoringState" : INSTALLED_AUTOSTART
}
```

Para desativar o monitoramento remoto para um dispositivo autônomo

- Use o `set-features` comando e defina o valor do `remote-monitoring-state` parâmetro como`INSTALLED_ONLY`. O dispositivo Snow Family não carregará mais registros periodicamente e não AWS monitorará nem notificará você se ocorrerem problemas com o serviço enquanto o monitoramento remoto estiver desativado.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-local-ip
```

O comando retorna o seguinte:

```
{
    "RemoteMonitoringState" : INSTALLED_ONLY
}
```

Para desativar o monitoramento remoto para um cluster de dispositivos

- Use o `set-features` comando e defina o valor do `remote-monitoring-state` parâmetro `INSTALLED_ONLY` para cada dispositivo da família Snow no cluster.

```
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-1-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-2-local-ip
snowballEdge set-features /
  --remote-monitoring-state INSTALLED_ONLY
  --manifest-file path/to/manifest.bin
  --unlock-code unlock-code
  --endpoint https://snow-device-3-local-ip
```

Cada vez que você executa o comando, ele retorna o seguinte.

```
{
    "RemoteMonitoringState" : INSTALLED_ONLY
}
```

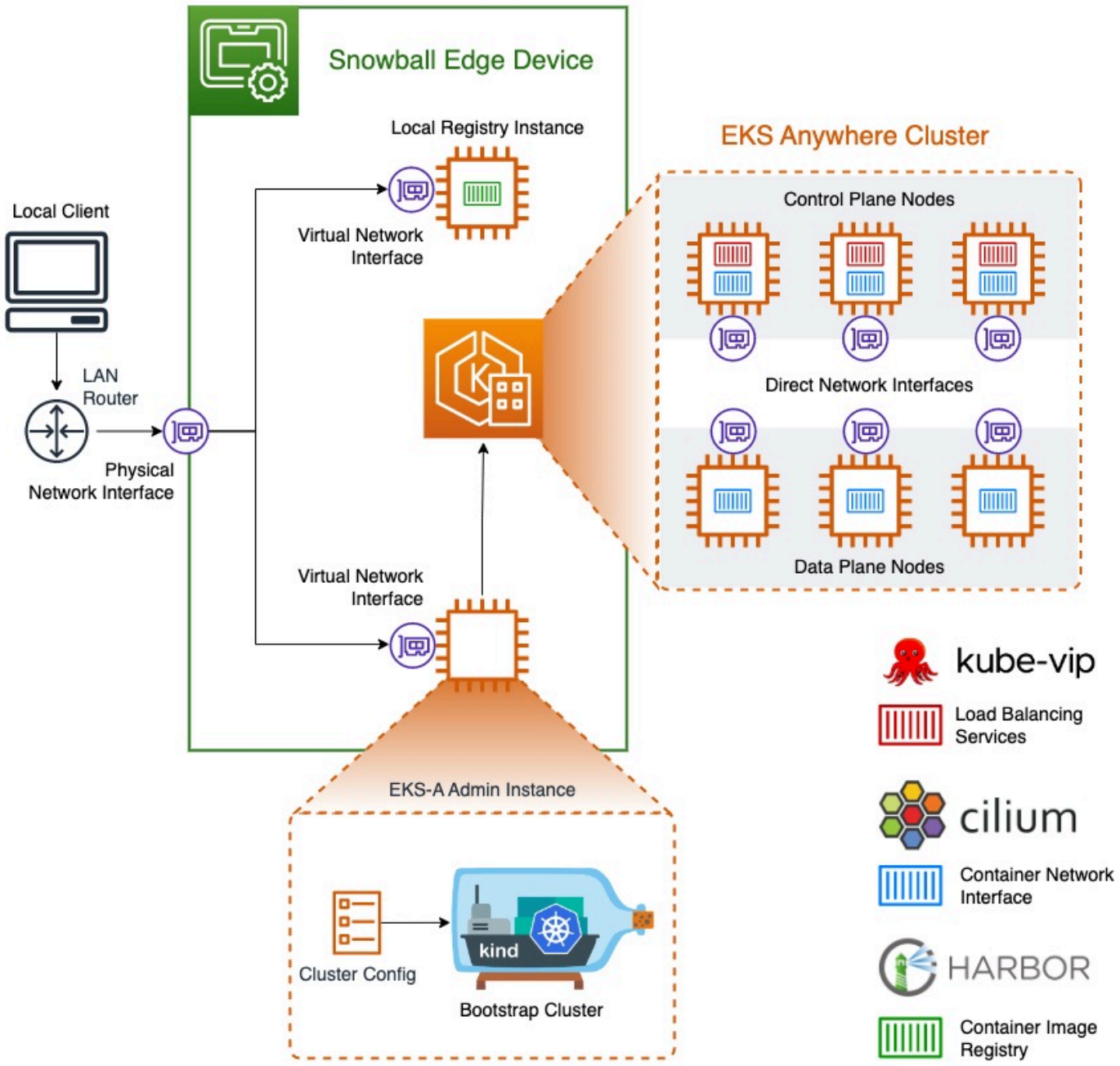
Usando o Amazon EKS Anywhere on AWS Snow

O Amazon EKS Anywhere on AWS Snow ajuda você a criar e operar clusters Kubernetes em dispositivos da família Snow. O Kubernetes é um software de código aberto usado para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres. Você pode usar o Amazon EKS Anywhere em um dispositivo Snowball Edge com ou sem uma conexão de rede externa. Para usar o Amazon EKS Anywhere em um dispositivo sem uma conexão de rede externa, forneça um registro de contêiner para ser executado no dispositivo Snowball Edge. Para obter informações gerais sobre o Amazon EKS Anywhere, consulte a documentação do Amazon EKS Anywhere.

O uso do Amazon EKS Anywhere on AWS Snow fornece os seguintes recursos:

- Provisione um cluster Kubernetes (K8s) com o CLI do Amazon EKS Anywhere (eksctl anywhere) em dispositivos do Snowball Edge otimizado para computação. Você pode provisionar o Amazon EKS Anywhere em um único dispositivo Snowball Edge ou em três ou mais dispositivos para obter alta disponibilidade.
- Suporte para Cilium Container Network Interface (CNI).
- Support para Ubuntu 20.04 como sistema operacional de nó.

Esse diagrama ilustra um cluster do Amazon EKS Anywhere implantado em um dispositivo Snowball Edge.



Recomendamos que você crie seu cluster Kubernetes com a versão mais recente disponível do Kubernetes suportada pelo Amazon EKS Anywhere. Para obter mais informações, consulte Controle de versão do Amazon EKS-Anywhere. Se seu aplicativo exigir uma versão específica do Kubernetes, use qualquer versão do Kubernetes oferecida no suporte padrão ou estendido pelo Amazon EKS. Considere as datas de lançamento e suporte das versões do Kubernetes ao planejar o ciclo de vida de sua implantação. Isso ajudará você a evitar a possível perda de suporte para a versão

do Kubernetes que você pretende usar. Para obter mais informações, consulte o calendário de lançamento do Amazon EKS Kubernetes.

Para obter mais informações sobre o Amazon EKS Anywhere on AWS Snow, consulte a documentação do Amazon EKS Anywhere.

Tópicos

Ações a serem concluídas antes de comprar um dispositivo Snowball Edge para o Amazon EKS Anywhere on Snow AWS

No momento, o Amazon EKS Anywhere é compatível com o Snowball Edge otimizado para computação e otimizado para computação com dispositivos de unidade de processamento gráfico (GPU). Antes de comprar um dispositivo Snowball Edge, há algumas coisas que você deve fazer para se preparar.

- Crie e forneça uma imagem do sistema operacional para usar na criação de máquinas virtuais no dispositivo.
- Sua rede deve ter um endereço IP estático disponível para o endpoint do plano de controle K8s e permitir o Protocolo de Resolução de Endereço (ARP).
- Seu dispositivo Snowball Edge deve ter portas específicas abertas. Para obter mais informações sobre portas, consulte Portas e protocolos na documentação do Amazon EKS Anywhere.

Tópicos

Crie uma AMI da distribuição Ubuntu EKS

Para criar a AMI da distribuição Ubuntu EKS, consulte Criar imagens de nós do Snow.

O nome da AMI gerada seguirá o padrão `capa-ami-ubuntu-20.04-version-timestamp`. Por exemplo, `capa-ami-ubuntu-20.04-v1.24-1672424524`.

Crie uma AMI Harbor

Configure uma AMI de registro privado do Harbor para incluir no dispositivo Snowball Edge para que você possa usar o Amazon EKS Anywhere no dispositivo sem uma conexão de rede externa. Se você não usar o Amazon EKS Anywhere enquanto o dispositivo Snowball Edge estiver desconectado da rede externa, ou se tiver um registro privado do Kubernetes em uma AMI para usar no dispositivo, pule esta seção.

Para criar a AMI do registro local do Harbor, consulte Criar uma AMI do Harbor.

Solicitando um dispositivo Snowball Edge para uso com o Amazon EKS Anywhere on Snow AWS

Para solicitar que seu Snowball Edge seja otimizado para computação ou para computação otimizada com dispositivo de GPU, consulte Criando um trabalho para solicitar um dispositivo da família Snow neste guia e lembre-se desses itens durante o processo de pedido:

- Na etapa 1, escolha o tipo de tarefa Somente computação e armazenamento locais.
- Na etapa 2, escolha o tipo de dispositivo Snowball Edge otimizado para computação ou Snowball Edge otimizado para computação com GPU.
- Na etapa 3, escolha Amazon EKS Anywhere on AWS Snow e escolha a versão do Kubernetes de que você precisa.

> **Note**
>
> Para fornecer o software mais recente, podemos configurar o dispositivo com uma versão do ESK Anywhere mais recente do que a que está disponível atualmente. Para obter mais informações, versionamento no Guia do usuário do Amazon EKS.
> Recomendamos que você crie seu cluster Kubernetes com a versão mais recente disponível do Kubernetes suportada pelo Amazon EKS Anywhere. Para obter mais informações, consulte Controle de versão do Amazon EKS-Anywhere. Se seu aplicativo

exigir uma versão específica do Kubernetes, use qualquer versão do Kubernetes oferecida no suporte padrão ou estendido pelo Amazon EKS. Considere as datas de lançamento e suporte das versões do Kubernetes ao planejar o ciclo de vida de sua implantação. Isso ajudará você a evitar a possível perda de suporte para a versão do Kubernetes que você pretende usar. Para obter mais informações, consulte o calendário de lançamento do Amazon EKS Kubernetes.

- Escolha AMIs para incluir em seu dispositivo, incluindo a AMI da distribuição do EKS (consulte Crie uma AMI da distribuição Ubuntu EKS) e, opcionalmente, a AMI do Harbor que você criou (consulte Crie uma AMI Harbor).
- Se você precisar de vários dispositivos Snowball Edge para obter alta disponibilidade, escolha o número de dispositivos necessários em Alta disponibilidade.

Depois de receber seu dispositivo ou dispositivos Snowball Edge, configure o Amazon EKS Anywhere de acordo com Configuração e execução do Amazon EKS Anywhere em dispositivos Snowball Edge.

Configuração e execução do Amazon EKS Anywhere em dispositivos Snowball Edge

Siga esses procedimentos para configurar e iniciar o Amazon EKS Anywhere em seus dispositivos Snowball Edge. Em seguida, para configurar o Amazon EKS Anywhere para operar em dispositivos desconectados, conclua procedimentos adicionais antes de desconectar esses dispositivos da rede externa. Para ter mais informações, consulte Configuração do Amazon EKS Anywhere on AWS Snow para operação desconectada.

Tópicos

- Configuração inicial
- Configuração e execução automática do Amazon EKS Anywhere em dispositivos Snowball Edge
- Configurando e executando o Amazon EKS Anywhere em dispositivos Snowball Edge manualmente

Configuração inicial

Execute a configuração inicial em cada dispositivo Snowball Edge conectando o dispositivo à sua rede local, baixando o Snowball Edge Client, obtendo credenciais e desbloqueando o dispositivo.

Execute a configuração inicial

1. Faça o download e instale o Snowball Edge Client. Para ter mais informações, consulte Baixar e instalar o cliente do Snowball Edge.
2. Conecte o dispositivo à rede local. Para ter mais informações, consulte Conectar-se à rede local.
3. Obtenha credenciais para desbloquear seu dispositivo. Para ter mais informações, consulte Obter credenciais para acessar um dispositivo Snow Family.
4. Desbloqueie o dispositivo. Para ter mais informações, consulte Desbloqueando o dispositivo Snow Family. Você também pode usar uma ferramenta de script em vez de desbloquear dispositivos manualmente. Consulte Desbloquear dispositivos.

Configuração e execução automática do Amazon EKS Anywhere em dispositivos Snowball Edge

Você pode usar exemplos de ferramentas de script para configurar o ambiente e executar uma instância administrativa do Amazon EKS Anywhere ou pode fazer isso manualmente. Para usar as ferramentas de script, consulte Desbloquear dispositivos e ambiente de configuração para o Amazon EKS Anywhere. Depois que o ambiente estiver configurado e a instância administrativa do Amazon EKS Anywhere estiver em execução, se você precisar configurar o Amazon EKS Anywhere para operar no dispositivo Snowball Edge enquanto estiver desconectado de uma rede, consulte Configuração do Amazon EKS Anywhere on AWS Snow para operação desconectada. Caso contrário, consulte Criação e manutenção de clusters em dispositivos Snowball Edge.

Para configurar manualmente o ambiente e executar uma instância administrativa do Amazon EKS Anywhere, consulte Configurando e executando o Amazon EKS Anywhere em dispositivos Snowball Edge manualmente.

Configurando e executando o Amazon EKS Anywhere em dispositivos Snowball Edge manualmente

Tópicos

- Crie um AWS CLI perfil
- Crie um usuário local do IAM do Amazon EKS Anywhere
- (Opcional) Crie e importe uma chave Secure Shell
- Execute uma instância administrativa do Amazon EKS Anywhere e transfira arquivos de credenciais e certificados para ela

Crie um AWS CLI perfil

Crie um AWS CLI perfil para armazenar credenciais para uso durante todo o processo de configuração dos dispositivos Snowball Edge e da instância administrativa do Amazon EKS Anywhere. Para obter mais informações sobre AWS CLI perfis, consulte Perfis nomeados para o AWS CLI no Guia AWS Command Line Interface do Usuário.

Você pode usar uma ferramenta de script de amostra para criar automaticamente o AWS CLI perfil e o usuário local do IAM do Amazon EKS Anywhere. Consulte Criar arquivo de credenciais e certificados. Depois de usar o script, continue com (Opcional) Crie e importe uma chave Secure Shell. Caso contrário, siga este procedimento e, em seguida, os procedimentos em Crie um usuário local do IAM do Amazon EKS Anywhere.

> **Note**
>
> Faça isso para cada dispositivo Snowball Edge que você configurar.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge list-access-keys --endpoint
 https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-code
{
 "AccessKeyIds" : [ "xxxx" ]
}
```

Use o valor de `AccessKeyIds` como o valor do parâmetro `access-key-id` do comando `get-secret-access-key`.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge get-secret-access-key --access-key-
id ACCESS_KEY_ID --endpoint https://snowball-ip --manifest-file path-to-manifest-file
 --unlock-code unlock-code
[snowballEdge]
aws_access_key_id = xxx
aws_secret_access_key = xxx
```

Use o valor de `aws_access_key_id` e `aws_secret_access_key` como valores de `AWS Access Key ID` e `AWS Secret Access Key` do AWS CLI perfil.

```
aws configure --profile profile-name
AWS Access Key ID [None]: aws_access_key_id
AWS Secret Access Key [None]: aws_secret_access_key
Default region name [None]: snow
```

Crie um usuário local do IAM do Amazon EKS Anywhere

Para obter as melhores práticas de segurança, crie um usuário local do IAM para o Amazon EKS Anywhere no dispositivo Snowball Edge. Isso pode ser feito manualmente por meio dos procedimentos a seguir.

> **Note**
>
> Faça isso para cada dispositivo Snowball Edge que você usa.

Criar um usuário local

Use o comando `create-user` para criar o usuário IAM do Amazon EKS Anywhere.

```
aws iam create-user --user-name user-name --endpoint http://snowball-ip:6078 --
profile profile-name
    {
        "User": {
            "Path": "/",
            "UserName": "eks-a-user",
            "UserId": "AIDACKCEVSQ6C2EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/eks-a-user",
            "CreateDate": "2022-04-06T00:13:35.665000+00:00"
        }
    }
```

Crie uma política para o usuário local

Crie um documento de política, use-o para criar uma política do IAM e anexe essa política ao usuário local do Amazon EKS Anywhere.

Para criar um documento de política e anexá-lo ao usuário local do Amazon EKS Anywhere

1. Crie um documento de política e salve-o no computador. Copie a política abaixo para o documento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snowballdevice:DescribeDevice",
        "snowballdevice:CreateDirectNetworkInterface",
        "snowballdevice:DeleteDirectNetworkInterface",
        "snowballdevice:DescribeDirectNetworkInterfaces",
        "snowballdevice:DescribeDeviceSoftware"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:TerminateInstances",
        "ec2:ImportKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeImages",
        "ec2:DeleteTags"
      ],
      "Resource": ["*"]
    }
  ]
}
```

2. Use o comando `create-policy` para criar uma política do IAM com base no documento de política. O valor do parâmetro `--policy-document` deve usar o caminho absoluto para o arquivo de política. Por exemplo, `file:///home/user/policy-name.json`.

```
aws iam create-policy --policy-name policy-name --policy-document file:///home/
user/policy-name.json --endpoint http://snowball-ip:6078 --profile profile-name
{
    "Policy": {
        "PolicyName": "policy-name",
        "PolicyId":
 "ANPACEMGEZDGNBVGY3TQOJQGEZAAAABP76TE5MKAAAABCCOTR2IJ43NBTJRZBU",
        "Arn": "arn:aws:iam::123456789012:policy/policy-name",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-04-06T04:46:56.907000+00:00",
        "UpdateDate": "2022-04-06T04:46:56.907000+00:00"
    }
}
```

3. Use o comando `attach-user-policy` para anexar a política do IAM ao usuário local do Amazon EKS Anywhere.

```
aws iam attach-user-policy --policy-arn policy-arn --user-name user-name --endpoint
 http://snowball-ip:6078 --profile profile-name
```

Criar uma chave de acesso e um arquivo de credencial

Crie uma chave de acesso para o usuário local do IAM do Amazon EKS Anywhere. Em seguida, crie um arquivo de credencial e inclua nele os valores `AccessKeyId` e `SecretAccessKey` gerados para o usuário local. O arquivo de credencial será usado posteriormente pela instância administrativa do Amazon EKS Anywhere.

1. Use o comando `create-access-key` para criar uma chave de acesso para o usuário local do Amazon EKS Anywhere.

```
aws iam create-access-key --user-name user-name --endpoint http://snowball-ip:6078
 --profile profile-name
    {
        "AccessKey": {
```

```
            "UserName": "eks-a-user",
            "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "Status": "Active",
            "SecretAccessKey": "RTT/wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
            "CreateDate": "2022-04-06T04:23:46.139000+00:00"
        }
    }
```

2. Crie um arquivo de credencial. Nele, salve os valores `AccessKeyId` e `SecretAccessKey` no formato a seguir.

```
[snowball-ip]
aws_access_key_id = ABCDEFGHIJKLMNOPQR2T
aws_secret_access_key = AfSD7sYz/TBZtzkReBl6PuuISzJ2WtNkeePw+nNzJ
region = snow
```

> **Note**
>
> Se você estiver trabalhando com vários dispositivos Snowball Edge, a ordem das credenciais no arquivo não importa, mas as credenciais de todos os dispositivos precisam estar em um arquivo.

Criar um arquivo de certificados para a instância administrativa

A instância administrativa do Amazon EKS Anywhere precisa dos certificados dos dispositivos Snowball Edge para ser executada neles. Crie um arquivo de certificados contendo o certificado para acessar os dispositivos Snowball Edge para uso posterior pela instância administrativa do Amazon EKS Anywhere.

Para criar um arquivo de certificados

1. Use o comando `list-certificates` para obter certificados para cada dispositivo Snowball Edge que você planeja usar.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge list-certificates --endpoint
 https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-
code
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-device:::certificate/xxx",
    "SubjectAlternativeNames" : [ "ID:JID-xxx" ]
  } ]
}
```

2. Use o valor de `CertificateArn` como valor para o parâmetro `--certificate-arn` do comando `get-certificate`.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge get-certificate --certificate-arn ARN
 --endpoint https://snowball-ip --manifest-file path-to-manifest-file --unlock-
code unlock-code
```

3. Crie um arquivo de certificado de dispositivo. Coloque a saída de `get-certificate` no arquivo de certificado. A seguir, veja um exemplo de como salvar a saída.

> **Note**
>
> Se você estiver trabalhando com vários dispositivos Snowball Edge, a ordem das credenciais no arquivo não importa, mas as credenciais de todos os dispositivos precisam estar em um arquivo.

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGVla3NhIHNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXDCCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----
```

4. Repita o procedimento Crie um usuário local do IAM do Amazon EKS Anywhere para criar um usuário local do IAM para o Amazon EKS Anywhere em todos os dispositivos Snowball Edge.

(Opcional) Crie e importe uma chave Secure Shell

Use esse procedimento opcional para criar uma chave Secure Shell (SSH) para acessar todas as instâncias de nós do Amazon EKS Anywhere e importar a chave pública para todos os dispositivos Snowball Edge. Mantenha e proteja esse arquivo de chave.

Se você pular esse procedimento, o Amazon EKS Anywhere criará e importará uma chave SSH automaticamente quando for necessário. Essa chave será armazenada na instância administrativa em `${PWD}/${CLUSTER_NAME}/eks-a-id_rsa`.

Crie uma chave SSH e importe-a para a instância do Amazon EKS Anywhere

1. Use o comando `ssh-keygen` para gerar uma chave SSH.

```
ssh-keygen -t rsa -C "key-name" -f path-to-key-file
```

2. Use o comando `import-key-pair` para importar a chave do seu computador para o dispositivo Snowball Edge.

> **Note**
>
> O valor do parâmetro `key-name` deve ser o mesmo quando você importa a chave para todos os dispositivos.

```
aws ec2 import-key-pair --key-name key-name --public-key-material fileb:///path/to/
key-file --endpoint http://snowball-ip:8008 --profile profile-name
{
    "KeyFingerprint": "5b:0c:fd:e1:a0:69:05:4c:aa:43:f3:3b:3e:04:7f:51",
    "KeyName": "default",
    "KeyPairId": "s.key-85edb5d820c92a6f8"
}
```

Execute uma instância administrativa do Amazon EKS Anywhere e transfira arquivos de credenciais e certificados para ela

Execute uma instância administrativa do Amazon EKS Anywhere

Siga este procedimento para executar manualmente uma instância administrativa do Amazon EKS Anywhere, configurar uma interface de rede virtual (VNI) para a instância administrativa, verificar o status da instância, criar uma chave SSH e conectar-se à instância administrativa com ela. Você pode usar uma ferramenta de script de amostra para automatizar a criação de uma instância administrativa do Amazon EKS Anywhere e a transferência de arquivos de credenciais e certificados para essa instância. Consulte Criar instância administrativa do Amazon EKS Anywhere. Depois que a ferramenta de script for concluída, você poderá entrar por ssh na instância e criar clusters consultando a Criação e manutenção de clusters em dispositivos Snowball Edge. Se você quiser configurar a instância do Amazon EKS Anywhere manualmente, use as seguintes etapas.

> **Note**
>
> Se você estiver usando mais de um dispositivo Snowball Edge para provisionar o cluster, poderá iniciar uma instância administrativa do Amazon EKS Anywhere em qualquer um dos dispositivos do Snowball Edge.

Para executar uma instância administrativa do Amazon EKS Anywhere

1. Use o comando `create-key-pair` para criar uma chave SSH para a instância administrativa do Amazon EKS Anywhere. O comando salva a chave em `$PWD/key-file-name`.

   ```
   aws ec2 create-key-pair --key-name key-name --query 'KeyMaterial' --output text --
   endpoint http://snowball ip:8008 --profile profile-name > key-file-name
   ```

2. Use o comando `describe-images` para encontrar o nome da imagem que começa com `eks-anywhere-admin` na saída.

   ```
   aws ec2 describe-images --endpoint http://snowball-ip:8008 --profile profile-name
   ```

3. Use o comando `run-instance` para iniciar uma instância de administração eks-a com a imagem de administrador do Amazon EKS Anywhere.

```
aws ec2 run-instances --image-id eks-a-admin-image-id --key-name key-name --
instance-type sbe-c.xlarge --endpoint http://snowball-ip:8008 --profile profile-
name
```

4. Use o comando `describe-instances` para verificar o estado da instância do Amazon EKS Anywhere. Espere até que o comando indique que o estado da instância é `running` antes de continuar.

```
aws ec2 describe-instances --instance-id instance-id --endpoint http://snowball-
ip:8008 --profile profile-name
```

5. Na saída do comando `describe-device`, observe o valor de `PhysicalNetworkInterfaceId` para a interface de rede física conectada à sua rede. Isso será usado para criar uma VNI.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge describe-device --endpoint
 https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-
code
```

6. Crie uma VNI para a instância administrativa do Amazon EKS Anywhere. Use o valor de `PhysicalNetworkInterfaceId` como o valor do parâmetro `physical-network-interface-id`.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge create-virtual-network-interface
 --ip-address-assignment dhcp --physical-network-interface-id PNI --endpoint
 https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-
code
```

7. Use o valor de `IpAddress` como o valor do parâmetro `public-ip` do comando `associate-address` para associar o endereço público à instância administrativa do Amazon EKS Anywhere.

```
aws ec2 associate-address --instance-id instance-id --public-ip VNI-IP --endpoint
 http://snowball-ip:8008 --profile profile-name
```

8. Conecte-se à instância administrativa do Amazon EKS Anywhere por SSH.

```
ssh -i path-to-key ec2-user@VNI-IP
```

Transferir arquivos de certificado e credencial para a instância administrativa

Depois que a instância administrativa do Amazon EKS Anywhere estiver em execução, transfira as credenciais e os certificados dos seus dispositivos Snowball Edge para a instância administrativa. Execute o seguinte comando no mesmo diretório em que você salvou os arquivos de credenciais e certificados em Criar uma chave de acesso e um arquivo de credencial e Criar um arquivo de certificados para a instância administrativa.

```
scp -i path-to-key path-to-credentials-file path-to-certificates-file ec2-user@eks-admin-instance-ip:~
```

Verifique o conteúdo dos arquivos na instância administrativa do Amazon EKS Anywhere. Veja a seguir exemplos dos arquivos de credenciais e certificados.

```
[192.168.1.1]
aws_access_key_id = EMGEZDGNBVGY3TQOJQGEZB5ULEAAIWHWUJDXEXAMPLE
aws_secret_access_key = AUHpqjO0GZQHEYXDbN0neLNlfR0gEXAMPLE
region = snow

[192.168.1.2]
aws_access_key_id = EMGEZDGNBVGY3TQOJQGEZG5O7F3FJUCMYRMI4KPIEXAMPLE
aws_secret_access_key = kY4Cl8+RJAwq/bu28Y8fUJepwqhDEXAMPLE
region = snow
```

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGVla3NhIHNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXDCCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
```

```
...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
KJ0FPl2PAYPEjxr81/PoCXfZeARBzN9WLUH5yz1ta+sYUJouzhzWuLJYA1xqcCPY
mhVlkRsN4hVdlBNRnCCpRF766yjdJeibKVzXQxoXoZBjrOkuGwqRy3d3ndjK77h4
OR5Fv9mjGf7CjcaSjk/4iwmZvRSaQacb0YG5GVeb4mfUAuVtuFoMeYfnAgMBAAGj
azBpMAwGA1UdEwQFMAMBAf8wHQYDVR0OBBYEFL/bRcnBRuSM5+FcYFa8HfIBomdF
...
-----END CERTIFICATE-----
```

Configuração do Amazon EKS Anywhere on AWS Snow para operação desconectada

Conclua essa configuração adicional do Amazon EKS Anywhere no dispositivo Snowball Edge enquanto ele estiver conectado a uma rede para preparar o Amazon EKS Anywhere para ser executado em um ambiente sem uma conexão de rede externa.

Para configurar o Amazon EKS Anywhere para uso desconectado com seu próprio registro local e privado do Kubernetes, consulte Configuração do espelho do registro na documentação do EKS Anywhere.

Se você criou uma AMI de registro privado do Harbor, siga os procedimentos nesta seção.

Tópicos

- Configurar o registro do Harbor em um dispositivo Snowball Edge
- Use o registro Harbor na instância administrativa do Amazon EKS Anywhere

Configurar o registro do Harbor em um dispositivo Snowball Edge

Consulte Configurar o Harbor em um dispositivo Snowball Edge.

Use o registro Harbor na instância administrativa do Amazon EKS Anywhere

Consulte Importar imagens de contêineres do Amazon EKS Anywhere para o registro local do Harbor em um dispositivo Snowball Edge.

Criação e manutenção de clusters em dispositivos Snowball Edge

Práticas recomendadas para criar clusters

Para criar um cluster do Amazon EKS Anywhere, consulte Create Snow clusters.

Lembre-se das seguintes melhores práticas ao criar clusters do Amazon EKS Anywhere em dispositivos Snowball Edge:

- Antes de criar um cluster em um intervalo de endereços IP estáticos, certifique-se de que não haja outros clusters em seu dispositivo Snowball Edge usando o mesmo intervalo de endereços IP.
- Antes de criar um cluster com endereçamento DHCP em seu dispositivo Snowball Edge, certifique-se de que todos os intervalos de endereços IP estáticos em uso para clusters não estejam na sub-rede do pool DHCP.
- Ao criar mais de um cluster, espere até que um cluster seja provisionado e executado com sucesso antes de criar outro.

Atualizando clusters

Para atualizar uma AMI de administrador do Amazon EKS Anywhere ou uma AMI de distribuição EKS, entre em contato com AWS Support. AWS Support fornecerá uma atualização do Snowball Edge contendo a AMI atualizada. Em seguida, baixe e instale a atualização do Snowball Edge. Consulte Download de atualizações e Instalação de atualizações.

Depois de atualizar sua AMI do Amazon EKS Anywhere, você precisa iniciar uma nova instância administrativa do Amazon EKS Anywhere. Consulte Execute uma instância administrativa do Amazon EKS Anywhere. Em seguida, copie os arquivos-chave, a pasta do cluster, as credenciais e os certificados da instância administrativa anterior para a instância atualizada. Eles estão em uma pasta com o nome do cluster.

Limpando os recursos do cluster

Se você criar vários clusters em seus dispositivos Snowball Edge e não os excluir corretamente ou se houver um problema no cluster e o cluster criar nós substitutos após a retomada, haverá vazamento de recursos. Uma ferramenta de script de amostra está disponível para você modificar e usar para limpar sua instância administrativa do Amazon EKS Anywhere e seus dispositivos Snowball Edge. Consulte as ferramentas de limpeza do Amazon EKS Anywhere on AWS Snow.

Usar o IAM localmente

O AWS Identity and Access Management (IAM) ajuda você a controlar com segurança o acesso aos recursos da AWS que são executados no dispositivo AWS Snowball Edge. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.

O IAM é aceito localmente no dispositivo. É possível usar o serviço local do IAM para criar usuários e anexar políticas do IAM a eles. É possível usar essas políticas para permitir o acesso necessário para realizar as tarefas atribuídas. Por exemplo, é possível permitir que um usuário transfira dados, mas limitar a sua capacidade de criar instâncias compatíveis com o Amazon EC2.

Além disso, é possível criar credenciais locais baseadas na sessão usando o AWS Security Token Service (AWS STS) no dispositivo. Para obter informações sobre o serviço do IAM, consulte Conceitos básicos no Guia do usuário do IAM.

As credenciais raiz do dispositivo não podem ser desativadas e não é possível usar políticas na conta para negar explicitamente o acesso ao usuário raiz da Conta da AWS. Recomendamos proteger as chaves de acesso do usuário raiz e criar credenciais de usuário do IAM para a interação diária com o dispositivo.

> **Important**
>
> A documentação nesta seção se aplica ao uso local do IAM em um dispositivo AWS Snowball Edge. Para obter informações sobre como usar o IAM na Nuvem AWS, consulte Identity and Access Management em AWS Snowball.
> Para que os serviços da AWS funcionem corretamente em um Snowball Edge, é necessário ativar as portas dos serviços. Para obter mais detalhes, consulte Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge.

Tópicos

- Usar a AWS CLI e as operações da API no Snowball Edge
- Lista de comandos compatíveis da AWS CLI para o IAM em um Snowball Edge
- Exemplos de política do IAM
- Exemplo de TrustPolicy

Usar a AWS CLI e as operações da API no Snowball Edge

Ao usar a AWS CLI ou as operações da API para emitir comandos do IAM, do AWS STS, do Amazon S3 e do Amazon EC2 no dispositivo Snowball Edge, é necessário especificar a `region` como "`snow`". É possível fazer isso usando `aws configure` ou dentro do próprio comando, como nos exemplos a seguir.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Ou

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> O ID de chave de acesso e a chave de acesso secreta que são usados localmente no AWS Snowball Edge não podem ser trocados com as chaves na Nuvem AWS.

Lista de comandos compatíveis da AWS CLI para o IAM em um Snowball Edge

Veja a seguir uma descrição do subconjunto de comandos e opções da AWS CLI para o IAM que são compatíveis com dispositivos Snowball Edge. Se um comando ou opção não estiver listado abaixo, não é compatível. Os parâmetros não compatíveis com comandos são anotados na descrição.

- attach-role-policy: anexa a política gerenciada especificada ao perfil determinado do IAM.
- attach-user-policy: anexa a política gerenciada especificada ao usuário determinado.

- create-access-key: cria uma chave de acesso secreta local do IAM e o ID de chave de acesso da AWS correspondente para o usuário especificado.
- create-policy: cria uma política gerenciada do IAM para o dispositivo.
- create-role: cria um perfil local do IAM para o dispositivo. Os seguintes parâmetros não são compatíveis:
  - `Tags`
  - `PermissionsBoundary`
- create-user: cria um usuário local do IAM para o dispositivo. Os seguintes parâmetros não são compatíveis:
  - `Tags`
  - `PermissionsBoundary`
- delete-access-key: cria uma chave de acesso secreta local do IAM e o ID de chave de acesso da AWS para o usuário especificado.
- delete-policy: exclui a política gerenciada especificada.
- delete-role: exclui o perfil especificado.
- delete-user: exclui o usuário especificado.
- detach-role-policy: remove a política gerenciada especificada d perfil determinado.
- detach-user-policy: remove a política gerenciada especificada do usuário determinado.
- get-policy: recupera informações sobre a política gerenciada especificada, incluindo a versão padrão da política e o número total de usuários, grupos e perfis locais do IAM aos quais a política está anexada.
- get-policy-version: recupera informações sobre a versão especificada da política gerenciada determinada, incluindo o documento da política.
- get-role recupera informações sobre o perfil especificado incluindo o caminho, o GUID, o ARN e a política de confiança do perfil que concede permissão para assumi-lo.
- get-user: recupera informações sobre o usuário do IAM especificado, incluindo a data de criação do usuário, o caminho, o ID exclusivo e o ARN.
- list-access-keys: exibe informações sobre os IDs de chave de acesso associados ao usuário do IAM especificado.
- list-attached-role-policies: lista todas as políticas gerenciadas que estão anexadas ao perfil do IAM especificado.

- list-attached-user-policies: lista todas as políticas gerenciadas que estão anexadas ao usuário do IAM especificado.
- list-entities-for-policy: lista todos os usuários, grupos e perfis locais do IAM aos quais a política gerenciada especificada está anexada.
  - `--EntityFilter`: somente os valores `user` e `role` são compatíveis.
- list-policies: lista todas as políticas gerenciadas que estão disponíveis na Conta da AWS local. O seguinte parâmetro não é compatível:
  - `--PolicyUsageFilter`
- list-roles: lista os perfis locais do IAM que têm o prefixo do caminho especificado.
- list-users: lista os usuários do IAM que têm o prefixo do caminho especificado.
- update-access-key: altera o status da chave de acesso especificada de Ativo para Inativo ou vice-versa.
- update-assume-role-policy: atualiza a política que concede a uma entidade do IAM permissão para assumir um perfil.
- update-role: atualiza a descrição ou a configuração da duração máxima da sessão de um perfil.
- update-user: atualiza o nome e/ou o caminho do usuário do IAM especificado.

Operações compatíveis da API do IAM

Veja a seguir as operações da API do IAM que podem ser usadas com um Snowball Edge, com links para as descrições na Referência da API do IAM.

- AttachRolePolicy: anexa a política gerenciada especificada ao perfil determinado do IAM.
- AttachUserPolicy: anexa a política gerenciada especificada ao usuário determinado.
- CreateAccessKey: cria uma chave de acesso secreta local do IAM e o ID de chave de acesso da AWS correspondente para o usuário especificado.
- CreatePolicy: cria uma política gerenciada do IAM para o dispositivo.
- CreateRole: cria um perfil local do IAM para o dispositivo.
- CreateUser: cria um usuário local do IAM para o dispositivo.

  Os seguintes parâmetros não são compatíveis:
  - `Tags`
  - `PermissionsBoundary`

- DeleteAccessKey: exclui a chave de acesso especificada.
- DeletePolicy: exclui a política gerenciada especificada.
- DeleteRole: exclui o perfil especificado.
- DeleteUser: exclui o usuário especificado.
- DetachRolePolicy: remove a política gerenciada especificada do perfil determinado.
- DetachUserPolicy: remove a política gerenciada especificada do usuário determinado.
- GetPolicy: recupera informações sobre a política gerenciada especificada, incluindo a versão padrão da política e o número total de usuários, grupos e perfis locais do IAM aos quais a política está anexada.
- GetPolicyVersion: recupera informações sobre a versão especificada da política gerenciada determinada, incluindo o documento da política.
- GetRole: recupera informações sobre o perfil especificado, incluindo o caminho, o GUID, o ARN e a política de confiança do perfil que concede permissão para assumi-lo.
- GetUser: recupera informações sobre o usuário do IAM especificado, incluindo a data de criação do usuário, o caminho, o ID exclusivo e o ARN.
- ListAccessKeys: exibe informações sobre os IDs de chave de acesso associados ao usuário do IAM especificado.
- ListAttachedRolePolicies: lista todas as políticas gerenciadas que estão anexadas ao perfil do IAM especificado.
- ListAttachedUserPolicies: lista todas as políticas gerenciadas que estão anexadas ao usuário do IAM especificado.
- ListEntitiesForPolicy: recupera informações sobre o usuário do IAM especificado, incluindo a data de criação, o caminho, o ID exclusivo e o ARN do usuário.
  - `--EntityFilter`: somente os valores `user` e `role` são compatíveis.
- ListPolicies: lista todas as políticas gerenciadas que estão disponíveis na Conta da AWS local. O seguinte parâmetro não é compatível:
  - `--PolicyUsageFilter`
- ListRoles: lista os perfis locais do IAM que têm o prefixo do caminho especificado.
- ListUsers: lista os usuários do IAM que têm o prefixo do caminho especificado.
- UpdateAccessKey: altera o status da chave de acesso especificada de Ativo para Inativo ou vice-versa.

- UpdateAssumeRolePolicy: atualiza a política que concede a uma entidade do IAM permissão para assumir um perfil.
- UpdateRole: atualiza a descrição ou a configuração da duração máxima da sessão de um perfil.
- UpdateUser: atualiza o nome e/ou o caminho do usuário do IAM especificado.

Versão e gramática compatíveis com a política do IAM

Veja a seguir a versão de suporte 2012-10-17 do IAM da política do IAM e um subconjunto da gramática da política.

Tipo de política	Gramática compatível
Políticas baseadas em identidade (política de usuário/função)	“`Effect`, "`Action`" e "`Resource`" **Note** O IAM local não oferece suporte para "`Condition `", "`NotAction `", "`NotResource `" e "`Principal `".
Políticas baseadas em recursos (política de confiança da função)	"`Effect`", "`Action`" e "`Principal `" **Note** Para a entidade principal, somente o ID da Conta da AWS ou o ID da entidade principal é permitido.

Exemplos de política do IAM

Note

Os usuários do AWS Identity and Access Management (IAM) precisam de permissões do "`snowballdevice:*`" para usar a aplicação AWS OpsHub for Snow Family para gerenciar dispositivos da Família Snow.

Veja a seguir exemplos de politicas que concedem permissões para um dispositivo Snowball Edge.

Exemplo 1: Permite a chamada GetUser para um exemplo de usuário por meio da API do IAM

Use a política a seguir para permitir a chamada GetUser para um exemplo de usuário por meio da API do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:GetUser",
            "Resource": "arn:aws:iam:::user/example-user"
        }
    ]
}
```

Exemplo 2: Permite acesso total à API do Amazon S3

Use a política a seguir para permitir o acesso total à API do Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"

        }
    ]
}
```

Exemplo 3: Permite o acesso de leitura e gravação a um bucket específico do Amazon S3

Use a política a seguir para permitir o acesso de leitura e gravação a um bucket específico.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucket-name"
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": "arn:aws:s3:::bucket-name/*"
        }
    ]
}
```

Exemplo 4: Permite o acesso List, Get e Put a um bucket específico do Amazon S3

Use a política a seguir para permitir o acesso List, Get e Put a um bucket específico do S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::examplebucket/*"
        }
    ]
}
```

Exemplo 5: Permite acesso total à API do Amazon EC2

Use a política a seguir para permitir o acesso total ao Amazon EC2.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```

Exemplo 6: Permite acesso para iniciar e interromper as instâncias compatíveis com o Amazon EC2

Use a política a seguir para permitir o acesso para iniciar e interromper as instâncias do Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo 7: Nega chamadas para DescribeLaunchTemplates, mas permite chamadas para DescribeImages

Use a seguinte política para negar chamadas para `DescribeLaunchTemplates`, mas permitir todas as chamadas para `DescribeImages`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
```

```
                "ec2:DescribeLaunchTemplates"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo 8: Política para chamadas da API

Lista todas as políticas gerenciadas que estão disponíveis no dispositivo Snow, incluindo suas próprias políticas gerenciadas definidas pelo cliente. Mais detalhes em list-policies.

```
aws iam list-policies --endpoint http://ip-address:6078 --profile snowballEdge --region
 snow
{
    "Policies": [
        {
            "PolicyName": "Administrator",
            "Description": "Root user admin policy for Account 123456789012",
            "CreateDate": "2020-03-04T17:44:59.412Z",
            "AttachmentCount": 1,
            "IsAttachable": true,
            "PolicyId": "policy-id",
            "DefaultVersionId": "v1",
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:policy/Administrator",
            "UpdateDate": "2020-03-04T19:10:45.620Z"
        }
    ]
}
```

Exemplo de TrustPolicy

Uma política de confiança exibe um conjunto de credenciais temporárias de segurança que pode ser usado para acessar recursos da AWS aos quais talvez você não tenha acesso normalmente.

Essas credenciais de segurança temporárias consistem em um ID de chave de acesso, uma chave de acesso secreta e um token de segurança. Normalmente, você usa `AssumeRole` na conta para acesso entre contas.

Veja a seguir um exemplo de política de confiança. Para obter mais informações sobre a política de confiança, consulte AssumeRole na Referência da API do AWS Security Token Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::AccountId:root" //You can use the Principal ID
 instead of the account ID.
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

Usar o AWS Security Token Service

O AWS Security Token Service (AWS STS) permite solicitar credenciais temporárias de privilégio limitado para usuários do IAM.

> **Important**
>
> Para que os serviços da AWS funcionem corretamente em um Snowball Edge, é necessário ativar as portas dos serviços. Para obter mais detalhes, consulte Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge.

Tópicos

- Usar a AWS CLI e as operações de API no Snowball Edge

- Comandos da AWS CLI compatíveis com o AWS STS no Snowball Edge
- Operações compatíveis da API do AWS STS

Usar a AWS CLI e as operações de API no Snowball Edge

Ao usar o AWS CLI ou as operações de API para emitir IAM, AWS STS, os comandos do Amazon S3 e do Amazon EC2 no dispositivo Snowball Edge, você deve especificar o `region` como "`snow`". Você pode fazer isso usando `AWS configure` ou dentro do próprio comando, como nos exemplos a seguir.

```
aws configure --profile snowballEdge
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Ou

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> O ID de chave de acesso e a chave de acesso secreta que são usados localmente no AWS Snowball Edge não podem ser trocados com as chaves na Nuvem AWS.

Comandos da AWS CLI compatíveis com o AWS STS no Snowball Edge

Somente o comando assume-role é compatível localmente.

Há suporte para os seguintes parâmetros `assume-role`:

- `role-arn`
- `role-session-name`
- `duration-seconds`

Exemplo de comando

Para assumir uma função, use o seguinte comando.

```
    aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/example-role" --
role-session-name AWSCLI-Session  --endpoint http://snow-device-IP-address:7078
```

Para obter mais informações sobre como usar o comando `assume-role`, consulte Como faço para assumir um perfil do IAM usando o AWS CLI?

Para obter mais informações sobre como usar o AWS STS, consulte Solicitação de credenciais de segurança temporárias no Manual do usuário do IAM.

Operações compatíveis da API do AWS STS

Somente a API AssumeRole API é compatível localmente.

Há suporte para os seguintes parâmetros `AssumeRole`:

- `RoleArn`
- `RoleSessionName`
- `DurationSeconds`

Exemplo

Para assumir uma função, use o seguinte.

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=AssumeRole
&RoleSessionName=session-example
&RoleArn=arn:aws:iam::123456789012:role/demo
&DurationSeconds=3600
```

Gerenciar certificados de chave pública

É possível interagir com segurança com serviços da AWS executados em um dispositivo Snowball Edge ou em um cluster de dispositivos Snowball Edge por meio do protocolo HTTPS fornecendo um

certificado de chave pública. É possível usar o protocolo HTTPS para interagir com serviços da AWS, como o IAM, o Amazon EC2, o adaptador do S3, o armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, o Amazon EC2 Systems Manager e o AWS STS em dispositivos Snowball Edge. No caso de um cluster de dispositivos, um único certificado é necessário, e ele pode ser gerado por qualquer dispositivo no cluster. Depois que um dispositivo Snowball Edge gera o certificado e você desbloqueia o dispositivo, é possível usar os comandos do cliente do Snowball Edge para listar, obter e excluir o certificado.

Um dispositivo Snowball Edge gera um certificado quando ocorrem os seguintes eventos:

- O dispositivo ou o cluster Snowball Edge é desbloqueado pela primeira vez.
- O dispositivo ou o cluster Snowball Edge é desbloqueado após a exclusão do certificado (usando o comando `delete-certificate` ou Renovar certificado no AWS OpsHub).
- O dispositivo ou o cluster Snowball Edge é reinicializado e desbloqueado após a expiração do certificado.

Sempre que um novo certificado é gerado, o certificado antigo deixa de ser válido. Um certificado é válido por um período de um ano a partir do dia em que foi gerado.

Também é possível usar o AWS OpsHub for Snow Family para gerenciar certificados de chave pública. Para obter mais informações, consulte Gerenciar certificados de chave pública usando o OpsHub neste guia.

Tópicos

Listar o certificado

Use o comando `list-certificates` para ver os nomes dos recursos da Amazon (ARNs) do certificado atual.

```
snowballEdge list-certificates
```

Example Exemplo da saída **`list-certificates`**

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

Obter certificados

Use o comando `get-certificate` para ver o conteúdo do certificado com base no ARN fornecido. Use o comando `list-certificates` para obter o ARN do certificado a ser usado como o parâmetro `certificate-arn`.

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

Example Exemplo da saída **`get-certificate`**

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

Para obter informações sobre como configurar o certificado, consulte Especificação do adaptador do S3 como endpoint do AWS CLI.

Excluir certificados

Use o comando `delete-certificate` para excluir o certificado atual. Use o comando `list-certificates` para obter o ARN do certificado a ser usado como o parâmetro `certificate-arn`. Para gerar um novo certificado, reinicialize o Snowball Edge ou cada Snowball Edge em um cluster. Consulte Reinicializando o dispositivo da Família Snow ou use o comando `snowballEdge reboot-device`.

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

Example Exemplo da saída **`delete-certificate`**

```
  The certificate has been deleted from your Snow device. Please reboot your Snowball
 Edge or Snowball Edge cluster to generate a new certificate.
```

Portas necessárias para usar os serviços da AWS em um dispositivo AWS Snowball Edge

Para que os serviços da AWS funcionem corretamente em um dispositivo AWS Snowball Edge, é necessário permitir as portas de rede do serviço.

Veja a seguir uma lista de portas de rede necessárias para cada serviço da AWS.

Porta	Protocolo	Comentário
22 (HTTP)	TCP	Verificação de integridade do dispositivo e para EC2 SSH
443 (HTTPS)	TCP	Endpoint do HTTPS da API do S3 e da API do S3 Control
2049 (HTTP)	TCP	Endpoint de NFS
6078 (HTTP)	TCP	Endpoint do HTTP do IAM
6089 (HTTPS)	TCP	Endpoint do HTTPS do IAM
7078 (HTTP)	TCP	Endpoint do HTTP do STS
7089 (HTTPS)	TCP	Endpoint do HTTPS do STS

Porta	Protocolo	Comentário
8080 (HTTP)	TCP	Endpoint de HTTP do adaptador do S3
8008 (HTTP)	TCP	Endpoint do HTTP do EC2
8243 (HTTPS)	TCP	Endpoint do HTTPS do EC2
9091 (HTTP)	TCP	Endpoint para gerenciamento de dispositivos
9092	TCP	Entrada para EKS Anywhere e controlador de dispositivo CAPAS
8242	TCP	Entrada para o endpoint do HTTPS do EC2 para EKS Anywhere
6443	TCP	Entrada para o endpoint da API do Kubernetes do EKS Anywhere
2379	TCP	Entrada para o endpoint da API do Etcd do EKS Anywhere
2380	TCP	Entrada para o endpoint da API do Etcd do EKS Anywhere

Usar o AWS Snow Device Management para gerenciar dispositivos

O AWS Snow Device Management permite que você gerencie seu dispositivo da Família Snow e serviços da AWS 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

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 Conectando-se às de rede local.
- Desbloqueie o dispositivo Snow Family. Para obter mais informações, consulte Desbloqueando o Snowball Edge 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

Na Conta da AWS da qual o dispositivo foi pedido, crie um perfil do AWS Identity and Access Management (IAM) e adicione a política a seguir ao perfil. 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 comandos AWS CLI que você pode usar para gerenciar remotamente os dispositivos da Família Snow remotamente com o Snow Device Management. Você também pode realizar algumas tarefas de gerenciamento remoto usando o AWS OpsHub for Snow Family. 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 à Região da AWS onde foi provisionado.

Tópicos

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
InternalServerException
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-ficthmqoc2phtlef \
--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
InternalServerException
ThrottlingException
AccessDeniedException
```

Saída

```
{
    "associatedWithJob": "JID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",
    "deviceCapacities": [
```

```
        {
            "available": 158892032000,
            "name": "HDD Storage",
            "total": 158892032000,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 0,
            "name": "SSD Storage",
            "total": 0,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 3,
            "name": "vCPU",
            "total": 3,
            "unit": "Number",
            "used": 0
        },
        {
            "available": 5368709120,
            "name": "Memory",
            "total": 5368709120,
            "unit": "Byte",
            "used": 0
        },
        {
            "available": 0,
            "name": "GPU",
            "total": 0,
            "unit": "Number",
            "used": 0
        }
    ],
    "deviceState": "UNLOCKED",
    "deviceType": "SNC1_HDD",
    "lastReachedOutAt": "2021-07-23T21:21:56.120000+00:00",
    "lastUpdatedAt": "2021-07-23T21:21:56.120000+00:00",
    "managedDeviceId": "smd-fictqic6gcldf111",
    "managedDeviceArn": "arn:aws:snow-device-management:us-west-2:000000000000:managed-
device/smd-fictqic6gcldf111"
    "physicalNetworkInterfaces": [
```

```
        {
            "defaultGateway": "10.0.0.1",
            "ipAddress": "10.0.0.2",
            "ipAddressAssignment": "DHCP",
            "macAddress": "ab:cd:ef:12:34:56",
            "netmask": "255.255.252.0",
            "physicalConnectorType": "RJ45",
            "physicalNetworkInterfaceId": "s.ni-530f866d526d4b111"
        },
        {
            "defaultGateway": "10.0.0.1",
            "ipAddress": "0.0.0.0",
            "ipAddressAssignment": "STATIC",
            "macAddress": "ab:cd:ef:12:34:57",
            "netmask": "0.0.0.0",
            "physicalConnectorType": "RJ45",
            "physicalNetworkInterfaceId": "s.ni-8abc787f0a6750111"
        }
    ],
    "software": {
        "installState": "NA",
        "installedVersion": "122",
        "installingVersion": "NA"
    },
    "tags": {
        "Project": "PrototypeA"
    }
}
```


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 comando `describe-device`, 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
InternalServerException
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
InternalServerException
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
InternalServerException
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 Como usar as opções de paginação do AWS CLI no "Manual do usuário da interface de linha de comando da AWS".

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
InternalServerException
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 Como usar as opções de paginação do AWS CLI no "Manual do usuário da interface de linha de comando da AWS".

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
InternalServerException
ThrottlingException
AccessDeniedException
```

Saída

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

Listar atributos disponíveis

Para retornar uma lista dos atributos da AWS disponíveis para um dispositivo, use o comando `list-device-resources`. 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 Como usar as opções de paginação do AWS CLI no "Manual do usuário da interface de linha de comando da AWS".

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
InternalServerException
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
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Saída

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

Listar tarefas por status

Use o comando `list-tasks` para retornar uma lista de tarefas dos dispositivos na região AWS 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 Como usar as opções de paginação do AWS CLI no "Manual do usuário da interface de linha de comando da AWS".

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 K8VAMqKiP2Cf4xGkmH8GMyZrgOF8FUb+d1OKTP9+P4pUb+8PhW+6MiXh4= \
--max-results 10
```

Exceções

```
ValidationException
```

```
InternalServerException
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
```

```
InternalServerException
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
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Noções básicas sobre trabalhos do AWS Snowball Edge

Trabalho no AWS Snowball é uma unidade específica de trabalho definida quando é criado no console ou na API de gerenciamento de trabalhos. Com o dispositivo AWS Snowball Edge, existem três tipos diferentes de trabalho, todos eles com funcionalidade de armazenamento e computação locais. Essa funcionalidade usa a interface de arquivos ou a interface do Amazon S3 para ler e gravar dados. Ele aciona funções do Lambda com base nas ações da API de objetos PUT do Amazon S3 que são executadas localmente no dispositivo AWS Snowball Edge.

- Importar trabalhos para o Amazon S3: a transferência de 80 TB ou menos de dados locais copiados em um único dispositivo e, depois, movidos para o Amazon S3. Para trabalhos de importação, os dispositivos e trabalhos do Snowball têm um one-to-one relacionamento. Cada trabalho tem exatamente um dispositivo associado a ele. Se for necessário importar mais dados, é possível criar novos trabalhos de importação ou clonar os já existentes. Ao devolver um dispositivo desse tipo de trabalho, esses dados são importados para o Amazon S3.
- Trabalhos de exportação do Amazon S3: a transferência de qualquer volume de dados (localizados no Amazon S3), copiados em qualquer quantidade de dispositivos Snowball Edge e depois movidos de um dispositivo AWS Snowball Edge por vez para o destino de dados on-premises. Quando você cria um trabalho de exportação, ele é dividido em partes do trabalho. Cada parte de trabalho não tem mais de 80 TB de tamanho e tem apenas um dispositivo AWS Snowball Edge associado. Ao devolver um dispositivo desse tipo de trabalho, ele é apagado.
- Somente trabalhos de computação e armazenamento local: esses trabalhos envolvem um dispositivo AWS Snowball Edge ou vários dispositivos usados em um cluster. Os trabalhos não começam com dados nos buckets, como um trabalho de exportação, e não podem ter dados importados para o Amazon S3 no final, como um trabalho de importação. Ao devolver um dispositivo desse tipo de trabalho, ele é apagado. Com esse tipo de trabalho, também existe a opção de criar um cluster de dispositivos. Um cluster melhora a durabilidade do armazenamento local e pode ser escalonado para mais ou para menos com capacidade de armazenamento de dados local.

  Nas regiões onde o Lambda não está disponível, esse tipo de trabalho será denominado Somente armazenamento local.

Detalhes do trabalho

Antes de criar um trabalho, verifique se os pré-requisitos foram atendidos. Cada trabalho é definido pelos detalhes especificados quando ele é criado. A tabela a seguir descreve todos os detalhes de um trabalho.

Identificador do console	Identificador da API	Descrição detalhada
Nome do trabalho	`Description`	Um nome para o trabalho contendo caracteres alfanuméricos, espaços e qualquer caractere Unicode especial.
Tipo de trabalho	`JobType`	O tipo de trabalho, seja de importação, exportação ou de computação e armazenam ento local.
ID do trabalho	`JobId`	Rótulo exclusivo de 39 caracteres que identifica o trabalho. O trabalho do ID aparece na parte inferior da etiqueta de entrega que aparece na tela E Ink e no nome de um arquivo manifesto de trabalho.
Endereço	`AddressId`	O endereço para o qual o dispositivo será enviado. No caso da API, este é o ID do tipo de dados do endereço.
Data da criação	CreationDate	A data em que esse trabalho foi criado.
Velocidade de entrega	`ShippingOption`	As opções de velocidade baseiam-se na região. Para

Identificador do console	Identificador da API	Descrição detalhada
		ter mais informações, consulte Prazos de entrega.
ARN do perfil do IAM	RoleARN	Esse nome do recurso da Amazon (ARN) é o perfil do AWS Identity and Access Management (IAM), que é criado durante a criação do trabalho com permissões de gravação para os buckets do Amazon S3. O processo de criação é automático, e o perfil do IAM que você permite ao AWS Snowball assumir é usado apenas para copiar os dados entre os buckets do S3 e o Snowball. Para ter mais informações, consulte Permissões necessárias para usar o console do AWS Snowball.
AWS KMSChave do	`KmsKeyARN`	No AWS Snowball, o AWS Key Management Service (AWS KMS) criptogra fa as chaves em cada Snowball. Ao criar o trabalho, é possível escolher ou criar um ARN para uma chave de criptografia do AWS KMS que você possui. Para ter mais informações, consulte AWS Key Management Service em AWS Snowball Edge.

Identificador do console	Identificador da API	Descrição detalhada
Capacidade do Snowball	`SnowballCapacityPreference`	A capacidade de armazenamento do AWS Snowball dispositivo solicitado nesta tarefa. O tamanho disponível depende da Região da AWS.
Serviços de armazenamento	N/D	O serviço de armazenamento da AWS associado a esse trabalho, nesse caso o Amazon S3.
Recursos	`Resources`	Os recursos do serviço de armazenamento da AWS associados ao trabalho. Neste caso, esses são os buckets do Amazon S3 para ou dos quais os dados são transferidos.
Tipo de trabalho	`JobType`	O tipo de trabalho, seja de importação, exportação ou de computação e armazenamento local.
Tipo de Snowball	`SnowballType`	O tipo de dispositivo da família Snow solicitado nesta tarefa.
ID do cluster	`ClusterId`	Rótulo exclusivo de 39 caracteres que identifica o cluster.

Status dos trabalhos

Cada dispositivo AWS Snowball Edge tem um status que muda para indicar o status atual do trabalho. Essas informações de status do trabalho não refletem a integridade, o status de processamento atual ou o armazenamento usado para os dispositivos associados.

Como ver o status de um trabalho

1. Faça login no Console de Gerenciamento da família AWS Snow.
2. No Painel de trabalhos, selecione o trabalho.
3. Clique no nome do trabalho no console.
4. O painel Status do trabalho estará localizado próximo à parte superior e refletirá o status do trabalho.

Status de trabalhos do dispositivo AWS Snowball Edge

Identificador do console	Identificador da API	Descrição do status
Trabalho criado	`New`	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.
Preparar o dispositivo	`PreparingAppliance`	A AWS está preparando um dispositivo para o trabalho.
Exportação	`InProgress`	A AWS está exportando os dados do Amazon S3 para um dispositivo.
Preparação de entrega	`PreparingShipment`	A AWS está preparando o envio de um dispositi vo para você. As informações de

Identificador do console	Identificador da API	Descrição do status
		rastreamento de envio esperadas são fornecidas aos clientes no status.
Em trânsito	`InTransitToCustomer`	O dispositivo foi enviado para o endereço fornecido durante a criação do trabalho.
Entregue	`WithCustomer`	O dispositivo chegou ao endereço indicado durante a criação do trabalho.
Em trânsito para a AWS	`InTransitToAWS`	O dispositivo foi enviado de volta para a AWS.
No departamento de triagem	`WithAWSSortingFacility`	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.

Identificador do console	Identificador da API	Descrição do status
Na AWS	`WithAWS`	O envio chegou na AWS. Se estiver importando dados, a importação normalmente começa em um dia da chegada.
Importação	`InProgress`	A AWS está importando os dados para o Amazon Simple Storage Service (Amazon S3).
Concluído	`Complete`	O trabalho ou parte do trabalho foi concluída com êxito.
Cancelado	`Cancelled`	O trabalho foi cancelado.

Status dos clusters

Cada cluster tem um status que muda para apontar o status do progresso geral do cluster. Cada nó individual do cluster tem seu próprio status de trabalho.

Essas informações de status do cluster não refletem o estado, o status de processamento atual ou o armazenamento usado para o cluster ou seus nós.

Identificador do console	Identificador da API	Descrição do status
Aguardando quórum	`AwaitingQuorum`	O cluster ainda não foi criado porque

Identificador do console	Identificador da API	Descrição do status
		não há nós suficient es para iniciar o processamento da solicitação de clusters. Para que um cluster seja criado, ele precisa ter pelo menos cinco nós.
Pendente	`Pending`	O cluster foi criado e seus nós prontos para entrega estão sendo obtidos. Com esse status de trabalho do nó, é possível acompanhar o status de cada nó.
Entregue	`InUse`	Pelo menos um nó do cluster está no endereço fornecido durante a criação do trabalho.
Concluído	`Complete`	Todos os nós do cluster foram devolvidos à AWS.

Identificador do console	Identificador da API	Descrição do status
Cancelado	`Cancelled`	A solicitação para fazer um cluster foi cancelada. As solicitações de clusters só podem ser canceladas antes de entrarem para o status de Pendente.

Importar trabalhos para o Amazon S3

Com um trabalho de importação, os dados são copiados no dispositivo AWS Snowball Edge com o adaptador do Amazon S3 integrado ou o ponto de montagem NFS. A fonte de dados para um trabalho de importação deve ser no local. Em outras palavras, os dispositivos de armazenamento que contêm os dados a serem transferidos devem estar fisicamente localizados no endereço fornecido quando o trabalho foi criado.

Ao importar arquivos, cada arquivo se torna um objeto no Amazon S3 e cada diretório se torna um prefixo. Se os dados forem importados para um bucket existente, todos os objetos existentes com os mesmos nomes que os objetos recém-importados são substituídos. O tipo de trabalho de importação também tem recurso de funcionalidade de armazenamento e computação. Essa funcionalidade usa a interface de arquivos ou o adaptador do Amazon S3 para ler e gravar dados e aciona funções do Lambda com base nas ações da API de objetos PUT do Amazon S3 que são executadas localmente no dispositivo AWS Snowball Edge.

Quando todos os dados tiverem sido importados para os buckets do Amazon S3 especificados na Nuvem AWS, a AWS realizará um apagamento completo do dispositivo. Esse apagamento segue os padrões 800-88 do NIST.

Após a conclusão da importação, você pode fazer o download de um relatório de trabalho. Esse relatório alerta sobre objetos que falharam no processo de importação. É possível encontrar informações adicionais no sucesso e os logs de falha.

> **Important**
>
> Não exclua as cópias locais dos dados transferidos até que seja possível verificar os resultados do relatório de conclusão do trabalho e analisar os logs de importação.

Trabalhos de exportação do Amazon S3

> **Note**
>
> No momento, tags e metadados NÃO são compatíveis, ou seja, todas as tags e os metadados seriam removidos ao exportar objetos dos buckets do S3.

A fonte de dados para um trabalho de exportação é um ou mais buckets do Amazon S3. Assim que os dados de uma parte do trabalho forem movidos do Amazon S3 para um dispositivo AWS Snowball Edge, será possível baixar um relatório de trabalho. Esse relatório alerta sobre objetos cuja transferência para o dispositivo falhou. Você encontrará mais informações nos logs de sucesso e de falha do trabalho.

É possível exportar qualquer quantidade de objetos para cada trabalho de exportação usando tantos dispositivos quanto necessários para concluir a transferência. Cada dispositivo AWS Snowball Edge de partes de um trabalho de exportação é entregue um após o outro, com dispositivos subsequentes enviados depois que a última parte do trabalho assume o status Em trânsito para a AWS.

Ao copiar objetos no destino dos dados on-premises a partir de um dispositivo usando o adaptador do Amazon S3 ou o ponto de montagem do NFS, esses objetos são salvos como arquivos. Se os objetos forem copiados em um local que já contém arquivos, todos os outros arquivos existentes com os mesmos nomes são substituídos. O tipo de trabalho de exportação também tem recurso de funcionalidade de armazenamento e computação. Essa funcionalidade usa a interface de arquivos ou o adaptador do Amazon S3 para ler e gravar dados e aciona funções do Lambda com base nas ações da API de objetos PUT do Amazon S3 que são executadas localmente no dispositivo AWS Snowball Edge.

Quando a AWS recebe um dispositivo devolvido, este é totalmente apagado de acordo com os padrões 800-88 do NIST.

> **Important**
>
> Os dados que você deseja exportar para um dispositivo Snow devem estar no Amazon S3. Todos os dados no Amazon S3 Glacier que você planeja exportar para o dispositivo Snow precisarão ser descongelados ou movidos para a classe de armazenamento S3 antes de serem exportados. Faça isso antes de criar o trabalho de exportação do Snow.
> Não altere, atualize nem exclua objetos do Amazon S3 exportados até que seja possível verificar se todo o conteúdo para o trabalho inteiro foi copiado para o destino de dados on-premises.

Ao criar um trabalho de exportação, é possível exportar um bucket do Amazon S3 inteiro ou um intervalo específico de chaves de objetos.

Utilização de intervalos de exportação

Quando um trabalho de exportação é criado no Console de Gerenciamento da família AWS Snow ou com a API de gerenciamento de trabalhos, é possível exportar um bucket do Amazon S3 inteiro ou um intervalo específico de chaves de objetos. Os nomes de chaves de objetos identificam exclusivamente objetos em um bucket. Caso um intervalo deva ser exportado, o tamanho do intervalo é definido fornecendo um intervalo inclusivo de início, um intervalo inclusivo de término, ou ambos.

Os intervalos são classificados como binário UTF-8. Os dados binários UTF-8 são classificados da seguinte forma:

- Os números 0 a 9 vêm antes de caracteres de letras maiúsculas e minúsculas em inglês.
- Os caracteres em maiúsculas em inglês vêm antes de todos os caracteres em minúsculas em inglês.
- Os caracteres em minúsculas em inglês vêm por último quando são classificados em relação a caracteres em maiúsculas e números em inglês.
- Os caracteres especiais são classificados entre os outros conjuntos de caracteres.

Para obter mais informações sobre os aspectos específicos do UTF-8, consulte UTF-8 na Wikipedia.

Exemplos de intervalo de exportação

Suponha que exista um bucket contendo os seguintes objetos e prefixos, classificados em ordem binária de UTF-8:

- 01
- Aardvark
- Aardwolf
- Aasvogel/maçã
- Aasvogel/arrow/object1
- Aasvogel/arrow/object2
- Aasvogel/banana
- Aasvogel/banker/object1
- Aasvogel/banker/object2
- Aasvogel/cereja
- Banana
- Carro

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
(none)	(none)	Todos os objetos no bucket
(none)	Aasvogel	01 Aardvark Aardwolf Aasvogel/maçã Aasvogel/arrow/object1

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
		Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cereja
(none)	Aasvogel/banana	01 Aardvark Aardwolf Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
Aasvogel	(none)	Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cereja Banana Carro

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
Aardwolf	(none)	Aardwolf Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cereja Banana Carro

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
Aar	(none)	Aardvark Aardwolf Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cereja Banana Carro

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
carro	(none)	Nenhum objeto é exportado e, ao tentar criar o trabalho, é obtida uma mensagem de erro. Observe que o carro é classificado abaixo de Carro, de acordo com os valores binários de UTF-8.
Aar	Aarrr	Aardvark Aardwolf
Aasvogel/arrow	Aasvogel/arrox	Aasvogel/arrow/object1 Aasvogel/arrow/object2

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
Aasvogel/maçã	Aasvogel/banana	Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana
Aasvogel/maçã	Aasvogel/banker	Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
Aasvogel/maçã	Aasvogel/cereja	Aasvogel/maçã Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cereja

Suponha que você tenha esses três buckets e queira copiar todos os objetos da folder2.

- s3://bucket/folder1/
- s3://bucket/folder2/
- s3://bucket/folder3/

Início do intervalo especificado	Final do intervalo especificado	Objetos no intervalo que serão exportados
folder2/	folder2/	Todos os objetos no bucket folder2.

Práticas recomendadas para trabalhos de exportação

- Garanta que os dados estejam no Amazon S3, agrupe pequenos arquivos antes de ordenar o trabalho
- Certifique-se de que os intervalos de chaves sejam especificados na definição do trabalho de exportação se você tiver milhões de objetos no bucket.
- Atualize as chaves de objeto para remover a barra no nome, pois objetos com barras finais nos nomes (/ ou \) não são transferidos para o Snowball Edge.
- Para buckets do S3, a limitação do tamanho do objeto é de 255 caracteres.
- Para buckets do S3 habilitados para versão, somente a versão atual dos objetos é exportada.
- Os marcadores de exclusão não são exportados.

Somente trabalhos de computação e armazenamento local

Os trabalhos locais de computação e armazenamento permitem que você use o armazenamento compatível com o Amazon S3 em dispositivos da família Snow localmente, sem uma conexão com a internet. Você não pode exportar dados do Amazon S3 para o dispositivo nem importar dados para o Amazon S3 quando o dispositivo é devolvido.

Tópicos

- Trabalhos de armazenamento local
- Opção de cluster local

Trabalhos de armazenamento local

Você pode ler e gravar objetos em um AWS Snowball Edge dispositivo usando armazenamento compatível com Amazon S3 em dispositivos da família Snow ou no adaptador S3. Ao solicitar um dispositivo, se optar por usar o adaptador S3, você também escolhe quais buckets Amazon S3 serão incluídos no dispositivo quando você o receber. Se você optar por usar o armazenamento compatível com o Amazon S3 em dispositivos da família Snow, nenhum bucket do Amazon S3 será incluído no dispositivo quando você o receber.

Você pode criar buckets do Amazon S3 nos dispositivos Snowball Edge para armazenar e recuperar objetos no local para aplicativos que exigem acesso e processamento de dados locais e residência de dados. O armazenamento compatível do Amazon S3 em dispositivos da Família Snow fornece uma nova classe de armazenamento, `SNOW`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos Snowball Edge. É possível usar os mesmos atributos e APIs nos buckets do Snowball Edge da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso ciclo de vida do bucket, criptografia e marcação. Quando o dispositivo ou dispositivos são devolvidosAWS, todos os dados criados ou armazenados no armazenamento compatível com o Amazon S3 nos dispositivos da família Snow são apagados. Para obter mais informações, consulte Trabalhos somente de computação e armazenamento locais.

Para obter mais informações, consulte Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow neste guia.

Ao terminar de usar o dispositivo, devolva-o para a AWS. O dispositivo será apagado. Esse apagamento segue os padrões 800-88 do Instituto Nacional de Padrões e Tecnologia (NIST).

Opção de cluster local

Cluster é um agrupamento lógico de dispositivos Snowball Edge, em grupos de 3 a 16 dispositivos. Um cluster é criado como um trabalho único, que oferece maior durabilidade e tamanho de armazenamento em comparação com outras ofertas de trabalho do AWS Snowball. Para obter mais informações sobre trabalhos de cluster, consulte Visão geral do cluster neste guia.

Clonagem de um trabalho no console

Ao criar um trabalho de importação ou um trabalho de computação e armazenamento local pela primeira vez, pode ser detectado que é necessário mais de um dispositivo AWS Snowball Edge.

Como os trabalhos de importação e os trabalhos de computação e armazenamento local são associados a um único dispositivo, exigir mais de um dispositivo significa que é preciso criar mais de um trabalho. Ao criar trabalhos adicionais, pode-se passar novamente pelo assistente de criação de trabalhos no console ou clonar um trabalho existente.

> **Note**
>
> A clonagem de um trabalho é um atalho disponível no console que facilita a criação de trabalhos adicionais. Se estiver criando trabalhos com a API de gerenciamento de trabalhos, basta simplesmente executar o comando de criação de trabalho novamente.

Clonar um trabalho significa recriá-lo com precisão, exceto em caso de um nome modificado automaticamente. A clonagem é um processo simples.

Para clonar um trabalho no console

1. No Console de Gerenciamento da família AWS Snow, escolha o trabalho na tabela.
2. Em Ações, escolha Clonar trabalho.

   O assistente Criar trabalho é aberto na última página, Etapa 6: Revisar.
3. Examine as informações e faça as alterações desejadas selecionando o botão Editar correspondente.
4. Para criar o trabalho clonado, selecione Criar trabalho.

Os trabalhos clonados recebem nomes no formato ***Nome do trabalho***-clone-***número***. O número é adicionado automaticamente ao nome do trabalho e representa o número de clonagens desse trabalho depois da primeira vez que foi clonado. Por exemplo, AprilFinanceReports-clone representa o primeiro trabalho clonado do AprilFinanceReportstrabalho e DataCenterMigration-clone-42 representa o quadragésimo segundo clone do trabalho. DataCenterMigration

Práticas recomendadas para usar o dispositivo Snowball Edge

Para ajudar a obter o máximo benefício e satisfação com seu AWS Snowball Edge dispositivo, recomendamos que você siga estas práticas recomendadas.

Segurança

A seguir estão as recomendações e as melhores práticas para manter a segurança ao trabalhar com um AWS Snowball Edge dispositivo.

Segurança geral

- Se você notar algo que pareça suspeito no AWS Snowball Edge dispositivo, não o conecte à sua rede interna. Em vez disso, entre em contato com o AWS Support para receber um novo dispositivo AWS Snowball Edge .
- Recomendamos não salvar uma cópia do código de desbloqueio no mesmo local na estação de trabalho que o manifesto para esse trabalho. Salvá-los em locais diferentes ajuda a impedir que pessoas não autorizadas tenham acesso ao AWS Snowball Edge 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 Snowball Edge dispositivo a indivíduos que têm acesso aos arquivos salvos no servidor e ao endereço de e-mail do usuário.
- As credenciais exibidas, quando você executa os list-access-keys comandos do cliente Snowball Edge get-secret-access-key e, são um par de chaves de acesso usadas para acessar seu dispositivo.

  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 porque só funcionam para os recursos locais associados ao seu trabalho.
- Se você achar que suas credenciais foram perdidas ou comprometidas, solicite um novo arquivo de manifesto e desbloqueie o código seguindo o processo de atualização do certificado SSL do dispositivo. Consulte Atualizar o certificado SSL.

Para obter informações sobre como usar políticas AWS Identity and Access Management (IAM) para controlar o acesso, consultePolíticas gerenciadas pela AWS (predefinidas) para o AWS Snowball Edge.

Segurança de rede

- Recomendamos que você use apenas um método por vez para ler e gravar dados em um bucket local em um AWS Snowball Edge dispositivo. Usar ao mesmo tempo a interface de arquivos e o adaptador do Amazon S3 no mesmo bucket do Amazon S3 poderá resultar em conflitos de leitura/gravação.
- Para evitar corromper seus dados, não desconecte o AWS Snowball Edge dispositivo nem altere suas configurações de rede ao transferir dados.
- Os arquivos que estiverem sendo gravados em um dispositivo deverão estar em estado estático. Os arquivos modificados enquanto estão sendo gravados podem resultar em conflitos de leitura/gravação.
- Para obter mais informações sobre como melhorar o desempenho do seu AWS Snowball Edge dispositivo, consultePerformance.

Gerenciamento de recursos

Considere as práticas recomendadas a seguir para gerenciar trabalhos e recursos em seu dispositivo AWS Snowball Edge .

- Os 10 dias gratuitos para realizar sua transferência de dados no local começam no dia seguinte à chegada do AWS Snowball Edge dispositivo ao seu data center. Isso só é aplicável a dispositivos do tipo Snowball Edge.
- O status de Trabalho criado é o único no qual é possível cancelar um trabalho. Quando um trabalho muda para outro status, não é possível cancelar o trabalho. Isso se aplica aos clusters.
- Para trabalhos de importação, não exclua as cópias locais dos dados transferidos enquanto a importação para o Amazon S3 não for concluída com êxito. Como parte do processo, verifique os resultados da transferência de dados.

Performance

> **Note**
>
> O desempenho da transferência de dados que você experimenta variará com base no ambiente de rede, nos sistemas operacionais, no método de cópia, no protocolo, no desempenho de leitura dos dados de origem e nas características do conjunto de dados, como o tamanho do arquivo. Para determinar as taxas e os tempos de transferência de dados precisos, recomendamos que você meça o desempenho por meio de proof-of-concept testes em seu ambiente.

A seguir, você encontrará recomendações e informações sobre o desempenho AWS Snowball Edge do dispositivo. Esta seção descreve o desempenho em termos gerais, porque os ambientes on-premises têm uma forma diferente de fazer as coisas; diferentes tecnologias de rede, hardware diferente, diferentes sistemas operacionais, procedimentos diferentes e assim por diante.

A tabela a seguir descreve como a taxa de transferência da rede afeta o tempo necessário para preencher um dispositivo Snowball Edge com dados. A transferência de arquivos menores reduz a velocidade de transferência devido a uma sobrecarga maior. Se tiver vários arquivos pequenos, é recomendável compactá-los em arquivos maiores antes de transferi-los para o dispositivo Snowball Edge.

Taxa (MB/s)	Tempo de transferência de 82 TB
800	1,22 dia
450	2,11 dias
400	2,37 dias
300	3,16 dias
277	3,42 dias
200	4,75 dias
100	9,49 dias

Taxa (MB/s)	Tempo de transferência de 82 TB
60	15,53 dias
30	31,06 dias
10	85,42 dias

Para fornecer orientações significativas sobre desempenho, as seções a seguir descrevem como determinar quando usar o AWS Snowball Edge dispositivo e como aproveitar ao máximo o serviço.

Tópicos

Recomendações de desempenho

As práticas abaixo são altamente recomendadas, porque elas têm o maior impacto na melhoria do desempenho da transferência de dados:

- Recomendamos que você não tenha mais de 500 mil arquivos ou diretórios dentro de cada diretório.
- Recomendamos que todos os arquivos transferidos para um dispositivo Snowball Edge não tenham menos de 1 MB de tamanho.
- Se tiver muitos arquivos menores que 1 MB, recomendamos compactá-los em arquivos maiores antes de transferi-los para um dispositivo Snowball Edge.

Acelerar a transferência de dados

Uma das melhores maneiras de melhorar o desempenho de um AWS Snowball Edge dispositivo é acelerar a transferência de dados de e para um dispositivo. Geralmente, é possível melhorar a velocidade de transferência da fonte de dados para o dispositivo das formas a seguir. A lista abaixo é ordenada do maior para o menor impacto positivo no desempenho:

1. Execute várias operações de gravação ao mesmo tempo: para fazer isso, execute cada comando de várias janelas de terminal em um computador com uma conexão de rede com um único dispositivo AWS Snowball Edge .
2. Transfira arquivos pequenos em lotes: cada operação de cópia tem alguma sobrecarga por causa da criptografia. Para acelerar o processo, reúna os arquivos em lote em um único arquivo. Ao agrupar os arquivos em lote, eles podem ser extraídos automaticamente quando importados para o Amazon S3. Para ter mais informações, consulte Agrupar arquivos pequenos em lote.
3. Não execute outras operações nos arquivos durante a transferência: renomear arquivos durante a transferência, alterar os metadados ou gravar dados nos arquivos durante uma operação de cópia terá impacto negativo no desempenho da transferência. Recomendamos que os arquivos permaneçam em um estado estático durante a transferência.
4. Reduza o uso de rede local: seu dispositivo AWS Snowball Edge se comunica em sua rede local. Por isso, reduzir o tráfego de rede local entre o dispositivo AWS Snowball Edge , o switch ao qual ele está conectado e o computador que hospeda a fonte de dados pode melhorar as velocidades de transferência de dados.
5. Elimine saltos desnecessários — recomendamos que você configure seu AWS Snowball Edge dispositivo, sua fonte de dados e o computador que executa a conexão de terminal entre eles para que sejam as únicas máquinas se comunicando por meio de um único switch. Isso pode melhorar as velocidades de transferência de dados.

Atualização de software em dispositivos Snowball Edge

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 Snowball Edge 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 as workloads no dispositivo e reiniciá-lo.

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

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 Snowball Edge 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 Utilização do Snowball Edge Client.
- (Opcional) Recomendamos configurar um perfil para o Snowball Edge Client. Para obter mais informações, consulte Configurando um perfil para o Snowball Edge Client.
- Para armazenamento compatível com o Amazon S3 em dispositivos da Família Snow em dispositivos Snowball Edge em cluster, interrompa o serviço S3-Snow e desative a inicialização automática. Consulte Configurando o armazenamento compatível com o Amazon S3 no serviço de dispositivos da família Snow para inicialização automática.

> **Note**
>
> Para dispositivos em cluster, todos os comandos precisam ser executados para cada dispositivo.

Agora que concluiu essas tarefas, você pode fazer download e instalar atualizações para dispositivos Snowball Edge.

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 Snowball Edge, consulte `configure-auto-update-strategy` Atualizando um Snowball Edge.

> **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 baixar as atualizações do software Snowball Edge para dispositivos autônomos

1. Abra uma janela de terminal e verifique se o dispositivo do Snowball Edge 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
   ```

Para verificar e baixar as atualizações do software Snowball Edge para clusters de dispositivos

1. Abra uma janela de terminal e certifique-se de que todos os dispositivos do Snowball Edge no cluster estejam desbloqueados usando o comando. `snowballEdge describe-device` Se os dispositivos estiverem bloqueados, use o `snowballEdge unlock-cluster` comando para desbloqueá-los. Para obter mais informações, consulte Desbloqueando o Snowball Edge.
2. Quando todos os dispositivos no cluster estiverem desbloqueados, para cada dispositivo no cluster, execute o `check-for-updates` comando. Esse comando retorna a versão mais recente disponível do software Snowball Edge, além da versão atual instalada no dispositivo.

```
snowballEdge check-for-updates --unlock-code 29-character-unlock-code --manifest-
file path/to/manifest/file.bin --endpoint https://ip-address-of-snow-device
```

> **Note**
>
> O código de desbloqueio e o arquivo de manifesto são os mesmos para todos os dispositivos no cluster.

Example de **`check-for-updates`** comando

```
{
"InstalledVersion" : "118",
"LatestVersion" : "119"
}
```

Se o valor do `LatestVersion` nome for maior que o valor do `InstalledVersion` nome, uma atualização estará disponível.

3. Para cada dispositivo no cluster, use o `download-updates` comando para baixar a atualização.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

> **Note**
>
> Para sistemas operacionais Windows, formate o valor do `uri` parâmetro da seguinte forma:
>
> ```
> snowballEdge download-updates --uri file:/C:/path/to/local-update
> ```

4. Para verificar o status desse download para cada dispositivo no cluster, use o `describe-device-software` comando.

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

Example da saída do **`describe-device-software`** comando

```
{
"InstalledVersion" : "118",
"InstallingVersion" : "119",
"InstallState" : "DOWNLOADED",
"CertificateExpiry" : "Sat Mar 30 16:47:51 UTC 2024"
}
```

Se o valor do `InstallState` nome for`DOWNLOADED`, o download da atualização será feito e estará disponível para instalação.

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.

Para clusters de dispositivos Snowball Edge, a atualização deve ser baixada e instalada para cada dispositivo no cluster.

> **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 Snowball Edge 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 Desbloqueando o Snowball Edge.
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
   ```

   Example 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
   ```

   Example 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.

4. 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
```

Example 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.
```

5. Execute o comando `snowballEdge install-updates`.
6. 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 Snowball Edge. 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 como desbloquear o dispositivo, consulte Desbloqueando o dispositivo Snowball Desbloqueando o 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 Snowball Edge, além da versão atual instalada no dispositivo.

Para instalar atualizações de software que já foram baixadas em um cluster de dispositivos Snowball Edge

1. Para cada dispositivo no cluster, execute o `describe-device` comando para determinar se os dispositivos estão desbloqueados. Se os dispositivos estiverem bloqueados, use o `unlock-cluster` comando para desbloqueá-los. Para obter mais informações, consulte Desbloqueando o Snowball Edge.
2. Para cada dispositivo no cluster, 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
   ```

   Example 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
   ```

   Example 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.

4. Para cada dispositivo no cluster, 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
```

Example 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.
```

5. Para cada dispositivo no cluster, execute o `install-updates` comando.

```
snowballEdge install-updates
```

6. Você pode verificar o status dessa instalação com o comando `describe-device-software`.

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

Example da saída do **`describe-device-service`** comando

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Quando isso acontecer `Install StateRequires Reboot`, você instalou com sucesso a atualização de software do seu dispositivo Snowball Edge. A instalação de uma atualização não a aplica automaticamente ao dispositivo. Para concluir a instalação da atualização, o dispositivo deve ser reiniciado.

> **Warning**
>
> Reiniciar o dispositivo Snowball Edge sem interromper todas as atividades no dispositivo pode resultar na perda de dados.

7. Reinicialize todos os dispositivos no cluster, desbloqueie o cluster e reinicialize todos os dispositivos no cluster novamente. Isso conclui a instalação das atualizações de software baixadas. Para obter mais informações sobre a reinicialização dos dispositivos, consulte Reinicializando o dispositivo da família Snow. Para obter mais informações sobre como desbloquear o cluster de dispositivos, consulte Desbloqueando o Snowball Edge.

8. Depois que cada dispositivo no cluster for reinicializado duas vezes, desbloqueie o cluster e use o `check-for-updates` comando para verificar se o dispositivo foi atualizado. Esse comando retorna a versão mais recente disponível do software Snowball Edge, além da versão atual instalada no dispositivo. Se a versão atual e a versão mais recente disponível forem iguais, o dispositivo foi atualizado com êxito.

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.

A atualização do certificado SSL é feita por meio do cliente Snowball Edge. 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 Snowball Edge usando o cliente AWS Edge.

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.

   Example 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.

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
```

Segurança para AWS Snowball Edge

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Snowball, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Snowball. Os tópicos a seguir mostram como configurar para atender AWS Snowball aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Snowball recursos.

Tópicos

Proteção de dados no AWS Snowball Edge

AWS Snowball está em conformidade com o modelo de responsabilidade AWS compartilhada, que inclui regulamentos e diretrizes para proteção de dados. AWS é responsável por proteger a

infraestrutura global que executa todos os AWS serviços. AWS mantém o controle sobre os dados hospedados nessa infraestrutura, incluindo os controles de configuração de segurança para lidar com o conteúdo do cliente e os dados pessoais. AWS clientes e parceiros da APN, atuando como controladores ou processadores de dados, são responsáveis por quaisquer dados pessoais que coloquem no. Nuvem AWS

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS Identity and Access Management (IAM), para que cada usuário receba somente as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Recomendamos usar o TLS 1.2 ou posterior.

- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Snowball ou outros AWS serviços usando o console, a API ou AWS os SDKs. AWS CLI Todos os dados inseridos por você no AWS Snowball ou em outros serviços podem ser separados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

Para obter mais informações sobre proteção de dados, consulte a publicação Modelo de responsabilidade compartilhada da AWS e do RGPD no Blog de segurança da AWS .

Tópicos

Proteção de dados na nuvem

AWS Snowball protege seus dados quando você está importando ou exportando dados para o Amazon S3, quando você cria um trabalho para solicitar um dispositivo da família Snow e quando seu dispositivo é atualizado. As seções a seguir descrevem como você pode proteger seus dados quando usa o Snowball Edge e está on-line ou interagindo AWS na nuvem.

Tópicos

Criptografia para AWS Snowball Edge

Quando você estiver usando um Snowball Edge para importar dados para S3, todos os dados transferidos para um dispositivo são protegidos por criptografia SSL pela rede. Para proteger dados em repouso, o AWS Snowball Edge usa criptografia do lado do servidor (SSE).

Criptografia do lado do servidor no Edge AWS Snowball

AWS Snowball O Edge oferece suporte à criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). A criptografia do lado do servidor tem a ver com proteção de dados em repouso, e o SSE-S3 tem criptografia multifator forte para proteger os dados em repouso no Amazon S3. Para obter mais informações sobre o SSE-S3, consulte Proteção de dados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) no Manual do usuário do Amazon Simple Storage Service.

Atualmente, o AWS Snowball Edge não oferece criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). O armazenamento compatível com Amazon S3 em dispositivos da Família Snow oferece SSS-C para trabalhos locais de computação e armazenamento. No entanto, você pode usar esse tipo de SSE para proteger dados que foram importados, ou talvez você já a esteja usando nos dados que deseja exportar. Nesses casos, tenha em mente o seguinte:

- Importar:

Se quiser usar SSE-C para criptografar os objetos que importou para o Amazon S3, prefira a criptografia SSE-KMS ou SSE-S3 estabelecida como parte da política desse bucket. No entanto, se você precisar usar o SSE-C para criptografar os objetos que você importou para o Amazon S3, precisará copiar o objeto dentro do seu bucket para criptografar com o SSE-C. Um exemplo de comando CLI para fazer isso é mostrado abaixo:

```
aws s3 cp s3://mybucket/object.txt s3://mybucket/object.txt --sse-c --sse-c-key
 1234567891SAMPLEKEY
```

ou

```
aws s3 cp s3://mybucket s3://mybucket --sse-c --sse-c-key 1234567891SAMPLEKEY --
recursive
```

- Exportar: se quiser exportar objetos criptografados com SSE-SSE, copie esses objetos para outro bucket que não tenha criptografia do lado do servidor ou que tenha SSE-KMS ou SSE-S3 especificada na política desse bucket.

Habilitação de SSE-S3 para dados importados para o Amazon S3 de um Snowball Edge

Use o procedimento a seguir no Console de Gerenciamento do Amazon S3 para ativar o SSE-S3 para dados importados para o Amazon S3. Nenhuma configuração é necessária no Console de Gerenciamento da família AWS Snow ou no próprio dispositivo Snowball.

Para habilitar a criptografia SSE-S3 para os dados que você estiver importando para o Amazon S3, defina as políticas de bucket para todos os buckets para os quais você estiver importando dados. Você atualiza as políticas para negar a permissão de objeto de upload (`s3:PutObject`) se a solicitação de upload não incluir o cabeçalho `x-amz-server-side-encryption`.

Para habilitar o SSE-S3 para dados importados para o Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione o bucket para o qual você deseja importar os dados na lista de buckets.
3. Escolha Permissões.
4. Escolha Bucket Policy.

5. No Bucket policy editor, insira a política a seguir. Substitua todas as instâncias de *YourBucket* nessa política com o nome real do seu bucket.

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```

6. Escolha Salvar.

Você acabou de configurar seu bucket do Amazon S3. Quando os dados são importados para esse bucket, eles são protegidos pelo SSE-S3. Repita esse procedimento para qualquer outro bucket, conforme necessário.

AWS Key Management Service em AWS Snowball Edge

AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle das chaves de criptografia usadas para criptografar seus dados. AWS KMS usa módulos de segurança de hardware (HSMs) para proteger a segurança de suas chaves. Especificamente, o Amazon Resource Name (ARN) da AWS KMS chave que você escolhe para um trabalho no AWS Snowball Edge está associado a uma chave KMS. Essa chave do KMS é usada para criptografar o código de desbloqueio do trabalho. O código de desbloqueio é usado para descriptografar a camada superior de criptografia no arquivo manifesto. As chaves de criptografia armazenadas no arquivo manifesto são usadas para criptografar e descriptografar dados no dispositivo.

No AWS Snowball Edge, AWS KMS protege as chaves de criptografia usadas para proteger os dados em cada AWS Snowball Edge dispositivo. Ao criar o trabalho, você também pode escolher uma chave KMS existente. A especificação do ARN de AWS KMS uma chave AWS Snowball indica AWS KMS keys qual usar para criptografar as chaves exclusivas no dispositivo. AWS Snowball Edge Para obter mais informações sobre as server-side-encryption opções do Amazon S3 suportadas pelo AWS Snowball Edge, consulte. Criptografia do lado do servidor no Edge AWS Snowball

Usando o cliente gerenciado AWS KMS keys para o Snowball Edge

Se você quiser usar o cliente AWS KMS keys gerenciado do Snowball Edge criado para sua conta, siga estas etapas.

Para selecionar a AWS KMS keys para seu trabalho

1. No Console de Gerenciamento da família AWS Snow, escolha Criar trabalho.
2. Selecione o tipo de trabalho e, em seguida, Avançar.
3. Forneça os dados de entrega e, em seguida, escolha Avançar.
4. Preencha os dados do trabalho e, em seguida, escolha Avançar.
5. Defina as opções de segurança. Em Criptografia, para a chave KMS, escolha a chave personalizada Chave gerenciada pela AWS ou uma chave criada anteriormente em AWS KMS, ou escolha Inserir um ARN da chave se precisar inserir uma chave pertencente a uma conta separada.

> **Note**
>
> O ARN do AWS KMS key é um identificador globalmente exclusivo para chaves gerenciadas pelo cliente.

6. Escolha Avançar para concluir a seleção de seu AWS KMS key.
7. Conceda acesso à chave do KMS ao usuário do IAM do dispositivo Snow.

    a. No console do IAM (https://console.aws.amazon.com/iam/), acesse Chaves de criptografia e abra a chave KMS que você escolheu usar para criptografar os dados no dispositivo.

    b. Em Usuários chave, selecione Adicionar, pesquise o usuário do IAM do dispositivo Snow e selecione Anexar.

Criação de uma chave de criptografia de envelope do KMS personalizada

Você tem a opção de usar sua própria chave de criptografia de AWS KMS envelope personalizada com o AWS Snowball Edge. Se optar por criar uma chave própria, ela deve ser criada na mesma região em que o trabalho foi criado.

Para criar sua própria AWS KMS chave para um trabalho, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.

Proteção de dados no seu dispositivo

Protegendo seu AWS Snowball Edge

A seguir estão alguns pontos de segurança que recomendamos que você considere ao usar o AWS Snowball Edge e também algumas informações de alto nível sobre outras precauções de segurança que tomamos quando um dispositivo chega AWS para processamento.

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 cada dispositivo AWS Snowball Edge seja robusto, o clima pode danificar 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**
>
> Os dispositivos AWS Snowball Edge são 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 o adaptador do Amazon S3, os metadados de objeto não são mantidos. Os únicos metadados que permanecem os mesmos são `filename` e `filesize`. Todos os outros metadados são definidos como no exemplo a seguir: `-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]`
- 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). AWS Snowball O Edge usa várias camadas de segurança projetadas para proteger seus dados, incluindo compartimentos invioláveis, criptografia de 256 bits e um TPM padrão do setor projetado para fornecer segurança e cadeia completa de custódia para seus dados.
- Assim que um trabalho de transferência de dados tiver sido processado e verificado, a AWS executa um apagamento de software do dispositivo do Snowball que segue as diretrizes de limpeza de mídia do Instituto Nacional de Padrões e Tecnologia (NIST).

Validação de tags NFC

Os dispositivos Snowball Edge otimizado para computação e Snowball Edge otimizado para armazenamento (para transferência de dados) têm tags NFC incorporadas. Você pode digitalizar essas tags com o aplicativo de verificação do AWS Snowball Edge, 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.

O procedimento a seguir descreve como validar as tags NFC em um dispositivo Snowball Edge. Antes de começar, verifique se você primeiramente executou as cinco etapas a seguir do exercício de conceitos básicos:

1. Crie seu trabalho do Snowball Edge. Para obter mais informações, consulte Criação de um trabalho para solicitar um dispositivo Snow Family
2. Receba o dispositivo. Para ter mais informações, consulte Receber o Snowball Edge.
3. Conecte-se à sua rede local. Para ter mais informações, consulte Conectar-se à rede local.
4. Obtenha suas credenciais e ferramentas. Para ter mais informações, consulte Obter credenciais para acessar um dispositivo Snow Family.
5. Faça o download e instale o Snowball Edge Client. Para ter mais informações, consulte Baixar e instalar o cliente do Snowball Edge.

Para validar as etiquetas NFC

1. Execute o comando do cliente Snowball Edge `snowballEdge get-app-qr-code`. Se você executar esse comando para um nó em um cluster, forneça o número de série (`--device-sn`) para obter um código QR para um único nó. Repita essa etapa para cada nó no cluster. 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. Você pode digitalizar essas tags usando o aplicativo AWS Snowball Edge Verification no Android.

   > **Note**
   >
   > O aplicativo AWS Snowball Edge Verification não está disponível para download, mas se você tiver um dispositivo com o aplicativo já instalado, poderá usá-lo.
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:

- Confirme se o dispositivo tem as opções otimizadas para computação do Snowball Edge (com ou sem GPU).
- Se você tiver o aplicativo em outro dispositivo, tente usar esse dispositivo.
- 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.

Identity and Access Management em AWS Snowball

Cada AWS Snowball trabalho deve ser autenticado. Para fazer isso, crie e gerencie os usuários do IAM na sua conta. Utilizando o IAM, é possível criar e gerenciar usuários e permissões na AWS.

AWS Snowball os usuários devem ter determinadas permissões relacionadas ao IAM para acessar o AWS Snowball AWS Management Console para criar empregos. Um usuário do IAM que cria um trabalho de importação ou exportação também deve ter acesso aos recursos corretos do Amazon Simple Storage Service (Amazon S3), como os buckets do Amazon S3 a serem usados para o trabalho, os recursos, o tópico do Amazon SNS e a AMI compatível com o Amazon EC2 para trabalhos de computação periférica. AWS KMS

> **Important**
>
> Para obter informações sobre como usar o IAM localmente no seu dispositivo, consulte Usar o IAM localmente.

Tópicos

- Controle de acesso para o console da Família Snow e trabalhos de criação

Controle de acesso para o console da Família Snow e trabalhos de criação

Assim como ocorre com todos os serviços da AWS, o acesso ao AWS Snowball requer credenciais que a AWS possa usar para autenticar solicitações. Essas credenciais devem ter permissões para acessar os recursos da AWS, como um bucket do Amazon S3 ou uma função do AWS Lambda. O AWS Snowball difere de duas maneiras:

1. Os trabalhos no AWS Snowball não têm nomes de recurso da Amazon (ARNs).

2. Cabe a você o controle de acesso físico e à rede de um dispositivo on-premises.

Consulte Identity and Access Management para AWS Snow Family para obter detalhes sobre como é possível usar o AWS Identity and Access Management (IAM) e o AWS Snowball para ajudar a proteger seus recursos controlando quem pode acessá-los na Nuvem AWS, bem como recomendações de controle de acesso local.

Identity and Access Management para AWS Snow Family

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Snow Family os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciamento do acesso usando políticas
- Como AWS Snow Family funciona com o IAM
- Exemplos de políticas baseadas em identidade para AWS Snow Family
- Solução de problemas AWS Snow Family de identidade e acesso

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Snow Family.

Usuário do serviço — Se você usar o AWS Snow Family serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Snow Family recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no AWS Snow Family, consulte Solução de problemas AWS Snow Family de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Snow Family recursos da sua empresa, provavelmente tem acesso total AWS Snow Family a. É seu trabalho determinar quais AWS Snow Family recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Snow Family, consulteComo AWS Snow Family funciona com o IAM.

Administrador do IAM – Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao AWS Snow Family. Para ver exemplos de políticas AWS Snow Family baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para AWS Snow Family

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação

multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do usuário do AWS IAM Identity Center .

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a

diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política

gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Snow Family funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Snow Family, saiba com quais recursos do IAM estão disponíveis para uso AWS Snow Family.

Recursos do IAM que você pode usar com AWS Snow Family

Recurso do IAM	AWS Snow Family apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações de políticas	Sim

Recurso do IAM	AWS Snow Family apoio
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados ao serviço	Não

Para ter uma visão de alto nível de como AWS Snow Family e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AWS Snow Family

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. ‘Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos

que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS Snow Family

Para ver exemplos de políticas AWS Snow Family baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Snow Family

Políticas baseadas em recursos dentro AWS Snow Family

Oferece suporte a políticas baseadas em atributos	Sim

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar um principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações políticas para AWS Snow Family

Oferece suporte a ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS Snow Family ações, consulte Ações definidas por AWS Snow Family na Referência de Autorização de Serviço.

As ações de política AWS Snow Family usam o seguinte prefixo antes da ação:

```
snowball
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "snowball:action1",
      "snowball:action2"
         ]
```

Para ver exemplos de políticas AWS Snow Family baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Snow Family

Recursos políticos para AWS Snow Family

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como

prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de AWS Snow Family recursos e seus ARNs, consulte Recursos definidos por AWS Snow Family na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Snow Family.

Para ver exemplos de políticas AWS Snow Family baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Snow Family

Chaves de condição de política para AWS Snow Family

Compatível com chaves de condição de política específicas do serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de AWS Snow Family condição, consulte Chaves de condição AWS Snow Family na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Snow Family.

Para ver exemplos de políticas AWS Snow Family baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Snow Family

ACLs em AWS Snow Family

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS Snow Family

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS Snow Family

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS trabalhar com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS Snow Family

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS Snow Family

Oferece suporte a perfis de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AWS Snow Family a funcionalidade. Edite as funções de serviço somente quando AWS Snow Family fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS Snow Family

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços do AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

Exemplos de políticas baseadas em identidade para AWS Snow Family

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Snow Family . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Snow Family, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Snow Family na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de políticas
- Usar o console do AWS Snow Family
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Snow Family recursos em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do AWS Snow Family

Para acessar o AWS Snow Family console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Snow Family recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o AWS Snow Family console, anexe também a política AWS Snow Family *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas AWS Snow Family de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Snow Family um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Snow Family
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Snow Family recursos

Não estou autorizado a realizar uma ação em AWS Snow Family

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `snowball:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 snowball:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `snowball:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Snow Family.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Snow Family. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Snow Family recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Snow Family compatível com esses recursos, consulteComo AWS Snow Family funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Controle de acesso na Nuvem AWS

Você pode ter credenciais válidas para autenticar suas solicitações na AWS. No entanto, a menos que tenha permissões, não é possível criar ou acessar os recursos da AWS. Por exemplo, você deve ter permissões para criar um trabalho para solicitar um dispositivo Snow Family.

As seções a seguir descrevem como gerenciar permissões baseadas na nuvem para o AWS Snowball. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso aos seus recursos na Nuvem AWS
- Usar políticas baseadas em identidade (políticas do IAM) para o AWS Snowball

Visão geral do gerenciamento de permissões de acesso aos seus recursos na Nuvem AWS

Cada recurso da AWS pertence a uma Conta da AWS, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões. Um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e perfis), e alguns serviços (como o AWS Lambda) também aceitam a anexação de políticas de permissões a recursos.

> **Note**
>
> Um administrador da conta (ou usuário administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Tópicos

- Recursos e operações
- Noções básicas sobre propriedade de recursos
- Gerenciar o acesso a recursos na Nuvem AWS
- Especificar elementos da política: ações, efeitos e entidades principais
- Especificar condições em uma política

Recursos e operações

No AWS Snowball, o recurso principal é um trabalho. O AWS Snowball também tem dispositivos como o Snowball e o AWS Snowball Edge; no entanto, somente é possível usar esses dispositivos no contexto de um trabalho existente. Os buckets do Amazon S3 e as funções do Lambda são recursos do Amazon S3 e do Lambda respectivamente.

Como mencionado anteriormente, os trabalhos não têm nomes de recurso da Amazon (ARNs) associados a eles. Mas outros recursos de serviços, como os buckets do Amazon S3, têm ARNs exclusivos associados a eles, conforme mostrado na tabela a seguir.

O AWS Snowball fornece um conjunto de operações para criar e gerenciar trabalhos. Para uma lista de operações disponíveis, consulte a Referência da API do AWS Snowball.

Noções básicas sobre propriedade de recursos

A Conta da AWS possui os recursos criados na conta, independentemente de quem os criou. Mais especificamente, o proprietário do recurso é a Conta da AWS da entidade principal (ou seja, a conta raiz, um usuário do IAM ou um perfil do IAM) que autentica a solicitação de criação de recursos. Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta raiz da sua Conta da AWS para criar um bucket do S3, sua Conta da AWS será a proprietária do recurso (no AWS Snowball, o recurso é o trabalho).
- Se você criar um usuário do IAM em seu Conta da AWS e conceder permissões para criar um trabalho para solicitar um dispositivo da família Snow para esse usuário, o usuário poderá criar um trabalho para solicitar um dispositivo da família Snow. Porém, sua Conta da AWS à qual o usuário pertence, é proprietária do recurso de trabalho.
- Se você criar uma função do IAM na sua Conta da AWS com permissões para criar um trabalho, qualquer pessoa que possa assumir a função poderá criar um trabalho para solicitar um dispositivo da família Snow. Sua Conta da AWS, à qual o perfil pertence, é a proprietária do recurso de trabalho.

Gerenciar o acesso a recursos na Nuvem AWS

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação de políticas de permissões.

> **Note**
>
> Esta seção discute o uso do IAM no contexto do AWS Snowball. Não são fornecidas informações detalhadas sobre o serviço IAM. Para obter a documentação completa do IAM, consulte O que é o IAM? no Guia do usuário do IAM. Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte a Referência de política do AWS IAM no Guia do usuário do IAM.

As políticas associadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM), e as políticas associadas a um recurso são conhecidas como políticas baseadas em recurso. O AWS Snowball aceita apenas políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em recurso

Políticas baseadas em recurso

Outros serviços, como o Amazon S3, também aceitam políticas de permissões baseadas em recurso. Por exemplo, você pode anexar uma política a um bucket do S3 para gerenciar permissões de acesso a esse bucket. O AWS Snowball não aceita políticas baseadas em recurso.

Especificar elementos da política: ações, efeitos e entidades principais

Para cada trabalho (consulte Recursos e operações), o serviço define um conjunto de operações de API (consulte Referência da API do AWS Snowball) para criar e gerenciar o trabalho em questão. Para conceder permissões a essas operações da API, o AWS Snowball define um conjunto de ações que podem ser especificadas em uma política. Por exemplo, para um trabalho, são definidas as ações a seguir: `CreateJob`, `CancelJob`, e `DescribeJob`. Observe que a execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política mais básicos:

- Recurso: em uma política, você usa um nome do recurso da Amazon (ARN) para identificar o recurso a que a política se aplica. Para ter mais informações, consulte Recursos e operações.

  > **Note**
  >
  > Isso é possível no Amazon S3, no Amazon EC2, no AWS Lambda, no AWS KMS e em muitos outros serviços.
  > O Snowball não aceita a especificação do ARN de um recurso no elemento `Resource` de uma declaração de política do IAM. Para conceder acesso ao Snowball, especifique `“Resource”: “*”` na política.

- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Por exemplo, dependendo do `Effect` especificado, o `snowball:*` concede ou nega as permissões de usuário para realizar todas as operações.

  > **Note**
  >
  > Isso é possível no Amazon EC2, no Amazon S3 e no IAM.

- Efeito: você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.

  > **Note**
  >
  > Isso é possível no Amazon EC2, no Amazon S3 e no IAM.

- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é implicitamente a entidade principal. Para as políticas baseadas em recurso, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (aplica-se somente a políticas baseadas em recurso). O AWS Snowball não aceita politicas baseadas em recurso.

Para saber mais sobre a sintaxe e as descrições da política do IAM, consulte a Referência de política do AWS IAM no Guia do usuário do IAM.

Para obter uma tabela que mostra todas as ações de API do AWS Snowball, consulte Permissões da API do AWS Snowball: referência de ações, recursos e condições.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar as condições de quando uma política deverá entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condition no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do AWS Snowball. Mas existem chaves de condição em toda a AWS que você pode usar conforme apropriado. Para obter uma lista completa de chaves de toda a AWS, consulte Available Keys for Conditions no Guia do usuário do IAM.

Usar políticas baseadas em identidade (políticas do IAM) para o AWS Snowball

Este tópico fornece exemplos de políticas baseadas em identidade que demonstram como um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e perfis). Deste modo, essas políticas concedem permissões para realizar operações nos recursos do AWS Snowball na Nuvem AWS.

> **Important**
>
> Recomendamos analisar primeiro os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos recursos do AWS Snowball. Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos seus recursos na Nuvem AWS.

As seções neste tópico abrangem o seguinte:

- Permissões necessárias para usar o console do AWS Snowball
- Políticas gerenciadas pela AWS (predefinidas) para o AWS Snowball Edge
- Exemplos de política gerenciada pelo cliente

A seguir, um exemplo de uma política de permissões.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
       "Effect": "Allow",
       "Action": [
          "snowball:*",
          "importexport:*"
       ],
       "Resource": "*"
    }
  ]
}
```

A política tem duas instruções:

- A primeira instrução concede permissões para três ações do Amazon S3 (`s3:GetBucketLocation`, `s3:GetObject` e `s3:ListBucket`) em todos os buckets do Amazon S3 usando `arn:aws:s3:::*` como nome do recurso da Amazon (ARN). O ARN especifica um caractere curinga (*) para que o usuário possa escolher qualquer um ou todos os buckets do Amazon S3 para exportar dados.
- A segunda instrução concede permissões para todas as ações do AWS Snowball. Como essas ações não comportam permissões em nível de recursos, a política especifica o caractere curinga (*) e o valor `Resource` também especifica um caractere curinga.

A política não especifica o elemento `Principal` porque, em uma política baseada em identidade, não se especifica a entidade principal que obtém as permissões. Quando você anexar uma política a um usuário, o usuário será a entidade principal implícita. Quando você anexa uma política de permissões a um perfil do IAM, a entidade principal identificada na política de confiança do perfil obtém as permissões.

Para ver uma tabela mostrando todas as ações da API de gerenciamento de trabalhos do AWS Snowball e os recursos aos quais elas se aplicam, consulte Permissões da API do AWS Snowball: referência de ações, recursos e condições.

Permissões necessárias para usar o console do AWS Snowball

A tabela de referência de permissões lista as operações da API de gerenciamento de trabalhos do AWS Snowball e mostra as permissões necessárias para cada operação. Para obter mais informações sobre operações da API de gerenciamento de trabalhos, consulte Permissões da API do AWS Snowball: referência de ações, recursos e condições.

Para usar o Console de Gerenciamento da família AWS Snow, é necessário conceder permissões para ações adicionais, como mostrado na política de permissões a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction",
```

```
                "lambda:GetFunctionConfiguration"
            ],
            "Resource": "arn:aws:lambda:*::function:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:RetireGrant",
                "kms:ListKeys",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:ListRoles",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "importexport.amazonaws.com"
                }
            }
        },
        {
           "Effect": "Allow",
           "Action": [
                "ec2:DescribeImages",
                "ec2:ModifyImageAttribute"
           ],
           "Resource": [
                "*"
           ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sns:Subscribe"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "greengrass:getServiceRoleForAccount"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "snowball:*"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

O console do AWS Snowball precisa dessas permissões adicionais pelos seguintes motivos:

- `ec2:`: permitem que o usuário descreva instâncias compatíveis do EC2 e modifiquem seus atributos para fins de computação local. Para ter mais informações, consulte Usar instâncias de computação compatíveis com o Amazon EC2.
- `kms:`: permitem que o usuário crie ou escolha a chave do KMS que vai criptografar seus dados. Para ter mais informações, consulte AWS Key Management Service em AWS Snowball Edge.
- `iam:`: permitem que o usuário crie ou escolha um ARN do perfil do IAM que o AWS Snowball assumirá para acessar os recursos da AWS associados à criação e ao processamento do trabalho.
- `sns:`: permitem que o usuário crie ou escolha as notificações do Amazon SNS para os trabalhos criados por ele. Para ter mais informações, consulte Notificações para dispositivos da família Snow.

Políticas gerenciadas pela AWS (predefinidas) para o AWS Snowball Edge

A AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. As políticas gerenciadas concedem permissões necessárias para casos de uso comuns, de maneira que você possa evitar a necessidade de investigar quais permissões são necessárias. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Você pode usar as políticas gerenciadas pela AWS a seguir com o AWS Snowball.

Criar uma política do perfil do IAM para o Snowball Edge

É necessário criar uma política de perfil do IAM com permissões de leitura e gravação para os buckets do Amazon S3. O perfil do IAM também deve ter uma relação de confiança com o Snowball. Ter uma relação de confiança significa que a AWS pode gravar os dados no Snowball e nos buckets do Amazon S3, dependendo de você estar importando ou exportando dados.

Quando você cria um trabalho para solicitar um dispositivo da família Snow noConsole de Gerenciamento da família AWS Snow, a criação da função IAM necessária ocorre na etapa 4 na seção Permissão. Esse processo é automático. O perfil do IAM que você permitir que o Snowball assuma será usado apenas para gravar os dados no bucket quando o Snowball chega à AWS com os dados transferidos. O procedimento a seguir descreve esse processo.

Como criar o perfil do IAM para seu trabalho de importação

1. Faça login no AWS Management Console e abra o AWS Snowball console em https://console.aws.amazon.com/importexport/.
2. Escolha Criar trabalho.
3. Na primeira etapa, preencha os detalhes do trabalho de importação no Amazon S3 e escolha Próximo.
4. Na segunda etapa, em Permissão, escolha Criar/Selecionar perfil do IAM.

   O console de gerenciamento do IAM será aberto, mostrando o perfil do IAM que a AWS usa para copiar objetos nos buckets especificados do Amazon S3.
5. Revise os detalhes nessa página e selecione Permitir.

   Você voltará ao Console de Gerenciamento da família AWS Snow, onde ARN do perfil selecionado do IAM) contém o nome do recurso da Amazon (ARN) para o perfil do IAM que você acabou de criar.
6. Escolha Próximo para concluir a criação do perfil do IAM.

O procedimento anterior cria um perfil do IAM que tem permissões de gravação para os buckets do Amazon S3 para os quais planeja importar dados. O perfil do IAM criado tem uma das estruturas a seguir, dependendo de ele ser para um trabalho de importação ou exportação.

Perfil do IAM para um trabalho de importação

```
        {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
```

```
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl",
        "s3:ListBucket",
        "s3:HeadBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Se você usar criptografia do lado do servidor com chaves gerenciadas pelo AWS KMS (SSE-KMS) para criptografar os buckets do Amazon S3 associados ao trabalho de importação, também será necessário adicionar a instrução a seguir ao perfil do IAM.

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

Se os tamanhos de objeto forem maiores, o cliente do Amazon S3 usado para o processo de importação usará carregamento fracionado. Se você iniciar um carregamento fracionado usando SSE-KMS, todas as partes carregadas serão criptografadas usando a chave do AWS KMS especificada. Como as partes são criptografadas, elas devem ser descriptografadas antes de serem montadas para concluir o carregamento fracionado. Portanto, você deve ter permissão para descriptografar a chave do AWS KMS (`kms:Decrypt`) quando executa um carregamento fracionado no Amazon S3 com SSE-KMS.

Veja a seguir um exemplo de um perfil do IAM necessário para um trabalho de importação que precisa da permissão `kms:Decrypt`.

```
{
    "Effect": "Allow",
     "Action": [
       "kms:GenerateDataKey","kms:Decrypt"

     ],
     "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-
efgh-111111111111"
}
```

Veja a seguir um exemplo de um perfil do IAM necessário para um trabalho de exportação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Se você usar criptografia do lado do servidor com chaves gerenciadas pelo AWS KMS para criptografar os buckets do Amazon S3 associados ao seu trabalho de exportação, também será necessário adicionar a instrução a seguir ao perfil do IAM.

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

```
}
```

Você pode criar suas próprias políticas do IAM personalizadas para conceder permissões para operações de API destinadas ao gerenciamento de trabalhos do AWS Snowball. Você pode anexar essas políticas personalizadas a usuários ou grupos do IAM que exijam essas permissões.

Exemplos de política gerenciada pelo cliente

Nesta seção, você encontrará exemplos de políticas de usuário que concedam permissões para diversas ações de gerenciamento de trabalhos do AWS Snowball. Essas políticas funcionam quando você está usando SDKs da AWS ou a AWS CLI. Ao usar o console, você precisa conceder permissões adicionais específicas ao console, o que é abordado em Permissões necessárias para usar o console do AWS Snowball.

> **Note**
>
> Todos os exemplos usam a região us-west-2 e contêm IDs de conta fictícios.

Exemplos

- Exemplo 1: Política de função que permite que um usuário crie um Job para solicitar um dispositivo da família Snow com a API
- Exemplo 2: política de perfil para criação de trabalhos de importação
- Exemplo 3: política de perfil para criação de trabalhos de exportação
- Exemplo 4: política de confiança e permissões de perfil esperadas
- Permissões da API do AWS Snowball: referência de ações, recursos e condições

Exemplo 1: Política de função que permite que um usuário crie um Job para solicitar um dispositivo da família Snow com a API

A política de permissões a seguir é um componente necessário a qualquer política usada para conceder permissão de criação de trabalho ou cluster usando a API de gerenciamento de trabalhos. A instrução é necessária como uma declaração de política de relacionamento de confiança para o perfil do IAM do Snowball.

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

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

Exemplo 2: política de perfil para criação de trabalhos de importação

Você usa a política de confiança de perfil a seguir para criar trabalhos de importação para o Snowball Edge que usam o AWS Lambda habilitado por funções do AWS IoT Greengrass.

```
                {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:GetBucketLocation",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucket",
                "s3:HeadBucket",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:PutObjectAcl",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "snowball:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:AttachPrincipalPolicy",
                "iot:AttachThingPrincipal",
                "iot:CreateKeysAndCertificate",
                "iot:CreatePolicy",
                "iot:CreateThing",
                "iot:DescribeEndpoint",
                "iot:GetPolicy"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "greengrass:CreateCoreDefinition",
                "greengrass:CreateDeployment",
                "greengrass:CreateDeviceDefinition",
                "greengrass:CreateFunctionDefinition",
                "greengrass:CreateGroup",
                "greengrass:CreateGroupVersion",
                "greengrass:CreateLoggerDefinition",
```

```
                "greengrass:CreateSubscriptionDefinition",
                "greengrass:GetDeploymentStatus",
                "greengrass:UpdateGroupCertificateConfiguration",
                "greengrass:CreateGroupCertificateAuthority",
                "greengrass:GetGroupCertificateAuthority",
                "greengrass:ListGroupCertificateAuthorities",
                "greengrass:ListDeployments",
                "greengrass:GetGroup",
                "greengrass:GetGroupVersion",
                "greengrass:GetCoreDefinitionVersion"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Exemplo 3: política de perfil para criação de trabalhos de exportação

Você usa a política de confiança de perfil seguinte para a criação de trabalhos de exportação para o Snowball Edge que usam o AWS Lambda habilitado por funções do AWS IoT Greengrass.

```
                    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
           "Effect": "Allow",
           "Action": [
                "snowball:*"
           ],
```

```
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:AttachPrincipalPolicy",
                "iot:AttachThingPrincipal",
                "iot:CreateKeysAndCertificate",
                "iot:CreatePolicy",
                "iot:CreateThing",
                "iot:DescribeEndpoint",
                "iot:GetPolicy"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "greengrass:CreateCoreDefinition",
                "greengrass:CreateDeployment",
                "greengrass:CreateDeviceDefinition",
                "greengrass:CreateFunctionDefinition",
                "greengrass:CreateGroup",
                "greengrass:CreateGroupVersion",
                "greengrass:CreateLoggerDefinition",
                "greengrass:CreateSubscriptionDefinition",
                "greengrass:GetDeploymentStatus",
                "greengrass:UpdateGroupCertificateConfiguration",
                "greengrass:CreateGroupCertificateAuthority",
                "greengrass:GetGroupCertificateAuthority",
                "greengrass:ListGroupCertificateAuthorities",
```

```
                "greengrass:ListDeployments",
                "greengrass:GetGroup",
                "greengrass:GetGroupVersion",
                "greengrass:GetCoreDefinitionVersion"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Exemplo 4: política de confiança e permissões de perfil esperadas

A política de permissões de perfil esperadas a seguir é necessária para o uso de um perfil de serviço existente. Essa configuração é realizada apenas uma vez.

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": ["[[snsArn]]"]
        },
        {
            "Effect": "Allow",
            "Action":
            [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricData",
                "cloudwatch:PutMetricData"
            ],
            "Resource":
            [
                "*"
            ],
            "Condition": {
                    "StringEquals": {
                        "cloudwatch:namespace": "AWS/SnowFamily"
                    }
            }
```

```
        }
    ]
}
```

A política de confiança de perfil esperada a seguir é necessária para o uso de um perfil de serviço existente. Essa configuração é realizada apenas uma vez.

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

Permissões da API do AWS Snowball: referência de ações, recursos e condições

Ao configurar Controle de acesso na Nuvem AWS e escrever uma política de permissões que você pode anexar a uma identidade do IAM (políticas baseadas em identidade), é possível usar a lista de a seguir como referência. A inclui cada operação da API e gerenciamento de trabalhos do AWS Snowball e as ações correspondentes para as quais você pode conceder permissões para executar a ação. Ela também inclui, para cada operação da API, o recurso da AWS para o qual você pode conceder as permissões. Você especifica as ações no campo `Action` da política e o valor do recurso no campo `Resource` da política.

Você pode usar as chaves de condição utilizadas por toda a AWS em suas políticas do AWS Snowball para expressar condições. Para obter uma lista completa das chaves da AWS, consulte Available Keys no Guia do usuário do IAM.

> **Note**
>
> Para especificar uma ação, use o prefixo `snowball:` seguido do nome da operação da API (por exemplo, `snowball:CreateJob`).

Registro em log e monitoramento no AWS Snowball

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Snowball suas AWS soluções. Você deve coletar dados de monitoramento para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus AWS Snowball recursos e responder a possíveis incidentes:

AWS CloudTrail Registros

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço na AWS Snowball Job Management API ou ao usar o AWS Console. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação de API que foi feita ao AWS Snowball serviço, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Registrar em log chamadas de API do AWS Snowball Edge com o AWS CloudTrail.

Validação de conformidade para AWS Snowball

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança de infraestrutura em AWS Snowball

Como serviço gerenciado, AWS Snow Family é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Snow Family pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Validação de dados com trabalhos do Snowball Edge

A seguir, você encontrará informações sobre como o AWS Snowball Edge valida transferências de dados e as etapas manuais que você pode seguir para ajudar a garantir a integridade dos dados durante e depois de um trabalho.

Tópicos

Validação de soma de verificação de dados transferidos

Quando você copia um arquivo de uma fonte de dados local usando o Amazon S3 para o Snowball Edge, várias somas de verificação são criadas. Essas somas de verificação são usadas para validar automaticamente os dados à medida que são transferidos.

Em um nível mais alto, essas somas de verificação são criadas para cada arquivo (ou para partes de arquivos grandes). Para o Snowball Edge, essas somas de verificação são visíveis quando você executa o comando do AWS CLI a seguir em relação a um bucket no dispositivo. As somas de verificação são usadas para validar a integridade dos dados durante as transferências e ajudam a garantir que os dados sejam copiados corretamente.

```
aws s3api list-objects --bucket bucket-name --endpoint http://ip:8080 --profile edge-
profile
```

Quando essas somas de verificação não corresponderem, não importaremos os dados associados para o Amazon S3.

Criação de inventário local durante a transferência do Snowball

Crie um inventário local dos arquivos copiados para o Snowball ao usar o adaptador do Amazon S3 ou CLI. O conteúdo do inventário local pode ser usado para comparar com o que está no armazenamento ou no servidor local.

Por exemplo,

```
aws s3 cp folder/ s3://bucket --recursive > inventory.txt
```

Erros de validação comuns

Quando ocorrer um erro de validação, os dados correspondentes (um arquivo ou uma parte de um arquivo grande) não serão gravados no destino. As causas comuns para erros de validação são as seguintes:

- Tentativa de copiar links simbólicos.
- Tentativa de copiar arquivos que estão sendo ativamente modificados. A tentativa falha ao validar a soma de verificação e é marcada como falha na transferência.
- Tentativa de copiar arquivos maiores que 5 TB.
- Tentativa de copiar tamanhos de peças maiores que 2 GiB.
- Tentativa de copiar arquivos para um dispositivo Snowball Edge que já tenha alcançado a capacidade máxima de armazenamento físico de dados.
- Tentativa de copiar arquivos para um dispositivo Snowball Edge que não siga as diretrizes de nomeação de chave de objeto do Amazon S3.

Quando qualquer um desses erros de validação ocorrer, ele será registrado. Você pode executar etapas para identificar manualmente em quais arquivos houve falha de validação e por quê. Para obter mais informações, consulte Validação manual de dados para o Snowball Edge após a importação para o Amazon S3.

Validação manual de dados para o Snowball Edge após a importação para o Amazon S3

Após a conclusão de um trabalho de importação, você terá várias opções para validar manualmente os dados no Amazon S3, conforme descrito a seguir.

Verificar o relatório de conclusão do trabalho e os logs associados

Sempre que os dados forem importados ou exportados do Amazon S3, será disponibilizado um relatório de trabalho em PDF para download. Para trabalhos de importação, esse relatório será

disponibilizado ao final do processo de importação. Para ter mais informações, consulte Obter o relatório e logs de conclusão de trabalho no console.

Inventário do S3

Se você transferiu uma grande quantidade de dados para o Amazon S3 em vários trabalhos, verificar cada relatório de conclusão pode não ser um uso eficiente do tempo. Em vez disso, você pode obter um inventário de todos os objetos em um ou mais buckets do Amazon S3. O Inventário Amazon S3 fornece um arquivo de valores em formato CSV (separado por vírgulas) mostrando seus objetos e os metadados correspondentes por dia ou por semana. Esse arquivo abrange objetos de um bucket do Amazon S3 ou de um prefixo compartilhado (ou seja, objetos que tenham nomes que comecem com uma string em comum).

Assim que tiver o inventário dos buckets do Amazon S3 para o qual importou os dados, você poderá facilmente compará-los com os arquivos que transferiu em seu local dos dados de origem. Dessa forma, você poderá identificar rapidamente quais arquivos não foram transferidos.

Use o comando de sincronização do Amazon S3

Se a sua estação de trabalho puder se conectar com a Internet, você poderá fazer uma validação final de todos os seus arquivos transferidos executando o comando `aws s3 sync` da AWS CLI. Esse comando sincroniza diretórios e prefixos do S3. Esse comando copia os arquivos novos e atualizados recursivamente a partir do diretório de origem para o destino. Para obter mais informações, consulte sync na Referência de comandos do AWS CLI.

> **Important**
>
> Se você especificar seu armazenamento local como o destino para esse comando, certifique-se de fazer um backup dos arquivos que sincronizar. Esses arquivos são substituídos pelo conteúdo na origem do Amazon S3 especificada.

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 o trabalho, cada endereço de e-mail que você tiver especificado para obter notificações do Amazon SNS receberá um e-mail de notificações da AWS solicitando 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. O 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 gerenciada pela AWS não podem receber alterações no status do trabalho do Snow porque o perfil do IAM de importação do Snow não tem acesso à chave KMS gerenciada pela AWS para executar as ações `Decrypt` e `GenerateDataKey`. Além disso, as políticas de chaves KMS gerenciadas pela AWS 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.
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 KMS da AWS. Consulte

   c. Para cada tipo de KMS, são exibidos descrição, conta e ARN do KMS.
5. Para usar uma chave personalizada da sua conta da AWS, escolha o campo Chave do AWS KMS e selecione a chave personalizada do KMS na lista. Para obter instruções sobre como criar KMSs personalizados, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.

   Para usar um ARN personalizado do KMS de sua conta da AWS ou de outra conta da AWS, insira-o no campo Chave do KMS da AWS.
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 no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o Seletor de regiões 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	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) has been created. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Preparação do dispositivo	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being prepared. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Exportação	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being Exported. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Em trânsito	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is in transit to you. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Entregue	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) was delivered to you. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Em trânsito para a AWS	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is in transit to AWS. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

No departamento de triagem	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is at AWS sorting facility. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Na AWS	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is at AWS. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Importação	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is being imported. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Concluído	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) complete.\nThanks for using AWS Snow Family.\nCan you take a quick survey on your experience? Survey here: http://bit.ly/1pLQJMY. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Status do trabalho	Notificações do SNS

Status do trabalho	Notificações do SNS

Cancelado	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) was canceled. More info - https://console.aws.amazon.com/importexport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Registrar em log chamadas de API do AWS Snowball Edge com o AWS CloudTrail

O serviço Snowball ou da Família AWS Snow se integra ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço. O CloudTrail captura todas as chamadas de API para o serviço da Família AWS Snow. As chamadas capturadas incluem as do console da Família AWS Snowball e as de código para a API de gerenciamento de trabalhos da Família AWS Snowball. Se você criar uma trilha, será possível habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para chamadas de API da Família AWS Snowball. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Com as informações coletadas pelo CloudTrail, você pode determinar qual solicitação foi feita para a API da Família AWS Snowball, o endereço IP da solicitação feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do AWS Snowball Edge no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no AWS Snowball Edge, ela é registrada em um evento do CloudTrail com outros eventos de serviços da AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Trabalhar com o histórico de eventos do CloudTrail no Guia do Usuário do AWS CloudTrail.

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS Snowball Edge, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos no log de todas as Regiões da AWS na partição da AWS e entrega os arquivos de log ao bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail

- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações de gerenciamento de trabalhos são documentadas em Referência da API do AWS Snowball e são registradas pelo CloudTrail com as seguintes exceções:

- A operação CreateAddress não é registrada para proteger informações confidenciais do cliente.
- Todas as chamadas de API somente leitura (para operações de API que começam com o prefixo de `Get`, `Describe` ou `List`) não registram elementos de resposta.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou AWS Identity and Access Management (usuário do IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail no Guia do usuário do AWS CloudTrail.

Noções básicas sobre entradas de arquivos de log para o AWS Snowball Edge

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a operação DescribeJob.

```
      {"Records": [
    {
        "eventVersion": "1.05",
        "userIdentity": {
            "type": "Root",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:root",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {"attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-22T21:58:38Z"
            }},
            "invokedBy": "signin.amazonaws.com"
        },
        "eventTime": "2019-01-22T22:02:21Z",
        "eventSource": "snowball.amazonaws.com",
        "eventName": "DescribeJob",
        "awsRegion": "eu-west-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "signin.amazonaws.com",
        "requestParameters": {"jobId": "JIDa1b2c3d4-0123-abcd-1234-0123456789ab"},
        "responseElements": null,
        "requestID": "12345678-abcd-1234-abcd-ab0123456789",
        "eventID": "33c7ff7c-3efa-4d81-801e-7489fe6fff62",
        "eventType": "AwsApiCall",
        "recipientAccountId": "444455556666"
    }
]}
```

AWS Snowball Cotas Edge

A seguir, você encontrará informações sobre as limitações de uso do AWS Snowball Edge dispositivo.

> **Important**
>
> Ao transferir dados para o Amazon Simple Storage Service (Amazon S3) usando um Snowball Edge, lembre-se de que determinados objetos do Amazon S3 podem variar de tamanho, de um mínimo de 0 byte a, no máximo, 5 terabytes (TB).

Disponibilidade da região para AWS Snowball Edge

A tabela a seguir destaca as regiões em que AWS Snowball Edge está disponível.

Região	Disponibilidade do Snowball Edge
Leste dos EUA (Ohio)	✓
Leste dos EUA (N. da Virgínia)	✓
Oeste dos EUA (N. da Califórnia)	✓
Oeste dos EUA (Oregon)	✓
AWS GovCloud (Leste dos EUA)	✓
AWS GovCloud (Oeste dos EUA)	✓
Canadá (Central)	✓
Ásia-Pacífico (Jacarta)	✓
Ásia-Pacífico (Mumbai)	✓
Ásia-Pacífico (Osaka)	✓
Ásia-Pacífico (Seul)	✓

Região	Disponibilidade do Snowball Edge
Ásia-Pacífico (Singapura)	✓
Ásia-Pacífico (Sydney)	✓
Ásia-Pacífico (Tóquio)	✓
Europa (Frankfurt)	✓
Europa (Irlanda)	✓
Europa (Londres)	✓
Europa (Milão)	✓
Europa (Paris)	✓
Europa (Estocolmo)	✓
Oriente Médio (Emirados Árabes Unidos)	✓
América do Sul (São Paulo)	✓

Para obter informações sobre AWS regiões e endpoints suportados, consulte os endpoints e cotas da família AWS Snow no Referência geral da AWS

Limitações para AWS Snowball Edge trabalhos

Existem as seguintes limitações para a criação de tarefas de AWS Snowball Edge dispositivos:

- Por motivos de segurança, os trabalhos usando um AWS Snowball Edge dispositivo devem ser concluídos em até 360 dias após a preparação. Se você precisar manter um ou mais dispositivos por mais de 360 dias, consulteAtualizar o certificado SSL. Caso contrário, após 360 dias, o dispositivo ficará bloqueado, não poderá mais ser acessado e deverá ser devolvido. Se o AWS Snowball Edge dispositivo ficar bloqueado durante um trabalho de importação, ainda poderemos transferir os dados existentes no dispositivo para o Amazon S3.
- AWS Snowball O Edge oferece suporte à criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) e à criptografia do lado do servidor com

chaves gerenciadas (SSE-KMS). AWS Key Management Service O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow oferece SSS-C para trabalhos de computação e armazenamento locais. Para ter mais informações, consulte Como proteger dados usando criptografia do lado do servidor no Guia do usuário do Amazon Simple Storage Service.

- Se você estiver usando um AWS Snowball Edge dispositivo para importar dados e precisar transferir mais dados do que cabem em um único dispositivo Snowball Edge, crie trabalhos adicionais. Cada trabalho de exportação pode usar vários dispositivos Snowball Edge.
- O limite de serviço padrão para a quantidade de dispositivos Snowball Edge que é possível ter por vez é um por conta, por Região da AWS. Se quiser aumentar o limite de serviço ou criar um trabalho de cluster, entre em contato com o AWS Support.
- Os metadados de objetos transferidos para um dispositivo não persistem. Os únicos metadados que permanecem os mesmos são `filename` e `filesize`. Todos os outros metadados são definidos como no seguinte exemplo:

```
-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]
```

Limites de taxa em AWS Snowball Edge

O limitador de taxa é usado para controlar a taxa de solicitações em um ambiente de cluster de servidores.

Limite de conexão do adaptador do Amazon Snow S3

O limite máximo de conexão é mil para o Snowball Edge no Amazon S3. Todas as conexões além de mil são descartadas.

Limitações de transferência de dados on-premises com um dispositivo Snowball Edge

Existem as seguintes limitações para transferir dados de ou para um AWS Snowball Edge dispositivo local:

- Os arquivos devem estar em um estado estático enquanto estiverem sendo gravados. Arquivos que são modificados enquanto estão sendo transferidos não são importados para o Amazon S3.
- Os quadros jumbo não são compatíveis, ou seja, quadros Ethernet com mais de 1.500 bytes de carga útil.

- Ao selecionar quais dados devem ser exportados, lembre-se de que os objetos com barra final nos nomes (/ ou \) não serão transferidos. Antes de exportar qualquer objeto com barras finais, atualize os nomes para remover a barra.
- Ao usar transferência de dados fracionada, o tamanho máximo da parte é de 2 GiB.

Limitações de remessa de um Snowball Edge

As seguintes limitações existem para o envio de um AWS Snowball Edge dispositivo:

- AWS não enviará um dispositivo Snowball Edge para uma caixa postal.
- AWS não enviará um dispositivo Snowball Edge entre regiões fora dos EUA — por exemplo, da UE (Irlanda) para a UE (Frankfurt) ou para a Ásia-Pacífico (Sydney).
- Mover um dispositivo Snowball Edge para um endereço fora do país especificado quando o trabalho foi criado não é permitido e é uma violação dos termos de AWS serviço.

Para obter mais informações sobre envio, consulte Considerações de envio para dispositivos da Família Snow.

Limitações de processamento do Snowball Edge devolvido para importação

Para importar seus dados para AWS, o dispositivo deve atender aos seguintes requisitos:

- O AWS Snowball Edge dispositivo não deve ser comprometido. Exceto para abrir as três portas na frente, traseira e superior, ou para adicionar e substituir o filtro de ar opcional, não abra o AWS Snowball Edge dispositivo por nenhum motivo.
- O dispositivo não deve estar fisicamente danificado. Para evitar danos, feche as três portas do dispositivo Snowball Edge até que as travas façam um clique.
- A tela E Ink no dispositivo Snowball Edge deve estar visível. Também deve mostrar a etiqueta de devolução que foi gerada automaticamente quando você terminou de transferir seus dados para o AWS Snowball Edge dispositivo.

> **Note**
>
> Todos os dispositivos Snowball Edge devolvidos que não atenderem a esses requisitos serão apagados sem o trabalho executado.

Solução de problemas AWS Snowball do E

Lembre-se das diretrizes gerais a seguir ao solucionar problemas.

- Os objetos no Amazon S3 têm um limite máximo de tamanho de arquivo de 5 TB.
- Os objetos transferidos para um AWS Snowball Edge dispositivo têm um tamanho máximo de chave de 933 bytes. Os nomes de chaves que incluem caracteres com mais de 1 byte cada ainda têm 933 bytes de tamanho máximo da chave. Ao determinar o tamanho da chave, inclua o nome do arquivo ou do objeto e também seu caminho ou prefixos. Desse modo, arquivos com nomes de arquivos curtos em um caminho muito aninhado podem ter chaves com mais de 933 bytes. O nome do bucket não é incluído no caminho ao determinar o tamanho da chave. Estes são alguns exemplos.

Nome do objeto	Nome do bucket	Nome do bucket e do caminho	Comprimento da chave
`sunflower-1.jpg`	`pictures`	`sunflower-1.jpg`	15 caracteres
`receipts.csv`	`MyTaxInfo`	`/Users/Eric/Documents/2016/January/`	47 caracteres
`bhv.1`	`$7$zWwwXKQj$gLAOoZCj$r8p`	`/.VfV/FqGC3QN$7BXys3KHYePfuIOMNjY83dVx ugPYlxVg/evpcQEJLT/rSwZc$MlVVf/$hwefVISRqwepB$/BiiD/PP`	135 caracteres

Nome do objeto	Nome do bucket	Nome do bucket e do caminho	Comprimento da chave
		`F$twRAjrD/fIMp/0NY`	

- Por motivos de segurança, os trabalhos usando um AWS Snowball Edge dispositivo devem ser concluídos em até 360 dias após a preparação. Se você precisar manter um ou mais dispositivos por mais de 360 dias, consulteAtualizar o certificado SSL. Caso contrário, após 360 dias, o dispositivo ficará bloqueado, não poderá mais ser acessado e deverá ser devolvido. Se o AWS Snowball Edge dispositivo ficar bloqueado durante um trabalho de importação, ainda poderemos transferir os dados existentes no dispositivo para o Amazon S3.
- Se você encontrar erros inesperados ao usar um AWS Snowball Edge dispositivo, queremos saber mais sobre isso. Copie os registros relevantes e inclua-os junto com uma breve descrição dos problemas que você encontrou em uma mensagem para AWS Support. Para obter mais informações sobre logs, consulte Comandos para o Snowball Edge Client.

Tópicos

Como identificar seu dispositivo

Use o comando `describe-device` para encontrar o tipo de dispositivo e, em seguida, procure o valor retornado de `DeviceType` na tabela abaixo para determinar a configuração.

```
snowballEdge describe-device
```

Example da saída **`describe-device`**

```
{
"DeviceId" : "JID-206843500001-35-92-20-211-23-06-02-18-24",
"UnlockStatus" : {
  "State" : "UNLOCKED"
},
"ActiveNetworkInterface" : {
  "IpAddress" : "127.0.0.1"
},
"PhysicalNetworkInterfaces" : [ {
  "PhysicalNetworkInterfaceId" : "s.ni-8d0ef958ec860ac7c",
  "PhysicalConnectorType" : "RJ45",
  "IpAddressAssignment" : "DHCP",
  "IpAddress" : "172.31.25.194",
  "Netmask" : "255.255.240.0",
  "DefaultGateway" : "172.31.16.1",
  "MacAddress" : "02:38:30:12:a3:7b"
} ],
"DeviceCapacities" : [ {
  "Name" : "HDD Storage",
  "Unit" : "Byte",
  "Total" : 39736350227824,
  "Available" : 985536581632
}, {
  "Name" : "SSD Storage",
  "Unit" : "Byte",
  "Total" : 6979321856000,
  "Available" : 6979321856000
}, {
  "Name" : "vCPU",
  "Unit" : "Number",
```

```
    "Total" : 52,
    "Available" : 52
  }, {
    "Name" : "Memory",
    "Unit" : "Byte",
    "Total" : 223338299392,
    "Available" : 223338299392
  }, {
    "Name" : "GPU",
    "Unit" : "Number",
    "Total" : 0,
    "Available" : 0
  } ],
  "DeviceType" : "EDGE_C"
}
```

`DeviceType` e configurações de dispositivos da Família Snow

Valor do **`DeviceType`**	Configuração do dispositivo
`EDGE`	Snowball Edge otimizado para armazenamento (com funcionalidade de computação do EC2)
`EDGE_C`	Snowball Edge otimizado para computação com AMD EPYC Gen1 e HDD
`EDGE_CG`	Snowball Edge otimizado para computação com AMD EPYC Gen1, HDD e GPU
`EDGE_S`	Snowball Edge otimizado para armazenamento
`V3_5C`	Snowball Edge otimizado para computação com AMD EPYC Gen2 e NVME
`V3_5S`	Otimizado para armazenamento do Snowball Edge

Para obter mais informações sobre configurações de dispositivos do Snowball Edge, consulte AWS Snowball Diferenças do dispositivo Edge.

Solução de problemas de inicialização

As informações a seguir podem ajudá-lo a solucionar certos problemas que você possa ter com a inicialização de seus dispositivos da Família Snow.

- Aguarde 10 minutos para que um dispositivo inicialize. Evite mover ou usar o dispositivo durante esse período.
- Verifique se as duas extremidades do cabo que fornece alimentação estão conectadas com segurança.
- Substitua o cabo de alimentação por outro cabo que você saiba que está bom.
- Conecte o cabo que fornece energia a outra fonte de alimentação que você sabe que está boa.

Solução de problemas com a tela LCD durante a inicialização

Às vezes, depois de ligar um dispositivo Snowball Edge, a tela LCD pode encontrar um problema.

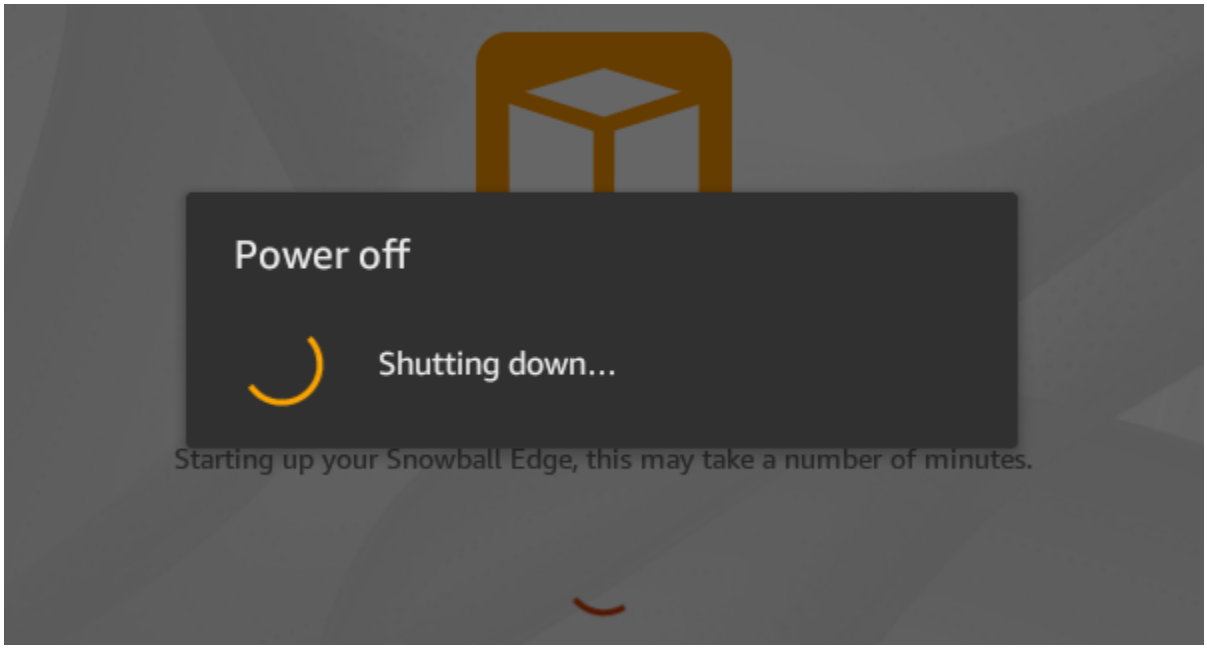
- A tela LCD fica preta e não exibe uma imagem depois que você conecta o dispositivo Snowball Edge à alimentação e pressiona o botão liga/desliga acima da tela LCD.
- A tela LCD não passa da configuração do Snowball Edge. Isso pode levar alguns minutos. mensagem e a tela de configuração de rede não aparece.

Ação a ser tomada quando a tela LCD estiver preta após pressionar o botão liga/desliga

1. Verifique se o dispositivo Snowball Edge está conectado a uma fonte de alimentação e se a fonte de alimentação está fornecendo energia.
2. Deixe o dispositivo conectado à fonte de alimentação por 1 a 2 horas. Verifique se as portas na parte frontal e traseira do dispositivo estão abertas.
3. Volte para o dispositivo e a tela LCD estará pronta para uso.

Ação a ser tomada quando o Snowball Edge não avança para a tela de configuração de rede

1. Deixe a tela ficar na mensagem Configurando seu Snowball Edge, isso pode levar alguns minutos por 10 minutos.
2. Na tela, escolha o botão Reiniciar exibição. A mensagem Desligando... aparecerá e, em seguida, a mensagem Configurando seu Snowball Edge. Isso pode levar alguns minutos aparecerá e o dispositivo iniciará normalmente.



Se a tela LCD não passar da mensagem Configuração do Snowball Edge, isso pode levar alguns minutos após usar o botão Reiniciar exibição, use o procedimento a seguir.

Medida a ser tomada

1. Acima da tela LCD, pressione o botão liga/desliga para desligar o dispositivo.

2. Desconecte todos os cabos do dispositivo.
3. Deixe o dispositivo desligado e desconectado por 20 minutos.
4. Conecte os cabos de energia e rede.
5. Acima da tela LCD, pressione o botão liga/desliga para ligar o dispositivo.

Se o problema persistir, entre em contato AWS Support para devolver o dispositivo e receber um novo dispositivo Snowball Edge.

Solução de problemas de conexão

As informações a seguir podem ajudar a solucionar determinados problemas que possam ocorrer com a conexão ao Snowball Edge:

- Roteadores e switches que funcionam a uma taxa de 100 megabytes por segundo não funcionam com um Snowball Edge. Recomendamos usar switches que funcionam a uma taxa de 1 GB por segundo (ou mais rápido).
- Caso ocorram erros estranhos de conexão com o dispositivo, desligue o Snowball Edge, desconecte todos os cabos e aguarde 10 minutos. Após os 10 minutos, reinicie o dispositivo e tente novamente.
- Verifique se nenhum software antivírus ou firewalls bloqueiam a conexão de rede do dispositivo Snowball Edge.
- Esteja ciente de que a interface de arquivos e a interface do Amazon S3 têm endereços IP diferentes.

Para obter solução de problemas de conexão mais avançadas, siga as seguintes etapas:

- Se não puder se comunicar com o Snowball Edge, efetue o "ping" no endereço IP do dispositivo. Se o ping retornar `no connect`, confirme o endereço IP para o dispositivo e confirme a configuração de rede local.
- Se o endereço IP estiver correto e as luzes na parte de trás do dispositivo estiverem piscando, use o telnet para testar o dispositivo nas portas 22, 9091 e 8080. Testar a porta 22 determina se o Snowball Edge está funcionando corretamente. O teste da porta 9091 determina se a AWS CLI pode ser usada para enviar comandos ao dispositivo. Testar a porta 8080 ajuda a garantir que o dispositivo pode gravar nos buckets do Amazon S3 presentes apenas com o adaptador do S3. Caso consiga se conectar na porta 22, mas não na porta 8080, primeiro desligue o Snowball Edge

e, em seguida, desconecte todos os cabos. Aguarde 10 minutos e, em seguida, reconecte-o e inicie novamente.

Solução de problemas de **`unlock-device`** comando

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 Snowpara 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.

Solução de problemas do arquivo manifesto

Cada trabalho tem um arquivo manifesto específico associado a ele. Se você criar vários trabalhos, acompanhe qual manifesto se refere a cada trabalho.

Se você perder um arquivo de manifesto ou se um arquivo de manifesto estiver corrompido, você poderá baixar o arquivo de manifesto para um trabalho específico novamente. Você faz isso usando o console ou uma das AWS APIs. AWS CLI

Solução de problemas de credenciais

Use os tópicos a seguir para ajudar a resolver problemas das credenciais com o Snowball Edge.

Não foi possível localizar AWS CLI as credenciais

Se você estiver se comunicando com o AWS Snowball Edge dispositivo por meio da interface do Amazon S3 usando AWS CLI o, você pode encontrar uma mensagem de erro que diz Não foi possível localizar as credenciais. Você pode configurar as credenciais executando “aws configure”.

Medida a ser tomada

Configure AWS as credenciais que ele AWS CLI usa para executar comandos para você. Para obter mais informações, consulte Configuração da AWS CLI no Guia do usuário da AWS Command Line Interface .

Mensagem de erro: verifique sua chave de acesso secreta e a assinatura

Ao usar a interface do Amazon S3 para transferir dados para um Snowball Edge, você pode encontrar a seguinte mensagem de erro.

```
An error occurred (SignatureDoesNotMatch) when calling the CreateMultipartUpload
 operation: The request signature we calculated does not match the signature you
 provided.
Check your AWS secret access key and signing method. For more details go to:
http://docs.aws.amazon.com/AmazonS3/latest/dev/
RESTAuthentication.html#ConstructingTheAuthenticationHeader
```

Medida a ser tomada

Obtenha suas credenciais do Snowball Edge Client. Para ter mais informações, consulte Como obter as credenciais.

Solucionando problemas de interface NFS

O dispositivo da família Snow pode indicar que o status da interface NFS é`DEACTIVATED`. Isso pode ocorrer se o dispositivo da família Snow for desligado sem primeiro interromper a interface NFS.

Medida a ser tomada

Para corrigir o problema, pare e reinicie o serviço NFS usando as etapas a seguir.

1. Use o `describe-service` comando para determinar o status do serviço:

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

O comando retorna o seguinte:

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

2. Use o `stop-service` comando para interromper o serviço NFS.

```
snowballEdge stop-service --service-id nfs
```

3. Use o `start-service` comando para iniciar o serviço NFS. Para obter mais informações, consulte Iniciando o serviço NFS no dispositivo Snow Family.

```
snowballEdge start-service  --virtual-network-interface-arns vni-arn --service-id
 nfs  --service-configuration  AllowedHosts=0.0.0.0/0
```

4. Use o `describe-service` comando para garantir que o serviço esteja em execução.

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

Se o valor do `State` nome for`ACTIVE`, o serviço de interface NFS está ativo.

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

Solução de problemas de transferência de dados

Se tiver problemas de desempenho ao transferir dados para ou de um Snowball Edge, consulte Performance para obter recomendações e orientações sobre como melhorar o desempenho de transferência. As considerações a seguir podem ajudar a solucionar problemas que possam ocorrer com transferências de dados para ou de um Snowball Edge.

- Não é possível transferir dados para o diretório raiz do Snowball Edge. Se estiver com problemas para transferir dados para o dispositivo, verifique se está transferindo dados para um subdiretório. Os subdiretórios de nível superior têm os nomes dos buckets do Amazon S3 incluídos no trabalho. Coloque os dados nesses subdiretórios.
- Se estiver usando Linux e não puder fazer o upload de arquivos com caracteres UTF-8 para um dispositivo AWS Snowball Edge , isto pode se dever a que o servidor Linux não reconhece codificação de caracteres UTF-8. Corrija essa questão instalando o pacote `locales` no servidor Linux e configure-o para usar uma das configurações locais do UTF-8, como `en_US.UTF-8`. O pacote `locales` pode ser configurado exportando a variável de ambiente `LC_ALL`, por exemplo: `export LC_ALL=en_US.UTF-8`
- Ao usar a interface do Amazon S3 com o AWS CLI, você pode trabalhar com arquivos ou pastas com espaços em seus nomes, como `my photo.jpg` ou. `My Documents` No entanto, certifique-se de que você lida com os espaços corretamente. Para obter mais informações, consulte Especificar valores de parâmetro para o AWS CLI no Manual do usuário do AWS Command Line Interface .

Solução de AWS CLI problemas

Use os tópicos a seguir para ajudar a resolver problemas ao trabalhar com um dispositivo AWS Snowball Edge e o AWS CLI.

AWS CLI mensagem de erro: “O perfil não pode ser nulo”

Ao trabalhar com o AWS CLI, você pode encontrar uma mensagem de erro que diz que o perfil não pode ser nulo. Você pode encontrar esse erro se o AWS CLI não tiver sido instalado ou se um AWS CLI perfil não tiver sido configurado.

Medida a ser tomada

Certifique-se de ter baixado e configurado o AWS CLI em sua estação de trabalho. Para obter mais informações, consulte Instalar o AWS CLI Usando o Instalador Integrado (Linux, macOS ou Unix) no AWS Command Line Interface Guia do Usuário.

Erro de ponteiro nulo ao transferir dados com o AWS CLI

Ao usar o AWS CLI para transferir dados, você pode encontrar um erro de ponteiro nulo. Esse erro pode ocorrer nas seguintes condições:

- Se o nome de arquivo especificado estiver digitado errado, por exemplo, `flowwer.png` ou `flower.npg` em vez de `flower.png`
- Se o caminho especificado estiver incorreto, por exemplo, `C:\Doccuments\flower.png` em vez de `C:\Documents\flower.png`
- Se o arquivo estiver corrompido

Medida a ser tomada

Confirme se o nome de arquivo e o caminho estão corretos e tente novamente. Caso esse problema permaneça, confirme se o arquivo não foi corrompido, aborte a transferência ou tente reparar o arquivo.

Solução de problemas de tarefas de importação

Às vezes, ocorre falha na importação dos arquivos para o Amazon S3. Se ocorrer o seguinte problema, tente as ações especificadas para resolvê-lo. Se ocorrer uma falha na importação de um arquivo, talvez seja necessário importá-lo novamente. Talvez seja necessário um novo trabalho para importá-lo novamente para o Snowball Edge.

Falha ao importar arquivos para o Amazon S3 devido a caracteres inválidos em nomes de objetos

Esse problema ocorrerá se o nome de um arquivo ou pasta tiver caracteres incompatíveis com o Amazon S3. O Amazon S3 tem regras sobre quais caracteres podem ser usados em nomes de objetos. Para obter mais informações, consulte Criar nomes de chave de objeto no Manual do usuário do Amazon S3.

Medida a ser tomada

Se você encontrar esse problema, verá a lista de arquivos e pastas que apresentaram falha na importação no relatório de conclusão de seu trabalho.

Em alguns casos, a lista é grande demais ou os arquivos na lista são muito grandes para serem transferidos pela Internet. Nesses casos, você deve criar um novo trabalho de importação do Snowball, alterar os nomes dos arquivos e das pastas para cumprir as regras do Amazon S3 e transferir os arquivos novamente.

Se os arquivos forem pequenos e não houver um grande número deles, você poderá copiá-los para o Amazon S3 por meio do AWS CLI ou do. AWS Management Console Para obter mais informações, consulte Como carregar arquivos e pastas em um bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

Solução de problemas de trabalho de exportação

Às vezes, ocorrem falhas na exportação de arquivos para sua estação de trabalho. Se ocorrer o seguinte problema, tente as ações especificadas para resolvê-lo. Se ocorrer uma falha na exportação de um arquivo, talvez seja necessário exportá-lo novamente. Talvez seja necessário um novo trabalho para exportá-lo novamente para o Snowball Edge.

Falha ao exportar arquivos para um Microsoft Windows Server

Poderá ocorrer uma falha na exportação de um arquivo para um Microsoft Windows Server se o nome dele ou de uma pasta relacionada estiver em um formato não suportado pelo Windows. Por exemplo, se o nome do arquivo ou da pasta tiver dois-pontos (`:`), ocorrerá uma falha na exportação porque o Windows não permite esse caractere em nomes de arquivos e pastas.

Medida a ser tomada

1. Faça uma lista dos nomes que estão causando o erro. Você pode encontrar os nomes dos arquivos e das pastas com falha na exportação em seus logs. Para ter mais informações, consulte AWS Snowball Edge Registros.

2. Altere os nomes dos objetos no Amazon S3 que estão causando o problema para remover ou substituir os caracteres sem suporte.
3. Se a lista de nomes for grande demais ou se os arquivos na lista forem muito grandes para serem transferidos pela Internet, crie um novo trabalho de exportação especificamente para esses objetos.

   Se os arquivos forem pequenos e não houver um grande número deles, copie os objetos renomeados do Amazon S3 por meio do ou AWS CLI do. AWS Management Console Para obter mais informações, consulte Como fazer download de um objeto de um bucket do S3? no Guia do usuário do Amazon Simple Storage Service.

Histórico do documento

- Versão da API: 1.0
- Última atualização da documentação: 14 de março de 2024

A tabela a seguir descreve alterações importantes feitas no Guia do desenvolvedor do AWS Snowball Edge após julho de 2018. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
O gateway de fita em dispositivos Snowball Edge foi descontinuado	A funcionalidade Tape Gateway não está mais disponível nos dispositivos Snowball Edge.	14 de março de 2024
Interface de arquivo obsoleta	A interface de arquivos não está mais disponível para transferência de dados.	1º de março de 2024
Armazenamento compatível com Amazon S3 em dispositivos da família Snow disponível em dispositivos Snowball Edge de 210 TB otimizados para armazenamento	O armazenamento compatível com o Amazon S3 em dispositivos da família Snow está disponível para armazenamento S3 em dispositivos de 210 TB otimizados para armazenamento do Snowball Edge. Para obter mais informações, consulte Usando o armazenamento compatível com o Amazon S3 em dispositivos da família Snow.	26 de fevereiro de 2024
Inclua AMIs personalizadas ao solicitar dispositivos	Agora, as imagens personalizadas da Amazon Machine podem ser pré-carregadas	15 de novembro de 2023

	durante o pedido AWS Snow Family de trabalhos. Para obter mais informações, consulte Adicionar uma AMI de AWS Marketplace.	
Armazenamento compatível com o Amazon S3 em dispositivos da Família Snow, disponível ao público em geral	O armazenamento compatível com o Amazon S3 em dispositivos da Família Snow é compatível com dispositivos Snowball Edge otimizados para computação. Para obter mais informações, consulte Amazon S3 compatible storage on Snow Family devices.	20 de abril de 2023
Novo Região da AWS suporte	AWS Snowball agora é suportado na região do Oriente Médio (EAU). Para obter informações sobre endpoints para essa região, consulte Snowball Edge Endpoints and Quotas na Referência geral da AWS. Para obter informações sobre envio, consulte Shipping Considerations for Snowball Edge.	6 de março de 2023

Novo Região da AWS suporte	AWS Snowball agora tem suporte na região Ásia-Pacífico (Jacarta). Para obter informações sobre endpoints para essa região, consulte Snowball Edge Endpoints and Quotas na Referência geral da AWS. Para obter informações sobre envio, consulte Shipping Considerations for Snowball Edge.	7 de setembro de 2022
Migração de grandes volumes de dados para o Snowball Edge	O Snowball Edge agora é compatível com a automação de um plano de migração de grandes volumes de dados. Para obter mais informações, se desejar, consulte Large Data Migration (etapas manuais) e Create a Large Data Migration Plan para iniciar a automação.	27 de abril de 2022

Apresentando AWS Snow Device Management	O Snow Device Management permite que você gerencie seu dispositivo Snowball Edge e AWS serviços locais remotamente. Todos os dispositivos Snowball Edge oferecem suporte ao Snow Device Management e ele vem pré-instalado em novos dispositivos na maioria dos lugares em que o Regiões da AWS Snowball Edge está disponível. Para obter mais informações, consulte Usando AWS Snow Device Management para gerenciar dispositivos	27 de abril de 2022
Configuração do NFS para Snowball Edge	Foi adicionada a Configuração do NFS para Snowball Edge para dispositivos otimizados para armazenamento.	21 de abril de 2022
Limites de taxa para o balanceador de carga	O Snowball Edge já é compatível com Limites de taxa para distribuir solicitações em um ambiente de cluster de servidores.	19 de abril de 2022
Suporte para Snowball Edge com Gateway de Fitas	Agora é possível solicitar um dispositivo Snowball Edge especialmente configura do para hospedar o serviço Gateway de Fitas. Essa combinação de tecnologias viabiliza a migração segura de dados em fita off-line.	30 de novembro de 2021

Suporte para configuração do servidor NTP (Network Time Protocol)	Os dispositivos Snowball Edge já são compatíveis com a configuração de servidor NTP (Network Time Protocol).	16 de novembro de 2021
Suporte para transferência de dados off-line do NFS	Os dispositivos Snowball Edge já são compatíveis com a transferência de dados off-line usando NFS. Para obter mais informações, consulte Using NFS for Offline Data Transfer.	4 de agosto de 2021
Novo Região da AWS suporte	Os dispositivos Snowball Edge agora estão disponíveis na África (Cidade do Cabo). Região da AWS Para obter mais informações, consulte Snowball Edge Endpoints and Quotas na Referência geral da AWS. Para obter informações sobre envio, consulte Shipping Considerations for Snowball Edge.	23 de novembro de 2020
Suporte para importação da própria imagem para o dispositivo	Agora é possível importar um snapshot de sua imagem para o dispositivo Snowball Edge e registrá-lo como uma imagem de máquina da Amazon (AMI) compatível com o Amazon EC2. Para obter mais informações, consulte Importing an Image into Your Device as an Amazon EC2 AMI.	9 de novembro de 2020

Novo Região da AWS suporte	Os dispositivos Snowball Edge agora estão disponíveis na Europa (Milão). Região da AWS Para obter mais informações, consulte Snowball Edge Endpoints and Quotas na Referência geral da AWS. Para obter informações sobre envio, consulte Shipping Considerations for Snowball Edge.	30 de setembro de 2020
Reestruturação de conteúdo	Criou uma seção de introdução que se alinha ao Console de Gerenciamento da família AWS Snow fluxo de trabalho e atualizou outras seções para maior clareza. Para obter mais informações, consulte Getting Started with an AWS Snowball Edge.	17 de setembro de 2020
Apresentando AWS OpsHub for Snow Family	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. Para obter mais informações, consulte Usando AWS OpsHub for Snow Family para gerenciar dispositivos Snowball.	16 de abril de 2020

AWS Identity and Access Management (IAM) agora está disponível localmente no AWS Snowball Edge dispositivo	Agora você pode usar AWS Identity and Access Management (IAM) para controlar com segurança o acesso aos AWS recursos em execução no seu AWS Snowball Edge dispositivo. Para obter mais informações, consulte Usar o IAM localmente.	16 de abril de 2020
Apresentação de uma nova opção de dispositivo Snowball Edge otimizado para armazenamento (para transferência de dados)	Agora o Snowball adiciona um novo dispositivo otimizado para armazenamento baseado nos dispositivos atuais de GPU e otimizados para computação. Para obter mais informações, consulte Snowball Edge Device Options.	23 de março de 2020
Suporte à validação de tags do NFC	Os dispositivos Snowball Edge otimizados para computação (com ou sem a GPU) têm tags NFC integradas. Você pode digitalizar essas tags com o aplicativo AWS Snowball Edge Verification, disponível no Android. Para obter mais informações, consulte Validação de tags NFC.	13 de dezembro de 2018

Os grupos de segurança agora estão disponíveis para instâncias de computação	Os grupos de segurança em dispositivos Snowball Edge são semelhantes a grupos de segurança na Nuvem AWS, com algumas diferenças sutis. Para obter mais informações, consulte Security Groups in Snowball Edge Devices.	26 de novembro de 2018
Apresentação da atualização on-premises	Agora é possível atualizar o software que possibilita que um dispositivo Snowball Edge seja executado no ambiente local. Observe que as atualizações locais exigem uma conexão com a Internet. Para obter mais informações, consulte Updating an Snowball Edge.	26 de novembro de 2018
Apresentação das novas opções de dispositivos Snowball Edge	Os dispositivos Snowball Edge são fornecidos em três opções: otimizados para armazenamento, otimizados para computação e com GPU. Para obter mais informaçõ es, consulte Snowball Edge Device Options.	15 de novembro de 2018
Novo Região da AWS suporte	Os dispositivos Snowball Edge já estão disponíveis na Ásia-Pacífico (Mumbai). Observe que as instâncias de computação e AWS Lambda desenvolvidas por não AWS IoT Greengrass são suportada s nessa região.	24 de setembro de 2018

Apresentação de suporte para instâncias de computação do Amazon EC2 em dispositivos Snowball Edge	AWS Snowball agora oferece suporte a trabalhos locais usando instâncias computacionais do Amazon EC2 executadas em dispositivos Snowball Edge.	17 de julho de 2018
Conteúdo da solução de problemas aprimorado	O capítulo sobre solução de problemas foi atualizado e reorganizado.	11 de julho de 2018

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.